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

# IJEIE

## International Journal of Electronics and Information Engineering

Vol. 7, No. 2 (Dec. 2017)

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. 7, No. 2 (Dec. 1, 2017)**

# SMS-Based Automated E-Notice Board using Mobile Technology

Abayomi O. Agbeyangi, Joseph O. Odiete, and Olusegun Olatinwo
*(Corresponding author: Abayomi O. Agbeyangi)*

Department of Computer Engineering, Moshood Abiola Polytechnic, Abeokuta, Ogun State, Nigeria
(Email: abayomiagbeyangi@gmail.com)
*(Received July 14, 2017; revised and accepted Aug. 30, 2017)*

**Abstract**

Notice boards are seen as a means of disseminating useful information but challenges arise when there is need to update this information. In this paper, we present the development of an SMS controlled E-notice board which can be updated automatically and remotely. The system was implemented using a GSM Module IC controlled by a Microcontroller and an LCD display. The GSM module receives the message to be displayed as SMS, then transmits the message through the COM port to the microcontroller to validate the SMS and then displays the message on the LCD display. The results from the testing show that the E-notice board performs excellently on the various test conducted although there are some challenges that can be taken as further research.

*Keywords: Automated system, E-notice board, GSM module, Microcontroller, SMS*

## 1 Introduction

The possibility of sending messages through GSM has tremendously changed the way we communicate. Short or long messages can now be sent wirelessly from one end to the other remotely. The opportunity present by this can be harnessed using a microcontroller with a GSM Module to control a display board remotely by sending SMS to the GSM Module to display messages on a display board. According to [17], the simple tasks involved in displaying a message on a digital notice board may be terribly cumbersome and typically needs technical skills.

Using GSM mobile for displaying SMS on LCD notice board through wireless communication have been used in many ways [1, 2, 7, 9, 10, 12, 13, 15, 16, 17]. By using GSM networks, it is possible to decode the received SMS on the mobile phone to function in a particular way as necessary.

The adverts nowadays are going digital with the advent of LCD and LED display board. The big shops and the shopping centers today use digital displays. Also, in trains and buses stations, information for commuters is displayed on digital boards. People are now adapted to the idea of the world at its finger-tips.

As noted in [1], GSM systems operate at different frequency bands. For 2G, GSM networks operate in 900MHz or 1800MHz bands while most 3G networks operate in 2100MHz frequency band. With the alliance of microcontroller, GSM module could be further used for some of the very innovative applications including, GSM based home security system, GSM based robot control, GSM based DC motor controller, GSM based stepper motor controller, etc.

The GSM modem is a class of wireless MODEM devices that are designed for communication between a computer and GSM network [4]. It requires a SIM (Subscriber Identity Module) card just like mobile phones to activate communication with the network. They need AT commands, for interacting with processor or controller, which are communicated through serial communication. These commands are sent by the controller/processor. The MODEM sends back a result after it receives a command. Different AT commands supported by the MODEM can be sent by the processor/controller/computer to interact with the GSM and GPRS cellular network [4].

Specifically, GSM/GPRS module (Figure 1) assembles a GSM/GPRS modem with standard communication interfaces like RS-232 (Serial Port), USB etc., so that it can be easily interfaced with a computer or a microprocessor/microcontroller based system [4]. This interfacing enables the module to be useful in many GSM network enabled applications.

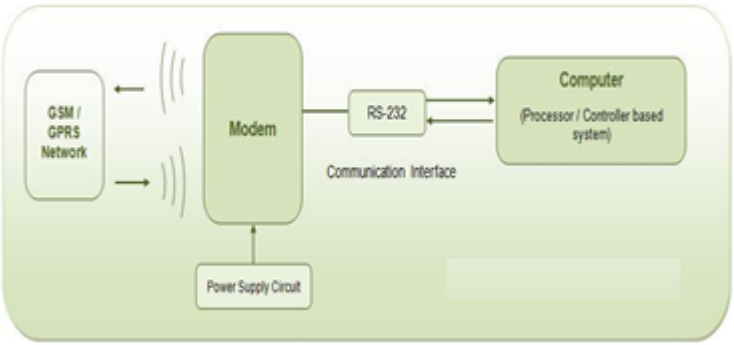


Figure 1: A GSM/GPRS Module Architecture
Source: [4]

According to [3], a GSM modem can also be a standard GSM mobile phone with the appropriate cable and software driver to connect to a serial port or USB port on the computer. But GSM module is usually preferable to a GSM mobile phone even if the former can perform the same operation. The GSM module has a wide range of applications in transaction terminals, supply chain management, security applications, weather stations and GPRS mode remote data logging among many others.

The remaining part of the paper is structured as follows: Section 2 highlighted some related works to this study; Section 3 explains the material and methods used. Section 4 discusses the results obtained, while Section 5 concludes the paper.

## 2 Related Works

In the work of [1], a multiuser SMS Based Wireless Electronic Notice Board, the work is aimed at displaying notices in colleges on electronic notice board by sending messages in form of SMS through mobile phone. It is a wireless transmission system which has very fewer errors and maintenance. The hardware board contains microcontroller AT89C52 at the heart of the system. The microcontroller is interfaced with GSM Modem via MAX232 level converter. It is used to convert RS232 voltage levels to TTL voltage levels and vice versa. The hardware also has a 64K EEPROM chip AT24C64. This EEPROM is used to store the timings and messages to be displayed. It also contains a real time

clock DS1307 to maintain and track the circuit time. A 16x2 Character LCD display is attached to the microcontroller for display. They propose a multicast SMS architecture over their backbone network. The circuit simulation indicates that the proposed approach has optimal efficiency by adjusting parameters, and the proposed architecture efficiently provides self-routing capability and multicast functionality in their cellular back-bone network. The study also provides further insight on the issues of multicast wireless cellular backbone network and demonstrates a referable methodology to propose and analyze a multicast cellular backbone network, which can promote the technology of personal communication network.

The user interface and the efficiency of mobile device network have been seen as the main concerns in the design of mobile device enabled application. In [1, 2, 9], the design uses single layered touch screen based user interface. Unlike conventional multi-layered user interface, a single-layered user interface will make the user interface more user-friendly with smaller size. The memory requirements can be further reduced by implementing it in low-level languages. After design and implementation of the user interface, they integrate the user interface with the hardware of mobile devices through serial port with the help of AT commands. The current trend of increasing instant messaging (IM) use and its potential growth motivate their study. It offers a novel exploration of users? preferences for IM in the context of the use of other traditional and new communication media: face-to-face, telephone, email, and short messaging service (SMS) in two distinct cultures: Australia and China. It examines the impact of demographics, media experience, media richness perception, and national culture on media preferences. Their results, based on a student survey conducted in the two countries, show that women prefer IM for communication activities that require more attention and personal presence and prefer email for communication activities that require less personal presence. Communication technology experience may predict the adoption of new technology, such as IM and SMS, but has no effect on media that are already widely adopted, such as email. Email was clustered with face-to-face and telephone as the most preferred media for any communication activity, while IM and SMS clustered together and were the least preferred media for communication. After controlling for demographics and media experience, it was found out that significant cultural differences in IM, telephone, and email preferences. Chinese preferred to use IM and telephone, while Australians preferred to use email. The cultural impact on technology use is persistent.

In [6], it was shown that display boards are one of the major communications media for mass media. They were able to also prove that local language can be added as a variation in the project by using graphics and other decoding techniques. They further show that the design saves time, energy and hence environment by reducing the cost of printing and photocopying as information can be display to a large number of people via GSM network.

It was also shown in [5] that, introducing the concept of wireless technology in the field of communication, we can make our communication more efficient and faster, with greater efficiency messages can be displayed with fewer errors and maintenance. Other works of note can also be found in [8, 11, 14].

# 3 Material and Method

The main problem that prompts us to undergo this research work was the inability of display boards in most places particularly tertiary institution to be easily updated. This work seeks to eliminate this challenge by allowing for easy update of notice board electronically via GSM Network. The message that is to be displayed is sent through an SMS from a mobile phone to the authorized SIM in the GSM module. The microcontroller receives the SMS from the authorized transmitter, validates the sending Mobile Identification Number (MIN) and displays the desired information on the Liquid Crystal Display (LCD) which serves as the notice board. The core components used are:

- 18F26K22 microcontroller
- GSM module
- Power supply
- 16x2 LCD display
- SIM (MTN Nigeria)

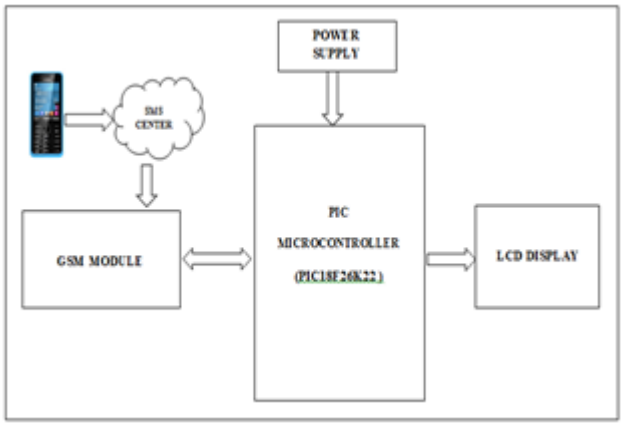


Figure 2: Block diagram of the E-notice Board

The diagram as shown in Figure 2 presents the block diagram of the system which shows the architecture of the system.

The circuit diagram presented in Figure 3 shows the connection between the LCD display and Microcontroller. Also in Figure 4, the procedure for the operation of the system is shown in a flowchart. The flowchart explains the step-by-step operation of the E-notice board. First, the incoming message is checked if valid, i.e. it's from a valid source. If this is true, the message is displayed otherwise, it is rejected and keep displaying the old message.

# 4 Results and Discussion

The implementation of the design passed all the necessary design test conducted. Each stage in the development process was tested and evaluated in reference to the existing setup. This test shows that the system performs relatively well as compared to the existing system. The functionality was further confirmed by sending messages to the display and each messages having authenticated to be valid was displayed.

The prototype of the complete system is shown in Figure 5. In the figure, the system enclosure was opened showing the interconnection between the various component. Figure 6 shows the neatly coupled E-notice board prototype.

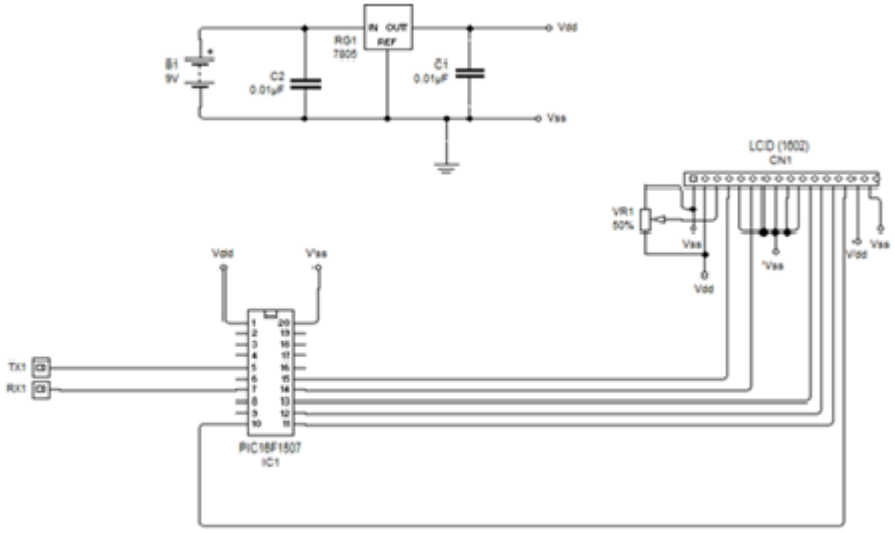


Figure 3: Circuit diagram showing LCD connection with the microcontroller

## 5 Conclusions

The development of the e-notice board shows how the use of GSM technology can be applied to enhance the functionality and flexibility of a modern notice board. Although the design can only display 60 characters due to the size of the LCD display used, it can be extended to a bigger display using the same technology. The design proves to be cost-effective by taking the advantages of the inexpensive components used. The area noted for further research is the enhancement of the design using a bigger electronics display board.

## References

[1] M. Baby, G. Divya, G. Harini, and Y. E. Slesser, "Sms based wireless e-notice board," *International Journal of Advanced Electrical and Electronics Engineering (IJAEEE)*, vol. 2, no. 6, pp. 106–110, 2013.

[2] M. Baby, P. Harini, Y. E. Slesser, Y. Tejaswi, K. Ramajyothi, M. Sailaja, and K. A. Sumantha, "Sms based wireless e-notice board," *International Journal of Emerging Technology and Advanced Engineering*, vol. 3, no. 3, pp. 181–185, 2013.

[3] ElProCus. "What is gsm: Architecture and working of gsm module with circuit,". Retrieved from `https://www.elprocus.com/gsm-architecture-features-working/`, 20th February, 2017.

[4] Engineersgarage.com. "Gsm/gprs module,". Retrieved from `https://www.engineersgarage.com/articles/gsm-gprs-modules` on 20th February, 2017.

[5] R. Gowtham, K. Kavipriya, G. Kesavaraj, A. Natheena, and S. Maragatharaj, "Multiuser short message service based wireless electronic notice board," *International Journal of Engineering and Computer Science*, vol. 2, no. 4, pp. 1035–1041, 2013.

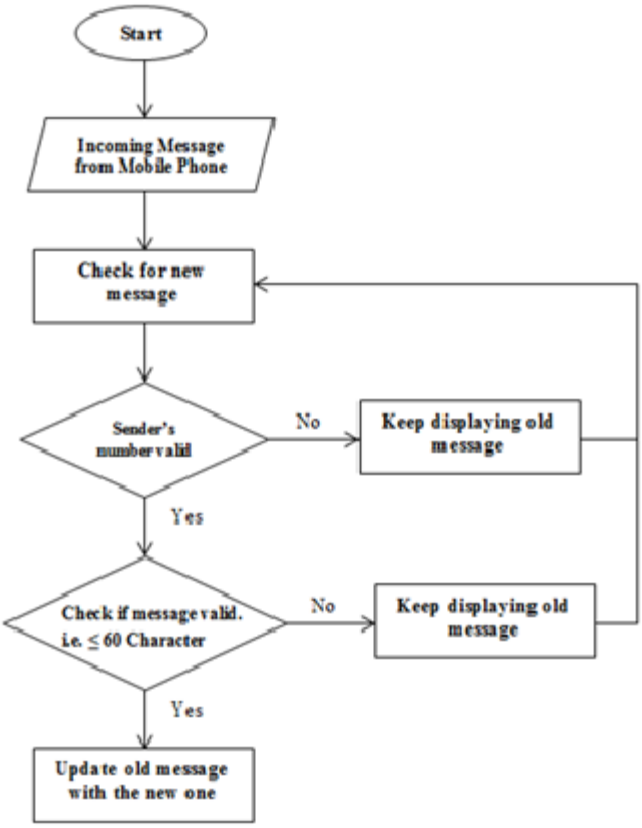


Figure 4: Flowchart of the E-notice Board


Figure 5: The E-notice Board Setup

Figure 6: The E-notice Board Prototype after coupling

[6] F. Kamdari, A. Malhotra, and P. Mahadik, "Display message on notice board using gsm," *Advance in Electronic and Electric Engineering*, vol. 3, no. 7, pp. 827–832, 2013.
[7] P. U. Ketkar, K. P. Tayade, A. P. Kulkarni, and R. M. Tugnayat, "Gsm mobile phone based led scrolling message display system," *International Journal of Scientific Engineering and Technology*, vol. 2, no. 3, pp. 149–155, 2013.
[8] J. Komal, S. Sana, S. Swapnali, B. Jasmin, and R. N. Mahind, "Android based college notification system," *International Research Journal of Engineering and Technology (IRJET)*, vol. 3, no. 3, pp. 1768–1770, 2016.
[9] P. Kumar, V. Bhrdwaj, K. Pal, N. S. Rathor, and A. Mishra, "Gsm based e-notice board: Wireless communication," *International Journal of Soft Computing and Engineering*, vol. 2, no. 3, pp. 601–605, 2012.
[10] P. S. Kumar, V. Priyanka, L. Surekha, and Y. H. Reddy, "Gsm based wireless electronic notice board display through arm7 and led," *International Journal of Advanced Technology and Innovative Research*, vol. 8, no. 5, pp. 0864–0868, 2016.
[11] A. Meenachi, S. Kowsalya, and P. P. Kumar, "Wireless e-notice board using wi-fi and bluetooth technology," *Journal of Network Communications and Emerging Technologies (JNCET)*, vol. 6, no. 4, pp. 14–20, 2016.
[12] P. Mishra, P. Singh, and S. Gupta, "Sms based wireless notice board display using gsm mobile," *International Journal of Advance Research in Science and Engineering*, vol. 2, no. 10, pp. 20–24, 2013.
[13] A. Mujumdar, V. Niranjane, and D. Sagne, "Scrolling led display using wireless transmission," *International Journal of Engineering Development and Research*, vol. 2, no. 1, pp. 475–478, 2014.
[14] K. G. Ramchandra and J. Rohit, "Wireless digital notice board using gsm technology," *International Research Journal of Engineering and Technology (IRJET)*, vol. 2, no. 9, pp. 57–59, 2015.
[15] B. Saini, R. Devi, S. Dhankhar, S. Haque, and J. Kaur, "Smart led display boards," *International Journal of Electronic and Electrical Engineering*, vol. 7, no. 10, pp. 1057–1067, 2014.

[16] N. S. Sarma, N. S. Raju, T. V. Rao, B. D. Prasad, B. V. Satyanarayana, and N. P. Kumar, "A basic research on gsm based secured advertising system," *Journal of Information, Knowledge and Research in Electronics And Communication*, vol. 2, no. 2, pp. 933–936, 2013.

[17] A. M. Zungeru, G. D. Obikoya, O. F. Uche, and T. Eli, "Design and implementation of a gsm-based scrolling message display board," *International Journal of Computational Science, Information Technology and Control Engineering (IJCSITCE)*, vol. 1, no. 3, pp. 21–31, 2014.

## Biography

**Abayomi O. Agbeyangi** is currently a PhD student at the Department of Computer Science and Engineering, Obafemi Awolowo University, Ile-Ife, Nigeria. His research interests are focused on Artificial Intelligence (machine translation and natural language processing), Networking and Embedded Systems.

**Joseph O. Odiete** is a lecturer at the Department of Computer Engineering, Moshood Abiola Polytechnic, Abeokuta, Ogun State. He is a registered and practicing Engineer and a researcher whose research interests are focused on Networking and Embedded Systems.

**Olusegun Olatinwo** is a lecturer at the Department of Computer Engineering, Moshood Abiola Polytechnic, Abeokuta, Ogun State. He is a registered and practicing Engineer and a researcher whose research interests are focused on Biometric Technology, Networking and Embedded Systems.

I.J. of Electronics and Information Engineering, Vol.7, No.2, PP.61-67, Dec. 2017 (DOI: 10.6636/IJEIE.201712.7(2).02) 

# Anonymity and Certificateless Property Could Not Be Acquired Concurrently

Lihua Liu[1], Zhenzhen Guo[1], Zhengjun Cao[2], Zhen Chen[2]

*(Corresponding author: Zhengjun Cao)*

Department of Mathematics, Shanghai Maritime University, Shanghai, 201306, China[1].
1550 Haigang Ave, Pudong Xinqu, Shanghai Shi, China
(Email: caozhj@shu.edu.cn)
Department of Mathematics, Shanghai University, Shanghai 200444, China[2].
*(Received Sept. 1, 2017; revised and accepted Oct. 9, 2017)*

**Abstract**

We show that the anonymous certificateless authentication scheme [IEEE TIFS, 9(12), 2014, 2327-2339] is very vulnerable to denial-of-service (DoS) attacks, because it does not develop a mechanism to help an application provider to verify the validity of a service request. A malicious attacker can launch massive requests without being detected. We would like to stress that anonymity and certificateless property could not be acquired concurrently. We think the availability should be put first above all else when one designs a cryptographic scheme.

*Keywords: Anonymity; Availability; Certificateless Cryptography; Denial-of-service Attack*

## 1 Introduction

In computing, a denial-of-service (DoS) attack is an attempt to make a machine or network resource unavailable to its intended users, such as to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet. Harassing calls and malicious calls attacks which can be easily launched and hidden, are the most serious problems. The scale of DoS attacks has continued to rise over recent years.

Certificateless cryptography [1] is a variant of ID-based cryptography [5,11,21,23] in order to prevent the key escrow problem. Its key generation process is split between the key generation center (KGC) and the user. Notice that in certificateless cryptography the identity information no longer forms the entire public key. That is, the user's public key is not discoverable from only the user's identity string and the KGC's public key. Thus, the user's public key must be published by himself. Naturally, the method of distributing the user's public key does not have to be secure. The identity string and the KGC's public key can be used to verify that the obtained public key belongs to the identity string.

Key-replacement attack against certificateless cryptographic schemes is broadly adopted by [13, 14, 15,18,19,20]. In certificateless cryptography, it is still a challenge to efficiently form basic trust between communicating entities.

Anonymity is used to describe situations where the acting person's name is unknown. Its important idea is that a person could be non-identifiable, unreachable or untrackable. Hsien et al. [8, 9, 12, 16, 17]

studied the problems of public auditing and attribute-based access control with user revocation in the scenario of cloud computing.

Very recently, Xiong [24] has proposed an anonymous certificateless remote authentication scheme. In this note, we remark that the scheme is very vulnerable to DoS attacks. In the scheme an application provider cannot distinguish between the spoofed requests and legitimate requests. So, the victim responds to the spoofed requests as it normally would do. The weakness makes the scheme lose its availability entirely.

## 2 Review of Xiong's Scheme

The scheme involves three entities: the wireless body area networks (WBAN) client, the application provider (AP) and the network manager (NM). All clients are equipped with certain terminals, i.e., wearable sensors, biosensor and portable medical device, which are preloaded with public parameters and registered with the NM before they can access the medical services provided by AP. An application provider represents a medical institution such as a hospital or a clinic, which is also preloaded with public parameters and registered with the NM.

The scheme [24] can be briefly described as follows.

**Initialization.** NM sets the system public parameters as

$$\{\mathbb{F}_p, E/\mathbb{F}_p, G, P, P_{pub}, H_1, H_2, H_3, H_4, \mathrm{MAC}_{(\cdot)}(\cdot)\},$$

and sets the master secret key as $x$. We refer to the original [24] for the details.

**AP-Registration.** An AP with identity $ID_{AP}$ picks a secret value $x_{ID_{AP}} \in \mathbb{Z}_p^*$ and sets his public key as $upk_{ID_{AP}} = x_{ID_{AP}}P$. Upon receiving this AP's identity $ID_{AP}$ and the public key $upk_{ID_{AP}}$, NM picks $r_{ID_{AP}} \in \mathbb{Z}_p^*$, computes

$$\begin{aligned} R_{ID_{AP}} &= r_{ID_{AP}}P, \\ h_{ID_{AP}} &= H_1(ID_{AP} \| R_{ID_{AP}} \| upk_{ID_{AP}}), \\ s_{ID_{AP}} &= r_{ID_{AP}} + h_{ID_{AP}}x, \end{aligned}$$

and returns the partial private key $(s_{ID_{AP}}, R_{ID_{AP}})$ to this AP secretly.

**Client-Registration.** A client with the real identity $ID_R$ selects an pseudo-identity $ID_C$, picks a secret value $x_{ID_C} \in \mathbb{Z}_p^*$ and sets his public key as $upk_{ID_C} = x_{ID_C}P$. Upon receiving the client's real identity $ID_R$, pseudo-identity $ID_C$ and the public key $upk_{ID_C}$, NM picks $r_{ID_C} \in \mathbb{Z}_p^*$, computes

$$\begin{aligned} R_{ID_C} &= r_{ID_C}P, \\ h_{ID_C} &= H_1(ID_C \| R_{ID_C} \| upk_{ID_C}), \\ s_{ID_C} &= r_{ID_C} + h_{ID_C}x, \end{aligned}$$

and returns the partial private key $(s_{ID_C}, R_{ID_C})$ and a group of $\{ID_{AP}$, $upk_{ID_{AP}}, R_{ID_{AP}}\}$ for different APs to this client secretly.

**Authentication.** It consists of the following steps.

**Request.** A client associated with the pseudo-identity $ID_C$ picks $a \in \mathbb{Z}_p^*$ and computes $T_A = aP$. Pick the time $t_c \in \{0,1\}^{l_2}$ at the terminal, and compute

$$\begin{aligned} r &= H_2(ID_C, upk_{ID_C}, R_{ID_C}, T_A, t_c), \\ C_1 &= rP \\ C_2 &= H_3(r(upk_{ID_{AP}} + R_{ID_{AP}} + H_1(ID_{AP}\|R_{ID_{AP}}\|upk_{ID_{AP}})P_{pub})) \\ &\quad \oplus (ID_C\|upk_{ID_C}\|R_{ID_C}\|T_A\|t_c). \end{aligned}$$

Send a service request message $(C_1, C_2)$ to the target AP.

**Response.** Upon receiving $(C_1, C_2)$, the requested AP performs the following steps to authenticate the requesting client.

**Step 1.** Compute

$$ID_C\|upk_{ID_C}\|R_{ID_C}\|T_A\|t_c = H_3((x_{ID_{AP}} + s_{ID_{AP}})C_1) \oplus C_2.$$

**Step 2.** Check the freshness of $t_c$ and

$$H_2(ID_C, upk_{ID_C}, R_{ID_C}, T_A, t_c)P \stackrel{?}{=} C_1.$$

**Step 3.** Pick $b \in \mathbb{Z}_p^*$, compute

$$\begin{aligned} T_B &= bP,\ K_{AP-C}^2 = bT_A, \\ K_{AP-C}^1 &= s_{ID_{AP}}T_A + x_{ID_{AP}}T_A + b \cdot upk_{ID_C} \\ &\quad + b(R_{ID_C} + H_1(ID_C\|R_{ID_C}\|upk_{ID_C})P_{pub}), \\ key &= H_4\left(ID_C, ID_{AP}, upk_{ID_C}, upk_{ID_{AP}}, R_{ID_C}, R_{ID_{AP}}, T_A, T_B, K_{AP-C}^1, K_{AP-C}^2\right). \end{aligned}$$

**Step 4.** Return $(\mathrm{MAC}_{key}(T_B), T_B)$ to the client.

**Key-Extraction.** See the original description in [24].

# 3 Cryptanalysis of Xiong's Scheme

## 3.1 On Three Kinds of Public Information

In public-key cryptography, public parameters play an essential role. The public parameters bound to a cryptographic system are called system's public parameters, which can be shared by all users in the system. The public parameters bound to a special user are called user's public key, which can be used to authenticate the source of data.

Notice that in order to *bind one public key to an entity*, it is usual to introduce a trusted third party (TTP) who is generally assumed to be honest and fair. TTP is responsible for issuing public key certificates. However, TTP has no access to the secret or private keys of users.

Before creating a public-key certificate for Alice, TTP must take appropriate measures to verify the identity of Alice and that the public key to be certificated actually belongs to Alice. To this end, it is conventional that *Alice has to appear before the TTP with a passport as proof of identity*, and submit her public key along with evidence that she knows the corresponding private key [22]. Explicitly, a user's public key satisfies:

- It must be authenticated and issued by a certification authority.

- It should be easily verified and accessible to any user.
- It should be repeatedly usable in the life duration because the cost to generate and distribute a user's public key is somewhat expensive.

Some literatures have confused user's public key with user's public parameters. Strictly speaking, user's public parameters are issued by the user himself. These parameters could be *unauthentic*, but can be repeatedly used.

Table 1: Comparisons of different public information

| | |
|---|---|
| ID number | *simple*, easy to remember,<br>associated with a certificate issued<br>by some government department for *daily use* |
| user' public key | *complex*, hard to remember,<br>associated with a certificate issued<br>by some social institute for *cryptographic use* |
| user's public parameters | *complex*, hard to remember,<br>published directly by a user for *cryptographic use* |

Identity-based cryptography [23] aims to simplify the authentication of public key by merely using an identity string as a certain user's public key. In common identity-based cryptosystem [2,3,4,5,6,7,10], there is a trusted party, called the private key generator (PKG), who generates the secret key for each user's identity. As the PKG generates and holds the secret key for all users, a complete trust must be placed on the PKG. We refer to Table 1 for the comparisons of different public information.

## 3.2 On Three Kinds of Cryptography

In a public-key system, a participator has to authenticate the legitimation of the invoked public key. The verification relies on a public key infrastructure (PKI) which vouches for the connection between the intended receiver's identity and a particular public key.

Identity-based encryption removes the need for a PKI, replacing it with the need for PKG for assigning all users' private keys. In 2003, Al-Riyami and Paterson [1] put forth a new primitive, certificateless cryptography, that avoids the drawbacks of both traditional public-key cryptography and identity-based cryptography. See Table 2 for the comparisons of three kinds of cryptography.

We here would like to stress that in certificateless cryptography [13,14,15,18], the invoked ID number must be legitimate. Actually, the credibility of the invoked ID number originates just from its associated certificate, which is issued by the relevant government department, such as passport issuing authority. This means the so-called certificateless cryptography is *not totally certificateless*. It has to make use of the certificate associated to a certain ID in order to build trust. Some researchers have misunderstood the essence and proposed several false attacks against certificateless cryptography by replacing users' IDs optionally.

## 3.3 Xiong's Scheme is Vulnerable to DoS Attacks

Xiong's scheme is an anonymous certificateless authentication one. It satisfies:

**Anonymity.** A client is not forced to invoke his true ID number when he sends a request to the application provider AP.

Table 2: Comparisons of three kinds of cryptography

| | public-key cryptography | ID-based cryptography | certificateless cryptography |
|---|---|---|---|
| ID number | —— | invoked, certificate-checking for a fresh ID number | invoked, certificate-checking for a fresh ID number |
| user's public key/parameters | invoked, certificate-checking, for a fresh *public key* | —— | invoked, no certificate-checking for *public parameters* |
| secret key | set by the user, *exclusive* | totally assigned by some social institute, *nonexclusive* | partially assigned by some social institute, *partially exclusive* |

**Certificateless.** The invoked user's public parameters are not certified when AP responds to an anonymous request.

It is easy to find that an application provider cannot immediately authenticate the validity and source of a service request. *A malicious adversary can launch massive requests in order to make an application provider unavailable to its legitimate users.* What makes it more serious is that the adversary's malicious behaviors cannot be detected by the victim and the network manager.

We now describe a possible attack launched by an outer adversary as follows. The adversary generates an pseudo-identity $\widehat{ID}$, chooses two random elements in $G$ and sets them as the public parameters $upk_{\widehat{ID}}, R_{\widehat{ID}}$ respectively. For the target AP with the public parameter $\{ID_{AP}, upk_{ID_{AP}}, R_{ID_{AP}}\}$, the adversary picks a random $T \in G$ and the time $\widehat{t} \in \{0,1\}^{l_2}$ at the terminal, and computes

$$\begin{aligned} r &= H_2(\widehat{ID}, upk_{\widehat{ID}}, R_{\widehat{ID}}, T, \widehat{t}), \\ \widehat{C}_1 &= rP, \\ \widehat{C}_2 &= H_3(r(upk_{ID_{AP}} + R_{ID_{AP}} + H_1(ID_{AP} \| R_{ID_{AP}} \\ &\qquad \| upk_{ID_{AP}}) P_{pub})) \oplus (\widehat{ID} \| upk_{\widehat{ID}} \| R_{\widehat{ID}} \| T \| \widehat{t}). \end{aligned}$$

Send the request message $(\widehat{C}_1, \widehat{C}_2)$ to the target AP.

The request will pass the AP's checking process. In fact,

$$\begin{aligned} & H_3((x_{ID_{AP}} + s_{ID_{AP}})\widehat{C}_1) \oplus \widehat{C}_2 \\ = \; & H_3((x_{ID_{AP}} + r_{ID_{AP}} + h_{ID_{AP}} x)\widehat{C}_1) \oplus \widehat{C}_2 \\ = \; & H_3(r(x_{ID_{AP}} P + r_{ID_{AP}} P + h_{ID_{AP}} xP)) \oplus \widehat{C}_2 \\ = \; & \widehat{ID} \| upk_{\widehat{ID}} \| R_{\widehat{ID}} \| T \| \widehat{t} \end{aligned}$$

Moreover,

$$H_2(\widehat{ID}, upk_{\widehat{ID}}, R_{\widehat{ID}}, T, \widehat{t})P = \widehat{C}_1.$$

All in all, AP cannot recognize the spoofed request and will respond to it as normally do.

It claims that Xiong's scheme can provide mutual authentication, session key establishment and nonrepudiation. Particularly, the real identity of the requesting client cannot be revealed by anyone. We want to point out that the function that a patient can anonymously access a clinic is *double-edged*. It protects the client's privacy perfectly, but puts the clinic in jeopardy.

## 4 Conclusion

We show that anonymity and certificateless property could not be acquired concurrently because application providers cannot verify the validity of requests. We would like to stress that one must carefully evaluate the design objectives in order to ensure the availability of a cryptographic system.

## Acknowledgements

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

## References

[1] S. Al-Riyami and K. Paterson, "Certificateless public key cryptography," in *Proceedings of 9th International Conference on the Theory and Application of Cryptology and Information Security, Advances in Cryptology (ASIACRYPT'03)*, pp. 452–473, Taipei, Taiwan, Dec. 2003.

[2] D. Boneh and X. Boyen, "Short signatures without random oracles," *Journal of Cryptology*, vol. 21, no. 2, pp. 149–177, 2008.

[3] D. Boneh and X. Boyen, "Efficient selective identity-based encryption without random oracles," *Journal of Cryptology*, vol. 24, no. 4, pp. 659–693, 2011.

[4] D. Boneh, R. Canetti, S. Haleviand, J. Katz, "Chosen-ciphertext security from identity-based encryption," *SIAM Journal on Computing*, vol. 36, no. 5, pp. 1301–1328, 2007.

[5] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in *Proceedings of 21st Annual International Cryptology Conference, Advances in Cryptology (CRYPTO'01)*, pp. 213–229, Santa Barbara, California, USA, Aug. 2001.

[6] D. Boneh, A. Raghunathan, and G. Segev, "Function-private identity-based encryption: Hiding the function in functional encryption," in *Proceedings of 33rd Annual Cryptology Conference, Advances in Cryptology (CRYPTO'13)*, pp. 461–478, Santa Barbara, CA, USA, Aug. 2013.

[7] D. Boneh, H. Shacham, and B. Lynn, "Short signatures from the weil pairing," *Journal of Cryptology*, vol. 17, no. 4, pp. 297–319, 2004.

[8] Z. Cao, L. Liu, and O. Markowitch, "Analysis of one scheme for enabling cloud storage auditing with verifible outsourcing of key updates," *International Journal of Network Security*, vol. 19, no. 6, pp. 950–954, 2017.

[9] W. Chao, C. Tsai, and M. Hwang, "An improved key-management scheme for hierarchical access control," *International Journal of Network Security*, vol. 19, no. 4, pp. 639–643, 2017.

[10] J. Coron, "A variant of boneh-franklin ibe with a tight reduction in the random oracle model," *Design, Codes and Cryptography*, vol. 50, no. 1, pp. 115–133, 2009.

[11] L. Deng, H. Huang, and Y. Qu, "Identity based proxy signature from rsa without pairings," *International Journal of Network Security*, vol. 19, no. 2, pp. 229–235, 2017.

[12] W. F. Hsien, C. C. Yang, and M. S. Hwang, "A survey of public auditing for secure data storage in cloud computing," *International Journal of Network Security*, vol. 18, no. 1, pp. 133–142, 2016.

[13] B. Hu, D. Wong, Z. Zhang, and X. Deng, "Key replacement attack against a generic construction of certificateless signature," in *Proceedings of 11th Australasian Conference Information Security and Privacy (ACISP'06)*, pp. 235–246, Melbourne, Australia, July 2006.

[14] X. Huang, W. Susilo, Y. Mu, and F. Zhang, "On the security of certificateless signature schemes from asiacrypt 2003," in *Proceedings of 4th International Conference, Cryptology and Network Security (CANS'05)*, pp. 13–25, Xiamen, China, Dec. 2005.

[15] J. Lai and W. Kou, "Self-generated-certificate public key encryption without pairing," in *Proceedings of 10th International Conference on Practice and Theory in Public-Key Cryptography (PKC'07)*, pp. 476–489, Beijing, China, Apr. 2007.
[16] C. W. Liu, W. F. Hsien, C. C. Yang, and M. S. Hwang, "A survey of attribute-based access control with user revocation in cloud data storage," *International Journal of Network Security*, vol. 18, no. 5, pp. 900–916, 2016.
[17] C. W. Liu, W. F. Hsien, C. C. Yang, and M. S. Hwang, "A survey of public auditing for shared data storage with user revocation in cloud computing," *International Journal of Network Security*, vol. 18, no. 4, pp. 650–666, 2016.
[18] J. Liu, Z. Zhang, X. Chen, and K. Kwak, "Certificateless remote anonymous authentication schemes for wirelessbody area networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 2, pp. 332–342, 2014.
[19] L. Liu, Z. Cao, and O. Markowitch, "A note on design flaws in one aggregated-proof based hierarchical authentication scheme for the internet of things," *International Journal of Electronics and Information Engineering*, vol. 5, no. 2, pp. 79–82, 2016.
[20] L. Liu, W. Kong, Z. Cao, and J. Wang, "Analysis of one certificateless encryption for secure data sharing in public clouds," *International Journal of Electronics and Information Engineering*, vol. 6, no. 2, pp. 108–113, 2017.
[21] L. Liu and J. Ye, "A homomorphic universal re-encryptor for identity-based encryption," *International Journal of Network Security*, vol. 19, no. 1, pp. 11–19, 2017.
[22] A. Menezes, P. Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*, USA: CRC Press, 1996.
[23] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Proceedings of Advances in Cryptology (CRYPTO'84)*, pp. 47–53, Santa Barbara, California, USA, Aug. 1984.
[24] H. Xiong, "Cost-effective scalable and anonymous certificateless remote authentication protocol," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 12, pp. 2327–2339, 2014.

## 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.

**Zhenzhen Guo** 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 served as a post-doctor in Computer Sciences Department, Université Libre de Bruxelles, from 2008 to 2010. His research interests include cryptography, discrete logarithms and quantum computation.

**Zhen Chen** is currently pursuing his M.S. degree from Department of Mathematics, Shanghai University. His research interests include information security and cryptography.

# Overview of Using Private Cloud Model with GIS

Salah E. Elgazzar, Ahmed A. Saleh, Hazem M. El-Bakry
*(Corresponding author: Hazem M. El-Bakry)*

Information Systems Department, Faculty of Computer and Information Sciences, Mansoura University
El Gomhouria St, Mansoura, Dakahlia Governorate 35516, Egypt
(Email: helbakry5@yahoo.com)

*(Received Sept. 1, 2017; revised and accepted Oct. 9, 2017)*

**Abstract**

Cloud computing is an emerging computing technology that enter many fields due to its benefits; which are the high speed in processing as it depends on parallel computing, high storage capacity, and high speed of data transfer. In GIS, when dealing with raster data, the main obstacles are the data size- a characteristic of raster data- and the need for long processing time. By benefiting of Cloud computing, GIS raster data model used easily without worrying about its obstacles. This paper highlights the recent researches that relates the integration of GIS and private Cloud computing model through studying the published papers related to this area. Our review effort led to that the cloud computing service model in all studies was Platform as a Service (PaaS), studies conducted are in its preliminary stages, and these studies had different point of interest; storage - processing - an attempt to develop a Software as a Service (SaaS) for civil engineering sector.

*Keywords: Cloud Computing; GIS; Private Cloud Computing*

## 1 Introduction

One of the rising computing technology nowadays is Cloud computing. Cloud computing, according to National Institute of Standards and Technology NIST, "is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" [3].

A Geographic Information System (GIS) enable us to visualize, question, analyze, and interpret data to understand relationships, patterns, and trends. GIS benefits organizations of all sizes and in almost every industry. The interest and the awareness in the value of GIS is growing [8]. Data is considered the backbone of any information system. In GIS, data are represented in two models, vector and raster data models. Vector model represents the world as a collection of coordinates connected with line or arcs, while raster model represents the world as a grid of pixels. The main issues when dealing with the raster model is the data size and the time needed for processing its data. By benefitting from Cloud computing, we can use easily the raster data model. In this paper, we try to identify the recent findings in the area of integrating GIS with private Cloud computing model. A systematic literature reviews were conducted based on a structure search process. The keywords "GIS" and "private cloud"

were used and the search was limited to ABI/INFORM database Computer Science Index - ProQuest computing, Applied Science & Technology Source - EBSCO, and Google scholar.

This paper is organized as follows. Section 2 presents an overview of Cloud computing and GIS. The details of the review process is presented in Section 3. In Section 4 the results of the review is presented and discussed. Section 5 presents the conclusion of this study.

# 2 Cloud Computing and GIS

This section is divided into two subsections. The first is for an overview of Cloud computing technology and the second is about GIS.

## 2.1 Overview of Cloud Computing

One of the recent rising computing technology is Cloud computing. Cloud computing, according to National Institute of Standards and Technology NIST, "is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" [3, 14] (See Figure 1).

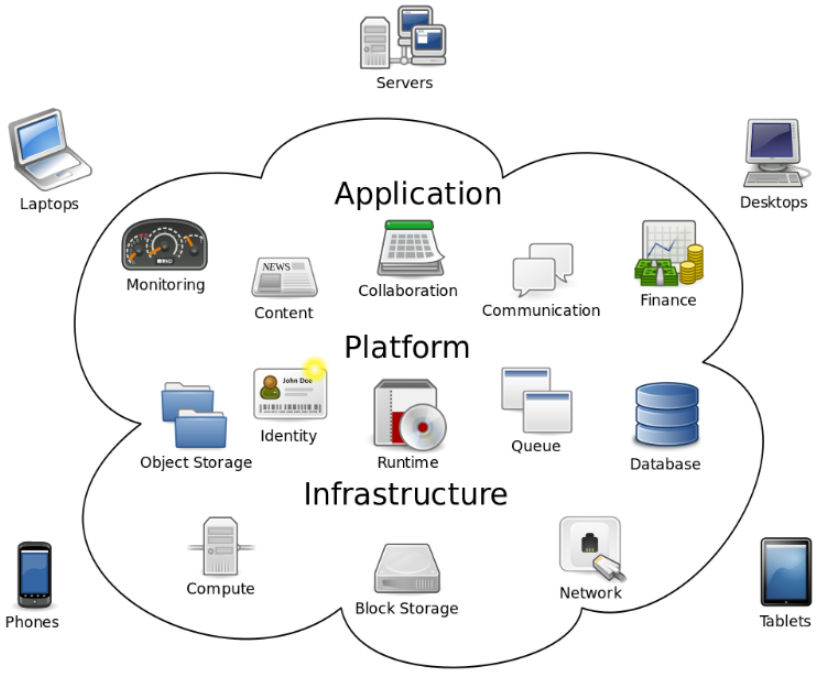


Figure 1: Cloud computing

The cloud model is composed of five essential characteristics, three service models, and four deployment models [14].

#### 2.1.1 Essential Characteristics

1) On-demand self-service. A consumer/tenant can alter his computing capabilities (e.g., server time and network storage) from the service provider as needed automatically without the need of any support.

2) Broad network access. Cloud resource can be accessed through different device types (e.g., mobile phones, tablets, laptops, and workstations) and from various locations.

3) Resource pooling. The Cloud computing resources (e.g., storage, processing, memory, and network bandwidth) are pooled to serve multiple consumers/tenants either physical or virtual. These resources can be adjusted to suit the needs of every consumer, and the consumer does not need to know the exact location of resources provided.

4) Rapid elasticity. (scalable services). For the consumer/tenant, the resources available for provisioning often seems unlimited and can be obtained in any quantity at any time.

5) Measured service. Cloud provider automatically measure, monitor, and control the use of cloud resource (e.g., storage used, processing used, bandwidth consumed, and active user accounts) for different reasons (e.g. billing, effective use of resources, and overall predictive planning).

#### 2.1.2 Service Models

Cloud computing services are divided into three service models, namely: Infrastructure as a Service, Platform as a Service, and Software as a Service, these three models conform the Cloud computing stack (See Figure 2):

1) Infrastructure as a Service (IaaS): In this service model, the consumer/tenant is capable to provision different cloud resources (e.g. processing, storage, networks, and other fundamental computing resources) and the consumer/tenant is able to deploy and run software system, which can include operating systems and applications. The consumer/tenant only control the software system not the cloud infrastructure; and he possibly has a limited control some networking components (e.g., host firewalls). Infrastructure services are the base layer of cloud computing systems [3, 17].

2) Platform as a Service (PaaS): In this service model, the consumer/tenant is capable to deploy onto the cloud infrastructure his applications that are supported by the provider technology. The consumer/tenant only has control over his staff (the deployed applications, its settings) and does not have control of the underlying cloud infrastructure [3].

3) Software as a Service (SaaS): In this service model, the consumer/tenant is to use the applications offered by the cloud provider. The consumer/tenant only manages the setting of the applications he uses [3].

#### 2.1.3 Deployment Models

Cloud computing can be presented/deployed using four different models. Regardless of the service model adopted in the cloud, the cloud can classified as Public, Private, Community, and Hybrid cloud depending on the adopted deployment model (See Figure 3).

1) Public cloud: The cloud is hosted by a third party organization, and located off premise at multiple locations outside the consumer organization. This cloud is "made available in a pay-as-you-go manner to the general public" [2]. Also, public cloud may be free.

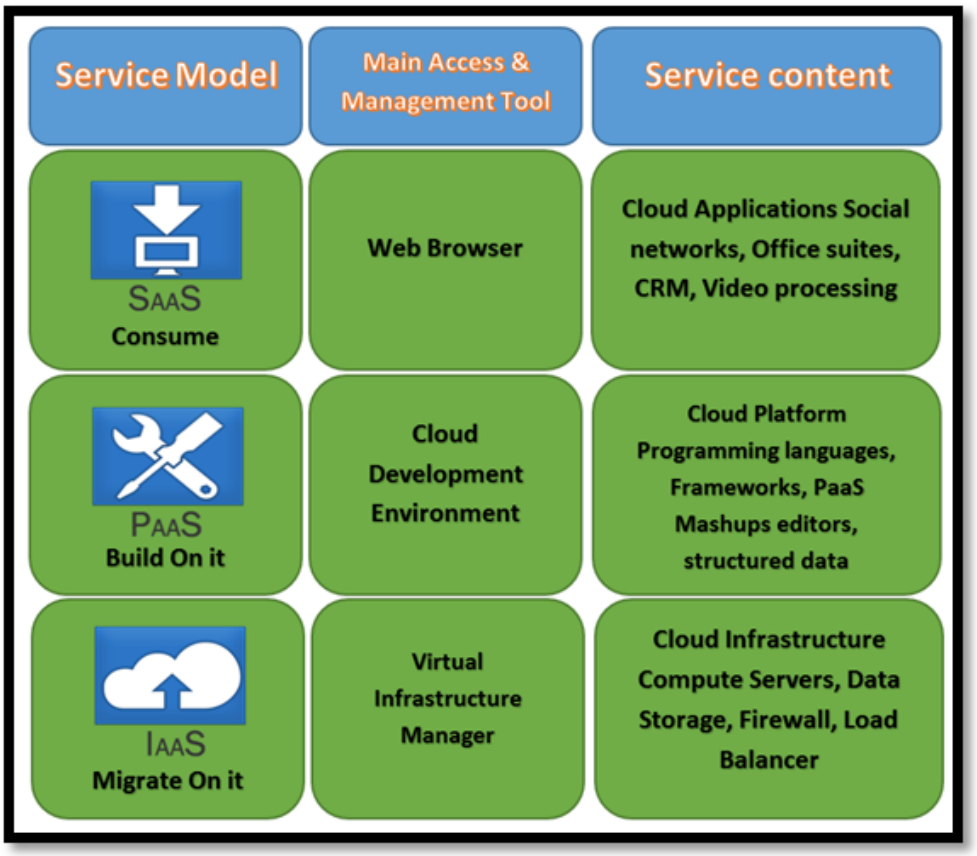


Figure 2: Cloud-computing stack [17]

2) Private cloud: The cloud infrastructure is provisioned for exclusive use by a single organization serving multiple consumers (e.g., business units). The organization itself or a third party, or some combination of them may manage the Private cloud, and it may be hosted on or off premises [3].

3) Community cloud: A specific community of organizations that have common concerns (e.g., mission, security requirements, policy, jurisdiction, and compliance considerations) provisions the cloud infrastructure for exclusive use. One or more of the organizations in the community may own, manage, and operate this model, or get a third party to perform these tasks, or some combination of both, and it may exist on or off premises [3].

4) Hybrid cloud: The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that keep unique entities, though the clouds are bounded together offering the benefits of multiple deployment models (e.g., cloud bursting for load balancing between clouds) [3, 4].

5) To sum up, Cloud Computing has five key characteristics (on-demand self-service; broad network access; resource pooling; rapid elasticity; and measured service), three delivery models (SaaS -

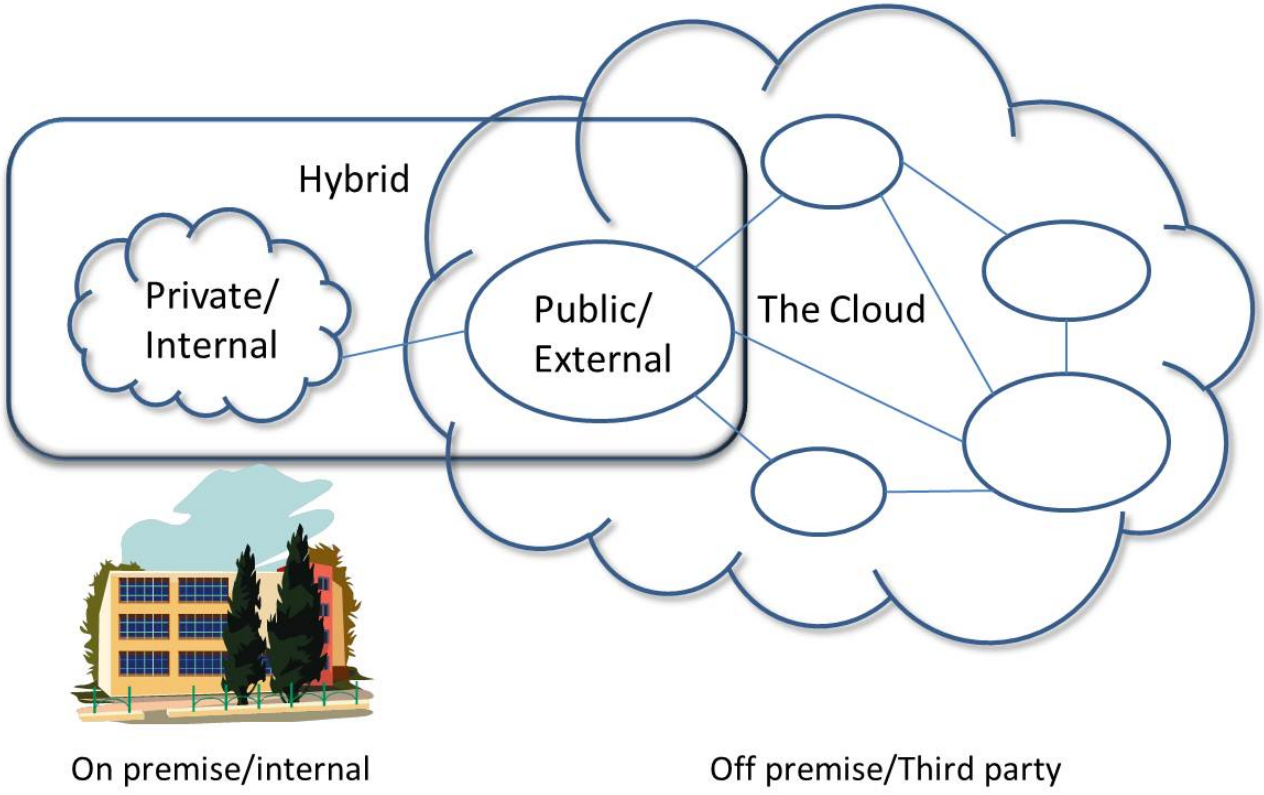


Figure 3: Cloud computing deployment types [16]

software as a service, PaaS - platform as a service, IaaS - infrastructure as a service), and four deployment models (private, community, public, hybrid) [9] (See Figure 4).

## 2.2 GIS in Business

GIS is an integrated collection of computer software and data used to view and manage information about geographic places, analyze spatial relationships, and model spatial processes. A GIS provides a framework for gathering and organizing spatial data and related information so that it can be displayed and analyzed [8]. Furthermore, GIS enables the geographic mapping of information such as the locations of customers, competitors, suppliers, sales prospects, suppliers, and partners. GIS can be used for site selection, trade area analysis, environmental analysis, sales territory design, and the targeting of marketing [11].

The current market has huge amount of data. This data could be sales, inventory, retail, real estate, insurance, or any other kind of information. Most of this business data is spatial data-that identifies the geographic location of features and boundaries on Earth -. Therefore, business today depends on GIS to analyze this data spatially. Business GIS and mapping have evolved into a formidable tool by which corporate world can use spatial information to manage their business [6]. GIS is customized to the business requirements, can improve the productivity of the business. Especially for companies trying

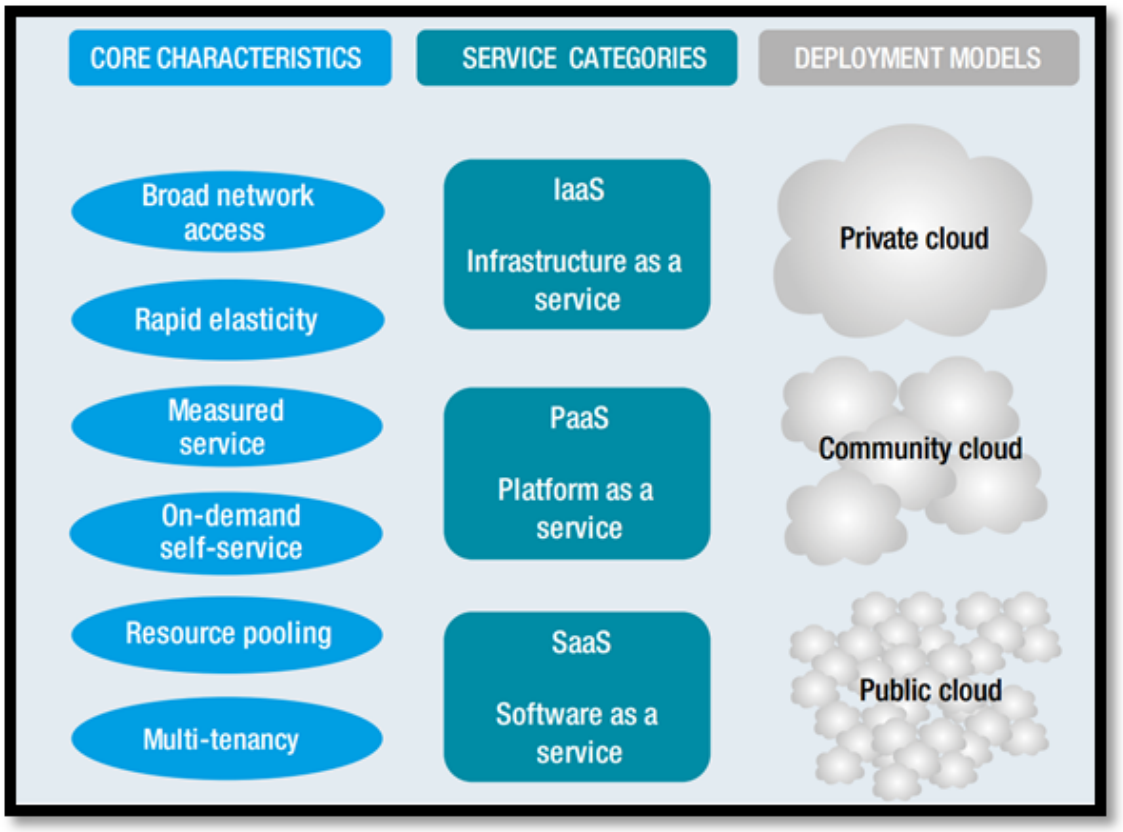


Figure 4: Characteristics and types of cloud computing

to identify uncovered markets, GIS would efficiently assist in identification of new customers, optimize media campaigns, cutting costs, finding new retail distribution centers, aligning sales territories to utilize the sales force efficiently and monitoring business trends and performance spatially [10].

GIS includes a variety of advanced features in information processing, and its basic functionality is data collection, management, processing, analysis and output. Relying on these basic functions, GIS implements a variety of applications using spatial analysis, modeling, network technology, database and data integration technology, and further development environment to meet the broad needs of users.

The emergence of cloud computing brings a new solution to massive data storage, data processing, spatial analysis. Thanks to cloud computing, the needed massive data can be scheduled and processed in parallel entirely within the cloud instead of being transferred on the network.

## 3 Methodology

In order to perform our overview of GIS and private cloud, a descriptive study was adopted by performing a systematic literature reviews that based on a structured search process. The key words "GIS" and "private cloud" were used and the search was limited to ABI/INFORM database Computer Science Index - ProQuest computing, Applied Science & Technology Source - EBSCO, and Google scholar.

Papers resulting from this search were investigated carefully to understand the current research areas between GIS and private cloud. Next, the results, derived from our understanding, were discussed leading to number of research questions.

Just four papers that form our search results that focus on both GIS and "Private Cloud". These papers were published as follow: one paper in 2012, two papers in 2014, and one paper in 2015.

# 4 Results

Jun Chen et al. [7], discussed the internal private cloud framework and the design of distributed file system under the LAN environment. Then they analyzed how to store image pyramids for raster data in the distributed file system, and then proposed the Map/Reduce technology based on G/S mode (G: geological data browser or grid browser, S: spatial information server), to achieve load-balancing strategy for data download. This paper concentrated on the storage and the display of GIS raster data in the framework of the private cloud. At the end of this study, they concluded that when data nodes -in the private cloud- increase, the raster data download speeds continue to increase, until the flow limit of the client network card. With this, they have proved the significance of private cloud store and display raster data [7].

Ekkarat Boonchieng et al. [5] used GIS and Private Cloud to develop a smart phones software named "SaraphiHealth" to collect medical data about the residents of a certain district in Thailand. They used the PaaS service model of cloud computing by using the open source software "OpenNode" to build their private cloud. Then they developed their own software to collect the medical data. The focus in this search was to collect medical data of residents from a developed software for both Android and iOS platforms or from a web-based application, then generate different types of reports (tables, figures and maps). Their work emphasized on the ability to benefit from integrating GIS with "Private Cloud" to add value to the business. That benefit was proven through the report generated from the system that had a major benefit directly to the Saraphi District Hospital. Healthcare providers were able to use the basic health data to provide a specific home healthcare service and to create health promotion activities according to medical needs of the people in community [5].

In 2014, Fifth International Conference on Computing for Geospatial Research and Application, Sang-Yong Kang and Young-Hoon Lee used GIS and "private Cloud" with expert system software, and Open Geospatial Consortium (OGC) [13] software technology to support Civil Engineering design process. They used the SaaS cloud service model to develop their system by uploading the software using to a private cloud. They claimed that they developed the first harmonized application service platform in mixing civil engineering and cloud computing area. Their system was called CEDP (Civil Engineering Design support SaaS cloud Platform). The developed system collected a real-time field survey data then sent it to the remote Geo-cloud platform. The Expert software analyzed the collected data to draw the Civil Engineering survey line automatically in the CEDP platform. After that the basic design drawings were drawn. The GIS map receives the result immediately. Therefore, the future view of the civil construction product can be viewed within a day [12].

Dejian Zhang et al. developed a prototype web-based decision support for watershed management (DSS-WMRJ) [18] (See Figure 5).

DSS-WMRJ was based integration between Geoserver as a web-GIS tool, SWAT- Soil and Water Assessment Tool- as a modelling component, and a private cloud adopting Hadoop [1]. The system was organized in four tiers: the presentation tier, the proxy tier, the application tier, and the database and model tier as in Figure 6.

Then, they generated a scenario that took about 111 minutes to finish in the series processing and tested the developed system with that scenario. The developed system performed that scenario in about 5 minutes. Considering that, their private cloud consists of eight TaskTracker and each TaskTracker

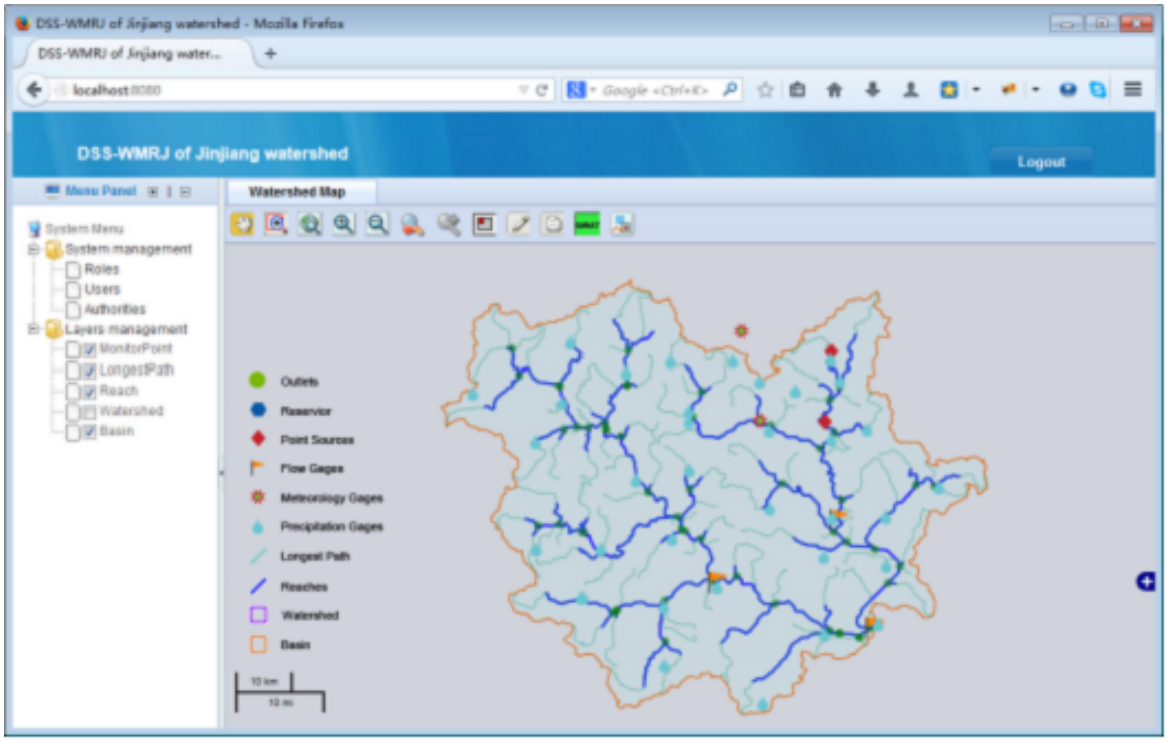


Figure 5: Main interface of DSS-WMRJ

was allowed to perform four tasks simultaneously. From these results, they concluded that the lowest simulation time that could be achieved is about 2.14 minutes by using 23 TaskTrackers (See Figure 7).

They performed another test on their system by comparing it with a widely used SWAT (Soil Water Assessment Tool) auto-calibration tool (SWAT-CUP) [15], which operates on a PC. SWAT-CUP took 97.9 min to finish 92 simulations, while their system only took 4.4 min when running on eight TaskTrackers.

Therefore, they proved the significant of integrating private cloud capabilities to GIS software as their proposed model simulation service substantially reduced the execution time by parallelizing the model simulations.

## 5 Conclusion

Due to the importance and spread of GIS systems and the new emerging of cloud computing, this research investigated the studies that had been performed in benefitting from cloud computing (private cloud) capabilities to leverage the performance of GIS systems especially the systems that manipulate raster data. A descriptive study was conducted to review the literature in GIS and private cloud. Using ABI/INFORM database Computer Science Index -ProQuest computing, Applied Science & Technology Source -EBSCO, and Google scholar search engine a search was conducted, and there were only four studies found. A main discover from this study is that the integration between GIS and raster models of GIS is in its earlier stage. All studies performed used the PaaS service model of the cloud computing

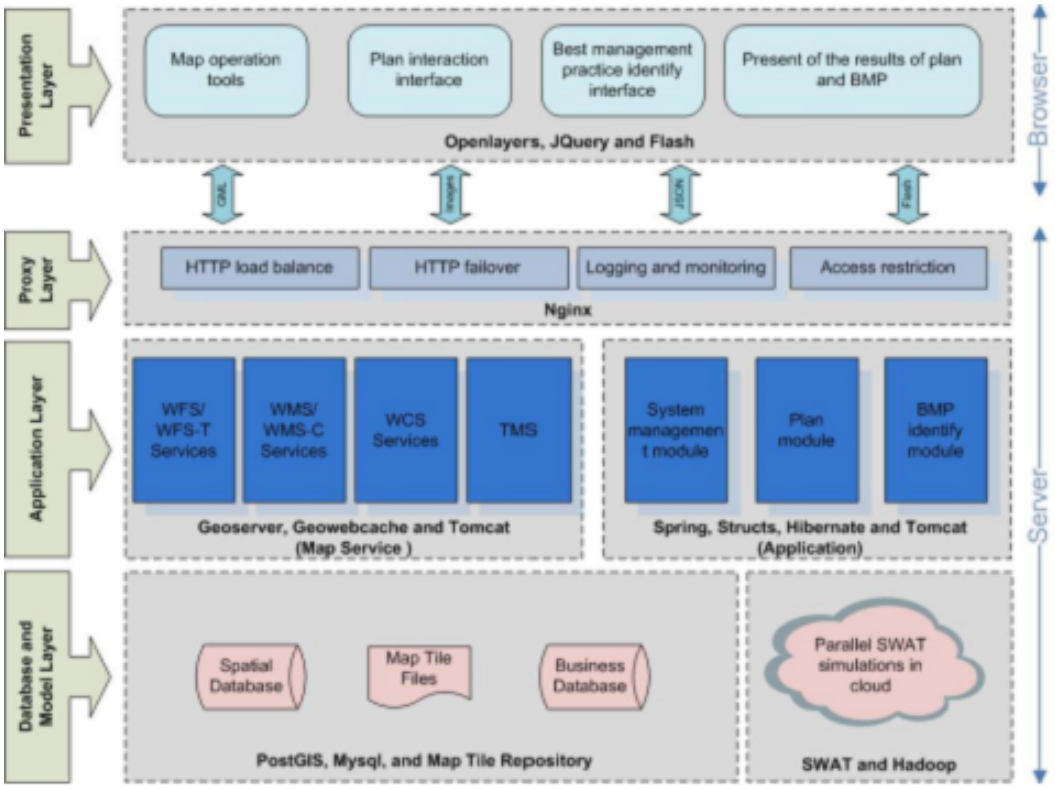


Figure 6: The system architecture of decision support system for watershed management (DSS-WMRJ)

service models and offered their software to their customers. Only one study claimed to develop the first CEDP SaaS service model of the cloud computing that relates to the use of GIS in the area of Civil Engineering.

## References

[1] Apache Hadoop, *What Is Apache Hadoop?*, Oct. 5, 2017. (`https://hadoop.apache.org/`)

[2] M. Armbrust, A. Fox, R. Griffith, Anthony D. Joseph, R. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica and M. Zaharia, *Above the Clouds: A Berkeley View of Cloud Computing*, UC Berkeley Reliable Adaptive Distributed Systems Laboratory, 2009.

[3] L. Badger, T. Grace, R. VoasPatt-Corner and J. Voas, *Cloud Computing Synopsis and Recommendations*, National Institute of Standards and Technology, Gaithersburg, 2012.

[4] T. Bittman, *Mind the Gap: Here Comes Hybrid Cloud*, Sep. 24, 2012. (`http://blogs.gartner.com/thomas_bittman/2012/09/24/mind-the-gap-here-comes-hybrid-cloud/`)

[5] E. Boonchieng, W. Boonchieng, W. Senaratana and J. Singkaew, "Development of mHealth for public health information collection, with GIS, using private cloud: A case study of Saraphi district, in *International Conference on Computer Science and Engineering Conference*, Chiang Mai, Thailand, 2014.

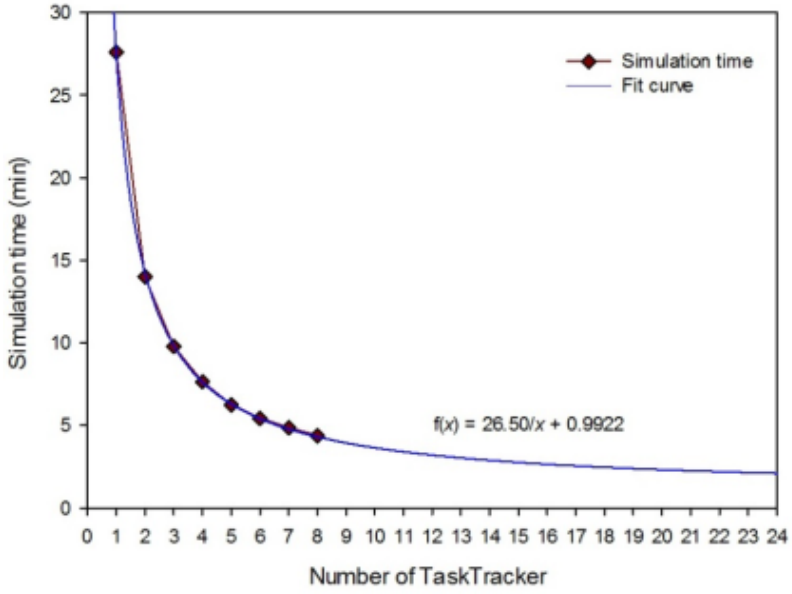


Figure 7: The performance of the model simulation service

[6] T. R. Carr, "Geographic information systems in the public sector," in *Geographic Information Systems in the Public Sector*, pp. 252–270, Hershey, PA, USA, IGI Global, 2003.
[7] J. Chen, H. Wang and H. Lu, "Research for GIS raster data storage and display under the frame-Work of private cloud," in *International Conference on Computer Science and Electronics Engineering*, 2012.
[8] ESRI, *What is GIS*, 14 Oct. 2015. (`http://www.esri.com/what-is-gis`)
[9] I. Foster, Y. Zhao, I. Raicu and S. Lu, "Cloud computing and grid computing 360-degree compared," in *Grid Computing Environments Workshop*, 2008.
[10] R. R. Harmon, "Marketing Information Systems," *Encyclopedia of Information Systems*, vol. 3, pp. 137–151, 2003.
[11] A. A. Ismael and S. Bashir, "Applications of GIS in business decision making: The case of Egypt," *International Journal of Computer Applications*, vol. 94, no. 14, pp. 31–36, May 2014.
[12] S. Y. Kang and Y. H. Lee, "The implementation of geo-cloud SaaS system for supporting the civil engineering design using BRMS open software," in *Proceedings of the 2014 Fifth International Conference on Computing for Geospatial Research and Application*, 2014.
[13] OGC, *Open Geospatial Consortium*, 15 Oct. 2015. (`http://www.opengeospatial.org/`)
[14] M. Peter and G. Timothy, *The NIST Definition of Cloud*, National Institute of Standards and Technology, Washington DC, 2011.
[15] SWAT, *SWAT-CUP 5.1.6.2*, Dec. 2016. (`http://swat.tamu.edu/software/swat-cup/`)
[16] Synergygs, *We Bring People and Technology Together*, Oct. 27, 2017. (`http://www.synergygs.com/Solutions/CloudServices/`)
[17] W. Voorsluys, J. Broberg and R. Buyya, "Layers and types of clouds," in *Cloud Computing: Principles and Paradigms*, NJ, John Wiley & Sons, Inc. 2011.
[18] D. Zhang, C. Xingwei and Y. Huaxia, *Development of a Prototype Web-Based Decision Support System for Watershed Management*, Water, pp. 780–793, 2015.

## Biography

**Salah E. Elgazzar** graduated from Faculty of Computer and Information Sciences, Mansoura University, Mansoura, Egypt in 2001. Salah received his master degree in 2012 in Information Systems from the same. His main research interests are in the areas of GIS, Cloud Computing, Databases, and Information Systems.

**Ahmed A. Saleh** is a full professor in information systems department, Mansoura University. EYGPT. He is the Vice Dean for Graduate Studies and Research. His current research interests are GIS, business intelligence, digital image processing, and pattern recognition.

**Hazem El-Bakry** (Mansoura, EGYPT 20-9-1970) received B.Sc. degree in Electronics Engineering, and M.Sc. in Electrical Communication Engineering from the Faculty of Engineering, Mansoura University - Egypt, in 1992 and 1995 respectively. Dr. El-Bakry received Ph. D degree from University of Aizu-Japan in 2007. Currently, he is associate professor at the Faculty of Computer Science and Information Systems - Mansoura University-Egypt. His research interests include neural networks, pattern recognition, image processing, biometrics, cooperative intelligent systems and electronic circuits. In these areas, he has published many papers in major international journals and refereed international conferences. According to academic measurements, now the total number of citations for his publications is 2997. The H-index of his publications is 28. Dr. El-Bakry has the United States Patent No. 20060098887, 2006. Furthermore, he is associate editor and referee for some major journals. Moreover, he has been awarded the Japanese Computer and Communication prize in April 2006 and the best paper prize in two conferences cited by ACM. Dr. El-Bakry has been selected in who Asia 2006 and BIC 100 educators in Africa 2008.

# Common Private Exponent Attack on Multi Prime RSA

Santosh Kumar Ravva
*(Corresponding author: Santosh Kumar Ravva)*

Department of IT, MVGR College of Engineering
Vijayaram Nagar campus, Chintalavalasa, Vizianagaram, Andhra Pradesh 535005, India
(Email: santosh@mvgrce.edu.in)
*(Received Aug, 5, 2017; revised and accepted Oct. 10, 2017)*

**Abstract**

Multiprime RSA is a variant of RSA, where the modulus is the product of three or more prime numbers. In this paper, we attack Multiprime RSA. Our attack assumes that many instances of Multiprime RSA all use different moduli, but somehow all use the same secret exponent. Our attack generalizes the existing attack on RSA by Hinek. We use lattice reduction techniques to recover the bound for secret exponent.

*Keywords: Lattices; Lattice Reduction; Multiprime RSA*

## 1 Introduction

### 1.1 Multiprime RSA

RSA cryptosystem [1–8, 11, 13, 15–17] is most popular cryptosystem from its invention Multi Prime RSA: Multi Prime RSA is a simple extension of RSA in which the modulus is the product of $r$ distinct primes. In this paper, we consider only balanced primes. If we arrange the primes in increasing order, $p_i < p_{(i+1)}$ for $i = 1, 2, \cdots, r$, then we assume that $4 < 1/2N^{(1/r)} < p_1 < N^{(1/r)} < p_r < 2N^{(1/r)}$. The key generation algorithm is same as the key generation algorithm for RSA except here we require $r$ distinct primes. As usual, the public and private key are defines as $ed \equiv 1(\mathrm{mod}\,\phi(N))$, where $k$ is some positive integer. As in RSA, one can replace $\phi(N)$ with $N - s$. Expanding $\phi(N)$, it follows that $s$ can be written as

$$\begin{aligned} s &= N - \phi(N) \\ &= N - \prod_{(i=1)}^{r} (p_i - 1) \\ &= \sum_{(i=1)}^{r} \frac{N}{p_i} - \sum_{(i,j=1)}^{r} \frac{N}{(p_i p_j)} + \sum_{(i,j,k=1)}^{r} \frac{N}{(p_i p_j p_k)} + \cdots + (-1)^r. \end{aligned}$$

The above expression of $s$ combined with the condition for balanced primes, an upper bound on $s$ is given by $|s| < (2r-1)N^{(1-1/r)}$.

Thus, there are $(r-1)/r$ most significant bits are common in the $\phi(N)$ and $N$, so $N$ is a good approximation for $\phi(N)$.

### 1.2 Comparison Between RSA and Multiprime RSA

The encryption algorithm for multiprime RSA is same as the encryption algorithm for RSA. Given plain text message $m$, the cipher text is calculated by $c = m^e \bmod N$. The decryption for multi prime RSA is same as the decryption for RSA, if one consider the standard decryption. If decryption uses Chinese remaindering theorem, the decryption algorithm for the multi prime RSA is the obvious extension to the decryption algorithm for CRT-RSA. The efficiency of multi prime RSA depends on two issues. First one is, the complexity of generating the $r$ distinct primes is lower than the generating two distinct primes for the original RSA. The second one is, if Chinese remaindering is used for the decryption, then the decryption costs are lower than the decryption costs for CRT-RSA.

### 1.3 Breaking Multiprime RSA

If the factorization of modulus is known, then one can break the modulus. In RSA, it is sufficient to recover the private exponent or to compute $\phi(N)$ since there are polynomial time algorithms that can factor the modulus given either of these. But there is a different issue for the multi prime RSA. There are no polynomial time algorithms that can factor the modulus given the private exponent or $\phi(N)$. But if we know the multiple of $\phi(N)$, the results of Miller can be used to probabilistically factor the modulus. Also from $ed \equiv 1 \bmod (\phi(N))$, knowing $d$ is sufficient to obtain the private exponent in order to (probabilistically) factor the modulus.

In this paper, we attack on the Multi prime RSA, if multi prime RSA is used in broadcast scenario. That is, the same message broadcasts to several people with same private exponent but different moduli. Rest of the paper is organized as follows. In Section 2, we introduce some mathematical preliminaries, In Section 3, we sketch the attack with justification. In Section 4, we provide some experimental results.

## 2 Terminology

### 2.1 Lattices

Let $B = \{b_1, b_2, \cdots, b_n\}$ be set of n linearly independent vectors in $R^m$. The lattice generated by $B$ is the set $L(B) = \{\sum_{(i=1)}^{n} x_i \overrightarrow{b_i} : x_i \in Z\}$. That is, the set of all integer linear combinations of the basis vectors. The set $B$ is called basis and we can compactly represent it as an $m \times n$ matrix each column of whose is a basis vector: $B = [b_1, b_2, \cdots, b_n]$. The rank of the lattice is defined as $rank(L) = n$ while its dimension is defined as $dim(L) = m$. The volume (determinant) of a lattice denoted by $vol(L)$, is the $n$ dimensional volume of the parallelepiped spanned by any of it bases. For full dimensional lattice $vol(L) = |det(B)|$. Since lattice is discrete, there exists a smallest vector. The necessary condition for a vector $v$ to be a smallest vector in the lattice is $||v|| \leq \sqrt{n} vol(L)^{\frac{1}{n}}$, which is called Minkoswki's bound. This bound is useful as it allows for constructing the bounds on certain attacks. For good introduction of lattices and their applications refer [12, 14].

Finding the shortest vector in the lattice is a hard problem. There are some approximation algorithms to find a shortest vector in the lattice. Here we use the LLL algorithm, because it is well suited in the most of the attacks in practice.

## 2.2 Lattice Reduction

Lattice reduction is a problem to find the reduced basis of the given lattice. Reduced basis is the basis of the lattice such that the vectors are near orthogonal. So many versions exist to find reduced basis, but the one given by Lenstra, Lovasz, Lovasz is a special one, called LLL reduced. Because there exist a polynomial time algorithm for this reduction called LLL algorithm. This problem is not only solving the reduced problem, it also gives solution to the shortest vector problem in some extent.

**Definition 1** (LLL Reduced)**.** *Let $b_1, b_2, \cdots, b_n$ be a basis for a lattice and let $b_1^*, b_2^*, \cdots, b_n^*$ be its Gram-Schimdt orthogonalization. The basis $b_1, b_2, \cdots, b_n$ is said to be Lovaász-reduced or LLL-reduced, if the Gram-Schimdt coefficients satisfy $|\mu_{(i,j)}| \leq 1/2$ for $1 \leq j < i \leq n$, and $||b_i^* + \mu_{(i,i-1)} b_i^*||^2 \geq \frac{3}{4}||b_{(i-1)}^*||^2$ for $1 < i \leq n$, or equivalently $||b_i^*||^2 \geq (\frac{3}{4} - \mu_{(i,i-1)}^2)||b_{(i-1)}^*||^2$ for $1 < i \leq n$.*

A useful property of LLL reduced basis is that the bound for each vector depends on only the dimension and the volume. The property stated as in [14]. Let $L$ be a lattice spanned by linearly independent vectors $b_1, b_2, \cdots, b_n$, where $b_1, b_2, \cdots, b_n \in R^n$. By $b_1^*, b_2^*, \cdots, b_n^*$, we denote the vectors obtained by applying the Gram-Schimdt process to the vectors $b_1, b_2, \cdots, b_n$. It is known that given basis $b_1, b_2, \cdots, b_n$ of lattice $L$, LLL reduced find a new basis $b_1, b_2, \cdots, b_n$ of $L$ with the following properties:

$$\begin{aligned} ||b_i^*||^2 &\leq 2||b_{(i+1)}^*||^2; \\ ||b_1|| &\leq 2^{(n/2)} det(L)^{(1/n)}; \\ ||b_2|| &\leq 2^{(n/2)} det(L)^{(1/(n-1))}. \end{aligned}$$

The determinant of is defined as $det(L) = \prod_{(i=1)}^{w} ||b_i^*||$, where $||$ denotes the Euclidean norm on vectors. The LLL algorithm is the first algorithm to compute LLL reduced basis efficiently. For given a m dimensional lattice with n dimensional lattice vectors the LLL algorithm has run time $o(nm^5B^3)$, where $B$ is the bound on the bit length of the input basis vectors.

## 2.3 Existing Attacks on Multiprime RSA

The most of the attacks on RSA can be generalized into Multi prime RSA. The first attack is the Wiener attack, stated in [9].

**Attack 1:** Let $N$ be an r-prime modulus with balanced primes, let $e$ be a valid public exponent and $d$ be its corresponding private exponent. Given the public key $(N, e)$, if the private exponent satisfies $d \leq \frac{N^{(1/r)}}{(2k(2r-1))}$, then the modulus can be (probabilistically) factored in time polynomial in $\log N$ for every $r \geq 2$.

The second attack is generalization Boneh-Durfee attack on RSA.

**Attack 2:** For every $\epsilon > 0$ and integer $r \geq 2$ there exists an $n_0$ such that, for every $n > n_0$, the following holds: Let $N$ be an $n$-bit $r$-prime RSA modulus with balanced primes, let $e = N^\alpha$ be a valid public exponent and let $d = N^\delta$ be its corresponding private exponent. Given the public key $(N, e)$, if the private exponent satisfies $\delta \leq \frac{1}{3r}(4r - 1 - 2\sqrt{(r-1)(r-1+3\alpha r)}) - \epsilon$, then the modulus can be (probabilistically) factored in time polynomial in n under some assumption. The above attacks are for the single instance of Multiprime RSA. There are some attacks on Multiprime RSA by considering the several instances of the same message. For example, common modulus attacks, in which same message send to the different people with the same modulus. The encryption and decryption exponents may be different. The second type is common private exponent attack, in which same message send to the different people with the same private exponent but may be

different moduli and different public exponents, called common private exponent attack. In this paper, we consider the common private exponent attack on Multiprime RSA. The attack exists in the case of RSA and it is stated in [10]. We mention the same here.

**Attack 3:** For any integer $r \geq 1$, let $N_1, N_2, \cdots, N_r$ be balanced RSA moduli satisfying $N_1 < N_2 < \cdots < N_r < 2N_1$. Let $(e, N_1), \cdots, (e, N_r)$ be valid public RSA keys each with the same private exponent $d < N_r^{\delta_r}$. If $\delta_r < \frac{1}{2} - \frac{1}{2(r+1)} - \log_{N_r}(6)$, then all of the moduli can be factored in time polynomial in $\log(N_r)$ and $r$, under the some assumption. For the justification of above attack please refer [10]. In the next section, we introduce the attack on Multi prime RSA and its proof.

# 3 Attack on Multiprime RSA

## 3.1 Attack

For any integer $n \geq 1$, let $N_1, N_2, \cdots, N_n$ be balanced Multi prime RSA with $r$ primes $N_1 < N_2 < N_3 < \cdots < N_n < 2N_1$. Let $(e_1, N_1), \cdots, (e_n, N_n)$ be valid Multi prime RSA public keys each with the same private exponent $d < N_n^{\delta_n}$. If $\delta_n < \frac{n}{r(n+1)} - \log_{N_n}(4r-2)$, then all of the moduli can be factored in time polynomial in $log(N_n)$ and $n$.

## 3.2 Justification

Let $M = \lfloor N_n^{1-1/r} \rfloor$. Given the $n$ public keys $(e_1, N_1), \cdots, (e_n, N_n)$ and $d$ is a secret exponent for all instances. We begin by considering the $n$ key equations, $e_i d = 1 + k_i(N_i - s_i)$ along with the trivial equation $dM = dM$, written as

$$\begin{aligned} dM &= dM \\ e_1 d - N_1 k_2 &= 1 - k_1 s_1 \\ e_2 d - N_2 k_2 &= 1 - k_2 s_2 \\ \vdots &\ \cdots\ \vdots \\ e_n d - N_n k_n &= 1 - k_n s_n. \end{aligned}$$

The above system of equations can be written as $x_n B_n = v_n$, where $x_n = (d, k_1, k_2, \cdots, k_n)$ and

$$B_n = \begin{bmatrix} M & e_1 & e_2 & \cdots & e_n \\ 0 & -N_1 & 0 & \cdots & 0 \\ 0 & 0 & -N_2 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & -N_n \end{bmatrix}$$

$$v_n = (dM, 1 - k_1 s_1, \cdots, 1 - k_n s_n).$$

The vector $v_r$ is an integer linear combination of the rows in the matrix $B_n$ and hence is a vector in the lattice $L$ generated by the rows in $B_n$. Since $N_i \leq N_r < 2N_1$, $k_i < d < N_n^{\delta_n}$ and $|s_i| < (2r-1)N^{1-1/r}$ for each $i = 1, 2, \cdots, n$, so the vector $v_r$ satisfies $||v_r|| < \sqrt{1 + n(2r-1)^2} N_n^{\delta_n + 1 - 1/r}$ Since

$$\begin{aligned} ||v_r||^2 &= (dM)^2 + (1 - k_1 s_1)^2 + \cdots + (1 - k_n s_n)^2 \\ &\leq (N_n^{\delta_n + 1 - 1/r})^2 + (1 - N_n^{\delta_n + 1 - 1/r}(2r-1))^2 + \cdots + (1 - N_n^{\delta_n + 1 - 1/r}(2r-1))^2 \\ &= (N_n^{\delta_n + 1 - 1/r})^2 + n(1 - N_n^{\delta_n + 1 - 1/r}(2r-1))^2 (1 + (2r-1)^2 n)(N_n^{\delta_n + 1 - 1/r})^2 \end{aligned}$$

So we have $||v_r|| < \sqrt{(1+(2r-1)^2 n)}(N_n^{\delta_n+1-1/r})$, and that the volume of the lattice $L$, given by $vol(L) = |det(B_n)|$, satisfies $vol(L) = |M\prod_{i=1}^{n}(-N_i)| = \lfloor N_n^{1-1/r} \rfloor \prod_{(} i = 1)^n N_i > (N_n/2)^{(n+1-1/r)}$. From Minkowski's bound, a necessary condition for the vector $v_r$ to be a smallest vector in $L$ is given by $||v_r|| < \sqrt{(n+1)}vol(L)^{1/(n+1)}$. Using the bounds on the norm of the vector and the volume of the lattice, a sufficient condition to hold is given by

$$\sqrt{(1+(2r-1)^2 n)}(N_n^{\delta_n+1-1/r}) < \sqrt{(n+1)}(\frac{N_n}{2})^{\frac{(n+1-1/r)}{n+1}}.$$

This implies, we have

$$N_n^{\delta_n+1-1/r} < c_r(N_n/2)^{(n+1-1/r)/(n+1)}$$

where

$$c_r = \sqrt{(n+1)/(1+(2r-1)^2 n)}\frac{1}{2^{\frac{n+1-1/r}{n+1}}} > (\frac{1}{2r-1})(\frac{1}{2}).$$

Compare both sides, we get $\delta_n + 1 - \frac{1}{r} < \frac{n+1-1/r}{n+1} - log_{N_r}(4r-2)$. After simplification, we get $\delta_n < \frac{n}{r(n+1)} - log_{N_n}(4r-2)$. When $r = 2$, the bound equals the bound in paper [10]. So when the secret exponent is smaller than $\delta_n$ the vector $v_n$ has satisfied the Minkowski condition, be a smallest vector in $L$. Once the vector $v_r$ is obtained we can easily factor all the moduli. From the vector $v_r$, one knows the secret exponent $d$, in turn one can compute all $k_i$'s by using the key equations $k_i = (e_i d - (1 - k_i s_i))/N_i$. From $k_i$ and $d$, one can compute $\phi(N_i) = ((e_i d - 1))/k_i$. But unfortunately, there are no deterministic algorithm to compute $N$ from $\phi(N)$, if $N$ is a product of three or more numbers. But there is probabilistic algorithm exists (MILLER-RABIN) to compute $N$ from multiplies of $\phi(N)$.

### 3.3 Experiment

We experiment the above attack for three instances. Nowadays, the RSA modulus is 1024 bits. We have used SAGE [18] for doing all these calculations. SAGE is freely available library. Three prime numbers for first instance:

678224911547330147986093478199894602593795041304121
356008546789157286634233311790115626404827023528453

708474419409040323979429386144644006183852481685383 4
157533954737018090407412508042238507192729488148447

828346832316245278301181800872378365263256994356978 7
508593486612416664768064854308634917469458300641893

The modulus for first instance:

398024795024305840124369861539672861111929755976852 0
695572645927280948679742221358560108539147387672145

574643409748972694085815527592515664472066189903103 1
522690868149669416945173654237687392100009851224373

19541190560655827101547807228059049070711486816874756733628515821129274795766950122704822438920471354633

Three prime numbers for second instance:

71120169507825139393011721508380795392301356799993404329308829287965322187893848856635244767431974369394565359706261800235586539334646285991321427933608889275210263010247136380569841822416543375070004144969

831615330978053369821654235749067344253850420322046198145556589073651698625683011146540568528100707475998145556589073651698625683011146540568528100707475 9

The modulus for second instance:

27001648007623835482389897920964481234532039596767564213705847103070691433360873238346650547680848576726636901769349674889016838942316143898411650895896357722682461314710330128572111448604468952040247034828

589030309100752044066927082988483345824214157060099793449174827350127577530136537328977377886600084126993417482735012757753013653732897737788660008412699

Three prime numbers for third instance:

76730163938348479418436407046786527818633593896607373194425715528473638194881751524097124372630554682975379377625980756674993647185666423139370139650686519661326651087495523193337905537175550892781423101475395342771000978217135825503436485980920045858078257716039638576857698703568752771925132861090440121039

The modulus for third instance:

22263884435801899802674759303805697118713636041607865050241467520224236994613949002378961803652819286865268402008312979469194065931803571405154678409393428008287143020782113965268621088147936991953030971885345586049749710343725079072259921947094667298031310268129091213627461107186143417969409326052521570199211407462652061593242990053988875085597119382340151922114074626520615932429900539888750855971193823401519211407462652061593242990053988875085597119382340151921140746265206159324299005398887508559711938234015

3105007419987038334725462998580666261416020578531 63

5308109008933276203679728495107812325549485871417366
9303492310857231139594433868938634043144459068982 91

2119793582905597408376302854193204396705586325089051
5172176815644818293351350176858042929175335888246598

2883389358246566502277619747972818488039725499948416
8424329817143275109089960954166997075208366701088 68

9304160319616246259106477604741756147202782693272850
2990669900313407789582291247443002991333846832628 67

9214326962234346157232636108621562614756258379734978
8995398374738646556691575593272639249325630981537 63

0717332367652942964470071103121685572068347403827092
6642579369967114661791898215918972554266588263846 06

6663987418662932813667046547312332170293695173445553
8817764161319041341966649291837448413131907014696 3

The first value in the first row is

2309542821222233650603721891697875739820443719904888
6616394269835061822150861033880299792988103869722 33

4054274505558853052439730156818794631040078649621592708 45
1671327366552059289826564670952931069623218348216863948 8

The required private exponent is 1.54783815979006e61 Actually this is the secret exponent, we have used in the beginning of the attack. We retrieved by using LLL algorithm. The attack uses the prime numbers of the length 1024 bits with $r = 3, 4$. If the instances are more, then one can easily break the system.

## 3.4 Practical Effectiveness

The above attack is only heuristic; the original value lies in the practice. Already we showed the successful attack as toy example. We checked the random instances of Multi prime RSA with 1024 bits moduli when a common private exponent is shared among different moduli in the range $2 \leq n \leq 10$ and $r = 3, 4$. We use the SAGE Library for experimentation. We observe that, if more instances are available, then one can easily break the system for for the values of $r = 3, 4$. We use LLL algorithm from above library. The complexity of the attack is dominated by the LLL algorithm. The complexity of the LLL algorithm is a polynomial time algorithm in size of the lattice and the exponential in size of the entries in the lattice. Most of the times, we retrieved the actual value, but some times we get the nearer value to the actual value. We have done some experiments for the size of the modulus 2048 also.

# 4 Conclusion

We showed that Lattice methods can recover the secret exponent in a certain kind of "Multi prime RSA" setting. Our attack assumes that many instances of RSA all use different multi-prime moduli, but somehow all use same secret exponent. In this scenario, we investigate about the smallness of the secret exponent. If it is less than the above bound, then one can break the system. We also observe that if the number of instances is increasing, then the breaking the system becomes easy. We use LLL algorithm to attack this system. LLL algorithm has so many applications in the fields like cryptology, Communications and Number theory.

# References


[1] K. Banarjee, S. N. Mandal, S. K. Das, "Improved trail division technique for primality checking in RSA algorithm," *International Journal of Computer Network and Information Security*, vol. 5, no. 9, July 2013.

[2] D. Boneh, "Twenty years of attacks on the RSA cryptosystem," *Notices of the American Mathematical Society*, vol. 46, no. 2, pp. 203-213, 1999.

[3] D. Boneh, G. Durfee, "Cryptanalysis of RSA with private key d less than N0:292," in *Advances in Cryptology (Eurocrypt'99)*, Lecture Notes in Computer Science 1952, pp. 1-11, 1999.

[4] D. Coppersmith, "Finding a small root of a bivaraite integer equation: Factoring with high Bits Known," in *Lecture Notes in Computer Science*, vol. 1070, pp. 178-189, Springer, 1996.

[5] M. Ernst, E. Jochemsz, A. May, B. de Weger, "Partial key exposure attacks on RSA up to full size exponents," in *Advanced in Cryptology (EUROCRYPT'05)*, pp. 1-11, 2000.

[6] H. Graham, "Finding small roots of univariate modular equations revisited," in *Lecture Notes in Computer Science*, vol. 1355, pp. 131-142, Springer, 1997.

[7] J. Hastad, "Solving simultaneous modular equations of low degree," *SIAM Journal of Computing*, vol. 17, no. 2, pp. 336-341, Apr. 1988.

[8] M. Hermann and A. May, "Solving linear equations modulo divisors:on factoring given any bits," in *Lecture Notes in Computer Science*, pp. 406-424, 2008.

[9] M. J. Hinek, "On the security of multi-prime RSA," *Journal of Mathematical Cryptology*, vol. 2, no. 2, pp. 117-147, July 2008.

[10] M. J. Hinek, *Small Private Exponent Partial Key-Exposure Attacks On Multi Prime RSA*, Centre for Applied Cryptographic Research, University of Waterloo, 2004.

[11] E. Jochemsz, A. May, "A strategy of finding roots of multivariate polynomials with new applications in attacking RSA variants," in *Lecture Notes in Computer Science*, pp. 267-282, 2006.

[12] R. S. Kumar, C. Narasimham, S. P. Setty, "Lattice based tools for cryptanalysis in various applications," in *International Conference on Computer Science and Information Technology*, pp. 530-537, 2012.

[13] R. S. Kumar, C. Narasimham, S. P. Settee, "Generalization of Boneh-Duree's attack on arbitrary public exponent RSA," *Interantional Journal of Computer applications*, vol. 49, no. 19, 2012.

[14] A. Lenstra, H. Lenstra, L. Lovasz, "Factoring polynomials with rational coeffiecients," *Mathematiche Annalen*, vol. 261, pp. 515-534, 1982.

[15] Y. Lu, R. Zhang, and D. Lin, "Factoring multi-power RSA modulus $N = p^r q$ with partial known bits," in *Lecture Notes in Computer Science*, vol. 7959, pp. 57-71, 2013.

[16] Y. Lu, R. Zhang, and D. Lin, "Factoring RSA modulus with known bits from both p and q:a lattice method," in *Lecture Notes in Computer Science*, vol. 7873, pp. 393-404, 2013.

[17] R. Rivest, A. Shamir and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120-126, 1978.

[18] W. A. Stein, et al., *Sage Mathematical Software*, The Sage Development Team, 2011. (`http://ww.sagemath.org`)

## Biography

**Dr. Santosh Kumar Ravva** working as Sr.Asst.prof in the department of Information Technology in MVGR College of Engineering, Vizianagaram, India. He published more than 10 publications in various journals in the area of cryptology. His research interests are Cryptanalysis of RSA, Access control in Wireless sensor networks, Attribute based encryption schemes for cloud computing. He is member in IEI, IAENG, and life member in CRSI.

# One Private Broadcast Encryption Scheme Revisited

Lihua Liu[1], Yang Li[1], Zhengjun Cao[2], Zhen Chen[2]
*(Corresponding author: Zhengjun Cao)*

Department of Mathematics, Shanghai Maritime University[1]
Haigang Ave 1550, Shanghai 201306, China
(Email: caozhj@shu.edu.cn)
Department of Mathematics, Shanghai University[2]
Shangda Road 99, Shanghai 200444, China
*(Received Sept. 10, 2017; revised and accepted Oct. 27, 2017)*

**Abstract**

The cryptographic primitive of private broadcast encryption introduced by Barth, Boneh and Waters, is used to encrypt a message for several recipients while hiding the identities of the recipients. In BBW construction, a recipient has to first decrypt the received ciphertext in order to extract the verification key for one-time signature. The recipient then uses the verification key to check whether the ciphertext is malformed. The BBW construction did not consider that information delivered over a channel, especially over a broadcast channel, should be authenticated as to its origin. We would like to stress that the conventional public key signature suffices to authenticate data origin and filter out all malformed ciphertexts. We also discuss the disadvantages of the primitive of one-time signature used in BBW construction.

*Keywords: Key Management; Man-in-middle Attack; One-time Signature; Private Broadcast Encryption*

## 1 Introduction

Authentication is always a hot topic in network security. Various methods have been developed for this or that application scenarios. For example, in 2017 Ling et al. [18] proposed one-time password authentication scheme for WSN. Tsai et al. [37] put forth a publicly verifiable authenticated encryption scheme based on factoring and discrete logarithms. Ma [20] considered the problem of NFC communications-based mutual authentication for the Internet of things. Tbatou et al. [36] studied a mutuel Kerberos authentication protocol for distributed systems. Hou and Wang [14] proposed a remote authentication scheme from elliptic curve cryptosystem.

Cao et al. pointed out the flaws in some authentication scheme [7, 19]. Moon et al. [24] presented a smart card based password authentication scheme.

In 2016, Maitra et al. [21] considered the problem of user authentication for hierarchical wireless sensor networks without tamper-proof smart card. Sun and Chang [34] analyzed an authentication scheme for access control in mobile pay-TV systems. Xie et al. [38] put forth a roaming authentication

protocol for cloud-assisted body sensor networks. In the same year, Goswami and Ghoshal [13] suggested a method for imperceptible image authentication using wavelets. Chang et al. [8] presented an anonymous and biometrics-based multi-server authentication scheme using smart cards. Aboshosha et al. [1] proposed an authentication protocol based on machine-metrics and RC4-EA hashing.

The cryptographic primitive of broadcast encryption was formalized by Fiat and Naor [9], which requires that the broadcaster encrypts a message such that a particular set of users can decrypt the message sent over a broadcast channel. The Fiat-Naor broadcast encryption and the works [10, 11, 16, 32, 33] use a combinatorial approach. This approach has to right the balance between the efficiency and the number of colluders that the system is resistant to. Recently, Boneh et al. [6, 12] have constructed some broadcast encrypt systems. In these systems, the public parameters must be updated to allow more users.

In 2006, Barth, Boneh and Waters [2] put forth a new cryptographic primitive, private broadcast encryption, which is used to encrypt a message to several recipients while hiding the identities of the recipients. The primitive has many applications. For example, commercial sites can use it to protect identities of customers because competitors might use this information for targeted advertising. Their construction [2] is secure against an active attacker while achieving good efficiency. In the construction, a recipient has to first decrypt the received ciphertext to extract the verification key for one-time signature. He then uses the verification key to check whether the ciphertext is malformed. The authors did not consider that information delivered over a channel, especially over a broadcast channel, should be authenticated as to its origin. For example, in real life a listener must first authenticate the identity of the broadcaster. It is unwise to decrypt the received message without authenticating its origin.

In this note, we would like to point out that BBW broadcast encryption scheme is somewhat impractical because it fails to develop a mechanism to authenticate data origin, while the data origin authentication is very important to a broadcast encryption. We also remark that the conventional public key signature suffices to authenticate data origin and filter out all malformed ciphertexts. Besides, we discuss the disadvantages of the primitive of one-time signature used in BBW construction.

## 2 Review of BBW Broadcast Encryption

The BBW private broadcast encryption uses a public key encryption that has key indistinguishability under CCA attacks (IK-CCA) to encrypt the ciphertext component for each recipient. It then generates a random signature and verification key for a one-time, strongly unforgeable signature scheme [17, 30]. It includes the verification key in each public key encryption and then signs the entire ciphertext with the signing key.

Suppose that (Init, Gen, Enc, Dec) is a strongly-correct IK-CCA public key scheme, (Sig-Gen, Sig, Ver) is a strongly existentially unforgeable signature scheme, and $(E, D)$ are semantically secure symmetric key encryption and decryption algorithms. The private broadcast encryption system can be described as follows.

**Setup:** Given a security parameter $\lambda$, it generates global parameters $I$ for the system. Return $\mathsf{Init}(\lambda)$.

**Keygen:** Given the global parameters $I$, it generates public-secret key pairs. For each user $i$, run $(pk_i, sk_i) \leftarrow \mathrm{Gen}(I)$, return $(pk_i, sk_i)$ and publish $pk_i$.

**Encrypt:** Given a set of public keys $S = pk_1, \cdots, pk_n$ generated by $\mathrm{Keygen}(I)$ and a message $M$, it generates a ciphertext $C$.

1) $(vk, sk) \leftarrow \mathsf{Sig\text{-}Gen}(\lambda)$.
2) Choose a random symmetric key $K$.

3) For each $pk_i \in S$, $c_i \leftarrow \mathsf{Enc}_{pk_i}(vk||K)$.
4) Let $C_1$ be the concatenation of the $c_i$, in random order.
5) $C_2 \leftarrow E_K(M)$.
6) $\sigma \leftarrow \mathsf{Sig}_{sk}(C_1||C_2)$.
7) Return the ciphertext $C = \sigma||C_1||C_2$.

**Decrypt:** Given a ciphertext $C$ and a secret key $sk_i$, return $M$ if the corresponding public key $pk_i \in S$, where $S$ is the set used to generate $C$. Decrypt can also return $\perp$ if $pk_i \notin S$ or if $C$ is malformed. User $i$ parses $C$ as $\sigma||C_1||C_2$ and $C_1 = c_1||\cdots||c_n$. For each $j \in \{1, \cdots, n\}$.

1) $p \leftarrow \mathsf{Dec}(sk_i, c_j)$.
2) If $p$ is $\perp$, then continue to the next $j$.
3) Otherwise, parse $p$ as $vk||K$.
4) If $\mathsf{Ver}_{vk}(C_1||C_2, \sigma)$, return $M = D_K(C_2)$.

# 3 Analysis of BBW Broadcast Encryption

The BBW broadcast encryption scheme [2] can provide recipient privacy. But we find the construction has the following drawbacks.

- The scheme assigns a pair of keys $(pk_i, sk_i)$ to each recipient $i$ for public key encryption and decryption. But it does not assign a pair of keys $(pk_B, sk_B)$ to the broadcaster for public key signature. The drawback leads the authors to not specify the procedure of data origin authentication. An intending recipient can extract the verification key to authenticate data origin only after he successfully completes the procedure of public key decryption. That is to say, they adopt the strategy of *data origin authentication coming after public key decryption.*

  We want to stress that the construction is somewhat impractical because the data origin authentication is very important to a broadcast encryption. In real life, a listener must first authenticate the identity of the broadcaster. The listener then decides whether to decrypt the broadcasted message or not. *It is unwise to decrypt the received message without authenticating its origin.* Indeed, the problem of SPAM is getting more and more serious, which has greatly affected our normal daily life and the public communication environment.

- The main purpose of introducing the one-time signature in their construction is to ensure that an adversary cannot extract a ciphertext component from the challenge ciphertext and use it in another ciphertext because it will be unable to sign the new ciphertext under the same verification key. Simply speaking, its purpose is to filter out the malformed ciphertexts. We should stress that the conventional public key signature suffices to authenticate data origin and filter out the malformed ciphertexts. It is unnecessary to introduce another mechanism to check the malformed ciphertexts.

- The scheme specifies that the algorithm of Encrypt generates a random signature and verification key for a one-time, strongly unforgeable signature scheme. It means that *the broadcaster binds his identity with the verification key by himself*, not by a trusted third party. The description is incorrect. We stress that the verification key for signature, even for one-time signature, must be authenticated by a trusted third party. It should be easily accessible and publicly available to the verifier. Otherwise, the signature scheme is vulnerable to man-in-the-middle attack.

- In the original scheme, the sign $\perp$ is unspecified. Thus, each recipient can not decide which $c_j$ is intended for him. Only after $vk$ is derived successfully and the verification $\mathsf{Ver}_{vk}(C_1||C_2, \sigma)$ passes, he can decide it. This incurs more cost because the recipient has to do the same number of public key decryptions $\mathsf{Dec}(sk_i, c_j)$ as that of verifications $\mathsf{Ver}_{vk}(C_1||C_2, \sigma)$.

# 4 An Improvement of BBW Broadcast Encryption

In this section, we propose an improvement of BBW broadcast encryption. See Table 1 for the description.

The basic idea behind the improvement is to assign a pair of keys $(pk_B, sk_B)$ to the broadcaster for public key signature. The setting makes it possible for a recipient to authenticate data origin first of all. If it succeeds, he then proceeds to the public key decryption. The strategy can greatly reduce a recipient's computational cost because it successfully filters out all origin-unknown and malformed ciphertexts.

Table 1: BBW broadcast encryption scheme and an improvement

| BBW broadcast encryption scheme | An improvement |
|---|---|
| Keygen: For each user $i$, return $(pk_i, sk_i)$ for public key encryption. Publish $pk_i$. | Keygen: For each user $i$, return $(pk_i, sk_i)$ for public key encryption. Publish $pk_i$. For the broadcaster, return $(pk_B, sk_B)$ for public key signatures. Publish $pk_B$. |
| Encrypt: Choose one-time signature keys $(vk, sk)$. Pick a random symmetric key $K$. For each $pk_i \in S$, $c_i \leftarrow \mathsf{Enc}_{pk_i}(vk\|\|K)$. Let $C_1$ be the concatenation of the $c_i$, in random order. $C_2 \leftarrow E_K(M)$, $\sigma \leftarrow \mathsf{Sig}_{sk}(C_1\|\|C_2)$. Return $C = \sigma\|\|C_1\|\|C_2$. | Encrypt: Invoke $(pk_B, sk_B)$. Pick a random symmetric key $K$. For each $pk_i \in S$, $c_i \leftarrow \mathsf{Enc}_{pk_i}(pk_B\|\|K)$. Let $C_1$ be the concatenation of the $c_i$, in random order. $C_2 \leftarrow E_K(M)$, $\sigma \leftarrow \mathsf{Sig}_{sk_B}(C_1\|\|C_2)$. Return $C = \sigma\|\|C_1\|\|C_2$. |
| Decrypt: User $i$ parses $C$ as $\sigma\|\|C_1\|\|C_2$ and $C_1 = c_1\|\|\cdots\|\|c_n$. For each $j \in \{1, \cdots, n\}$, $p \leftarrow \mathsf{Dec}(sk_i, c_j)$. If $p$ is $\perp$, then continue to the next $j$. Otherwise, parse $p$ as $vk\|\|K$. If $\mathsf{Ver}_{vk}(C_1\|\|C_2, \sigma)$, return $M = D_K(C_2)$. | Decrypt: User $i$ parses $C$ as $\sigma\|\|C_1\|\|C_2$ and $C_1 = c_1\|\|\cdots\|\|c_n$. If $\mathsf{Ver}_{pk_B}(C_1\|\|C_2, \sigma)$ fails, return $\perp$. Otherwise, for each $j \in \{1, \cdots, n\}$, $p \leftarrow \mathsf{Dec}(sk_i, c_j)$. Parse $p$ as $pk'_B\|\|K'$. If $pk'_B \neq pk_B$, then continue to the next $j$. Otherwise, return $M' = D_{K'}(C_2)$. |

The Encryption algorithm computes

$$c_i = \mathsf{Enc}_{pk_i}(pk_B||K)$$

for each $pk_i \in S$. The added header $pk_B$ helps each user $i$ to decide which component of the ciphertext is intended for himself, because the probability of that the header of $\mathsf{Dec}(sk_i, c_j)$ equals to the header of $\mathsf{Dec}(sk_i, c_k)$ is negligible, where $j \neq k$. Note that in the original scheme the sign $\perp$ is unspecified. For convenience, we suggest to introduce the header $pk_B$ for checking the intending receiver.

The main difference between the original scheme and its improvement is that *data origin authentication must come before public key decryption*. In the original decryption algorithm, a user $i$ has to complete the procedure of public key decryption at first. He then extracts the verification key for one-time signature to filter out malformed ciphertexts. As we pointed out before, the setting results in that the original scheme is vulnerable to *man-in-the-middle attack* because the user $i$ does not access to the verification key through proper channels. To resist this trivial attack, we adopt the mechanism of public key signature instead of one-time signature.

## 5 Further Discussions on One-time Signature

The primitive of one-time signature was invented by Lamport [17] in 1979. Each Lamport public key can only be used to sign one single message, which means many keys have to be published if many messages are to be signed. A hash tree can be used on those public keys, publishing the top hash of the hash tree instead. But this increases the size of the resulting signature because parts of the hash tree have to be included in the signature.

Researchers are familiar with one-time signature scheme presented by Merkle [22], which is based on one-way functions, as opposed to trapdoor functions that are used in public key signatures. Bleichenbacher and Maurer [4, 5] had suggested one-time signatures based on acyclic graphs.

One-time signatures have been considered to be impractical because of complicated key management and long signature size. Merkle [22, 23] introduced the method of tree authentication to alleviate the problem of key management for a large number of one-time signatures. Rohatgi [29] proposed some techniques to reduce the signature size. Perrig [26] introduced hash chains for key management. Reyzin and Reyzin [28] introduced a one-time signature scheme that has faster signature and verification times (for a single signature). This scheme was improved by Pieprzyk et al. [27]. The recent works of [3,15,35] have improved Merkle's hash-tree method.

The one-time signature presented by Zaverucha and Stinson [39] requires that PK size is of $O(\kappa n)$ bits, where $\kappa$ is the DL security parameter and $n$ is the number of bits in the message to sign. Naor et al. [25] suggest that when fast signatures are required, some one-time signatures can be a promising alternative to the public-key signatures.

Although these one-time signatures are interesting, we would like to stress that the problem of efficient key management for one-time signatures still remains open. This is due to that the cost to guarantee the authenticity of a user's public key is expensive in the scenario of Public Key Infrastructure (PKI for short). In nature, PKI entails that a user's public key should be repeatedly usable in the life duration. This means the primitive of one-time signature is somewhat incompatible with PKI.

The conventional public key signatures are claimed to be vulnerable to quantum computers. But the performances of current quantum computers, D-Wave One and D-Wave Two, mitigate the threat. In May 2014, researchers [31] at UC Berkeley and IBM published a classical model explaining the D-Wave machine's observed behavior, suggesting that it may not be a quantum computer. Any predictions on quantum computers have become more uncertain since the announcements of D-Wave systems. In the current situation, we think that it is unnecessary to use one-time signatures to replace conventional public key signatures.

## 6 Conclusion

In this paper we present an improvement of Barth-Boneh-Waters private broadcast encryption scheme. We also discuss the disadvantages of one-time signature used in their construction and stress that the

primitive is inappropriate for a broadcast system because of its complicated key management and long signature size.

## Acknowledgements

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

## References

[1] A. Aboshosha, K. A. ElDahshan, E. K. Elsayed, and A. A. Elngar, "Secure authentication protocol based on machine-metrics and rc4-ea hashing," *International Journal of Network Security*, vol. 18, no. 6, pp. 1080–1088, 2016.

[2] A. Barth, D. Boneh, and B. Waters, "Privacy in encrypted content distribution using private broadcast encryption," in *Proceedings of 10th International Conference of Financial Cryptography and Data Securityb (FC'06)*, pp. 52–64, Anguilla, British West Indies, Mar. 2006.

[3] P. Berman, M. Karpinski, and Y. Nekrich, "Optimal trade-off for merkle tree traversal," *Electronic Colloquium on Computational Complexity*, no. 049, 2004.

[4] D. Bleichenbacher and U. Maurer, "Directed acyclic graphs, one-way functions and digital signatures," in *Proceedings of 14th Annual International Cryptology Conference, Advances in Cryptology (CRYPTO'94)*, pp. 75–82, Santa Barbara, California, USA, Aug. 1994.

[5] D. Bleichenbacher and U. Maurer, "On the efficiency of one-time digital signatures," in *Proceedings of International Conference on the Theory and Applications of Cryptology and Information, Advances in Cryptology (ASIACRYPT'96)*, pp. 145–158, Kyongju, Korea, Nov. 1996.

[6] D. Boneh, C. Gentry, and B. Waters, "Collusion resistant broadcast encryption with short ciphertexts and private keys," in *Proceedings of 25th Annual International Cryptology Conference, Advances in Cryptology (CRYPTO'05)*, pp. 258–275, Santa Barbara, California, USA, Aug. 2005.

[7] Z. J. Cao, L. H. Liu, and O. Markowitch, "Analysis of one scheme for enabling cloud storage auditing with verifible outsourcing of key updates," *International Journal of Network Security*, vol. 19, no. 6, pp. 950–954, 2017.

[8] C. C. Chang, W. Y. Hsueh, and T. F. Cheng, "An advanced anonymous and biometrics-based multi-server authentication scheme using smart cards," *International Journal of Network Security*, vol. 18, no. 6, pp. 1010–1021, 2016.

[9] A. Fiat and M. Naor, "Broadcast encryption," in *Proceedings of 13th Annual International Cryptology Conference, Advances in Cryptology (CRYPTO'93)*, pp. 480–491, Santa Barbara, California, USA, Aug. 1993.

[10] E. Gafni, J. Staddon, and Y. L. Yin, "Efficient methods for integrating traceability and broadcast encryption," in *Proceedings of 19th Annual International Cryptology Conference, Advances in Cryptology (CRYPTO'99)*, pp. 372–387, Santa Barbara, California, USA, Aug. 1999.

[11] J. Garay, J. Staddon, and A. Wool, "Long-lived broadcast encryption," in *Proceedings of 20th Annual International Cryptology Conference, Advances in Cryptology (CRYPTO'00)*, pp. 333–352, Santa Barbara, California, USA, Aug. 2000.

[12] C. Gentry and B. Waters, "Adaptive security in broadcast encryption systems," in *Proceedings of 28th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Advances in Cryptology (EUROCRYPT'09)*, pp. 171–188, Cologne, Germany, Apr. 2009.

[13] A. Goswami and N. Ghoshal, "Imperceptible image authentication using wavelets," *International Journal of Network Security*, vol. 18, no. 5, pp. 861–873, 2016.

[14] G. F. Hou and Z. J. Wang, "A robust and efficient remote authentication scheme from elliptic curve cryptosystem," *International Journal of Network Security*, vol. 19, no. 6, pp. 904–911, 2017.
[15] M. Jakobsson, F. Leighton, S. Micali, and M. Szydlo, "Fractal merkle tree representation and traversal," in *Proceedings of The Cryptographers' Track at the RSA Conference, Topics in Cryptology (CT-RSA'03)*, pp. 314–326, San Francisco, CA, USA, April 2003.
[16] R. Kumar, S. Rajagopalan, and A. Sahai, "Coding constructions for blacklisting problems without computational assumptions," in *Proceedings of 19th Annual International Cryptology Conference, Advances in Cryptology (CRYPTO'99)*, pp. 609–623, Santa Barbara, California, USA, Aug. 1999.
[17] L. Lamport, "Constructing digital signatures from one-way function," *Technical Report SRI-CSL-98, SRI International*, 1979.
[18] C. H. Ling, C. C. Lee, C. C. Yang, and M. S. Hwang, "A secure and efficient one-time password authentication scheme for wsn," *International Journal of Network Security*, vol. 19, no. 2, pp. 177–181, 2017.
[19] L. H. Liu, W. P. Kong, Z. J. Cao, and J. B. Wang, "Analysis of one certificateless encryption for secure data sharing in public clouds," *International Journal of Electronics and Information Engineering*, vol. 6, no. 2, pp. 108–113, 2017.
[20] Y. N. Ma, "NFC communications-based mutual authentication scheme for the internet of things," *International Journal of Network Security*, vol. 19, no. 4, pp. 631–638, 2017.
[21] T. Maitra, R. Amin, D. Giri, and P. D. Srivastava, "An efficient and robust user authentication scheme for hierarchical wireless sensor networks without tamper-proof smart card," *International Journal of Network Security*, vol. 18, no. 3, pp. 553–564, 2016.
[22] R. Merkle, "A digital signature based on a conventional encryption function," in *Proceedings of CRYPTO 1987*, pp. 369–378, 1987.
[23] R. Merkle, "A certified digital signature," in *Proceedings of 9th Annual International Cryptology Conference, Advances in Cryptology (CRYPTO'89)*, pp. 218–238, Santa Barbara, California, USA, Aug. 1989.
[24] J. Moon, D. Lee, J. Jung, and D. Won, "Improvement of efficient and secure smart card based password authentication scheme," *International Journal of Network Security*, vol. 19, no. 6, pp. 1053–1061, 2017.
[25] D. Naor, A. Shenhav, and A. Wool, "One-time signatures revisited: have they become practical," *IACR Cryptology ePrint Archive*, no. 442, 2005.
[26] A. Perrig, "The biba one-time signature and broadcast authentication protocol," in *Proceedings of the 8th ACM Conference on Computer and Communications Security (CCS'01)*, pp. 28–37, Philadelphia, Pennsylvania, USA, Nov. 2001.
[27] J. Pieprzyk, H. X. Wang, and C. P. Xing, "Multiple-time signature schemes against adaptive chosen message attacks," in *Proceedings of 10th Annual International Workshop, Selected Areas in Cryptography (SAC'03)*, pp. 88–100, Ottawa, Canada, Aug. 2003.
[28] L. Reyzin and N. Reyzin, "Better than biba: short one-time signatures with fast signing and verifying," in *Proceedings of 7th Australian Conference, Information Security and Privacy (ACISP'02)*, pp. 144–153, Melbourne, Australia, July 2002.
[29] P. Rohatgi, "A compact and fast hybrid signature scheme for multicast packet authentication," in *Proceedings of the 6th ACM Conference on Computer and Communications Security (CCS'99)*, pp. 93–100, Singapore, Nov. 1999.
[30] J. Rompel, "One-way functions are necessary and sufficient for secure signatures," in *Proceedings of the 22nd Annual ACM Symposium on Theory of Computing (STOC'90)*, p. 387394, Baltimore, Maryland, USA, May 1990.
[31] S. W. Shin, G. Smith, J. Smolin, and U. Vazirani, "How 'quantum' is the d-wave machine?," `http://arxiv.org/abs/1401.7087`, 2014.

[32] D. Stinson, "On some methods for unconditionally secure key distribution and broadcast encryption," *Design, Codes and Cryptography*, vol. 12, no. 3, pp. 215–243, 1997.
[33] D. Stinson and T. Trung, "Some new results on key distribution patterns and broadcast encryption," *Design, Codes and Cryptography*, vol. 14, no. 3, pp. 261–279, 1998.
[34] C. Y. Sun and C. C. Chang, "Cryptanalysis of a secure and efficient authentication scheme for access control in mobile pay-tv systems," *International Journal of Network Security*, vol. 18, no. 3, pp. 594–596, 2016.
[35] M. Szydlo, "Merkle tree traversal in log space and time," in *Proceedings of International Conference on the Theory and Applications of Cryptographic Techniques, Advances in Cryptology (EUROCRYPT'04)*, pp. 541–554, Interlaken, Switzerland, May 2004.
[36] Z. Tbatou, A. Asimi, Y. Asimi, Y. Sadqi, and A. Guezzaz, "A new mutuel kerberos authentication protocol for distributed systems," *International Journal of Network Security*, vol. 19, no. 6, pp. 889–898, 2017.
[37] C. Y. Tsai, C. Y. Liu, S. C. Tsaur, and M. S. Hwang, "A publicly verifiable authenticated encryption scheme based on factoring and discrete logarithms," *International Journal of Network Security*, vol. 19, no. 3, pp. 443–448, 2017.
[38] Q. Q. Xie, S. R. Jiang, L. M. Wang, and C. C. Chang, "Composable secure roaming authentication protocol for cloud-assisted body sensor networks," *International Journal of Network Security*, vol. 18, no. 5, pp. 816–831, 2016.
[39] G. Zaverucha and D. Stinson, "Short one-time signatures," *Advances in Mathematics of Communications*, vol. 5, no. 3, pp. 473–488, 2011.

## 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.

**Yang Li** is currently pursuing his 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 served as a post-doctor in Computer Sciences Department, Université Libre de Bruxelles, from 2008 to 2010. His research interests include cryptography, discrete logarithms and quantum computation.

**Zhen Chen** is currently pursuing his M.S. degree from Department of Mathematics, Shanghai University. His research interests include information security and cryptography.

# Hidden Data Transmission with Variable DNA Technology

Ravinder Paspula, K. Chiranjeevi, S. Laxman Kumar
*(Corresponding author: Ravinder Paspula)*

Computer Science and Engineering, Institute of Aeronautical Engineering
Jawaharlal Nehru Technological University Hyderabad
Kukatpally, Hyderabad - 500 085, Telangana, India
(Email: ravindra.paspula@gmail.com)
*(Received Feb. 21, 2017; revised and accepted Apr. 23 & June 6, 2017)*

**Abstract**

DNA cryptography is a new promising direction in cryptography research that emerged with the evolution in DNA computing field. DNA can be used not only to store and transmit the information, but also to perform computation. Although in its primitive stage, DNA cryptography is shown to be very effective. In this the concept of DNA is being used in the encryption and decryption process. This also proposes a unique cipher text generation procedure as well as a new key generation procedure. This proposal wants to design a method which contains two rounds. For each round, we secretly select a reference DNA sequence and a secret Key (SK). In the first round process, generate a secured symmetric, a secretly selected DNA sequence S and cipher block chaining mode(CBC)-a Conventional cryptography technique which generate a intermediate form of cipher text and in the second round process, the intermediate form of cipher text converted into final cipher text(S) using a reference DNA Sequences and convert this into faked DNA Sequence called human made DNA Sequence(S') so it will become a more complicated for intruder to extract original message from faked DNA Sequence(S') send this faked DNA Sequence to the receiver together with many other DNA, or DNA-like sequences to the receiver.

*Keywords: Encryption; Decryption; Key Generation; Cipher Text; DNA Cryptography*

## 1 Introduction

### 1.1 Introduction to Cryptography

In the era of information technology, the possibility that the information stored in a person's computer or the information that are being transferred through network of computers or internet being read by other people is very high. This causes a major concern for privacy, identity theft, electronic payments, corporate security, military communications and many others. We need an efficient and simple way of securing the electronic documents from being read or used by people other than who are authorized to do it. Cryptography is a standard way of securing the electronic documents. Basic idea of Cryptography: Basic idea of cryptography is to mumble-jumble the original message into something that is unreadable or to something that is readable but makes no sense of what the original message is. To retrieve

the original message again, we have to transform the mumble-jumbled message back into the original message again.

### 1.2 Basic Terminologies used in Cryptography

Data that can be read and understood without any special measures is called plaintext or clear text. This is the message or data that has to be secured. The method of disguising plaintext in such a way as to hide its substance is called encryption. Encrypting plaintext results in unreadable gibberish called cipher text. You use encryption to ensure that information is hidden from anyone for whom it is not intended, even those who can see the encrypted data. The process of reverting cipher text to its original plaintext is called decryption.

Cryptography is the science of mathematics to encrypt and decrypt data. Cryptography enables us to store sensitive information or transmit it across insecure networks like Internet so that no one else other the intended recipient can read it. Cryptanalysis is the art of breaking Ciphers that is retrieving the original message without knowing the proper key. Cryptography deals with all aspects of secure messaging, authentication, digital signatures, electronic money, and other applications.

DNA is a small molecule that encodes genetic information which is very essential for execution and growth of all organisms. DNA stands for Deoxyribo Nucleic Acid. DNA is a polymer made up of monomers called Deoxyribo nucleotides [1]. Every nucleotide consists of three main parts: Deoxyribose, sugar and phosphate group and a nitrogenous base. The nitrogenous bases are Adenine, Guanine, Cytosine and Thymine ("A", "G", "C", "T"). DNA is formed by a double helix which is formed by base pairs attached to a sugar-phosphate backbone.DNA (Deoxyribose Nucleic Acid) computing, also known as molecular computing which is a new approach that provides parallel computation, developed by Adleman. DNA computing was designed for solving a class of difficult computational problems in which the computing time can grow exponentially with problem size (the 'NP- Complete' or non-deterministic polynomial time complete problem). DNA computer is basically a collection of specially selected DNA strand which all together will result in the solution to some problem, depending on the nature of problem.

## 2 Review of International Status

For every living cell, DNA is a basic storage medium. Its main functionality is to absorb and transmit the data of life for billions years. Near about 10 trillions of DNA molecules could fit into a space of a marble size. Since all these molecules can process data simultaneously, theoretically, we can perform massive parallel computations in a small space at one time. DNA computing is more generally known as molecular computing. Computing with DNA offers a completely new paradigm for computation. The main idea of computing with DNA is to encode data in a DNA strand form in order to simulate arithmetical and logical operations. The main operation of DNA computing is called Synthesis, which is a process of designing and restructuring information in DNA sequence form. In DNA computing, designing and synthesizing information in the DNA sequence form is an important process where wrong design might leads to wrong result.

There are large number of researcher groups that take an initiative to implement DNA concept in the solutions of applications like cryptography, scheduling, clustering, encryption, forecasting and even tried to employ it in signal and image processing application. On the other hand, some other researchers in this field are working on proposing DNA algorithm employed in information security technology. For example, Boneh *et al.* and Adleman et al. [5] have proposed a model to break a Data Encryption Stan-dard(DES) as a alternative way for encryption data technology. DNA cryptography has been proposed by Gehani *et al.* Kartalopoulos and Tanaka *et al.* as a new born cryptography

field. Beside DNA cryptography and DES, there are some development in DNA Steganography and DNA certification. Recently, DNA is employed as an intrusion detection model for computer and telecommunication systems by Boukerche *et al.* Among all DNA computing models proposed in this research area DNA certification is most matured and the application is most widely studied.

There are large number of researcher groups that take an initiative to implement DNA concept in the solutions of 978142449190211$26.00 ©2011 IEEE applications like cryptography, scheduling, clustering, encryption, forecasting and even tried to employ it in signal and image processing application. On the other hand, some other researchers in this field are working on proposing DNA algorithm employed in information security technology [4].

For example, Boneh *et al.* and Adleman *et al.* [5] have proposed a model to break a Data Encryption Standard (DES) as a alternative way for encryption data technology. DNA cryptography has been proposed by Gehani *et al.* [4], Kartalopoulos and Tanaka *et al.* as a newborn cryptography field. Beside DNA cryptography and DES, there are some development in DNA steganography and DNA certification. Recently, DNA is employed as an intrusion detection model for computer and telecommunication systems by Boukerche *et al.*. Among all DNA computing models proposed in this research area DNA certification is most matured and the application is most widely studied.

Jin-Shiuh Taur *et al.* proposed a way referred to as Table Lookup Substitution methodology (TLSM) that might double the capability of message activity. In TSLM, they need replaced the complementary rule with a rule table. The key plan of the TLSM is to increase the 1-bit complementary rule into a 2-bit rule table so every conversion of letters will represent 2 bits of the secret message.

In the method by Cheng Guo, Shiu, the hiding procedure substitutes another letter for an existing letter on a special location set by the algorithm. The embedding algorithm encompasses a conversion operates that converts a given letter with a selected letter outlined by the complementary rule. For example, if a complementary rule is outline as (AC)(CG)(GT)(TA), then the result of c(G) are going to be T, and therefore the result of c(T) are going to be A. To boot, the substitution methodology can convert the letter s into s (unchanged), c(s) and c (c (s)) once the secrete message is 0, 1 and no data, respectively.

Mohammad Reza Abbasy, *et al.* proposed an information hiding methodology wherever data was efficiently encoded and decoded following the properties of DNA sequence. Complementary combine rules of DNA were employed in their methodology.

Kritika Gupta, Shailendra Singh has been projected a DNA Based Cryptological Techniques for an encryption algorithm based on OTP (one-time-pad) that involve data encryption using traditional mathematical operations and/or data manipulating DNA techniques. However once an encryption algorithm has been applied and therefore the data is transmitted on the transmission media: there's a clear stage that the data, although within the cipher type gets manipulated by any interceptor. Snehal Javheri, Rahul Kulkarni proposed an algorithmic program has two phases in consequence: these are Primary Cipher text generation using exploitation substitution methodology followed by Final Cipher text generation exploitation DNA digital secret writing.

In the Primary Cipher text generation phase, the coding algorithmic program uses OTP (one-time-pad) key generation theme, since nearly one key for one piece of data is sufficient to supply voluminous strength in coding technique. The projected methodology uses indiscriminately generated symmetrical key of 8 bits size by the supposed receiver and provided to the sender. Therefore the sender can have partial information of the personal key solely and so it generates the remainder part of the keys to cipher the data.

The Byte values are extracted from the input data or message. The additional secret writing method works on unsigned byte values of the input data or text referred to as plain text. These byte values are replaced by combination of alphabets and special symbols exploitation substitution methodology. And so this substitution worths are regenerate into its binary value. So as to embed lots of security

additional bits are padded at each ends of the first cipher text. These additional bits are nothing however the file size information that is provided to the receiver through key. So the secret key, the data of primer pairs are shared between sender and receiver through the secret key channel. In the DNA digital secret writing section, the Ultimate Cipher text is generated from Primary Cipher text exploitation DNA digital encryption technique. From a process purpose of read, cannot process the DNA molecules as in sort of alphabets, therefore the DNA sequence encryption is employed during this methodology through that the binary knowledge is regenerate into DNA format and it's vice versa. Guangzhao Cui, Limin Qin, Yanfeng Wang, Xuncai Zhang [4] proposed a secrete writing theme by exploitation the technologies of DNA synthesis, PCR amplification and DNA digital secrete writing additionally because the theory of ancient cryptography. The supposed PCR two primer pairs was used because the key of this theme that not severally designed by sender or receiver, however severally designed by the entire cooperation of sender and receiver. This operation might increase the safety of this secrete writing theme. The standard secretes writing methodology and DNA digital cryptography is wont to preprocess to the plaintext. Through this preprocess operation will get fully different cipher text from the identical plaintext, which might effectively stop attack from a potential word as PCR primers. The quality of biological troublesome issues and cryptography computing difficulties give a double security safeguards for the theme, and therefore the security analysis secrete writing theme has high confidential strength. Ritu Gupta, Anchal Jain symmetric-key encoding algorithmic rule supported the DNA approach is projected. The initial key sequence is enlarged to desire length victimization projected key growth technique guided by the pseudo random sequence. The advantage is that there's no need to send an extended key over the channel. The variable key growth in encoding method combined with DNA addition and complement makes the technique sufficiently secure. A DNA sequence consists of four nucleic acid bases A (adenine), C (cytosine), G (guanine), T (thymine), wherever A and T are complementary, and G and C are complementary. Also use C, T, A and G to denote 00, 01, 10, 11 (the corresponding decimal digits are $-0123||$). By victimization this encoding technique every 8-bit component worth of the gray scale image is pictured as a nucleotide string of length four. Reciprocally to decrypt the nucleotide string will get a binary sequence simply. In total $4! = 24$ forms of writing, there are only 8 of them will meet complementary rule , for instance, the decimal digits ?0123? (the corresponding binary range is $-00011011||$) will be encoded in to one of them, like $-CTAG||$, $-CATG||$, $-GATC||$, $-GTAC||$, $-TCGA||$, $-TGCA||$, $-ACGT||$ or $-AGCT||$. There are total six legal complementary rules [**?**] that are as follows:

$$(AT)(TC)(CG)(GA),$$
$$(AT)(TG)(GC)(GA),$$
$$(AC)(CT)(TG)(GA),$$
$$(AC)(CG)(GT)(TA),$$
$$(AG)(GT)(TC)(CA),$$
$$(AG)(GC)(CT)(TA).$$

Any one of them for instance, (AG) (GC) (CT) (TA) is applied to projected methodology.

## 3 Review of National Status

Since security is one of the most important issues, evolve of cryptography and cryptographic analysis is considered as the fields of on-going research. The latest development on this field is DNA cryptography. It has emerged after the disclosure of computational ability of Deoxyribo Nucleic Acid (DNA). DNA cryptography uses DNA as the computational tool along with several molecular techniques to manipulate

it. Due to very high storage capacity of DNA, this field is becoming very promising. Currently it is in the development phase and it requires a lot of work and research to reach a mature stage. By reviewing all the potential and cutting edge technology of current research, this paper shows the directions that need to be addressed further in the field of DNA cryptography.

Secure communication can be achieved by employing strong cryptography to ensure confidentiality (nondisclosure of secret information), integrity (prevention of data alteration), authentication (proof of identity), and non-repudiation (unique, non-contestable message origin). These goals can be accomplished through a combination of symmetric-key algorithms (e.g. AES, DES, RC4), public-key algorithms (e.g. RSA, ECC), and cryptographic hash functions (e.g. MD5, SHA) [3]. In the recent year few works on qualitative and quantitative analysis on DNA based Cryptography as well as many new Cryptographic techniques were proposed by the researchers [1, 5, 3]. Bibhash Roy, *et al.* [3, 4, 2, 6] proposed a DNA sequencing based encryption and decryption process. The authors propose a unique cipher text generation procedure as well as a new key generation procedure. But the experimental result shows that the encryption process requires high time complexity. This paper is enhanced from our previous proposed work. This paper includes the procedures like public and private key generations; encryption and decryption for secure data communication using DNA based digital encoding technique in Mobile Adhoc Networks. This paper also shows the experimental result using Simulators and Emulators and proved to be far better technique as compared to other existing systems in terms of energy consumption, Time of execution, Data Security. K. Menaka, proposed a data hiding method where the algorithm first randomly selects a DNA sequence. The message to be encoded is then taken and each letter in the faked DNA sequence. Each letter in the message is converted into its ASCII equivalent and they are then converted into equivalent binary form. Each two digits in the converted binary sequence are converted as per Table then, the message index position (first position of each letter) in the faked DNA sequence is applied to each letter of the converted sequence. Each digit in the resultant sequence is replaced with its equivalent three digit binary value and the equivalent alphabet value is replaced for the binary value. For example, if they obtained binary value is 010 011 101 ..., then it will be replaced as C D F ... where A has the value 000; B has 001 and so on. The resultant sequence of alphabets is transmitted over to the receiver. In the receiver side, the reverse process is done in which the original receiver knows the complementary rules and the randomly selected DNA sequence. The message to be sent is then encoded with the fake DNA sequence.

Debnath Bhattacharyya [1] developed an algorithm for data encryption using DNA sequencing. In their algorithm, they have used the concept of indexing the DNA Sequencing and transmitting the message to the receiver. They have not used any complementary rules.

Ms. Amruta D. Umalkar with the quick development of new technology and data process technology, the knowledge is unremarkable transmitted via the net. The vital data in transmission is definitely intercepted by unknown person or hacker. So as to reinforce the knowledge security, encryption becomes a vital analysis is direction. A message cryptography formula supported deoxyribonucleic acid (Deoxyribo Nucleic Acid) sequence for presenting during this paper. The most purpose of this formula is to write the message with the premise of complementary rules deoxyribonucleic acid sequence.

## 4 Importance of the Proposal in the Context of Current Status

The current scenario is such that the assurance of security in large open networks has become the need of the hour. With increase in the rate of crimes, one needs to take precautions to protect the data in an efficient manner from all possible attacks. This application plays an important role in providing security for military communications, financial transactions, corporate and political issues. Basically for this need we have undertaken the task of providing such a secured package, which provides secured data transmission environment to the user? This all is possible using cryptography. Explaining each

aspect in detail as follows, beginning with Cryptography. Cryptography is one of the major concerned areas of computer and data security and a very promising direction in cryptography research is known as DNA Cryptography.

DNA computational logic can be used in cryptography for encrypting, storing and transmitting the information, as well as for computation. Although in its primitive stage, DNA cryptography is shown to be very effective. In this the concept of DNA is being used in the encryption and decryption process. The theoretical analysis and implementations shows this method to be efficient in computation, storage and transmission; and it is very powerful against certain attacks. This also proposes a unique cipher text generation procedure as well as a new key generation procedure. Finally, to demonstrate the performance of the proposed method, its implementation is explained and the results are analyzed.

In cryptography, cipher text is the result of encryption performed on plaintext using an algorithm, called a cipher. Cipher text is also known as encrypted or encoded information because it contains a form of the original plaintext that is unreadable by a human or computer without the proper cipher to decrypt it. Decryption, the inverse of encryption, is the process of turning cipher text into readable plaintext. Cipher text is not to be confused with code text because the latter is a result of a code, not a cipher. Providing computer security in large open networks such as the Internet is one of the frontiers of computer science today. Yet, providing security is not so simple, and many technical challenges need to be solved to provide the high assurance.

For providing better security and reliable data transmission, a new method of encryption process is proposed here. This proposed algorithm consists of two rounds which work on the binary values of the message or plaintext. In this algorithm, binary values or bits are read from the plaintext. A session key, a random number and DNA sequence is shared through a secure channel between sender and receiver prior to communication establishment. The session key bears the information about the key that is used for encrypting the message.

In actual scenario, DNA cryptography is far away from realization because in current time it can be performed only in labs using chemical operations. In order to provide better security and reliable data transmission an effective method of DNA based cryptography is proposed here. In this method the mixture of mathematical and biological concepts are used to get the encrypted data in the form DNA sequences. The benefit of this scheme is that it makes difficult to read and guess about data (plain text).The proposed algorithm has two phases in consequence: these are Primary Cipher text generation using substitution method followed by Final Cipher text generation using DNA digital coding.

In the Primary Cipher text generation phase, the encryption algorithm uses OTP (one-time-pad) key generation scheme, since almost one key for one piece of information is sufficient to provide lots of strength in encoding technique. The proposed method uses randomly generated symmetric key of 8 bits size by the intended receiver and provided to the sender. Thus the sender will have a partial knowledge of the private key only and then it generates the rest part of the keys (Private Keys: Levels 1 and 2) to encode the information. The Byte values are extracted from the input file or message. The further encryption process works on unsigned byte values of the input file or text called as plain text. These byte values are replaced by combination of alphabets and special symbols using substitution method. And then this substitution values are converted into its binary value. In order to embed more security extra bits are padded at both the ends of the primary cipher text. These extra bits are nothing but the file size information, which is provided to the receiver through Level 2 key. Thus the secret key, the information of primer pairs are shared between sender and receiver through the secret channel.

In the DNA digital coding phase, the Final Cipher text is generated from Primary Cipher text using DNA digital encoding technique. From a computational point of view, we cannot process the DNA molecules as in form of alphabets, so the DNA sequence encoding is used in this method through which the binary data is converted into DNA format and it's vice versa. The four subunits of DNA molecule called as nucleotide bases: A: adenine; G: Guanine; C: Cytosine and T: Thymine are converted into 2

bit binary as A: 0(00), T: 1(01), C: 2(10), G: 3(11). Obviously, there are 4! =24 possible coding patterns by this encoding format. However, according to the Watson-Crick complementarily rule, in double helix DNA structure, the two DNA strands are held together complementary in terms of sequence, i.e. A to T and C to G. As per the rules, 3(11) is complement of 0(00) and 2(10) of 1(01). So among 24 patterns, only 8 kinds of patterns (0123CTAG, 0123CATG, 0123GTAC, 0123GATC, 0123TCGA, 0123TGCA, 0123ACGT AND 0123AGCT) are fit as per complimentary rule of the nucleotide bases. Thus A and T are corresponds to '00' and '11'respectively and C and G to '01' and '10' respectively. So substitution rule is A=00, T=11, C=01 and G=10 as illustrate in Table 1.

Table 1: DNA digital Coding Coding

| DNA nucleotide | Decimal | Binary |
|---|---|---|
| A | 0 | 00 |
| C | 1 | 01 |
| G | 2 | 10 |
| T | 3 | 11 |

The round 1 key for encryption is computed based on the response of a random number generator and the information about the key is send to the receiving side through a private channel [4]. Sender will use a random number generator to generate a random number, and then this number along with the shared secret key will go through a function that will produce round 1 encryption key (KE). The same function will generate the session key as the information of the key that is being used. Then each 8-bit block of plaintext will go through the round 1 encryption by round 1 encryption key (KE) using cipher block chaining methods. The output of one block will be used as the key for the next block.

In encryption round 2, sender will select a DNA sequence randomly from publicly available DNA sequences [1, 2]. This DNA sequence is one of the key of encryption round 2. Receiving side must have the information about the used DNA sequence. Then this selected DNA sequence will be converted into binary string using binary coding scheme. This binary string is then segmented into k-bit (Rn-random number) blocks. Each block of the intermediate cipher text is to be inserted before the each block of the DNA sequence. When the length of DNA sequence is less than the length of the intermediate cipher text, the DNA sequence will be repeated. And when the case is reversed then the extra bit from the DNA sequence will be removed after that concatenate all blocks and then convert into a faked DNA sequence also called as human made DNA sequence using binary coding scheme of DNA. This final cipher text has extra information including starting and ending primers that is not linked up with the original message. Keywords:-security, encryption, decryption, key generation, cipher text, DNA cryptography.

## 5 Work Plan Methodology

For providing better security and reliable data transmission, a new method of encryption process is proposed here. This proposed algorithm consists of two rounds which work on the binary values of the message or plaintext. In this algorithm, binary values or bits are read from the plaintext. A session key, a random number and DNA sequence is shared through a secure channel between sender and receiver prior to communication establishment. The session key bears the information about the key that is used for encrypting the message.

The round 1 key for encryption is computed based on the response of a random number generator

and the information about the key is send to the receiving side through a private channel [4]. Sender will use a random number generator to generate a random number, and then this number along with the shared secret key will go through a function that will produce round 1 encryption key (KE). The same function will generate the session key as the information of the key that is being used. Then each 8-bit block of plaintext will go through the round 1 encryption by round 1 encryption key (KE) using cipher block chaining methods. The output of one block will be used as the key for the next block.

In encryption round 2, sender will select a DNA sequence randomly from publicly available DNA sequences [1, 2]. This DNA sequence is one of the key of encryption round 2. Receiving side must have the information about the used DNA sequence.

Then this selected DNA sequence will be converted into binary string using binary coding scheme. This binary string is then segmented into k-bit (Rn-random number) blocks. Each block of the intermediate cipher text is to be inserted before the each block of the DNA sequence. When the length of DNA sequence is less than the length of the intermediate cipher text, the DNA sequence will be repeated. And when the case is reversed then the extra bit from the DNA sequence will be removed after that concatenate all blocks and then convert into a faked DNA sequence also called as human made DNA sequence using binary coding scheme of DNA. This final cipher text has extra information including starting and ending primers that is not linked up with the original message.

## 5.1 Phase I

For providing better security and reliable data transmission, a new method of encryption process is proposed here. This proposed algorithm consists of two rounds which work on the binary values of the message or plaintext. In this algorithm, binary values or bits are read from the plaintext. A session key, a random number and DNA sequence is shared through a secure channel between sender and receiver prior to communication establishment. The session key bears the information about the key that is used for encrypting the message.

The round 1 key for encryption is computed based on the response of a random number generator and the information about the key is send to the receiving side through a private channel [4]. Sender will use a random number generator to generate a random number, and then this number along with the shared secret key will go through a function that will produce round 1 encryption key (KE).

**Steps for Encryption (Round 1)**

**Step 1:** Conversion from Plain text to binary bits 1. Read Binary bits from Plaintext and divide into 8 bit blocks.

**Step 2:** Generate a Common secrete Key (SK)

1) Define a common secret key (SK) (by using Random Generator);
2) Select DNA Sequence;
3) Complementary Rules;
4) DNA Binary coding Rules;
5) All are shared between sender and receiver prior to communication (16-bit).

**Step 3:** Compute Session Key (KS).
Compute Session Key based Secret Key (PK) and a Random Number (Rn).

**Step 4:** Compute Encryption Key for Encryption (KE).
Compute Session Key based on secret key and Random Number(Rn).

]Step 5:] Compute 1st Level Cipher Text.
Generate: Level 1 cipher Text by Performing XOR Operation on Step 1 and Step 2.

**Steps for Encryption (Round 2)**

**Step 1:** Select DNA sequence (S).

1) Code S into a binary sequence by using the binary coding scheme.
2) Divide S into segments whereby each segment contains k bits. (Select k randomly).

**Step 2:** Divide the First level cipher text into k bits (FCT) block.

**Step 3:** Encrypt the DNA Sequence.

1) Insert bits from (FCT), once at a time, into the beginning of segments of S.
2) Concatenating the above segments.
3) Use the binary code scheme to convert the above segments into faked DNA sequences.
4) Add extra information.

## 5.2 Phase II: Procedure for Sharing Key

Round 1 Session Key Generation and Sharing.

A common secret key (PK) is shared between sender and receiver prior to communication (16-bit).

Sending End Computations:

**Step 1:** Sender will use a random number generator and select one random number which is of 16-bit (Rn).

**Step 2:** Divide the random number 'Rn' into 2 parts each of having 8-bit (RnL and RnR).

**Step 3:** Divide the shared secret key into 2 parts as PKL and PKR. Both of these are of 8-bit.

**Step 4:** Now PKL will get XOR with RnR and PKR will get XOR with RnL.

$$\begin{aligned} RL &= PKL \oplus RnR \\ RR &= PKR \oplus RnL. \end{aligned}$$

**Step 5:** Both of the results will be further sub-divided into 2 parts namely RL1, RL2 and RR1, RR2 having 4-bit each.

**Step 6:** Make 4 bit EX-OR Operation between RL1 and RL2 and between RL2 and RL1.

$$\begin{aligned} T1 &= RL1 \oplus RR2 \\ T2 &= RL2 \oplus RR1. \end{aligned}$$

**Step 7:** Concatenate these 4-bit results, T1 and T2, which will give Encryption key of 8-bit for round 1.

$$KE = K1 = concate(T1, T2).$$

**Step 8:** Session key computation for round1. Compute, $tmp = PK \oplus Rn$.

**Step 9:** Divide 'tmp' by 16 and convert the remainder into its equivalent hex form and keep it in 'KS1' Divide the result once again by 16 keeping hex form of the remainder in 'KS2'.Do until the result is less than 16 (KS3, KS4, ... KSn).

**Step 10:** Make together all the 'KSs' in order to get the round 1 session key KS.

**Step 11:** Send 'KS' as round 1 session key through a secure channel along with round 2's session key.

### 5.3 Phase III: Session Key Computation

$$\begin{aligned} tmp &= PK \oplus Rn = 49429 \oplus 6255 = 55674. \\ KS1 &= 55674\%16 = 10 = A(hexform). \\ tmp &= 55674/16 = 3479. \\ KS2 &= 3479\%16 = 7 = 7(hexform). \\ tmp &= 3479/16 = 217. \\ KS3 &= 217\%16 = 9 = 9(hexform). \\ tmp &= 217/16 = 13. \\ KS4 &= 13 = D(hexform). \end{aligned}$$

Session key, KS = A79D.

**Receiving End Computations: Input:** Shared secret key 'PK' and session key 'KS'.

**Step 1:** Separate all the digits of 'KS' and convert these into their equivalent decimal form, e.g. KS = A79D (say), KS1=10, KS2=7, KS3=9, KS4=13.

**Step 2:** Computation of decryption key as follows:

$$\begin{aligned} tmp &= KSn; \\ tmp &= (tmp \times 16) + KSn - 1 \end{aligned}$$

continue upto KS1. Random number, $Rn = tmp \oplus PK$, e.g.

$$\begin{aligned} tmp1 &= (13 \times 16) + 9 = 217; \\ tmp2 &= (217 \times 16) + 7 = 3479; \\ tmp &= tmp3 = (3479 \times 16) + 10 = 55674; \\ Rn &= (49429 \oplus 55674) = 6255. \end{aligned}$$

**Step 3:** Divide the random number 'Rn' into 2 parts each of having 8-bit (RnL and RnR) and divide the shared secret key into 2 parts as PKL and PKR. Both of these are of 8-bit.

**Step 4:** Now PKL will get XOR with RnR and PKR will get XOR with RnL.

$$\begin{aligned} RL &= PKL \oplus RnR \\ RR &= PKR \oplus RnL \\ RL &= 193 \oplus 111 = 174; \\ RR &= 21 \oplus 24 = 13. \end{aligned}$$

**Step 5:** Both of the results will be further sub-divided into 2 parts namely RL1, RL2 and RR1, RR2 having 4-bit each.

**Step 6:** Make 4-bit EX-OR operation between RL1 and RR2 and between RL2 and RR1.

$$\begin{aligned} T1 &= RL1 \oplus RR2; \\ T2 &= RL2 \oplus RR1; \\ T1 &= 10 \oplus 13 = 7; \\ T2 &= 14 \oplus 0 = 14. \end{aligned}$$

**Step 7:** Concatenate these 4-bit results, T1 and T2, which will give Decryption key of 8-bit for round 1. $K1 = concate(T1, T2)$. Decryption key, $KD = K1 = concate(0111, 1110) = 01111110 = 126$.

**Key Sharing for Round 2**

Generate a number randomly that will be used as round 2 key for the second round of encryption process. This key will give the size of extra bit that is to be added with the cipher text, to make the cipher text more complicated to the intruders. Select a DNA sequence randomly from publicly available DNA sequences [1]. The round key 2 and the selected DNA sequence are to be sent at the receiver end prior to communication. In encryption round 2, sender will select a DNA sequence randomly from publicly available DNA sequences [1, 2]. This DNA sequence is one of the key of encryption round 2. Receiving side must have the information about the used DNA sequence.

### 5.4 Expected Output and Outcome of the Proposal

1) Time complexity of encryption and decryption process is to be reduced. The time required for encryption and encryption process is trying to be reduced considerably.

2) Security of data transmission is increased with better encryption and decryption process applied for critical services like defense and external affairs.

3) The authorization of receiving end is to be improved extensively.

## References

[1] L. M. Adleman, "Molecular computation of solutions to combinatorial problems," *Science*, vol. 266, no. 5187, pp. 1021–1024, Nov. 1994.

[2] B. Anam, K. Sakib, M. Hossain, K. Dhal, "Review on the advancements of DNA cryptography," *arXiv preprint arXiv:1010.0186*, 2010.

[3] A. Gehani, T. LaBean and J. Reif, "DNA-based cryptography", *Lecture Notes in Computer Science*, vol. 2950, pp. 167–188, Springer, 2003.

[4] A. Kahate, *Computer and Network Security*, Tata McGraw-Hill Publication Company Lited, Third Edition, 2013.

[5] A. Khalili, J. Katz, and W. Arbaugh, "Toward secure key distribution in truly ad-hoc networks," in *Proceedings of the IEEE Symposium on Applications and the Internet Workshops*, pp. 342–346, 2003.

[6] B. Roy, G. Rakshit, P. Singha, A. Majumder, D. Datta, "An improved symmetric key cryptography with DNA based strong cipher," in *International Conference on Devices and Communications (ICDeCom'11)*, pp. 1–5, 2011.

# 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.