

## Short Paper

---

### An Anonymous Endorsement System

WEI-CHI KU AND SHENG-DE WANG

*Department of Electrical Engineering*

*National Taiwan University*

*Taipei, 106 Taiwan*

*E-mail: sdwang@hpc.ee.ntu.edu.tw*

The expression of one's opinion through endorsement is one of the simplest methods of democratic participation. The result of an endorsement can be used to evaluate whether a certain subject should deserve a higher attention. In some cases, the endorsers desire privacy protection. However, conventional paper-based endorsement systems provide neither convenience nor well privacy protection for the endorsers. In addition, current electronic anonymous voting schemes are unsuitable for anonymous endorsement. This motivates us to develop an anonymous endorsement system that can be realized on computer networks. The proposed system satisfies completeness, soundness, privacy, unreusability, eligibility, and verifiability. In practice, the proposed system can be integrated with the conventional paper-based endorsement system.

**Keywords:** anonymous endorsement, privacy, security, digital signature, untraceable email system

#### 1. INTRODUCTION

The expression of one's opinion through endorsement is one of the simplest methods of democratic participation. The result of an endorsement can be used to evaluate whether or not the subject should deserve further attention. The endorsement subject may be a request to recall an elected representative, an approval of someone's qualification as a candidate for a large scale election, a proposal for certain public project, and so on. For instance, in most democratic countries, it is only when the number of endorsements exceeds a certain quorum that the vote for recalling a delinquent officer can be held. Theoretically, the result of the endorsement depends on the intention of the individual. In practice, the result may also be affected by the method that carries it out. To endorse the subject with the conventional paper-based endorsement method, one must

---

Received May 15, 2000; revised August 14, 2000; accepted September 26, 2000.  
Communicated by Chi Sung Laih.

go to a particular place that may be far from one's domicile. In addition, the endorser's privacy is not well protected in that the identity of the endorser is revealed to at least a group of verifiers. In some situations only when the endorser's privacy can be protected, the endorsers may feel free to express their views without fear of retaliation. The inconvenience and unease of the conventional paper-based endorsement method often makes people more likely to abandon their rights. Moreover, if the number of endorsers is large, manual verification of the endorsement book will be a tedious task. Therefore, we are motivated to design an anonymous endorsement system that can be realized on computer networks.

Many voting schemes, e.g., [1-12], have been proposed from both theoretical and practical perspectives. However, these voting schemes are unsuitable for anonymous endorsement since the voter must personally register for each election. If one who wants to endorse a subject requiring personal registration, the endorser's privacy will be violated. In this paper, we describe a practical anonymous endorsement system. By extending the *blind signature technique* [13, 14], the power of the authority can be distributed among an administrator and several scrutineers [9]. The proposed system satisfies completeness, soundness, privacy, unreusability, eligibility, and verifiability. In addition, the proposed system does not assume that the member will behave well.

## 2. REVIEW OF BLIND SIGNATURE TECHNIQUES

The concept of the blind signature was first introduced by Chaum [13], and an alternative implementation can be found in [14]. The blind signature scheme ensures that the signature requester can prevent the signer from acquiring the exact correspondence between the signed message and the signature requester. The blind signature scheme proposed in [13] is based on RSA [15], and can be restated as follows. Suppose that the private exponent, the public exponent, and the modulus of the signer, say Bob, are, respectively,  $d_{Bob}$ ,  $e_{Bob}$ , and  $n_{Bob}$ . To make the paper more concise, we define four operations:

$$\text{Sign}_{Bob}(a) \equiv a^{d_{Bob}} \pmod{n_{Bob}} \quad (1)$$

$$\text{Sign}_{Bob}^{-1}(a) \equiv a^{e_{Bob}} \pmod{n_{Bob}} \quad (2)$$

$$\text{Hide}_{Bob}(a, b) \equiv b^{e_{Bob}} \cdot a \pmod{n_{Bob}} \quad (3)$$

$$\text{Unstrap}_{Bob}(a, b) \equiv b^{-1} \cdot a \pmod{n_{Bob}} \quad (4)$$

where  $a$  and  $b \in [1, n_{Bob}-1]$ . If someone, say Alice, wishes to obtain the signature of Bob on message  $M \in [1, n_{Bob}-1]$  without revealing its content, she generates a secret number  $r \in [1, n_{Bob}-1]$ , calculates  $w = \text{Hide}_{Bob}(M, r)$ , and then sends  $w$  to Bob. Next, Bob calculates  $x = \text{Sign}_{Bob}(w)$  and sends  $x$  back to Alice. Upon receiving  $x$ , Alice first calculates  $y = \text{Unstrap}_{Bob}(x, r)$ , and then calculates  $z = \text{Sign}_{Bob}^{-1}(y)$ . Alice checks whether the equation  $z = M$  holds. If it is true, Alice has obtained  $\text{Sign}_{Bob}(M)$  without revealing its content.

The blind signature scheme can be extended to distribute the power of authority among several parties [9] in the proposed anonymous endorsement system. Suppose there are  $t$  signers,  $P_1, P_2, \dots$ , and  $P_t$  with  $M < n_{P_1} < n_{P_2} < \dots < n_{P_t}$ . We can orderly obtain the blind signature of  $P_1$  on  $M$ , the blind signature of  $P_2$  on  $\text{Sign}_{P_1}(M)$ ,  $\dots$ , and the blind signature of  $P_t$  on  $\text{Sign}_{P_{t-1}}(\text{Sign}_{P_{t-2}} \dots (\text{Sign}_{P_1}(M) \dots ))$ . We use  $\text{BS}(M | P_1, P_2, \dots, P_t)$  to denote the whole operation.

### 3. ANONYMOUS ENDORSEMENT SYSTEM

The proposed system involves an administrator ( $A$ ), a set of  $N$  scrutineer ( $S_1, S_2, \dots$ , and  $S_N$ ), and the members. Three assumptions are made in the proposed system, (1) the existence of an untraceable email system, e.g., the mix-net [1] or the dc-net [16], (2) at least one of  $A, S_1, S_2, \dots$ , and  $S_N$  is trusted, and (3) the existence of a one-way permutation function, which implies  $P \neq NP$  [17]. Although no one-way permutation function has yet been found, many researchers [8, 10, 18–20] believe that the discrete logarithm function is a candidate for the one-way permutation function. For example,  $f(x) = g^x \bmod Q$ , where  $Q$  denotes a large prime,  $x \in [1, Q-1]$  represents an integer with large entropy, and  $g$  is a generator of  $Z_Q^*$ .

The operation of the proposed system can be divided into six phases. In Phase 1 (the initiation phase),  $A, S_1, S_2, \dots$ , and  $S_N$  generate their respective RSA key pairs. In Phase 2 (the registration phase), each member registers his public key with  $A$ . In Phase 3 (the ticket distribution phase), each member receives a set of  $p$  tickets after sending a request to  $A, S_1, S_2, \dots$ , and  $S_N$  for ticket distribution. The value of  $p$  is the maximum number of endorsements that can be held following this ticket distribution. In Phase 4 (the endorsement origination phase), the subject originator sends a request to  $A$ . Then,  $A$  announces the subject, subject number (suppose  $k$ ), and the email address of the originator. In Phase 5 (the endorsement phase), if the member wants to endorse this subject, he sends his  $k^{\text{th}}$  ticket to the originator by using an untraceable email system [1, 16]. In Phase 6 (the verification and tally phase),  $A$  publishes the collected tickets sent from the originator for public verification and counting. The tally of the verified tickets in the endorsement table represents the number of endorsers of the subject.

#### Phase 1. Initiation

$A$  generates a sequence of  $p$  RSA key pairs in which  $d_{A\langle i \rangle}$ ,  $e_{A\langle i \rangle}$  and  $n_{A\langle i \rangle}$ , denote his  $i^{\text{th}}$  private exponent, public exponent, and modulus, respectively. Each  $S_j$ , where  $j \in \{1, 2, \dots, N\}$ , generates his RSA key pair in which  $d_{S_j}$  denotes the private exponent,  $e_{S_j}$  denotes the public exponent, and  $n_{S_j}$  denotes the modulus, such that  $n_{A\langle i \rangle} < n_{S_1} < n_{S_2} < \dots < n_{S_N}$  for  $i = 1, 2, \dots, p$ . In addition, a one-way permutation function  $f(\ )$  and a one-way hash function  $h(\ )$ , e.g., SHA-1 [21], are predetermined and published.

#### Phase 2. Registration

To register as a member, someone, say  $u$ , first generates his RSA key pair, including  $d_u$ ,  $e_u$ , and  $n_u$ . Next,  $u$  registers with  $e_u$  and  $n_u$  with  $A$ . After successfully authenticating

$u$ ,  $A$  calculates  $\text{Sign}_{A\langle i \rangle}(h(u \parallel e_u \parallel n_u))$  and then publishes the result and  $\{u \parallel e_u \parallel n_u\}$ , where  $\parallel$  denotes concatenation. In this phase, member's privacy is not required.

### Phase 3. Ticket Distribution

When the registration phase is completed,  $A$  originates a ticket distribution by announcing an identifier, say  $Y$ , which is an unpredictable and non-repeated number. The member  $u$  generates a sequence of long random numbers  $R_{\langle i \rangle}$ , where  $i = 1, 2, \dots, p$ , and then calculates his *hidden identities* according to the following formula:

$$\alpha_{u\langle i \rangle} = f(ID_u \parallel R_{\langle i \rangle}), \text{ for } i = 1, 2, \dots, p. \quad (5)$$

Next, member  $u$  generates a secret number  $r$ , and calculates

$$\beta_{u\langle i \rangle}^{(0)} = \text{Hide}_{A\langle i \rangle}(\{Y \parallel \alpha_{u\langle i \rangle}\}, r), \text{ for } i = 1, 2, \dots, p, \quad (6)$$

$$\text{req}_u^{(0)} = \text{Sign}_u(h(Y \parallel \beta_{u\langle 1 \rangle}^{(0)} \parallel \beta_{u\langle 2 \rangle}^{(0)} \parallel \dots \parallel \beta_{u\langle p \rangle}^{(0)})), \quad (7)$$

and sends  $\{Y \parallel \beta_{u\langle 1 \rangle}^{(0)} \parallel \beta_{u\langle 2 \rangle}^{(0)} \parallel \dots \parallel \beta_{u\langle p \rangle}^{(0)} \parallel \text{req}_u^{(0)}\}$  to  $A$ . If  $h(Y \parallel \beta_{u\langle 1 \rangle}^{(0)} \parallel \beta_{u\langle 2 \rangle}^{(0)} \parallel \dots \parallel \beta_{u\langle p \rangle}^{(0)}) \neq \text{Sign}_u^{-1}(\text{req}_u^{(0)})$ ,  $A$  rejects the request. Otherwise,  $A$  signs each  $\beta_{u\langle i \rangle}^{(0)}$  with his  $i^{\text{th}}$  private key to derive  $\text{Sign}_{A\langle i \rangle}(\beta_{u\langle i \rangle}^{(0)})$ , denoted by  $\lambda_{u\langle i \rangle}^{(0)}$ , where  $i = 1, \dots, p$ . Next,  $A$  sends  $\lambda_{u\langle i \rangle}^{(0)}$ ,  $i = 1, 2, \dots, p$ , back to  $u$ . Then,  $u$  calculates

$$t_{u\langle i \rangle}^{(0)} = \text{Unstrap}_A(\lambda_{u\langle i \rangle}^{(0)}, r), \text{ for } i = 1, 2, \dots, p. \quad (8)$$

If  $\text{Sign}_{A\langle i \rangle}^{-1}(t_{u\langle i \rangle}^{(0)}) = \{Y \parallel \alpha_{u\langle i \rangle}\}$  holds for  $i = 1, \dots, p$ , member  $u$  will believe  $\text{BS}(\{Y \parallel \alpha_{u\langle i \rangle}\} \mid A\langle i \rangle) = t_{u\langle i \rangle}^{(0)}$  where  $i = 1, \dots, p$ . After that,  $u$  calculates

$$\beta_{u\langle i \rangle}^{(1)} = \text{Hide}_{S_i}(t_{u\langle i \rangle}^{(0)}, r), \text{ for } i = 1, 2, \dots, p, \quad (9)$$

$$\text{req}_u^{(1)} = \text{Sign}_u(h(Y \parallel \beta_{u\langle 1 \rangle}^{(1)} \parallel \beta_{u\langle 2 \rangle}^{(1)} \parallel \dots \parallel \beta_{u\langle p \rangle}^{(1)})). \quad (10)$$

Next, he sends  $\{Y \parallel \beta_{u\langle 1 \rangle}^{(1)} \parallel \beta_{u\langle 2 \rangle}^{(1)} \parallel \dots \parallel \beta_{u\langle p \rangle}^{(1)} \parallel \text{req}_u^{(1)}\}$  to  $S_I$ . After verifying  $\text{req}_u^{(1)}$ ,  $S_I$  calculates and sends  $\lambda_{u\langle i \rangle}^{(1)} = \text{Sign}_{S_i}(\beta_{u\langle i \rangle}^{(1)})$ ,  $i = 1, \dots, p$ , back to  $u$ . Then,  $u$  calculates

$$t_{u\langle i \rangle}^{(1)} = \text{Unstrap}_{S_i}(\lambda_{u\langle i \rangle}^{(1)}, r), \text{ for } i = 1, 2, \dots, p. \quad (11)$$

If  $\text{Sign}_{S_i}^{-1}(t_{u\langle i \rangle}^{(1)}) = t_{u\langle i \rangle}^{(0)}$  holds for  $i = 1, \dots, p$ ,  $u$  will believe  $\text{BS}(\{Y \parallel \alpha_{u\langle i \rangle}\} \mid A\langle i \rangle, S_I) = t_{u\langle i \rangle}^{(1)}$  where  $i = 1, \dots, p$ . Similarly,  $u$  can further obtain the blind signatures of  $S_2, S_3, \dots$ , and  $S_{N-1}$  in order. Finally,  $u$  will obtain  $\text{BS}(\{Y \parallel \alpha_{u\langle i \rangle}\} \mid A\langle i \rangle, S_I, S_2, \dots, S_N)$ , i.e.,  $t_{u\langle i \rangle}^{(N)}$ , and item  $t_{u\langle i \rangle}^{(N)}$ , denoted by  $T_{u\langle i \rangle}$  for simplicity, will be used as the  $i^{\text{th}}$  ticket of member  $u$ . In this phase the serial number of  $k$  the subject being endorsed is set to one.

#### Phase 4. Endorsement Origination

If someone, say  $G$ , wants to originate an anonymous endorsement for a subject  $SUB$ , he can send his request to  $A$ . If  $SUB$  is legal,  $A$  assigns  $k$  to the identifier of  $SUB$  and announces the endorsement by publishing  $\{SUB \parallel k \parallel G \parallel AD_G\}$  and  $\text{Sign}_{A \langle k \rangle}(h(Y \parallel SUB \parallel k \parallel G \parallel AD_G))$ , where  $AD_G$  denotes the email address of  $G$ .

#### Phase 5. Endorsement

If member  $u$  wants to endorse  $SUB$ , he can send his  $k^{\text{th}}$  ticket,  $T_{u \langle k \rangle}$ , to  $G$  through an untraceable email system. All tickets received are recorded in the endorsement table.

#### Phase 6. Verification and Tally

When the endorsement phase is completed,  $G$  signs the endorsement table and sends the signature as well as the endorsement table to  $A$ . Then,  $A$  removes the duplicate tickets, and sorts and verifies the rest in the endorsement table. Next,  $A$  signs the sorted, duplicate-free and verified endorsement table, and publishes it and its signature for public verification and counting. In addition, the original endorsement table with its signature received from  $G$  is also published. Anyone can check to see whether the following equation holds:

$$\text{Sign}_{A \langle k \rangle}^{-1}(\text{Sign}_{S_1}^{-1}(\text{Sign}_{S_2}^{-1}(\dots(\text{Sign}_{S_N}^{-1}(T_{u \langle k \rangle})))))) = (Y \parallel \alpha_{u \langle k \rangle}). \quad (12)$$

If it is true, the number of endorsers for  $SUB$  is the tally of the verified tickets. In addition, the value of  $k$  is increased by one, and if  $k > p$ , the system returns to Phase 3; otherwise, the system enters Phase 4.

### 4. SECURITY ANALYSIS

Here, we adopt the security criteria [4, 10] for a voting scheme with slight modifications to evaluate the security of the proposed system.

**Theorem 1 (completeness).** All collected tickets are counted correctly.

**Sketch of Proof:** The ticket presented by each member should be counted correctly in the endorsement table. If all the hidden identities within the collected tickets are generated according to Eq.(5), all collected tickets will be accepted. However, if a member  $x$  randomly generates his hidden identity, there are two cases: (Case 1)  $\alpha_{x \langle i \rangle}$  differs from the hidden identities of other endorsers, implying that  $T_{x \langle i \rangle}$  differs from the endorsing tickets of other endorsers; or (Case 2)  $\alpha_{x \langle i \rangle}$  occasionally equals the hidden identity of a rule-abiding endorser  $y$ , which implies  $T_{x \langle i \rangle}$  collides with  $T_{y \langle i \rangle}$ . In this case, the duplicate tickets will be removed. We can reasonably regard that  $T_{y \langle i \rangle}$  is accepted, while  $T_{x \langle i \rangle}$  is rejected. On the other hand, since the tickets are collected by the originator of the anonymous endorsement rather than the administrator, it is reasonable that the collected tickets will not be intentionally dropped. Hence, the proposed system

is complete.

**Theorem 2 (soundness).** No one can disrupt the anonymous endorsement.

**Sketch of Proof:** It is only when all of  $A, S_1, S_2, \dots,$  and  $S_N$  conspire that forged tickets can be generated. However, this contradicts the assumption that at least one of  $A, S_1, S_2, \dots,$  and  $S_N$  is trusted. Therefore, the proposed system is sound.

**Theorem 3 (privacy).** The relationship between the endorser and his ticket is concealed.

**Sketch of Proof:** Since  $R_{\langle i \rangle}$  is a long random number selected by member  $u$ , it is computationally infeasible for others to deduce  $\alpha_{u\langle i \rangle}$  from  $ID_u$ , and *vice versa* according to Eq.(5). Thus, the system provides endorser's privacy.

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

**Sketch of Proof:** As each ticket can be used for one and only one specific endorsement, the proposed system satisfies unreusability.

**Theorem 5 (eligibility).** Only a member can endorse.

**Sketch of Proof:** Since the outsider can neither successfully obtain tickets nor forge valid tickets (by Theorem 2), the proposed system provides eligibility.

**Theorem 6 (verifiability).** The result of an anonymous endorsement can be verified individually and universally.

**Sketch of Proof:** By recognizing the hidden identity, the endorser can confirm whether his ticket is placed correctly in the endorsement table. Hence, the proposed system is individually verifiable. In addition, anyone can check the validity of all published tickets by using the public keys of  $A$  and the scrutineers. By Theorem 1, the system is universally verifiable.

## 5. CONCLUSIONS

We have proposed an anonymous endorsement system that can be realized on existing computer networks. We do not assume that the member must follow the hidden identity generation procedure. If a member does not generate his hidden identities accordingly, his hidden identities may collide with others. This system ensures that rule-abiding members can endorse successfully. On the contrary, the rights of the rule-contradicting members are not protected. For practical use, the proposed system can be integrated with the conventional paper-based endorsement mechanism. However, the members of the anonymous endorsement system are restricted to endorsing through the anonymous endorsement system. The endorsement of the members of the anonymous endorsement system will not be counted in the conventional paper-based endorsement book. The final endorsement result is the summation of the endorsement tally in the paper-based endorsement book and the tally of the tickets in the endorsement table.

## REFERENCES

1. D. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," *Communications of ACM*, Vol. 24, 1981, pp. 84-88.
2. D. Chaum, "Elections with unconditionally secret ballots and disruption equivalent to breaking RSA," in *Proceedings of EuroCrypt'88*, 1988, pp. 177-182.
3. K. Ohta, "An electrical voting scheme using a single administrator," 1988 *Spring National Convention Record (Japan)*, *IEICE*, Vol. 1, 1988, A-294, pp. 296.
4. A. Fujioka, T. Okamoto, and K. Ohta, "A practical secret voting scheme for large scale elections," in *Proceedings of AusCrypt'92*, 1992, pp. 244-251.
5. T. Okamoto, A. Fujioka, and K. Ohta, "A practical large scale secret voting scheme based on non-anonymous channels," in *Proceedings of the 1993 Symposium on Cryptography and Information Security*, 1993, 1C, pp. 12.
6. C. Park, K. Itoh, and K. Kurosawa, "Efficient anonymous channel and all/nothing election scheme," in *Proceedings of EuroCrypt'93*, 1994, pp. 248-258.
7. K. Sako and J. Kilian, "Receipt-free mix-type voting scheme — A practical solution to the implementation of a voting booth," in *Proceedings of EuroCrypt '95*, 1995, pp. 393-403.
8. W. Juang and C. Lei, "A collision-free secret ballot protocol for computerized general elections," *Computers & Security*, Vol. 15, 1996, pp. 339-348.
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*, 1986, pp. 52-62.
10. K. Sako and J. Kilian, "Secure voting using partially compatible homomorphisms," in *Proceedings of Crypto'94*, 1995, pp. 411-424.
11. W. Juang and C. Lei, "A secure and practical electronic voting scheme for real world environments," *IEICE Transactions on Fundamentals*, Vol. E80-A, 1997, pp. 64-71.
12. W.-C. Ku and S.-D. Wang, "A secure and practical electronic voting scheme," *Computer Communications*, Vol. 22, 1999, 279-286.
13. D. Chaum, "Blind signature for untraceable payments," in *Proceedings of Crypto'82*, 1983, pp. 199-203.
14. J. L. Camenisch, J. M. Preteau, and M. A. Stadler, "Blind signature schemes based on the discrete logarithm problem," *Rump Session of EuroCrypt'94*, 1995, pp. 428-432.
15. R. L. Rivest, A. Shamir, L. Adleman, "A method for obtaining digital signatures and public key cryptosystems," *Communications of the ACM*, 1978, pp. 120-126.
16. D. Chaum, "The dining cryptographers problem: Unconditional sender and recipient untraceability," *Journal of Cryptology*, Vol. 1, 1988, pp. 65-67.
17. M. R. Garey and D. S. Johnson, *Computer and Intractability – A Guide to The Theory of NP-Completeness*, Murray Hill, 1979.
18. T. El Gamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transactions on Information Theory*, Vol. IT-31, 1985, pp. 469-472.
19. W. Diffie and M. E. Hellman, "New direction in cryptography," *IEEE Transactions on Information Theory*, Vol. IT-22, 1976, pp. 644-654.
20. S. Pohlig and M. E. Hellman, "An improved algorithm for computing logarithms

over GF(p) and its cryptographic significance,” *IEEE Transactions on Information Theory*, Vol. IT-24, 1978, pp. 106-110.

21. National Institute of Standards and Technology, “Secure hash standard,” NIST FIPS PUB 180-1, U.S. Department of Commerce, April 1995.

**Wei-Chi Ku** (顧維祺) was born in Taiwan on April 13, 1967. He received the B.S. degree in Computer Science and Information Engineering from National Chiao Tung University, Taiwan, in 1990, and the M.S. degree in Computer Science and Information Engineering from National Cheng Kung University, Taiwan, in 1992. From 1992 to 1994, he was a Reserve Officer, and served in the National Defense Management College, Taipei, Taiwan. In 2000, he received the Ph.D. degree in Electrical Engineering from National Taiwan University, Taiwan. In 2001, he joined the faculty of the Department of Computer Science and Information Engineering at Fu Jen Catholic University, where he is currently an associate professor. His research interests include cryptology and network security.

**Sheng-De Wang** (王勝德) was born in Taiwan on November 5, 1957. He received the B.S. degree from National Tsing Hua University, Hsinchu, Taiwan, in 1980, and the M.S. and the Ph.D. degrees in Electrical Engineering from National Taiwan University, Taipei, Taiwan in 1982 and 1986, respectively. In 1986, he joined the faculty of the Department of Electrical Engineering at National Taiwan University, where he is currently a professor. His research interests include parallel processing, artificial intelligence, information security, and neuro-computing. Dr. Wang is a member of the Association for Computing Machinery, the International Neural Networks Community, and the IEEE Computer Society. He is also a member of the Phi Tau Honor society.