Multi-authority E-voting System Based on Group Blind Signature

http://dx.doi.org/10.3991/ijoe.v11i9.5072

Haibin Wang[*1], Xia Liu[2], Sheng Zhao[1], Lina Huo[2]
[1] Xingtai Polytechnic College, Xingtai, Hebei, China
[2] Xingtai University, Xingtai, Hebei, China

***Abstract*—Targeting at some problems such as the control of a single authority and guarantee of privacy of multi-authority, this paper proposes a double-blind multi-authority e-voting system based Ghadafi's group blind signature and SP-signature. By introducing multi-authority, this paper solves the control problem of a single authority. By using the SP-signature, voters cannot vote for others. The new system voter can protect confidentiality of voting information and the privacy of authority. Finally, the security of the new e-voting system is analyzed which includes eligibility, privacy, universal verifiability, uncoercibility, unreusability and fairness.**

***Index Terms*—E-voting system, Groth-Sahai proof, Group blind signature, Multi-authority, SP-signature.**

I. INTRODUCTION

Election and voting are the reflection of democracy of a country. And the electronic voting system is an important tool for fair voting. It includes three voting modes: traditional voting, electronic voting and network voting. Traditional voting costs time and labor, and has high error probability. Network voting is seldom used because of the insecurity of network. Electronic voting is widely used because it is secure and saves time and energy.

Due to the importance of electronic voting, many scholars have conducted researches on it. Chaum [1]first introduced the concept of electronic voting. In 2011, Philip et al. [2]constructed an multi-authority electronic voting system in which the identity of authority was not confidential. In 2011, Okediran et al. [3]constructed a electronic voting system framework open to several authorities whose identities were public. The areas voters belonging to could be known, which weakens the privacy of voters. In 2012, Olusola et al. [4] summarized the basic concepts of electronic voting system, depict the development of electronic voting and concludes the characteristics ofelectronic voting system. In 2013, Shubhangi et al. [8] built a safe electronic voting system (simply called "e-voting system" in the following) by homomorphic technology. But there is only one authority in this system. Thus the voting result could be easily controlled by the authority.

From the above analysis, it can be known that e-voting system is either single-authority or multi-authority. The voting result is easily controlled in the former, but the identity of authority is public in the latter, which leaks part of voters' information and damages a certain privacy of voters. Based on Ghadafi's group blind signature agreement and Abe's structural signature, this paper constructs a multi-authority and double-private e-voting system to guarantee both the reliability of voting result and the identity of authority so as to protect voters.

This paper proposes the basic definitions in chapter 2, constructs e-voting system in chapter 3, analyzes the security of new system in chapter 4 and gives the summary in chapter 5.

II. BASIC DEFINITIONS

Definition 1: Bilinear Pairings. Bilinear pairings is a map satisfying the following conditions. Definition $\hat{e}: G_1 \times G_2 \to G_3$, where G_1、G_2 and G_3 is a p multiplicative cyclic group, and p is prime number ; g and h are generators of $G_1$and G_2.

a) (Bilinear) if $\forall x \in G_1$, $y \in G_2$ and $a, b \in Z_p^*$, than $\hat{e}(x^a, y^b) = \hat{e}(x, y)^{ab}$;
b) (Non-degeneration) $\hat{e}(g, h) \neq 1$;
c) (Computability) e is a calculable polynomial time.

Definition 2 SXDH Problem[9] if $(p, G_1, G_2, G_3, e, g, h)$ are a prime number order group, where p is prime number ; g and h are generators of $G_1$and G_2, and $\hat{e}: G_1 \times G_2 \to G_3$. SXDH (Symmetric External Diffe-Hellman) problem means DDH problem is difficult on $G_1$and G_2.

If are given, the advantageAdv_A^{DDH} for attackers to judge $c = ab$ can be neglected, which means DDH is difficult on G_1. Similarly, if $g_2, g_2^{a_2}, g_2^{b_2}, g_2^{c_2} \in G_2$are given, the advantage$Adv_A^{DDH}$ for attackers to judge $c_2 = a_2 b_2$ can also be neglected which means DDH is difficult on G_2,

Definition 3: SFP Problem [10] SFP (Simultaneous Flexible Pairing Assumption) problem is: if $g_z, h_z, g_r, h_u \in G_1, (a, a_2), (b, b_2) \in G_1 \times G_2$ are given, $R_j = (z, r, s, t, u, v, w)(j = 1, \cdots, q)$ are randomly selected to define that attacker Acan find $z^*, r^*, st^*, u^*, v^*, w^*$ and the advantage to satisfy $\hat{e}(a, \tilde{a}) = \hat{e}(g_z, z)\hat{e}(g_r, r)\hat{e}(s, t)$ and $\hat{e}(b, \tilde{b}) = \hat{e}(h_z, z)\hat{e}(h_u, u)\hat{e}(v, w)$,$u)e(v, w)$ is Adv_A^{SFP} $(z^* \neq 1, z^* \neq z \in R_j)$.

In polynomial time, Adv_A^{SFP} can be neglected.

Definition 4 (SP Signature) The validation key, message and signature of SP (Structure-Preserving Signature) [10] are bilinear group elements. The verification equation of the above elements is bilinear product equation. This signature can resist the adaptation message attack, as follows:

Key generation:

if $g_r, h_u \in G_1, \gamma_i, \delta_i, \gamma_z, \delta_z, \alpha, \beta \in Z_p^*$, $\in Z_p^*$ are given, calculate $g_i = g_r^{\gamma_i}, h_i = h_u^{\delta_i}$, $g_z = g_r^{\gamma_z}, h_z = h_u^{\delta_z}$ and use $Extend()$ to calculate $\{a_i, b_i\}_{i=0}^1$ and $\{c_i, d_i\}_{i=0}^1$ then $vk = (g_z, h_z, g_r, h_u, \{a_i, b_i, c_i, d_i\}_{i=0}^1)$, $g_i = g_r^{\gamma_i}, h_i = h_u^{\delta_i}, g_z = g_r^{\gamma_z}, h_z = h_u^{\delta_z}, \{a_i, \tilde{a}_i\}_{i=0}^1 \leftarrow \text{Extend}(g_r, \tilde{g}^{\alpha}), \{b_i, \tilde{b}_i\}_{i=0}^1 \leftarrow \text{Extend}(h_r, \tilde{g}^{\beta})$ $vk, \gamma_z, \delta_z, \alpha, \beta, \{\gamma_i, \delta_i\}_{i=0}^1)$.

Signature: for $\{m_i\}_{i=1}^n$ of G_1, randomly select $\zeta, \rho,$ $\zeta, \rho, \theta, \varphi, \omega \in Z_p$ to calculate $z = g_1^{\zeta}, r = g_1^{\alpha-\rho\theta-\gamma_z\zeta} \prod_{i=1}^k m_i^{-\gamma_i}$, $z = \tilde{g}^{\zeta}, r = \tilde{g}^{\alpha-\rho\theta-\gamma_z\zeta} \prod_{i=1}^k m_i^{-\gamma_i}, s = g_r^{\rho}, t = \tilde{g}^r, u = \tilde{g}^{\beta-\varphi\omega-\delta_z\zeta} \prod_{i=1}^k m_i^{-\delta_i}, v = h_u^{\varphi}, w = \tilde{g}^{\omega}$ g_1^{ω}. And signature is $\sigma = (z, r, s, t, u, v, w)$, simply as $\text{SPSign}(m)$.

Verification: check $e(a_0, b_0)e(a_1, b_1) = e(g_z, z)e(g_r, r)$ $e(s, t)\prod_{i=1}^k e(g_i, m_i)$ and $e(c_0, d_0)e(c_1, d_1) = e(h_z, z)$ $\hat{e}(b_0, \tilde{b}_0)\hat{e}(b_1, \tilde{b}_1) = \hat{e}(h_z, z)\hat{e}(h_u, u)\hat{e}(v, w)\prod_{i=1}^k \hat{e}(h_i, m_i)$ If they are equal, the verification of signature is valid.

Definition 5 GS Certification [9] The certification of non-interactive zero-knowledge in relative bilinear group equations is given in standard model. It is suitable for various bilinear group element in group equation, including: bilinear product equation, scalar multiplication equation and quadratic equation. This paper just introduces the bilinear product equation under the SXDH hypothesis, as follows,

$\mathcal{X}_1, \cdots, \mathcal{X}_n, \mathcal{A}_i \in G_1, \mathcal{Y}_1, \cdots, \mathcal{Y}_n, \mathcal{B}_i \in G_2, t_3 \in G_3, \gamma_{i,j} \in Z_n$ $G_3, \gamma_{i,j} \in Z_n$ are given, and the bilinear equation is listed in the following.

$\prod_{i=1}^n \hat{e}(\mathcal{A}_i, \mathcal{Y}_i) \bullet \prod_{i=1}^m \hat{e}(\mathcal{X}_i, \mathcal{B}_i) \bullet \prod_{i=1}^m \prod_{j=1}^n \hat{e}(\mathcal{X}_i, \mathcal{Y}_j)^{\gamma_{i,j}} = t_3$

$x_1, \mathrm{L}\ , x_n, y_1, \mathrm{L}\ , y_n \in Z_p$ are variates. In order to verify that the variates satisfy the above bilinear equation, GS commitment has to be made first, that is, $GScom(\mathcal{X}_1), \cdots, (y_n)$ $GScom(\mathcal{X}_n), GScom(\mathcal{Y}_1), \cdots, GScom(\mathcal{Y}_n)$, simply as $C_{\mathcal{X}_1}, \cdots, C_{\mathcal{X}_n}, C_{\mathcal{Y}_1}, \cdots, C_{\mathcal{Y}_n}$. Then bilinear product equation is used for certification. Finally, the certifier send variate commitment and the relative certification to verifier, and verifier can prove whether the given variates can satisfy bilinear equation.

Definition 6 Group Signature [11] Ghadafi has constructed a group signature in 2013 to protect not only the correctness of message but also the privacy of signers. The specific group signature process is as follows:

Join the agreement: by using SP signature in Definition 4, signers can acquire signature certificate, the group manager saves the corresponding certificates and public key.

Group Signature: a user selects $g_r, h_u \in G_1, \gamma_i, \delta_i, \gamma_z, \delta_z, \alpha, \beta \in Z_p^*, G_2$, and M_1 and M_2 is the signed message. Calculate $Q_1 = g_1^q, Q_2 = g_2^q, Co = T^q \cdot M_1$ to give the corresponding zero-knowledge certification ψ, and send (Co, ψ) to the signer; then the signer select $r, c \in Z_p^*$, to calculate:

$H = (K \cdot T^r \cdot Co)^{1/(s+c)}, C_1 = F^c, C_2 = g_2^c, R_1^{'} = g_1^r$, $R_2^{'} = g_2^r$. Here s is the secret key for the signer. If $\sigma = (H, C_1, C_2, R_1^{'}, R_2^{'})$, calculate the group signature of M_1 and M_2 Ω, and then send $(R_1^{'}, R_2^{'}, \Omega)$ to the user. Finally the user verify the group signature Ω. If it is correct, calculate $R_1 = R_1^{'} \cdot Q_1, R_2 = R_2^{'} \cdot Q_2$ to get the final group signature Ω_1, simply recorded as $GGBS(M)$.

III. ELECTRONIC VOTING SYSTEM

Electronic voting system consists of four participants: the trusted third party TTP, group manager GM, voter U_i and authority AU. The trusted third party is responsible for extracting the voter who repeats voting; the group manager is in charge of the participation of authority and the counting of voting; voters are the one who conduct voting; the authority is in charge of collecting ballots from voters in one area. There is one authority in one area. He is in charge of collecting the ballots from voters in this area and then hand them over to the group manager. The group manager is responsible for the whole voting statistics. If there is voter who repeats voting, the group manager will send him to the trusted third party who will recover the identity of the repeat voter.

A. Basic Parameters

In the following, there are the basic parameters for multi-authority voting system. λ is the safety parameter, G_1, G_2 and G_3 are the prime numbers of p. Authority generates two pairs of public and secret keys (sk_i, pk_i) and (ssk_i, spk_i). The first pair of public and secret key is used to send out the certificates of voting. The send pair is used to sign the first pair to generate the certificate of authority. The group manager generates his own public and secret key pair (sk_{GM}, pk_{GM}). Voters generate their own public and secret key pair (sk_{U_i}, pk_{U_i}) which is used to prevent repeated voting and signing and sending voter's own ballot to avoid others' forging voters' own ballots. The trusted third party generates commitment and decommitment pair (ck_{TTP}, ek_{TTP}).

B. Join the Agreement

The agreement allows the legal authority join in the group and he can acquire the certificate from the group manager and uses it to send voting qualification to voters, as follows:

(1) Authority → Group Manager: authority selects $sk_i = s_i \in Z_p^*, pk_i = (S_1 = g_1^s, S_2 = g_2^s)$ and gene5rates SP signature $sig_i = SPSign(pk_i)$, and sends sig_i, pk_i to the manager;

(2) Group Manager → Authority: group manager verifies the public key of the authority to judge whether the authority is the legal regional manager and whether he will be granted the certificate. If one of the condition can not be satisfied, the agreement will terminate; or the group manager divide pk_i into (S_1, S_2) to judge whether SP blind signature is correct. If it is not, the agreement terminates; or he will use his own private key and use SP blind signature to generate the authority's public key pk_i into signature σ_i, and finally the group manager send certificate σ_i to the authority.

(3) Authority: the authority judges whether the certificate is correct, and if it is not, the agreement will terminate; or saves his own certificate σ_i.

C. Register the Agreement

This agreement allows voters to register to their regional authority to obtain the right to vote. Only the registered users have the right to vote. The agreement is as follows:

(1) Voter → Authority: a voter chooses a random number $S \in Z_p^*$, and uses the commitment key given by the trusted third party to generate a commitment of the random number C_S and the corresponding certificate π_S, and then sends C_S, pk_{U_i}, π_S to the authority.

(2) Authority → Voter: the authority verifies the correctness of π_S and the qualification of the voter (such as age). If one of them is not correct, the agreement will terminate; or the authority generates the voter's commitment into a group blind signature $GGBS(C_S)$.

(3) Voter: the voter verifies the correctness of the group blind signature. If it is not correct, the agreement will terminate; or the voter obtains the $GGBS(C_S)$ of the random number's commitment.

D. Voting Agreement

This agreement allows voters to vote for authority. In order to avoid other voters pretending this voter to vote, the voter generates SP signature for his ballot. It is not mandatory because SP signature cannot be forged. The randomization proved by Groth-Sahai commitment and zero-knowledge can be used to randomize $GGBS(C_S)$ (the commitment of random number, the certification of corresponding correctness and group blind signature) into $GGBS'(C_S)$ in order to protect the group blind signature from being linked, as follows:

(1) Authority → Voter: the authority chooses a random number $R \in Z_p^*$ which guarantees the freshness of the user's vote to make the electronic voting system non-repeatable.

(2) Voter → Authority: the information of the user U_i 's vote can be marked as P. In order to avoid the authority knowing what the users vote before the end of voting, U_i can use the commitment key of the trusted third party to generate the voting message into commitment C_P and the corresponding correctness certification π_P. The user can use SP signature to generate $SP(C_P)$ to avoid other users voter for U_i himself. To avoid repeatable voting, the user can generate a safe tag $Tag = pk_{U_i} \cdot g_1^{S \cdot R}$ and the certification of corresponding correctness π_T. Voters can send

$Piao = \{C'_S, \pi'_S, C_P, \pi_P, Tag, \pi_T, SP(C_P), GGBS'(C_S)\}$ to the authority.

(3) Authority: he can grant the right to verify the correctness of the group blind signature $GGBS'(C_S)$. If it is correct, it means the voter is a legal user who can be certificated by the electronic voting system. Then the authority verifies whether the random number R is fresh. If it is not fresh, it means that U_i repeats the voting; or it means that U_i's vote is exclusive. Thus, it prevents U_i from repeating the vote.

E. Vote Counting Agreement

None of voters can vote when the voting time is over. The agreement allows the regional authority to count the ballots voted by users of this region. If submitted the group blind signature, the certification of corresponding commitment and the SP signature are correct, the voter is legal and has voted right ballot, as follows:

(1) Authority → Group Manager: the authority sends the collected legal votes $Piao$ to the group manager.

(2) Group Manager → Trusted Third Party: the group manager verifies whether the votes submitted by the authority is legal. If it is legal, he will submit the votes to the trusted third party.

(3) Trusted Third Party → Group Manager: the trusted third party verifies the legality of the votes, extracts the votes by his own commitment secret key ek_{TTP} and sends the votes to the group manager.

(4) Group Manager: the group manager counts the total number of votes and publishes the record of voting $Piao$ and the result. The user can verify whether his vote is in the result. And all the people can verify the legality and the correctness of the total votes.

IV. ANALYSIS OF SECURITY

If the Ghadafi group blind signature cannot be forged, SP signature cannot be fake, discrete logarithm problem is difficult and Groth-Sahai certification is zero-knowledge, the new multi-authorized electronic voting system can meet the requirement of authentication, confidentiality, overall verifiability, non-mandatory, non-repeatablity, and fairness, as follows:

(1) Authentication

Authentication means that only the legal voters can vote.

In the registered agreement, the authority should authenticate the legality of voter's identity. If it is legal, the authority will distribute a group blind signature to the voter. The generated group blind signature can be turned into an anonymous code for the voter. Because Ghadafi group blind signature cannot be forged, no attacker can forge the legal identity of the user, which can protect the authentication of the voter.

(2) Confidentiality

Confidentiality means no attacker can link the vote with its voter.

In the registered agreement, the voter submits his own public key and random number commitment and in the voting agreement, what the user submitted is the update random number commitment and the certification of corresponding correctness. Because Groth-Sahai certification is zero-knowledge, no attacker can link the update commitment and certification with the former commitment and certification. Thus, the new multi-authorized electronic voting system is confidential.

(3) Overall Verifiability

The overall verifiability means that any voters can verify the legality of others' votes.

In the voting agreement, what the users submitted are Ghahafi group blind signature and SP blind signature. Because group blind signature is pubic for verification, everyone can verify the legality of users' votes.

(4) Non-mandatory

Non-mandatory means any attacker cannot force users to generate unwilling votes.

In the voting agreement, the user will generate SP signature for his own vote. Because SP signature cannot be forged, no attacker can force the user to vote against his will.

(5) Non-repeatability

Non-repeatability means any voter cannot vote twice for the same message.

In the voting agreement, the voter needs to submit a security tag which is implanted in user's public key and a random number of the authority. If the user votes twice for the same vote, there will be two different random numbers corresponding to the authority. Thus, the user's public key will be counted by the authority, which guarantee the non-repeatability of the multi-authorized electronic voting system, as follows:

If the user votes twice for the message S, the security tags contained in the votes are $Tag_1 = pk_{U_i} \cdot g_1^{S \cdot R_1}$ and $Tag_2 = pk_{U_i} \cdot g_1^{S \cdot R_2}$. The following formula ① can restore the identity of the voter.

$$
\begin{aligned}
&(Tag_1^{R_2} / Tag_2^{R_1})^{1/(R_2-R_1)} \\
&= (pk_{U_i} \cdot g_1^{S \cdot R_1})^{R_2} (pk_{U_i} \cdot g_1^{S \cdot R_2})^{R_1} \\
&= (pk_{U_i}^{R_2-R_1})^{1/(R_2-R_1)} \\
&= pk_{U_i}
\end{aligned}
$$

(6) Fairness

Fairness means no one can figure out and change the result of the voting.

In the voting system, the votes are commitment and the corresponding blind signature. The blind signatures are certificates for Groth-Sahai zero-knowledge and both Groth-Sahai commitment and zero-knowledge certificate are zero-knowledge, so no one can obtain any message from the commitment and corresponding blind signature before the end of voting. Thus, the new multi-authority electronic voting system is fair.

V. CONCLUSION

This paper first constructs a double-blind multi-authority electronic voting system by Ghadafi group blind signature and SP blind signature. In the new system, the confidentiality of the votes and the authority can be protected. Several authorities are introduced to solve the problem that one single authority can easily control the voting result. Meanwhile, the new system can meet the requirement of authentication, confidentiality, overall verifiability, non-mandatory, non-repeatablity, and fairness, which improves the security of the electronic voting system.

REFERENCES

[1] D L Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms [J]. Communications of ACM, Vol. 24, pp. 84-88, 1981. http://dx.doi.org/10.1145/358549.358563

[2] A A Philip, S A Simon and A O Arowolo. A receipt-free multi-authority e-voting system [J]. International Journal of Computer Applications, Vol 30, No 6, 2011.

[3] E O Omidiora, S O Olabiyisi, R A Ganiyu and O O Alo. A Framework for a Multifaceted electronic voting system [J]. International Journal of Applied Science and Technology, Vol 1, No.4; July, 2011.

[4] O O Olusola and O E Olusayo. A review of the underlying concepts of electronic voting [J]. In Information and Knowledge Management, ISSN 2224-5758, Vol 2, No.1, 2012.

[5] V Cortier and C Wiedling. A Formal Analysis of the Norwegian E-voting Protocol [J]. LNCS 7215, pp. 109–128, Springer-Verlag Berlin Heidelberg, 2012.

[6] A Huszti. A homomorphic encryption-based secure electronic voting scheme [J], Publ. Math. Debrecen 79/3-4, 479-496, 2011. http://dx.doi.org/10.5486/PMD.2011.5142

[7] X Yi and E Okamoto. Practical Remote End-to-End Voting Schem[C], EGOVIS 2011, LNCS 6866, pp. 386–400, 2011.

[8] S S Shinde, S Shukla and D K Chitre. Secure e-voting using homomorphic technology [J]. International Journal of emerging Technology and Advanced Engineering, Vol 3, No. 8, 2013.

[9] J Groth and A Sahai. Efficient Non-interactive proof systems for bilinear groups[C]. In EUROCRYPT'08, LNCS 4968, SPringer, pp. 415-432, 2008.

[10] M Abe, G Fuchsbauer, J Groth, K Haralambiev and M Ohkubo. Structure-preserving signatures and commitments to group elements [C]. In CRYPTO'10, LNCS 6223, SPringer, pp. 209-236, 2010.

[11] E Ghadafi. Formalizing group blind signatures and practical constructions without random oracles [C]. In ACISP 2013, LNCS 7959, pp. 330-346, 2013.

[12] V. Auletta, C. Blundo and S. Cimato. "A Web Service Based Micro-payment System," in Proceeding of the 11th IEEE Symposium on Computers and Communications (ISCC'06), Sardinia, Italy, pp.328-333, 2006. http://dx.doi.org/10.1109/ISCC.2006.20

[13] M. Lee, and K. Kim. "A Micro-payment System for Multiple-Shopping". In Proceedings of the Symposium on Cryptography and Information Security 2002 (SCIS 2002), Shirahama, Japan.

[14] R. Parhonyi. "An interconnection architecture for micropayment systems". In Proceedings of the Seventh International Conference on Electronic Commerce, Xian, China, pp. 633-640, 2005. http://dx.doi.org/10.1145/1089551.1089665

[15] Kim, S. and Lee, W. A PayWord-based micro-payment protocol supporting multiple payments. In Proc. of the International Conference on Computer Communications and Networks, pp. 609-612, 2003.

[16] Rivest, R., Shamir, A. and Adleman, L. A Method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, vol. 21, no. 2, pp. 120-126, 1978. http://dx.doi.org/10.1145/359340.359342

[17] Schneier, B. Applied Cryptography. John Wiley & Sons, 1996.

AUTHORS

Wang Haibin is with Information and Engineering Department, Xingtai Polytechnic College, Xingtai, Hebei, 054035, China. He was born in Xing tai city, Hebei province of china in 1982. His research direction is the application of virtual reality technology. (e-mail: seashorewang@qq.com).

Liu xia, is with College of mathematics and information technology, Xingtai University, Xingtai, Hebei, 054001, China. She was born in Xing tai city, Hebei province of china in 1982. Her research direction is the security of network. (e-mail: 41028315@qq.com).

Zhao sheng is with Information and Engineering Department, Xingtai Polytechnic College, Xingtai, Hebei, 054035, China. He was born in Hubei province of china in 1980. His research direction is electronic commerce. (e-mail: 593826346@qq.com)

Huo Lina is with College of mathematics and information technology, Xingtai University, Xingtai, Hebei, 054001, China. She was born in HengShui city, Hebei province of china in 1982. Her research direction is the application of virtual reality technology. (e-mail: huolinana@163.com).

Submitted 21 September 2015. Published as resubmitted by the authors 20 October 2015.