A Study on Pairing Functions for Cryptography

B. Reddaiah, PhD
Assistant Professor
YSR Engineering College of
YOGI VEMANA UNIVERSITY
Proddatur, A.P, India

ABSTRACT
Now a day's every organization believes that the important asset in their organization is data. Secure data communication through network is needed as organizations tend to move data from one place to other place for business activities. In these situations variety of security mechanisms are needed to overcome security attacks. The range of security is based on diffusion of data and confusion. To achieve high security algorithms that are developed to protect data must be different in their structure. The use of special functions in the algorithms defines the strength of each algorithm. In this paper different types of pairing functions are discussed that has a unique nature of handling real numbers while processing. The pairing functions discussed have their own advantages and disadvantages which are also discussed in this work.

Keywords
Security mechanisms, Security attack, Cantor paring, Elegant pairing, Tate Pairing, Weil pairing.

1. INTRODUCTION
E-commerce is filed that is growing with a rapid speed in the field of computers and electronics. Every individual today is using the service provided by e-commerce than traditional one. Because of this companies are looking for security measures that provide security for their data as well as customer's data. As electronic business field is growing every day with greater pace and large number of secured applications are essential. From the olden days a systematic approach to protect data is Cryptography. This science has an elongated and attractive history [5]. This developed into a crucial element of modem systems [4]. In past Julius Caesar also designed encoding and decoding methods to transfer confidential armed forces information to officials [7].

Security provided by crypto systems is entirely based on functions build with mathematical operations. By using cryptography enciphering and deciphering text was started around 1900 BC when Egyptians first used a derivation of the standard hieroglyphics of the day to communicate [3]. The underlying principle is to hide the information from unauthorized people. To make this possible the original text is transformed into meaningless text to keep safe [2]. In order to change original text into meaningless text a strong mechanisms are needed. Information security is based on the encoding and decoding procedures and the strong point is the secret key [6]. Along with key a strong function in both algorithms is required to derive the meaningless text that cannot be easily broken. In this work different types of pairing cryptographic functions for elliptic curve cryptography with their advantages and disadvantages are discussed.

Modern cryptography begins from the works of Feistal at IBM during the later 1960's and early 1970's. Data Encryption Standards (DES) was implemented by NIST for encrypting uncategorized information in 1977. DES is now substituted by Advance Encryption Standards (AES) which is a new typical advancement. Later another milestone took place during 1978 with the development of RSA algorithm. RSA is the foremost fully developed public-key algorithm. This innovation answered the key exchange problems of cryptography. RSA also projected the world wide suitable standard practices like authentication and electronic signature in modern cryptography. In 1980's elliptic curve cryptography was more accepted due to its strength per bit contrast to existing public key algorithms. Elliptic curve cryptography is capable to generate superior security by means of key of small size.

This supremacy of elliptic curve cryptography over RSA resulted in efficient handling of bandwidth and speedy implementation. This property of elliptic curve cryptography made it extremely attractive in the area of cryptography. In 1993 chaotic cryptography was launched which acquires benefit of the multipart performance of chaotic dynamic systems to hide from view or cover information. Since then a lot of different implementations on this fundamental thought are proposed. The chaotic actions can be illustrated by its excessive sensitivity to early circumstances and it show the way to long term changeability.

In 2005 another concept in cryptography called policy based cryptography was formalized. This presents a framework for performing cryptography operations with respect to strategies formalized as monotone Boolean expressions presented in typical normal forms. A policy based encryption system permits enciphering of the message with respect to a policy in such a means that barely the policy objection users are capable to decipher the message. A policy is made of conjunctions and disjunctions of situations, where each situation is satisfied by a digital official document representing the signature of a particular official document issuer on a definite assertion. A user is thus obedient with a policy if and only if he has been issued a eligible set of recommendations for the policy. Policy based enciphering fit in to a promising relation of cryptographic systems. Policy supported cryptosystems have the capability allocation to join together encryption with credential supported right to use structures. This capability permits quite a few motivating applications in dissimilar circumstance but not limited to unaware access control, trust negotiation and cryptographic workflow.

An additional exciting part is quantum cryptography. This took place as a possible answer to the key founding problem, but the capacity has broadened significantly. Most of the present research focuses on experimental physics but the impact of the consequences might be considerable.

2. PRINCIPLES OF CRYPTOGRAPHY

Cryptography is essential to use in situations that demands privacy to protect data, trade secrets. For example business transactions, e-commerce and extramarital affairs. Every organization develops their own mechanisms to provide security for valuable information. These organizations use secure mechanisms through which sender and receiver can communicate with each other. The science of cryptography is divided into symmetric cryptography and asymmetric cryptography. Symmetric crypto systems have five ingredients such as plain text, encryption algorithm, key, cipher text and decryption algorithm. Whereas asymmetric crypto systems have six ingredients in which key is different from symmetric. Here key is in two forms as public key and private key. The strength of the encryption and decryption algorithms depends on the size of the key that is used to process.

In both symmetric and asymmetric crypto systems encryption procedures are applied to transform original message to meaningless text. Decryption procedure is applied to get back original message from meaningless text. These two algorithms stand as the backbone of the entire process in cryptography along with key. The processing of text to get other from is defined in these algorithms and these algorithms process the text to give other form. So it is up to the organizations to develop strong algorithms that process the text. The outcome of these systems is to achieve confusion and diffusion. The goal is to achieve more diffusion in the outcome text so that it makes unauthorized people feel difficult in getting the original information. A small change in the text should produce a great change in the outcome that may leads to confusion, so that the intended receiver of the message can receive the message securely.

Security is made possible in cryptography by using mathematical operations. Mathematics plays an important role in developing the security mechanisms to protect from security attacks from unauthorized people. Every function in crypto systems is based on these mathematical operations. Operations like addition, subtraction, OR, XOR etc. are used in building functions. By using these in different forms organizations build their functions to provide security. So, modern cryptography deeply stands on mathematical theory and computer science practice. Cryptographic algorithms are intended around computational hardness, hypothesis making such algorithms difficult to break in practice by any unauthorized person. To look at these it is possible to break them theoretically but it is infeasible to break them practically. Therefore these systems are computationally secure. Other than this cryptography supports mathematical functions. In this work mathematical pairing functions are discussed which can be used as a part of encryption and decryption algorithms.

3. MATHEMATCIS AS BACKDROP

Elliptic curves are being used in cryptography since 1985. This elliptic curve cryptosystems have a number of advantages above other systems. For instance, there is a large variety of parameters for a user to select from. Given any prime power $q = p^f$, ($p \neq 2, 3$), The elliptic curve over F_q by the equation can be described as

$$E: y^2 = x^3 + ax + b$$

where a and b in F_q are selected so that $4a^3 + 27b^2 \neq 0$. Another important aspect is that, elliptic curve cryptosystems can present the similar intensity of security when compared with other systems with a much lesser key length. This asset has made elliptic curve cryptography an increasingly well accepted. A point on the elliptic curve E is represented as an ordered pair (x, y) fulfilling E:y2=x3+ax+b. The coordinates x and y are elements of the finite field F_q. There is a method to "add" two points on an elliptic curve, and forever obtain one more point. There is in addition exceptional point indicated by ∞. The significant property of the point ∞ is that if P is any point on the curve E, then $P + \infty = P$.

A pairing is a function e that gets a pair of two points on an elliptic curve gives an element in a finite field as output.

$$e(P_1+P_2,Q)=e(P_1,Q)*e(P_2,Q),$$

where * represents multiplication in the finite field. Even though in theory pairings exist for any elliptic curve, when put into practice there are curves whose pairings that are inappropriate for crypto systems.

4. PAIRING FUNCTIONS

Pairing functions on elliptic curve cryptography is a very strong area for research in cryptography. Commercially importance for the pairing functions is growing every day because of its uniqueness and strength in providing security. Many companies are looking to use pairing functions in order to develop secure crypto systems. In 1991 for the first time pairings are used in cryptography. They used to attack certain elliptic curve cryptosystems that used super singular elliptic curves. So much of effort is being made on pairings to apply on cryptographic systems. Joux [10]. This work focused on one-round tripartite Di_e-Hellman protocol with pairings during 2000, and work by Barreto's `Pairing-Based Crypto Lounge' [8]. Pairings are now common and appropriate to many portion of cryptography. The popular pairing functions for crypto systems that are supported by elliptic curve cryptography are given below.

4.1 Cantor pairing Function

The Cantor pairing function has two forms of functions. It has a function for encryption algorithm and separate function for decryption algorithm. For encoding the message paring function is applied where as de-paring is applied in decoding to the message.

The Cantor pairing function is [1]

$$P(a, b) = ((a+b)^2+3a+b)/2 = N$$

The Cantor de-pairing function is

$$R = (\sqrt{8N + 1} - 1)/2;$$

where a - Text, b - Key, N - Integer value

$$a = N - (R*(R+1)/2);$$

$$b = ((R*(R+3))/2)-N;$$

The main strength of the Cantor pairing function in crypto systems is that it is simple to use and it is less complex while processing the text. This is best for smaller dimensional values.

Cantor paring function has its own set of drawbacks. In general paring functions are used for higher dimensional values. But in Cantor pairing function it is not possible to use large dimensional values, usually for triple ordered functions and more.

4.2 Elegant pairing Function

This is the pairing function that works on different dimensional values. The forms of this pairing function are elegant pairing for encryption and elegant un-pair for decryption.

Scheme of work (Elegant pairing)

Where x and y are non-negative integers, Elegant pair[x, y] outputs a single non-negative integer that is uniquely associated with that pair.

$$\text{Elegant Pair[x, y]} = \begin{cases} y^2 + x \;\; x \neq \max\,[x, y] \\ x^2 + x + y \;\; x == \max\,[x, y] \end{cases}$$

The inverse function elegant un-pair [Z] outputs the pair associated with each non-negative integer Z

Elegant un-pair

$$Z = \begin{cases} \{z - [\sqrt{z}]^2,\ [\sqrt{z}]\} & z - [\sqrt{z}]^2 < [\sqrt{z}] \\ \{[\sqrt{z}],\ z - [\sqrt{z}]^2 - [\sqrt{z}]\} & z - [\sqrt{z}]^2 \geq [\sqrt{z}] \end{cases}$$

The advantage of elegant pairing is that it can be used to process all kinds of integers. On the other side the disadvantage of this function is that it consumes time for computation.

4.3 Tate pairing Function

The Tate paring function is having its strength as bi-linearity in encoding and decoding the data. Further Tate pairing function is also non-degeneracy. The Tate paring function can be applied on two dependant points as trivial. This difficulty can be answered by means of distortion maps, recommended by Verheul [9]. The modified parings are also referred in Tate as distortion maps. Tate pairing function is bilinear and non-degenerate. Time utilization is an important problem in Tate so it is necessary to focus on speed up of the computations in Tate.

4.4 Weil pairing Function

As of Tate pairings Weil parings is also bi-linearity and non-degeneracy is required. So, Weil pairing function is bilinear and non-degenerate. Work is to be initiated on increasing the computational pace of the Weil pairing as it takes more time to process.

Modified pairings are used in most pairing-based cryptography like tripartite Diffie-Hellman [15], identity-based encryption [11], identity-based signatures [13, 14, 17], short signatures [12, 19], identity-based chameleon hash [18], and identification scheme [16]. Especially, a lot of pairing-based cryptographic functions need computing special values of modified Weil pairing [14, 17, 16, 18, 19].

5. CONCLUSION

In developing crypto systems different functions are used to increase the security to the data. The recent trend in cryptography is elliptical curve cryptography that is gaining its importance. This is because even though the size of the key is reduced pairing function produce good security. In other cases key management is becoming a difficult task. A detailed description is given on different paring functions that are supported by cryptography. Elliptical curve cryptography is also well discussed.

5.1 Future Scope

Future pairing functions can be improvised to provide better security and to increase the speed of computation of the functions.

6. REFERENCES

[1] B. Reddaiah, R Pradeep kumar Reddy, S. Hari Krishna "Enciphering using Bit–wise logical operators and paring function with text generated hidden key," IJCA (0975-8887), Vol. 121, No. 8, July 2015: pp. 30-35.

[2] P. P Charles & P. L. Shari, "Security in Computing: 4th edition", Prentice-Hall, Inc.,2008.

[3] S. Hebert, "A Brief History of Cryptography", an article available at http://cybercrimes.net/aindex.html

[4] A. S. Tanenbaum, "Modern Operating Systems", Prentice Hall, 2003.

[5] D. KHAN, "The Codebreakers", Macmillan Publishing Company, New York, 1967.

[6] Behrouz A. Forouzan, Cryptography and Network Security, Special Indian Edition, TATA McGraw Hill.

[7] S. William, Cryptography and Network Security: Principles and Practice, 2nd edition, Prentice-Hall, Inc., 1999 pp 23-50

[8] http://planeta.terra.com.br/informatica/paulobarreto/pblounge.html

[9] E. Verheul, "Evidence than super singular elliptic curve cryptosystems," Advances in Cryptology – Eurocrypt 2001, Lecture Notes in Computer Science 2045 (2001), pp.195-210.

[10] A. Joux, "A one-round protocol for tripartite Di_e-Hellman," Algorithm Number Theory Symposium { ANTS-IV, Lecture Notes on Computer Science 1838, Springer-Verlag (2000), pp. 385{394.

[11] D. Boneh, M. Franklin, "Identity-based encryption from Weil pairing," Advances in cryptology – Crypto 2001, Lecture Notes on Computer Science 2139, Springer-Verlag (2001), pp. 213-229.

[12] D. Boneh, B. Lynn, h. Shacham, "Short signatures from the weil pairing," Advances in cryptology – Asiacrypt 2001, Lecture Notes on Computer Science 2248, Springer-Verlag (2002), pp. 514-532.

[13] J. C. Cha, J. H. Cheon, " An Identity-Based Signature from Gap Diffie-Hellman Groups," Practice and Theory in Public Key Cryptography – PKC 2003, Lecture Notes on Computer Science 2567, Springer-Verlag (2003), pp. 18-30.

[14] F. He, "Efficient Identity Based Signature Schemes Based on Pairing," Selected Areas in Cryptography – SAC 2002, Lecture Notes on Computer Science 2595, Springer-Verlag (2003), pp. 310-324.

[15] A. Joux, " A one-round protocol for tripartite Diffie-Hellman," Algorithm Number Theory Symposium – ANTS-IV, Lecture Notes on Computer Science 1838, Springer-Verlag (2000), pp. 385-394.

[16] M. Kim, H. Kim, K. Kim, " A New Identification Scheme based on the Gap Diffie-Hellman Problem," 2002 Symposium on Cryptography and Information

security (SCIS2002), Shirahama, Japan, Jan. 29 – Feb. 1, 2003, vol. /2, pp. 349-352.

[17] K. G. Paterson, "ID-based signatures from pairings on elliptic curves," Electronics Letters 38(18) (200), pp. 1025-1026.

[18] F. Zhang, R. Safavi-Naini, W. Susilo, "ID-Based Chameleon Hashes from Bilinear Pairings," Cryptology ePrint Archive, Report 2003/208.

[19] F. Zhang, R. Safavi-Naini, W. Susilo, "An Efficient Signature Scheme from Bilinear Pairings and Its Applications," Practice and Theory in Public Key Cryptography – PKC 2004, Singapore(SG), March 2004, Lecture Notes on Computer Science 2947, Springer-Verlag (2004), pp. 277-290.

7. AUTHOR PROFILE

Dr. B. Reddaiah received Ph.D. degree in Computer Science and Engineering in the faculty of Engineering in 2015 from Acharya Nagarjuna University, Andhra Pradesh. He is working as Assistant Professor, Department of computer Science and Engineering, YSR Engineering College of Yogi Vemana University, Proddatur, Andhra Pradesh. His current research is focused on Software Engineering, Cryptography and Network Security and Digital Image Processing. He has published papers both in National & International Journals.

.