ISSN 2313-1527 (PRINT)
ISSN 2313-1535 (ONLINE)

IJEIE

International Journal of Electronics
and Information Engineering

Vol. 9, No. 2 (Dec. 2019)

INTERNATIONAL JOURNAL OF ELECTRONICS & INFORMATION ENGINEERING

PUBLISHING OFFICE

Min-Shiang Hwang
Department of Computer Science & Information Engineering, Asia University, Taichung 41354, Taiwan, R.O.C.
Email: mshwang@asia.edu.tw

International Journal of Electronics and Information Engineering is published both in traditional paper form (ISSN 2313-1527) and in Internet (ISSN 2313-1535) at http://ijeie.jalaxy.com.tw

PUBLISHER: Candy C. H. Lin

23-75, P.O. Box, Taichung, Taiwan 40199, R.O.C.

International Journal of Electronics and Information Engineering

Vol. 9, No. 2 (Dec. 1, 2018)

Analog Circuit Design Using A Single EXCCCII

Sudhanshu Maheshwari

(Corresponding author: Sudhanshu Maheshwari)

Department of Electronics Engineering, Aligarh Muslim University
Aligarh, India
(Email: sudhanshu_maheshwari@rediffmail.com)

(Received Aug. 14, 2018; revised and accepted Sept. 14, 2018)

Abstract

This paper presents a brief review on the advances in analog signal processing, with special emphasis on current-mode building blocks and their applications. The developments and recent trends are discussed and some novel analog signal processing circuits are proposed. The new proposed circuits employ a single Extra-X Current Controlled Conveyor and are verified through simulation results. The main focus is on the realization of simple, tunable analog circuits suited for CMOS integration.

Keywords: Analog Signal Processing; Current-Mode Circuits; Electronic Circuit Design

1 Introduction

All practical communication and instrumentation applications demand high performance circuits for processing of natural signals and their faithful interpretation by the humanity. More recently the use of sensors have further led to the development of efficient circuits to be employed, before applying digital techniques. Thus, the area of analog signal processing has become one of the potential research areas. The growing dependencies on digital techniques have led to an ever increasing demand for analog interfaces.

The design of circuits with high accuracy, good dynamic range, low supply operation, low power and large bandwidth requirements have led to the growing need of processing analog signals in current-mode, besides the more conventional voltage-mode. The use of current-mode circuits has thus increased [7, 8, 17–19]. The developments and recent trends are deliberated herein, with subsequent sections presenting a brief review of advances, along with some most recent developments.

2 Track of Analog Building Blocks

Early twentieth century witnessed the era of analog computing, where, operational amplifier and passive components fulfilled the task of performing variety of computations. The need of programming the functions realized, led to the development of operational trans-conductance amplifiers based analog systems. The dynamic range demands led to further researches, most important of them being the introduction of current conveyors. These were like both the operational amplifier and operational trans-conductance amplifiers together and even more, by allowing excellent voltage and current following capabilities simultaneously. With growing needs of high performance analog circuits and systems, the current conveyors became a versatile block of choice for analog signal processing. Moreover, in recent times, the impetus has again shifted towards analog computing. The role of field programmable analog arrays is going to increase in near future. The need of electronically tunable analog blocks has become a mandatory requirement for most of the applications.

The useful analog functions range from simple interfaces to amplifying and linear computing units, along with non-linear functions like comparison, detection, multiplication and so on. Nowadays, the current conveyor applications encompass linear and non-linear functions, capable of implementing a workable analog sub-system/system. The current-mode active building blocks have gone through a continuous phase of evolvement, in form of current conveyors, differential form of current conveyors, tunable current conveyors, hybrid of two current-mode units and many more. For instance, besides the more conventional CCII, DVCC, FDCCII, CCCII and CCCCTA are some of the very popular building blocks. Recently, EXCCII and tunable EXCCII have also emerged as potential choice [2–4, 9, 10, 13–16, 21]. On the other hand, the current mode building blocks continue to find recent space in literature [1, 5, 6, 20].

3 Brief Review

The developments aiming for high performance analog sub-systems have witnessed migration from CCII [17–19] to its tunable version in CCCII [4, 7, 8], which resulted in electronically tunable analog circuits and systems. The availability of CCCII made it feasible to realize electronically tunable analog signal processing circuits, which covered simple tunable components, amplifiers, filters oscillators and a variety of other applications. Another direction of research was motivated by the benefits of differential signal processing, which led to the design and applications of DVCC and FDCCII [2, 3, 13, 15]. The DVCC found favor for realizing diverse electronic circuit functions. The emergence of CMOS circuitry for DVCC led to its wide applications for simple first order functions, biquad filters, oscillators. The more complicated block, FDCCII was equally well exploited for realizing analog filters and oscillators with attractive features.

The DXCCII was introduced later, but soon found many applications; and several enhancements were made to it, that ensured wider versatility of this block. The versatility of active building block was the cause of popularity of DXCCII [14,21], which underwent some interesting modifications as well. On the other hand, a second degree of tunability was imparted to CCCII, by using CCCCTA [16]. With electronic tuning as the motivating factor, CCCCTA was employed in a large number of filtering applications. The motive was to provide independent and electronic control over the parameters of the designed filters. Very recently, EXCCII was proposed to reduce the circuit complexity of realizations built around various current-mode active elements. The EXCCII with buffered output and EXCCCII were also suggested as possible building blocks, for extending the domain of EXCCII based circuits to electronically tunable ones [9]. The applications and advantages of EXCCII/EXCCCII are attracting most recent attention in literature [10].

Out of the above mentioned building blocks, the DVCC, FDCCII, DXCCII and EXCCII are useful for differential realizations, but lack inherent tuning. CCCII and CCCCTA provide electronically tunable realizations. Nonetheless, effective solutions to impart tuning have also been discovered for DVCC, DXCCII and EXCCII based realizations.

4 New Proposed Circuits

In order to further advance the existing knowledge on EXCCII/EXCCCII, a simple yet novel circuit is next introduced, which employs an EXCCCII, which is characterized by port relationship given in Equation (1). The details of this active element are already available in recent literature [9,10].

$$i_y = 0; v_{x_i} = v_y + i_{x_i} R_{x_i}; i_{Z_i} = i_{x_i}; i = 1, 2. \tag{1}$$

The proposed circuit is shown in Figure 1, which realizes a simple voltage-mode, electronically tunable, first order filter with all-pass characteristics. The circuit in Figure 1 uses Z_2- stage with a current gain of '2', whereas, the Z_1 stage is un-used. The voltage transfer function is given as below.

$$\frac{v_o}{v_{in}} = (\frac{s - 1/R_x C}{s + 1/R_x C}) \tag{2}$$

In deriving Equation (2), it is assumed that the two X-stages are identical and exhibit equal intrinsic resistances ($R_{x_1} = R_{x_2} = R_x$). It may be noted that Rx depends on the bias current of EXCCCII with inverse square root relationship [10]. The circuit provides a constant unity gain at all frequencies, while a phase shift dependent on frequency, which is as below.

$$\phi = 180^o - 2tan^{-1}(\omega R_x C) \tag{3}$$

It is evident that the phase shift depends on Rx, which is electronically tunable through the bias current I_o of EXCCCII. The proposed all-pass filter has useful applications as phase-shifter, delay equalizer, design of higher order filters and oscillators. The simulation results for the circuit of Figure 1 are shown in Figures 2-5. The circuit is designed using C=10pF and bias current $I_o = 70\mu A$. The frequency response is given in Figure 2, showing unity gain and frequency dependent phase, with the pole-frequency of 11.8MHz; whereas the time domain input at pole-frequency and 90^o phase shifted output are shown in Figure 3. The output spectrum is given in Figure 4, showing at least -30dB suppression of harmonics. The electronic tuning aspect is given in Figure 5, where, constant gain and varying phase-shift is seen, which is being controlled by the bias current of EXCCCII. It may be noted that the bias current is varied in steps of 10 μA, from 50-90 μA.

Another application circuit of EXCCCII is next proposed, which is shown in Figure 6. The circuit realizes a precision full-wave rectifier, which finds interesting applications in communication and instrumentation. The additional Z2+ stage provides the control voltage for switch transistor M_s, which conducts during positive cycle of input signal, causing the output to follow the input. For the negative cycle, the voltage at Z2+ is negative, and the switch is off, thus the output phase reverses with respect to input. A sample result is given in Figure 7, where a 10 KHz input signal is shown along with its rectified output.

Another interesting application of EXCCCII is next shown in obtaining binary phase shift keying modulation. The circuit is given in Figure 8. The modulating signal controls the switch Ms, and accordingly, the carrier signal switches between two phases, resulting in binary phase shift keying modulation. The modulating signal (V_m), the carrier signal (V_c) and the resulting output (V_o), as marked in Figure 8 are shown plotted in Figure 9, which justify the circuit's functionality.

5 Conclusion

This paper presents a brief review of analog signal processing trends, with emphasis on the developments in current mode analog building blocks. Some interesting, simple yet novel circuits are also proposed,

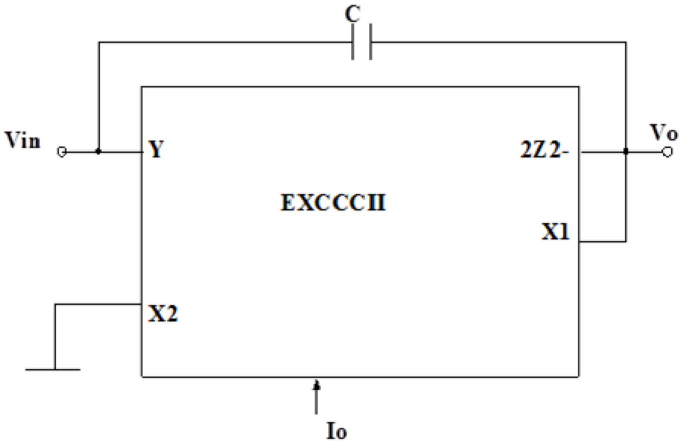


Figure 1: Proposed all-pass filter of first order

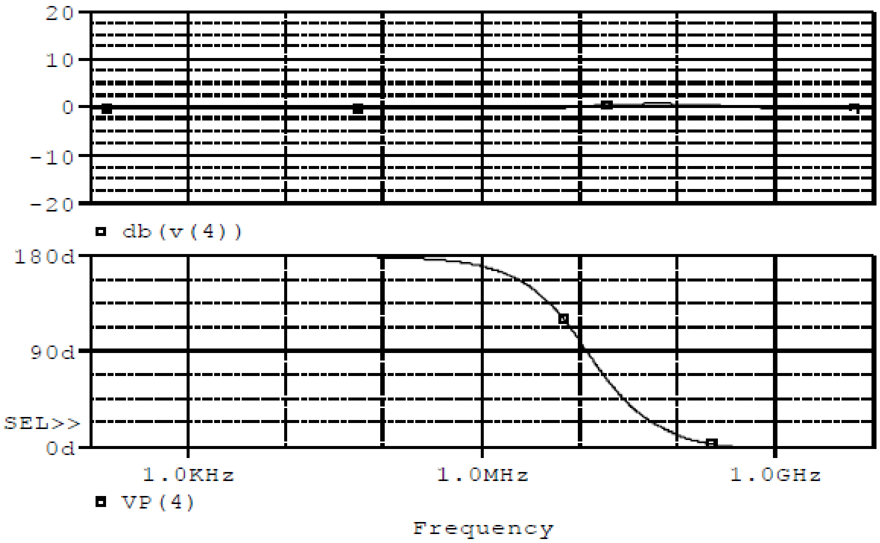


Figure 2: Gain and Phase plots for the circuit of Figure 1

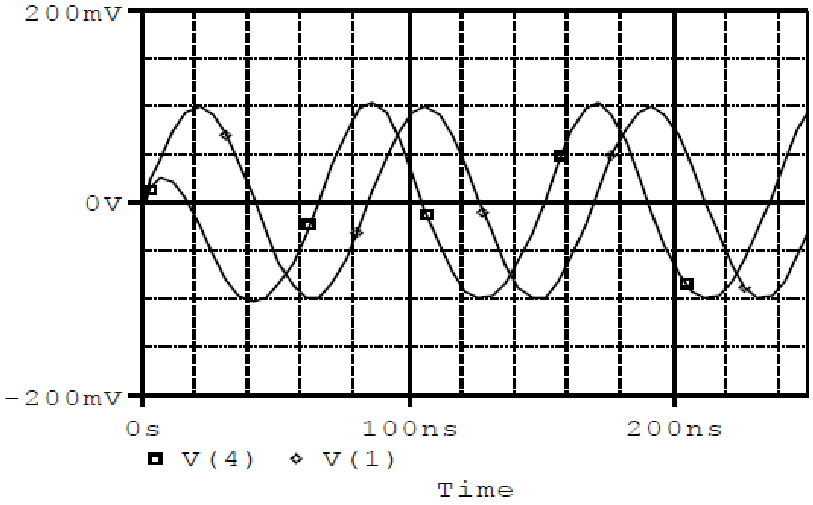


Figure 3: Input v(1) at 11.8 MHz and 90^o phase shifted output V(4)

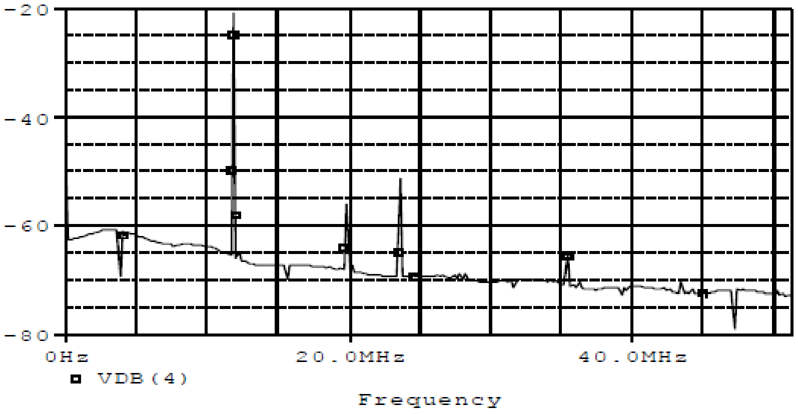


Figure 4: Spectrum of output showing at least -30dB suppression of harmonics

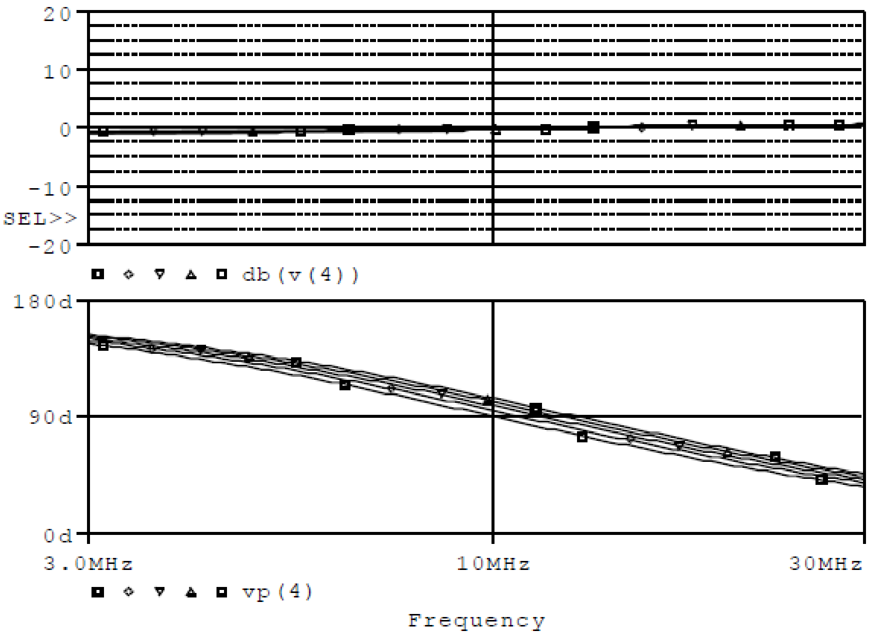


Figure 5: Constant gain and tunable phase for varying I_o

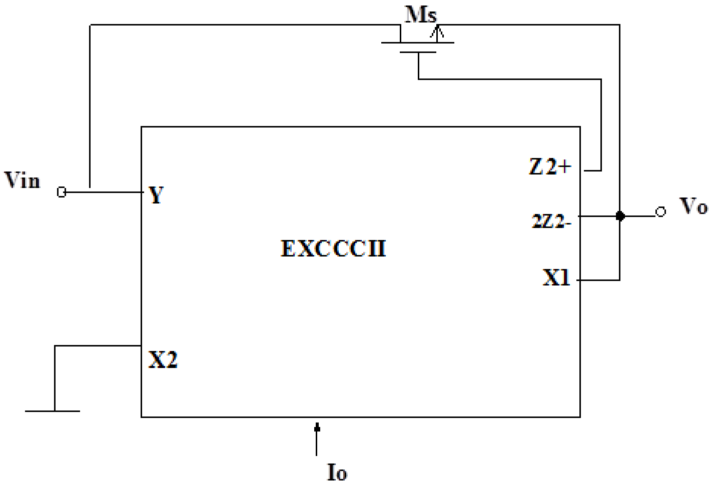


Figure 6: Proposed full wave precision rectifier circuit

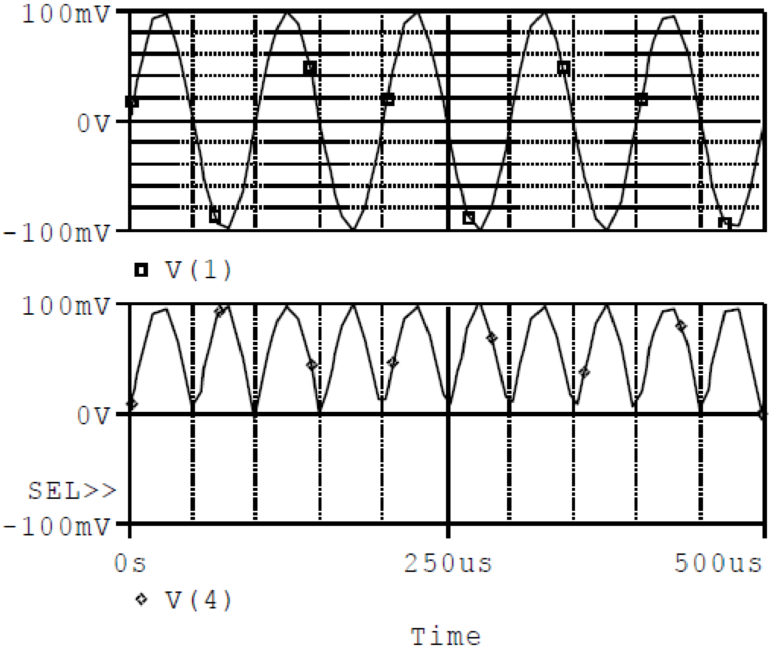


Figure 7: Input and rectified output for Figure 6

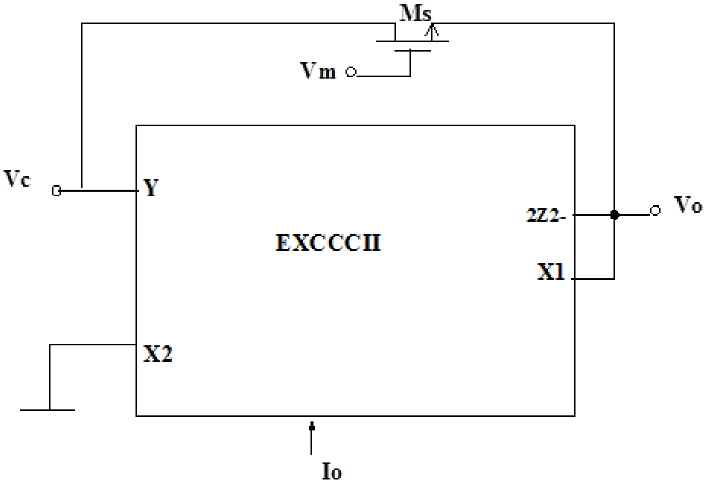


Figure 8: Proposed BPSK circuit

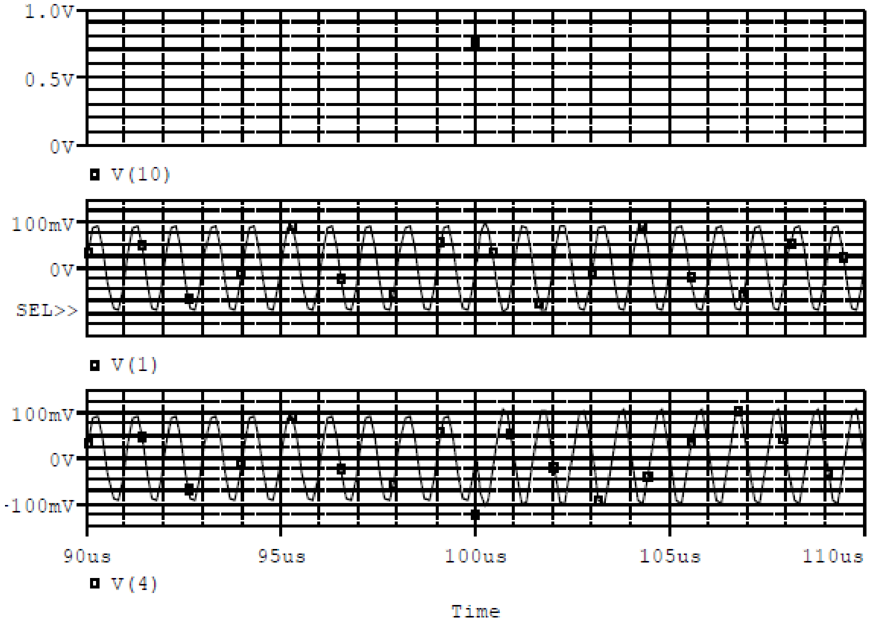


Figure 9: Modulating signal (5 KHz), carrier signal (1 MHz) and resulting BPSK signal

which employ a relatively new analog building block, extra-X current conveyor. The proposed application circuits realize electronic functions, namely all-pass filter, precision rectifier and binary phases shift keying modulation, whose functionality is verified through simulation results. The area of analog signal processing is expected to benefit from the use of extra-X current conveyor, with increasingly diverse applications in electronics and communication systems. The appearance of this work is expected to promote related studies' coverage in the International Journal of Electronics and Information Engineering journal, which is presently missing.

References

[1] H. P. Chen, Y. S. Hwang, Y. T. Ku, "A systematic realization of third-order quadrature oscillator with controllable amplitude," *AEU International Journal of Electronics and Communications*, vol. 79, pp. 64-73, 2017.

[2] A. A. El-Adawy, A. M. Soliman, H. O. Elwan, "A novel fully differential current conveyor and applications for analog VLSI," *IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing*, vol. 47, no. 4, pp. 306-313, 2000.

[3] H. O. Elwan, A. M. Soliman, "Novel CMOS differential voltage current conveyor and its applications," *IEE Proceedings - Circuits, Devices and Systems*, vol. 144, no. 3, pp. 195-200, 1997.

[4] A. Fabre, O. Saaid, F. Wiest, C. Boucheron, "High frequency applications based on a new current controlled conveyor," *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, vol. 43, no. 2, pp. 82-91, 1996.

[5] S. J. G. Gift, B. Maundy, "Versatile precision full-wave rectifiers for instrumentation and measurements," *IEEE Transactions on Instrumentation and Measurementm*, vol. 56, no. 5, pp. 1703-1710, 2007.

[6] J. W. Horng, "DVCCs based high input impedance voltage-mode first-order allpass, highpass and lowpass filters employing grounded capacitor and resistor," *Radioengineering Journal*, vol. 19, no. 4, pp. 653-656, 2010.

[7] I. A. Khan, M. H. Zaidi, "Multifunctional translinear-C current-mode filter," *International Journal of Electronics*, vol. 87, no. 9, pp. 1047-1051, 2000.

[8] I. A. Khan, M. H. Zaidi, "A novel ideal floating inductor using translinear conveyors," *Active and Passive Electronic Components*, vol. 26, no. 2, pp. 87-89, 2002.

[9] S. Maheshwari, "Current conveyor all-pass sections: brief review and novel solution," *The Scientific World Journal*, DOI. 10.1155/2013/429391, 2013.

[10] S. Maheshwari, "Voltage-mode full-wave precision rectifier and an extended application as ASK/BPSK circuit using a single EXCCII," *AEU International Journal of Electronics and Communications*, vol. 84, pp. 234-241, 2018.

[11] S. Maheshwari, "Tuning approach for first order filters and new current-mode circuit example," *IET Circuits Devices and Systems*, vol. 12, no. 4, pp. 478-485, July 2018.

[12] S. Maheshwari, "Some analog filters of reduced complexity with shelving and multifunctional characteristics," *Journal of Circuits Systems and Computers*, vol. 27, no. 10, 1850150, 2018.

[13] S. Maheshwari, B. Chaturvedi, "High output impedance CMQOs using DVCCs and grounded components," *International Journal of Circuit Theorem And Applications*, vol. 39, no. 4, pp. 427-435, 2011.

[14] S. Maheshwari, B. Chaturvedi, "Additional high input low output impedance analog networks," *Active and Passive Electronic Components*, vol. 2013, Article ID 574925, 9 pages, 2013.

[15] S. Maheshwari, J. Mohan, D. S. Chauhan, "Novel cascadable all-pass/notch filters using a single FDCCII and grounded capacitors," *Circuits, Systems, and Signal Processing*, vol. 30, no. 3, pp 643-654, June 2011.

[16] S. Maheshwari, S. V. Singh, D. S. Chauhan, "Electronically tunable low-voltage mixed-mode universal biquad filter," *IET Circuits Devices and Systems*, vol. 5, no. 3, pp. 149-158, May 2011.

[17] A. S. Sedra, K. C. Smith, "A second-generation current conveyor and its applications," *IEEE Transactions on Circuit Theory*, vol. 17, no. 1, pp. 132-134, 1970.

[18] C. Toumazou, F. J. Ledgey, "Universal active filter using current conveyors," *Electronics Letters*, vol. 22, no. 12, pp. 662-664, 1986.

[19] B. Wilson, "Recent developments in current conveyors and current-mode circuits," *IEE Proceedings G (Circuits, Devices and Systems)*, vol. 137, no. 2, pp. 63-77, April 1990.

[20] J. Wu, E. I. El-Masry, "Design of current-mode ladder filters using coupled-biquads," *IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing*, vol. 45, no. 11, pp. 1445-1454, 1998.

[21] A. Zeki, A. Toker, "The dual-X current conveyor (DXCCII): A new active device for tunable continuous-time filters," *International Journal of Electronics*, vol. 89, no. 12, pp. 913-923, 2003.

Biography

Sudhanshu Maheshwari works as Professor in the Department of Electronics Engineering, A.M. U., Aligarh, India. He has published more than 100 referred International Journal papers and large number of conference papers in the area of current-mode analog signal processing circuits.

An Efficient Public Key Cryptosystem

Maheshika W.D.M.G. Dissanayake

(Corresponding author: Maheshika W.D.M.G. Dissanayake)

Department of Computer Engineering, Faculty of Engineering, University of Peradeniya, Sri Lanka
135/1, Inner Harbour Road, Trincomalee, Sri Lanka
(Email: maheshi14d@gmail.com)

(Received July 2, 2018; revised and accepted Oct. 22, 2018)

Abstract

In this paper a new, efficient public key cryptosystem is presented. This system is based on some special behaviors of powers of 2 and matrices. This is a practical method. The introduced public key cryptosystem is very simple. But, difficult to find the sending message in easily. There are two public keys and two private keys in this new cryptosystem. Therefore two ciphertexts and two plaintexts are in the cryptosystem. A new modulus is introduced for encryption and decryption process and it is very familiar to computer science. In this method we hide the message in a matrix. This situation makes a difficult puzzle for adversaries.

Keywords: ElGamal Cryptosystem; IND Security; OW Security; Public Key Cryptosystem; RSA Cryptosystem

1 Introduction

Introducing a simple and practical public key cryptosystems is a very important and necessary need in world. Solving time, cost and complexity problems of cryptosystems are ongoing research areas in Cryptography. Many countries are trying to find a better public key cryptosystem and fund more to research projects based on developing security of public key cryptosystems. There are many public key cryptosystems have been developed in world. But, we cant trust 100 % none of those systems yet. These also take high cost, high complexity and low speed. Therefore, almost all are very suitable for short messages. However, some public key cryptosystems are very popular and useful. Example: RSA public key cryptosystem, ElGamal public key cryptosystem.

The proposed method with numerical examples, proof, procedure, key generation and computational complexity are presented in Section 2. Sections 3 discusses the security of the proposed public key cryptosystem.

Definition 1. *The set of integers $\{0, 1, 2, \cdots, n-1\}$ is defined as the integers mod n and denoted by Z_n.*

Definition 2. *The multiplicative group of Z_n is $Z_n^* = \{a \in Z_n | \gcd(a, n) = 1\}$.*

Definition 3. *Euler's 1st Theorem: If a and n are coprime then, $a^{\phi(n)} \bmod n \equiv 1$.*

Definition 4. *Euler's 2nd Theorem: If $n = p \times q$, $a < n$, k is an integer, then $a^{k \times \phi(n)+1} \bmod n \equiv a$; Here it is removed that a and n are coprime.*

Definition 5. *A public key cryptosystem is a tuple of probabilistic polynomial - time algorithm (Kgen, Enc, Dec) such that:*

1) *Kgen is a probabilistic key generation algorithm that takes as input 1^k for a security parameter $k \in N$ and returns a public key pk and a secret key sk. The public key pk defines a space M, called message space.*

2) *Enc is a probabilistic algorithm that takes as input a public key pk and a message $m \in M$ and returns a ciphertext c.*

3) *Dec is a deterministic algorithm that takes as input a secret key sk and a ciphertext c, and returns a message m or the reject symbol $\perp$. Moreover a further fundamental property is required correctness. We want that for every $k \in N$, every pair $(pk, sk) \leftarrow Kgen(1^k)$, and for every message $m \in M$, the following equation holds:*

$$Pr[Dec(sk, Enc(pk, m)) = m] = 1.$$

Definition 6. *One-Wayness (OW): A public key cryptosystem is said to be one-wayness if for all probabilistic polynomial time algorithms A, for every $\alpha > 0$ and sufficiently large k,*

$$Pr[A(pk, c) = Dec(sk, c) = m] < 1/k^{\alpha}.$$

Where, $c \leftarrow Enc(pk, m), (pk, sk) \leftarrow Kgen(1^k)$ and m is any message in message space M.

1.1 RSA public key cryptosystem [11]

This public key cryptosystem was introduced by R.L. Rivest, A. Shamir and L. Adleman in 1978. This system was the first practical public key cryptosystem. Following is the RSA scheme.

1) Two large prime numbers are generated. Let p and q.

2) Modulus n is generated by multiplying p and q.

3) The totient of n is $\phi(n) = (p-1).(q-1)$ is calculated.

4) Public Key - A prime number e is selected. where $3 \leq e \leq \phi(n)$ and $\gcd[e, \phi(n)] = 1$; gcd means greatest common divisor. Private Key: The inverse of e with respect to mod $\phi(n)$ is calculated.

5) The RSA function for message m and key k is, $F(m, k) \equiv m^k \bmod n$. Encryption: $m^e \bmod n \equiv c$. Decryption: $c^d \bmod n \equiv m$.

RSA is a very slow cryptosystem for long messages. Therefore, it is suitable for small messages. The security of RSA is based on the infeasibility of factorization large n. However, RSA does not immune for IND-CPA, CCA1 or CCA2. But, the security of RSA can be increased with combining some cryptographic schemes. For an example, RSA is IND-CPA, CCA1 and CCA2 secure with OAEP (Optimal Asymmetric Encryption Padding). But, note that the RSA will failure with a single bit error during the transmission. Therefore, we need a clear transmission media !

1.2 The ElGamal cryptosystem [13]

This public key cryptosystem was introduced by Taher Elgamal in 1985.

Step 1: Global elements: Let any large prime number p and a primitive root g of p.

Step 2: Decryption key: x-private, Calculate $g^x \bmod p$, where $x \in Z$. Publish $(p, g, g^x \bmod p)$.

Step 3: Encryption: Let the message is m; $(0 < m < p)$ and choose y-private $(0 < y < p)$. Compute $b \equiv g^y \bmod p$. Then, $c \equiv m.a^y \bmod p$. Send $(b,\ c)$.

Step 4: Decryption: Compute $b^x \bmod p \equiv a^y$. Then, $m \equiv a^{y^{-1}} \bmod p$. The security of ElGamal cryptosystem is depended on the discrete logarithm problem. This system is also very suitable for small messages. It is IND-CPA secure. But, it is not secure for CCA.

2 Proposed Cryptosystem

In this paper, I get the message in a numerical form. But, we can get any standard representation for a large message. Consider we have to encrypt a message m. In the proposed method, the public encryption key is $(e, r, 2^q)$. Here e and r are any large prime numbers less than q and q is a very large positive integer. We should select another prime number $g(< 2m)$ and set the message m and g in a 2×2 matrix X as the determinant of the matrix is odd. We do not encrypt the message m by raising it to the eth power modulo 2^q.We encrypt the determinant of the matrix by raising it to the eth power modulo 2^q. We also have to send g for the decryption. Because of without g, we can not get the message m. We also encrypt g by raising it to the rth power modulo 2^q. Now, we have two ciphertexts C_1 and C_2. C_1 is also in a 2×2 matrix Y. When we decrypt determinant of Y raise it to another power d modulo 2^q and decrypt B raise it to another power s modulo 2^q, we can find the message m. So the decryption key is $(d, s, 2^q)$. There are two encryption algorithms and two decryption algorithms are in this cryptosystem.

Encryption Algorithm 1:
E(Determinant of Y) $\equiv [(\text{Determinant of } X)^e] \bmod 2^q$, for message m and g.

Encryption Algorithm 2:
$E(B) \equiv [A^r] \bmod 2^q$, only for g.

Decryption Algorithm 1:
D(Determinant of X) $\equiv [(\text{Determinant of } Y)^d] \bmod 2^q$, for ciphertext C_1.

Decryption Algorithm 2:
$D(A) \equiv [B^s] \bmod 2^q$, for ciphertext C_2.

You can use this system with following steps.

1) Let any large integer p and another large integer $q \in Z$ such that $p \leq q$ and $a^{2^p} \bmod 2^q \equiv 1$, which are chosen at randomly; a is odd. (The selection of p and q is very important).

2) Calculate 2^p and 2^q. (here, 2^q will be public).

3) Choose prime numbers e and r, such that. $2 \leq (e, r) \leq 2^p$ (for public keys); Here $\gcd[e, 2^p]$ and $\gcd[r, 2^p]$ are always 1. (gcd means greatest common divisor).

4) Determine d as modular multiplicative inverse of $e \bmod 2^p$ and s as modular multiplicative inverse of $r \bmod 2^p$ (for private keys).

$$ed \bmod 2^p \equiv 1$$
$$rs \bmod 2^p \equiv 1.$$

Again it is essential that $(ed)^{2^p} \bmod 2^q \equiv 1$ and $(rs)^{2^p} \bmod 2^q \equiv 1$.

5) Then for the message m, we should hide the message in a matrix as follows: The value of g should be odd and less than to *2m*. The determinant of the matrix should be less than to 2^p. Then the determinant of the matrix is odd. Let the matrix is X,

$$X = \begin{pmatrix} m & g \\ 1 & 2 \end{pmatrix}$$

Here m is the message. m and 2 should be in the main diagonal of the matrix. The determinant of X is always odd.

6) Calculate: determinant(X) $= 2m - g$:

Encryption: Determinant (Y) $\equiv [(determinant(X))^e] \bmod 2^q$; Here determinant (X) is always being odd number.

$$k \equiv [g^r] \bmod 2^q.$$

7) Decryption: Determinant (X) $\equiv [(determinant(Y))^d] \bmod 2^q$:

$$g \equiv [k^s] \bmod 2^q.$$

Now we can calculate the message m easily. Because of we know the value g.

$$m = (determinant(X) + g)/2.$$

2.1 Examples

Example 1. *Let $p = 7$ and $q = 8$; $(a^{2^7} \bmod 2^8 \equiv 1)$; $2^p = 128$ and $2^q = 256$. Let the public keys $e = 11$ and $r = 7$; $(\gcd(11, 128) = 1$ and $\gcd(7, 128) = 1)$. Then for the private keys d and s, $ed \bmod 128 \equiv 1$. i.e. $11 \times d \bmod 128 \equiv 1$; $d = 35$; $rs \bmod 128 \equiv 1$. i.e. $7 \times s \bmod 128 \equiv 1$; $s = 55$. Note that $(11 \times 35)^{2^7} \bmod 2^8 \equiv 1$ and $(7 \times 55)^{2^7} \bmod 2^8 \equiv 1$.*

Let the message is $m = 14$ and $g = 21$. Then we set the message in a 2×2 matrix as the determinant of the matrix is odd.

$$X = \begin{pmatrix} 14 & 21 \\ 1 & 2 \end{pmatrix}$$

Determinant $(X) = (14 \times 2) - 21 = 7$. The encryption equations, Determinant $(Y) \equiv [(determinant(X))^e] \bmod 2^q$; Determinant (Y) $\equiv 7^{11} \bmod 256 \equiv 151$; $k \equiv [g^r] \bmod 2^q$; $k \equiv 21^7 \bmod 256; \equiv 29$.

The decryption equations, Determinant (X) $\equiv [(determinant(Y))^d] \bmod 2^q$. Determinant (X) $\equiv 151^{35} \bmod 256; \equiv 7$; $g \equiv [k^s] \bmod 2^q$; $g \equiv 29^{55} \bmod 256; \equiv 21$; $2m - g = Determinant(X)$; $2m - 21 = 7$; $m = 14$.

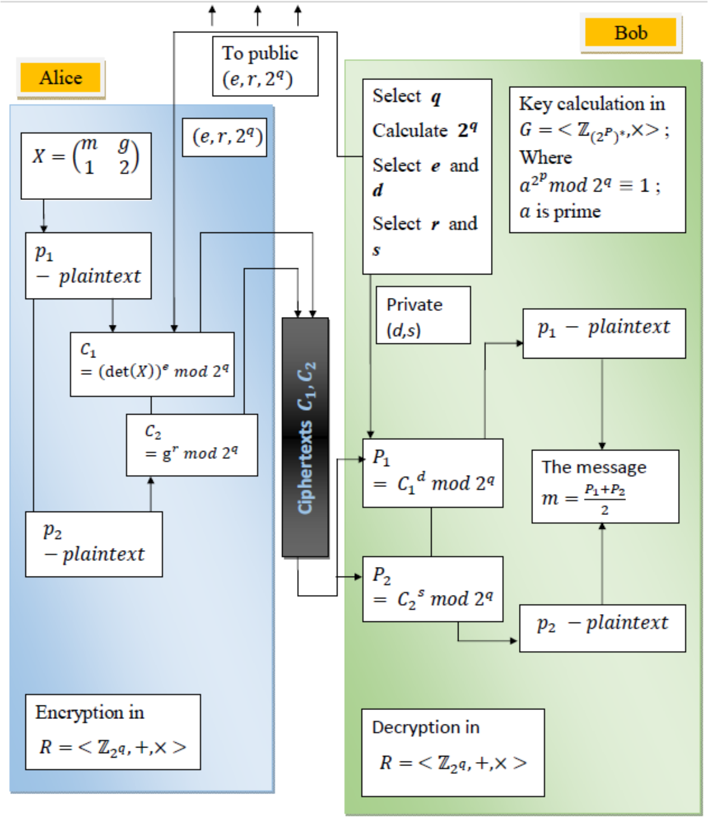


Figure 1: Procedure of the introduced cryptosystem

Example 2. *Let $p = 6$ and $q = 10$; (a^{2^6} mod $2^{10} \equiv 1$); $2^6 = 64$ and $2^{10} = 1024$. Let the public keys e = 19 and r = 29; (no matter $\gcd(19, 64) = 1$ and $\gcd(29, 64) = 1$). Then for the private keys d and s, ed mod $64 \equiv 1$. i.e. $19 \times d$ mod $64 \equiv 1$; d = 27; rs mod $64 \equiv 1$. i.e. $29 \times s$ mod $128 \equiv 1$; s = 53.*

Let the message is m = 33 and g = 7. Then we set the message in a 2×2 matrix as the determinant of the matrix is odd.

$$X = \begin{pmatrix} 33 & 7 \\ 1 & 2 \end{pmatrix}$$

Determinant $(X) = (33 \times 2) - 7 = 59$. The encryption equations, Determinant $(Y) \equiv [(determinant(X))^e]$ mod 2^q. Determinant $(Y) \equiv 59^{19}$ mod $1024 \equiv 387$; $k \equiv [g^r]$ mod 2^q; $k \equiv 7^{29}$ mod $1024 \equiv 871$.

The decryption equations, Determinant $(X) \equiv [(determinant(Y))^d]$ mod 2^q. Determinant $(X) \equiv 387^{27}$ mod $1024 \equiv 59$; $g \equiv [k^s]$ mod 2^q; $g \equiv 871^{53}$ mod $1024 \equiv 7$; $2m - g = Determinant(X)$; $2m - 7 = 59$; $m = 33$.

2.2 The Procedure

The procedure of the proposed public key cryptosystem is shown by Figure 1.

2.3 Proofs

Theorem 1. *For all a, a is odd and $n \in Z$, then $a^{2^n} \bmod 2^n \equiv 1$.*

Proof. Since p is an odd number we can write p as, $p = 2x - 1; x \in z$, when $x = 1$, $2x - 1 = 1$. i.e. $1^{2^n} \bmod 2^n \equiv 1$ is obviously true.

Assume that the theorem $p^{2^n} \bmod 2^n \equiv 1$ is true. i.e. $(2x-1)^{2^n} \bmod 2^n \equiv 1$ is true. (Next odd number, $P + 2 = 2x - 1 + 2 = 2x + 1 or [2(x+1) - 1] = 2x + 1$). Then, By the Binomial Theorem,

$$\begin{aligned}(2x+1)^{2^n} &= (2x)^{2^n} + \binom{2^n}{1}(2x)^{2^n-1} + \binom{2^n}{2}(2x)^{2^n-2} + \ldots + \binom{2^n}{2^n-1}(2x) + 1 \\ &= (2)^{2^n}(x)^{2^n} + \binom{2^n}{1}(2x)^{2^n-1} + \binom{2^n}{2}(2x)^{2^n-2} + \ldots + \binom{2^n}{2^n-1}(2x) + 1 \\ &= 2^n 2^{2^n-n}(x)^{2^n} + \binom{2^n}{1}(2x)^{2^n-1} + \binom{2^n}{2}(2x)^{2^n-2} + \ldots + \binom{2^n}{2^n-1}(2x) + 1.\end{aligned}$$

Taken mod2^n, $(2x+1)^{2^n} \bmod 2^n \equiv 1$. i.e. $(p+2)^{2^n} \bmod 2^n \equiv 1$. Since we also know that $p^{2^n} \bmod 2^n \equiv 1$ is true. Then for next odd number $(p+2)^{2^n} \bmod 2^n \equiv 1$ as desired. □

Proof of the new cryptosystem:

Proof. Since we choose p and q as $a^{2^p} \bmod 2^q \equiv 1$ and $p < q$, $a^{2^p} \bmod 2^q \equiv 1$; $a^{k2^p} \bmod 2^q \equiv 1$; $aa^{k2^p} \bmod 2^q \equiv a$; $a^{k.2^p+1} \bmod 2^q \equiv a$.

Now we can prove this cryptosystem using above theorem. $P_1 = C_1^d \bmod 2^q = ((det(X))^e \bmod 2^q)^d \bmod 2^q = (det(X))^{e.d} \bmod 2^q$. Since e and d are odd numbers and inverses of mod2^p:

$$\begin{aligned}ed &= k_1.2^p + 1 \\ P_1 &= (det(X))^{ed} \bmod 2^q \\ &= (det(X))^{k_1.2^p+1} \bmod 2^q.\end{aligned}$$

Using above theorem, $P_1 = det(X) \bmod 2^q$. Similarly, $P_2 = C_2^s \bmod 2^q = (g^r \bmod 2^q)^s \bmod 2^q = (g)^{rs} \bmod 2^q$. Since r and s are odd numbers and inverses of mod2^p:

$$\begin{aligned}rs &= k_2 2^p + 1 \\ P_2 &= (g)^{rs} \bmod 2^q \\ &= (g)^{k_2.2^p+1} \bmod 2^q.\end{aligned}$$

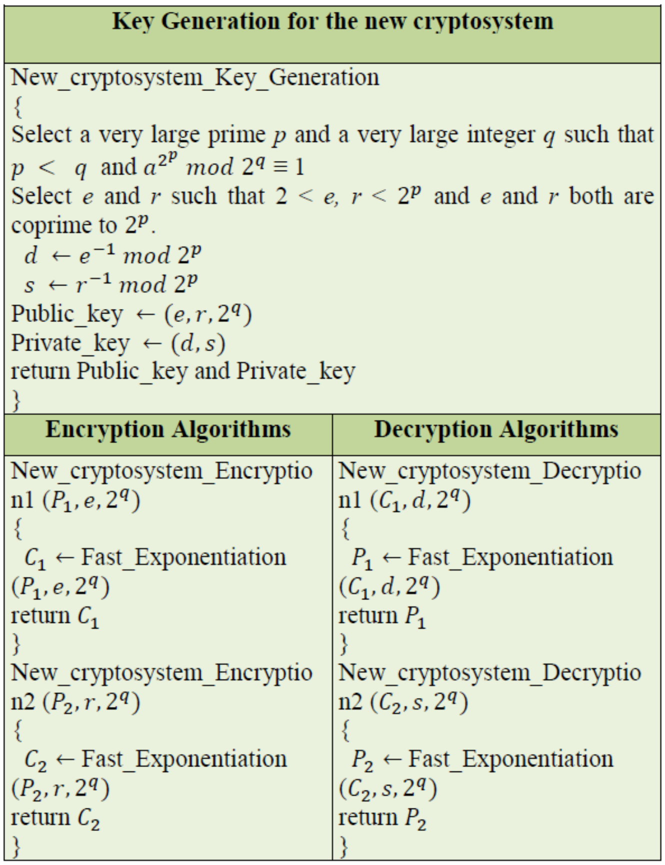
Using above theorem, $P_2 = g \bmod 2^q$. Then, $(P_1 + P_2)/2 = (det(X) + g)/2 = (2m - g + g)/2 = m$. □

2.4 Key Generation for the New Cryptosystem

Key generation of the proposed public key cryptosystem is shown by Figure 2.

2.5 Computational Complexity

This cryptosystem uses modular exponentiation for encryption and decryption processes. Therefore if we use the fast exponentiation algorithm then the computational complexity is in polynomial time.



<table>
<tr><th colspan="2">Key Generation for the new cryptosystem</th></tr>
<tr><td colspan="2">New_cryptosystem_Key_Generation
{
Select a very large prime p and a very large integer q such that $p < q$ and $a^{2^p} \; mod \; 2^q \equiv 1$
Select e and r such that $2 < e, r < 2^p$ and e and r both are coprime to 2^p.
$d \leftarrow e^{-1} \; mod \; 2^p$
$s \leftarrow r^{-1} \; mod \; 2^p$
Public_key ← $(e, r, 2^q)$
Private_key ← (d, s)
return Public_key and Private_key
}</td></tr>
<tr><th>Encryption Algorithms</th><th>Decryption Algorithms</th></tr>
<tr><td>New_cryptosystem_Encryption1 $(P_1, e, 2^q)$
{
$C_1 \leftarrow$ Fast_Exponentiation $(P_1, e, 2^q)$
return C_1
}
New_cryptosystem_Encryption2 $(P_2, r, 2^q)$
{
$C_2 \leftarrow$ Fast_Exponentiation $(P_2, r, 2^q)$
return C_2
}</td><td>New_cryptosystem_Decryption1 $(C_1, d, 2^q)$
{
$P_1 \leftarrow$ Fast_Exponentiation $(C_1, d, 2^q)$
return P_1
}
New_cryptosystem_Decryption2 $(C_2, s, 2^q)$
{
$P_2 \leftarrow$ Fast_Exponentiation $(C_2, s, 2^q)$
return P_2
}</td></tr>
</table>

Figure 2: Key Generation of the introduced cryptosystem

3 Security of the Proposed Public Key Cryptosystem

There are several adversaries and attacks models in cryptography. A cryptosystem is secure if the success probability of an attacker trying to break the cryptosystem is small. An adversary can access the encryption oracle in a Chosen Plaintext Attack (CPA). In a non adaptive Chosen Ciphertext Attack (CCA1) and in an adaptive Chosen Ciphertext Attack (CCA2) an adversary can access the decryption oracle. In CCA1, the adversary cannot make further accesses to the decryption oracle before guessing. In CCA2, the adversary can make further accesses to the decryption oracle, but he cannot submit the challenge ciphertext.

The security of this system is depended on the selection of p and q. We can get many numbers for p for selected q as $a^{2^p} \bmod 2^q \equiv 1$; where a is an odd. Note that according to the Euler's theorem, there is at least two numbers for p as $a^{2^p} \bmod 2^q \equiv 1$. These values are $p = q$ and $p = q - 1$.

Recalling Euler's 1st Theorem, $a^{\phi(n)} \bmod 2^q \equiv 1$. When $n = 2^q$, we can write $\phi(2^q) = 2^q - 2^{q-1}$; (Because of 2 is a prime number).

The special case is $\phi(2^q)$ is always equal to 2^{q-1}. This behavior is unique only for 2. Therefore, $a^{2^{q-1}} \bmod 2^q \equiv 1$. Example: $\phi(2^{10}) = 2^{10} - 2^9 = 1024 - 512 = 512 = 2^9$.

Example 3. *Let $a = 535463$ and $q = 16$. Then,*

$$\begin{aligned}535463^{2^{13}} \bmod 2^{16} &\equiv 1\\ 535463^{2^{14}} \bmod 2^{16} &\equiv 1\\ 535463^{2^{15}} \bmod 2^{16} &\equiv 1\\ 535463^{2^{16}} \bmod 2^{16} &\equiv 1.\end{aligned}$$

An adversary has to choose one value for p in $\{13, 14, 15, 16\}$. Now the adversary has to try four times to find p in this situation if and only if the adversary knows the value of a. But, here a is equal to $e.d$ and $r.s$. The adversary does not know the values of d and s.

Example 4. *Let $a = 65527$ and $q = 7$. Then,*

$$\begin{aligned}65527^{2^4} \bmod 2^7 &\equiv 1\\ 65527^{2^5} \bmod 2^7 &\equiv 1\\ 65527^{2^6} \bmod 2^7 &\equiv 1\\ 65527^{2^7} \bmod 2^7 &\equiv 1.\end{aligned}$$

An adversary has to choose one value for p in $\{4, 5, 6, 7\}$. Now the adversary has to try four times to find p in this situation too. Again a is equal to $e.d$ and $r.s$. The adversary does not know the values of d and s.

According to above examples, the adversary has another problem too. Because of we choose p as $(e.d)^{2^p} \bmod 2^q \equiv 1$ and $(r.s)^{2^p} \bmod 2^q \equiv 1$. If the adversary wants to find p then she should know the values of d and s.

Since there are at least two values as $a^{2^p} \bmod 2^q \equiv 1$, if we choose two values for p as p_1 and p_2 in calculation of ed and rs then the security of this system will increase again.

Example:

$$\begin{aligned}&ed \bmod 2^{p_1} \equiv 1;\\ &(ed)^{2^{p_1}} \bmod 2^q \equiv 1\\ &rs \bmod 2^{p_2} \equiv 1;\\ &(rs)^{2^{p_2}} \bmod 2^q \equiv 1.\end{aligned}$$

Now the adversary has to find the values of d, s, p_1, and p_2.

3.1 Chosen Ciphertext Attack on the New Cryptosystem

Assume that Alice creates two ciphertexts C_1 and C_2.

$$C_1 \equiv (det(X))^e \bmod 2^q$$
$$C_2 \equiv g^r \bmod 2^q.$$

Now Alice sends C_1 and C_2 to Bob. Also assume that Bob will decrypt arbitrary ciphertexts for Eve other than C_1 and C_2. Eve intercepts C_1 and C_2 and uses the following steps to find P_1 and P_2.

Step 1: Eve chooses two random integers u_1 and $u_2 \in Z^*_{2^q}$.

Step 2: Eve calculates $v_1 = C_1.u_1^e \bmod 2^q$ and $v_2 = C_2.u_2^r \bmod 2^q$.

Step 3: Eve sends v_1 and v_2 to Bob for decryption and get W.

But, in this case finding of the original message from W, is very difficult to Eve. $2W = v_1^d + v_2^s (\bmod 2^q)$; (See the procedure - Figure 1).

$$\begin{aligned} 2W &= (C_1.u_1^e)^d + (C_2.u_2^r)^s (\bmod 2^q) \\ 2W &= C_1^d.u_1 + C_2^s.u_2 (\bmod 2^q) \\ 2W &= P_1.u_1 + P_2.u_2 (\bmod 2^q). \end{aligned}$$

If Eve can find P_1 and P_2 then the message is $(P_1 + P_2)/2$. But, now Eve has a new problem. She has to find P_1 and P_2 again. Therefore the new cryptosystem immunes for a chosen ciphertext attack. Therefore, this public key cryptosystem is OW-CCA2 secure.

3.2 Attacks on the Modulus

If Eve can find the value of p then she can break the system easily. Therefore Bob should choose good values for p and q as $p \leq q$ and $a^{2^p} \bmod 2^q \equiv 1$; where, $a = e.d$ and $a = r.s$. Now Eve is in a difficult situation of finding p. Because of she does not know the values d and s too.

3.3 Semantic Security

The semantic security is also known as indistinguishability of encryption (IND). In IND, the attacker should not get any information about the plaintext given its encryption.

The adversary $A = (A_1, A_2)$ is said to (k, ϵ, τ)-break IND when $Adv_\epsilon^{IND}(A) =; 2 \times_{b,x}^{Pr} [(pk, sk) \leftarrow GEN(1^k), (m_0, m_1, s) \leftarrow A_1(pk), c \leftarrow ENC_pk(mb)$: $A_2(m_0, m_1, s, c) = b]-1 \geq \epsilon$. Where the probability is taken over the random coins of the experiment according to the distribution induced by $GEN(1^k)$ as well as the ones the adversary, where $b \in \{0, 1\}$ and $m_0, m_1 \in M$. A must run at most τ steps and it is imposed that $|m_0| = |m_1|$. An encryption scheme is said to be IND secure if no probabilistic algorithm can (k, ϵ, τ)-break IND for $\tau \leq poly(k)$ and $\epsilon \geq 1/poly(k)$ [12]. This public key cryptosystem is IND secure with OAEP (Optimal Asymmetric Encryption Padding).

4 Conclusions

The modulus of this new cryptosystem is 2^n. Therefore we can get many advantages using hash functions like Whirlpool or SHA-512, with the new cryptosystem, because of these functions use modulus $2^n; n = 3$ and $n = 10$ respectively.

There is a special case when $e = 13$ and $p = 6$ and $q = 10$. That is the system is not work for $e^{-1} \bmod 2^p \equiv 13^{-1} \bmod 2^6 \equiv 5$. But the system is work for $e^{-1} \bmod 2^p \equiv 13^{-1} \bmod 2^6 \equiv 69$. Again this system is not work for $e = 5$ and $p = 6$ and $q = 10$. That is the system is not work for $e^{-1} \bmod 2^p \equiv 5^{-1} \bmod 2^6 \equiv 13$. But the system is work for $e^{-1} \bmod 2^p \equiv 5^{-1} \bmod 2^6 \equiv 77$. Therefore, we can use these points to increase the security of the system. Because of the valid d is known only by Bob.

5 Acknowledgment

I would like to thank Dr. Sandirigama M. (Department of Computer Engineering, Faculty of Engineering, University of Peradeniya, Sri Lanka) for providing helpful feedback and advice in this research. I also gratefully acknowledge the anonymous reviewers for their valuable comments.

References

[1] B. A. Forouzan, D. Mukhopadhyay, *Cryptography and Network Security*, Special Indian Edition, ISBN: 10:0-07-070208-X, pp. 265-296 and pp. 306-352, 2010.

[2] D. Boneh, “Simplified OAEP for the RSAS and Rabin functions,” in *Proceedings of CRYPTO'01*, Springer-Verlag, LNCS 2139, pp. 275-291, 2001.

[3] D. Pointcheval, “New public key cryptosystems based on the dependent-RSA problem,” *Advances in Cryptology (EUROCRYPT'99)*, Springer-Verlag, LNCS 1592, pp. 239-254, 1999.

[4] E. Fujisaki, T. Okamoto, “How to enhance the security of public key encryption at minimum cost,” in *PKC'99*, Springer-Verlag, LNCS 1560, pp. 53-68, 1999.

[5] G. Lu, L. Xue, X. Nie, Z. Qin, ”Cryptanalysis of novel extended multivariate public key cryptosystem with invertible cycle,” *International Journal of Network Security*, vol. 20, no. 3, pp. 509-514, 2018.

[6] H. Zhu, L. Wang, S. Qui, X. Niu, “New public key encryption with equality test based on non-Abelian factorization problems,” *KSII Transactions on Internet and Information Systems*, vol. 12, no. 02, pp. 764-785, 2018.

[7] M. Bellare, P. Rogaway, “Random oracles are practical: A paradigm for designing efficient protocols,” in *Proceedings of the 1st ACM Conference on Computer and Communications Security*, pp. 62-73, 1993.

[8] M. Naor and M. Yung, “Public-key cryptosystems provably secure against chosen ciphertext attacks,” in *Proceedings of the 22nd STOC'90*, ACM Press, pp. 427-437, 1990.

[9] P. Paillier, D. Pointcheval, “Efficient public key cryptosystem provably secure against active adversaries,” in *Advances in Cryptography (ASIACRYPT'99)*, Springer-Verlag, LNCS 1716, pp. 165-179, 1999.

[10] R. Cramer and V. Shoup, “A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack,” in *Crypto'98*, Springer-Verlag, LNCS 1462, pp 13-25, 1998.

[11] R. Rivest, A. Shamir, L. Adleman, “A method for obtaining digital signature and public key cryptosystems,” *Communications of the ACM*, vol. 21, pp. 120-126, 1978.

[12] S. Goldwasser and S. Micali, “Probabilistic encryption,” *Journal of Computer and System Sciences*, vol. 28, no. 2, pp. 270-299, 1984.

[13] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transactions on Information Theory*, vol. 31, pp. 469-472, 1985.

[14] T. Hanoymak, "On provable security of cryptographic schemes," *International Journal of Information Security Science*, vol. 2, no. 2, pp. 44-56, 2013.

[15] T. Okamoto, S. Uchiyama, "A new public key cryptosystem as secure as factoring," in *EUROCRYPT'98*, Springer-Verlag, LNCS 1403, pp. 308-318, 1998.

[16] T. Y. Wu, J. C. W. Lin, C. M. Chen, Y. M. Tseng, J. Frnda, L. Sevcik, M. Voznak, "A brief review of revocable ID-based public key cryptosystem," *Perspective in Science*, vol. 7, pp. 81-86, 2016.

[17] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Transaction on Information Theory*, vol. 22, pp. 644-654, 1976.

[18] W.D.M.G.M. Dissanayake, "An improvement of basic ElGamal public key cryptosystem," *International Journal of Computer Applications Technology Research*, vol. 7, no. 2, pp. 40-44, 2018.

[19] Y. Hashimoto, *Multivariate Public Key Cryptosystem*, Springer Nature Singapore Pte Ltd, pp. 17-42, 2018.

[20] Z. Liu, X. Yang, W. Zhong, Y. Han, "An efficient and practical public key cryptosystem with CCA-security on standard model," *Tsinghua Science and Technology*, vol. 19, pp. 486-495, 2014.

Biography

Maheshika W.D.M.G. Dissanayake received her BSc degree in Computer Science, Mathematics and Applicable Mathematics from University of Ruhuna, Sri Lanka. Now, she is an MPhil candidate at Department of Computer Engineering, Faculty of Engineering, University of Peradeniya, Sri Lanka. Her research interests include Cryptography and Network Security.

Monitoring and Detection the Cognition Roots Using Quad Copter

Diaa Salama Abdul Minaam[1], H. M. Abdul Kader[2], Eman Mahmoud[1]

(Corresponding author: D. S. Abdul Minaam)

Information System Department, Faculty of Computers and Information, Benha University[1]
El-Shaheed Farid Nada, Qism Banha, Banha, Al Qalyubia Governorate 13511, Egypt
Information System Department, Faculty of Computers and Information, Menufyia University[2]
(Email: diaa.salama@fci.bu.edu.eg)

(Received Mar. 28, 2018; revised and accepted July 31, 2018)

Abstract

The importance of traffic lies in our daily life in terms of facilitating the transition from one place to another to accomplish the work and many other purposes. The Traffic Problem which becomes one of the biggest problems currently existing in reality. it can be felt at peak time when employees going to their work, students going to their schools and universities as well as the time of return to their homes thus affects in wasting time, reduces production and many of the negative impacts on the society and citizens. These problems are air pollution, crowded roads, and unsuitable roads. There are many researches to solve these problems. Our proposed module offers a solution to solve traffic problem using the internet of things (IoT) technology. The results of this paper are to monitor the traffic environment and trying to detect the cognition roots anytime anywhere using the Quad Copter. Our solution shows superiority on other modules used to solve traffic problem.

Keywords: Cognition Roots; Quad Copter; Traffic Problem

1 Introduction

In the last few years, there were a growing interest in solving traffic problems by providing good ways to facilitate traffic leads to saving time and increasing production, this is considered one of the reasons leading to the rise of the economic situation, also providing a proper traffic system and control of car exhausts. Traffic problems include crowded roads that become a sign of very bad signs that distinguish Egypt now which came from large number of cars and Lack of road capacity [1]. One of the problem caused by crowded roads impacts on health by disabling the ambulances from reaching hospitals quickly. On the other side unsuitable roads are also another bad sign now in Egypt. They become impassable and filled with bumpy.

With the increasing of population density and the large number of transportation, despite that there is difficulty to find suitable means of transport. However, several practical questions arise when dealing with traffic problem like it is important to identify the suitable roads free of industrial bumps; also it is key to predict wasting in time Also traffic problem affects health by delaying ambulances loaded with patients to get to hospital in time to answer all these questions, we present an original approach which help us in solving the previous problems. With this goal, this work seeks to monitor the roads and manage traffic that considers the way for the implementation of Intelligent Transportation System (ITS) [2]. ITS is a comprehensive solution for real-time traffic management that relies on data collection from vehicles [19], road sides units (RSU) and other sensors [20], which are entities that can interact and cooperate among themselves, creating a vehicular network.

Providing solution to avoid traffic cognition is very clear. There are lots of application seek to do that. The most popular application toward this end is Waze. However, Waze is not an ITS as it depends on information sent from drivers using their smartphones; also routs suggested to users are based exclusively on shortest-path algorithms without taking into account the proposed road capacity. The Internet of Things (IoT) [12] is fundamentally transforming the transportation industry. Next generation intelligent transportation systems will optimize the movement of people and goods, improving economics, public safety, and the environment.

Our contribution is to provide a solution using Quad copter. These solution focus on solving the problem or part of it that needs to collect data from every unit on the road such vehicles, RSU and other sensors, these entities interact among themselves to provide a good solution. However, these entities need huge cost to be applying in a large scale area. In this paper, we offer a new technique that depends on Internet of Things. This technique can detect when the cognition is forming and provide information about traffic condition with saving the cost. This technique is quad copter. Quad copter is different from other application as it reduces the cost by using fewer sensors than other applications.

2 Related Work

Traffic jam is a big problem that large countries suffer from it and trying all the time to detect crowded roads to be able to supply smart solutions taking in consideration the cost of implementation. There are a lot of researches in traffic field all of them depend on more than two or three sensors which cost huge budget to cover large area.

Menon et al. [4] Proposes a framework to understand the feasibility of implementing Internet of Things in bus transportation system in Singapore to help consumer know the arrival time of the bus based on the speed of bus which depend on more than sensor in one bus. The research was aimed to find out the feasibility of using of Internet of things in the bus transportation system in Singapore and to validate whether it improves the consumer experience. The design proposed by us has capitalized on the advantages provided by IoT by giving real time data to the consumers for each bus route. Through the Impact analysis and Competitive analysis with one of the most used bus mobile applications Iris NextBus in Singapore, it was found that IoT application if implemented would clearly outweigh NextBus in almost all the parameters. These parameters include time management, time saving, bus efficiency management, bus crowd management and in the number of options being offered to users. It would cater to all the sections of the society satisfying their varying needs.

Souza et al. [2] Proposes CHIMERA (Congestion avoidance througH a traffIc classification MEchanism and a Re-routing Algorithm) based on applying sensors in the area of interest which cooperate together like road side units and vehicles. CHIMERA composed of three main procedures; first procedure is Road network and communication model which divides the road with sensors that present communication models to help in collecting road data. Second procedure is Data processing and congestion detection. CHIMERA employs the k-Nearest Neighbor algorithm (KNN) to classify congestion levels on roads. CHIMERA uses the average road speed and the density of vehicles in the road as input parameters. The output of the algorithm is the traffic condition. Third procedure is Re-routing and traffic balancing. Re-routing algorithm works under the boundaries imposed by the RSU coverage. CHIMERA calculates alternative routes by using the K-Shortest Path algorithm based on road weights. CHIMERA may assign different paths to different vehicles, thus performing a load balance across alternative paths

Bauza et al. [5] presents CoTEC (COperative Traffic congestion detECtion), a novel cooperative technique based on Vehicle-to Vehicle (V2V) communications which apply sensors in vehicles to be able to detect road traffic cognition. CoTEC uses messages in order to inform all vehicles about traffic conditions and detects a potential congestion condition locally at each vehicle. Therefore, upon detecting a traffic jam, each vehicle broadcasts its own estimation about the traffic jam and, then, with all estimations, vehicles collaboratively detect and characterize the road traffic congestion. However, the mechanism employed to identify the traffic condition can cause an overload in the network due to the periodic beacon messages and the local estimations disseminated by all vehicles. Furthermore, despite being able to detect congestion, no mechanism to minimize or control the traffic jam is presented. In addition, CoTEC was proposed to operate exclusively on highway scenarios.

Brennand et al. [3] implements a distributed ITS for detecting and controlling congestions. To this end, RSUs are distributed across the city to ensure total coverage of the region. In addition, each RSU is responsible for managing congestion only in the area covered by its communication radius. Thus, vehicles can interact with several RSUs along their paths.

Pan et al. [18] propose a centralized system to acquire, in real-time, the vehicle geographic position, speed and direction as a means to detect traffic jams. Once detected, vehicles are re-routed based on two different algorithms. First, Dynamic Shortest Path (DSP), which routes vehicles using the shortest path which also has the lowest, traveled time. However, one shortcoming of this algorithm is the possibility to move the congestion to another spot. Second, Random k Shortest Paths (RkSP), which randomly chooses a route among k shortest path routes. The goal of this algorithm is to avoid switching congestion from one spot to another by balancing the re-routed traffic among several paths. This scheme does not implement a real-time mechanism to detect congestion as it occurs; only detecting it during the next re-routing phase.

Manna et al. [6] thesis presented the design of a system to give a solution for detecting vehicles causing environmental pollution. It monitored air pollution on roads and track vehicles which cause pollution over a specified limit using Internet of Things (IoT), Wireless Sensor Networks (WSN), and Geographical Information System (GIS) to address the problem.

Xavier et al. [7] purposed comparative study and performance evaluation of various locations finding techniques for mobile tracking and its application for studying traffic densities in highways and lateral roads.

Hasan Omar Al-Sakran [8] purposed a framework for real-time traffic information acquisition and monitoring architecture based Internet of Things, RFID, wireless sensor network (WSN), GPS, cloud computing, agent and other advanced technologies to collect, store, manage and supervise traffic information.

Ming Chen [9] thesis presented a systematic study of methodologies used to set signal timing plans for evacuation was undertaken to move people out from an endangered area as quickly as possible so as to avoid casualties.

Many other researchers who are recognized in literature on IoT applications such as [21], and [22] studied the important of IoT application in our life. IoT researchers suggested many new different applications, such as smart homes, e-health systems, wearable devices, smart kitchen etc [23, 24]. Also these IoT systems required Security and Safety [25–31].

3 Proposed Model

Quad copter is the proposed solution that simulates the intelligent transportation system (ITS) with lower cost. It is a four-motor aircraft, two motors move with clockwise, the others move with counter clockwise. Quad copter package include the recommended complete list of the specific parts that were used and tested for building complete quad copter.

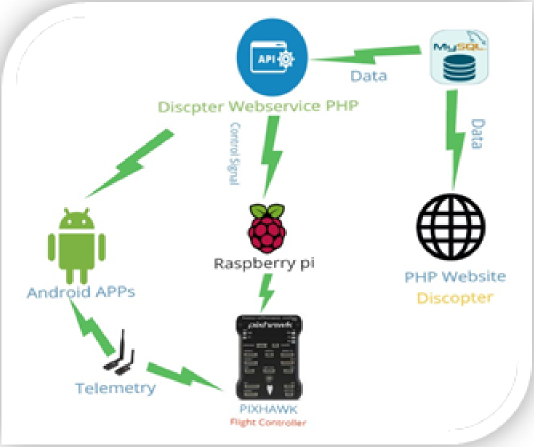


Figure 1: The model of the system

The parts needed to build a quad copter:

1) Frame: Frame is a needed part to house all the other components of the quad copter. The frame used in the proposed quad copter is strong, light, and have a built-in power distribution board (PDB) that allows easy and clean building of the wire and circuits in the quad copter.

2) Brushless Motor: Brushless motor considered one of the main three parts of the aircraft. The obvious purpose of these motors is to spin the propellers. Motors are rated by kilovolts as kilovolts is the one which determine the quad copter speed and thrust, The higher the kilovolts, the higher the speed, the lower the thrust and vice versa. We need four motor for the quad copter.

3) Electronic Speed Control (ESC): ESC is the second important item in the quad copter. Its importance lies in using it with motors as it tells the motors how fast to spin at any given time. The ESCs are then connected directly to the battery. ESCs control the speed of motors according to signals received from flight control board.

4) Flight Control Board (PIXHAWAK CONTROL): The flight control board is the 'brain' of the quad copter which can identify the sensors, accessories and direction of the quad copter through mission planner. Mission planner is the software that is considers the interface of the flight control board. PIXHAWAK CONTROL is an independent, open-hardware project aiming to provide high-end autopilot hardware for the academic Autopilot Software. The Pixhawk autopilot module runs a very efficient real-time operating system (RTOS), which provides a POSIX-style environment (i.e. printf(), pthreads, /dev/ttyS1, open(), write(), poll(), ioctl(), etc).

5) Sensors x4: There are four sensors using for building the model. Sensor is a device that detects and responds to some type of input from the physical environment. The specific input could be light, heat, motion, moisture, pressure, or any one of a great number of other environmental phenomena. The output is generally a signal that is converted to human-readable display at the sensor location or transmitted electronically over a network for reading or further processing.

a. The first sensor: Safety Switch sensor For added safety, vehicles using PIXHAWK have to use an on-vehicle safety switch. The switch includes a status led and should protrude through the vehicle body. It allows arming a fixed-wing aircraft immediately before takeoff and indicates the system status.

b. The second sensor: Pixhawk LED sensor. LED gives different flashing that has various meanings:

   - Flashing red and blue: Initializing gyroscopes. Hold the vehicle still and level while it initializes the sensors.
   - Flashing blue: Disarmed, no GPS lock found. Autopilot, loiter and return-to-launch modes require GPS lock.
   - Solid blue: Armed with no GPS lock.
   - Flashing green: Disarmed (ready to arm), GPS lock acquired. Quick double tone when disarming from the armed state.
   - Fast Flashing green: Same as above but GPS is using SBAS (so should have better position estimate).
   - Solid green - with single long tone at time of arming: Armed, GPS lock acquired. Ready to fly!
   - Double flashing yellow: Failing pre-arm checks (system refuses to arm).
   - Single Flashing yellow: Radio failsafe activated.
   - Flashing yellow - with quick beeping tone: Battery failsafe activated.
   - Flashing yellow and blue - with high-high-high-low tone sequence (dah-dah-dah-doh): GPS glitch or GPS failsafe activated.
   - Flashing red and yellow - with rising tone: EKF or Inertial Nav failure.
   - Flashing purple and yellow: Barometer glitch.
   - Solid Red: Error.

c. The third PPM Encoder sensor: The PPM encoder allows to encode up to 8 PWM (pulse width modulated) signals into one PPM (pulse position modulation) signal.

   Table 1 is failsafe output value. New interrupt system that handles certain Futaba receivers better (simultaneous changes on groups of R/C channels in fast intervals) (this was already present in v2.3.13).

   Adapted behavior in case of channel loss: If one channel is lost, it will be set according to the following table. The other channels will continue working.

Table 1: Failsafe output values

Channel 1	Roll	Set to center (1500 μs)
Channel 2	Pitch	Set to center (1500 μs)
Channel 3	Throttle	Set to low (900 μs)
Channel 4	Yaw	Set to center (1500 μs)
Channel 5	$\cdots$	Remain at last value
Channel 6	$\cdots$	Remain at last value
Channel 7	$\cdots$	Remain at last value
Channel 8	$\cdots$	Remain at last value

d. The fourth sensor: USB sensor This port can be mounted on the outside of the plane / copter / rover and provides convenient access. Helps us to make configuration for Quad copter.

6) Radio transmitter and receiver: Radio transmitter and receiver allow controlling quad copter flight.

7) Propeller (2 clockwise and 2 counter-clockwise): Propellers are responsible for lifting and landing the quad copter which has four propellers, two propellers spin counter-clockwise, and the other spin clockwise.

8) Battery (battery 335200 mA): Battery is the third and last important part in quad copter components. Quad copter typically uses LiPo battery which indicates 3 cells in parallel. Each cell is 3.7 volts so this battery is rated at 11.1 volts. LiPo batteries also have a C rating and a power rating in mAh (which stands for milliamps per hour). The C rating describes the rate at which the power can be drawn from the battery, and the power rating describes how much power the battery can supply.

9) Charger: Charging LiPos is a complex process, because there are usually multiple cells within the battery that must be charged and discharged at the same rate. Therefore we must have a balance charger.

10) GPS 8M: Used to locate the quad copter, this new design incorporates the HMC5883L digital compass, using the Ublox latest 8series module providing a convenient method of mounting the compass away from sources of interference that may be present in the confines of the vehicle. It features active circuitry for the ceramic patch antenna, rechargeable backup battery for warm starts and is shipped pre-configured for use with Pixhawk.

11) Power Module: Integrate most of the components needed for a complete, efficient, switching regulator-based power supply into one package. typically consisting of one or more microcontroller or microprocessor connected to peripheral sensors used for navigation.

12) Power Distribution Board (PDB): PDB distribute the power on your drone, and provides a neat and tidy way of connecting your battery to all of your ESC's on your aircraft. A PDB has positive pads/terminals which are all connected and negative terminals/pads which are all connected. This way when you solder all of the red wire from your ESC's and battery to the positive pads on the PDB, and the black wires to all the negative pads, they will all become connected so your battery can provide power to all of your ESC's.

13) SiK Telemetry Radio: A SiK Telemetry Radio is one of the easiest ways to setup a telemetry connection between your APM/Pixhawk and a ground station.

    Connecting to Pixhawk Use the 6 pin DF13 connector that should have come with the radio to connect the radio to your Pixhawk's "Telem 1" ("Telem 2" or "Serial 4/5" can also be used but the default recommendation is "Telem1").

14) Digital Camera: Digital camera records and stores photographic images in digital form. Many current models are also able to capture sound or video, in addition to still images. Capture is usually accomplished by use of a photo sensor, using a charged coupled device (CCD).These stored images can be uploaded to a computer immediately or stored in the camera for to be uploaded into a computer or printer later. Images may also be archived on a photographic compact disc or external hard disk.

4 System Implementation

To be able to use quad copter we should connect it to the pc throw flight controllers. Mission Planner is the flight controllers used to connect the quad copter to the pc using Radio transmitter and receiver.

Connecting the radio to your Windows PC is as simple as connecting the micro USB cable (which should have been included with the radio) to your PC. The necessary drivers should be installed automatically and the radio will appear as a new "USB Serial Port" in the Windows Device Manager under Ports (COM & LPT). The Mission Planner's COM Port selection drop-down should also contain the same new COM port. Figure 2 shows the connection with mission planner.

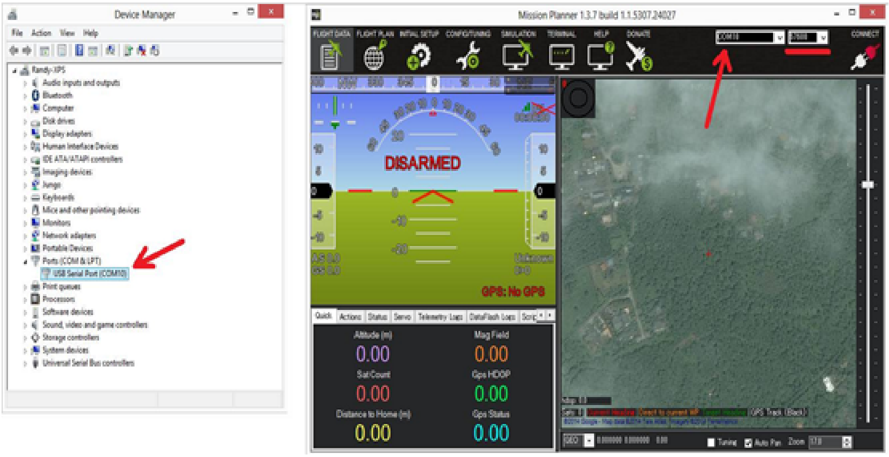


Figure 2: The connection with mission planner

After set up Quad copter on Mission planner, Quad copter flies on suitable height to cover an area of interest of roads, so it will be able to take photos of roads which clarify the condition of the roads. These photos sent through cloud to the specialists in traffic department and general authority of road development.

5 Results and Analysis

We have applied the quad copter and flew at a height of 50 meters in the vicinity of Al Ahram in Benha city and the camera recorded video monitoring traffic in this area at different time periods.

The general authority of road development will launch the quad copter and control the places of its presence throughout the day, so that the quad copter can be able to send live picture of the roads throughout the day which enables specialists to take these images and analyze it then give results to help in solving the traffic system, develop various proposals to eliminate traffic barriers and draw routes for beneficiaries based on monitoring the movement of cars in different ways.

6 Conclusions and Future Work

We propose Quad copter, a solution used to detect roads condition through taking real time images of the road on day long, Through which I know the status of the road without the need for help from people or cars on the road that make quad copter an independent system in monitoring the roads.

A quad copter flew in different parts of Banha and recorded many videos describing the state of the different roads, which helps to detect the congestion and think of solutions to the traffic crisis.

We look forward to providing mobile application that sends real time solution after processing images taken by quad copter.

7 Limitation

The failure of a component of the quad copter or it collision by any obstacle in the air, so we must take into an account the flight on an appropriate area and at an appropriate height.

References

[1] P. Gawade, A. Meeankshi, "IOT based smart public transport system," *International Journal of Scientific and Research Publications*, vol. 7, no. 7, pp. 390-396, July 2017.

[2] M. A. de Souza, S. R. Yokoyama, G. Maia, A. Loureiro, and L. Villas, "Real-time path planning to prevent traffic jam through an intelligent transportation system," in *IEEE Symposium on Computer and communication (ISCC'16)*, Messina Italy, Aug. 2016.

[3] C. Brennad, A. Mariano, G. Maia, A. Boukerche, A. Loureiro, and L. Villas, "An intelligent transportation system for detection and control of congested roads in urban centers," in *IEEE Symposium on Computers and Communications (ISCC'15)*, July 2015.

[4] A. Menon, R. Sinha, D. Ediga, S. Iyer, "Implementation of internet of things in bus transport system of Singapore," *Asian Journal of Engineering Research*, vol. 1, no. 7, pp. 8-17, 2013.

[5] R. Bauza, J. Gozalvez, "Traffic congestion detection in large-scale scenarios using vehicle-to-vehicle communications," *Journal of Network and Computer Applications*, vol. 36, no. 5, pp. 1295-1307, 2013.

[6] S. Manna, *Environmental Pollution Monitoring Using GIS and Internet of Things*, Master Thesis, Faculty of Engineering and Technology, Jadavpur University, May 2014.

[7] P. M. Xavier, R. Nedunchezhian, "A comparative study on road traffic management systems," *International Journal of Research in Engineering and Technology*, vol. 3, no. 15, pp. 108-112, Dec. 2014.

[8] H. O. Al-Sakran, "Intelligent traffic information system based on integration of internet of things and agent technology," *International Journal of Advanced Computer Science and Applications*, vol. 6, no. 2, pp. 37-43, 2015.

[9] M. Chen, *Traffic Signal Timing for Urban Evacuation*, Master Thesis, Faculty of the Graduate School, University of Maryland, 2005.

[10] P. Spiess, S. Karnouskos, D. Guinard, D. Savio, O. Baecker, L. M. Sa de Souza, and V. Trifa, "SOA-based integration of the internet of things in enterprise services," in *Proceedings of the 2009 IEEE International Conference on Web Services (ICWS'09)*, pp. 968-975, 2009.

[11] T. Ridel, N. Fantana, A. Genaid, D. Yordanov, H. R. Schmidtke and M. Biegl, "Using web service gateways and code generation for sustainable iot system development," in *Internet of Things (IoT'10)*, pp. 1-8, 2010.

[12] J. Gao, F. L. Liu, H. S. Ning, and B. F. Wang, "RFID coding, name and information service for internet of things," in *IET Conference on Wireless, Mobile and Sensor Networks*, pp. 36-39, 2007.

[13] F. H. Mohammed, R. Esmail, "Survey on IoT services: Classifications and applications," *International Journal of Science and Research*, vol. 4, no. 1, pp. 2125-2127, 2015.

[14] B. Yan, G. Huang, "Supply chain information transmission based on RFID and internet of thing," in *International Conference on Computing, Communication, Control, and Management*, vol. 4, pp. 166-169, 2009.

[15] M. Thomas, S. Meyer, K. Spemer, S. Meissner, T. Braun, "On IoT-services: survey, classification and enterprise integration," in *IEEE International Conference InGreen Computing and Communications (GreenCom'12)*, pp. 257-260, 2012.

[16] X. Yu, F. Sun, X. Cheng, "Intelligent urban traffic management system based on cloud computing and internet of things," in *International Conference on Computer Science & Service System*, pp. 2169-2172, 2012.

[17] L. Xiao, "A new application for intelligent traffic monitoring system," *Journal of Networks*, vol. 6, no. 6, 2011.

[18] J. Pan, M. Khan, I. Sandu Popa, K. Zeitouni, and C. Borcea, "Proactive vehicle re-routing strategies for congestion avoidance," in *IEEE 8th International Conference on Distributed Computing in Sensor Systems (DCOSS'12)*, pp. 265-272, 2012.

[19] F. D. da Cunha, L. Villas, A. Boukerche, G. Maia, A. C. Viana, R. A. F. Mini, and A. A. F. Loureiro, "Data communication in vanets: Protocols, applications and challenges," *Ad Hoc Networks*, vol. 44, pp. 90-103, 2016.

[20] M. Wang, H. Shan, R. Lu, R. Zhang, X. Shen, and F. Bai, "Real-time path planning based on hybrid-Vanet-enhanced transportation system," *IEEE Transactions on Vehicular Technology*, May 2015.

[21] D. S. AbdElminaam, "Smart kitchen: Automated cooker technique using IoTclassification," *International Journal of Electronics and Information Engineering*, vol. 9, no. 1, pp. 1-10, Sep. 2018.

[22] D. S. AbdElminaam, "SHAS-IoT: Smart home automation system (SHAS) using internet of things (IoT) to improve safety and security," *Research of Applied Science*, vol. 13, no. 3, pp. 209-215, Mar. 2018.

[23] D. S. AbdElminaam, "Smart life saver system for alzheimer patients, down syndromes, and child missing using IoT," *Asian Journal of Applied Sciences*, vol. 6, no. 1, pp. 21-37, Feb. 2018.

[24] D. S. AbdElminaam, T. M. M. Alenezi and M. A. S. Ali, "Smartsepog: IoT based system for enhancement of the performance of KJO oil and gas fields in Kuwait," *Far East Journal of Electronics and Communications*, vol. 18, no. 6, pp. 915-944, June 2018.

[25] C. H. Wei, M. S. Hwang and A. Y. H. Chin, "An improved authentication protocol for mobile agent device in RFID," *International Journal of Mobile Communications*, vol. 10, no. 5, pp. 508-520, 2012.

[26] C. C. Lee, I-En Liao, M. S. Hwang, "An extended certificate-based authentication and security protocol for mobile networks," *Information Technology and Control*, vol. 38, no. 1, pp. 61-66, 2009.

[27] D. S. AbdElminaam, H. M. Abdul Kader, M. M. Hadhoud, and S. M. El-Sayed, "Elastic framework for augmenting the performance of mobile applications using cloud computing," in *Proceedings of IEEE ICENCO*, pp. 134-141, 2013.

[28] C. T. Li, M. S. Hwang, "An online biometrics-based secret sharing scheme for multiparty cryptosystem using smart cards," *International Journal of Innovative Computing, Information and Control*, vol. 6, no. 5, pp. 2181-2188, May 2010.

[29] H. M. A. Kader, M. M. Hadhoud, S. M. El-Sayed, D. S. AbdElminaam, "Performance evaluation of new hybrid encryption algorithms to be used for mobile cloud computing," *International Journal of Technology Enhancements And Emerging Engineering Research*, vol. 2, no. 4, 2014.

[30] D. S. AbdElminaam, H. M. A. Kader, M. M. Hadhoud, "Energy efficiency of encryption schemes for wireless devices," *International Journal of Computer Theory and Engineering*, vol. 1, no. 3, pp. 302-309, 2009.

[31] D. S. AbdElminaam, H. M. A. Kader, M. M. Hadhoud, S. M. El-Sayedr, "Increase the performance of mobile smartphones using partition and migration of mobile applications to cloud computing," *International Journal Of Technology Enhancements And Emerging Engineering Research*, vol. 2, no. 5, pp. 34-44, 2014.

Biography

Diaa Salama Abdul-Minaam was born on November 23, 1982, in KafrSakr, Sharkia, Egypt. He received the B.S from Faculty of Computers & Informatics, Zagazig University, Egypt in 2004 with grade very good with honor, and obtains the master degree in information system from the faculty of computers and information, menufia university, Egypt in 2009 specializing in Cryptography and network security. He obtained his Ph.D. degree in information system from the faculty of computers and information, menufia university, Egypt in 2015. He is currently a Lecturer in Information systems department, Faculty of Computers and Information, Benha University, Egypt since 2011. He has worked on a number of research topics.Diaa has contributed more than 30+ technical papers in the areas of wireless networks, wireless network security, Information security and Internet applications, Cloud Computing, Mobile Cloud Computing, Internet of Things, Machine learning in international journals, international conferences, local journals and local conferences. He majors in Cryptography, Network Security, IoT, Big Data, Cloud Computing. (Mobile: +201019511000 ; E-mail: ds_desert@yahoo.com)

Hatem Abdul-kader obtained his B. S. and M. SC. (by research) both in Electrical Engineering from the Alexandria University, Faculty of Engineering, Egypt in 1990 and 1995 respectively. He obtained his Ph.D. degree in Electrical Engineering also from Alexandria University, Faculty of Engineering, and Egypt in 2001 specializing in neural networks and applications. He is currently a Lecturer in Information systems department, Faculty of Computers and Information, Menoufya University, Egypt since 2004. He has worked on a number of research topics and consulted for a number of organizations.

Eman Mahmoud received the B.S from Faculty of Computers & Informatics, Benha University with grade very good with honor, and registered for the master degree in information system from the faculty of computers and information, Benha university, Egypt in 2016 specializing in IoT

Biometrics: The Future of Banking and Financial Service Industry in Nigeria

Richman Charles Agidi
(Corresponding author: Richman Charles Agidi)

Information System Department, Faculty of Computers and Information, Benha University[1]
Computer Engineering Technology Student, Houdegbe North American University Benin
06 BP 2080, Route de Porto Novo Cotonou, Agblangandan, Benin
(Email: richykleen1st@gmail.com)

(Received Aug. 6, 2018; revised and accepted Nov. 3, 2018)

Abstract

As the world becomes increasingly more digital, the number of passwords people have to manage is becoming a serious problem. Financial institutions need to investigate acceptable biometric alternatives for authenticating mobile banking; users that balance both security and simplicity. Consequently, companies and government authorities are becoming increasingly committed to developing more convenient and secure means to access that information, allowing people to organize their lives digitally without hassle of fear of fraud. Biometrics, the science of measuring and statistically analyzing biological data, is still in its infancy but already a number of technological applications of its principles have been developed and adopted in order to increase the security and efficiency of the adopter's operations. Immigration desks at international airports are perhaps the most visible example of the potential of biometrics, as the latest passports and biometric cards allow airport authorities to more accurately log the arrival and departure of their visitors through fingerprint and eye scans. This provides a much more reliable and efficient method of verification than relying solely on human Agents. Those same principles of security and efficiency are what make the adoption of biometrics such an attractive prospect to banking institutions across the world. With the average banking customer handling a wider range of financial transactions online through desktop and mobile devices, the need for easy and safe access to their banking data is becoming a top priority for banking service providers wanting to differentiate themselves from their competitors.

Keywords: Adopted Countries; Banking; Biometric On; Financial Service Industry; Functionality; Security

1 Introduction

Biometric technologies, such as finger vein or iris recognition, have been the mainstay of science fiction movies and literature for decades. Perhaps, that is why some people, including decision makers of financial institutions, think of them as mere curiosity. When all the while, banks are already using their enormous potential to make banking more secure and convenient than ever before, gaining approval and appreciation from both individual and corporate customers. Let's take a closer look at how biometrics redefines digital banking.

According to a report by Deloitte, the majority of individuals aged 16-24 view security measures, such as passwords, as ”an annoying extra step before making an online payment”. It probably would have been more bearable if this annoyance really ensured secure transactions. But 2017 saw some of the biggest data breaches ever. Financial institutions were not spared, with as many as 400,000 accounts compromised in one attack alone .Aware of all that, management of banking institutions have been experimenting with various other methods. Some of them include passphrases, social sign-ins, multiple devices, or even multi-factor authentications that may include various combinations of those methods with a password for increased security. Even the sheer number of these methods shows that there is no clear winner. All of them compromise either security or user experience to some extent. Therefore, further research has been carried out to take the banking industry to a world beyond passwords.

For the past decade, biometrics has been by far the most promising and prolific direction in which progress in authenticating users has been moving. Biometrics is the study of distinctive and measurable human characteristics that can be used to label and describe any individual. Those characteristics, or biometric identifiers, can be anything from fingerprints and veins, palm veins, iris, retina, face, voice, or even handwritten signature - as long as it is something unique for any individual. For example, the patterns of blood vessels in the finger or palm are so complex that no two individuals possess the same. The identifier’s lack of propensity to change with time or due to illness is also very important. All the identifiers mentioned above meet these conditions, albeit with some exceptions (e.g. iris texture may change as a result of certain surgeries).Since traditional methods of authenticating have been consistently proving such security hazard and UX pain, some financial service decision makers began to realize that a whole new method would be welcomed by users. Furthermore, everyone wanted to be at the forefront of designing long-awaited standards of user authentication. As research and development of biometric technologies progresses, more and more banks jumped on the bandwagon.

Lloyds Banking Group, a major British bank, partnered with Microsoft to offer their customers a new way to access their accounts from Windows 10 devices - via fingerprint or facial recognition. What’s important, the device can recognize the face of the user - as opposed to an image, ensuring that no impersonator will be able to exploit it. Aside of clear security benefits, Lloyds’ representatives believe that getting rid of passwords in favor of this quick and highly personalized method will greatly improve user experience.

KB Kookmin Bank, one of the largest financial institutions in South Korea, is already enjoying great success with biometric technologies. Its innovative use of iris scanner of mobile devices to allow its customers to access their accounts earned them the top spot on Korea’s Highest Brand of the Year survey in 2016. The technology used by IDFC (Infrastructure Development Finance Company), a major financial company from India, is perhaps one of the most exciting examples of leveraging the potential of biometrics. At its base is Aadhaar - a 12-digit unique number issued to all Indian citizens based on both biometric and demographic data. As a result, their Aadhaar number and fingerprint is enough to make payments with participating vendors.

Innovative companies and startups from the financial sector are constantly leveraging biometrics to improve the solutions they offer. For example here at Live Bank’s we have created a virtual branch platform, which allows banks to combine the advantages of physical locations and self-care online banking. This platform also makes use of biometric identifiers to improve security and user experience. During the eKYC process, remote onboarding of new customers, the solution uses facial biometrics to verify customer’s identity and compare them to their ID. The process has been launched with great success at Bank Zachodni WBK in Poland, and let the bank acquire a lot of new customers.

2 Biometric Banking

Biometrics is a technology powered method of personal identification that leverages unique biological patterns on and in human body. These irregular and asymmetric patterns are found in iris and retina inside eyes, fingerprints, vein pattern beneath the skin, facial pattern, DNA sequence, voice print, gait, typing rhythm, etc. Irregularities in formation of these patterns make them good enough to be considered as unique for a person. For example, in over 100 year's history of fingerprinting, fingerprints from different fingers were never found to be the same. Biometric characteristics do not even repeat in twins and they remain unchanged throughout the life of a person. Different fingers of same person too have different fingerprints. These qualities of biometric traits make them an ideal method for personal identification. The rapid digitization of banking services combined with the continued need to adopt stricter customer and employee identification protocols to prevent identity theft and fraud has set the table for biometric identification technology to become an integral and strategic part of financial service security platforms. Acting as a strong authentication tool to help secure ATM, brick and mortar, and online transactions, biometrics in banking also helps to increase customer trust and improve brand reputation. The necessity for a stronger authentication solution became inevitable in banking services because of the growing pace of sophisticated transactional technology adoption along with the unfortunate rise in fraud and security breaches due to reliance on traditional security systems such as passwords.

Biometrics is automated methods of recognizing customers through their biological characteristics and traits such as fingerprints, finger vein patterns, iris, and voice recognition. Biometric characteristics are unique for every individual and difficult to forge, which is why biometric verification and authentication is commonplace in immigration control, law enforcement, and forensic studies. Many banks worldwide are already using biometrics with their banking systems to authenticate employees and customers and among all banks utilizing biometrics, and ability to offer more security than traditional personal identification numbers (PINs) and passwords.

Application of Biometrics in Banking.

Biometric technology is slowly replacing traditional passwords and token-based electronic access, signature-based branch service access, and PIN-based access in mobile banking and at ATMs. Here are ways that banks can use biometric technology to improve banking services and better protect customer assets.

Biometrics in Branch Banking.

Financial service institutions are using fingerprint and finger vein biometrics in banking for customer identification in their branches because these two biometric authentication methods deliver fast results that are suitable for the busiest branches of a bank. Moreover, finger print and finger vein systems are user friendly, easy to use and ensure reliable security. When customers visit branches they can be authenticated at the counter through fingerprint and finger vein biometric scanners that match the customer's existing biometric template within the bank database, and after successful authentication, the customer will be allowed to move forward with their banking transactions.

Biometrics in Banking ATMs.

Using biometrics in banking ATMs is popular in developed countries and the adoption rate is growing significantly. There are two approaches for customer authentication in ATMs - a customer using only biometrics and a bank card or a PIN along with biometric authentication. Therefore, facial recognition, fingerprints, finger vein patterns and iris recognition are the most suitable in ATMs as these biological traits can be easily authenticated in this environment. Furthermore, these types of biometric modalities also have other advantages such as flexibility, compactness, and accuracy.

Issues with the current ATM Network.

- ATM Card frauds;
- Use of ATM card duplicators;
- Card sharing by family and friends;
- Inability to trace the wrongful users;
- ATM PINs can be shared on phone or recorded using secret cameras.

Biometric ATM Solve the issues and Offer.

- Single/Multi factor Biometric Authentication: Fingerprint, Iris, Face, Pal vein;
- Multifactor Authentication: Card + PIN + Biometrics;
- Online or offline Authentication using smart cards;
- Card less Authentication " Biometrics is combination of card or PIN;
- Application of Biometric ATM;
- Banking & Finance;
- Food coupons / Tickets / Canteen ATM;
- Membership Verification ATM;
- Transaction / Check Deposit ATM;
- Self Service ATM;
- Retail ATM.

Other Solutions.

- Wall mount Biometric ATM & Transaction terminals;
- Full size Biometric ATM;
- Biometrics Touchscreen ATM.

3 Biometrics For Internet

Banking Many computers, laptops, and even smart phones already have webcams, microphones, and fingerprint scanners, offering flexibility for banks to easily adopt biometric authentication in online banking services with fingerprint, finger vein, facial, and voice recognition. When customers attempt to access their account, some banks now require them to provide a biometric credential first. Some banks require biometric authentication beside the traditional password to make authentication stronger, also known as a "multi-factor" authentication system. This helps banking institutions to protect customer identities from being compromised by cyber criminals and any others trying to illegally obtain sensitive customer information to commit a crime.

Biometrics in Mobile Banking.

Mobile banking is growing rapidly worldwide, and according to Juniper Research, 400 million people performed a mobile banking transaction in 2013. Despite this large number, many bank customers still have a lack of trust over the security of mobile banking platforms and concerns over security. Banking transactions or customer services could be performed through a voice or speech recognition system where customers need to verify their identity using the microphone in their phones.

With emerging cases of mobile banking fraud, banks have to ensure the ultimate protection of sensitive customer data with cutting-edge technology. Our experience in banking software development proves that biometric authentication can become an effective information security measure for banks.

Single Sign on Solution for More Effective Password Management.

Banks and financial institutions are suffering from network security and data breaches worldwide. According to a recent ACI Worldwide Survey, 44%of customer financial accounts have been compromised and 15% of breaches cause fraud. In a 2013 Pok?mon Institute Survey, it was reported that an average cost of these types of incidents is $9.4 million. Banks can easily adopt biometric single sign on (SSO) solutions into their network for password management, identity management, data and network security, and two factor authentications. This system will eliminate vulnerable passwords and loopholes of a bank data security system and will protect both banks and customers from unauthorized access and data breaches. Furthermore, a biometric SSO system will mitigate other security risks and regulatory fines for government compliance.

Providing indisputable client side authentication, file encryption, and password automation with strong encryption.

The increasing number of enterprise security data security breaches combined with the pressure on the financial services industry to implement methods of password management, identity management, data and network security, and two factor authentications has never been stronger. The sharing or theft of user passwords still remains the number one reason that corporate data is compromised. We help to solve this problem by allowing the financial services industry the ability to implement a centralized password management repository for single sign-on and secure access to internal applications. With convenient integration into Active Directory, our secure single sign-on password management software with a choice of fingerprint or finger vein biometrics leaves the IT department in complete control. With a single solution that supports strong authentication techniques; financial service institutions can protect corporate data while ensuring industry mandated compliance with regulations such as Sarbanes-Oxley. The authentication framework utilizes biometrics, smart cards, TPM security chips, tokens, and other devices to protect login, password management (single sign-on), file and folder encryption, email, VPN access, and other sensitive operations on the typical PC.

Single Sign on Solution for More Effective Password Management Benefits.

- Eliminate vulnerable passwords that are used to protect data, emails, login, etc.
- Easily scale from one to thousands of users with multiple types of authentication devices.
- Generate real-time reports showing which users are accessing specific PC's, networks, and applications.

4 Biometric Functionality

The phase comprises a series of steps (See Figure 1)- input acquisition, digital signal processing, and feature extraction and enrolment. The recognition process could be either identification or verification. The steps followed here are input acquisition, digital signal processing. The biometric sample could be a voice print which is an audio signal. Fingerprint, iris scan, facial scan which are all image signals. Images are digital Signals of a spatial type. Digital signal processing is essential to filter out noise and have the signal in the pure form. Usually, several filtration techniques and algorithms are employed to achieve this and prepare the input signal for feature extraction. Feature extraction is the process by which salient information in the biometric input that uniquely characterizes the input is extracted from the input. Feature extraction is a dimensionality reduction .The extracted features are hence encrypted and stored as a biometric template in a Database or memory chip. Feature extraction is done with the help of some computational algorithms. The extracted biometric data comprise a template. Enrolment is the process of registering a user biometric input in a database.

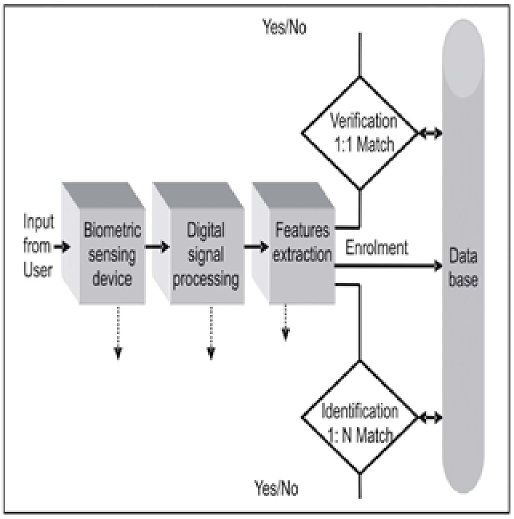


Figure 1: Automatic Biometric system ⋯ Richman Charles)

Memory chip in a card. The database is a collection of records of biometric templates of enrolled users. The blocks for verification and identification are decision boxes. Verification is a process of checking a user biometric input against a stored biometric and outputting a yes/no result.

Identification is the process of verifying a user biometric input against a database of many templates and outputting a present/absent result.

Finally a decision is taken by a biometric system depending on the set threshold for a Biometric decision in the recognition algorithm. A score generated on or above the Threshold grants a yes and a score below the threshold grants a 'no'.

In this Bio-Sec project (Figure 2), the roles and responsibilities were clearly defined as revolving around access provisions and authentication processes.

Finding of the case study conducted in this research work paved way in deriving the security framework of the Bo-sec project. An overview of the security framework indicating the RSA token process map that is aimed to support both security management policies and user guidelines is shown in Figure 3. Bio-Sec is proposed to provide two basic types of access control tools using finger print technology

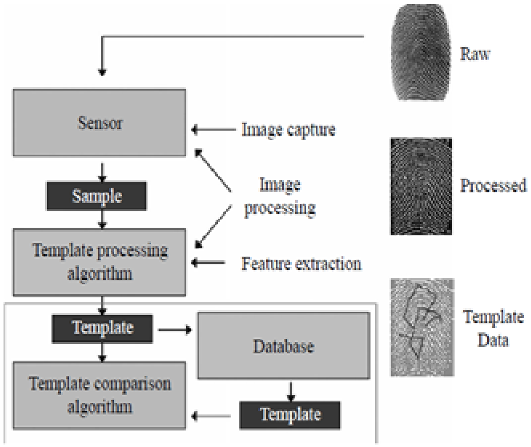


Figure 2: Proposed biometrics security components. Source–(Bio Sec project)

with Smartcards or Bio-Secure Integrated ID cards to be utilized for access to this service and SSL.

A Bio-Sec user group with 15 members was formed for providing feedback, testing and making recommendations on behalf of their own business transactions. Amendments to the security guidelines for the Bank's existing security framework were developed in consultation with the Bio-Sec user group. An action plan was developed to train the employees formally on the introduction and The integration of biometrics to their work environment. Any security program must include other managerial controls, means of recovering from breaches of security, and above all awareness and acceptance by the users to make an information system trustworthy. This study reveals that when qualities such as accuracy, ease of use, adaptability, and technological advantage are offered together, there is no question that biometrics will ensure a highly secure banking environment. Hence, project Bio-Sec was initiated to create a positive and secure data management policy by giving importance to human rights protection. It adopts a combination of biometric techniques with data management policies that could abide by data protection standards and laws (Figure 3).

5 Biometric Security

Biometric security is mainly implemented in environments with critical physical security requirements or that are highly prone to identity theft. Biometric security-based systems or engines store human body characteristics that do not change over an individual's lifetime. These include fingerprints, eye texture, voice, hand patterns and facial recognition.

An individual's body characteristics are pre-stored in a biometric security system or scanner, which may be accessed by authorized personnel. When an individual walks into a facility or tries to gain access to a system, the biometric scanner evaluates his/her physical characteristics, which are matched with stored records. If a match is located, the individual is granted access.

Biometric security devices play a crucial role in verifying a person's identity by enforcing access control methods through their unique biological traits. In this lesson, we will cover optical, fingerprint, and voice recognition, which are used to identify and authenticate a person, as well as cover the pros and cons of using these devices.

Retina and Iris Recognition: Retina scanners use the blood vessels in the back of the eye for authen-

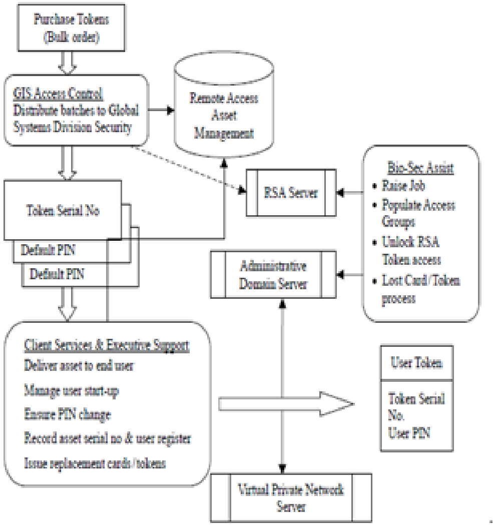


Figure 3: Bio Sec RSA token process map. Source by (Bio Sec project)

tication. The blood vessel pattern in the back of the eye is unique to the individual. This method is very intrusive and is not widely accepted because it breaches a person's medical privacy. For example, possible discovery of disease in the eye or other medical conditions may alert the company and can cause employment issues.

The iris scanner, which measures an individual's iris pattern, is non-intrusive. Each person has a different color pattern in the iris, and therefore, the iris scanner is used to measure these characteristics. It is more popular within the security field.

Replay attack (also known as a playback attack) is when a person uses someone else's credentials without their permission. The chances of replay attacks are very low on retina and iris scanners because it is nearly impossible to copy the retina and iris of someone else to use for impersonation. While retina and iris recognition systems do keep information and areas safe from intruders, these systems are very expensive. A good way to remember that the retina scanner is the more intrusive of the two when it comes to medical privacy of Retina is intrusive

The many faces of biometrics, there are a lot of biometric identifiers:

- Finger/palm vein: Using unique vein patterns present beneath the skin's surface in a finger or palm.

- Fingerprint recognition: Confirming identity based on the comparison of two fingerprints. This method is especially popular with mobile devices.

- Voice/speaker recognition: Refers to recognizing an individual by the characteristics of their voice (as opposed to speech recognition, which recognizes what is being said).

- Face recognition: Using various technologies such as computer algorithms or 3D sensors to recognize a face using measures such as relative position, shape or size of eyes, nose, jaws and more.

- Iris recognition: Leverages the complex patterns of the irises in the eye of each individual.

- Retinal scanning: Often confused with iris recognition, refers to the identification of blood vessels in the human retina.

- Handwritten signature: Using handwritten signature patterns to identify an individual.

However, finding a biometric identifier is merely the first step to making it a feasible technology for the banking industry. That's because each method worth consideration must be highly secure, provide protection from piracy, be socially acceptable, be practical and simple to use, and universal. As a result, only some biometric technologies have already made their way into banking mainstream. In particular, it's finger vein, fingerprint, face, voice and handwritten signature.

Biometric technologies in banking are still rapidly growing. And the trend is sure to continue. It's not surprising, considering just how many benefits it provides for financial institutions. Aside from minimizing various security risks (both internal and external frauds) and improving customer user experience, it can also greatly help in cost optimization. By introducing biometrics into its banking processes, it's possible to eliminate the bulk of paper documents and cards and reduce time dedicated to customer service and call center operations.

6 Biometrics Adopted

Countries Biometrics is a technology powered method of personal identification that leverages unique biological patterns on and in human body. These irregular and asymmetric patterns are found in iris and retina inside eyes, fingerprints, vein pattern beneath the skin, facial pattern, DNA sequence, voice print, gait, typing rhythm, etc. Irregularities in formation of these patterns make them good enough to be considered as unique for a person. For example, in over 100 year's history of fingerprinting, fingerprints from different fingers were never found to be the same. Biometric characteristics do not even repeat in twins and they remain unchanged throughout the life of a person. Different fingers of same person too have different fingerprints. These qualities of biometric traits make them an ideal method for personal identification.

Some of the banks that have already adopted biometric identification and authentication to address inadequacies of traditional system worldwide.

Lloyds Banking Group plc. which is one of the major financial institutions serving business as well as individual customers, has partnered with Microsoft to enable their customers to login to their banking services and authenticate transaction with fingerprint and facial recognition. User biometric data will be stored locally and encrypted to safeguard it from any misuse. Lloyds Banking Group becomes the first financial institution to have this kind of partnership with Microsoft. It is expected to enhance user experience and security. With this implementation, customers can login into their Lloyds Bank, Halifax and Bank of Scotland internet banking sites.

KB Kookmin Bank: It was ranked first among mobile banks by Brand stock at Korea's Highest Brand of the year survey in 2016. This achievement was the result of KB Kookmin Bank's continuous efforts towards biometric enabled secure mobile banking. It was among a few that leveraged iris scanner of a mobile device to authenticate customer for accessing their account. This functionality was originally provisioned for Samsung's flagship device Galaxy Note 7, but the mobile phone maker had to recall the devices amid multiple instances of device battery exploding or catching fire. However, with the launch of Samsung Galaxy S8, KB Kookmin updated its mobile banking app for the new smartphone to leverage the iris scanner of the device. User authentication with iris for accessing accounts was made possible by Samsung Pass API (Application Programming Interface), which enables partners to leverage the iris scanner of device for user authentication. Authentication with iris scanner is set to enhance user experience as customers had to go through rigorous verification process in the past to prove their identity.

Australia and New Zealand Banking Group, popularly known as ANZ Bank has announced that it will be using voice biometrics for customer identification and authentication. This will help secure transactions over $1000 and enhancing user experience at the same time. This feature will be available to ANZ bank's staff and select user group initially as a test run and will be rolled out for all the customers later this year. This initiative is the next step towards safer and convenient mobile banking using customer biometrics. ANZ will use the same voice print technology being used by Barclays Wealth, which is one of the major financial institutions. The voice print solution is provided by Nuance, which is world-leader in voice recognition and voice biometrics technology, providing speech recognition and speaker recognition solutions to numerous clients across the globe. With this solution, customers will be able to authenticate with their voice via ANZ Go Money mobile app. Voice recognition feature will also be rolling out to ANZ's other digital services as well.

JP Morgan Chase is one the largest multinational banking and financial services companies serving millions of individual, government and corporate clients. With its foundation dating back over 200 years, it is one of the oldest financial institutions in the United States. JP Morgan Chase has abandoned password based authentication for its mobile app in favor of inbuilt biometric fingerprint sensor on iOS and Android mobile devices. It has even eliminated need of passwords for authenticating money transfers or payments which was earlier a mandate, even if customers had enabled fingerprint security. Chase has confirmed that none its mobile app functions will require passwords based authentication, making user fingerprints the sole guardian of banking security.

Oversea-Chinese Banking Corporation Limited or OCBC Bank is Singapore's oldest local bank. Starting off with local banking services, OCBC bank now has offices in 18 countries serving individual as well as business clients. The bank has upgraded its mobile banking app with a feature called OCBC One Touch, which is basically the integration of Apple Touch ID with the mobile banking app. With this feature, OCBC customers can check account balance and time deposits as well as status of incoming or outgoing funds, with just the touch of a finger. Users need to login with User ID and password and activate the feature within the app. The OCBC mobile banking app with fingerprint integration is available for Touch ID enabled iPhones running iOS version 8 or above. For Android, the feature is available only on select Samsung's Android devices; however, the bank has plans to bring the functionality to other Android devices as well.

MasterCard Headquartered in New York, provides its payment processing and payment card services around the world. The company is leveraging facial biometrics for payment authentication, colloquially known as "Elfie Pay". User can authenticate a payment by capturing their face on their smartphone camera. The feature has been rolled out in several countries with many others to follow. MasterCard has plans to make the technology available across the globe in the future. MasterCard calls this technology MasterCard Identity Check, which leverage user smartphone's camera or fingerprint sensor to authenticate a payment, users can use either to verify their identity.

Gulf Bank is one of the major banking and financial services companies of Kuwait, offering wide range of financial products and services across the country. The bank has partnered with Doan; a company specialized in biometric solutions, to integrate its mobile banking application with IdentityX biometric platform. IdentityX platform is developed by Daon to impart biometric ability across a wide range of applications. This integration will enable Gulf Bank customers to authenticate identity with their biometric identifiers like fingerprints and facial features to access their account on mobile banking app. The bank expects that integrating biometric authentication will enable customers to perform wide array of banking transactions efficiently and securely.

Nequi is a digital-only subsidiary of Bancolombia, the largest bank of Colombia. Nequi provides financial service via smartphones on Android as well as IOS mobile platforms. Users can save, send or receive money, make payments and withdraw money from Ban Colombia ATMs. Nequi has implemented biometric integration to its app in partnership with Daon, a company specialized in biometric solutions.

With this integration, Nequi customers will be able to authenticate their identity with a selfie. Whenever they reset password, change SIM card or reactivate their accounts, app will ask for user authentication, which is as easy as taking a selfie. The app makes use of biometric facial recognition technology to identify and authenticate users. Nequi is also looking to introduce voice authentication in future to layer the security of its services

Citi Group Inc. is an American multinational financial institution providing financial services across the globe. With several subsidiaries around the world, Citi Group is the 4th largest bank in the United States in terms of assets and ranked 29th on Fortune 500 list in 2016 in terms of size. Citi group became the first company that launched voice authentication in May 2016 across Asia Pacific region, which was widely adopted by the customers and hit a million marks in March 2017, much earlier than anticipated. Citi Bank customers from Australia, Hong Kong, India, Malaysia, Philippines, Singapore, Taiwan, Thailand and Vietnam are leveraging voice biometric.

Authentication to access the financial Services provided by the bank.

Voice authentication is providing frictionless access to information and transactions by eliminating requirement of manual identity verification, which is not only time consuming but also frustrating at times. Remembering PINs or answers of security questions to verify identity is another burden that biometric voice authentication has eliminated.

Riding the wave of biometric authentication, Citi Bank is set to safeguard more of its services with it. The bank is going to introduce an application that will bring banking, money movement and wealth management services in one application. The application will make use of user biometrics to safeguard and authenticate transactions. This step is in line with bank's new operating model.

7 Biometric Payment

The biometrics industry as a whole has enjoyed considerable growth in recent years, and not least in the financial services sector. More and more banking and other financial transactions are being done online, and fraudsters have followed suit, launching ever-more sophisticated attacks. As the risk of digital fraud and theft has escalated, many organizations have looked for solutions in the form of biometric security. These kinds of solutions also happen to be way more convenient for end users, who appreciate being able to replace a complicated password with a fingerprint or face scan.

With these factors in play, the rise of biometric FINTECH has only become more pronounced in recent years and months. Here are some of the latest trends in the ongoing ascent of biometric banking and payments:

- The rise of mobile payments means the rise of biometric authorization.
- Biometric authentication is also coming to physical payment cards.
- And biometrics are increasingly being used for account access, even replacing debit cards at the ATM.

8 Prospect For Tech Profits

In just the last year, the application of biometrics has virtually exploded. It is now seen as a secure method for providing authentication in order to prevent fraud in online banking. According to recently released research data, the use of biometrics in financial and banking services is expected to top $8 billion by the year 2020.

Innovative technologies are now addressing these security concerns. Among the foremost technologies paving the path for the future of data security is biometrics. Biometrics is certainly not a new concept, but until the iPhone 5S, featuring a Touch ID fingerprint reading sensor, hit the market, biometrics were largely relegated to high-security facilities. When Apple purchased AuthenTec in 2012, it may have been among the first smartphone companies to provide biometric technology, but it certainly was not the last. Samsung quickly followed suit with a similar technology in the Galaxy S5. As the dawn of a digital payment age advances, the banking industry has begun to investigate increasingly innovative methods of authentication. While the use of thumbprints is included in this array of methods, the tools for facilitating unique identification that are emerging are by no means combined to identification systems based on fingerprints.

Funding is also being generated for other technology that can be used to ensure a secure, and foolproof, identification process, which is so critical to such sectors as the banking industry. Eye-Verify, the creator of Eye-print ID, for instance, announced the completion of a Series. An equity funding round last summer to the tune of $6 million. Companies participating in that round of funding included Wells Fargo and Sprint. As a result of that round of funding, Eye-Verify will be able to spur mass adoption of its distinctive Eye-print ID biometric technology in a more direct manner in various markets, including financial services.

Investing in Biometrics: As the future of the banking industry becomes increasingly interconnected with biometric technology, more and more investors have begun to direct their own funds toward the financing of biometrics initiatives. Prior to taking such a plunge, however, it is important to conduct due diligence.

Investors considering investing in biometrics targeted at the banking industry will discover there are certainly numerous reasons for doing so, including the potential for unparalleled growth and the opportunity to invest early in the adoption cycle within a developing marketplace. While potential profits associated with early-stage investing in a technology such as biometrics are undeniably appealing, investors must ensure they do not fall for the hype surrounding the industry. Biometrics can be quite broad in nature, including everything from iris scans to fingerprint identification to cardiac signatures. Taking the time to understand as much as possible about the technology behind a new security measure is vital to protecting your investment.

Biometrics for the banking industry is still in the early stages, but it is quickly evolving into a global standard. Investing in biometrics now could prove to be a lucrative opportunity as banks around the world begin the race toward heightened security.

Biometrics can provide a number of important security measures. Do not assume that a company is a sound investment simply because it boasts that its technology is based on biometrics. Prospective investors considering investing in biometric technology in the banking industry would do well to take the time to understand as much as possible about the technology, why it makes sense in that particular application, and whether the technology has the potential for widespread adoption.

9 Important Factors Of Biometric

In Banking And Financial Services Industry The future of biometric authentication technology looks rather promising, as the number of mobile devices with biometric capabilities constantly grows [1]. Besides, a new study by Grand View Research estimated that in less than a decade the global biometrics technology market. Apart from the market trend, several reasons exist why banks should take advantage of biometric technology.

Biometrics is infiltrating the financial industry. As the digital age expands, it is important to find a balance between security and accessibility. Electronics have permeated virtually every aspect of our lives. As we store more and more information online or in mobile apps, it is important to strike a balance between security and accessibility. But, memorizing dozens of passwords had many consumers overwhelmed. Now, the focus is shifting towards implementing efficient, user-friendly security measures that will still provide exceptional protection. Traditional passwords are becoming a thing of the past.

Biometrics is quickly finding their place in banking security. Because certain traits -like fingerprints, eyes, and heart rate- are uniquely our own, they offer a potential for greater security than passwords. While passwords can be shared (intentionally or otherwise), biometrics are extremely difficult to replicate. Despite all the excitement, biometric technology still has a while to go before it can be completely dependable. Here are four important factors to be aware of as we keep our eye on biometrics.

They are device dependent: Biometric security features like voice, face, or fingerprint recognition most likely require a specific device in order for users to access their personal information. This could lead to problems if passwords are completely eliminated. If banking apps require biometrics authentication to access accounts, and those security measures require certain devices, they risk isolating a percentage of customers. Instead, banks should take a hybrid approach when implementing biometrics. Richard Parris, chief executive at Intercede, said that instead of only using biometrics, ”businesses need to be looking at strong authentication that incorporates three distinct elements- possession (something you have, such as a smartphone), knowledge (something you know, such as a PIN), and inherence (something you are, such as an iris scan).” This combination of new technology with existing access control will allow for a smoother transition into biometrics, as well as extreme accountability. However, it is also important to continue research on accessible biometric features beyond devices.

Protecting Banking Information - Biometric technology provides the strongest method of authentication that protects banking information from being compromised by unauthorized personnel.

Fast and Accurate Branch Banking: Biometric technology provides fast and accurate identification for the banking industry. Customers can be quickly authenticated in mere seconds through a fast biometric scan. ” Protection against Insider Fraud: Biometric identification of employees performing transactions on the back end is a crucial step to ensuring identity protection and reducing fraud. Biometrics in banking will help financial institutions to prevent insider fraud by establishing secure employee authentication, accountability and concrete audit trail of each transaction.

Secure Online Banking: Over the past years the banking sector has been suffering from massive online service cyber-attacks. In most of these cases customers lose their money from the negative effects of identity theft. Biometrics in banking helps the bank to protect customer identities when using online banking services.

ATMs with Biometrics: Biometrics in banking for ATMs authentication brings outstanding benefits to both customers and banks. This system now gives customers flexibility to make transactions without bringing bank cards. Banks can avoid the costs and liabilities of customer problems due to lost or stolen bank cards.

Audit Trails: Banks can easily track and monitor employee and customer activity in the system to create concrete audit trails with biometric technology solutions.

Fast, Secure and Accurate Customer Care Service: The banking sector is always in need of tighter security solutions to provide improved and more secure customer care service over the phone and internet.

A biometric voice recognition system for example provides a secure and flexible solution to verify any customers executing transactions outside of a brick and mortar environment.

Demand is high, but experience is not: A study by the Department of Computer Science at the University of Oxford and MasterCard showed that 93 percent of consumers in the finance sector are interested in using biometric authentication methods. However, consumers seem to be a few steps ahead of professionals in the financial industry. While 92 percent of the industry says they’re interested in deploying mobile biometrics, only 13 percent have already done so. Perhaps this is because although 88 percent of professionals expect to be involved in decisions regarding biometrics, only 36 percent of them believe they have adequate experience. Two thirds of the professionals say they have little to no experience at all. Biometrics is a learning curve for everyone. But, before a new form of banking security can be implemented, it must be fully understood.

There's no doubt biometrics are on the rise for banking security, but it may be a while before identity authentication without passwords is completely secure.

10 Research Methodology

This research study adopts a qualitative approach where previous studies related to biometrics were analyzed and discussed. This study is completely based on the literature review and the findings and suggestions were recommended based on the analysis review. Various studies related to biometrics in the past were considered and critically evaluated in the context of the banking and financial industry to develop the research of the study.

10.1 Findings

It was clearly identified that most of the studies related to acceptance of the technology considered the TAM model which clearly reveals that Still TAM is considered as a relevant model when it comes to the acceptance of technology to understand the attitude of human behavior and intention to accept the technology which is biometrics in the context of this study. The major determinants which relate to the intention to adopt the mentioned technology are perceived usefulness and the ease of use. Apart from this the concept of Self efficacy was also identified as a contributing factor in order to accept the technology. Therefore it is very clear that the perception of users towards the adoption of biometrics in banking and financial industry is directly influenced by the attitude of users and their intention to make use of the technology.

10.2 Contribution of the Study

The biometric technology has been in talks for a long time especially in the financial sector. Many studies have considered using finger prints as an additional security measure but since the development of mobile banking there is an emphasis on the voice enabled security which is an added advantage. According to a study by Mercator Advisory Group on payment authentication points out that "biometrics has been long on promise and short on delivery". The scope of biometrics is large in financial service industry especially in countries like Latin America and Europe. Having a voice authentication as a biometric measure in the field of financial service would enhance the security and effectiveness of the system. The study has contributed both theoretically and academically, the paper brides the gaps in the existing literature and also recommends to implement voice enabled biometric authentication for better banking operations.

11 Conclusion

Though biometric authentication doesn't ensure 100% effectiveness, it's currently far more effective than passwords alone. And if banks combine the commonly used passwords with biometrics, they can bring in a two-factor authentication system that is now considered the most secure method to prevent data breaches in the banking industry.

Due to the role of customer trust and loyalty in the success of banks, and thus in the economic development of countries, banks should provide convenient and more secured banking services to customers. Biometric technology, integrated with an existing traditional security system, will empower banks to deploy the highest level of authentication security possible.

Of course, biometric technologies are not completely immune to frauds. Experts also need to be wary of people's attitude to various identifiers - fingerprinting is not the only one that many individuals find objectionable. Another problem is the fact that on rare occasions, due to illness or advanced, it's difficult or impossible to identify an individual using certain metrics (e.g. skin lesions & fingerprinting or blood vessel diseases). Some ways in which banks attempt to counter it is employing more than one biometric identifier at the same time.

Despite all these issues, various biometric technologies have repeatedly proven to be both more secure and convenient that any traditional way of authenticating users. Considering just how much has been achieved in the banking industry only in the past 10 years, it can be expected that biometric technologies for authentication will continue to be refined for the good of everyone. We should all keep our fingers crossed.

References

[1] R. C. Agidi, "Using biometric in solving terrorism and crime activities in Nigeria," *Techsplend Journal of Technology*, vol. 1, no. 12, Jan. 2018.

[2] Board of Governors of the Federal Reserve System, *Consumers and Mobile Financial Services 2016*, Mar. 2016. (https://www.federalreserve.gov/econresdata/consumers-and-mobile-financial-services-report-201603.pdf)

[3] A. Chuvakin, *Highlights from Verizon Data Breach Report 2015*, July 20, 2017. (http://blogs.gartner.com/anton-chuvakin/2015/05/18/highlights-from-verizon-data-breach-report-2015/)

[4] J. Conroy, *Moving Beyond the Password: Consumers' Views on Authentication*, Mar. 21, 2017. (http://www.aitegroup.com/report/moving-beyond-password-consumers%E2%80%99-views-authentication)

[5] S. Furnell and K. Evangelatos, "Public awareness and perceptions of biometrics," *Computer Fraud and Security*, vol. 2007, no. 1, pp. 8-13, 2007.

[6] Grand View Research, *Biometrics Technology Market Analysis Report By End-Use (Government, Banking & Finance, Transport/Logistics, Defense & Security), By Application (AFIS, Iris, Non-AFIS), and Segment Forecasts, 2018 - 2025*, Market Research Report, Sep. 2018. (http://www.grandviewresearch.com/industry-analysis/biometrics-industry)

[7] D. Kumar, Y. Ryu, "A brief introduction of biometrics and fingerprint payment technology," in *Second International Conference on Future Generation Communication and Networking Symposia*, 2008.

[8] J. Lee, *Biometric Authentication to be Used in over 600M Mobile Devices by 2021: Juniper Research*, Nov. 29, 2016. (http://www.biometricupdate.com/201611/biometric-authentication-to-be-used-in-over-600m-mobile-devices-by-2021-juniper-research)

[9] S. Venkatraman and I. Delpachitra, "Biometrics in banking security: A case study," *Information Management & Computer Security*, vol. 16, no. 4, pp. 415-430, 2008.

Biography

Richman Charles Agidi

Algorithms for Subset Sum Problem

Lihua Liu[1], Lili Wang[1], Zhengjun Cao[2], Xiqi Wang[2]

(Corresponding author: Zhengjun Cao)

Department of Mathematics, Shanghai Maritime University, Haigang Ave 1550, Shanghai, 201306, China[1]

Department of Mathematics, Shanghai University, Shangda Road 99, Shanghai, 200444, China[2]

(Email: caozhj@shu.edu.cn)

(Received Sept. 29; Revised and accepted Nov. 3, 2018)

Abstract

Given a set (or multiset) S of n numbers and a target number t, the subset sum problem is to decide if there is a subset of S that sums up to t. There are several methods for solving this problem, including exhaustive search, divide-and-conquer method, and Bellman's dynamic programming method. However, none of them could generate universal and light code. In this paper, we present a new deterministic algorithm based on a novel data arrangement, which could generate such code and return all solutions. If n is small enough, it is efficient for usual purpose. We also present a probabilistic version with one-sided error and a greedy algorithm which could generate a solution with minimized variance.

Keywords: Deterministic Algorithm; Dynamic Programming; Greedy Algorithm; Knapsack Problem; Probabilistic Algorithm; Subset Sum Problem

1 Introduction

In computer science the subset sum problem is that: given a set (or multiset) of numbers, is there a non-empty subset whose sum is equal to a given number? The problem is generally expressed as follows: given numbers $w_1, \cdots, w_n$ along with a target number t, the task is to determine whether there exists a subset $X \subset \{1, \ldots, n\}$ such that

$$w(X) := \sum_{i \in X} w_i = t$$

Such an X is referred to as a solution. For example, $t = 5, w_1 = 1, w_2 = 2, w_3 = 3, w_4 = 4$. Clearly, $5 = 1 + 4 = 2 + 3$. It has two solutions.

This problem is related to knapsack problem and has many applications in computer sciences [4, 5, 10, 15, 19, 21, 22, 24]. For example, in 2017 Lee [14] studied the sparse subset sum problem in fully homomorphic encryption. Curtis and Sanches [14] discussed the implementation of an algorithm for subset-sum problem on GPU. Kolpakov *et al.* [13] analyzed the complexity of solving the subset sum problem with the branch-and-bound method. In 2018, Gourves [7] investigated subset sum problems with digraph constraints. Nikolaev and Ushakov [16] extended subset sum problem to polycyclic groups. Wang and Nguyen [23] proposed the k-subset sum problem over finite fields. Pferschy *et al.* [18] discussed a Stackelberg subset sum game.

In 1956, Bellman [2] introduced the dynamic programming method for subset sum, which was revisited [17, 20]. Let $A = \{w_1, w_2, \cdots, w_n\}$ and $A_j = \{w_1, w_2, \cdots, w_j\}$, $1 \leq j \leq n$. Let $T[A_j, t] = 1$ if

t can be expressed as the sum of some members of A_j, otherwise $T[A_j, t] = 0$. We have the following recurrence formula

$$T[A_j, t] = \max\{T[A_{j-1}, t], T[A_{j-1}, t - w_j]\} \tag{1}$$

It is claimed that Bellman's method solves subset sum problem in $O(nt)$ time. In fact,

$$\begin{aligned}
T[A_j, t] &= \max\{T[A_{j-1}, t], T[A_{j-1}, t - w_j]\} \qquad \text{(1 addition)}\\
&= \max\{T[A_{j-2}, t], T[A_{j-2}, t - w_{j-1}], T[A_{j-2}, t - w_j], T[A_{j-2}, t - w_j - w_{j-1}]\} \ \text{(2 additions)}\\
&= \max\{T[A_{j-3}, t], T[A_{j-3}, t - w_{j-2}],\\
&\qquad T[A_{j-3}, t - w_{j-1}], T[A_{j-3}, t - w_{j-1} - w_{j-2}],\\
&\qquad T[A_{j-3}, t - w_j], T[A_{j-3}, t - w_j - w_{j-2}],\\
&\qquad T[A_{j-3}, t - w_j - w_{j-1}], T[A_{j-3}, t - w_j - w_{j-1} - w_{j-2}]\} \qquad \text{(4 additions)}\\
&= \max\{\cdots\}.
\end{aligned}$$

At the worst case, the method needs $O(2^n)$ additions and stores nt numbers of 1 or 0. Note that it is somewhat difficult to convert the recurrence method into universal and light code because of its naive data arrangement.

There are other several methods to solve subset sum problem, such as [3, 6, 8, 11, 12].

Very recently, Koiliaris and Xu [12] have introduced a new version of divide-and-conquer method for subset sum problem. It aims to improve the "conquer" step by taking advantage of the structure of the related sets. In 2017, Bringmann [3] presented a new algorithm for subset sum problem. For sets A, B of non-negative integers, it defines

$$A \oplus B = \{a + b \,|\, a \in A \cup \{0\}, b \in B \cup \{0\}\} \tag{2}$$

For any integer $t > 0$, define

$$A \oplus_t B := (A \oplus B) \cap \{0, \cdots, t\} \tag{3}$$

Given a set Z, randomly partition it into $Z = Z_1 \cup \cdots \cup Z_{k^2}$, i.e., assign any $z \in Z$ to a set Z_i where i is chosen independently and uniformly at random in $\{1, \cdots, k^2\}$. The basic subroutine of Bringmann's algorithm is the following.

ColorCoding(Z, t, k, δ): Given a set Z of positive integers, target t, size bound $k \geq 1$ and error probability $\delta > 0$, we solve SUBSETSUM with solution size at most k.

```
1: for $j = 1, \cdots, \lceil \log_{4/3}(1/\delta) \rceil$ do
2:     randomly partition $Z = Z_1 \cup \cdots \cup Z_{k^2}$
3:     $S_j = Z_1 \oplus_t \cdots \oplus_t Z_{k^2}$
4: return $\cup_j S_j$
```

Let $n_i = |Z_i| + 1$ for $i = 1, 2, \cdots, k^2$. In the Step 3 of each round, this algorithm needs

$$n_1 n_2 + \min\{n_1 n_2, t\} n_3 + \min\{\min\{n_1 n_2, t\} n_3, t\} n_4 \leq n_1 n_2 + t(n_3 + \cdots + n_{k^2}) \approx |Z| t.$$

Therefore, it takes $O(\lceil \log_{4/3}(1/\delta) \rceil |Z| t)$ additions totally. We would like to point out that none of these algorithms could generate concise and amicable code. Moreover, none of them can return all solutions for a usual set.

In this paper, we present a new algorithm based on a novel data arrangement, which could generate universal and light code and return all solutions. If n is small enough, it is efficient for usual purpose. We also present a probabilistic version for returning only a solution which runs in polynomial time with one-sided error, and a greedy algorithm which could generate a solution with minimized cardinal and variance.

2 A Deterministic Algorithm for Subset Sum Problem

2.1 Description of the New Algorithm

The new algorithm aims to find all solutions of the subset sum problem, $(w_1, \cdots, w_n; t)$. As we know, the general exhaust search method needs to compute $2^n - 1$ values,

$$\begin{aligned}
&w_1, w_2, \cdots, w_n, \\
&w_1 + w_2, w_1 + w_3, \cdots, w_1 + w_n, w_2 + w_3, \cdots, w_{n-1} + w_n, \\
&\cdots, \\
&w_1 + w_2 + \cdots + w_n.
\end{aligned}$$

and compares them with the target number t one by one. Note that these values are arranged naively which could not generate light programming code. Nevertheless, we find the following data arrangement is more heuristic.

$$t; t - w_1; t - w_2, t - w_1 - w_2; t - w_3, t - w_1 - w_3, t - w_2 - w_3, t - w_1 - w_2 - w_3;$$

$$t-w_4, t-w_1-w_4, t-w_2-w_4, t-w_1-w_2-w_4, t-w_3-w_4, t-w_1-w_3-w_4, t-w_2-w_3-w_4, t-w_1-w_2-w_3-w_4; \cdots$$

Surprisingly, *each item in the above sequence can be written down using only its position k*. For example,

if $k = 14$, $2(k-1) = 2(14-1) = 26 = (11010)_2$, and the item is $t - w_1 - w_3 - w_4$;

if $k = 9$, $2(k-1) = 2(9-1) = 16 = (10000)_2$, and the item is $t - w_4$;

if $k = 5$, $2(k-1) = 2(5-1) = 8 = (1000)_2$, and the item is $t - w_3$.

Based on this crucial observation, we present a new algorithm for subset sum problem as follows.

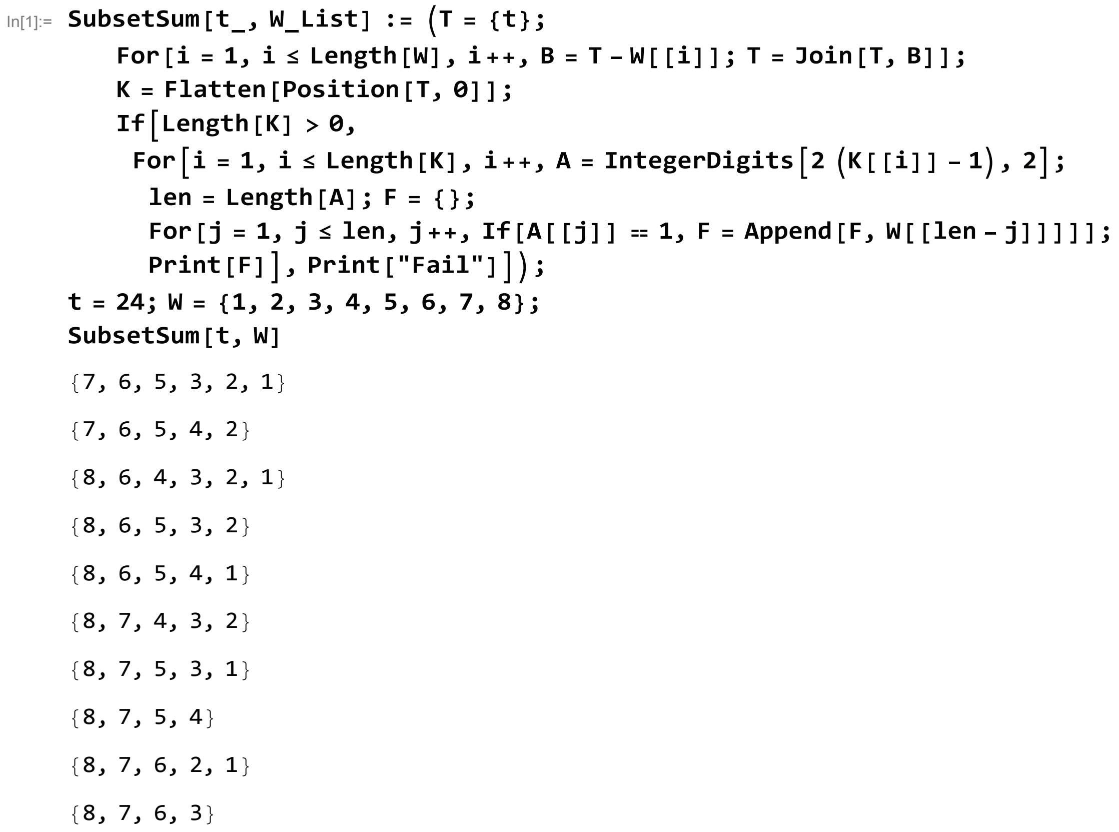
```
**Input**: $t, W = \{w_1, \cdots, w_n\}$.
**Output**: All solutions of $t$ with respect to $W$.
1: Compute $t, t - w_1, t - w_2, t - w_1 - w_2, \cdots, t - w_1 - w_2 - \cdots - w_n$.
2: Find all positions of 0 in the above sequence.
3: For each position $k$, compute the binary string $b_i b_{i-1} \cdots b_1 b_0$ of $2(k-1)$,
   and write down the solution $\{b_i \times w_i, b_{i-1} \times w_{i-1}, \cdots, b_1 \times w_1\}$.
```

We refer to the following Figure 1 for the light Mathematica code of the algorithm.

2.2 Complexity

The new algorithm is a variation of general exhaust search. Its novel data arrangement results directly in the practical and light code. It depends neither on any special property of the target number t, nor on the properties of the given sequence. So, it is universal for all cases.

It needs $O(2^n)$ basic arithmetic operations and stores $O(2^n)$ numbers. Clearly, if n is small enough, it works well. Otherwise, it becomes very hard because subset sum is a classical NP-complete problem [1,9]. However, it is the first algorithm for subset sum problem which *returns all solutions*.



```
In[1]:= SubsetSum[t_, W_List] := (T = {t};
          For[i = 1, i ≤ Length[W], i++, B = T - W[[i]]; T = Join[T, B]];
          K = Flatten[Position[T, 0]];
          If[Length[K] > 0,
           For[i = 1, i ≤ Length[K], i++, A = IntegerDigits[2 (K[[i]] - 1), 2];
            len = Length[A]; F = {};
            For[j = 1, j ≤ len, j++, If[A[[j]] == 1, F = Append[F, W[[len - j]]]]];
            Print[F]], Print["Fail"]]);
        t = 24; W = {1, 2, 3, 4, 5, 6, 7, 8};
        SubsetSum[t, W]

        {7, 6, 5, 3, 2, 1}

        {7, 6, 5, 4, 2}

        {8, 6, 4, 3, 2, 1}

        {8, 6, 5, 3, 2}

        {8, 6, 5, 4, 1}

        {8, 7, 4, 3, 2}

        {8, 7, 5, 3, 1}

        {8, 7, 5, 4}

        {8, 7, 6, 2, 1}

        {8, 7, 6, 3}
```

Figure 1: The practical code for the deterministic algorithm

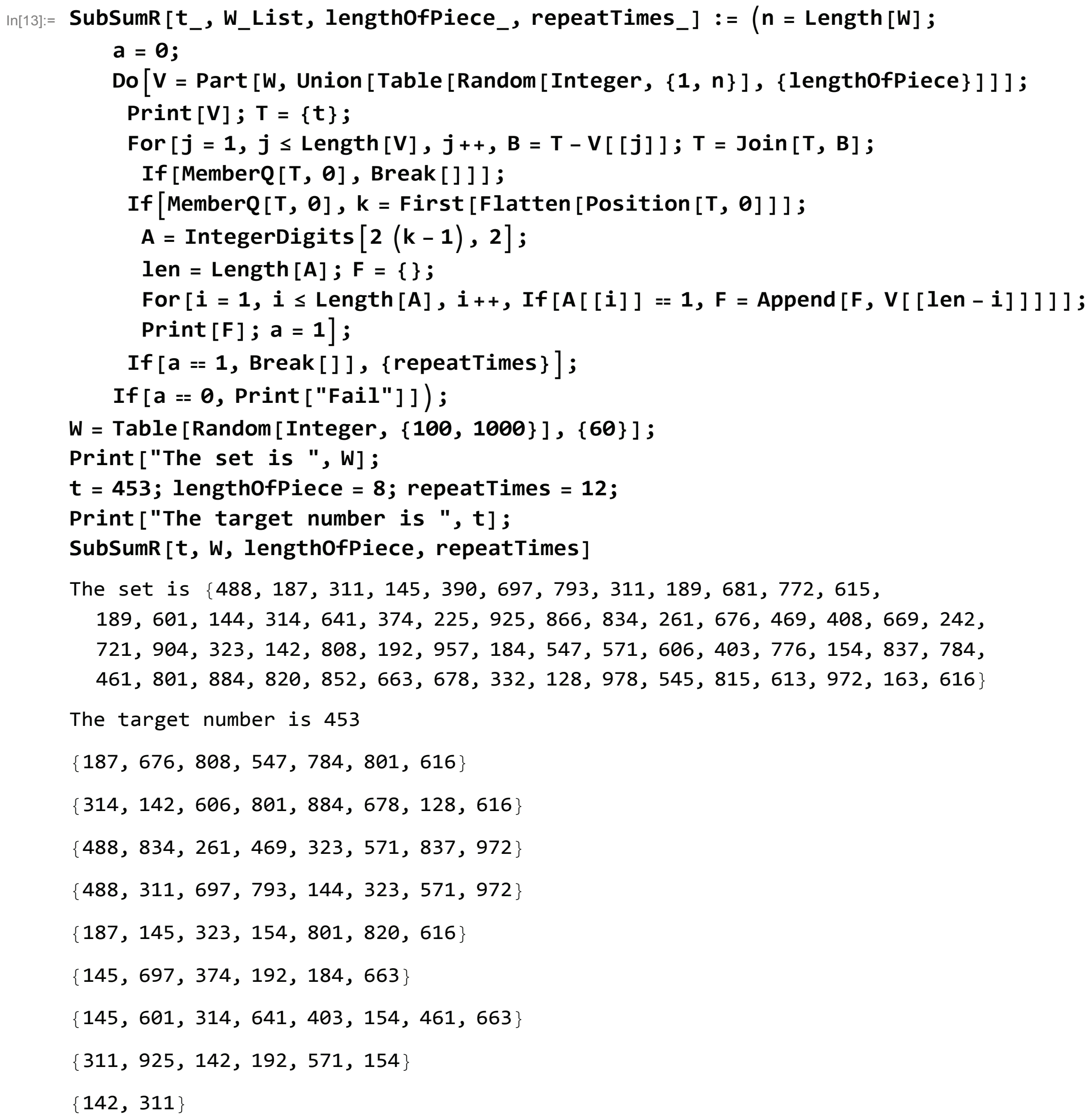
3 A Probabilistic Algorithm for Subset Sum Problem

If n is large and only one solution is wanted, one can randomly permutate the original sequence and truncate it into a short piece. Then repeat the process many times. The probabilistic algorithm can be described as follows.

```
**Input**: $t, W = \{w_1, \cdots, w_n\}$.
**Output**: A solution of $t$ with respect to $W$, or the failure notation “$\perp$”.
1: Randomly permutate the sequence $w_1, \cdots, w_n$ and
    truncate it into a short piece $w'_1, w'_2, \cdots, w'_k$.
2: Compute $t, t - w'_1, t - w'_2, t - w'_1 - w'_2, \cdots$.
3: Find the first position of 0 in the above sequence. For the position $k$,
    compute the binary string $b_i b_{i-1} \cdots b_1 b_0$ of $2(k-1)$ and write down
    the solution $\{b_i \times w'_i, b_{i-1} \times w'_{i-1}, \cdots, b_1 \times w'_1\}$.
4: If Step 3 fails, goto Step 1 and repeat the process for many times.
```

See the following Figure 2 for the practical code.

Figure 2: The practical code for the probabilistic algorithm



```
In[13]:= SubSumR[t_, W_List, lengthOfPiece_, repeatTimes_] := (n = Length[W];
            a = 0;
            Do[V = Part[W, Union[Table[Random[Integer, {1, n}], {lengthOfPiece}]]];
             Print[V]; T = {t};
             For[j = 1, j ≤ Length[V], j++, B = T - V[[j]]; T = Join[T, B];
              If[MemberQ[T, 0], Break[]]];
             If[MemberQ[T, 0], k = First[Flatten[Position[T, 0]]];
              A = IntegerDigits[2 (k - 1), 2];
              len = Length[A]; F = {};
              For[i = 1, i ≤ Length[A], i++, If[A[[i]] == 1, F = Append[F, V[[len - i]]]]];
              Print[F]; a = 1];
             If[a == 1, Break[]], {repeatTimes}];
            If[a == 0, Print["Fail"]]);
         W = Table[Random[Integer, {100, 1000}], {60}];
         Print["The set is ", W];
         t = 453; lengthOfPiece = 8; repeatTimes = 12;
         Print["The target number is ", t];
         SubSumR[t, W, lengthOfPiece, repeatTimes]

         The set is {488, 187, 311, 145, 390, 697, 793, 311, 189, 681, 772, 615,
           189, 601, 144, 314, 641, 374, 225, 925, 866, 834, 261, 676, 469, 408, 669, 242,
           721, 904, 323, 142, 808, 192, 957, 184, 547, 571, 606, 403, 776, 154, 837, 784,
           461, 801, 884, 820, 852, 663, 678, 332, 128, 978, 545, 815, 613, 972, 163, 616}

         The target number is 453

         {187, 676, 808, 547, 784, 801, 616}

         {314, 142, 606, 801, 884, 678, 128, 616}

         {488, 834, 261, 469, 323, 571, 837, 972}

         {488, 311, 697, 793, 144, 323, 571, 972}

         {187, 145, 323, 154, 801, 820, 616}

         {145, 697, 374, 192, 184, 663}

         {145, 601, 314, 641, 403, 154, 461, 663}

         {311, 925, 142, 192, 571, 154}

         {142, 311}
```

4 A Greedy Algorithm for Subset Sum Problem

As we mentioned before, the deterministic algorithm needs $O(2^n)$ basic arithmetic operations. It has to store

$$t, t-w_1, t-w_2, t-w_1-w_2, t-w_3, t-w_1-w_3, t-w_2-w_3, t-w_1-w_2-w_3,$$

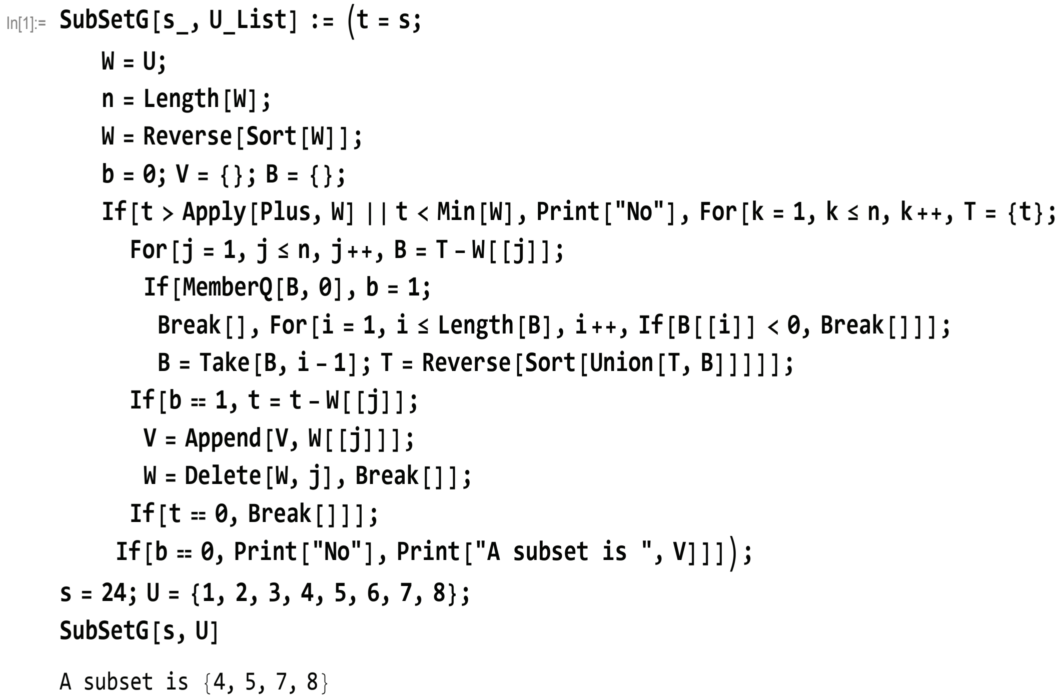
$$t-w_4, t-w_1-w_4, t-w_2-w_4, t-w_1-w_2-w_4, t-w_3-w_4, t-w_1-w_3-w_4, \cdots . \quad (4)$$

If all elements of the given set W are greater than 0, then there could be many negative integers in the above sequence. Clearly, these negative integers can be immediately deleted in each round if only one solution is wanted. Based on this observation, we present a greedy algorithm for subset sum problem.

```
Input: $t, W = \{w_1, \cdots, w_n\}, w_i > 0, i = 1, \cdots, n$, and $\ell$ (a bound for rounds).
Output: A solution of $t$ with respect to $W$ which is of minimized variance, or the failure notation "$\perp$".
1: Sort the sequence $w_1, \cdots, w_n$ decreasingly.
2: Compute the sequence $t, t - w_1, t - w_2, t - w_1 - w_2, \cdots$. Delete all negative integers and
   merge those multiple elements, and sort the new sequence decreasingly in each round.
3: Once 0 is found in the $k$-th round, return $w_k$. $t \leftarrow t - w_k$.
   If $t \neq 0$ and the round $k < \ell$, goto Step 2.
4: If $t = 0$, return the special solution which is of minimized variance. Otherwise, return "$\perp$".
```

In order to further reduce the computational cost, we suggest arrange the integers in W decreasingly, i.e., $w_1 \geq w_2 \geq \cdots \geq w_n$. In each round, those multiple elements can be merged immediately. Thus, the final solution is of *minimized cardinal and variance*. Of course, it needs least arithmetic operations. See the following Figure 3 for an illustration of the greedy algorithm.

Figure 3: The practical code for the greedy algorithm



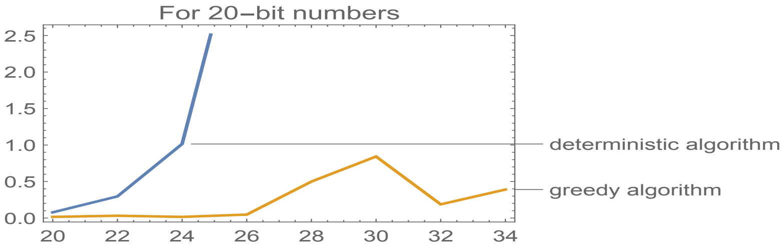
```
In[1]:= SubSetG[s_, U_List] := (t = s;
           W = U;
           n = Length[W];
           W = Reverse[Sort[W]];
           b = 0; V = {}; B = {};
           If[t > Apply[Plus, W] || t < Min[W], Print["No"], For[k = 1, k ≤ n, k++, T = {t};
             For[j = 1, j ≤ n, j++, B = T - W[[j]];
              If[MemberQ[B, 0], b = 1;
               Break[], For[i = 1, i ≤ Length[B], i++, If[B[[i]] < 0, Break[]]];
               B = Take[B, i - 1]; T = Reverse[Sort[Union[T, B]]]]];
             If[b == 1, t = t - W[[j]];
              V = Append[V, W[[j]]];
              W = Delete[W, j], Break[]];
             If[t == 0, Break[]]];
            If[b == 0, Print["No"], Print["A subset is ", V]]]);
        s = 24; U = {1, 2, 3, 4, 5, 6, 7, 8};
        SubSetG[s, U]

        A subset is {4, 5, 7, 8}
```

$t = 24, W = \{1, 2, 3, 4, 5, 6, 7, 8\}$	Sample variance s^2
$\{8, 7, 6, 2, 1\}$	9.7000
$\{8, 7, 5, 3, 1\}$	8.2000
$\{8, 6, 4, 3, 2, 1\}$	6.8000
$\{8, 6, 5, 4, 1\}$	6.7000
$\{8, 7, 4, 3, 2\}$	6.7000
$\{8, 6, 5, 3, 2\}$	5.7000
$\{7, 6, 5, 3, 2, 1\}$	5.6000
$\{8, 7, 6, 3\}$	4.6667
$\{7, 6, 5, 4, 2\}$	3.7000
$\{8, 7, 5, 4\}$	3.3333

The complexity of the greedy algorithm depends either on the position of least integer of the solution with minimized variance, or on the number of negative integers in the basic sequence. See the following Figure 4 for some experimental results.

Figure 4: Experimental results



The randomly picked integers are of 20-bit length. It shows that $n = 28$ is a practical threshold value for the deterministic algorithm on PC, which requires $O(2^{28})$ arithmetic operations. However, for a *random set* W, the threshold value for the greedy algorithm is expected to be greater than 64.

5 Conclusion

In this paper, we present several algorithms for subset sum problem which are based on a novel data arrangement. The deterministic is universal and practical which can find all solutions if the given set size is small enough. We also propose a probabilistic version and a greedy version for seeking a solution of subset sum problem. To the best of our knowledge, it is the first time to find such an efficient data arrangement which can directly generate practical and amicable code for the subset sum problem.

Acknowledgements

We thank the National Natural Science Foundation of China (61303200, 61411146001). We are grateful to the reviewers for their valuable suggestions.

References

[1] P. Austrin and *et al.*, "Dense sub-set sum may be the hardest," in *Proceedings of 33rd Symposium on Theoretical Aspects of Computer Science (STACS'2016)*, pp. 13:1–13:14, Orleans, France, Feb. 2016.

[2] R. Bellman, "Notes on the theory of dynamic programming iv - maximization over discrete sets," *Naval Research Logistics Quarterly*, vol. 3, no. 1-2, pp. 67–70, 1956.

[3] K. Bringmann, "A near-linear pseudopolynomial time algorithm for subset sum," in *Proceedings of 28th Annual ACM-SIAM Symposium on Discrete Algorithms (SODA 2017)*, pp. 1073–1084, Barcelona, Spain, Jan. 2017.

[4] G. Dantzig, "Discrete-variable extremum problems," *Operations Research*, vol. 5, no. 2, pp. 266–277, 1957.

[5] B. Faaland, "Solution of the value-independent knapsack problem by partitioning," *Operations Research*, vol. 21, no. 1, pp. 332–337, 1973.

[6] Z. Galil and O. Margalit, "An almost linear-time algorithm for the dense subset sum problem," *SIAM Journal on Computing*, vol. 20, no. 6, pp. 1157–1189, 1991.

[7] L. Gourves, J. Monnot, and L. Tlilane, "Subset sum problems with digraph constraints," *Journal of Combinatorial Optimization*, vol. 36, no. 3, pp. 937–964, 2018.

[8] Y. Hamidoune, A. Llad, and O. Serra, "On complete subsets of the cyclic group," *Journal of Combinatorial Theory, Series A*, vol. 115, no. 7, pp. 1279–1285, 2008.

[9] R. Karp., "Reducibility among combinatorial problems," in *Proceedings of Complexity of Computer Computations, The IBM Research Symposia Series*, pp. 85–103, 1972.

[10] H. Kellerer, U. Pferschy, and D. Pisinger, *Knapsack Problems.* USA: Springer, 2004.

[11] H. Kellerer and *et al.*, "An efficient fully polynomial approximation scheme for the subset sum problem," *Journal of Computer and System Sciences*, vol. 66, no. 2, pp. 349–370, 2003.

[12] K. Koiliaris and C. Xu, "A faster pseudopolynomial time algorithm for subset sum," in *Proceedings of 28th Annual ACM-SIAM Symposium on Discrete Algorithms (SODA 2017)*, pp. 1062–1072, Barcelona, Spain, Jan. 2017.

[13] R. M. Kolpakov, M. Posypkin, and S. T. T. Sin, "Complexity of solving the subset sum problem with the branch-and-bound method with domination and cardinality filtering," *Automation and Remote Control*, vol. 78, no. 3, pp. 463–474, 2017.

[14] M. S. Lee, "Sparse subset sum problem from gentry-halevi's fully homomorphic encryption," *IET Information Security*, vol. 11, no. 1, pp. 34–37, 2017.

[15] J. Nederlof, "A short note on merlin-arthur protocols for subset sum," *Information Processing Letters*, vol. 118, pp. 15–16, 2017.

[16] A. Nikolaev and A. Ushakov, "Subset sum problem in polycyclic groups," *Journal of Symbolic Computation*, vol. 84, pp. 84–94, 2018.

[17] U. Pferschy, "Dynamic programming revisited: Improving knapsack algorithms," *Computing*, vol. 63, no. 4, pp. 419–430, 1999.

[18] U. Pferschy, G. Nicosia, and A. Pacifici, "On a stackelberg subset sum game," *Electronic Notes in Discrete Mathematics*, vol. 69, pp. 133–140, 2018.

[19] D. Pisinger, "Linear time algorithms for knapsack problems with bounded weights," *Journal of Algorithms*, vol. 33, no. 1, pp. 1–14, 1999.

[20] D. Pisinger, "Dynamic programming on the word ram," *Algorithmica*, vol. 35, no. 2, pp. 128–145, 2003.

[21] Q. Tran, C. Chan, and G. Wang, "Evaluation of set-based queries with aggregation constraints," in *Proceedings of 20th ACM Conference on Information and Knowledge Management (CIKM 2011)*, pp. 1495–1504, Glasgow, United Kingdom, Oct. 2011.

[22] T. Uno, "Efficient computation of power indices for weighted majority games," in *Proceedings of 23rd International Symposium on Algorithms and Computation (ISAAC 2012)*, pp. 679–689, Taipei, Taiwan, Dec. 2012.

[23] W. Q. Wang and J. Nguyen, "The k-subset sum problem over finite fields," *Finite Fields and Their Applications*, vol. 51, pp. 204–217, 2018.

[24] R. Williams, "Strong eth breaks with merlin and arthur: short non-interactive proofs of batch evaluation," in *Proceedings of 31st Conference on Computational Complexity (CCC 2016)*, pp. 2:1–2:17, Tokyo, Japan, May 2016.

Biography

Lihua Liu is an associate professor with Department of Mathematics at Shanghai Maritime University. She received her Ph.D. degree in applied mathematics from Shanghai Jiao Tong University. Her research interests include combinatorics, cryptography and information security.

Lili Wang is currently pursuing her M.S. degree from Department of Mathematics, Shanghai Maritime university. Her research interests include combinatorics and cryptography.

Zhengjun Cao is an associate professor with Department of Mathematics at Shanghai University. He received his Ph.D. degree in applied mathematics from Academy of Mathematics and Systems Science, Chinese Academy of Sciences. He had served as a post-doctor in Computer Sciences Department, Université Libre de Bruxelles. His research interests include cryptography, discrete logarithms and quantum computation.

Xiqi Wang is currently pursuing his M.S. degree from Department of Mathematics, Shanghai university. His research interests include information security and cryptography.

A Lightweight and Efficient Data Sharing Scheme for Cloud Computing

Saeid Rezaei, Mohammad Ali Doostari, and Majid Bayat

(Corresponding author: Saeid Rezaei)

Department of Computer Engineering, Shahed University
Tehran Province, Tehran, Hasan Abad-e-Baqerof, Iran
(Email: saeid69.rezaei@gmail.com)

(Received Aug. 20, 2018; revised and accepted Nov. 3, 2018)

Abstract

Cloud storage is a useful service of cloud computing which allows users to upload their data in the cloud and share it with others. Although, this new service is affordable and practical, but it is associated with several privacy and security challenges. Nowadays, Attribute Based Encryption (ABE) is widely used to provide secure data sharing in the distributed environment such as cloud computing. Unfortunately, most of the existing ABE schemes are not suitable for resource-constraint cloud systems, because they use expensive bilinear pairing operation and thus they cause a very high encryption and decryption computation overhead. In this paper, we propose an efficient no-pairing and revocable ABE data sharing scheme based on Elliptic Curve Cryptography (ECC) for cloud storage systems. Moreover, a comprehensive security and performance analysis shows that our scheme is both secure and efficient.

Keywords: Attribute-based Encryption; Cloud Computing; Data Sharing; Elliptic Curve Cryptography; Security

1 Introduction

In recent years, cloud computing has received increasing attention in both academia and industry. This technology provides on demand and unlimited computing services and resources for users through the Internet or a private network. People can easily upload their data into the cloud storages and users can access the shared data where and when they need them [13]. Although, this new technology brings many advantages for users and organizations, but since sensitive data is stored beyond the organizational boundaries and thus users lose physical control over their data, it faces major security and privacy threats which are the most important concerns in cloud computing.

Due to the aforementioned threats, most organizations and users afraid to take advantage of cloud storage systems and it is believed that security and privacy risks are the main obstacles in moving towards cloud services. To deal with the security threats and preserve data confidentiality, so far, many security solutions have suggested by researchers [22,29]. Among the proposed methods, data encryption is one of the most practical tools for improving the security of the stored data [8,17,18].

Although, traditional encryption primitives provide secure access control to remotely stored data, but they suffer several shortcomings such as complicated Key management process by increasing the number of users in the system, failure to support fine-grained access control and low scalability. In addition, Data owners must always stay online to distribute keys among new users. Moreover, since traditional encryption models need to store a copy of each ciphertext for each single user with a different key, they require plenty of storage resources. To implement a secure, efficient and fine grained data sharing model, the following challenges need to be taken into consideration: firstly, data owners must provide access to data based on user's need; secondly, the scheme must allow the data owners to revoke existing users or add new users; thirdly, data confidentiality must be guaranteed against cloud server, attribute authority and unauthorized users and the users must be able to check the integrity of received data; finally, users must be able to access the shared data via their limited computing devices such as tablets and smartphones [4].

Recently, in order to overcome the said problems, Attribute-based encryption (ABE) technique has introduced [15]. ABE is a public key based one-to-many encryption technique that provides a flexible and fine-grained data access control in distributed systems such as cloud computing, smart grid, IoT and etc. Unfortunately, most of the existing data sharing schemes are not suitable for resource-constraint cloud systems, because they used expensive bilinear pairing operations and thus they involved a very high encryption and decryption computation overhead cost.

In this paper, with respect to the fact that ECC algorithm has stronger bit security than exponential-based public key cryptographic algorithms like RSA and can achieve the same level of security with smaller key sizes and higher computational efficiency, we propose a lightweight and efficient data sharing scheme for cloud storage systems. To preserve data confidentiality against unauthorized users, we use a key policy attribute based encryption (KP-ABE) and combine it with an elliptic curve encryption technique. In our scheme, expensive bilinear pairing operation in KP-ABE replaces with point scalar multiplication on ECC and makes a lightweight data sharing scheme which is quite suitable for using in computationally limited devices such as smart phones. Our proposed scheme also presents two important security requirements, user revocability and DoS attack resiliency. Finally, we compare the lightweight feature of our scheme with the existing ABE schemes and show that it is more efficient and practical than others.

1.1 Related Works

ABE can be seen as a generalization of Identity-based encryption [3] which was first proposed by Sahai and Waters. In an ABE scheme, data owner encrypts the message under a set of descriptive attributes and selects a threshold value as d. A user can decrypt the ciphertext if and only if there exist d of the given attributes in his/her key. In recent years, ABE has been widely used as a popular technique to provide user privacy and data security in distributed environment such as cloud computing. Based on the access control policy, ABE can be divided into two classes called key-policy ABE (KP-ABE) [6] and ciphertext policy ABE (CP-ABE) [2]. In a KP-ABE system, the access policy is set to user's private keys and the message is encrypted with a set of descriptive attributes. In this model, the access tree placed in the private key specifies which ciphertexts the user will be allowed to decrypt. Conversely, in CP-ABE, each user's secret key is associated with a set of attributes and sender determines an access structure on which user is allowed to decrypt the encrypted message.

Until now, several KP-ABE [14,16] and CP-ABE [19,20] schemes have been proposed by researchers, but most of them have major efficiency drawbacks and suffer from high computation overhead in encryption and decryption phases. These schemes are not suitable for mobile cloud computing scenario where users have resource constrained devices with limited computing power. Nowadays, ABE with low computation and communication costs has emerged as a hot topic.

In [27] Zhang et al. improved their previous work [26] and proposed a CP-ABE with constant computation cost and ciphertext size which supports AND-gate access policies with multiple attribute values and wildcards. Bayat and et al. [1] presented an efficient and revocable CP-ABE data sharing structure which decreases the computation overhead expenses by supporting partial decryption. Their scheme also preserved user privacy by hiding access policy and is immune against DoS attack. Zhang et al. [25] presented a novel scheme called match-then-decrypt. In this scheme an additional matching phase is introduced before the decryption phase. Their technique works by computing special components in ciphertexts, which are used to perform the test that whether the attribute private key matches the hidden access policy in ciphertexts without decryption. A privacy aware smart health access control system (PASH) is proposed in [28], where a large universe CP-ABE scheme with partially hidden access policies is introduced to deal with both data security and user privacy issues.There are also many works proposed to make further improvements on ABE, such as [9, 10, 24]

Unfortunately, all of the above schemes are based on the expensive bilinear pairing operation and because of their high computational costs are not suitable for cloud computing systems.

Recently, Yao and et al. [23] introduced a no-pairing ECC-based KP-ABE data sharing scheme which bilinear pairing operation has been replaced with point scalar multiplication on elliptic curve. This replacement makes their scheme efficient and it is suitable for using in resource constrained devices. However, their scheme does not support user revocation and it is also responsible for user to perform data decryption completely which can take a significant amount of time and resources.

1.2 Organization

The remaining of this paper is organized as follows. Section 2 introduces our system model, definitions, security requirements and the cryptographic preliminaries. Section 3 provides the details of our proposed scheme. In Section 4 and 5, we analyze the security requirements and performance evaluation of our scheme, respectively and finally, Section 6 contains the concluding remarks of the paper.

2 Preliminaries

In this section, we first define the architecture of the proposed data sharing model along with its framework and security requirements and then we will describe the briefly review of some cryptographic primitives. The notations used in our scheme are shown in Table 1.

2.1 System Model

Our system model is composed of four entities: an attribute authority, a cloud service provider, data owners (senders) and data consumers (users). They are shown in Figure 1.

Authorized Authority (AA). The AA is a semi trusted (honest but curious) key entity that is responsible for generating global public parameters and master secret keys. It takes charge of computing corresponding private keys for users and publishes the keys among them. It also is responsible for revoking the users. The AA is assumed to be honest but curious, that is, it will not deny services to any authorized users and it will correctly follow the proposed protocol, but it is curious about the data content and it would like to obtain as much private information as possible.

Cloud Service Provider (CSP). The CSP is a powerful computing entity with unlimited resources and is responsible for collecting and storing data from the owners. It also helps users decrypt the ciphertext by computing a large amount of decryption overhead. Like AA, the CSP is assumed to be honest but curious.

Data owner. The data owner is an entity who wishes to outsource data file to the CSP. Before transmission of data, it first encrypts the data under a set of attributes.

User. It is an entity who can freely query ciphertext from the cloud server. For this purpose, it first generates a token based on its key and requests access to the data by sending that token to the CSP.

Table 1: Notations of proposed scheme

Notations	Description
p	A large prime number.
F_p	A finite field with p elements.
E	An elliptic curve over a finite field F_p.
G	A generator point on the elliptic curve E.
O	The point at infinity.
Z_p	A finite integer set with $\{0, 1, ..., p-1\}$ as its elements.
Z_p^*	Z_p - $\{0\}$.
PS	One point scalar multiplication.
AA	Attribute Authority.
CSP	Cloud Service Provider.
MK	The system master private key.
PK	The system master public key.
GP	The public key parameters of the ABE scheme.
M	The shared data.
MAC	The message authentication code.
U	The number of the possible attributes.
ω	The number of the attributes used to encrypt data.

2.2 Definitions of Our Lightweight KP-ABE

In the following, we present an overview of the algorithms used in the attribute based data sharing system.

Setup$(\lambda\ , U) \rightarrow (MK, GP)$

The setup algorithm takes as input a security parameter λ and an attribute universe U and it outputs global public parameters GP and a master key MK for the system.

Encryption$(GP,\ M,\ \omega) \rightarrow CT$

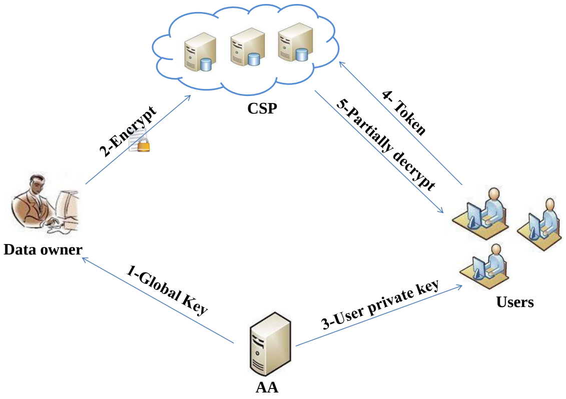


Figure 1: System model of our attribute-based data sharing

The encryption algorithm takes a message M, a set of descriptive attributes ω and the global parameters GP. It outputs a ciphertext CT.

KeyGen$(GP, MK, \Gamma) \rightarrow SK$

The key generation algorithm takes as input the global parameters GP, the master secret key MK and an access tree Γ. It generates a private key SK for each authorized user.

TokenGen$(GP, D) \rightarrow TK$

The user runs this algorithm in order to generate a decryption token TK.

Partial Decryption$(GP, TK, CT) \rightarrow CT_{Partial}$

The partial decryption algorithm takes as input the global parameters GP, the users token and the ciphertext. It outputs a partially decrypted ciphertext.

Decryption$(CT_{Partial}) \rightarrow (M, MAC_M)$

The decryption algorithm runs by user and it takes the partially decrypted ciphertext. It outputs the message M and the message authentication code MAC_M.

2.3 Security Requirements

- **Data cofidentiality** This means that only authorized users is allowed to access the data and unauthorized users, the AA and the CSP are unable to decrypt the message.

- **Data Integrity** This property guarantees the validity and accuracy of data over its entire life cycle. By using it, the user can easily detect any modifications, addition or deletion of data.

- **Denial of service (DoS) attack** Denial of service is a kind of attack which the attackers try to deny services to legitimate users. Such an attack can simply waste cloud's resources and limit the authorized users to utilize the facilities of the data sharing system.

- **Collusion resistance** Collusion resistance means a deterring process of combining keys by two or more unauthorized users in order not to allow them to decrypt a ciphertext that none of them can decrypt it individually. In this article, the CSP and the AA is assumed to be honest and do not engage in any active attack for colluding.

- **Revocation of users** User revocation is a vital issue in data sharing systems. It refers to the act of terminating a previously granted user. The revoked users should not be able to decrypt the ciphertext even if they have the corresponding keys.

2.4 Access Structure

Definition 1. (Access Structure [11]).

We denote $\mathbb{P} = \{P_1, P_2, ..., P_r\}$ be a set of attributes. A collection $\mathbb{A} \subseteq 2^{\{P_1, P_2, ..., P_r\}}$ is monotone if $\forall A_1, A_2$: if $A_1 \in \mathbb{A}$ and $A_1 \subseteq A_2$, then $A_2 \in \mathbb{A}$. An (monotone) access structure is a (monotone) collection $\mathbb{A}$ of non-empty subsets of $\mathbb{P} = \{P_1, P_2, ..., P_r\}$. That is, $\mathbb{A} \subseteq 2^{\{P_1, P_2, ..., P_r\}} / \{\emptyset\}$. The sets in $\mathbb{A}$ are called the authorized sets, and the sets not in $\mathbb{A}$ are called the unauthorized sets.

Definition 2. (Access Tree [6]).

Let T_R be the access tree with a root node R. In the access tree T_R, each non-leaf node is a threshold gate which is defined by its children and a threshold value. Let num_x is the number of children of a node x and k_x is its threshold value, then $0 < k_x \leq num_x$. The threshold gate is an OR gate if $K_x = 1$ and it is an AND gate if $K_x = n$. each leaf node x is corresponding to an attribute value and a threshold value $K_x = 1$.

We also define the parent of node x by $parent(x)$ and the function $index(x)$ returns the number associated with node x that is given by x's parent node. The children of every node x are numbered from

1 to num_x. The function $att(x)$ is defined only if x is a leaf node and denotes the attribute associated with the leaf node x in the tree. If an attributes set γ satisfies the access tree T_R, then $T_R(\gamma) = 1$. $T_R(\gamma)$ is computed recursively. If x is a non-leaf node, evaluate $T_x(\gamma)$ for all children x' of node x. $T_x(\gamma)$ returns 1 if and only if at least k_x children return 1. If x is a leaf node, then $T_x(\gamma)$ returns 1 if and only if $att(x) \in \gamma$.

2.5 Elliptic Curve Cryptography

Elliptic Curve Cryptography (ECC) is a public key cryptography that was originally introduced by Victor Miller and Neal Koblitz in 1985. Let p be a prime number and let $\mathbb{F}_p$ denotes the field of integers modulo p. An elliptic curve E over the finite field (or Galois Field) GF is defined by a cubic equation $y^2 = x^3 + a \cdot x + b$ where $a, b \in \mathbb{F}_p$ satisfy $4a^3 + 27b^2 \neq (mod\ p)$. Each different value of a and b form a different elliptic curve. The set of all points (x, y) which satisfies the above equation along with a point in infinity which denoted by ∞ lies on the elliptic curve. In the ECC, a random number is chosen as private key and the public key is a point in the curve which is constructed by multiplying the private key with the generator point G in the curve. The set of parameters to be used in ECC is presented in Table 1 .

In [5] you can see a detailed description of the ECC.

3 Our Construction

In this section, based on the preliminaries and system model, we introduce our lightweight KP-ABE scheme in detail. In the general view of the proposed data sharing scheme, the owner U_A generates a set of descriptive attributes and then he/she encrypts a message M by a symmetric cryptographic algorithm and sends the ciphertext to the cloud service provider. Here, we do not use any of the ABE expensive operations such as modular exponent or bilinear pairing. Instead, we use lightweight ECC operations along with a symmetric encryption algorithm. When a user U_B receives an associated key from the authority and wants to decrypt the stored data in the cloud servers, first the user U_B must generate a decryption token and send it to the CSP. While receiving the token, the CSP partially decrypts the stored ciphertext and sends the obtained message to the U_B. The user then can easily decrypt the ciphertext. The proposed data sharing scheme consist of six function module: *Setup*, *Encryption*, *KeyGen*, *TokenGen*, *Partial Decryption* and *Decryption*. They are described as follows:

- **Setup**(λ , U)$\rightarrow$($MK.GP$)

  The setup algorithm runs by the trusted attribute authority which takes as input a security parameter λ and the attribute universe U. It outputs global public parameters GP and the master key MK. For this purpose, the authority first selects a random number α from Z_P^* and it computes $PK = \alpha \cdot G$. Let $U = \{1, ..., n\}$ be a set of all attributes in the system, for each attribute $i \in U$, the authority chooses a random number $s_i \in Z_P^*$ and computes the public key of each attribute i as $P_i = s_i \cdot G$. The CSP selects a random value β as its secret key and computes $PK_{CSP} = \beta \cdot G$ as its public key. The authority does not know β and the CSP proofs the knowledge of β to the authority by using a zero knowledge proof protocol [12].The authority sets $MK = \{\alpha, \{s_1, ..., s_i\}_{i \in U}\}$ as its secret key and publishes the global parameters $GP = \{PK, PK_{CSP}, \{P_1, ..., P_i\}_{i \in U}\}$.

- **Encryption**(GP, M, ω)$\rightarrow$$CT$

  The encryption algorithm takes as input a message M, a set of descriptive attributes ω and the global parameters GP. When the owner U_A wants to encrypt a message under the set of attributes

ω, he/she chooses a value d randomly from Z_P^* and computes K and F as follows:

$$\begin{aligned} K &= d \cdot PK = (k_1, k_2) \\ F &= d \cdot PK_{CSP} = (f_1, f_2) \end{aligned} \tag{1}$$

If $K = O$, the authority re-chooses d randomly from Z_p^* to computes K until $K \neq O$. we consider the point (k_1, k_2) as encryption key and integrity key respectively, and compute ciphertext C and MAC_M for message M as follows:

$$\begin{aligned} C &= ENC(M, k_1) \\ C' &= ENC(C, f_1) \end{aligned} \tag{2}$$

$$MAC_M = HMAC(M, k_2) \tag{3}$$

in Equation (2), $ENC()$ is a symmetric encryption algorithm such as AES. The message M is encrypted under the key k_1 and then it re-encrypted with the key f_1 again, this causes the ciphertext C to be hidden of the authority sight. In Equation (3), $HMAC()$ is a cryptographic hash function which it generates the hash based message authentication code for message M according to the integrity key k_2. Finally, the owner U_A computes $C_i = d \cdot P_i$ for all of the attributes in ω and uploads $CT = (\omega, C', MAC_M, \{C_i\}_{i \in \omega}, H = d \cdot G)$ to the cloud service provider.

- **KeyGen**$(GP, MK, \Gamma) \rightarrow SK$

  Upon the request of a user U_B, the keyGen algorithm computes the decryption key for U_B in following manner. It chooses a polynomial q_x for each node x in the access tree Γ. These polynomials are chosen in a top to bottom manner, starting from the root node R. For each node x in the tree Γ, the authority sets the degree d_x of the polynomial q_x to be one less than the threshold k_x of that node, that is, $d_x = k_x - 1$. For the root node R, it sets $q_R(0) = \alpha$ (note that α is the secret value of authority) and then it sets rest of the points randomly to completely fix q_R. For any other node x, it sets $q_x(0) = q_{parent(x)}(index(x))$ and chooses d_x other points randomly such as $q_R(x)$. $Index(x)$ is the unique index number of x given by its parent.

  Let Y be the set of leaf nodes in the tree Γ and $att(y)$ denotes the attribute associated with the leaf node $y \in Y$. Once the polynomials have been completed, for all leaf nodes y, the KeyGen algorithm outputs the following values:

$$D_y = q_y(0)/s_i, i = att(y) \tag{4}$$

  Finally, the authority sends $D = (D_x, i = att(x)$ and $i \in \omega)$ as the private key for U_B.

- **TokenGen**$(GP, D) \rightarrow TK$

  At this phase, a user U_B generates a token TK_B based on his/her private key and sends it to the CSP to convey most of the decoding computational load to the CSP. For this purpose, U_B first selects a random number b from Z_P^* and computes $D' = \{D_x \cdot b = (q_x(0) \cdot b)/s_i\}_{i \in \omega}$. After that, the user U_B computes the point $Q = b \cdot PK_{CSP} = b \cdot \beta \cdot G = (q_1, q_2)$ and $B = b \cdot G$ and sets the token TK_B as follows:

$$TK_B = \{B, T_B = ENC_{q_1}(D', i = att(x), i \in \omega, T)\} \tag{5}$$

  Here, we use a timestamp T to defend against DOS attack. Upon receiving the token, the CSP decrypts T_B and checks the time stamp T. If it is valid, the CSP continues the partial decryption phase. $ENC(.)$ is a symmetric encryption function such as AES.

- **Partial Decryption**$(GP, TK_B, CT) \rightarrow CT_{Partial}$

  While receiving the token TK_B, the CSP computes the decryption key q_1 by using its secret key β as $Q = \beta \cdot B = \beta \cdot b \cdot G = (q_1, q_2)$ and decrypts T_B. If validation of the timestamp T is failed, the CSP rejects the partial decryption request. Otherwise, the CSP executes the partial decryption algorithm as follows. Let x be a node of tree Γ, we first define a recursive algorithm $DecryptNode(CT, D', x)$. Let $i = att(x)$, if x is a leaf node, then $DecryptNode(CT, D', x)$ is computed as follows:

  $$\begin{aligned} D'_x \cdot C_i = D_x \cdot b \cdot C_i &= q_x(0) \cdot s_i^{-1} \cdot b \cdot d \cdot s_i \cdot G \\ &= q_x(0) \cdot b \cdot d \cdot G. \end{aligned} \tag{6}$$

  This recursive algorithm outputs an element in elliptic curve group or $\perp$.

  If x be a non-leaf node, the algorithm $DecryptNode(CT, D', x)$ calls for all nodes z which are children of x, and the output is stored as F_z. Let L_x be an arbitrary k_x-sized set of child nodes z such that $F_z \neq \perp$. If there is not such a L_x, then the node was not satisfied and the function returns $\perp$ for $DecryptNode(CT, D', x)$. Otherwise, assume that $i = index(z)$ and $L'_x = \{index(z) : z \in L_x\}$, $DecryptNode(CT, D', x)$ can be calculated as follows:

  $$\begin{aligned} \sum_{z \in L_x} \Delta_{i,L'_x}(0) \cdot DecryptNode(CT, D', z) &= \sum_{z \in L_x} \Delta_{i,L'_x}(0) \cdot q_z(0) \cdot b \cdot d \cdot G \\ &= \sum_{z \in L_x} \Delta_{i,L'_x}(0) \cdot q_{parent(z)}(index(z)) \cdot b \cdot d \cdot G \\ &= \sum_{z \in L_x} \Delta_{i,L'_x}(0) \cdot q_x(i) \cdot b \cdot d \cdot G \\ &= q_x(0) \cdot b \cdot d \cdot G. \end{aligned} \tag{7}$$

  Based on the above, for the root node R of the access tree Γ, the output of $DecryptNode(CT, D', R) = q_R(0) \cdot b \cdot d \cdot G = \alpha \cdot b \cdot d \cdot G$. After computing the $DecryptNode(CT, TK_B, R)$, the CSP computes $F = \beta \cdot H = \beta \cdot d \cdot G = (f_1, f_2)$ and $C = DEC(C', f_1)$. Finally, the CSP sends $CT_{Partial} = \{\omega, C, MAC_M, N = DecryptNode(CT, D', R)\}$ to the user U_B. As shown in Equation (7), the cloud service provider cannot decrypt the ciphertext because does not know the value of b and it only helps the receiving users to easily decrypt the ciphertext.

- **Decryption**$(CT_{Partial}) \rightarrow (M, MAC_M)$

  Upon receiving the
  $CT_{Partial}$, the user U_B can easily compute the decryption and integrity keys. Since $N = \alpha \cdot b \cdot d \cdot G$, the Decryption algorithm simply divides out b and recovers the keys as Equation (8).

  $$\begin{aligned} C'_1 = N/b &= \alpha \cdot b \cdot d \cdot G \cdot b^{-1} \\ &= \alpha \cdot d \cdot G = (k'_1, k'_2) \end{aligned} \tag{8}$$

  The point (k'_1, k'_2) is decryption key and integrity key for message M respectively. Then the user can decrypt the message M as $M' = DEC(C, k'_1)$. the message M is correct if $HMAC(M', k'_2) = MAC_M$.

In order to revoke a user U_B, the authority securely sends all of the attributes of revoked user U_B to the CSP. When receiving the token, the CSP first checks whether all of the attributes of U_B exist in the token or not, if yes it rejects the token.

4 Security Analysis

In this section, we evaluate the security features of the proposed scheme. The security analysis focuses on the security requirements defined in section 2. The correctness of our scheme is based on the two following theorems:

Theorem 1. *A user can correctly decrypt M if and only if he holds an appropriate access structure in his/her key.*

Proof. In our scheme, each user's key is associated with an access tree where the leaf nodes are associated with attributes. A user can decrypt a ciphertext if and only if the access tree in his key is satisfied by the attributes associated with a ciphertext. □

Theorem 2. *Except for the authority, it is hard for any other parties to generate a valid secret key D.*

Proof. According to the Equation (4), in order to generate a valid secret key D, one needs the secret values S_i and α and without these values, no party can compute the valid secret key. Since these secret values are kept only by the trusted authority, other parties cannot compute the valid secret keys. Moreover, by using the property of Discrete Logarithm Problem *(DLP)*, it is almost impossible for the party to calculate the values S_i and α from the public parameters PK_{CSP} and PK respectively. Thus, the party cannot compute a valid secret key. □

In addition, our scheme achieves the following security goals.

- **Data confidentiality**

  In the proposed scheme, the data is encrypted by the data owner before uploading to the CSP. Therefore, only the users with appropriate private keys can correctly decrypt the message M and unauthorized users cannot obtain any information about the encrypted data. As defined in the TokenGen phase, the user blinds his private keys with a secret value b before generating a decryption token. Hence, when a user requests the CSP to partially decrypt the ciphertext by sending the token, the storage server cannot decrypt the ciphertext because it does not have the secret value b and thus unable to calculate the proper decryption key Equations ((6 and 7)). Another attack on the stored data can be occurred by the authority. Since it is a semi trusted entity, data confidentiality against it can be consider as another vital security criteria for secure data sharing. When the sender delivers the ciphertext to the CSP, the authority cannot decrypt it. This is because in accordance with the Encryption phase, the owner re-encrypts the ciphertext with the key f_1 and since f_1 is only computable by the sender and the CSP, the authority cannot decrypt the ciphertext C. Therefore, data confidentiality of the proposed scheme is immune against the curious authority, the CSP and unauthorized users. In addition, key escrow problem against the CSP and the authority is conquered.

- **Collusion resistance**

  This property is one of the most important security features in ABE. It means that, two or more unauthorized users cannot cooperatively act as a valid user and generate the corresponding key and decipher the encrypted data, even if they collude and combine their keys. In the keyGen phase, each user's attribute key is tied with a random polynomial so that users cannot combine their attribute keys to recover the message M. If different users combine their keys, the Equations (6 and 7) do not result in the correct value $\alpha \cdot b \cdot d \cdot G$. Therefore, our scheme achieves fully collusion secure.

- **Data integrity**

  According to the Encryption phase, the owner computes the message authentication code of the message M by using a hash function and sends it along with the other components to the CSP. After decrypting the message, the user computes the MAC again and compares it with the received one. If they both are equal, the message has not been modified. Thus, the assurance of the accuracy and consistency and correctness of data is guaranteed.

- **Denial of service attack** To achieve this, in TokenGen phase we have added a time stamp T to the token TK_B and encrypt it along with other data. When an active eavesdropper listens to the channel and steals the token, he cannot send it to the CSP repeatedly, because after decrypting the token by CSP, it first checks the time stamp and if it is valid, the CSP continues the partial decryption phase. Otherwise, the request is rejected. Thus, our scheme is immune against the DoS attack.

Table 2: The comparison of the security goals

Schemes	Key escrow	Data confidentiality	Data integrity	Collusion resistant	DoS attack resistant	Revocation of users
Yao's scheme [23]	Yes	Yes	Yes	Yes	No	No
proposed scheme	No	Yes	Yes	Yes	Yes	Yes

Table 3: Key length comparison of RSA and ECC [5]

Security level (bit)	RSA key length (bit)	ECC key length (bit)
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	512

- **Revocation of users**

  If the user quits the system, the scheme can revoke his access right from the system. That is, the authority securely sends all of the attributes of a revoked user U_B to the CSP. When receiving the token, the CSP first checks whether all of the attributes of U_B exist in the token or not, if yes it rejects the token. After the revocation process, the revoked user cannot access to the stored data even if the user has valid secret key. Our revocation process is efficient because there is no need to update any parameters such as non-revoked secret key update or data re-encryption.

We compare the security of our scheme with the Yao's data sharing scheme. The results are shown in Table 2. As shown, both schemes can achieve the data confidentiality and data integrity and are resistance to collusion attack. But the proposed scheme, as opposed to the Yao's scheme, is free from the key escrow property and it is immune against DoS attack. Moreover, it supports the user revocation procedure.

Table 4: Symbols and their meanings

Symbols	Meanings
L_T	The bit length of the timestamp.
L_{HMAC}	The bit length of the value derived from a hash function.
L_{SymKey}	The key length of a symmetric cryptography algorithm.
L_{Data}	The size of the data to be encrypted.
L_{PriECC} & L_{PubECC}	The private and public key sizes of the 160-bit ECC.
L_{PriRSA} & L_{PubRSA}	The private and public key sizes of the 1024-bit RSA.
L_{Point}	The size of a point on the elliptic curve.
L_{G_1} & L_{G_2}	The bit length of an element in G_1 and G_2 respectively.
k, l	The size of the attribute set associated with the ciphertext and the private key of a user, respectively.
t	The number of attributes associated with the token.
u	The size of the attributes space.

Table 5: The efficiency comparison

	Communication size (bit)			
Schemes	CT	PK	SK	T
Yao [23]	$(2k+2)d$	$(2u+2)d$	$l \cdot d$	–
Hohenberger [7]	$(k+3)6.4d$	$(u+2)6.4d$	$19.2l.d$	–
Bethencourt [2]	$(2k+3)6.4d$	$25.6d$	$(2l+1)6.4d$	–
Waters [21]	$(2k+3)6.4d$	$(u+3)6.4d$	$(l+2)6.4d$	–
Bayat [1]	$(2k+3)6.4d$	$19.2d$	$(3l+1)6.4d$	$(3t+1)6.4d$
Zhou [30]	$19.2d$	$(6u+1)6.4d$	$(2l+1)6.4d$	–
Goyal [6]	$(k+2)6.4d$	$(u+2)6.4d$	$6.4l \cdot d$	–
Our scheme	$(2k+4)d$	$(2u+4)d$	$l \cdot d$	$(t+2.18)d$

D^* is the division operation that is performed by end user in order to compute symmetric key and integrity key.

Table 6: The efficiency comparison (cont.)

	Comput. cost (ps)			Access
Schemes	Enc.	Dec.	Policy	structure
Yao [23]	$1+k$	$2k-1$	KP	Tree
Hohenberger [7]	$2k+22$	$4k+40$	KP	$LSSS$
Bethencourt [2]	$4k+22$	$40k+20$	CP	$Tree$
Waters [21]	$6k+26$	$60k+36$	CP	$LSSS$
Bayat [1]	$4k+44$	20	CP	$Tree$
Zhou [30]	26	$60k+20$	CP	$And^*_{+,-}$
Goyal [6]	$2k$	$40k$	KP	$Tree$
Our scheme	$2+k$	D^*	KP	$Tree$

D^* is the division operation that is performed by end user in order to compute symmetric key and integrity key.

5 Performance Evaluation and Implement

In this section, in order to present the efficiency of our proposed scheme, we evaluate the performance of our scheme in two areas of communication cost and computation overhead and compared it with the some of the previous KP-ABE and CP-ABE schemes. Then, we implemented the communication overhead of our work and two other basic schemes [2, 6] under the same condition for the comparison purposes.

5.1 Performance Analysis

For the sake of evaluation, we use the same metrics as [23]. Based on the used operations, ABE can be divided into two categories, RSA based scheme and ECC based scheme. Versus to our scheme that is based on ECC, most of the existing ABE schemes are based on bilinear pairing, which use two cyclic groups G_1 and G_2 of prime order P and a bilinear mapping $e : G_1 \times G_1 \rightarrow G_2$. Due to using of modular exponential operation, these schemes can be called RSA based. Since bilinear mapping and modular exponentiation are expensive operations, most of the existing RSA based ABE schemes suffer from high encryption and decryption overhead. As mentioned in Section 1, ECC is a secure, efficient and scalable public key encryption system which has stronger bit security than RSA. It means that, ECC can achieve the same level of security with smaller key sizes and higher computational efficiency. Table 3 shows a comparison between RSA and ECC key lengths [5]. The security level means the cryptographic strength provided by a symmetric encryption algorithm, using an n bits key. As we can see, on the same security level the key size of ECC is much less than that of RSA.

In order to simplify the comparison process, we assume that all ABE schemes to be compared with are under the same encryption attribute set and at the same security level that is equal to 160 bit ECC. We denote this security level by d. The symbols employed in the comparison are described in Table 4. Based on the above assumption and according to the Table 4, let $|L_T| = 0.18d, |L_{HMAC}| = |L_{SymKey}| = |L_{Data}| = |L_{PriECC}| = d, |L_{Point}| = |L_{PubECC}| = 2d, |L_{PriRSA}| = |L_{PubRSA}| = |L_{G_1}| = 6.4d$ and $|L_{G_2}| = 12.8d$.

The communication overhead depends on the length of the message to be transmitted which is consist of the ciphertext, public key and private key. Thus, we consider the lengths of these three parameters as the communication overhead metrics to measure and compare the communication overhead. In addition, we analyze the computation overhead of the proposed scheme based on the encryption and decryption algorithms. In the proposed scheme, the predominant computation operation involved in encryption and decryption algorithms is point scalar multiplication and the cost of other operations such as HMAC, arithmetic and logic operations can be ignored. In an RSA ABE scheme, the most expensive operations are bilinear mapping and modular exponentiation respectively, and we ignore the cost of all other operations. In order to ease the calculation of computation overhead, the point scalar multiplication can be taken as the unit of computation overhead in ABE schemes. Since the cost of bilinear mapping and modular exponentiation is much more than the point scalar multiplication, let the cost of one bilinear mapping is equal to 20 point scalar multiplication, and one modular exponential operation is 2 point scalar multiplication [23].

Tables 5 and 6 show a performance comparison in terms of the ciphertext size, the size of system public key, private key size, computation overheads of encryption and decryption, kind of policy and the expressiveness of access policy. In this Table, CT, PK, SK, T and LSSS are abbreviation for ciphertext size, public key size, private key size, token size and linear secret sharing schemes, respectively. In comparison to Yao's scheme, the proposed scheme does not increase the private key size and it only increases $2d$ bits (320 bits) to the ciphertext size and public key size and $(k + 2.18)d$ bits to the token which are acceptable for the security enhancements. From Tables 5 and 6, we can see that the computation complexity of encryption algorithm in our scheme is almost equal to Yao's scheme, but we convey most of the decryption computational load without disclosure of data to the CSP and the end user can decrypt the ciphertext easily and only by performing a division operation that we denote it by D^* in Tables 5 and 6. It is important to note that our scheme does not reveal any useful information to the CSP during partial decryption and thus the CSP is unable to recover the valid private key and access to the plaintext. The performance comparison with other KP-ABE and CP-ABE schemes are shown in Tables 5 and 6. From the Table, we can see that in most cases our scheme is more efficient in both communication and computation costs, as well as it achieves higher performance in privacy and security without increasing computational complexity and is quite suitable for using in computationally limited devices such as smart phones.

5.2 Implementation

We conduct simulation experiments for communication overhead of our scheme in terms of ciphertext size, public key size and private key size and compared them with Goyal et al.'s KP-ABE [6] scheme and Bethencourt et al.'s CP-ABE scheme [2] as the basic current ABE schemes. The comprehensive experiments are conducted by MATLAB on a Windows 7 machine with dual core 2.40-GHz CPU and 4-GB RAM. Figure 2 shows the comparison of ciphertext size versus the number of attributes used to create it. As can be seen, the ciphertext size on the three schemes increases linearly with the number of attributes, but by increasing number of attributes, our proposed scheme is more efficient than those two others. This efficiency is achieved by using ECC operations instead of expensive modular exponentiation and bilinear mapping operations. Figure 3 gives the public key size of our scheme, [6] and [2] versus the all number attributes used in the system. As Figure 3 shows, the public key size in our scheme is always shorter than that [6] and when the number of attributes is more than 11, the public key size in our scheme is longer than [2]. That is because the ciphertext size in [2] is independent of the number of attributes and it is always a constant value $25.6d$. Figure 4 presents the comparison of private key length versus the number of attributes used in access structure. As it is evident from Figure 4, the private key size increases linearly with the number of attributes, but with the increase of attributes, our proposed scheme act more efficient than other schemes. In total, we can say that our scheme outperform other ABE schemes in lightweight.

In addition, we simulate the communication overhead of our scheme in term of owner-to-CSP communication and user-to-CSP communication. Let n is the number of all users in the system ($n \leq 1000$) and the number of all attributes is 100 ($u = 100$). We plot the communication overhead in terms of the number of users n and the number of attributes k. We assume that each user has maximum half of the possible attributes ($k \leq 50$). Figure 5 shows the owner-to-CSP communication, where the owners encrypt the data and upload the encrypted data to the storage servers. As stated in Tables 5 and 6, the size of ciphertext is $(2k + 4)d$ bits, therefor, in the worst condition when all owners encrypt and upload their data Simultaneously, the communication overhead between the owners and the CSP for all owners is $((2k+4)d) \times n$ bits. Next, we consider the user-to-CSP communication overhead of proposed scheme as shown in Figure 6. According to the token size in Tables 5 and 6, the bit length of a token is $(k+2.18)d$ bits for one user. Therefore, the overall communication overhead between the users and the CSP is $((k + 2.18)d) \times n$ bits. Note that, these communication overheads are negligible by considering current communication technologies for cloud computing.

6 Conclusion

This paper introduced a revocable and lightweight data sharing system by using KP-ABE and ECC based operation. We convey most of the decryption computational load without disclosing any data to the cloud service provider. In addition, we presented detailed security analysis which shows that

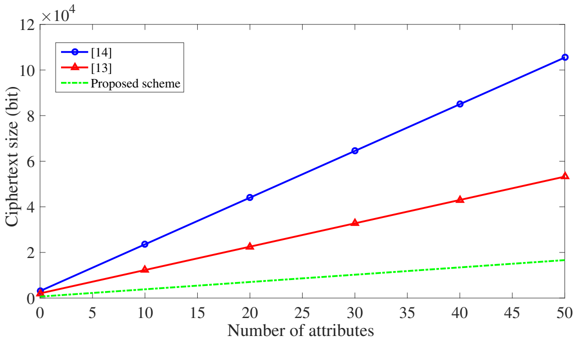


Figure 2: Comparison of ciphertext size

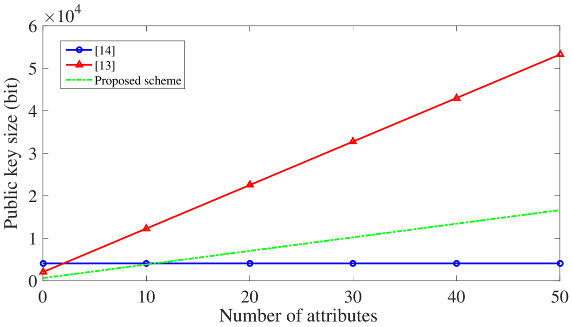


Figure 3: Comparison of public key size

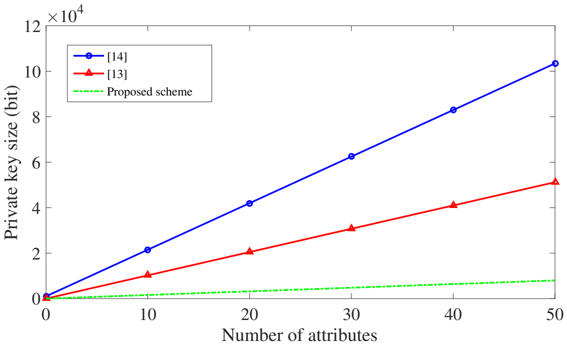


Figure 4: Comparison of private key size

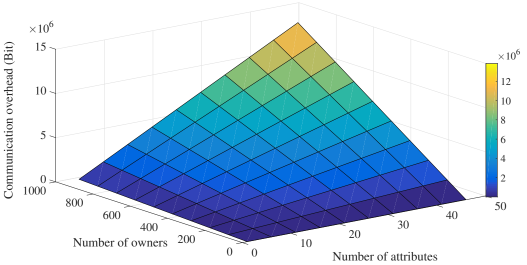


Figure 5: Owner-To-CSP communication overhead of our scheme

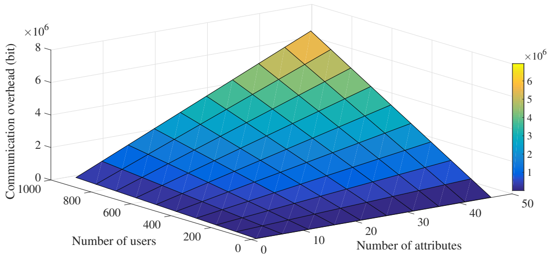


Figure 6: User-To-CSP communication overhead of our scheme

our scheme is secure enough for data sharing in the cloud computing. Moreover, we evaluated the performance of our scheme in computation and communication complexity and compared it with other ABE schemes. From the result we can see that the proposed scheme is low overhead and highly efficient. In our future research work, we will improve the generality of our scheme for using in a multi-authority environment.

Acknowledgments

The authors would like to thank the anonymous reviewers for their thorough reviews and highly appreciated comments and suggestions.

References

[1] Majid Bayat, Hamid Reza Arkian, and Mohammad Reza Aref, "A revocable attribute based data sharing scheme resilient to dos attacks in smart grid," *Wireless Networks*, vol. 21, no. 3, pp. 871–881, 2015.

[2] John Bethencourt, Amit Sahai, and Brent Waters, "Ciphertext-policy attribute-based encryption," in *2007 IEEE symposium on security and privacy (SP'07)*, pp. 321–334. IEEE, 2007.

[3] Dan Boneh and Matt Franklin, "Identity-based encryption from the weil pairing," in *Annual International Cryptology Conference*, pp. 213–229. Springer, 2001.

[4] Xin Dong, Jiadi Yu, Yuan Luo, Yingying Chen, Guangtao Xue, and Minglu Li, "Achieving an effective, scalable and privacy-preserving data sharing service in cloud computing," *computers & security*, vol. 42, pp. 151–164, 2014.

[5] Víctor Gayoso Martínez, Luis Hernández Encinas, and Carmen Sánchez Ávila, "A survey of the elliptic curve integrated encryption scheme," 2010.

[6] Vipul Goyal, Omkant Pandey, Amit Sahai, and Brent Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proceedings of the 13th ACM conference on Computer and communications security*, pp. 89–98. Acm, 2006.

[7] Susan Hohenberger and Brent Waters. "Attribute-based encryption with fast decryption,". in *Public-Key Cryptography–PKC 2013*, pp. 162–179. Springer, 2013.

[8] Caihui Lan, Haifeng Li, Shoulin Yin, and Lin Teng, "A new security cloud storage data encryption scheme based on identity proxy re-encryption.," *IJ Network Security*, vol. 19, no. 5, pp. 804–810, 2017.

[9] Jin Li, Yinghui Zhang, Xiaofeng Chen, and Yang Xiang, "Secure attribute-based data sharing for resource-limited users in cloud computing," *Computers & Security*, vol. 72, pp. 1–12, 2018.

[10] Ruixuan Li, Chenglin Shen, Heng He, Xiwu Gu, Zhiyong Xu, and Cheng-Zhong Xu, "A lightweight secure data sharing scheme for mobile cloud computing," *IEEE Transactions on Cloud Computing*, vol. 6, no. 2, pp. 344–357, 2018.

[11] Kaitai Liang, Liming Fang, Willy Susilo, and Duncan S Wong, "A ciphertext-policy attribute-based proxy re-encryption with chosen-ciphertext security," in *Intelligent Networking and Collaborative Systems (INCoS), 2013 5th International Conference on*, pp. 552–559. IEEE, 2013.

[12] Ueli Maurer, "Unifying zero-knowledge proofs of knowledge," in *International Conference on Cryptology in Africa*, pp. 272–286. Springer, 2009.

[13] San Murugesan and Irena Bojanova, "Cloud computing," *Encyclopedia of Cloud Computing*, vol. 13, no. 2, pp. 92–97, 2016.

[14] Yogachandran Rahulamathavan, Suresh Veluru, Jinguang Han, Rongxing Lu, Fei Li, and Muttukrishnan Rajarajan, "User collusion avoidance scheme for privacy-preserving decentralized key-policy attribute-based encryption," 2016.

[15] Amit Sahai and Brent Waters, "Fuzzy identity-based encryption," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 457–473. Springer, 2005.

[16] Yanfeng Shi, Qingji Zheng, Jiqiang Liu, and Zhen Han, "Directly revocable key-policy attribute-based encryption with verifiable ciphertext delegation," *Information Sciences*, vol. 295, pp. 221–231, 2015.

[17] Ilya A Sukhodolskiy and Sergey V Zapechnikov, "An access control model for cloud storage using attribute-based encryption," in *Young Researchers in Electrical and Electronic Engineering (EIConRus), 2017 IEEE Conference of Russian*, pp. 578–581. IEEE, 2017.

[18] Sreeja Cherillath Sukumaran and Mohammed Misbahuddin, "Dna cryptography for secure data storage in cloud.," *IJ Network Security*, vol. 20, no. 3, pp. 447–454, 2018.

[19] Nyamsuren Vaanchig, Hu Xiong, Wei Chen, and Zhiguang Qin, "Achieving collaborative cloud data storage by key-escrow-free multi-authority cp-abe scheme with dual-revocation," *International Journal of Network Security*, vol. 20, no. 1, pp. 95–109, 2018.

[20] Shulan Wang, Kaitai Liang, Joseph K Liu, Jianyong Chen, Jianping Yu, and Weixin Xie, "Attribute-based data sharing scheme revisited in cloud computing," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 8, pp. 1661–1673, 2016.

[21] Brent Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in *International Workshop on Public Key Cryptography*, pp. 53–70. Springer, 2011.

[22] J. Wei, W. Liu, and X. Hu, "Secure data sharing in cloud computing using revocable-storage identity-based encryption," *IEEE Transactions on Cloud Computing*, pp. 1–1, 2018.

[23] Xuanxia Yao, Zhi Chen, and Ye Tian, "A lightweight attribute-based encryption scheme for the internet of things," *Future Generation Computer Systems*, vol. 49, pp. 104–112, 2015.

[24] Lo-Yao Yeh, Pei-Yu Chiang, Yi-Lang Tsai, and Jiun-Long Huang, "Cloud-based fine-grained health information access control framework for lightweightiot devices with dynamic auditing andattribute revocation," *IEEE transactions on cloud computing*, vol. 6, no. 2, pp. 532–544, 2018.

[25] Yinghui Zhang, Xiaofeng Chen, Jin Li, Duncan S Wong, Hui Li, and Ilsun You, "Ensuring attribute privacy protection and fast decryption for outsourced data security in mobile cloud computing," *Information Sciences*, vol. 379, pp. 42–61, 2017.

[26] Yinghui Zhang, Dong Zheng, Xiaofeng Chen, Jin Li, and Hui Li, "Computationally efficient ciphertext-policy attribute-based encryption with constant-size ciphertexts," in *International Conference on Provable Security*, pp. 259–273. Springer, 2014.

[27] Yinghui Zhang, Dong Zheng, Xiaofeng Chen, Jin Li, and Hui Li, "Efficient attribute-based data sharing in mobile clouds," *Pervasive and Mobile Computing*, vol. 28, pp. 135–149, 2016.

[28] Yinghui Zhang, Dong Zheng, and Robert H Deng, "Security and privacy in smart health: efficient policy-hiding attribute-based access control," *IEEE Internet of Things Journal*, vol. 5, no. 3, pp. 2130–2145, 2018.

[29] Shungan Zhou, Ruiying Du, Jing Chen, Hua Deng, Jian Shen, and Huanguo Zhang, "Ssem: Secure, scalable and efficient multi-owner data sharing in clouds," *China Communications*, vol. 13, no. 8, pp. 231–243, 2016.

[30] Zhibin Zhou, Dijiang Huang, and Zhijie Wang, "Efficient privacy-preserving ciphertext-policy attribute based-encryption and broadcast encryption," *IEEE Transactions on Computers*, vol. 64, no. 1, pp. 126–138, 2015.

Biography

Saeid Rezaei was graduated from master degree in computer science. He is a researcher in Shahed University. His research interests include Cloud Computing and Storage, cryptography, privacy and digital signature schemes.

Mohammad Ali Doostari received his B.Sc. degree in Computer Engineering from Shiraz University in 1975. He received his M.Sc and Ph.D degrees from Kyoto University of Technology in the field of Information and Electronics Engineering. Upon graduation, he had been employed in Engineering and Technical College of Shahed University as a faculty member. From 2000, he has been involved in research works on IT Security and Smart Cards. His current research interests include areas of E-Voting, E-Payment, Trusted Computing, Smart Cards and cryptography.

Majid Bayat received his Ph.D. from the Department of Mathematics and Computer Sciences at Kharzmi University in Tehran, Iran. He is presently a Research Assistant of Kharzmi university and Information Systems and Security Lab (ISSL) of Sharif University in Tehran, Iran. His research interests include VANETs , smart grids, cryptographic protocols and provable security.

Guide for Authors

International Journal of Electronics and Information Engineering

International Journal of Electronics and Information Engineering (IJEIE) will be committed to the timely publication of very high-quality, peer-reviewed, original papers that advance the state-of-the art and applications of Electronics and Information Engineering. Topics will include, but not be limited to, the following: Algorithms, Bioinformatics, Computation Theory, AI, Fuzzy Systems, Embedded Systems, VLSI/EDA, Computer Networks, Information Security, Database, Data Mining, and Information Retrieval, Digital Content, Digital Life, and Human Computer Interaction, Image Processing, Computer Graphics, and Multimedia Technologies, Information Literacy, e-Learning, and Social Media, Mobile Computing, Wireless Communications, and Vehicular Technologies, Parallel, Peer-to-peer, Distributed, and Cloud Computing, Semiconductor, Software Engineering and Programming Languages, Telecommunication, etc.

1. Submission Procedure

Authors are strongly encouraged to submit their papers electronically by using online manuscript submission at http://ijeie.jalaxy.com.tw/.

2. General

Articles must be written in good English. Submission of an article implies that the work described has not been published previously, that it is not under consideration for publication elsewhere. It will not be published elsewhere in the same form, in English or in any other language, without the written consent of the Publisher.

2.1 Length Limitation:

All papers should be concisely written and be no longer than 30 double-spaced pages (12-point font, approximately 26 lines/page) including figures.

2.2 Title page

Title page should contain the article title, author(s) names and affiliations, address, an abstract not exceeding 100 words, and a list of three to five keywords.

2.3 Corresponding author

Clearly indicate who is willing to handle correspondence at all stages of refereeing and publication. Ensure that telephone and fax numbers (with country and area code) are provided in addition to the e-mail address and the complete postal address.

2.4 References

References should be listed alphabetically, in the same way as follows:

For a paper in a journal: M. S. Hwang, C. C. Chang, and K. F. Hwang, ``An ElGamal-like cryptosystem for enciphering large messages," *IEEE Transactions on Knowledge and Data Engineering*, vol. 14, no. 2, pp. 445--446, 2002.

For a book: Dorothy E. R. Denning, *Cryptography and Data Security*. Massachusetts: Addison-Wesley, 1982.

For a paper in a proceeding: M. S. Hwang, C. C. Lee, and Y. L. Tang, ``Two simple batch verifying multiple digital signatures," in *The Third International Conference on Information and Communication Security (ICICS2001)*, pp. 13--16, Xian, China, 2001.

In text, references should be indicated by [number].

2.5 Author benefits

No page charge is made.

Subscription Information

Individual subscriptions to IJEIE are available at the annual rate of US$ 200.00 or NT 6,000 (Taiwan). The rate is US$1000.00 or NT 30,000 (Taiwan) for institutional subscriptions. Price includes surface postage, packing and handling charges worldwide. Please make your payment payable to "Jalaxy Technique Co., LTD." For detailed information, please refer to http://ijeie.jalaxy.com.tw or Email to ijeieoffice@gmail.com.