E-voting with Receipt-freeness and Universal Verifiability Using E-voting Sheet

Her, Yong-Sork
Graduate School of Information Science and Electrical Engineering, Kyushu University

Imamoto, Kenji
Graduate School of Information Science and Electrical Engineering, Kyushu University

Sakurai, Kouichi
Faculty of Information Science and Electrical Engineering, Kyushu University

E-voting with Receipt-freeness and Universal Verifiability Using E-voting Sheet

Yong-Sork HER* Kenji IMAMOTO* Kouichi SAKURAI**
(*Graduate School of Information Science and Electrical Engineering, Kyushu University
**Faculty of Information Science and Electrical Engineering, Kyushu University)

1 Introduction

Sako and Killian[SK95] proposed mix-net e-voting system which satisfies receipt-freeness and universal verifiability in Eurocrypt'95. Michels and Horster pointed out that Sako-Killian scheme does not satisfy robustness and priacy[MH96]. Golle et al.[GJJS04] proposed universal re-encryption mix net which satisfies correctness and communication privacy. In this paper, we propose a novel mix-net e-voting system using Golle et al. 's universal re-encryption mix-net which satisfies receipt-free and universal verifiability as well as robustness and privacy. To achieve universal verifiability, receipt-freeness, and privacy, we introduce firstly *E-voting Sheet* which only a voter with *E-voting Sheet* can cast a vote and an *Overwritable Bulletin Board* which can be overwrited contents of bulletin board by each mix-center. To achieve anonymity of encrypted voting content and robustness, we use Golle et al.'s universal re-encryption mix-net.

2 E-voting Procedure

2.1 Entities

Voter V_i ($\{i \mid i = 1,..., z\}$): A voter cast a vote only by an election rule.

Mix center C_i ($\{j \mid j = 1,..., n\}$)

- Each mix-center generates a random encryption factor to re-encrypt *ES*, and re-encrypts *Voting Vector* which consists of encrypted voting content and encrypted *ES*.
- The last center recovers a voter's *ES* and compute the voting result.

ES-Center

- ES-center takes a valid voter list, and checks whether a voter is a valid voter or not through one-way untappable channel.
- He generates *ES* jointly with the last mix-center.

Bulletin Board BB

- Anyone can see contents of BB, but can not modify or erase it.

Overwritable Bulletin board OBB

- Only each mix-center overwrites contents in OBB. Other people can only see it.

2.2 Overview of e-voting

Our e-voting protocol runs as follows.

Issue of *ES*

1. We suppose that ES-center takes a valid voters list. ES-center and the last mix-center jointly generate *ES*.
2. After ES-center checks a voter's id and signature through one-way untappable channel, he sends *ES* and encrypted ES to a valid voter.
3. ES-center posts a valid voter's id to *BB*.

Voting stage

1. A voter chooses a voting content, and encrypts it with *ES*.
2. A voter generates *Voting Vector* which consists of encrypted voting content and encrypted *ES* by ES-center, and sends it to *OBB*.
3. The first mix-center gets *Voting Vector* from OBB and re-encrypts *Voting Vector* with his random encryption factor as the original universal re-encryption mix-net. He overwrites the old *Voting Vector* in OBB in a random order.
4. To prove a valid of mixing of the first mix-center, the first mix-center (Prover) proves to the second mix-center (Verifier) without leaking his random encryption factor (See appendix A). He sends his proof to the designated field of BB.
5. Other mix-centers from the second mix-center to $n-1$ mix-center re-encrypt *Voting Vector* with their random encryption factors and overwrite the old *Voting Vector* in OBB in order. Each mix-center proves his mixing to the next mix-center using the modified designated-verifier re-encryption proof.

Counting stage

1. The last mix-center decrypts a voter's *ES*. He computes the voting result with *ES*.
2. ES-center verifies the computed voting result with the number of issued *ES* and the published voting result by the last mix-center.

Table 1. Comparison of mix-net e-voting systems

Property	[PIK93]	[SK95]	[HS00]	Our scheme
Receipt-freeness	No	Yes	Yes	Yes
Universal Verifiability	No	Yes	Yes	Yes
Privacy	Yes	No	Yes	Yes
Robustness	Yes	No	Yes	Yes

3 Conclusion

We propose mix net e-voting system which satisfies robustness and privacy as well as receipt-freeness and universal verifiability as Table1. We introduce firstly E-voting Sheet, and use Overwritable Bulletin Board. For achieving universal verifiability

Acknowledgement

The research was partly supported by the Grant-in-Aid for Creative Scientific Research No.14GS0218 (Head of Researchers : Prof. Hiroto Yasuura, System LSI Research center, Kyushu University) of the Ministry of Education, Science and Culture (MEXT) and by the 21st Century COE Program 'Reconstruction of Social Infrastructure Related to Information Science and Electrical Engineering'. The first author was also supported by Grant for Non-Japanese Researcher of Foundation for C&C Promotion (This foundation is maintained with the donations from NEC Corp.).

References

[PIK93] C.Park, K.Itoh and K.Kurosawa," All/nothing election scheme and anonymous channel", Eurocrypt'93, 1993.

[SK95] K.Sako and J.Kilian, "Receipt-Free Mix-type Voting Scheme", Proceeding of Eurocrypt'95, LNCS921, Springer-Verlag, pp393-403,1995

[MH96] M.Michels and P.Horster, "Some remarks on a receipt-free and universally verifiable Mix-type voting scheme," Asiacrypt'96, pp125-132, 1996.

[HS00] M.Hirt and K.Sako, "Efficient receipt-free voting based on homomorphic encryption", Eurocrypt 2000, LNCS 1807, pp539-556, 2000.

[GJJS04] P.Golle, M. Jakobsson, A.Juels and P.Syverson, "Universal Re-encryption for Mixnets", CT-RSA 2004, LNCS 2964, pp163-178, 2004.