Secured Blinding Signature Protocol based on Linear Block Public Key Algorithm

Prakash Kuppuswamy
Computer Engineering & Networks Department
Jazan University, Jazan, KSA.

Saeed Q Y Al-Khalidi,
College of computer science & Information system,
Jazan University, Jazan, KSA.

ABSTRACT

Cryptography and Network Security is one of the most important and emerging research in academic and industry circles. Cryptography usage is a detailed design issue that is largely beyond the scope of the high-level algorithm description earlier. One obvious issue is key size. With many cryptography algorithms, the time it takes to crack a message varies directly with the size of the encryption key. This Research deals with a new cryptographic blinding signature protocol algorithm. The requirements for securing blind signature are privacy, authentication, integrity maintenance and non-repudiation. These are crucial and significant issues in recent times for E-voting which is transacted over the internet through e-commerce channels. A new method of security is suggested which is a based on block cipher algorithm.

Keywords

Public key, Private key, RSA blinding, Chaum’s blinding, signing, unblinding, inverse matrix.

1. INTRODUCTION

The concept of blind signatures was introduced by Chaum [1] as a method to digitally authenticate a message without knowing the contents of the message. A distinguishing feature of blind signature is their unlink ability: the signer cannot derive the correspondence between the signer process and the signature, which is later made public. This method, originally conceived for e-cash applications, was used by Fujioka etal[2]. Blind signature schemes have applications where the sender A (the customer) does not want the signer B(the bank) to be capable of associating a postiori a message m and a signature SB(m) to a specific instance of the protocol. This may be important in electronic cash applications where a message m might represent a monetary value which A can spend. When m and SB(m) are presented to receiver B for payment, B is unable to deduce which party was originally given the signed value. This allows sender A to remain anonymous so that spending patterns cannot be monitored.

Blind signature scheme needs an extensive list of security requirements. Without these security requirements, numerous opportunities for a widespread fraud and corruption may exist. In order to overcome these problems, an election should have the following requirements

- Authentication
- Privacy/confidentiality
- Integrity
- Non-repudiation

The main advantage of this new blind signature scheme is its rapidity, the Electronic Voting and e-cash process can make the contract easily and in well secured manner. The remainder of the paper is organized as follows: In Section 2, it has been described in brief the relative researches in public key security algorithm based on block cipher in the e-commerce industry. Section 3 provides the method and detailed steps on the proposed public key security algorithm. An implementation and the illustration are demonstrated in Section 4. In Section 5, the design of the experimental results and performance analysis is discussed. Finally conclusion offered in Section6.

2. RELATED WORKS

Blind signature schemes are two-party protocols between a sender A and a signer B. The basic idea is the following. A sends a piece of information to B which B signs and returns to A. From this signature, A can compute B’s signature on an a priori message m of A’s choice. At the completion of the protocol, B knows neither the message m nor the signature associated with it. The purpose of a blind signature is to prevent the signer B from observing the message it signs and the signature; hence, it is later unable to associate the signed message with the sender A. The blind signature protocol requires the following components:

1. A digital signature mechanism for signer B. SB(x) denotes the signature of B on x.

2. Functions f and g (known only to the sender) such that g(SB(f(m))) = SB(m). f is called a blinding function, g an unblinding function, and f(m) a blinded message.

Rivest, Shamir, Adlmen introduced RSA blinding signature Let n = pq be the product of two large random primes. The blinding function f : Zn –> Zn is defined by f(m) = m* k^e mod n and the unblinding function g : Zn –> Zn by g(m) = (k^{-1} * m) mod n. For this choice of f, g, and S_B, $g(S_B(f(m)))$ = $g(S_B(mk^e \bmod n)) = g(m^d k \bmod n) = m^d \bmod n = S_B(m)$, as a blind signature scheme[5].

David Chaum introduced Chaum’s blind signature protocol in 1983[1]. Blind signatures are typically employed in privacy-related protocols where the signer and message author are different parties.Cryptographic election systems (e-Vote), Digital cash schemes (e-Cash)[1]. A receives a signature of B on a blinded message. From this, A computes B’s signature on a message m chosen a priori by A, $0 \le m \le n - 1$. B has no knowledge of m nor the signature associated with m.

1. *Notation.* B’s RSA public and private keys are (n, e) and d, respectively. k is a random secret integer chosen by A satisfying $0 \le k \le n - 1$ and gcd(n; k) = 1.

2. *Protocol actions.*
a*) Blinding*- A computes $m^* = mk^e$ mod n and sends this to B.
b) *signing* B computes $s^* = (m^*)^d$ mod n which it sends to A.
c) *unblinding* A computes $s = k^{-1}s^*$ mod n, which is B’s signature on m.[4]

3. THE PROPOSED TECHNIQUE

One of the effective tools for ensuring the safety of blind signature scheme is the Public Key Infrastructures (PKI). It combines the digital signature and Hash function, which can be a public or a private is as acted its own.

The proposed method is very easy to adopt the coding of advanced language. Also it is very safe enough on the other side. RSA and Chaum's blind signature based algorithms are consumes a large amount of computing resources. For the above process, we are going to apply the new public key algorithm based on the linear block cipher or hill cipher.

3.1 Square matrix

Square matrix **A** = [a*ij*] of order n × n. Its n components a*ii* form the main diagonal, which runs from top left to bottom right. The cross diagonal runs from the bottom left to upper right. In New algorithm, we are choosing square matrix for the purpose of perfect calculation of det of matrix and invertible matrix, which we can use at the time of Encrypting the plain text *[5]*.

3.2 Inverse of a matrix

An inverse of a function, usually written as $f^{-1}(x)$, is a reflection of the original function, f(x), around the line y = x. Basically, every x value is changed to a y value and every y value is change to an x value *[5]*.

3.3 Modular function:

(a +b) mod n = [(a mod n) + (b mod n)] mod n…......…*(1)*
(a-b) mod n = [(a mod n) – (b mod n)] mod n…....…..*(2)*
(a * b) mod n = [(a mod n) x (b mod n)] mod n ....…...*(3)[7]*.

New proposed algorithm
i) Blinding m^{*}=(m • k • e) mod n
ii) Signing s^{*} = (m^{*} • d mod n) mod n
iii) Unblinding S=(s^{*} •k^{-1}) mod n

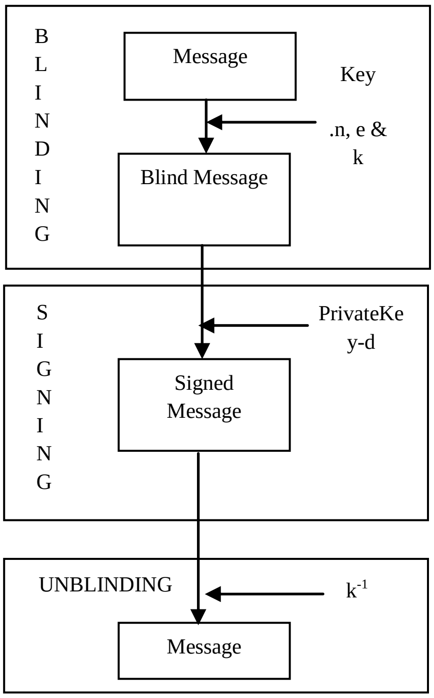

Fig. 1 Proposed blinding signature architecture

4. IMPLEMENTATION

In order to provide quick and simple blinding scheme, the size of linear matrix key has to be chosen effectively. For blinding small amount of data has been taken, there should not be any overhead to the encrypting system as well as there should not be any compromise on the security level.

Select Square matrix = $\begin{pmatrix} 3 & 2 \\ 3 & 4 \end{pmatrix}$

Finding inverse of matrix
C_{11} $[-1]^{1+1}$ x [4] = $[-1]^{2}$ x [4] = 4
C_{12} $[-1]^{1+2}$ x [3] = $[-1]^{3}$ x [3] = -3
C_{21} $[-1]^{2+1}$ x [3] = $[-1]^{3}$ x [2] = -2
C_{22} $[-1]^{2+2}$ x [4] = $[-1]^{4}$ x [3] = 3

$$-6 * \begin{pmatrix} 4 & -2 \\ -3 & 3 \end{pmatrix} \text{ mod } 37= \begin{pmatrix} -24 & 12 \\ 18 & -18 \end{pmatrix} \text{ mod}37= \begin{pmatrix} 13 & 12 \\ 18 & 19 \end{pmatrix}$$

Now we have
Let us select e = $\begin{pmatrix} 13 & 12 \\ 18 & 19 \end{pmatrix}$ and d = $\begin{pmatrix} 3 & 2 \\ 3 & 4 \end{pmatrix}$

And select random integer k=5 and k^{-1}=15
(Verification 5*15 mod 37 =1)

Now assume message is 'HE' i.e (8,5)

4.1 Blinding procedure

Blinding m^{*}=(m • k • e) mod n

$$.m = \begin{pmatrix} 8 \\ 5 \end{pmatrix} * \begin{pmatrix} 13 & 12 \\ 18 & 19 \end{pmatrix} *5 \text{ mod } 37 = \begin{pmatrix} 6 \\ 11 \end{pmatrix}$$

Now public key's are n =37 and e=$\begin{pmatrix} 13 & 12 \\ 18 & 19 \end{pmatrix}$and random integer =5

4.2 Signing procedure

Signing s^{*} = (m^{*} • d mod n) mod n

$$s^{*} = \begin{pmatrix} 6 \\ 11 \end{pmatrix} * \begin{pmatrix} 3 & 2 \\ 3 & 4 \end{pmatrix} \text{ mod } 37 = \begin{pmatrix} 3 \\ 25 \end{pmatrix}$$

4.3 Unblinding procedure

Unblinding S=(s^{*} • k^{-1}) mod n

$$S= \begin{pmatrix} 3 \\ 25 \end{pmatrix} * 15 \text{ mod } 37 = \begin{pmatrix} 45 \\ 375 \end{pmatrix} \text{mod } 37= \begin{pmatrix} 8 \\ 5 \end{pmatrix}$$

5. RESULT ANALYSIS

We proposed a linear block cipher or hill cipher prototype blinding scheme that implements security protocols that meet the security requirements of an blinding signature scheme. With this system, Electronic Voting and e-cash systems are operating. Blinding signature scheme is the universal verifiability since the public can verify the election results and e-cash with the help of the blinding signature scheme.

Then performance of new blinding method comparing with existing methods i.e. RSA and Chaum's blinding scheme. In figure2 showing the result of the blinding procedure, in figure3 shows the results of the signing procedure and figure 4 shows the result of the unbliding procedure with the sample of 100 characters as a message. The overall percentage of all the three blinding scheme given in the figure5, which can be shows better understanding of each individual blinding scheme performance.

The blinding signature scheme executes on PC computer of CPU Intel Pentium 4, 2.2 MHz Dual Core. The programs implemented using MATLAB. It is tested with messages and with different text of 100 characters.

Table 1. Comparison of blinding Scheme

Protocol	Blinding	Signing	Unblinding
RSA Blinding method	12 Sec.	10 Sec.	11Sec.
Chaum's blinding	10 Sec.	8 Sec.	10 Sec.
New proposal	12 Sec.	6 Sec.	9 Sec.
No. of characters 100			

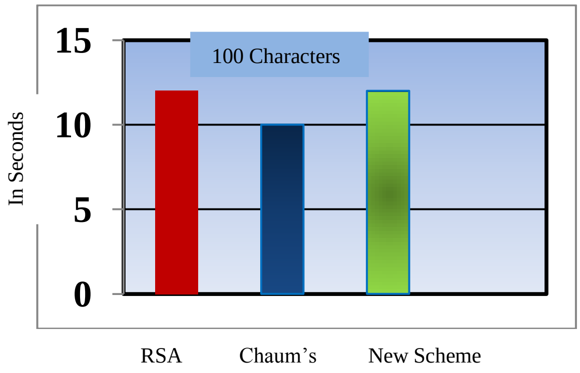

Fig. 2 Blinding performance

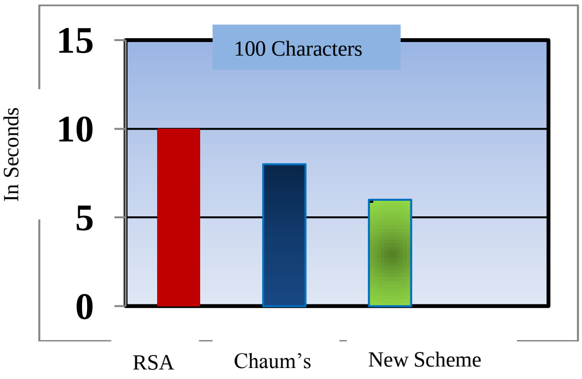

Fig. 3 Signing performance

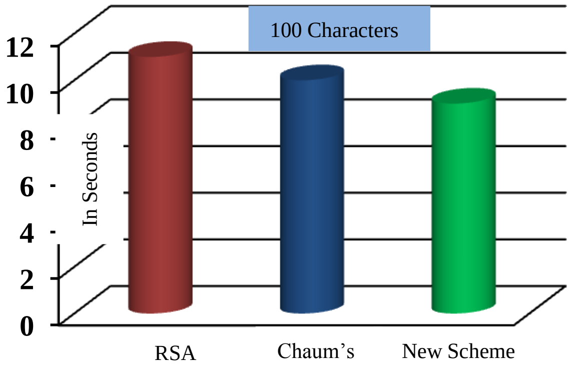

Fig. 4 Unblinding performance

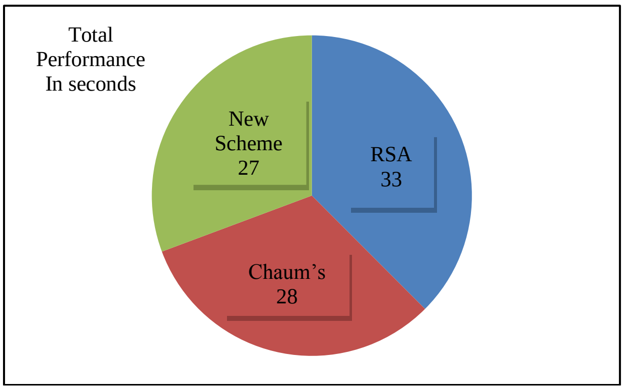

Fig. 5 Comparision of blinding scheme performance

6. CONCLUSIONS

The extensive research works in the area of cryptographic algorithms are expecting to produce more secured protocol for protecting the many data scheme. Especially, Security requirement is one of the most important goals for protocol system security designers. In the proposed paper, it has been designed for securing blinding signature scheme by using public key algorithm which is based on linear block cipher technique. The proposed method is used in many applicable areas such as e-cash and electronic voting system in secured approach. Also it will ensure the confidentiality, integrity and authentication. It has been tested the algorithm for various sizes of messages and parameters. The experimental results shows that the proposed method is improved the interacting performance, while providing high quality of security service for desired blinding signature protocol scheme.

Several points can be concluded from the experimental results. It has been concluded that the proposed method consumes least encryption time (computing time) and others has taken maximum time in encryption for same amount of the data.

7. REFERENCES

[1] Chaum.D, "Blind Signature for Untraceable Payments".Crypto'82, Springer-Verlag, pp.199-203,1983.

[2] A.Fujioka,T.Okamato and K.ohta. "A Practical Secret Voting Scheme for Large Scale Elections" AUSCRYPT'92,LNCS 1163,Springer-Verlag,pp. 125-132,1997.

[3] Nidhi Gupta, Praveen Kumar and Satish Chhokar, "A Secure Blind Signature Application in E Voting", Proceedings of the 5th National Conference -2011, New Delhi.

[4] A. Menezes, P. van Oorschot and S. Vanstone, "Handbook of Applied Cryptography" by CRC Press, 1996.

[5] David A. Santos, Linear Algebra Notes, January 2, 2010 Revision, dsantos@ccp.edu.

[6] Prakash Kuppuswamy, Dr.C. Chandrasekar, "Enrichment of Security through Cryptographic Public key Algorithm Based on Block cipher", IJCSE, ISSN : 0976-5166 Vol. 2 No. 3 Jun-Jul 2011 PP 347-355.

[7] Anoop MS, Public Key Cryptography Applications Algorithms and Mathematical Explanations, Tata Elxsi Ltd, India, anoopms@tataelxsi.co.in

[8] Prakash Kuppuswamy, Dr.Wajeb Gharibi, "Securing data using 4 variable linear block Asymmetric key Algorithm", IJCDS, ISSN: 2278-5183, Vol.No.1, Issue 3, October 2012.

[9] A. Baraani, J. Pieprzyk, R. Safavi, "A Practical Electronic Voting Protocol Using Threshold Schemes", Centre for Computer Security Research, Department of Computer Science, University of Wollongong, Australia, May 1994.

[10] J. Benaloh, D. Tuinstra, "Receipt-Free Secret-Ballot Elections", Clarckson University, 1994.

[11] J. Benaloh and M. Yung, "Distributing The Power Of A Government To Enhance The Privacy Of Votes", in Proc. of the 5th ACM Symposium on Principles of Distributed Computing, pages 52-62, August 1986.

[12] J. D. Cohen, M. J. Fischer, "A Robust And Verifiable Cryptographically Secure Election Scheme", in 26th Annual Symposium on Foundations of Computer Science, IEEE, pages 372-382, October 1985.

[13] J. Padhye, V. Firoiu, and D. Towsley, "A stochastic model of TCP Reno congestion avoidance and control," Univ. of Massachusetts, Amherst, MA, CMPSCI Tech. Rep. 99-02, 1999.

[14] Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification, IEEE Std. 802.11, 1997.

AUTHOR'S PROFILE

Prakash Kuppuswamy Lecturer, Computer Engineering & Networks Department in Jazan University, KSA He is research Scholar proceeding in 'Dravidian University'. He has published 12 International Research journals/Technical papers and participated in many international conferences in Rep. of Maldives, Libya and Ethiopia. His research area includes Cryptography, Bio-informatics and Network algorithms.

Dr. Saeed Q. Y. Al-Khalidi, Vice-Dean of College of Computer Sciences and Information Systems, Jazan University. He published many National & International papers, Journals. Also, he participated as a Reviewer in many international conferences worldwide. He completed Master Degree and Doctor of Philosophy in University of East Anglia. His research interests include: Information System development, approaches to systems analysis and the early stages of systems development process, IT/IS evaluation practices, E-readiness assessment.