A Pseudonymous Joint Signature Scheme

Wei-Chi Ku and Sheng-De Wang
Department of Electrical Engineering
National Taiwan University, Taipei 106, Taiwan
[wcku, sdwang]@star.ee.ntu.edu.tw

Abstract

The result of a joint signature is frequently used to evaluate whether the issuing matter should be decided further by a more formal decisive method like voting. Compared with the voting, the joint signature can be regarded as a less formal but simpler method to reflect the intention of people. In this paper, we propose a network-based pseudonymous joint signature scheme that can be practically operated over information networks. The scheme ensures the signer privacy which is critical in most political affairs.

1. Introduction

Opinions expression through voting is one of the most common methods to fulfill democracy. In addition to the voting in periodical elections, extraordinary voting for the exceptional matters is often called. Since it takes much time and money to hold a voting, careful evaluation for the necessity of the extraordinary voting is preferred. should be made in advance. In many democratic countries and societies, joint signature activity is one of the major methods to achieve this goal. The result of a joint signature can be used to estimate the rough intention of the people. In contrast to the voting, the joint signature concentrates on a single matter, which may be the request of recalling an elected people's representative, an approval of some one's candidate qualification for a large scale election, a proposal for public affairs and so on. For example, only when the number of signatures in the joint signature book exceeds the quorum, the voting for recalling an elected representative should be hold. To participate in a conventional paper-based joint signature activity, one has to go to the particular place possibly far from his regular daily life region. In addition, the identities of the signers are revealed by the joint signature book. Both concerns make us more likely to abandon our rights. Clearly, it is unnecessary and unanticipated that the iden-

ties of the signers should be revealed except for some special cases. For most public affairs, the signer's privacy desires to be protected so that the signer may feel free to express his view without hesitating he will be oppressed later. Consequently, it is hard to efficiently monitor the representatives we chose before. On the other hand, verifying all the signatures in a large joint signature book is tedious and difficult. Forged signatures cannot be easily found by using simple verification methods.

Seeing that information networks have facilitated many cumbersome works into simple ones in these decades, many network-based secret voting schemes have been proposed by researchers from both theoretical and practical points of view [1]-[10]. Since the result of an election is crucial and decisive, it would be inappropriate to directly apply these network-based secret ballot voting schemes in current political elections. In contrast, the result of a joint signature is used to evaluate whether the issuing matter should be decided further by using a more formal decisive method like conventional paper-based voting. In existing network-based secret voting schemes, the voter should register for each individual election. If one who wants to participate in a pseudonymous joint signature activity has to register first, the singer privacy is thus violated. However, the way of registration in existing network-based secret voting schemes is unsuitable for the pseudonymous joint signature schemes. In this paper, we propose a network-based pseudonymous joint signature scheme to estimate the approximate intend of people so that unnecessary voting can be avoided in an efficient and economical way.

2. Pseudonymous joint signature scheme

The model of the proposed scheme consists of members, a signature authority, a scrutiny committee containing several supervisors $S_1, S_2, \dots$, and S_j , and the signature collector. The proposed scheme assumes that an *untraceable email system*, e.g. [1] [12], is available. By means of an untraceable email system, the sender's iden-

tity of an email can be kept secret from others. Additionally, the *blind signature technique* [13][14] is also employed in the scheme. The major feature of blind signatures is called “unlinkability”, i.e., the signature owner can prevent the signer from acquiring the exact correspondence between the actual signing process performed by the signer and the signature which later is made public. For instance, RSA can be modified to achieve the blind signature function as in the following:

Assume that the RSA parameters of the readily signer is (p, q, n, e, d) . One who wishes to obtain the signature of the message *mesg* signed by the signer can generate a secret random number r and then compute

$$E(r) \times \text{mesg} = r^e \times \text{mesg} \bmod n.$$

This encrypted message, or *swaddled mesg*, is sent to the signer. Since the signer doesn't have r , he cannot obtain *mesg* from the received message even if he has the factors of n . The signer directly signs this swaddled *mesg* using d to form the corresponding blind signature *bs*, where

$$\begin{aligned} bs &= D(E(r) \times \text{mesg}) = (r^e \times \text{mesg})^d \bmod n \\ &= r \times \text{mesg}^d \bmod n. \end{aligned}$$

Upon receiving *bs*, the requester can use $(r^{-1} \bmod n)$ to retrieve the signature s from *BS* by computing

$$\begin{aligned} s &= r^{-1} \times bs \bmod n = r^{-1} \times (r \times \text{mesg}^d) \bmod n \\ &= \text{mesg}^d \bmod n. \end{aligned}$$

Then, it can be verified by examining

$$E(s) (= s^e \bmod n) = \text{mesg}.$$

Hence, the requester obtains the signature of *mesg* without revealing its content to the signer.

2.1. Preliminary

The proposed scheme is RSA-based such $S1, S2, \dots$, and Sj select their individual RSA parameters $(p_{S1}, q_{S1}, n_{S1}, e_{S1}, d_{S1})$, $(p_{S2}, q_{S2}, n_{S2}, e_{S2}, d_{S2})$, ..., and $(p_{Sj}, q_{Sj}, n_{Sj}, e_{Sj}, d_{Sj})$. And, each member m determines his RSA parameters $(p_m, q_m, n_m, e_m, d_m)$. In particular, the authority selects a set of k distinct key pairs $(e^{(1)}, d^{(1)})$, $(e^{(2)}, d^{(2)})$, ..., and $(e^{(k)}, d^{(k)})$ under the same RSA modulus $n (= p \times q)$, where k is the maximal number of permitted joint signature activities after a registration. During the set-up time, all participants publish their public keys and modulus. The authority publishes a *one-way permutation function* [8][16][15], f . It is convinced by some researchers that a one-way permutation function can be constructed. For example, a discrete logarithm function can be expressed as

$$f(x) = g^x \bmod Q,$$

where Q is a prime, x is an integer and g is a generator of Z_Q^* (a cyclic group under the generator g). When Q and the entropy of $x \in (0, Q)$ is large enough, f can be used as a one-way permutation function.

2.2. Registration

The member m produces k random strings $R_m^{(1)}, R_m^{(2)}, \dots, R_m^{(k)}$ and computes a set of k *one-time pseudonyms*:

$$P_m^{(i)} = f(ID_m, R_m^{(i)}), i = 1, 2, \dots, k.$$

Each $P_m^{(i)}$ can be regarded as an alternate of ID_m that will distinguish m from others without revealing his actual identity. Since the entropy of user identifications is small, $R_m^{(i)}$ is used to avoid the attack of an exhaustive try and then increase the security of f . $R_m^{(i)}$ is a long random bits string so that it is computationally infeasible to infer $P_m^{(i)}$ from ID_m and vice versa without knowing the corresponding $R_m^{(i)}$. Theoretically, we cannot infer ID_m from $f(ID_m, R_m^{(i)})$ if ID_m and $R_m^{(i)}$ are long enough (about 200 digits totally).

Remark 1: If some member do not follow the one-time pseudonym generation procedure to derive his pseudonym instead he just randomly assign that, his one-time pseudonyms may collide with others'.

To conduct a new registration, the authority announce the registration identifier w , which is a meaningful redundant string concatenated with a random string. The member m prepares the messages which are desired to be certified:

$$Y_m^{(i)} = (w, P_m^{(i)}), i = 1, 2, \dots, k.$$

Then, m generates another set of k distinct random strings $r_m^{(1)}, r_m^{(2)}, \dots$, and $r_m^{(k)}$ and computes the *swaddled* $Y_m^{(i)}$:

$$a_m^{(i)} = E_{(1)}(E_{S1}(E_{S2}(\dots(E_{Sj}(r_m^{(i)}))\dots))) \times (Y_m^{(i)}) \bmod n,$$

where $i = 1, 2, \dots, k$.

Next, m encrypts w concatenated with all $a_m^{(i)}$ using his private key d_m :

$$A_m = D_m(w, a_m^{(1)}, a_m^{(2)}, \dots, a_m^{(k)})$$

Finally, m sends A_m to the authority through a general email system.

The authority checks that A_m is actually issued by member m by computing $E_m(A_m)$ and examining that w is in its header. If so, the authority signs each $a_m^{(i)}$ (for $i = 1, \dots, k$) using the corresponding private key $d^{(i)}$ and presents the result $D_{(i)}(a_m^{(i)})$, $i = 1, \dots, k$, as well as the original A_m to the scrutiny committee for certification. The first scrutiny committee supervisor $S1$ checks the validity of A_m and $D_{(i)}(a_m^{(i)})$ (for $i = 1, \dots, k$), if the check succeeds, he signs each $D_{(i)}(a_m^{(i)})$ using his private key d_{S1} and then passes the result $D_{S1}(D_{(i)}(a_m^{(i)}))$ (for $i = 1, \dots, k$) as well as the original A_m to $S2$. Similarly, $S2$ first verifies the received data and then signs $D_{S1}(D_{(i)}(a_m^{(i)}))$ (for $i = 1, \dots, k$) using his private key d_{S2} and then passes them to the $S3$, etc. Finally, the last supervisor Sj produces the blind signatures as in the following.

$$\begin{aligned} b_m^{(i)} &= D_{Sj}(\dots(D_{S2}(D_{S1}(D_{(i)}(a_m^{(i)}))))\dots) \\ &= (r_m^{(i)}) \times D_{Sj}(\dots(D_{S2}(D_{S1}(D_{(i)}(Y_m^{(i)}))))\dots) \bmod n, \end{aligned}$$

where $i = 1, 2, \dots, k$.

S_j sends $b_m^{(i)}$ ($i = 1, 2, \dots, k$) back to the authority. The authority stores them in the ID_m entry of the registration database and sends a copy of them to m . According to the technique of blind signature, m obtains the signatures by computing:

$$\begin{aligned} c_m^{(i)} &= (r_m^{(i)})^{-1} \times b_m^{(i)} \bmod n \\ &= D_{S_j}(\dots(D_{S_2}(D_{S_1}(D_{(i)}(Y_m^{(i)}))))), i = 1, 2, \dots, k. \end{aligned}$$

The member m verifies the received $c_m^{(i)}$ (for $i = 1, 2, \dots, k$) using the public key of $S_j, \dots, S_2, S_1$, and the i^{th} public key of the authority. If he succeeds, he securely stores these certified $Y_m^{(i)}$, i.e., $c_m^{(i)}$ (for $i = 1, 2, \dots, k$), which will be used later as *signature tokens* in the joint signature activities.

2.3. Joint signing

To originate a pseudonymous joint signature on a matter, the originator should first issue a request to the authority. Then, the authority randomly assigns an unused value t within $\{1, 2, \dots, k\}$ as the *activity identifier*. Since this identifier cannot be repeatedly used, a registration can support at most k activities after one registration. At first, the authority announces the matter being signed in the coming activity and the activity identifier, i.e., t . If m wants to participate in this pseudonymous joint signature activity, he can send the signature token $c_m^{(t)}$ to the signature collector through the untraceable email system. The signature collector, abbreviated as collector, is recommended to be sponsored by the originator so that the possibility of denial of service can be reduced.

When the joint signing process is completely finished, all the signature tokens collected by the signature collector are sorted while the duplicated tokens should be removed and only one copy is remained. Then, the handled signature tokens are published on a bulletin board so that everyone can verify them using the public keys of the authority and the supervisors. And, all the verified signature tokens on the bulletin board form the *pseudonymous joint signature book*.

Remark 2: We don't assume that all members should follow the one-time pseudonym generation procedure. The proposed scheme ensures that the rule-abiding members can sign successfully; on the contrary, the malicious and the uncooperative members are not under protection.

3. Security analysis

The security criteria for a pseudonymous joint signature scheme is mainly adapted from the work presented by Fujioka *et al.* in [4], which contains a definition for the security of network-based secret ballot voting scheme. The criteria is used in this section to examine the security of the proposed scheme. In particular, the definition of

verification is adopted from [10], including two classes *individual verifiability* and *universal verifiability*.

Theorem 1 (completeness). *All valid signatures are counted correctly.*

Sketch of Proof: If each member produces his one-time pseudonyms according to the one-time pseudonym generation rule, all the valid signature tokens collected will be accepted. Considering another situation that some members intentionally or carelessly generate their one-time pseudonyms without following the rule and occasionally collide with the one well-generated by a rule-abiding member. According to the scheme, only one copy of the same signature tokens will be left. This can be regarded that the signature token of the rule-abiding member is accepted no matter he signs earlier or later than the rule-contradicting member. That is, we may reasonably regard that the rule-contradicting member has signed for him. On the other hand, since the signature tokens are collected by the collector, which is administrated by the originator of the pseudonymous joint signature activity, rather than the authority, the signature tokens will not be dropped. Hence, the proposed scheme is complete.

Theorem 2 (soundness). *No one can disrupt the pseudonymous joint signature.*

Sketch of Proof: The only situation of disruption is that the tally of collected valid signature tokens exceeds the number of total members. Spurious signature tokens can be generated when the authority and all the supervisors of the scrutiny committee conspire. However, this contradicts the assumption and we can conclude that the proposed scheme is sound.

Theorem 3 (privacy). *All signatures in the pseudonymous joint signature book are secret.*

Sketch of Proof: According to the properties of the one-way permutation function, the blind signature technique, and the untraceable email system, the relation between the actual identity of a member and his one-time pseudonyms cannot be traced. Therefore, the proposed scheme provides signer privacy.

Theorem 4 (unreusability). *No signature tokens can be used twice.*

Sketch of Proof: Since each registration identifier w is unpredictable and is different from the previous ones, reused old signature tokens will not be accepted. Thus, the proposed scheme meets the requirement of signature unreusability.

Theorem 5 (eligibility). *No one who isn't allowed to sign can sign.*

Sketch of Proof: Since the public key (including the

corresponding modulus) of each eligible member is verified and recorded in the database of the authority, the registration request from a non-member will not be accepted. On the other side, as n_m is selected by m and d_m is only known to himself, others cannot produce A_m to register as m and obtain signature tokens. Therefore, the proposed scheme provide eligibility.

Theorem 6 (verifiability). *The result of the pseudonymous joint signature can be verified individually and universally.*

Sketch of Proof: The signer can check that his signature token is placed correctly in the pseudonymous joint signature book by recognizing his one-time pseudonym. Hence, the proposed scheme is individually verifiable. In addition, everyone can check the validity of each published signature token using the public keys of the authority and the supervisors. Since spurious signature tokens cannot be added by the authority or the supervisors as we claim before, it can be ensured that the published signature tokens can be verified. Combined with the property of completeness, the proposed scheme is universally verifiable.

4. Conclusions

In this paper, we propose a pseudonymous joint signature scheme that can be practically operated over current information networks. Especially, the scheme ensures the signer privacy that is demanded in most political affairs. To provide fairness for people who do not have computers and communication devices at hand, the proposed scheme can be integrated with the conventional paper-based joint signature method to form a hybrid joint signature system. By intuition, the result of the hybrid system is the summation of the tally in the paper-based joint signature book and the tally of the signature tokens in the pseudonymous joint signature book. However, to avoid duplicated signatures, a signature in the paper-based joint signature book should be removed if the signer is a member of the pseudonymous joint signature system. To revoke a signature token, the member should present it to the authority. Then, the authority places it in the public revocation list. All the signature tokens appear in the revocation list will be removed from the pseudonymous joint signature book. However, few issues about human behaviors are investigated or analyzed in this paper. Conducts like bribe and persecution cannot be avoided in the proposed scheme; on the contrary, these problems probably become even more terrible. A member may be bribed or persecuted to present the signature tokens to the instigator. And, this problem should be solved in the future work.

References

- [1] D. Chaum, "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms", *Commun. ACM*, 24(2): 84–88, 1981.
- [2] D. Chaum, "Elections with Unconditionally Secret Ballots and Disruption Equivalent to Breaking RSA," *Advances in Cryptology-EUROCRYPT'88*: 177–182, 1988.
- [3] K. Ohta, "An Electrical Voting Scheme using a Single Administrator", *1988 Spring National Convention Record (Japan)*, IEICE, A-294, Mar., 1988.
- [4] A. Fujioka, T. Okamoto, K. Ohta, "A Practical Secret Voting Scheme for Large Scale Elections," *Advances in Cryptology-AUSCRYPT'92*: 244–251, 1992.
- [5] T. Okamoto, A. Fujioka and K. Ohta, "A Practical Large Scale Secret Voting Scheme based on Non-Anonymous Channels," *Proc. SCIS93*, 1C, Japan, Jan. 1993.
- [6] C. Park, K. Itoh, and K. Kurosawa, "Efficient Anonymous Channel and All/Nothing Election Scheme," *Advances in Cryptology-EUROCRYPT'93*: pp. 248–258, 1994.
- [7] K. Sako and J. Kilian, "Receipt-Free Mix-Type Voting Scheme — A Practical Solution to the Implementation of a Voting Booth," *Advances in Cryptology-EUROCRYPT'95*: 393–403, 1995.
- [8] W. Juang and C. Lei, "A Collision-free Secret Ballot Protocol for Computerized General Elections," *Computers & Security*, 15(4): 339–348, 1996.
- [9] J. Benaloh and M. Yung, "Distributing the Power of a Government to Enhance the Privacy of Voters," *ACM symposium on Principles of Distributed Computing*: 52–62, 1986.
- [10] K. Sako and J. Kilian, "Secure Voting using Partially Compatible Homomorphisms," *Advances in Cryptology-CRYPTO'94*: 411–424, 1995.
- [11] R. L. Rivest, A. Shamir, L. Adleman, "A Method for Obtaining Digital Signatures and Public Key Cryptosystems," *Commun. ACM*, pp. 120–126, 1978.
- [12] D. Chaum, "The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability," *Journal of Cryptology*, 1: 65–67, 1988.
- [13] D. Chaum, "Blind Signature for Untraceable Payments," *Advances in Cryptology-CRYPTO'82*: 199–203, 1983.
- [14] J. L. Camenisch, J. M. Preteau, M. A. Stadler, "Blind Signature Schemes based on the Discrete Logarithm Problem," *Rump session of Advances in Cryptology-EUROCRYPT'94*, Perugia, Italy, 1994.
- [15] W. Diffie and M. Hellman, "New Directions in Cryptography," *IEEE Trans. Info.*, IT-22(6): 644–654.
- [16] S. Pohlig and M. Hellman, "An Improved Algorithm for Computing Logarithms in GF(p) and Its Cryptographic Significance," *IEEE Trans. Info.*, 24(1): 106–111, Jan. 1978.