A Hybrid Digital Signature Scheme on Dependable and Secure Data

Addepalli V. N. Krishna[1], Addepalli Hari Narayana[2], Somanchi Krishna Murthy[3]
(Corresponding author: Addepalli V. N. Krishna)

Department of Computer Science and Engineering, Christ University, Bangaluru, India[1]
(Email: adapalli.krishna@christuniversity.in)
Electrical Engineering, IIT-Indore, India[2]
Applied Mathematics Department, DIAT, Pune, India[3]
(Received Jan. 27, 2017; revised and accepted Mar. 1 & Apr. 4, 2017)

Abstract

In Digital Signature Standard Algorithm, a Discrete Logarithm Problem is used to calculate signature. The minimum Key length to be used is 1024 bit length. The work involves a Discrete Logarithm Problem computation, an Inverse and Modular operations at sender's side. At Receiver's side it involves two Discrete Logarithm Problem computations and modular operations which involves more computing resources as the key length needed is 1024 bit length In the present work, a Cubc Spline Curve based Public Key algorithm (CSCPKC) is used for Discrete Logarithm computation and the key length used is approximately 120 bit which needs less computing resources. It involves a secret matrix key to be shared among the participants which generates Random number sequence to be used in Signature generating algorithm. This model works well for a relatively small team of participants in having an Authentication process for Secured and Smooth data transfer with limited computing resource utilization.

Keywords: Cubic Spline Curve Public Key Cryptography; Digital Signature; Private Matrix Key; Random Number; Side Channel Attacks

1 Introduction

Digital Signature Algorithm consists of two numbers that contains values which are computed as per specified algorithm within parameters. This mechanism helps for authentication of users and also it verifies the integrity of the message. Digital signatures are generated through DSA and verified. Signatures are generated in association with Public and Private Keys. Thus each signatory has their own set of Public and Private keys which are used for Authentication process.

Any symmetric encryption scheme uses a private key for secure data transfer [20]. In their work on "A new Mathematical model on encryption scheme for secure data transfer [12]", the authors considered not only key but also time stamp and nonce values to increase the strength of sub key generated. In addition the nonce value can also be used for acknowledgement support between participating parties. The model can be further improved by considering a non linear model where the key values vary with the data generated [11].

Most of the products and standards that use public-key cryptography for encryption and digital signatures use RSA or D-H algorithm today [5]. Recently, Elliptic Curve Cryptography has begun to challenge RSA. The principal attraction of ECC, compared to RSA, is that it appears to offer better security for a smaller key size, thereby reducing processing overhead.

Some recent works on application of ECC are cited here. [2, 3] Explains the engineering of ECC as a complex interdisciplinary research field encompassing such fields as mathematics, computer science and electrical engineering. The work [18] deals with adoption of Knapsack algorithm on ECC and its added advantages lie more security in real time applications. [7] Specifies the standard specifications for public key cryptography. Encryption to data supports the very important features like security, Confidentiality to data & Authentication of users. [15, 17] discussed the features of Numerical data analysis which helps in building a mathematical model. In works [9, 10], the authors discussed a new public key algorithm which is based on Cubic Spline curve Public Key Cryptography (CSCPKC). They made a comparative study of Cubic Spline curve based cryptography with ECC algorithm in terms of Key length and computing resources. They also worked on different scalar operations on CSCPKC which forms the security of the proposed algorithm. In [8] the author discussed a new & simple algorithm which generates a random number sequence. The sequence is not a time bound algorithm but it depends on the vector being used in the algorithm. Thus in this algorithm it generates a random sequence which can be used in Digital signatures and which consumes low computing resources when compared to standard random number generator algorithms. [14] discusses the Standard Digital Signature Scheme approved by Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, USA. In work [6], the author deals with application of Cubic Spline Interpolation in cryptosystems using Choatic Mapping Concept and discussed the strengths against crypto analysis. In work [22], the authors represented the Cubic spline curve in terms of Symmetric encryption mechanism and its crypto analytical strength. The works [1, 13, 19, 21, 24] deals with Survey, Relevance and importance of DSA in authentication process. The works deals with application of Block ciphers or application of ECC on DSA and its improvements in authentication process.

2 Modelling of The Problem

The work may be divided to two parts. The first part deals with the generation of random number sequence. The second part deals with generation of Cubic Spline curve Public Key algorithm to be used in Digital signature for Authentication purpose.

Algorithm to Generate Random Sequence:

1) A random matrix is being used as a key. Let it be A.
2) Generate a Ternary vector for N values, i.e from 0 to $N-1$. Let this be B.
3) Multiply $A \times B$.
4) Consider a modulus function on the product of Step 3 by some prime number.
5) Convert the output of Step 4 to decimal which forms a random number generated sequence.

Modeling of Cubic Spline Curve Problem (CSCPKC Algorithm):

Global Parameters:

- T_1, T_N: The first and the last data points (Considering the problem as natural Spline);
- n: number of nodal points on the curve considered (Δx being defined by number of points considered on the cubic spline curve);
- G: Base Sequence considered;
- t: Number of iterations considered (which specifies Δt considered in the algorithm);

- K: Random number considered from Random number sequence generator algorithm;
- P: Field considered.

For the 2 point on the curve:

$$\begin{aligned} B(2) &= -\alpha\frac{\Delta t}{\Delta x^2} \bmod P \\ A(2) &= 1+2\alpha\frac{\Delta t}{\Delta x^2} \bmod P \\ D(2) &= Y(2)+\alpha\frac{\Delta t}{\Delta x^2}\times D(1) \bmod P. \end{aligned}$$

For the points 3 to $n-2$:

$$\begin{aligned} B(I) &= -\alpha\frac{\Delta t}{\Delta x^2} \bmod P \\ C(I) &= B(I) \\ A(I) &= 1+2\alpha\frac{\Delta t}{\Delta x^2} \bmod P \\ D(I) &= Y(I). \end{aligned}$$

For the $n-1$ point:

$$\begin{aligned} C(N-1) &= -\alpha\frac{\Delta t}{\Delta x^2} \bmod P \\ A(N-1) &= 1+2\alpha\frac{\Delta t}{\Delta x^2} \bmod P \\ D(N-1) &= Y(N-1)+(\alpha\frac{\Delta t}{\Delta x^2})\times D_N. \end{aligned}$$

These conditions imply that T_1 is known in terms of T_2. Thus the point 2 is a relation between T_1, T_2 & T_3. But since T_1 is known, this relation reduces to a relation between T_2 and T_3. This process of substitution can be continued until T_{n-1} can be formally expressed as T_n. But since T_n is known we can obtain T_{n-1}. This enables us to begin back substitution process in which T_{n-2}, T_{n-3}, $\cdots$, T_3, T_2 can be obtained for one iteration. Thus the problem is solved by Tridiagonal matrix algorithm and the process is repeated for 'i' iterations.

A New Hybrid Digital Signature Algorithm:

Consider a CBSPKC algorithm, with global parameters like G, P, Public key being PB, X be the Private Key, K be the random number considered from the Random sequence generator algorithm.

Sender's Signature:

1) Calculate $V = G^K \bmod P$.
2) Calculate $V_1 = V^x \bmod P$.

Receiver's Verification:

1) Calculate $R = PB^K \bmod P$, if $R = V_1$, then verified.
2) If Integrity of the message is also to be considered, G can be replaced with $G + H(m)$ where $H(m)$ represents the hash value of the message sent.

Example:

Random Number Generator:

$$\begin{aligned}
\text{For } n &= 0:80\\
n_1 &= floor(n/3);\\
r_1 &= n - n_1 \times 3;\\
n_2 &= floor(n_1/3);\\
r_2 &= n_1 - n_2 \times 3;\\
n_3 &= floor(n_2/3);\\
r_3 &= n_2 - n_3 \times 3;\\
r_4 &= n_3;\\
r &= [r_4\ r_3\ r_2\ r_1];\\
r &= r';\\
a &= [3\ 4\ 2\ \ -6;\ 4\ \ -5\ 2\ 6;\ 3\ \ -2\ 6\ 8;\ 6\ \ -3\ 2\ 8];\\
r &= modulo(a \times r, 3);\\
r &= r(4,1) + r(3,1) \times 3 + r(2,1) \times 9 + r(1,1) \times 27\\
\text{end}
\end{aligned}$$

Sequence generated is 0, 8, 4, 74,79, 75, 80, 78, 77, 74, 53, 49, 45, 7, 3, $\cdots$ which is random in nature.

Depending on the session participation, random number can be considered. For the given problem the session considered is 14, so the random number considered $(K) = 7$.

CSCPKC:

Boundary Conditions: Both sides maintained at known data values, i.e $T_1 = 4$, $T_N = 7$;

Global Parameters: G, T_1, T_N, α, Δx, Δt;

N**:** Ternary Vector of 81 values considered;

n**:** 11 points considered on the cubic spline curve;

K**:** Random number;

t**:** Private key;

P**:** Field;

PB**:** Public key, (G^t);

Global Parameters:

$$\begin{aligned}
\alpha &= 4, \Delta t = 3, \Delta x = 3, t = 5, T_1 = 4, T_n = 7;\\
G &= 4\ 6\ 23\ 8\ 8\ 25\ 8\ 6\ 6\ 11\ 7.
\end{aligned}$$

Generating Public Key from Private key:

- Private key: $t = 5$;
- Public key: $(G)^5 = PB = G_2$;
- $PB = G_2 = 4\ 32\ 9\ 33\ 16\ 1\ 17\ 6\ 19\ 32\ 7$.

Sender's Signature:

1) Calculate $V = G^K \bmod P$;

$$V = 4\ 26\ 10\ 35\ 13\ 39\ 18\ 24\ 13\ 3\ 7\ \ = G_1$$

.

2) Calculate $V_1 = V^x \bmod P$;

$$V_1 = 4\ 11\ 29\ 0\ 3\ 11\ 13\ 11\ 14\ 15\ 7 = G_3.$$

Receiver's Verification:

1) Calculate $R = PB^K \bmod P$, if $R = V_1$, then verified.
2) $R = 4\ 11\ 29\ 0\ 3\ 11\ 13\ 11\ 14\ 15\ 7 = V_1 = G_3$ (Hence proved).

Complexity:

Consider the equation,

$$A_B = G^x \bmod P$$

where g is the generator; P be the field. Thus if we go by the complexity of the discrete logarithm problem, it is of the order of $e^{((\ln P)^{1/3} \ln(\ln P))^{2/3}} \times O(n) \times O(N)$ where n refers to number of nodal point considered on the curve and N refers to size of Ternary vector considered.

3 Conclusion

The work deals with development of new digital signature algorithm which can be used in a limited environment. The main advantage with this mechanism is it consumes very less computing resources for authentication purpose. It provides a combination of Random number generator algorithm which needs a Matrix Private Key to be shared among the participants and CSCPKC algorithm for generating the sequence which can be mapped for Digital signature. The work may be extended to Digital Signature Standard algorithm which needs more complex construction and computing resources for authentication and verification.

References

[1] N. Barik, K. Sunil, "A study on efficient digital signature scheme for E-governance security", *Global Journal of Science & Technology*, vol. 2, no. 3, 2012.

[2] R. C. C. Cheng, N. J. Baptiste, W. Luk, P. Y. K. Cheung, "Customizable elliptic curve cryptosystems", *IEEE Transactions on VLSI Systems*, vol. 13, no. 9, pp. 1048–1059, 2005.

[3] A. Cilardo, L. Coppolino, N. Mazzocca, L. Romano, "Elliptic curve cryptography engineering", *Proceedings of the IEEE*, vol. 94, no. 2, pp. 395–406, 2006.

[4] Cryptography Stack Exchange, *Time Complexity to Solve Discrete Log Problem*, Apr. 29, 2017. (`http://crypto.stackexchange.com/questions/12893/time-complexity-to-solve-discrete-log-problem`)

[5] W. Diffie, "The first ten years of public key cryptography", *Proceedings of IEEE*, vol. 76, no. 5, pp. 560–577, 1988.

[6] F. Hwu, C. Y. Ho, *The Interpolating Random Spline Cryptosystem and the Chaotic-map Public-key Cryptosystem*, University of Missouri - Rolla, CSc-93-09, May 1993. (`http://cs.mst.edu/media/academic/cs/documents/technicalreports/93-09.pdf`)

[7] IEEE, *Standard Specifications for Public Key Cryptography*, IEEE Standard 1363, 2000.

[8] A. V. N. Krishna, "A new algorithm for Random number generation in network security", *Journal for Scientific & Industrial Research*, vol. 64, pp. 791–793, 2005.

[9] A. V. N. Krishna, H. Narayana, "A cubic spline curve public key cryptography", *accepted with Journal for Discrete Mathematical Sciences and Cryptography.*

[10] A. V. N. Krishna, H. Narayana, V. K. Madhura, "Window method based cubic spline public key cryptography", *International Journal of Electronics and Information Engineering*, vol. 4, no. 2, pp. 94–102, 2016.

[11] A. V. N. Krishna, "A new non-linear model based encryption scheme with time stamp & acknowledgement support", *International Journal of Network Security*, vol. 13, no. 3, pp. 202–207, 2007.

[12] A. V. N. Krishna, A. V. Babu, "A new model based encryption scheme with time stamp & acknowledgement support", *International Journal of Network Security*, vol. 11, no. 3, pp. 172–176, 2010.

[13] P. Kuppuswamy, P. M. Appa, S. Q. Y. Al-Khalidi, "A new efficient digital signature scheme algorithm based on block cipher", *IOSR Journal of Computer Engineering*, vol. 7, no. 1, pp. 47–52, 2012.

[14] NIST, *Digital Signature Standard (DSS)*, Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, MD 20899-8900, July 2013.

[15] Numerical Methods for Scientific and Engineering Computation, M.K.Jain, SRK Iyengar and RK Jain, New Age International Publishers.

[16] S. V. Patankar, *Numerical Heat Transfer and Fluid Flow*, McGraw Hill, 1980.

[17] R. Ramanna, *Numerical methods*, pp. 78–85, 1990.

[18] R. Ramasamy, R. A. Prabakar, M. I. Devi, M. Suguna, "Knapsack based ECC encryption and decryption", *International Journal of Network Security*, vol. 9, no. 3, pp. 218–226, 2009.

[19] S. Singh et al., "Survey on techniques developed using digital signature: Public key cryptography", *International Journal of Computer Applications*, vol. 117, no. 16, May 2015.

[20] W. Stallings, *Cryptography and Network Security*, Prentice Hall, 4th Edition, 2006.

[21] S. R. Subramanya, K. Byung, "Digital signatures", *IEEE POTENTIALS*, pp. 5–8, 2006.

[22] N. Sun, T. Ayabe, K. Okumura, "An animation engine with cubic spline interpolation", in *Proceedings of International Conference on Intelligent Information Hiding & Multimedia Signal Processing*, pp. 109–112, 2008.

[23] S. Yakoubov, V. Gadepally, N. Schear, E. Shen, A. Yerukhimovich, "A survey of cryptographic approaches to securing big-data analytics in the cloud", in *IEEE High Performance Extreme Computing Conference (HPEC'14)*, pp. 1–6, 2014.

[24] Q. Zhang, Z. Li, C. Song, "The improvement of digital signature algorithm based on elliptic curve cryptography", in *2nd International Conference on Artificial Intelligence, Management Science and Electronic Commerce (AIMSEC'11)*, pp. 1689–1691, 2011.

Biography

Addepalli V. N. Krishna, working as Professor, Computer Science & Engineering, Faculty of Engineering, Christ University, having 22 years of teaching Experience. He was involved with WASE Program (WIPRO academic Software Engineering) a Collaborative Program between Wipro Technologies & BITS, Pilani between 2004-2011.He has 28 papers published In Journals of national and international repute. His Areas of Interest are Cryptography, Data Modeling, Data Mining and presently guiding 3 Students for their Doctoral studies.

Addepalli Hari Narayana is studying Electrical Engineering, IIT, Indore. His areas of Interest are Digital Signal Processing, Microprocessors and cryptography.

Somanchi Krishna Murthy is working as Head, Associate Professor, Department of Applied Mathematics, DIAT, Pune. He has experience of around 18 yrs and published work in Journals and conferences of National and International repute. His areas of Interest are Mathematical Modeling, Cryptography and Advanced Reinforced Polymers.