# Cryptanalysis on An E-voting Scheme over Computer Network

Baoyuan Kang

*Abstract*— **An electronic voting system makes it possible for the voters to cast their ballots over the computer network.Hence, voters can participate in elections without having to go to the polling places, which is more convenient and efficient. To design a practical voting scheme, Mu and Varadharajan proposed an anonymous secure electronic voting scheme to be applied over the network in 1998. However, Lin et al. showed that Mu and Varadharajan's scheme has a weakness. That is, voters can successfully vote more than once without being detected. To avoid this weakness, Lin et al.proposed a modified scheme. But, Recently, Hwang et al. showed that the Lin et al.'s modification allows the Authentication Server to identify the voters of published tickets so that voters will lose their privacy. Furthermore, they proposed an improved scheme to solve this problem and enhance the security. Unfortunately, this paper shows that Hwang et al.'s scheme has same weakness with Lin et al.'s scheme, that is, the Authentication Server can identify the voters of published tickets.**

*Index Terms*— **Electronic Voting, Cryptography, Blind Signature, ELGamal Public Key Cryptosystem.**

## I. Introduction

WITH the rapid development of computer network, the internet has become a necessity in many people's daily life. More and more routine works are handled electronically, and voting is no exception. In 1981, Chaum[1] first proposed the electronic voting system. An electronic voting system enables voters to perform electronic voting over computer network. In other words, people can cast their ballots at any time and in any place if people can access the network.Mobility and convenience are the most important properties which make electronic voting become more and more popular. However, a secure e-voting system should satisfy the following requirements:

(1) **Anonymity of voter.** No one can identify the voter of a cast ticket.
(2) **Unforgeability of ticket.** No one can generate a forged ticket to cheat the authority.
(3) **Perceptibility of double voting.** All double voting tickets will be detected and eliminated by the authority.

Mu and Varadharajan[2] have proposed an electronic voting system in 1998. Mu and Varadharajan's scheme is based on the EIGamal digital signature algorithm and is suitable for large-scale elections. Although in Mu and Varadharajan's scheme some integers 's inverse must be computed, but this difficulty can be easily overcomed [11]. Furthermore, compared with other schemes [3,4,5,6, 7,8], only Mu and Varadharajan's scheme can detect the illegal voters. However, Lin et al. [9] showed that the Mu and Varadharajan's scheme does not provide the perceptibility of double voting. This is, if a voter votes twice, the authority cannot detect the double voting tickets. Lin et al. then proposed a modified scheme to solve this problem. Unfortunately, Hwang et al. [10] showed that the authority has the ability to identify the owners of the cast tickets in the Lin et al.'s scheme. Therefore, the Lin et al.'s scheme cannot satisfy the requirement of anonymity of voter and thus is not able to protect the privacy of voters. Hwang et al. proposed an improved scheme to solve this problem. However, this paper shows that the Hwang et al.'s improved scheme has the same weakness with the Lin et al.'s scheme. Namely, the authority has the ability to identify the owners of the cast tickets in hwang et al.'s scheme.

The rest of this paper is organized as follows. In section 2, we will review the hwang et al.'s e-voting scheme. The weakness of Hwang et al.'s scheme is showed in section 3. Finally, some conclusions are made in section 4.

Baoyuan Kang is with the School of Mathematical sciences and Computing Technology,Central South University, Chang'sha,Hunan, 410075,China.
e-mail: (baoyuankang@yahoo.com.cn).

978-0-7695-3336-0/08 $25.00 © 2008 IEEE
DOI 10.1109/CSSE.2008.1345

IEEE computer society

## II. Review of Hwang et al.'s e-voting scheme

In this section, we describe the Hwang et al.'s electronic voting scheme. The Hwang et al.'s electronic voting scheme consist of the following participants:Voters(V), an Authentication Server(AS),Voting Servers(VS), a Ticket Counting Server(TCS), and a Certificate Authority(CA). For convenience, some useful notation is defined below:

- $(e_x, n_x), d_x$: the RSA public/private key pair of participant x.
- $Cert_x$: the public-key certificate of participant $x$, which is signed by CA.
- $p$: a large prime number, which is a public system parameter.
- $g$: $g \in Z_p^*$ is a public system parameter.
- $h$: $h \in Z_p^*$ is a public system parameter,$h \neq g$.
- $\|$: the operation of concatenation.

The Hwang et al.'s scheme works in three phases: the voting ticket obtaining phase, the voting and tickets collecting phase, and the tickets counting phase. These phases are described as follows.

### A. The voting ticket obtaining phase

(1) A voter $V$ chooses two blind factors $b_1$ and $b_2$ as well as two random numbers $k_1$ and $r$. Then, $V$ computes $w_1.w_1'$, $w_2.w_2'$ by using the following equations:
$w_1 = g^r b_1^{e_{AS}}$ mod $n_{AS}$
$w_1' = h^r b_1^{e_{AS}}$ mod $n_{AS}$
$w_2 = g^{k_1} b_2^{e_{AS}}$ mod $n_{AS}$
$w_2' = h^{k_1} b_2^{e_{AS}}$ mod $n_{AS}$
After that, $V$ sends
$\{V, AS, Cert_V, t, w_1, w_1', w_2, w_2', ((w_1 \parallel w_1' \parallel w_2 \parallel w_2' \parallel t)^{d_V}$ mod $n_V\}$ to AS, where $t$ is a timestamp.

(2) AS first verifies the validity of the timestamp $t$ and the certificate $Cert_V$ and then use $Cert_V$ to verify the signature$(w_1 \parallel w_1' \parallel w_2 \parallel w_2' \parallel t)^{d_V}$ mod $n_V$. If all verifications are successful, AS chooses a unique random number $k_2$ and computes:

$$\begin{aligned}
w_3 &= (k_2 \parallel t)^{e_V} mod n_V \\
w_4 &= (w_1 \times AS)^{d_{AS}} mod n_{AS} \\
&= (a_1 \times AS)^{d_{AS}} \times b_1 mod n_{AS} \\
w_5 &= (w_1' \times AS)^{d_{AS}} mod n_{AS} \\
&= (a_2 \times AS)^{d_{AS}} \times b_1 mod n_{AS} \\
w_6 &= (w_2 \times g^{k_2} \times AS)^{d_{AS}} mod n_{AS} \\
&= (y_1 \times AS)^{d_{AS}} \times b_2 mod n_{AS} \\
w_7 &= (w_2' \times h^{k_2} \times AS)^{d_{AS}} mod n_{AS} \\
&= (y_2 \times AS)^{d_{AS}} \times b_2^2 mod n_{AS}
\end{aligned}$$

where $a_1 = g^r$, $a_2 = h^r$, $y_1 = g^{k_1+k_2}$, and $y_2 = h^{2k_1+k_2}$. Then, AS delivers the messages $\{AS, V, w_3, (w_4 \parallel w_5 \parallel w_6 \parallel w_7 \parallel t)^{e_V}$ mod $n_V\}$ to $V$. Note that AS also records $k_2$ along with $V$'s identity in its database.

(3) $V$ decrypts $w_3$ to obtain $k_2$. Thus, $V$ can calculate $y_1$ and $y_2$ by using $g$, $h$, $k_1$, and $k_2$. In addition, $V$ also computes the signature $s_1$, $s_2$, and $s_3$ by the following equations:
$s_1 = w_4 \times b_1^{-1} = (a_1 \times AS)^{d_{AS}}$ mod $n_{AS}$
$s_2 = w_5 \times b_1^{-1} = (a_2 \times AS)^{d_{AS}}$ mod $n_{AS}$
$s_3 = w_6 \times b_2^{-1} = (y_1 \times AS)^{d_{AS}}$ mod $n_{AS}$
$s_4 = w_7 \times b_2^{-2} = (y_2 \times AS)^{d_{AS}}$ mod $n_{AS}$

(4) $V$ applies the EIGamal digital signature scheme to sign the voting content m. Let $y_1$ and $y_2$ be the public keys of the ELGamal Cryptosystem, and $x_1 = k_1 + k_2$ and $x_2 = 2k_1 + k_2$ be the corresponding private keys, such that $y_1 = g^{k_1+k_2}$ mod $p$ and $y_2 = h^{2k_1+k_2}$ mod $p$. $V$ generates two signature $(a_1, s_5)$ and $(a_2, s_6)$ of the voting content $m$ by using the following equation:
$s_5 = x_1^{-1}(ma_1 - r)$ mod $p - 1$
$s_6 = x_2^{-1}(ma_2 - r)$ mod $p - 1$
Then $V$ can obtain the voting ticket as
$T = \{s_1 \parallel s_2 \parallel s_3 \parallel s_4 \parallel s_5 \parallel s_6 \parallel a_1 \parallel a_2 \parallel y_1 \parallel y_2 \parallel m\}$.

### B. The voting and tickets collecting phase

(1) $V$ send the voting ticket $T$ to $VS$

(2) $VS$ verifies the validity of $a_1, a_2, y_1$ and $y_2$ by checking the following equations:
$AS \times a_1 =?s_1^{e_{AS}}$ mod $n_{AS}$
$AS \times a_2 =?s_2^{e_{AS}}$ mod $n_{AS}$
$AS \times y_1 =?s_3^{e_{AS}}$ mod $n_{AS}$
$AS \times y_2 =?s_4^{e_{AS}}$ mod $n_{AS}$
If the above equations hold, $VS$ further verifies the signature $(a_1, s_5)$ and $(a_2, s_6)$ of the voting content $m$ by checking the following equations:
$g^{ma_1} =?y_1^{s_5} \times a_1$ mod $p$
$h^{ma_2} =?y_2^{s_6} \times a_2$ mod $p$
If both verifications succeed, $VS$ stores $T$ in its database.

(3) After the voting time expires, $VS$ sends all the collected tickets to $TCS$.

### C. The tickets counting phase

Upon receiving all tickets from the Voting Servers, $TCS$ first detects the double voting tickets. $TCS$ checks $y_1, y_2, a_1$ and $a_2$ for every ticket to see whether they have been repetitively used. If these parameters appear in more than one ticket, then a double voting is detected. Moreover, if the voter uses the same parameters to sign different voting contents, $TCS$and $AS$ can cooperate to find the malicious voter as follows. Assume that $TCS$ discovers a voter using the same parameters $y_1, y_2, a_1$ and $a_2$ to sign two different voting contents $m$ and $m'$. Then $TCS$ can calculate
$x_1 = \frac{m'a_1 - ma_1}{s'_5 - s_5}$ mod $p-1$
$x_2 = \frac{m'a_2 - ma_2}{s'_6 - s_6}$ mod $p-1$
$k_1 = x_2 - x_1 = (2k_1 + k_2) - (k_1 + k_2)$
$k_2 = x_1 - k_1$
Finally, $TCS$ can identify the malicious voter by searching $AS$'s database to find out which voter is associated with the unique random number $k_2$.

mds

## III. Cryptanalysis on Hwang et al.'s scheme

Hwang et al. claimed that the anonymity of the voters is guaranteed bacause a voter can obtain an anonymous ticket from $AS$ by using the blind signature technique. However, this section shows that $AS$ can identify the owner of a cast ticket by some computation. Suppose $TCS$ has published all cast tickets and $AS$ wants to trace the owner of the ticket $T = \{s_1 \parallel s_2 \parallel s_3 \parallel s_4 \parallel s_5 \parallel s_6 \parallel a_1 \parallel a_2 \parallel y_1 \parallel y_2 \parallel m\}$. Then $AS$ can perform the following procedure:

(1) Since,
$s_5 = x_1^{-1}(ma_1 - r)$ mod $p-1$
$s_6 = x_2^{-1}(ma_2 - r)$ mod $p-1$
When multiplying $s_6$ and $s_5$ to both sides of these two equations respectively, we obtain
$x_1 s_5 s_6 = (ma_1 - r)s_6$ mod $p-1$
$x_2 s_5 s_6 = (ma_2 - r)s_5$ mod $p-1$
Then,
$(x_2 - x_1)s_5 s_6 = ((ma_2 - r)s_5 - (ma_1 - r)s_6)$ mod $p-1$.
But, $k_1 = x_2 - x_1$. So, when $s_5^{-1}$ and $s_6^{-1}$ exist (if $gcd(s_5, p-1) = gcd(s_6, p-1) = 1$, $s_5^{-1}$ and $s_6^{-1}$ exist. In the large-scale election, $s_5^{-1}$ and $s_6^{-1}$ can be computed with significant probability) following equation holds.
$k_1 = ((ma_2 - r)s_5 - (ma_1 - r)s_6)s_6^{-1}s_5^{-1}$ mod $p-1 = (ma_2 - r)s_6^{-1} - (ma_1 - r)s_5^{-1}$ mod $p-1$.
This implies,
$g^{k_1} = (g^r)^{s_5^{-1} - s_6^{-1}} g^{m(a_2 s_6^{-1} - a_1 s_5^{-1})}$ mod $p$
$h^{k_1} = (h^r)^{s_5^{-1} - s_6^{-1}} h^{m(a_2 s_6^{-1} - a_1 s_5^{-1})}$ mod $p$
Notice that,
$g^r = a_1$, $h^r = a_2$.
Hence,
$u = g^{k_1} = a_1^{s_5^{-1} - s_6^{-1}} g^{m(a_2 s_6^{-1} - a_1 s_5^{-1})}$ mod $p$
$v = h^{k_1} = a_2^{s_5^{-1} - s_6^{-1}} h^{m(a_2 s_6^{-1} - a_1 s_5^{-1})}$ mod $p$

(2) Select a record $(V', k'_2)$ from the database and check
$u \times g^{k'_2} =?y_1$
$v^2 \times h^{k'_2} =?y_2$
If the above equations hold, then output $V'$ and stop the procedure.

(3) Repeat step 2 until every record in the database has been searched.

Since all published tickets must be valid(because $VS$ checks the validity of the tickets in the voting and tickets collecting phase), this procedure can always succeed in finding out the voter of a vote. therefore, the Hwang et al.'s scheme cannot protect the anonymity of the voters.

## IV. Conclusion

This paper has shown that the Hwang et al.'s enhanced e-voting scheme has the same weakness with Lin et al.'s e-voting scheme, that is, the identities of voters of cast tickets can be traced by the Authentication Server.

# References

[1] D.Chaum, *Untraceable electronic mail, return addresses and digital pseudonyms*, Communications of the ACM 24(1981) 84-88.

[2] Y.Mu, V. Varadharajan, *Anonymous secure e-voting over a network*,proceedings of the 14th Annual Computer Security Applications Conference, ACSAC'98,1998,pp.293-299.

[3] D.Chaum, *Elections with unconditionally secret ballots and disruption equivalent to breaking RSA*, Advances in Cryptology, EUROCRYPT'88 (1988) 177-182.

[4] L. Cranor, R. Cytron, *Sensus: a security-conscious electronic polling system for the internet*, Proceedings of the Thirtieth Hawaii International Conference on system sciences, vol.3,1997, pp.561-570.

[5] G.Dini, *Electronic voting in a large-scale distributed system*, Networks 38 (2001) 22-32.

[6] A. Fujioka, T. Okamoto, K. Ohta, *A practical secret voting scheme for large-scale elections*, Advances in cryptology, AUSCRYPT'92, Lecture Notes in Computer Science 718 (1993) 244-251.

[7] C.L.Lei, C.I. Fan, *A universal single-authority election system*, IEICE Transactions on Fundamentals E81-A (10) (1998) 2186-2193.

[8] I. Ray, N. Narasimhamurthi, *An anonymous electronic voting protocol for voting over the internet*, Proceedings of Third International workship on Advanced Tssues of E-Commerce and Web-based Information System, San Juan, CA, 2001, pp.188-190.

[9] I.-C.Lin, M.-S. Hwang, C.-C. Chang, *Security enhancement for anonymous secure e-voting over a network*, Computer Standards and Interfaces 25 (2)(2003)131-139.

[10] S.-Y.Hwang, H.-A.Wen, T. Hwang, *On the security enhancement for anonymous secure e-voting over a network*, Computer Standards and Interfaces 27(2005)163-168.

[11] R.-H. F, O.-A. Daniel, G.-Z. Claudia,*Yet another improvement over the Mu-Varadharajan e-voting protocol*, Computer Standards and Interfaces 29(2007)471-480.