International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:7, No:7, 2013

Implementation of RSA Blind Signature on CryptO-0N2 Protocol

Esti Rahmawati Agustina and Is Esti Firmanesa

***Abstract*—**Blind Signature were introduced by Chaum. In this scheme, a signer can "sign" a document without knowing the document contain. This is particularly important in electronic voting. CryptO-0N2 is an electronic voting protocol which is development of CryptO-0N. During its development this protocol has not been furnished with the requirement of blind signature, so the choice of voters can be determined by counting center. In this paper will be presented of implementation of blind signature using RSA algorithm.

***Keywords*—**Blind signature, electronic voting protocol, RSA algorithm.

I. Introduction

THE schemes of digital signature allows someone to sign document in such way that everyone can verify the validity of authentic signatures, but no one can forge signatures of new documents [1]. Digital signature mechanism implement cryptographic features such us hash function and asymmetric algorithm (using private key and public key). Fig. 1 shows digital signature scheme [2].

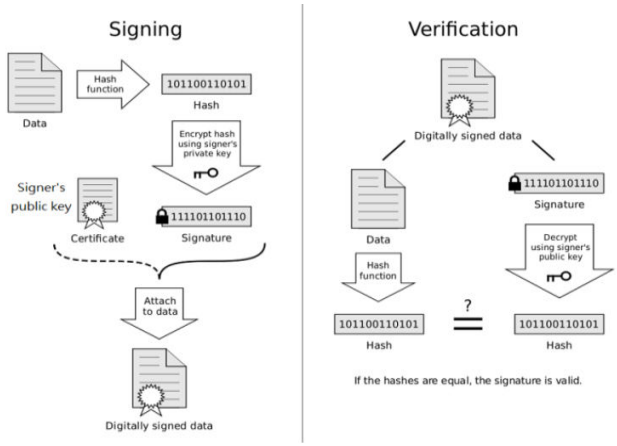

Fig. 1 Digital signature scheme

Blind Signature is one of the scheme of digital signature that was proposed by Chaum. In this mechanism, the document will be "blind" before signing in order to signer does not know content of document. Using of the blind signature can we found at activities or transaction that require anonymity function; for example digital cash schemes (e-cash) and cryptographic election system (e-voting). On e-voting, one of the system requirements is any ballot was approved by the authorities such us the tabulation center or election committee before the ballot have been calculated. This allows the authorities to check the voters and make sure voters are allowed to vote, and they do not put more than one vote. However, the tabulation center / election committee shall not know the choice of the voters so that the e-voting system required blind signature mechanism.

CryptO-0N2 is secure ubiquitous e-voting protocol [3]. This protocol support the Indonesia's election principle, which is *LUBER JURDIL* (direct, common, free, confidential, honest and fair). CryptO-0N2 implement the cryptographic features such hash function and RSA algorithm that use public key and private key. During its development, this protocol has not been furnished by blind signature for support anonymity.

This paper will presented the implementation of RSA blind signature on CryptO-0N2 protocol. The remainder of this paper is organized as follows. In Section II we describe our previous research about CryptO-0N2 protocol. Section III we overview the RSA algorithm, RSA blind signature protocol, and CryptO-0N2 protocol. In Section IV we describe the implementation of RSA blind signature scheme on CryptO-0N2 protocol while Section V we analyze the security after its implementation. We conclude in Section VI.

II. Previous Works

Our secure e-voting research was started at 2009 [4]. This first research focus on creating e-voting protocol and its implementation into a prototype of e-voting but the analysis has not been used common analysis method for protocol yet. We just analyze the protocol property in order to resistant with certain attack. In [3] we develop CryptO-0N (an early form of CryptO-0N2). This development focuses on characteristic CryptO-0N in order to be secure ubiquitous e-voting. Its mean voting can be done whenever, wherever, and however. In [5] and [6] we analyze CryptO-0N use logic approaches that are BAN logic and Boyd and Mao logic. In [7] we develop the successor of CryptO-0N protocol that is CryptO-0N2 protocol. The difference between previous and successor protocol is system infrastructure. The last protocol used client server system. In [8] we implement Virtual Private Network (VPN) for improve security network of e-voting. In [9] we develop kiosk e-voting system and implement certificate digital for improve the security of key storage, and also change one of the protocol property that is PIN (Private Identity Number) with iNum (identification Number).

Esti Rahmawati Agustina and Is Esti Firmanesa are with the National Crypto Agency, Jalan Harsono RM No 70, Pasar Minggu, South Jakarta, DKI Jakarta, Indonesia (corresponding author to provide phone: +62 7805814; fax: +62 78844104; e-mail: esti.rahmawati@lemsaneg.go.id, isesti.firmanesa@lemsaneg.go.id).

III. Preliminaries

A. RSA Algorithm

Ron Rivest, Adi Shamir, and Leonard Adleman introduced a new cryptographic algorithm, RSA in 1978. RSA is the most widely used public key cryptosystem. It may be used to provide both secrecy and digital signature. Its security is based on the intractability of the integer factorization problem [10].

B. Key Generation for RSA

Each entity creates an RSA public key corresponding private key.

1. Generate two large random (and distinct) primes and q, each roughly the same size.
2. Compute $n = pq$ and $\phi = (p-1)(q-1)$
3. Select a random integer e, $1 < e < \phi$, such that $gcd(e, \phi) = 1$
4. Compute the unique integer d, $1 < d < \phi$, such that $ed \equiv 1(mod\ \phi)$
5. Public key is (n, e), private key is d

C. Encryption

Entity who will encrypts a message m should do the following:

1. Obtain authentic public key (n, e)
2. Represent the message m in the interval$[0, n-1]$
3. Compute $c = m^e\ mod\ n$
4. Send the ciphertext c

D. Decryption

To recover plaintext m from c should do the following:
Use the private key d to recover $m = c^d\ mod\ n$

E. Formulation of RSA Algorithm

Table I shows formulation of this algorithm.

TABLE I
Formulation of RSA Algorithm

Formulation	Characteristic
p, q	secret
$n = p.q$	not secret
$\phi\ (n) = (p-1)(q-1)$	secret
$e\ (encryption\ key)$	no secret
$d\ (decryption\ key)$	secret
$m\ (plaintext)$	secret
$c\ (ciphertext)$	not secret

F. RSA Blind Signature Protocol

The RSA blind signature protocol as follow [2].

1. Each voter generates message m contain her/his votes.
2. Choose random number r for blinding factor, that is relatively prime to n
3. Use public key of authorities signature, e, and compute $m' \equiv mr^e\ (mod\ n)$
4. Voters send m' to signature authorities.
5. Authorities signature will sign m', $s' \equiv (m')^d\ (mod\ n)$, send s' to voters.
6. Voters will unblinding s' to get original message m and message that has been signed that is $(m)^d$. The computation as follows.

$s \equiv s' * r^{-1}\ (mod\ n)$. Because $r^{ed} = r$, so:
$\equiv (m')^d r^{-1}\ (mod\ n)$
$\equiv (m')^d r^{-1}\ (mod\ n)$
$\equiv (m')^d r^{-1}\ (mod\ n)$
$\equiv (mr^e)^d r^{-1}\ (mod\ n)$
$\equiv m^d r^{ed} r^{-1}\ (mod\ n)$
$\equiv m^d r r^{-1}\ (mod\ n)$
$\equiv m^d\ (mod\ n)$
Send m^d to Center Tabulating Facilities (CTF)

G. CryptO-0N2 Protocol [9]

CryptO-0N2 protocol consists of two processes. Firstly, authentication process and secondly voting process. Fig. 2 represents this protocol.

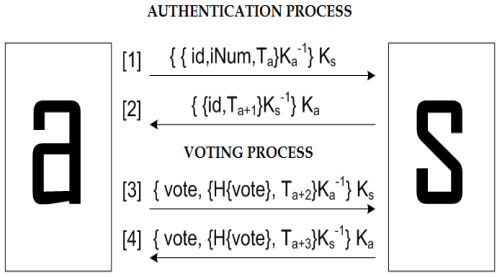

Fig. 2 CryptO-0N2 protocol scheme

TABLE II
Protocol Properties

Symbols	Means
a	Polling station
s	e-voting server
id	Voter's identity
$iNum$	Identification number
T_a	Timestamps
K_a	Public key a
K_s	Public key s
$K_a{}^{-1}$	Private key a
$K_s{}^{-1}$	Private key s
$vote$	Voter's vote
$H(vote)$	Hash function of vote

Authentication and voting process is as follows:

1. Polling station will send message to e-voting server that contains voter's identity, identification number, and timestamp. These three properties was signed used polling station's private key, then encrypted used e-voting server's public key.
2. e-voting server accept the first message, decrypting the message with e-voting server's private key, and then decrypting again with polling station's public key to verify the that the message actually came from polling station. Verification also carried out by checking the voter's identity of the database voters. If the verification is success the e-voting server send message to polling

station that contain voter's identity, timestamp plus 1. These two properties was signed used e-voting server's private key and then encrypted used polling station's public key.

This message sends to polling station.

3. Polling station accepts the second message. After getting the voter's identity as sign of success verification, voters will vote and polling station will send third message to e-voting server that contain vote, hash function of vote, and timestamp plus 2. This three properties was signed used polling station's private key, then encrypted used e-voting server's public key.
4. e-Voting server accept the third message, decrypting the message with e-voting server's private key, and then decrypting again with polling station's public key to verify the that the message actually came from polling station. The hash function of vote use to verify that vote was not modified by adversary. Then, e-voting servers center the vote for tabulating.

For printing the ballot, e-voting server will send fourth message to polling station that contain vote, hash function of vote and timestamp plus 3. This three properties was signed used e-voting server's private key and then encrypted used polling station's public key

Timestamp was used for freshness message assurance.

IV. Implementation

According to Section III, CryptO-0N2 protocol consists of two processes, authentication and voting. Authentication means verify the voters and voting means sending the vote. RSA blind signature was implemented on second process that is step 3 and 4.

Step 3: $\{vote, \{H(vote), T_{a+2}\}{K_a}^{-1}\}K_s$

Step 4: $\{vote, \{H(vote), T_{a+3}\}{K_s}^{-1}\}K_a$

The implementation is as follows.

TABLE III
Implementation of RSA Blind Signature

Step	Polling station		e-voting server (first server) for authentication
3	• Generates message that contain *vote.* • Choose random number r for blinding factor, that is relatively prime to n • Use public key of e-voting server (first server), e, and compute $vote' \equiv vote \,.r^{K_s} \,(mod\ n)$ • Send $vote'$ with others property on step 3 of CryptO-0N2 protocol, so step 3 change to be $\{\{vote', T_{a+2}\}{K_a}^{-1}\}K_s$	→	
4			• Decrypting the message and get $vote'$ • Sign $vote'$ with first server's private key, $sign(vote') = (vote')^{{K_s}^{-1}} \,mod\, n$ • Send $sign(vote')$ with others property on step 4 of CryptO-0N2 protocol, so step 4 change to be $\{\{sign(vote'), T_{a+3}\}{K_s}^{-1}\}K_a$
	• Decrypting the message and get $sign(vote')$ • Unblinding $sign(vote')$ to get ${vote}^{{K_s}^{-1}}$. The computation as follows. $sign(vote') \equiv (vote')^{K_a}\ (mod\ n)$ $\equiv (vote.r^{K_s})^{{K_s}^{-1}}\ (mod\ n)$ $\equiv vote^{{K_s}^{-1}} \,.\, r^{K_s{K_s}^{-1}}\ (mod\ n)$, with $r^{K_s{K_s}^{-1}} \equiv r$ $\equiv vote^{{K_s}^{-1}} \,.r\ (mod\ n)$ $vote^{{K_s}^{-1}} \equiv vote^{{K_s}^{-1}} \,.r\ (mod\ n).\ r^{-1}(mod\ n)$	←	

According to common blind signature scheme that needs two servers. This protocol also needs two servers for supporting voter's anonymity. They are authentication and tabulating server. Second server must have public and private key that is ${K_t}^{-1}$ for private key and K_t for public key. The voting tabulation is as follows:

TABLE IV
IMPLEMENTATION OF RSA BLIND SIGNATURE (CONTINUED)

Step	Polling station	e-voting server (second server) for tabulating
5	• Send $vote^{K_s{}^{-1}}$ with timestamp, sign with polling station's private key and encrypting with server;s public key. $\{\{vote^{K_s{}^{-1}}, H(vote^{K_s{}^{-1}})\} K_a{}^{-1}\}K_t$ →	• Decrypting the message and get $vote^{K_s{}^{-1}}$ then use authentication server's public key that is K_s for getting $vote$

This implementation led to step change in the CryptO-0N2 protocol. The new steps are as follows (Fig. 3).

Step 1.$\{id, iNum, T_a\}K_a{}^{-1}\}K_s$

Step 2.$\{id, T_{a+1}\}K_s{}^{-1}\}K_a$

Step 3.$\{\{vote', T_{a+2}\}K_a{}^{-1}\}K_s$

Step 4.$\{\{sign(vote'), T_{a+3}\}K_s{}^{-1}\}K_a$

Step 5.$\{\{vote^{K_s{}^{-1}}, H(vote^{K_s{}^{-1}})\}K_a{}^{-1}\}K_t$

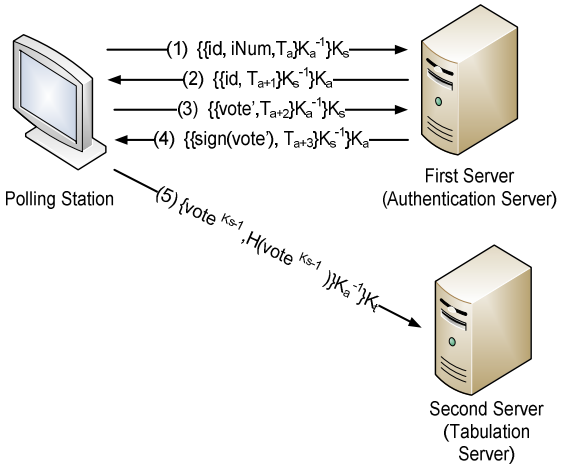

Fig. 3 CryptO-0N2 protocol scheme with RSA implementation

V. PROTOCOL ANALYSIS

The strengthness of CryptO-0N2 protocol implements RSA blind signature according to the strengthness of RSA algorithm. A blind signature schemes must meet two requirements that is blindness and non-forgeability characteristics. The analysis follows that requirement.

A. Blindness

Blindness characteristic on CryptO-0N2 protocol scheme use RSA algorithm will protect voter, in order to her/his vote cannot known by other entities, such us authentication server. This server just get blindness message that is *vote'*. And also the second server, tabulating center will not know the relationship between voter and his/her vote. The implementation of RSA blind signature meets this requirement.

B. Non-Forgeability

Non-forgeability characteristic on CryptO-0N2 protocol scheme use RSA algorithm will protect center tabulating from voter's fraud that can generate *vote* without signed from first server that is authentication server. Signing the *vote* can only be done by the authentication server using private key ($K_s{}^{-1}$). This private key is known only to the authentication server.

VI. CONCLUSION

CryptO-0N2 protocol with RSA blind signature implementation meets the requirement of blind signature scheme, which are blindness and non-forgeability.

Based on common blind signature scheme that needs two servers, this protocol also needs two servers for supporting voter's anonymity. That is authentication and tabulating server. RSA blind signature implementation cause additional step on CryptO-0N2 protocol.

REFERENCES

[1] Ari Juels, M.Luby and R. Ostrovsky, "*Security of Blind Siganture* (Extended Abstract)," in Burton S. Kaliski Jr., editor, Advanced in Cryptology – CRYPTO 97, vol. 1294 of Lecture Notes in Computer Science, Santa Barbara, CA, USA, August 17 – 21: Springer, Berlin, Germany, 1997, pp. 150 – 164.

[2] Rong-Jaye Chen, "*Blind Signature and Their Application*", http://people.cs.nctu.edu.tw/~rjchen/Crypto2010/Blind_Signature.pdf last access 20 April 2013.

[3] E.R. Agustina, P.Y. Prakasa, *CryptO-0N: Protocol Solution for Secure Ubiquitous e-Voting, CryptO-0N: Solusi Protokol untuk Secure Ubiquitous e-Voting (Translation Proceeding), Seminar Riset Teknologi Informasi (SRITI),2009.*

[4] P.Y Prakasa, I. Budiarso, E.R. Agustina, *Secure e-Election Application by Utilizing Cryptographic Function and Fingerprint Technology for Supporting e-Democracy, Aplikasi Secure e-Election dengan Memanfaatkan Fungsi Kriptografi dan Teknologi Fingerprint untuk Mendukung e-Democracy (Translation Proceeding), Seminar Nasional Informatika UPN Veteran Jogjakarta, 2009.*

[5] P.Y Prakasa, Z. Suhardono, E.R Agustina, *Logic Approach Analysis of CryptO-0N Protocol, Analisis Pendekatan Logic pada Protokol CryptO-0N (Translation Journal),InfoKripto, 2012.*

[6] E.R. Agustina, P.Y. Prakasa, B. Smith, "*Analysis of CryptO-0N Protocol using Boyd and Mao Logic Approach*,"2011, unpublished.

[7] P.Y. Prakasa, "*Application Engineering Secure e-Voting with CryptO-0N2 Protocol Implementation for Electronic Election, Rancang Bangun Aplikasi Secure e-Voting dengan Implementasi Protocol CryptO-0N2 untuk Pemilihan Umum Elektronis*", Tesis Magister Universitas Gunadarma, 2012.

[8] P.Y. Prakasa, E.R. Agustina, *Security Optimization System Secure e-Voting for Supporting Electronic Election, Optimalisasi Keamanan Sistem Secure e-Voting untuk Mendukung Pemilihan Umum Elektronik (Translation Journal), Jurnal Sandi, 2012.*

[9] P.Y. Prakasa, E.R. Agustina, *KIOSK Electronic Voting with Certificate Digital Implementation for Supporting Electronic Election Security, KIOSK Electronic Voting dengan Implementasi Sertifikat Digital untuk Pengamanan Pemilihan Umum Elektronis, 2013, submitted for publication.*

[10] A.J. Menezes, P.C van Oorschot, S.A Vanstone, *Handbook of Applied Cryptography (Book Style), CRC Press. Boca Raton,* 1997.