Journal of Theoretical and Applied Information Technology
31st December 2012. Vol. 46 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

ANONYMOUS E-VOTING SYSTEM BASED ON ID-BASED RING SIGNATURE

[1, 2]Lei Wu

[1]School of Information Science and Engineering, Shandong Normal University, Jinan 250014, Shandong, China

[2]Shandong Provincial Key Laboratory for Distributed Computer Software, Jinan 250014, Shandong, China

ABSTRACT

The design of an electronic voting system has been a hot research topic in the area of information security. Based on ID-based ring signature, blind signature, multi-verification technology and existed typical electronic voting models, an improved anonymous electronic voting system is designed. We proved that the new system has good properties of security: anonymity, eligibility, fairness, nonrepeatability, verifiability, etc., so it can avoid all the illegal behaviors. We also compare its performance with some typical systems. The new system is proved to be a practical and reliable electronic voting system, which can be used in mobile ad hoc network.

Keywords: *E-voting, Ring signature, Multi-Verification*

1. INTRODUCTION

In recent thirty years, scholars did a lot of works on research of electronic voting and proposed some E-voting protocols. These protocols are improved in security and efficiency. But till now there is not a satisfactory solution not only in theory but also in application. We briefly introduce the research improvement of E-voting.

The first modern E-voting scheme, was proposed by Chaum[1] in 1981. Based on public key cryptosystem, it use digital signature to hide the identity of voters, and complete the whole voting process through computer and network. In 1985, Cohen, Fisher[2] proposed the E-voting scheme based on homomorphism encryption. Then Benaloh, Yung, Iverson, Sako, Kilian, etc[3] proposed different E-voting schemes based on homomorphism encryption.

In the existing E-voting schemes, some schemes are too complex, unsuitable for large-scale voting. Some schemes have fatal security leaks. The first scheme suitable for large-scale E-voting is the FOO scheme proposed by Fujioka, Okamoto, Ohta[4] in 1992. This scheme use technologies of bit commitment and blind signature. It attracted extensive attentions, is looked as an E-voting scheme that can realize secure voting. After that, E-voting systems are widely applied in non-government sectors. A lot of research institute of colleges and companies improved the scheme and developed corresponding E-voting software system. EVOX system of MIT[5] and Sensu system of Washington University[6] are famous in them.

In the research of E-voting system, some scholars proposed different solutions for the security problem in FOO protocol, and designed E-voting systems suitable for different situations and motives. Cramer proposed an E-voting scheme[7] based on threshold homomorphic encryption, BBS, and zero knowledge exponential proof. It can satisfy anonymity and generalized verifiability, and has a good efficiency. Then to avoid the behavior of vote business and compulsory voting, Benaloh introduce the conception of E-voting receipt-free[8], a voter can't prove that he vote one special candidate to a third party. After that, scholars did a great amount of work in designing receipt-free E-voting scheme[9,10,11]. Martin[12] proved that the scheme of Benaloh is not receipt-free, in the multi-voting model. Lee[10,11] improved the scheme of Cramer. To let the scheme be receipt-free, Lee pulled in a trusted third party to be the verifier, but the scheme of Lee needs a fully trusted organization, in realistic voting process, it's a condition difficult to be satisfied.

2. PRELIMINARIES

2.1 Security Requirements of E-voting Scheme

A secure E-voting system should satisfy the following properties:

(1) Eligibility: A voter that has voting right can vote.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

(2) Privacy: The content of vote must be kept secret, except for a voter himself, nobody can relate a voter to the content of vote.
(3) Fairness: Before the end of vote, the intermediate result can't be leaked to avoid influencing the final vote result.
(4) Completeness: The system should authenticate and calculate every vote correctly, avoid tempering vote, forgetting valid vote, adding invalid vote, copying valid vote, leaking vote information, etc.
(5) Verifiability: Everyone or only the voter can verify the voting result is correct or not.
(6) Robustness: The system should have some fault-tolerant capabilities, if there is cheating behavior or being attacked, the voting is still in normal operation.
(7) Unreusability: Each legal voter can only vote once.
(8) Receipt-Free: A voter can't prove his vote content to a third party, any third party can't compel a voter to vote or abstain from voting.

To sum up, establishing a secure E-voting system has two main aims:
(1) The benefits of voters can't be violated, realize the anonymous voting, nobody can get information of voters from the votes;
(2) Ensure the fairness of voting result, avoid the cheating behaviors.

2.2 Compositions and Functions of E-voting System

An E-voting system is composed of voter module, vote administrative organization module and vote calculation module. The functions of the modules and submodules are as follows:

Voter Module
(1) Obtain vote signature submodule: Contact the vote signature organization and obtain a legal vote;
(2) Voting submodule: Contact the vote calculation organization, deliver his one legal vote;
(3) Obtain voting result submodule: Contact the vote calculation organization, obtain the voting result.

Vote Administrative Organization Module
(1) Vote signature submodule: Accept the legal voter's request and sign on the vote;
(2)Voter info manage submodule:Verify the voter's validity, record the voter's sign request, avoid the voter obtaining more than one legal vote.

Vote Calculation Module
(1) Vote signature verify submodule: Verify the vote's validity, avoid repeat vote;
(2) Valid vote calculation submodule: Complete the vote calculation and calculate the voting result;
(3) Voting result publish submodule: Publish the voting result.

3. NEW ANONYMOUS E-VOTING SYSTEM BASED ON RING SIGNATURE

In this section, we propose a new anonymous E-voting system based on ring signature.

3.1 Ring Signature Scheme

In the new E-voting system based on ring signature, we use the ID-based ring signature scheme proposed by Chow，Yiu and Hui[79] as the fundamental algorithm.

[Setup]

To setup an ID-based ring signature scheme, the trusted key generation center KGC, will select two cryptographic hash functions $H(\cdot)$ and $H_0(\cdot)$ such that $H:\{0,1\}^* \to G_1$ and $H_0:\{0,1\}^* \to Z_q^*$, where G_1 is an additive cyclic group of prime order q for some large prime q. The KGC randomly chooses a secret value $x \in_R Z_q^*$ and securely store it as the master secret key and compute the corresponding public key as $P_{pub} = xP$ where P is a generator of G_1. For a G_2, which is a multiplicative cyclic group of prime order q for the same large prime q, the KGC defines a bilinear pairing $e: G_1 \times G_1 \to G_2$ and publish the system parameters $< q, G_1, G_2, H(\cdot), H_0(\cdot), e(\cdot,\cdot), P, P_{pub} >$

[Kgen]

Any entity with identity $ID \in \{0,1\}^*$ can generate its own public key Q_{ID} by simply computing $Q_{ID} = H(ID) \in G_1$. To obtain the corresponding secret key, the entity must submit it's identity to the KGC, which sets the secret key S_{ID} of ID as $S_{ID} = x\ Q_{ID}$ and securely transmit this value back to the owner. For the ID-based ring signature scheme, the secret signing key is S_{ID} and the public signature verification key is Q_{ID}.

[Sign]

The set L of identities of n users is $L = \{ID_1, ID_2, ..., ID_n\}$ and the actual signer is indexed as s. The public key Q_{ID_s} of the signer is $Q_{ID_s} = H(ID_s) \in G_1$. The signing algorithm for a message m by signer ID_s, is as follows:

(1) Choose $U_i \in_R G_1$ and compute

$$h_i = H_0(m \| L \| U_i),\ \forall i \in \{1,...,n\} \setminus \{s\},$$

Journal of Theoretical and Applied Information Technology
31st December 2012. Vol. 46 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

(2) Choose $r_s^{'} \in Z_q^*$ and compute

$$U_s = r_s^{'} Q_{ID_s} - \sum_{i \neq s} \{U_i + h_i Q_{ID_i}\},$$

(3) Compute $h_s = H_0(m \| L \| U_s)$ and

$$V = (h_s + r_s^{'}) S_{ID_s},$$

(4) Output the signature on m as

$$\sigma = \{\cup_{i=1}^{n} \{U_i\}, V\}.$$

[Verify]

The verification of an ID-based ring signature by an entity that receives the tuple (m, L, σ) is as follows:

(1) Compute $h_i = H_0(m \| L \| U_i)$, $\forall i \in \{1,...,n\}$,

(2) Check the equality

$$e(P_{pub}, \sum_{i=1}^{n}(U_i + h_i Q_{ID_i})) = e(P, V)$$

and if the output of the test is true then accept the signature as correctly verified. Otherwise a value of false is output.

3.2 E-voting System Role Settings

Voter (v_i): Each voter v_i 's identity is ID_i , his public key is $Q_{ID_i} = H(ID_i)$. All legal voters' identities are published before the voting, total number is N .

Trusted Organization (TA): TA distributes warrants w_i to every legal voter through secure channel.

Vote Distribution Organization (DA): Distribute the only corresponding vote serial number to the legal voter and sign on it.

Registration Organization (RA): Verify the identity and warrant of legal voters, sign on the valid vote. If the vote of a legal voter is not correctly calculated by vote calculation organization, the voter can request RA to verify and calculate votes again. Calculation Organization (CA): Collect votes, calculate votes, get the voting result.

3.3 Description of E-voting System Based On Ring Signature

The new system has four phases: TA distributing warrants, DA distributing vote serial number, v_i voting cooperate with RA, CA collecting & calculating votes and publishing result.

(1) **TA Distributing Warrants**

A legal voter v_i sends request to TA anonymously, TA sends warrant w_i to v_i through secure channel, and save w_i to warrant list to avoid distributing warrants repeatedly. So each legal voter obtain the only vote warrant corresponding with his identity.

(2) **DA Distributing Vote Serial Number**

For N legal voters v_i , $i \in \{1,...,N\}$, there are N vote serial numbers vary from one to one to distinguish the votes. The serial numbers are denoted with M_i , $i \in \{1,...,N\}$. DA use a RSA signature system to verify the validity, the private key is d_{DA}, public key is (e_{DA}, n_{DA}) .

- The legal voter v_i , $i \in \{1,...,N\}$ randomly choose n_c other legal voters, form a ring that has n_d members. To be more secure, n_d ought to be large, $1 < n_d \leq N$, the set of identities of the ring is denoted as $L_d = \{v_1, v_2, ..., v_{n_d}\}$, v_i randomly choose message m_d , use the ring signature algorithm in 2.1

sign on m_d , generate ring signature

$$\sigma_d = \{\cup_{i=1}^{n_d} \{U_i\}, V_d\},$$

v_i sends $\{w_i, m_d, L_d, \sigma_d\}$ to DA.

- DA receives $\{w_i, m_d, L_d, \sigma_d\}$, first check w_i is in the warrant list or not, if not, sound a warning.

If w_i is in the warrant list, check w_i is in the serial number list, if yes, sound a warning.

If w_i is not in the serial number list, use the verification algorithm in 2.2, check $e(P_{pub}, \sum_{i=1}^{n_d}(U_i + h_i Q_{ID_i})) = e(P, V_d)$ is hold or not, if not, the signature is invalid, sound a warning; if the equation holds, the signature is valid, DA randomly choose a serial number M_i in the serial number set, and use the private key d_{DA} of RSA signature system to sign on the serial number, the signature is $\Omega_i = M_i^{d_{DA}} \bmod n_{DA}$.

- DA sends $\{w_i, M_i, \Omega_i\}$ to the voter v_i , and save $\{w_i, M_i, \Omega_i\}$ in the serial number list.

(3) **Legal Voter Voting Cooperate With RA Vote Generated**

The legal voter combines candidate's corresponding serial number C_i and DA serial number M_i to generate the vote E_i , $E_i = M_i \| C_i$.

Vote Blinded

To avoid leaking vote information in RA, the voter generates the blind signature of vote E_i . RA has its own RSA signature system, private key is d_{RA} , public key is (e_{RA}, n_{RA}) . Randomly chooses $k_i < n_{RA}$, generates the blinded vote $E_{Bi} = E_i \cdot k_i^{E_{RA}} \bmod n_{RA}$.

Journal of Theoretical and Applied Information Technology
31st December 2012. Vol. 46 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Ring Signature of Blinded Vote

The legal voter v_i , $i \in \{1,...,N\}$ randomly chooses n_r other legal voters, form a ring that has n_r members. To be more secure, n_r ought to be large, $1 < n_r \le N$, the set of identities of the ring is denoted as $L_r = \{v_1, v_2, ..., v_{n_r}\}$, v_i use the ring signature algorithm in 2.1 sign on blinded vote E_{Bi} , generate ring signature $\sigma_r = \{\cup_{i=1}^{n_r}\{U_i\}, V_r\}$, v_i sends $\{w_i, E_{Bi}, L_r, \sigma_r\}$ to RA.

RA Verify Ring Signature and Register the Blinded Vote

RA receives $\{w_i, E_{Bi}, L_r, \sigma_r\}$, first check w_i is in the warrant list or not, if not, sounds a warning.

If w_i is in the warrant list, check w_i is in the registration information list, if yes, sound a warning.

If w_i is not in the registration information list, use the verification algorithm in 3.2, check $e(P_{pub}, \sum_{i=1}^{n_r}(U_i + h_i Q_{ID_i})) = e(P, V_r)$ is hold or not, if not, the signature is invalid, sound a warning; if the equation holds, the signature is valid, RA use the private key d_{RA} of RSA signature system to sign on the blinded vote E_{Bi} , the signature is $\Phi_i = E_{Bi}^{\ d_{RA}} \bmod n_{RA}$.

RA sends $\{w_i, E_{Bi}, \Phi_i\}$ to the voter v_i , and save $\{w_i, E_{Bi}, \Phi_i\}$ in the registration information list.

Voter Unblinding and Obtain the Vote Signature

The voter v_i uses RA's public key e_{RA} to check $E_{Bi} = \Phi_i^{\ e_{RA}} \bmod n_{RA}$ is hold or not, if not, sends the request again, if it holds, Φ_i is correct, v_i unblinds to obtain the signature of the vote Λ_i ,

$$\begin{aligned}\Lambda_i &= k_i^{-1}\Phi_i \bmod n_{RA} = k^{-1}E_{Bi}^{\ d_{RA}} \bmod n_{RA} \\ &= k_i^{-1}\,(E_i \cdot k_i^{e_{RA}})^{d_{RA}} \bmod n_{RA} \\ &= E_i^{\ d_{RA}} \cdot k_i^{-1} \cdot k_i^{e_{RA}d_{RA}} \bmod n_{RA} \\ &= E_i^{\ d_{RA}} \bmod n_{RA}\end{aligned}$$

(4) **CA Collecting & Calculating Votes**

- The voter v_i sends $\{M_i, \Omega_i, E_i, \Lambda_i\}$ to CA.
- CA check if M_i is exist in the vote list or not, if exists, the vote is repeat, delete the vote. If not, CA uses DA's public key e_{DA} to check $M_i = \Omega_i^{e_{DA}} \bmod n_{DA}$ is hold or not, use RA's public key e_{RA} to check $E_i = \Lambda_i^{e_{RA}} \bmod n_{RA}$ is hold or not, if all hold, Ω_i and Λ_i are correct, to next step, otherwise delete the vote.
- Calculation Organization has its own RSA signature system, the private key is d_{CA} , public key is (e_{CA}, n_{CA}) . CA sign on E_i , the signature is denoted with Ψ_i , $\Psi_i = E_i^{\ d_{CA}} \bmod n_{CA}$, save $\{M_i, \Omega_i, E_i, \Lambda_i, \Psi_i\}$ in the vote list.
- After the voting , CA publish the vote list. If a legal voter find that his vote is not correctly calculated, then he sends $\{w_i, E_{Bi}, \Phi_i\}$ to RA, RA verifies its validity, and asks CA to calculate votes again.
- All voters have no objection for the vote list, CA calculates votes and publish the voting result.

4. ANALYSI SIS OF NEW SYSTEM

4.1 Security Analysis

(1) Anonymity

With the use of ring signature, ring signature's anonymity realizes on the voters. RA can't confirm the identity of the voter with the probability of no less than $1/n$. The voter requests for warrant anonymously. With the use of ring signature, blind signature, the voter's real identity is protected. If a legal voter's vote is not corrected calculated, he request calculating votes again through verification, the verification information blinds his identity information, his identity will not be disclosed. So with the use of ring signature, blind signature and secret channel, the anonymity of the voter is satisfied. Even if RA, DA, CA collude, they can't confirm the identity of the voter with the probability of no less than $1/n$.

(2) Eligibility

Via TA distributing warrants, only the legal voter can vote, illegal user can be identified and traced. In the vote distributing phase and vote registration phase, each legal voter uses private key and ring members' public key to generate ring signature .The adversary can't obtain the legal voter's private key, so he can't disguise himself as a legal voter to vote.

(3) Fairness

This system uses multi-verification technology, every vote is multi-signed and multi-verified with private keys of organizations and the legal voter. There is no possibility of forgery and temporary. The vote is blinded in the registration phase, RA can't obtain the information related to the vote, so in all phases there are signature scheme and

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

authentication system to avoid the illegal voting behaviors.

(4) Nonrepeatability

Through distributing vote serial number to legal voter (one to one), querying serial number list, registration information list, vote list, once a vote is repeated, then delete it. This can assure that one legal voter can only vote once.

(5) Verifiability

In the publish term after the voting, CA publishes the vote list, each legal voter

can verify whether his vote is correctly calculated or not. If there is some problem, he sends his identity information and vote information to RA, afer RA's verification, CA is requested to calculate votes again.

4.2 Performance Analysis

In Table 1. we compare the new system with four typical E-voting system in privacy, anonymity, correctness, verifiability, dropping out, vote collision, system participant, complexity and security. It shows that the new system is more secure and efficient.

Table 1 : Performance comparison of 5 systems

	FOO	MEM	BSM	SSM	NEW
Privacy	√	√	√	√	√
Anonymity	√	√	√	√	√
Correctness	√	√	√	√	√
Verifiability	×	×	√	√	√
Dropping Out	×	×	√	√	√
Vote Collision	×	√	√	√	√
System Participant	4	4	4	6	3
Complexity	Middle	Low	Middle	High	Low
Security	Low	Low	Middle	High	High

5. CONCLUSION

A new anonymous E-voting System Based on ID-based Ring Signature is proposed. We proved that the new system has good properties of security: anonymity, eligibility, fairness, nonrepeatability, verifiability, etc., it can avoid all the illegal behaviors. We also compare its performance with some typical systems. The new system is proved to be a practical and reliable electronic voting system, which can be used in mobile ad hoc network.

ACKNOWLEDGEMENTS

This work is supported by Shandong Provincial Natural Science Foundation (No. ZR2011FQ032) and Project of Shandong Province Higher Educational Science and Technology Program (No. J11LG33).

REFERENCES:

[1] Chaum D, "Untraceable electronic mail, return address, and digital Pseudonyms", *Communications of the ACM*, 1981.

[2] J.Cohen, M.Fisher, "A Robust and Verifiable Cryptographically Secure Election Scheme", *Proceedings of IEEE 26th Annual Symposium on Foundations of Computer Science*, l985, pp. 372-382.

[3] J.Benaloh, M.Yung, "Distributing the Power of A Government to Enhance the Privacy of Voters", *ACM Symposium on Principles of Distributed Computing*, 1986, pp. 52-62.

[4] A.Fujioka, T.Okamoto, K.Ohta, "A practical secret voting scheme for large scale election", *Advances in Cryptology-Auscrypt'92*, LNCS 718, Springer-Verlag, 1992, pp.244-260.

[5] Brandon, Wiliam, DuRette, "Multiple administ-rators for electronic voting", Bachelor Thesis, MIT, May 1999.

[6] Lorrie F, Ron K, Cytron S, "A Security-Conscious Electronic Polling System of the internet",http://www.research.all.com/lorrie/pubs/hicss/hicss.ps. 1997.

[7] Cramer R, Gennaro R, Schoenamakers B, "A secure and optimally efficient Multi-authority election scheme", *EUROCRYPT'97*, LNCS 1233, Konstanz, Germany, Berlin: Springer-Verlag, 1997, pp. 103-118.

[8] Benaloh J, Tuinstra D, "Receipt-free secret-ballot elections", *Proceedings of the 26th Symposium on Theory of Computing Montreal*, 1994, New York: ACM Press, 1994, pp.544-553.

[9] V.Niemi, A.Renvall, "How to Prevent Buying of Votes in computer elections", Josef Pieprzyk and Reihaneh Safavi-Naini eds, *ASIACRYPT'* 94,Wollongong, 1994,Berlin:Springer-Verlag, 1994, pp. 141-148.

[10]Lee B, Kim K, "Receipt-free electronic voting through collaboration of voter and honest verifier", *Proceedings of JWISC2000*, Okinawa, Japan, 2000, pp. 10l-108.

[11]Lee B, Kim K, "Receipt-free electronic voting scheme with a tamper- resistant randomizer", Pil Joong Lee and Chae Hoon Lim eds, *ICISC 2002*, LNCS 2587, Seoul, 2002, pp. 389-406.

[12]Martin H, Sako K, "Efficient receipt-free voting based on homomorphic Encryption", Preneel B ed. *EUROCRYPT'00*, LNCS 921, Binges, Belgique, 2000, pp. 539-556.