An Untraceable Voting Scheme Based on Pairs of Signatures

Kazi Md. Rokibul Alam[1], Adnan Maruf[1], Md. Rezaur Rahman Rakib[1], G. G. Md. Nawaz Ali[1,2], Peter Han Joo Chong[3], and Yasuhiko Morimoto[4]

(Corresponding author: G. G. Md. Nawaz Ali)

Department of CSE, Khulna University of Engineering & Technology, Khulna 9203, Bangladesh[1]
School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore[2]
Department of Electrical and Electronic Engineering, Auckland University of Technology, New Zealand[3]
Graduate School of Engineering, Hiroshima University, Higashi-Hiroshima 739-8521, Japan[4]
(Email: nawaz.ali@ntu.edu.sg)

(Received May 10, 2017; revised and accepted Sept. 9, 2017)

Abstract

This paper proposes a new electronic voting (e-voting) scheme that exploits 2 pairs of signatures of signing (election) authorities. One pair of signatures on each voter's same blinded token enables the voter to appear to authorities in consecutive election stages anonymously. Another pair of signatures on each voter's same blinded vote enables authorities to protect them from the voter's dishonesties. Namely, while a vote remains same within its 2 different signed forms, the voter cannot claim that her vote is disrupted by other entities while intentionally submitting a meaningless or invalid vote. The scheme is suitable for small community where the number of voters is not very high. Here for vote construction, Hwang *et al.*'s untraceable blind signature (BS) scheme is exploited. Thereby no mutually independent signing authority involved in the scheme is able to link the resulting vote-signature pair even when the signature is publicly revealed. When compared with existing schemes, the proposed scheme requires straightforward computations and minimal assumptions regarding trustworthiness, i.e., nothing can make the scheme unreliable while only a single authority is honest among multiple authorities. Moreover, it achieves major security aspects of e-voting in a simple way, namely, it conforms privacy, accuracy, un-reusability, fairness, universal verifiability, dispute-freeness, robustness, incoercibility and scalability

Keywords: Anonymous Credential; Electronic Voting; RSA; Signature Pairs; Untraceable Blind Signature

1 Introduction

Voting is the basic instrument to sustain democracy in any society. It authorizes an official mechanism for the people to express their views to the government. The conventional procedure of the voting system claims the voter to come in person to vote which results in low participation rate. 'Vote by e-mail' system has evolved for increasing the participation rate, especially, in the sparsely populated area. However, this process is time consuming for the authority because it demands extra effort for collecting and counting ballots manually [8]. With the promotion of computing devices, computer networks and cryptographic protocols; electronic voting (e-voting) scheme can be designed to overcome troubles of the conventional procedure. Moreover, election process can be made more appropriate and convenient by using e-voting scheme for the voter to vote at any time and place [19].

An ideal e-voting scheme must satisfy privacy, eligibility, un-reusability, accuracy, fairness, universal verifiability, dispute-freeness, receipt-freeness, robustness, incoercibility, practicality and scalability [14, 17, 24]. Among them, practicality and scalability are related with the implementation of the scheme, whereas others are regarded as security requirements. Without fulfilling these requirements, prevalent fraud and corruption may take place in the election. Nonetheless, attaining all of the requirements is a challenge. Moreover, compared to the traditional voting scheme, e-voting scheme is more vulnerable because it requires digital processing of election data.

This paper proposes a new e-voting scheme that employs 2 pairs of signatures of signing (election) authorities. A pair of signatures on each voter's same blinded vote is generated by multiple mutually independent signing authorities to ensure the correctness of vote construction and the honesty of authorities. Namely, even when unblinded signed vote in 2 different forms are meaningless, it ensures that the vote is meaningless from the beginning because it is impossible for an unauthorized entity to generate the signature pair of multiple authorities consistently. In addition, another pair of signatures on each

voter's same blinded token enables a voter to appear in consecutive election stages anonymously. Moreover, to enable a voter to be a registered one anonymously; the scheme adopts anonymous tag based credential proposed in [33].

The rest of this paper is organized as follows. Section 2 summarizes several related works with justification of the proposed scheme. Section 3 explains the cryptographic building blocks required to develop the proposed scheme. Section 4 states the configuration, Section 5 represents an overview and Section 6 illustrates the individual stages of the scheme. Section 7 discusses the performance analysis, and Section 8 describes the security analysis of the scheme. Finally, Section 9 concludes the paper.

2 Related Works

Extensive researches on e-voting schemes have been conducted till now. Recently, various homomorphic encryption, blind signature (BS) and mixnet based voting schemes have been proposed along with different cryptographic techniques. Several schemes achieve receipt-freeness by exploiting specialized hardware like tamper resistant randomizer (TRR) [20]. Moreover, to ensure the correctness of votes, they deploy zero knowledge proof (ZKP), which requires significant computations. Again, in these schemes, through specialized devices, authorities may figure out the random number of a voter and use it to link the voter which results that these schemes are not completely receipt-free. Although the criterion of TRR proposed in [20] is such that the voter who exploits it finally loses her knowledge on randomness, here TRR has impaired the practicality of this scheme. The scheme proposed in [3] satisfies major security requirements, and its deployed cryptosystem supports probabilistic, homomorphic and commutative [16] properties altogether. However, because of its exploited cryptosystem, keys of involved entities required for both encryption decryption and signing verification must be kept as secret. Therefore a voter needs to interact with authorities while encrypting her vote and/or confirming the correctness of encryption and signing operations. These increase the computation and communication overheads of involved entities, and make the scheme unscalable. The scheme proposed in [21] named as 'proxy e-voting scheme' exploits proxy signature to enable a voter to delegate a proxy to cast her vote. However because of its 'double voting detection' capability, while double voting occurs, the authority can identify the responsible voter. Thereby the link between the vote and its voter is revealed which sacrifices the privacy of the voter. Another scheme known as Helios [2], is the first web based, open auditing system that satisfies both individual and universal verifiability, but cannot provide a strong guarantee of privacy. It runs as a client program in a browser, and a voter can submit her vote by using the browser. Finally, while vote submission closes, it shuffles all encrypted votes to disable the link between a vote and its voter, and produces a non-interactive ZKP to prove the correctness of shuffling. In contrast, the vote construction procedure in our proposed scheme deploys public keys of signing authorities. Note that our scheme does not use either any complicated protocol like ZKP or any specialized hardware or software. Moreover, it ensures the privacy of the voter, does not reveal her identity in any circumstances, even if she submits a meaningless vote to disrupt voting.

E-voting schemes based on BS are simple and efficient to implement, support flexible vote formats and do not exploit complicated ZKP. But the voter's blinding factors can be used as a receipt of the vote and thereby the receipt-freeness is sacrificed. Also, since every vote is blinded and unblinded only by its corresponding voter, this yields universal verifiability [14, 28]. A scheme proposed in [11] is based on Chaum's BS. Herein while voting, a registered voter submits her unblinded signed vote anonymously. Later on, a list of received ballots is published that is accessible by all voters. Finally in order to decrypt the vote, each voter needs to interact with the tallying authority by sending her private key. Although the scheme satisfies privacy, fairness, scalability, etc; its' major limitation is that the registration authority can detect the abstaining registered voters and can add votes for them. The scheme proposed in [32] exploits a uniquely threshold BS to get blind threshold votes, and allows any registered voter to abstain from vote submission. It also uses threshold cryptosystem to guarantee the fairness among the candidates campaign. Although it satisfies practicality, scalability and robustness; it can achieve fairness and accuracy conditionally. Another scheme proposed in [6] deploys pseudo-voter identity (PVID) developed by Chaum's BS to ensure the voter's anonymity. It does not use other complex cryptographic algorithms like ZKP or homomorphic encryption, and has no physical assumptions such as untappable channels. However, it has shortcoming, i.e., while ballot generator, key generator and counter work together and conspire, they can modify casted votes. Also there is possibility that corrupted authority may trace the voter's IP over the internet. Moreover, the scheme is not so robust and can satisfy fairness and practicality conditionally. In contrast, though our proposed scheme is also based on BS, it deploys Hwang *et al.*'s BS which is utterly untraceable. Also, it engages multiple mutually independent signing authorities; thereby nothing can make the scheme unreliable while at least a single authority is honest. Moreover herein, since data about interactions among entities are publicly verifiable; disputes are resolvable.

Recently proposed some other schemes are Civitas [9], UVote [1], Cobra [4, 10] *etc.* Among them, Civitas [9] is based on the mechanism proposed in [18] and aims to satisfy both verifiability and incoercibility. However to attain incoercibility, it allows the voter to submit multiple votes where multiple votes with the same token are excluded during the tallying. Herein, each voter needs to include ZKPs indicating which earlier votes to be erased as well as

showing the knowledge of the choice and the token used in earlier votes. The scheme proposed in [4] also exploits ZKP. Although here incoercibility is achieved; unfortunately scalability and accuracy are traded-off. UVote [1] allows a registered voter to submit multiple votes from which only the last vote is counted, and thus satisfies incoercibility. Here initially a voter needs to register her primary account, and later on can add multiple accounts. But for verification, any notification and message is sent only to the primary account and it cannot be deleted online. Thus although verifiability is achieved, receipt-freeness is sacrificed because a receipt is provided to the voter. In Cobra [10], a registered voter's encrypted credential is attached with an encrypted bloom filter. The voter selects certain number of candidate passwords and registers anyone of them. Later on, the voter encrypts her vote using the registered password to regenerate the credential. Herein, as the voter can provide a fake or a panic password to the coercer and thereby he is unable to manipulate the voter; incoercibility is achieved but thereby verifiability is traded. On the contrary, our proposed scheme does not allow a voter either to use a fake credential or to submit her vote multiple times. Each voter appears to authorities for submitting and approving her vote anonymously. Also it exploits a pair of signatures of signing authorities on each voter's same blinded vote, i.e., each vote is constructed in 2 different forms that ensures the honesty of authorities.

There are some schemes known as paper based cryptographic voting schemes which are based on visual cryptography [5, 27]. However herein; a voter needs to envoy her computations in the voting booth. Therefore, the booth can easily identify the vote of a voter. Again, the paper ballots prepared in advance do not ensure privacy against its creators' [27]. Considering commercial e-voting scheme, Sandler *et al.* [30] have developed voting scheme which is based on cryptographic techniques and hardware/machines, like optical scan voting machine, direct/digital-recording electronic (DRE), *etc.* Being different, our proposed scheme is based on pairs of signatures, which does not require any complicated protocol, or any specialized hardware, but still it can provide a reliable voting scheme while only a single authority is honest among multiple authorities.

3 Cryptographic Building Blocks

The proposed scheme exploits several cryptographic tools. These are: Hwang *et al.*'s BS [25] for blinded signed vote construction, and Chaum' BS [7] for blinded signed token generation. Also, a pair of signatures on each voter's same blinded token is generated by signing authorities. Moreover, a pair of signatures of signing authorities on each voter's same blinded vote is generated. Besides while token acquisition, to authenticate a voter anonymously many mechanisms [13, 26, 33] are available and any one can be used, namely anonymous tag based credential proposed in [33]. This section describes the major cryptographic tools. Further, important notations that are used in this paper are summarized in Table 1.

3.1 Chaum's Blind Signature

Chaum's BS proposed in [7] is based on RSA cryptosystem and consists of five phases which are briefly described as follows.

1) *Initializing phase:* The signer (i.e., herein an election authority TM_i) randomly chooses 2 large primes p and q, and computes $n = p * q$ and $\varphi(n) = (p-1)*(q-1)$. The authority chooses 2 large numbers e and d such that $ed \equiv 1 \ mod \ \varphi(n)$ and the greatest common divisor (GCD) $(e, \varphi(n)) = 1$. Let (e, n) be the authority's public key and d be the authority's private signing key. The authority keeps (p, q, d) secure and publishes (e, n).

2) *Blinding phase:* The voter V_j has a message (i.e., herein the token T_j), and she wishes to have it signed by the authority. Now V_j randomly selects an integer r_j as the blinding factor, and computes the integer $\alpha = r_j^e * T_j \ mod \ n$ and submits it to the authority.

3) *Signing phase:* After receiving α from V_j, the authority computes the integer $t = \alpha^d \ mod \ n$ and sends it to V_j.

4) Unblinding phase: After receiving t from the authority, voter V_j computes $s = t * r_j^{-1} \ mod \ n$.

5) *Verifying phase:* As a result, s is the signature on the token T_j. Now anyone can verify the legitimacy of the signature by checking whether $s^e \equiv T_j \ mod \ n$.

Signature pairs on blinded token discussed in Section 3.3 is constructed based on this BS because cryptographic operations involved in its various phases are straightforward and their computations are also faster than that of Hwang *et al.*'s BS. Although it has some limitations [25], it is capable to conduct the registration stage (as discussed in Section 6.2) of the proposed scheme. Therefore instead of Hwang *et al.*'s BS, it is chosen here.

3.2 Hwang *et al.*'s Blind Signature

Hwang *et al.*'s BS proposed in [25] is also based on RSA cryptosystem. The advantage of this BS is that it satisfies requirements of an ideal BS scheme and specially overcomes the limitation of untraceability of Chaum's BS. Although a great number of BS schemes are available, most of them are unable to satisfy untraceability [25]. There are some untraceable BS schemes based on discrete logarithm problem proposed in [22,23]. However for vote construction, RSA based Hwang *et al.*'s BS is chosen for our proposed e-voting scheme. This is because, RSA based schemes are by far the easiest to understand and implement among all the public-key algorithms proposed over

Table 1: List of notations used in this paper

Notation	Description
V_j	Any Voter
v_j	Vote of V_j
T_j, r_j	Token and secret integer of V_j to blind T_j
ID_j, P/W_j	Identity and password of V_j
$T_j(A, ID_j, Z_j)$	Anonymous credential of V_j
$Z_j, U_j^{Z_j}$	A secret integer and used seal of V_j
A	Credential issuer
VM	Voting manger
TMs or $TM_1, \cdots, TM_P$	$P(\geq 2)$ Tallying managers
$e_{(1*)}, e_{(2*)}$	To blind T_j, 1st and 2nd form of public keys of $TM_1, \cdots, TM_P$
$d_{(1*)}, d_{(2*)}$	To sign on blinded T_j, 1st and 2nd form of signing keys of $TM_1, \cdots, TM_P$
$\alpha_{*1(rj,Tj)}$, $\alpha_{*2(rj,Tj)}$	1st and 2nd form of blinded T_j of V_j
$t(d_{(1*)}, \alpha_{*1}(r_j, T_j))$, $t(d_{(2*)}, \alpha_{*2}(r_j, T_j))$	1st and 2nd form of blinded signed T_j of V_j
$s(d_{(1*)}, T_j), s(d_{(2*)}, T_j)$	1st and 2nd form of unblinded signed T_j of V_j
$(r_{1j}, r_{2j}), (a_{1j}, a_{2j})$	Pair of secret integers and primes of V_j to blind v_j
$\{b_{(1*)}, b_{(2*)}\}$, $\{b'_{(1*)}, b'_{(2*)}\}$	2 pairs of primes of TM_1, $\cdots$, TM_P to sign on blinded v_j in 2 different forms
$e'_{(1*)}, e'_{(2*)}$	To blind v_j, 1st and 2nd form of public keys of $TM_1, \cdots, TM_P$
$d'_{(1*)}, d'_{(2*)}$	To sign on blinded v_j, 1st and 2nd form of signing keys of $TM_1, \cdots, TM_P$
$\{(w_{11j}, \cdots, w_{1Pj}), (u_{11j}, \cdots, u_{1Pj})\}$, $\{(w_{21j}, \cdots, w_{2Pj}), (u_{21j}, \cdots, u_{2Pj})\}$	2 pairs of integers of V_j to unblind v_j
$\alpha_{1*j}, \alpha_{2*j}$	1st and 2nd form of blinded v_j of V_j
$t_1(d'_{(1*)}, (\alpha_{1*j}, \alpha_{2*j}))$, $t_2(d'_{(2*)}, (\alpha_{1*j}, \alpha_{2*j}))$	1st and 2nd forms of blinded signed v_j of V_j
$s_1(d'_{(1*)}, v_{j*})$, $s_2(d'_{(2*)}, v_{j*})$	1st and 2nd form of unblinded signed v_j of V_j
BBs	Bulletin Boards

the years [31]. This BS also consists of five phases which are described as follows.

1) Initializing phase: This phase is same as the initializing phase in Chaum's BS. The authority TM_i keeps (p, q, d) secure where d is the authority's secret signing key and publishes (e, n) as public key.

2) Blinding phase: The voter V_j has a message (i.e., herein the vote v_j), and she wishes to have it signed by the authority. For this purpose, V_j randomly selects 2 distinct integers' r_1 and r_2 as the blinding factors. Then she randomly chooses 2 primes a_1 and a_2 such that $a_1 \neq a_2$ and $GCD\,(a_1, a_2)$, is 1. Then, V_j computes the blinded messages $\alpha_1 = r_1^e * v_j^{a_1}\ mod\ n$ and $\alpha_2 = r_2^e * v_j^{a_2}\ mod\ n$, and sends (α_1, α_2) to the authority.

3) Signing phase: After receiving (α_1, α_2) from V_j, the authority randomly chooses 2 primes b_1 and b_2 such that $b_1 \neq b_2$ and $GCD\,(b_1, b_2)$ is 1, and signs the blinded vote by computing $t_1 = \alpha_1^{(b_1 d)}\ mod\ n$ and $t_2 = \alpha_2^{(b_2 d)}\ mod\ n$. Then the authority sends them back to V_j along with (b_1, b_2). Note that (t_1, t_2, b_1, b_2) denote the blinded signatures.

4) Unblinding phase: After receiving (t_1, t_2, b_1, b_2) from the authority, voter V_j computes $a_1 b_1$ and $a_2 b_2$. Due to the four distinct primes (a_1, a_2, b_1, b_2) where $GCD\,(a_1, a_2) = 1$ and $GCD\,(b_1, b_2) = 1$, $GCD\,(a_1 b_1, a_2 b_2)$ is also equal to 1. When $GCD\,(a_1 b_1, a_2 b_2) = 1$, there must be exactly 2 integers w and u that satisfy the equation $a_1 b_1 w + a_2 b_2 u = 1$. It is called the Extended Euclidean algorithm. The four parameters (a_1, a_2, w, u) are kept secret by the V_j. Now the V_j computes $s_1 = t_1 * r_1^{-b_1} = v_j^{a_1 b_1 d}\ mod\ n$ and $s_2 = t_2 * r_2^{-b_2} = v_j^{a_2 b_2 d}\ mod\ n$. Then V_j can derive the signature s by computing $s = s_1^w * s_2^u\ mod\ n$ and publishes (v_j, s).

5) Verifying phase: As a result, s is the signature on the vote v_j. Now anyone can verify the legitimacy of the signature by checking whether $s^e \equiv v_j\ mod\ n$. In the following the notation $(mod\ n)$ is omitted.

Signature pairs on blinded vote discussed in Section 3.4 is constructed based on this scheme. As the scheme is completely untraceable, no one can know the link between the blinded signed vote of a voter and its corresponding unblinded signed form, therefore it is chosen here.

3.3 Signature Pairs on Blinded Token

Voter can act without disclosing her identity while showing her eligibility by using token. To prove her eligibility anonymously, voter V_j blinds her token T_j in 2 different sets i.e., calculates $\alpha_{*1}(r_j, T_j) = \{\alpha_{11}(r_j, T_j), \cdots, \alpha_{1P}(r_j, T_j)\} = \{(r_j^{e_{11}} * T_j), \cdots, (r_j^{e_{1P}} * T_j)\}$ and $\alpha_{*2}(r_j, T_j) = \{\alpha_{21}(r_j, T_j), \cdots, \alpha_{2P}(r_j, T_j)\} = \{(r_j^{e_{21}} * T_j), \cdots, (r_j^{e_{2P}} * T_j)\}$ using her secret blinding factor r_j and

authorities' public keys $e_{(1*)} = \{e_{(11)}, \cdots, e_{(1P)}\}$ and $e_{(2*)} = \{e_{(21)}, \cdots, e_{(2P)}\}$, respectively. While confirming the identity of V_j by anonymous tag based credential i.e., $T_j(A, ID_j, Z_j)$ of V_j, authorities $TM_1, \cdots, TM_P$ blindly sign on $\alpha_{*1}(r_j, T_j)$ and $\alpha_{*2}(r_j, T_j)$ to generate 2 different sets i.e., $t(d_{(1*)}, \alpha_{*1}(r_j, T_j)) = \{t(d_{(11)}, \alpha_{11}(r_j, T_j)), \cdots, t(d_{(1P)}, \alpha_{1P}(r_j, T_j))\} = \{\alpha_{11}(r_j, T_j)^{d_{11}}, \cdots, \alpha_{1P}(r_j, T_j)^{d_{1P}}\}$ and $t(d_{(2*)}, \alpha_{*2}(r_j, T_j)) = \{t(d_{(21)}, \alpha_{21}(r_j, T_j)), \cdots, t(d_{(2P)}, \alpha_{2P}(r_j, T_j))\} = \{\alpha_{21}(r_j, T_j)^{d_{21}}, \cdots, \alpha_{2P}(r_j, T_j)^{d_{2P}}\}$ by using their secret signing keys $d_{(1*)} = \{d_{(11)}, \cdots, d_{(1P)}\}$ and $d_{(2*)} = \{d_{(21)}, \cdots, d_{(2P)}\}$, respectively. Now V_j unblinds them into 2 unblinded signed tokens i.e., $s(d_{(1*)}, T_j) = \{s(d_{(11)}, T_j), \cdots, s(d_{(1P)}, T_j)\} = \{(\alpha_{11}(r_j, T_j)^{d_{11}}) * r_j^{-1}, \cdots, (\alpha_{1P}(r_j, T_j)^{d_{1P}}) * r_j^{-1}\}$ and $s(d_{(2*)}, T_j) = \{s(d_{(21)}, T_j), \cdots, s(d_{(2P)}, T_j)\} = \{(\alpha_{21}(r_j, T_j)^{d_{21}}) * r_j^{-1}, \cdots, (\alpha_{2P}(r_j, T_j)^{d_{2P}}) * r_j^{-1}\}$. Then, because authorities TMs have signed without knowing T_j, no one except V_j can know V_j from $s(d_{(1*)}, T_j)$ and $s(d_{(2*)}, T_j)$.

3.4 Signature Pairs on Blinded Vote

In vote submission stage the voter V_j uses her secret blinding factors (r_{1j}, r_{2j}), a pair of primes (a_{1j}, a_{2j}) and 1st form of public keys $e'_{(1*)} = \{e'_{(11)}, \cdots, e'_{(1P)}\}$ of authorities $TM_1, \cdots, TM_P$ to blind her vote v_j in the 1st form *i.e.*, V_j calculates $\alpha_{1*j} = \{(\alpha_{111j}, \alpha_{211j}), \cdots, (\alpha_{11Pj}, \alpha_{21Pj})\} = \{\{(r_{1j}{}^{e'11} * v_j{}^{a1j}), (r_{2j}{}^{e'11} * v_j{}^{a2\ j})\}, \cdots, \{(r_{1j}{}^{e'1P} * v_j{}^{a1j}), (r_{2j}{}^{e'1P} * v_j{}^{a2j})\}\}$. Similarly using 2nd form of public keys $e'_{(2*)} = \{e'_{(21)}, \cdots, e'_{(2P)}\}$ of $TM_1, \cdots, TM_P$, V_j blinds her v_j in the 2nd form *i.e.*, calculates $\alpha_{2*j} = \{(\alpha_{121j}, \alpha_{221j}), \cdots, (\alpha_{12Pj}, \alpha_{22Pj})\} = \{\{(r_{1j}{}^{e'21} * v_j{}^{a1j}), (r_{2j}{}^{e'21} * v_j{}^{a2j})\}, \cdots, \{(r_{1j}{}^{e'2P} * v_j{}^{a1j}), (r_{2j}{}^{e'2P} * v_j{}^{a2j})\}\}$. Here V_j blinds her vote *i.e.*, calculates $(\alpha_{1*j}, \alpha_{2*j})$ using individual public keys of independent authorities. Now authorities $TM_1, \cdots, TM_P$ sign on $(\alpha_{1*j}, \alpha_{2*j})$ using their 2 different sets of signing keys to generate 2 different forms of blinded signed vote. The 1st form of blinded signed vote is calculated as $t_1(d'_{(1*)}, (\alpha_{1*j}, \alpha_{2*j})) = \{(t_{111}, t_{211}), \cdots, (t_{11P}, t_{21P})\} = \Big\{\{(\alpha_{111j}{}^{b11d'11}), (\alpha_{211j}{}^{b21d'11})\}, \cdots, \{(\alpha_{11Pj}{}^{b1Pd'1P}), (\alpha_{21Pj}{}^{b2Pd'1P})\}\Big\}$. Similarly the 2nd form of blinded signed vote is calculated as $t_2(d'_{(2*)}, (\alpha_{1*j}, \alpha_{2*j})) = \{(t_{121}, t_{221}), \cdots, (t_{12P}, t_{22P})\} = \Big\{\{(\alpha_{121j}{}^{b'11d'21}), (\alpha_{221j}{}^{b'21d'21})\}, \cdots, \{(\alpha_{12Pj}{}^{b'1Pd'2P}), (\alpha_{22Pj}{}^{b'2Pd'2P})\}\Big\}$. Here 2 forms of blinded signed vote *i.e.*, $t_1(d'_{(1*)}, (\alpha_{1*j}, \alpha_{2*j}))$ and $t_2(d'_{(2*)}, (\alpha_{1*j}, \alpha_{2*j}))\}$ are generated by using the pair of signing keys $(d'_{(1*)}, d'_{(2*)})$ and 2 pairs of primes $\{(b_{(1*)}, b_{(2*)}), (b'_{(1*)}, b'_{(2*)})\}$ of $TM_1, \cdots, TM_P$ respectively; where $d'_{(1*)} = \{d'_{(11)}, \cdots, d'_{(1P)}\}$, $d'_{(2*)} = \{d'_{(21)}, \cdots, d'_{(2P)}\}$ and $b_{(1*)} = \{b_{(11)}, \cdots, b_{(1P)}\}$, $b_{(2*)} = \{b_{(21)}, \cdots, b_{(2P)}\}$, $b'_{(1*)} = \{b'_{(11)}, \cdots, b'_{(1P)}\}$, $b'_{(2*)} = \{b'_{(21)}, \cdots, b'_{(2P)}\}$. Now V_j generates 2 forms of unblinded signed vote from her blinded signed vote *i.e.*, calculates the 1st form $s_1(d'_{(1*)}, v_{j*}) = \{\{((v_j^{a_1jb_{11}d'_{11}})^{w_{11}}) \times ((v_j^{a_2jb_{11}d'_{11}})^{u_{11}})\}, \cdots, \{((v_j^{a_1jb_1Pd'_1P})^{w_1P}) \times ((v_j^{a_2jb_2Pd'_1P})^{u_1P})\}\}$ and the 2nd form $s_2(d'_{(2*)}, v_{j*}) = \{\{((v_j^{a_1jb_{21}d'_{21}})^{w_{21}}) \times ((v_j^{a_2jb_{21}d'_{21}})^{u_{21}})\}, \cdots, \{((v_j^{a_1jb_1Pd'_2P})^{w_2P}) \times ((v_j^{a_2jb_2Pd'_2P})^{u_2P})\}\}$. Herein for convenience, the signature derivation of the unblinding phase of Hwang *et al.*'s BS is directly shown where $\Big\{\{(w_{11j}, \cdots, w_{1Pj}), (u_{11j}, \cdots, u_{1Pj})\}$ and $\{(w_{21j}, \cdots, w_{2Pj}), (u_{21j}, \cdots, u_{2Pj})\}\Big\}$ are 2 pairs of integers of V_j. When each authority TM_i signs on $(\alpha_{1*j}, \alpha_{2*j})$ by his 2 different signing keys, it is impossible for any other entity to consistently generate 2 different signed forms *i.e.*, $\{t_1(d'_{(1*)}, (\alpha_{1*j}, \alpha_{2*j})), t_2(d'_{(2*)}, (\alpha_{1*j}, \alpha_{2*j}))\}$ in an unauthorized way because each TM_i knows only his secret signing key. V_j can convince herself that TMs have signed on $(\alpha_{1*j}, \alpha_{2*j})$ honestly when she unblinds $\{t_1(d'_{(1*)}, (\alpha_{1*j}, \alpha_{2*j})), t_2(d'_{(2*)}, (\alpha_{1*j}, \alpha_{2*j}))\}$ to $\{s_1(d'_{(1*)}, v_{j*}), s_2(d'_{(2*)}, v_{j*})\}$ and verifies the signatures.

3.5 Anonymous Tag Based Credential

Anonymous tag based credential $T_j(A, ID_j, Z_j)$ proposed in [33] provided by the credential issuer A enables a voter V_j to prove her eligibility to any entity e.g. voting manager VM without revealing her identity where ID_j and Z_j is the identity and a secret random integer of V_j. Here initially V_j shows her identity to A, then A gives the credential $T_j(A, ID_j, Z_j)$ to V_j if she is eligible. Later on, any entity including VM can force V_j to calculate the used seal $U_j^{Z_j}$ $(mod\ n)$ from a given integer U_j while using Z_j in $T_j(A, ID_j, Z_j)$ honestly without knowing Z_j himself. Here n is a large and appropriate public integer associated with $T_j(A, ID_j, Z_j)$ and in the following, the notation $(mod\ n)$ is omitted. Then, any entity like VM can use $U_j^{Z_j}$ as an evidence that V_j had shown $T_j(A, ID_j, Z_j)$ to him. In conclusion, together with the used seal $U_j^{Z_j}$ anonymous credential $T_j(A, ID_j, Z_j)$ satisfies anonymity, unlinkability, verifiability, unforgeability, soundness, and revocability [29, 33].

4 Configuration of the Scheme

The proposed scheme consists of N voters $V_j (j = 1, \cdots, N)$ where j means j-th voter, a single (or multiple) Voting manger VM, P mutually independent Tallying managers TM_i $(i = 1, \cdots, P)$ where P is at least 2, Credential issuer A and four bulletin boards (BBs) [17] namely, *VoterList, TokenList, VotingBoard* and *TallyingBoard*. Figure 1 shows the configurations of each BB at some arbitrary point during the election. Here all the relevant information of interactions among the entities at every stage of the election are posted on BBs, thereby the scheme becomes publicly verifiable. Roles of the above

ID	credential	blinded token
ID_1	$T_1(A, ID_1, Z_1)$	$\alpha_{*1}(r_1, T_2)$, $\alpha_{*2}(r_1, T_2)$
. . .	. . .	. . .
ID_j	$T_j(A, ID_j, Z_j)$	$\alpha_{*1}(r_j, T_j)$, $\alpha_{*2}(r_j, T_j)$
. . .	. . .	. . .
ID_N	$T_N(A, ID_N, Z_N)$	$\alpha_{*1}(r_N, T_8)$, $\alpha_{*2}(r_N, T_8)$

(a) VoterList

token	seal
T_1	-
. . .	. . .
T_j	U_j^{Zj}
. . .	. . .
T_N	U_N^{ZN}

(b) TokenList

blinded vote	approval
$\{t_1(d'_{(1*)}, (\alpha_{1*q}, \alpha_{2*q})), t_2(d'_{(2*)}, (\alpha_{1*q}, \alpha_{2*q}))\}$	$s(d_{(1*)}, T_{11})$
. . .	. . .
$\{t_1(d'_{(1*)}, (\alpha_{1*j}, \alpha_{2*j})), t_2(d'_{(2*)}, (\alpha_{1*j}, \alpha_{2*j}))\}$	$s(d_{(1*)}, T_j)$
. . .	. . .
$\{t_1(d'_{(1*)}, (\alpha_{1*c}, \alpha_{2*c})), t_2(d'_{(2*)}, (\alpha_{1*c}, \alpha_{2*c}))\}$	$s(d_{(1*)}, T_N)$

(c) VotingBoard

unblinded vote	approval
$s_1(d'_{(1*)}, v_{q*}), s_2(d'_{(2*)}, v_{q*})$	$s(d_{(2*)}, T_{11})$
. . .	. . .
$s_1(d'_{(1*)}, v_{j*}), s_2(d'_{(2*)}, v_{j*})$	$s(d_{(2*)}, T_j)$
. . .	. . .
$s_1(d'_{(1*)}, v_{c*}), s_2(d'_{(2*)}, v_{c*})$	$s(d_{(2*)}, T_N)$

(d) TallyingBoard

Figure 1: Configuration of bulletin boards

mentioned entities are as follows:

Voter V_j: Each voter V_j has her own ID_j and P/W_j to prove her eligibility to the credential issuer A while obtaining anonymous credential $T_j(A, ID_j, Z_j)$ from him. V_j uses seal $U_j^{Z_j}$ to approve the acquisition of unused token T_j, and secret blinding factor r_j to blind her token T_j to $\{\alpha_{*1}(r_j, T_j)$ and $\alpha_{*2}(r_j, T_j)\}$. She also has a pair of blinding factor $\{r_{1j}, r_{2j}\}$, a pair of primes $\{a_{1j}, a_{2j}\}$ and another 2 pairs of integers $\Big\{\{(w_{11j}, \cdots, w_{1Pj}), (u_{11j}, \cdots, u_{1Pj})\}$ and $\{(w_{21j}, \cdots, w_{2Pj}), (u_{21j}, \cdots, u_{2Pj})\}\Big\}$ to blind and unblind her vote v_j.

Voting manager *VM*: *VM* verifies V_j's eligibility anonymously using $T_j(A, ID_j, Z_j)$, puts voter's seal $U_j^{Z_j}$ on TokenList, blinded votes on *VotingBoard* and maintains *VoterList*, and *TallyingBoard* by putting data about voters, tokens and unblinded votes. *VM* also signs on each T_j prior to post on *TokenList*. If necessary multiple independent *VM* can be constructed for distributing its responsibility and achieving more reliability.

Tallying managers *TMs*: There are $P(P \geq 2)$ mutually independent TMs. Each TM_i has the responsibility to sign on blinded token $\{\alpha_{*1}(r_j, T_j)$ and $\alpha_{*2}(r_j, T_j)\}$ and blinded vote $(\alpha_{1*j}, \alpha_{2*j})$ with his 2 different forms of signing keys. TM_i has a pair of signing keys $\{d_{(1i)}, d_{(2i)}\}$ to sign on blinded token $\Big\{\alpha_{*1}(r_j, T_j)$ and$\alpha_{*2}(r_j, T_j)\Big\}$ in 2 different forms. To sign on a blinded vote he has a pair of signing keys $\{d'_{(1i)}, d'_{(2i)}\}$ and another 2 pairs of primes $\Big\{b_{(1i)}, b_{(2i)}\Big\}$, $\{b'_{(1i)}, b'_{(2i)}\}$. Here each signing key has its corresponding public key.

Credential issuer A: A is responsible to generate and issue an anonymous tag based credential $T_j(A, ID_j, Z_j)$ to each V_j.

VoterList: 3 parts named ID, credential and token parts form *VoterList*. ID part contains the ID_j of eligible V_j, credential part contains anonymous credential $T_j(A, ID_j, Z_j)$ and token part contains the blinded form of token i.e., $\Big\{\alpha_{*1}(r_j, T_j)$ and $\alpha_{*2}(r_j, T_j)\Big\}$ of its corresponding voter's ID as shown in Figure 1 (a). As this is a BB, anyone can monitor the list.

TokenList: *TokenList* consists of the token and seal parts, and permits an anonymous V_j to acquire T_j without collision. The token part maintains tokens i.e., unique numbers already prepared by *VM*. Through anonymous credential [33] while voter V_j picks a token T_j, *VM* puts V_j's seal $U_j^{Z_j}$ on seal part of *TokenList* as shown in Figure 1 (b).

VotingBoard: *VotingBoard* consists of the blinded vote and the approval part. Blinded vote part at t_j-th position contains 2 different forms of blinded signed vote of the voter to whom t_j-th token T_j is assigned. So, vote part consists of TMs' 1st and 2nd forms of signatures on blinded vote i.e., $t_1\Big(d'_{(1*)}, (\alpha_{1*j}, \alpha_{2*j})\Big)$ and $t_2\Big(d'_{(2*)}, (\alpha_{1*j}, \alpha_{2*j})\Big)$. Approval part contains the 1st form of unblinded signed T_j i.e., $s(d_{(1*)}, T_j)$ that approves the vote of V_j on *VotingBoard* as shown in Figure 1(c).

TallyingBoard: *TallyingBoard* contains an unblinded vote part and an approval part. Unblinded vote part contains the vote unblinded by its voter in 2 different signed forms i.e., $s_1(d'_{(1*)}, v_{j*})$ and $s_2(d'_{(2*)}, v_{j*})$. V_j approves the correctness of *TMs* signatures on her unblinded vote by putting the 2nd form of unblinded signed T_j i.e., $s(d_{(2*)}, T_j))$ signed by *TMs* on the approval part of TallyingBoard as shown in Figure 1 (d). Anyone can monitor voters who have unblinded and approved their votes.

5 Overview of the Scheme

The proposed scheme consists of 4 stages and this section briefly describes them as follows. Figure 2 represents the relationships and the data flows among entities involved in the stages of the scheme.

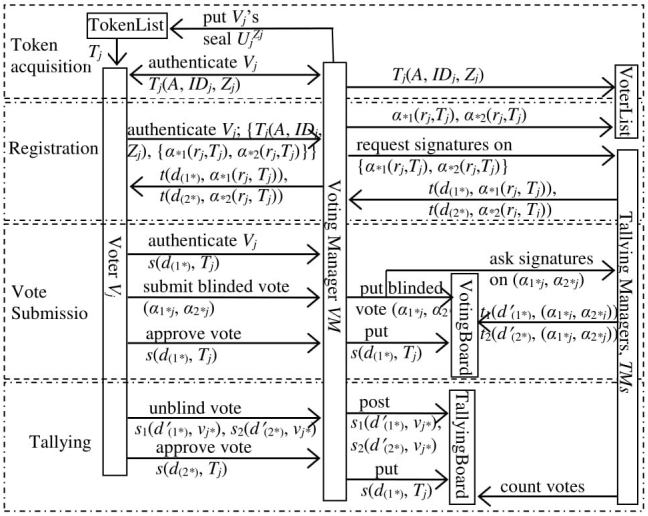

Figure 2: Relationships and data flow among entities of the scheme

5.1 Token Acquisition

Using anonymous credential $T_j(A, ID_j, Z_j)$ and seal $U_j^{Z_j}$, each anonymously authenticated voter V_j picks an unused token T_j from *TokenList*.

5.2 Registration

Voter V_j gets herself authenticated using credential $T_j(A, ID_j, Z_j)$. Then V_j submits her blinded token T_j i.e., $\left\{\alpha_{*1}(r_j, T_j) \text{ and } \alpha_{*2}(r_j, T_j)\right\}$ to *VM* to post it on *VoterList*. V_j gets 2 kinds of signatures of TMs on blinded T_j i.e., $t(d_{(1*)}, \alpha_{*1}(r_j, T_j))$ and $t(d_{(2*)}, \alpha_{*2}(r_j, T_j))$. These 2 forms of signed T_j help V_j to prove her eligibility in further stages. 1st form of unblinded signed T_j i.e., $s(d_{(1*)}, T_j)$ is used to approve V_j's vote on VotingBoard and 2nd form of unblinded signed T_j i.e., $s(d_{(2*)}, T_j))$ is used to approve V_j's unblinded signed vote on *TallyingBoard*.

5.3 Vote Submission

Employing Hwang *et al.*'s BS, V_j calculates $(\alpha_{1*j}, \alpha_{2*j})$ as her blinded vote as described in Section 3.4 and submits it along with $s(d_{(1*)}, T_j)$ to *VM*, to put $(\alpha_{1*j}, \alpha_{2*j})$ on *VotingBoard*. TMs sign on it by their 1st and 2nd form of signing keys i.e., produce $t_1(d'_{(1*)}, (\alpha_{1*j}, \alpha_{2*j}))$ and $t_2(d'_{(2*)}, (\alpha_{1*j}, \alpha_{2*j}))$. While checking her blinded vote on *VotingBoard*, V_j approves it by putting $s(d_{(1*)}, T_j)$ on the approval part of *VotingBoard*.

5.4 Tallying

While vote submission ends, every V_j unblinds her blinded signed vote by calculating $s_1(d'_{(1*)}, v_{j*})$ and $s_2(d'_{(2*)}, v_{j*})$ as discussed in Section 3.4. V_j checks the correctness of TMs' signatures and submits $s_1(d'_{(1*)}, v_{j*})$ and $s_2(d'_{(2*)}, v_{j*})$ to *VM* to be posted on *TallyingBoard*. Also by putting $s(d_{(2*)}, T_j)$ on the approval part of *TallyingBoard*, V_j approves her unblinded signed vote.

6 Individual Stages of the Scheme

The stages of the scheme proceed as follows.

6.1 Token Acquisition Stage

In this stage each voter V_j acquires a token T_j which is unique in the system, while maintaining the anonymity of V_j. For this purpose, at least N pre-generated tokens are put in *TokenList* from where a voter picks her token without collisions; where N is the number of eligible voters. Every T_j of *TokenList* has the signature of *VM* (this signature is different from $s(d_{(1*)}, T_j)$ and $s(d_{(2*)}, T_j)$, and ensures that T_j has been picked from *TokenList*). The authentication of V_j in this stage is not so essential. But the use of anonymous credential $T_j(A, ID_j, Z_j)$ protects T_j from being picked by unauthorized entities; and thereby *TokenList* remains as small as possible. During this stage V_j and *VM* interacts as follows:

1) *VM* anonymously authenticates eligible voter V_j by anonymous tag based credential [33].

2) After authentication, *VM* updates *VoterList* by putting $T_j(A, ID_j, Z_j)$ as shown in Figure 1(a).

3) Authenticated V_j picks an unused token T_j form *TokenList*, and *VM* puts his signature on the T_j (although this notation of signature is omitted in this paper). Now V_j submits her seal $U_j^{Z_j}$ to *VM*.

4) As T_j has been picked up by V_j, *VM* puts the seal $U_j^{Z_j}$ of V_j corresponding to it on *TokenList* as shown in Figure 1(b).

Security issues of this stage are as follows:

- *Single V_j may get multiple tokens:* *VM* puts the seal $U_j^{Z_j}$ of V_j corresponding to her T_j on *TokenList* in exchange of the credential. Therefore V_j cannot request multiple tokens.

- *A voter may not get a token:* As at least N tokens are generated, every voter gets a token. If any V_j cannot get a token, she can request repeatedly.

- A voter may use her own token: On T_j to get the signatures of *TMs*, *VM* accepts a token that has his (*VM*) signature. Therefore V_j cannot use her own T_j.

6.2 Registration Stage

Tallying managers *TMs* sign on 2 different forms of blinded T_j, i.e., $\alpha_{*1}(r_j, T_j)$ and $\alpha_{*2}(r_j, T_j)$ of Vj during this stage, inside of the voting booth. Firstly voter V_j

blinds her T_j in 2 different forms and then *TMs* blindly sign on them as described in Section 3.3, so that *TMs* sign on T_j without knowing its' content. This signed blinded T_j proves the eligibility of V_j anonymously in later stages. *VM* maintains *VoterList* as shown in Figure 1 (a) showing registered voter's *ID*, each voter's credential $T_j(A, ID_j, Z_j)$ and blinded T_j. As *VoterList* is public, anyone can monitor a registered V_j without knowing T_j as T_j on *VoterList* is in blinded form, i.e., $\{\alpha_{*1}(r_j, T_j)$ and $\alpha_{*2}(r_j, T_j)\}$. In this stage V_j and *VM* interacts as follows:

1) V_j blinds her token T_j in 2 different forms as $\{\alpha_{*1}(r_j, T_j)$ and $\alpha_{*2}(r_j, T_j)\}$using her secret blinding factor r_j.

2) V_j shows her credential $T_j(A, ID_j, Z_j)$ and blinded token $\{\alpha_{*1}(r_j, T_j)$ and $\alpha_{*2}(r_j, T_j)\}$ to *VM*.

3) After authentication, *VM* updates *VoterList* by putting $\{\alpha_{*1}(r_j, T_j)$ and $\alpha_{*2}(r_j, T_j)\}$ as shown in Figure 1(a). *VM* also sends $\{\alpha_{*1}(r_j, T_j)$ and $\alpha_{*2}(r_j, T_j)\}$ to mutually independent *TMs* for their signatures.

4) $TM_1, \cdots, TM_P$ sign on $\{\alpha_{*1}(r_j, T_j)$ and $\alpha_{*2}(r_j, T_j)\}$ to generate 2 different forms *i.e.*, calculate $t(d_{(1*)}, \alpha_{*1}(r_j, T_j))$ and $t(d_{(2*)}, \alpha_{*2}(r_j, T_j))$ and sends them to *VM* to be sent to V_j.

5) V_j checks the validity of signatures on blinded T_j.

Security issues of this stage are as follows:

- *VM may misuse signed T_j:* This security issue can arise if single *VM* is engaged and he gets corrupted. To avoid the issue, multiple *VM* can be employed. Thereby unless all *VM*s get corrupted, signatures of all *TMs* cannot be collected on T_j.
- *VM may put invalid signature on blinded T_j:* V_j can prove *VM*'s dishonesty by showing $\{\alpha_{*1}(r_j, T_j)$ and $\alpha_{*2}(r_j, T_j)\}$ and the incorrect signed token.
- *Signed token T_j may be given to a coercer:* If signed T_j is stolen, V_j is responsible for that. However for voting while V_j comes to a voting booth, she cannot interact with an external coercer. Authorities *e.g. VM* or *TMs* cannot coerce a voter unless all of them get corrupted.

6.3 Vote Submission Stage

V_j uses her 1st form of unblinded signed token *i.e.*, $s(d_{(1*)}, T_j)$ to be authenticated. *VM* checks V_j's validity by verifying the signatures of *TMs* on T_j *i.e.*, $s(d_{(1*)}, T_j)$. Then V_j blinds her vote v_j in 2 different forms by using blinding factors (r_{1j}, r_{2j}), primes (a_{1j}, a_{2j}) and *TMs*' public keys (e'_{1*}, e'_{2*}) by calculating $(\alpha_{1*j}, \alpha_{2*j})$ as described in Section 3.4 *i.e.*, 2 forms of blinded vote of V_j are

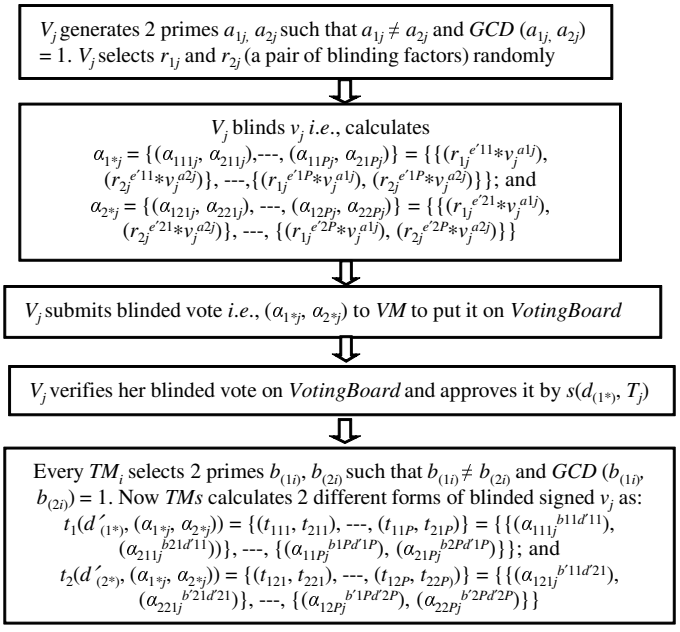

Figure 3: Vote construction procedure

$(\alpha_{1*j}, \alpha_{2*j})$. Now V_j sends $(\alpha_{1*j}, \alpha_{2*j})$ to *VM* to put on *VotingBoard*. After finding her blinded vote on *VotingBoard*, V_j approves it by sending $s(d_{(1*)}, T_j)$ to *VM* to be posted on the approval part of *VotingBoard*. Therefore anyone can monitor a voter who has submitted her blinded vote without knowing her identity and the actual vote. Finally *TM*s sign on the blinded vote to be put on *VotingBoard* with their 1st and 2nd forms of signatures *i.e.*, calculate $t_1(d'_{(1*)}, (\alpha_{1*j}, \alpha_{2*j}))$ and $t_2(d'_{(2*)}, (\alpha_{1*j}, \alpha_{2*j}))$ as described in Section 3.4. The vote construction procedure is shown in Figure 3. Steps of this stage are as follows:

1) V_j submits $s(d_{(1*)}, T_j)$ to *VM*. By checking only the validity of signatures on T_j that is not repeatedly used, *VM* checks the validity of V_j.

2) V_j blinds her vote v_j *i.e.*, calculates $(\alpha_{1*j}, \alpha_{2*j})$ as discussed in Section 3.4.

3) V_j submits $(\alpha_{1*j}, \alpha_{2*j})$ as blinded vote to *VM* to post it on *VotingBoard* (however, it is not shown on *VotingBoard*).

4) By checking her blinded vote on *VotingBoard*, V_j approves it by sending $s(d_{(1*)}, T_j)$ to be posted on *VotingBoard* also.

5) $TM_1, \cdots, TM_P$ sign on the blinded vote $(\alpha_{1*j}, \alpha_{2*j})$ on *VotingBoard* with their 1st and 2nd form of signatures *i.e.*, calculate $t_1(d'_{(1*)}, (\alpha_{1*j}, \alpha_{2*j}))$ and $t_2(d'_{(2*)}, (\alpha_{1*j}, \alpha_{2*j}))$ as discussed in Section 3.4 and post them on *VotingBoard* as shown in Figure 1(c).

For this stage the security issues are as follows:

- *Voter may submit invalid vote to disrupt voting:* V_j herself submits and approves her blinded signed vote

in 2 different forms on *VotingBoard*. Later on, V_j cannot claim that her vote is disrupted even if the vote is meaningless when unblinded vote in 2 signed forms *i.e.*, $s_1(d'_{(1*)}, v_{q*})$ and $s_2(d'_{(2*)}, v_{q*})$ are consistent.

- *VM may not put vote or put incorrect vote:* As *VoterList* is open to the public, repeatedly the V_j can ask *VM* to put her vote on *VotingBoard* by submitting the vote before her approval. If *VM* puts incorrect vote on *VotingBoard*, V_j can disapprove it.
- *Votes in VotingBoard can be modified by attacker:* As *VotingBoard* is open to the public, no one can modify its contents illegally.

6.4 Tallying Stage

All votes on *VotingBoard* are in blinded form. When vote submission ends, each voter needs to unblind her vote in 2 different signed forms *i.e.*, calculates $s_1(d'_{(1*)}, v_{j*})$ and $s_2(d'_{(2*)}, v_{j*})$ as described in Section 3.4. V_j checks the correctness of *TMs*' signatures on her blinded vote. Now V_j submits $s_1(d'_{(1*)}, v_{j*})$ and $s_2(d'_{(2*)}, v_{j*})$ to *VM* to put it on *TallyingBoard*. Then, V_j approves them by posting 2nd form of her signed T_j *i.e.*, $s(d_{(2*)}, T_j)$ on the approval part of *TallyingBoard*. Here V_j's data on *VotingBoard* and *TallyingBoard* may be corresponding or not. If corresponding, easily it is seen that the same blinded and unblinded signed vote on 2 *BBs* is approved by the same T_j. If not corresponding and no approval is put on *TallyingBoard*, no one including *TMs* can know the link between them because of Hwang *et al.*'s BS. Thus links among blinded signed vote on *VotingBoard*, unblinded signed vote on *TallyingBoard* and the identity of a registered V_j on *VoterList* is removed. Steps of this stage are as follows:

1) V_j unblinds her 2 forms of blinded signed vote as $\{s_1(d'_{(1*)}, v_{j*}), s_2(d'_{(2*)}, v_{j*})\}$ and checks the correctness of *TMs*' signatures on them.
2) V_j submits $s_1(d'_{(1*)}, v_{j*})$ and $s_2(d'_{(2*)}, v_{j*})$ to *VM* to post them on *TallyingBoard*.
3) By sending 2nd form of her unblinded signed T_j, *i.e.*, $s(d_{(2*)}, T_j)$ to *VM* to put it on the approval part of *TallyingBoard*, V_j approves her vote.

Security issues of this stage are as follows:

- *Voter may not unblind her vote:* If V_j does not unblind her vote, the vote cannot be considered for counting. However, it is obvious in any application of BS that the entity that blinds the data must unblinds it.
- *TMs may add or delete votes:* By this the numbers of votes on *VotingBoard* and *TallyingBoard* become different which is detectable by anyone.

7 Performance Analysis

This section evaluates the prototype of the proposed scheme and compares it with other schemes.

7.1 Experiment Setup

To measure the computation time requirement for Registration, Voting and Tallying stages, a prototype of the proposed scheme consists of 3 independent Tallying mangers is developed i.e. no client-server based web application is developed in a realistic environment where multiple entities are distributed over different places. Therefore all computation times do not include the communication time. The prototype is developed under the environment of Intel Core i3-3.10 GHz processor with 4 GBytes of RAM running on Windows 7 operating system. For cryptographic operations, GMP [12] with 1024 bit and 2048 bit modulus has been used. Besides, it is assumed that blinding factors, secret integers, primes, *etc.* of involved entities are prepared in advance. Also, operations of entities that are not related to cryptography are not considered.

7.2 Performance Evaluation

Table 2: Time requirement for registration, vote submission and tallying stages

	Stages (time in ms)					
Phase	Registration		Vote Submission		Tallying	
	1024 bit	2048bit	1024 bit	2048 bit	1024 bit	2048 bit
Blinding	0.216	0.804	4.740	17.136	–	–
Signing	3.672	23.130	26.220	179.898	–	–
Unblinding	0.018	0.072	–	–	11.322	40.374
Verification	–		–	–	0.234	0.888
Total	3.906	24.006	30.94	197.034	11.556	41.262

During Registration stage V_j blinds her token T_j in 2 different forms, *TMs* sign on them and V_j unblinds them to obtain unblinded signed T_j. As there are 3 *TMs*, V_j blinds her T_j in 6 forms, blinded T_j is signed by *TMs* and 6 forms are generated, and finally V_j unblinds them all. Vote submission stage consists of blinding the vote v_j in 2 different forms and signing on them. Because of 3 *TMs*, V_j blinds her v_j in 6 forms by using 2 different public keys of 3 *TMs*, and blinded v_j is signed by *TMs* and 6 forms are generated. In Tallying stage, voter V_j unblinds her blinded signed vote v_j in 6 forms and finally anyone can verify the vote. The time requirement for different operations in Registration, Vote submission and Tallying stages for the proposed scheme using GMP with 1024 bit and 2048 bit modulus has been summarized in Table 2. Using GMP the total time requirement for Registration, Vote submission and Tallying stages are 3.906ms, 30.94ms, and 11.556ms respectively for 1024 bit; while for 2048 bit it requires 24.006ms, 197.034ms and 41.262ms respectively.

7.3 Discussions

For unblinding any data using both Hwang *et al.*'s BS and Chaum's BS, equations that have the form like: $s = t \ . \ r^{-b} \bmod n$ — (1), are solved by using Extended Euclidean Algorithm [31] that finds out x and y when $ax + by = GCD\ (a,\ b)$. If $GCD\ (a,\ b)$ is 1, then $ax + by = 1$. Equation (1) can be rewritten as $r^b.\ s = ny + t$ where y is a positive integer. Hence, equation (1) becomes $r^b\ .(s/t) + \ n\ .(-\ y/t) = 1$. Now the value of (s/t) and $(-\ y/t)$ can be found by using Extended Euclidean Algorithm. As t is known, s can be easily calculated. The operations involved in unblinding phase of both schemes have been evaluated in this way. Chinese Remainder Theorem [31] is used to evaluate the signing phase of Chaum's BS that has shrunk the computation time of this phase.

The computation time requirement for blinding tokens and votes, signing on blinded tokens and votes and unblinding signed tokens and votes are directly proportional to the numbers of *TMs* involved in the scheme. Using GMP with 1024 bit modulus, 1000 votes can be counted within 12 seconds (0.011556 * 1000 = 11.556) which is feasible enough to implement in real world. To get an overview of the proposed scheme if 100 thousand voters (0.1 million) are considered using 1024 bit modulus implemented with GMP; the Registration, Vote Submission and Tallying stages can be completed within 78 minutes on a single server (*i.e.*, (0.046402 * 100000) = (4640.2secs/ 60) = 77.34 min).

7.4 Comparisons

Table 3: Computation time comparisons with other schemes

Schemes	CPU(GHz)	Memory	Coding	1024 bit modulus (time in ms)		
				Registration	Voting	Tallying
Proposed scheme	3.10	4 GB	GMP	3.906	30.94	11.556
CNSc	1.60	504 MB	GMP	47.1	308	171
DynaVote	1.60	752MB	Java	-	2470	208.3

The performance of prototype of the proposed scheme is compared with those of confirmation number (CN) based anonymous voting scheme (CNSc) proposed in [3], and DynaVote proposed in [6] which are available for comparisons, although the used hardware configurations and coding platforms are not same. Thereby the comparison is not an absolute one. Also, no comparison with schemes that deploy ZKP, e.g., Helios [2] Civitas [9] has been presented (a comparison with a ZKP based scheme is available in [3]) because for ZKP it requires huge computation time. Moreover, no comparison with schemes that allow the same voter to cast her vote multiple times, e.g., UVote [1] has been made because the proposed scheme does not consider the vote submission in this way. In CNSc [3], the voter's Registration stage is identical to the proposed scheme. In Voting stage, the vote construct consists of: i) the voter encrypts her vote, ii) 3 authorities' perform triple encryptions on it, iii) the voter decrypts it by her decryption key, iv) the voter verifies authorities' encryptions of vote, v) 3 authorities repeatedly sign on the encrypted vote in 2 different forms and on the confirmation number in a single form, and finally vi) the voter verifies both forms of authorities' signatures. The time requirement for tallying is comprised of decryptions and shuffles and verifications of 2 signed forms of votes and single signed form of CNs. In DynaVote [6] the prototype has been developed over the internet, and while considering 1000 votes the runtime requirement of each vote in Voting stage is 2470.042ms and in Tallying stage is 208.3ms. Although the communication between server and client uses multi-threading, it did not use this feature while testing the prototype. Here voting stage consists of ballot obtaining and vote casting phases, and while the number of votes increases, the time requirement decreases gradually. A comparison among the schemes for a single vote and its voter has been presented in Table 3.

7.5 Untraceability

The proposed scheme maintains the untraceability property of Hwang *et al.*'s BS referring to the fact that for any given valid signature $\{v_j,\ s(d'_{(i)},\ v_j)\}$, the authority TM_i is unable to link the signature to the vote. The demonstration is as follows. As described in Sections 6.3 and 3.4, the voter V_j submits her blinded vote *i.e.*, $(\alpha_{1ij},\ \alpha_{2ij})$, and TM_i signs on it *i.e.*, calculates $t(d'_{(i)},\ (\alpha_{1ij},\ \alpha_{2ij}))$ using his primes $(b_{1i},\ b_{2i})$. Now TM_i can store a set of records *i.e.*, $\{(\alpha_{1ij},\ \alpha_{2ij}),\ t(d'_{(i)},\ (\alpha_{1ij},\ \alpha_{2ij})),\ (b_{1i},\ b_{2i})\}$ for every blinded vote. During the Tallying stage when V_j reveals her unblinded signed vote as $\{s(d'_{(i)},\ v_j)\}$ by putting it on *TallyingBoard*, TM_i has no way to get any information regarding V_j's secret blinding factor $(r_{1j},\ r_{2j})$ from the stored information. Moreover, V_j's unblinded signed vote consists of two parts *i.e.*, $s(d'_{(i)},\ v_j)$ has been generated from $\{({v_j}^{a1jb1d'i})^{wj}\}$ and $\{({v_j}^{a2jb2d'i})^{uj}\}$ (as discussed in Section 3.2) and neither of which TM_i knows. Hence without knowing V_j's secret blinding factor $(r_{1j},\ r_{2j})$, pair of primes $(a_{1j},\ a_{2j})$ and integers $(w_j,\ u_j)$, TM_i cannot trace the BS. Here it is same for all authorities (*TMs*) while a vote v_j is constructed in any of 2 forms by any TM_i.

7.6 Further Extensions

An erasable-state voting booth as discussed in [29], can be deployed for the proposed scheme. Thereby, while the voter interacts with authorities, she is unable to memorize the complete list of information exchanged between herself and election authorities. For example, to construct her vote the voter uses lots of parameters like secret blinding factors, integers, primes *etc.* and later on she cannot reuse them. Thereby, she cannot prove her vote to any third party. Besides, the proposed scheme does not deploy

Table 4: Comparison of schemes based on security requirements

Schemes	Verifiable	Fair	Robust	Receipt-free	Accuracy	Dispute-free	Incoercible	Scalable	Practical	Major Tools
Proposed scheme	U	Y	Y	C	Y	Y	Y	Y	C	BS
Lee *et al.* [20]	U	C	C	Y	Y	N	N	C	N	Mixnet
CNSc [3]	U	Y	C	Y	Y	Y	Y	N	Y	HE, Mixnet
Fujioka *et al.* [11]	I	Y	N	N	N	N	N	Y	N	BS
Juang *et al.* [32]	I	C	C	N	C	N	N	Y	Y	BS
DynaVote [6]	I	C	NK	Y	Y	Y	Y	Y	C	BS
Helios [2]	Y	Y	Y	N	Y	N	N	N	Y	Mixnet, ZKP
Civitas [9]	I	Y	Y	Y	C	N	Y	N	N	Mixnet, ZKP
UVote [1]	I	Y	NK	N	Y	N	Y	NK	NK	Mixnet
Cobra [10]	N	Y	Y	Y	Y	NK	Y	N	N	HE

Y: Yes; N: No; NK: Not Known; I: Individually; U: Universally; C: Conditionally; P: Partially; BS: Blind Signature; HE: Homomorphic Encryption; ZKP: Zero Knowledge Proof;

any form of mixnet [15]. However, as discussed in [14]; a verifiable mixnet can also be incorporated herein. For this while vote submission, the voter submits her unblinded signed vote to the mixnet. When every voter completes her vote submission, the mixnet processes the encrypted votes i.e., either re-encrypts or decrypts and shuffles them. Finally an authority decrypts the votes shuffled by the mixnet and publishes the result on the BB. Herein, a little rearrangement of individual stages of the scheme will be required. Thereby, the scheme would become suitable for big community where the number of voters is high also.

8 Security Analysis

Based on major requirements, a comparison among the schemes has been presented in Table 4 where very basic requirements namely privacy, eligibility etc which are satisfied by almost schemes are omitted. But herein also, it is difficult to establish an absolute comparison because in many cases schemes cannot satisfy a particular requirement at the same level. Besides, the definition and the way of attaining requirements even may vary among schemes. For example to ensure un-reusability, some schemes assume that one voter can vote only once. But to attain incoercibility, many schemes enable one voter to cast her vote multiple times from which only a valid vote is counted. Also, there is tradeoffs among requirements. Therefore even by observing the Table, it is difficult to decide which particular scheme is the sole winner.

This section also discusses the way how the proposed scheme satisfies requirements of e-voting where their formal meanings are available in [14, 17, 24].

Privacy: By using 2 different forms of unblinded signed token, each voter submits as well as approves her vote anonymously. Thus, no one except the voter can know the link between blinded signed vote and its voter; and cannot identify a voter who did not submit her vote. Also the use of Hwang *et al.*'s BS disables entities even *TMs*' to link between blinded signed vote on *VotingBoard* and its unblinded signed form on *TallyingBoard* while they are not posted correspondingly, and the voter's approval does not appear on *TallyingBoard*.

Eligibility: While Token acquisition and Registration stages, the identity of the voter is identified by anonymous credential $T_j(A, ID_j, Z_j)$. Also to submit and approve the vote, the corresponding voter's identity is ensured by her unblinded signed T_j which is unique. Moreover, the token of each voter is signed by multiple authorities; therefore no one can forge signatures on T_j. Thus only eligible voters can participate in voting.

Un-reusability: While voter submits her vote using signed token, *VM* checks that the token is already used or not. Also the voter's blinded signed vote on *VotingBoard* and unblinded signed vote on *TallyingBoard* are approved by the same token only signed in 2 different forms; therefore multiple voting by a single voter is prevented.

Accuracy: Only unblinded signed votes approved by their voters appearing on *TallyingBoard* are considered for tallying. Thus all and only valid votes are counted.

Fairness: Every vote on *VotingBoard* is blinded by its corresponding voter and signed by all *TMs*; thereby no entity can know the interim voting results. Only the corresponding voter can unblind her vote during the Tallying stage.

Robustness: While even an invalid vote is identical within 2 unblinded signed forms, the voter cannot claim that her vote is disrupted; thus a voter can disrupt only her own vote. Also *VM* or *TMs* cannot disrupt the scheme if at least a single entity of them is honest among multiple entities.

Universal Verifiability: Every voter approves her blinded signed vote on *VotingBoard* and unblinded signed vote on *TallyingBoard* by her unique token signed in 2 different forms, which is publicly open. Moreover thereby, a registered voter can submit only a single vote. Thus the scheme ensures that all and only vote approved by its individual voter is counted.

Dispute-freeness: In the scheme, publicly-verifiable data about interactions among entities on different *BBs*, signature pairs on vote and signature pairs on unique token enable involved entities to resolve disputes.

Receipt-freeness: By deploying an erasable-state voting booth, receipt-freeness can be achieved. Due to an erasable-state voting booth, later on the voter cannot reuse her secret parameters to reconstruct the vote. Also as discussed in Section 6.3, the vote is constructed in distributed fashion through the involvement of the voter and *TMs*. Thereby, although the voter knows her blinded signed vote on *VotingBoard*, she cannot prove it to the coercer.

Incoercibility: When unblinded signed vote in 2 different forms are same, no one can claim that the vote is disrupted. Thus the scheme is free from randomization attack. Also a registered voter proves her identity to authorities anonymously through unique token signed by multiple authorities; therefore coercers cannot pretend to be a valid voter instead of herself. Thus the scheme is free from simulation attack.

Scalability: The scheme provides a scalable solution for major security aspects as discussed above. Also the prototype performance evaluation presented in Section 7 shows that the time requirement to implement the scheme is not so high.

Practicality: The scheme relies on an erasable-state voting booth to achieve receipt-freeness, although it is not yet implemented. Also herein, as BS is deployed for vote construction; obviously a voter needs to unblind her blinded signed vote later on. These impair the practicality. However, while the voter submits her unblinded signed vote to a mixnet as discussed in Section 7.6, the second problem is resolved.

9 Conclusions

The proposed e-voting scheme respects numerous requirements of a fair election. As a token cannot be linked with its' voter and her vote, and signing authorities are unable to link between a blinded signed vote and its' corresponding unblinded signed vote; the scheme is completely untraceable. Also, 2 different forms of signatures on a blinded token enable a voter to appear to authorities anonymously. Moreover, 2 different forms of signatures on same blinded vote prove the fairness of authorities. Even after unblinding if the vote within 2 signed forms is found meaningless, it ensures that the vote is meaningless from the beginning and intentionally submitted by the voter herself. In addition, the proposed scheme attains almost all essential requirements of e-voting in a simple way. It demonstrates that the computation time requirement for the proposed scheme is substantially small and makes the scheme scalable. A future plan of improvement is to evaluate the proposed scheme in more realistic environments where multiple authorities are distributed over different places, and many voters are involved.

References

[1] R. Abdelkader and M. Youssef, "Uvote: A ubiquitous e-voting system," in *3rd FTRA International Conference on Mobile, Ubiquitous, and Intelligent Computing (MUSIC'12)*, pp. 72–77, 2012.

[2] B. Adida, "Helios: Web-based open-audit voting," in *Proceedings of 17th USENIX Security Symposium*, Aug. 2008.

[3] K. Md. R. Alam, S. Tamura, S. Taniguchi, T. Yanase, "An anonymous voting scheme based on confirmation numbers," *IEEJ Transactions on Electronics, Information and Systems*, vol. 130, no. 11, pp. 2065–2073, 2010.

[4] R. Araujo, A. Barki, S. Brunet, and J. Traore, "Remote electronic voting can be efficient, verifiable and coercion-resistant," in *International Conference on Financial Cryptography and Data Security*, pp. 224–232, 2016.

[5] C. Burton, C. Culnane, and S. Schneider, "vvote: Verifiable electronic voting in practice," *IEEE Security Privacy*, vol. 14, pp. 64–73, July 2016.

[6] O. Cetinkaya and M. L. Loc, "Practical aspects of dynavote e-voting protocol," *Electronic Journal of E-government*, vol. 7, no. 4, pp. 327–338, 2009.

[7] D. Chaum, "Blind signatures system," *Advances in Cryptology (CRYPTO'83)*, pp. 153–156, 1983.

[8] D. L. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," *Communications of ACM*, vol. 24, pp. 84–90, Feb. 1981.

[9] M. R. Clarkson, S. Chong, and A. C. Myers, "Civitas: Toward a secure voting system," in *Proceedings of the 2008 IEEE Symposium on Security and Privacy*, pp. 354–368, 2008.

[10] A. Essex, J. Clark, and U. Hengartner, "Cobra: Toward concurrent ballot authorization for internet voting," in *International Conference on Electronic Voting Technology/Workshop on Trustworthy Elections (EVT/WOTE'12)*, 2012.

[11] A. Fujioka, T. Okamoto, and K. Ohta, "A practical secret voting scheme for large scale elections," in *Advances in Cryptology (AUSCRYPT'92)*, pp. 244–251, 1993.

[12] T. Granlund, *GNU Multiple Precision Arithmetic Library (GMP)*, Accessed, 2016.

[13] L. Han, Q. Xie, and W. Liu, "An improved biometric based authentication scheme with user anonymity using elliptic curve cryptosystem," *International Journal of Network Security*, vol. 19, no. 3, pp. 469–478, 2017.

[14] L. Huian, A. R. Kankanala, and X. Zou, "A taxonomy and comparison of remote voting schemes," in *23rd International Conference on Computer Communication and Networks (ICCCN'14)*, pp. 1–8, 2014.

[15] N. Islam, A. K. Md. Rokibul, and A. Rahman, "The effectiveness of mixnets-an empirical study," *Transaction on Computer Fraud and Security*, vol. 2013, no. 12, pp. 9–14, 2013.

[16] N. Islam, A. K. Md. Rokibul, and S. S. Rahman, "Commutative re-encryption techniques: Significance and analysis," *Information Security Journal: A Global Perspective*, vol. 24, no. 4, pp. 185–193, 2015.

[17] I. Jabbar and S. N. Alsaad, "Design and implementation of secure remote e-voting system using homomorphic encryption," *International Journal of Network Security*, vol. 19, no. 5, pp. 694–703, 2017.

[18] A. Juels, D. Catalano, and M. Jacobsson, "Coercion-resistant electronic elections," *Towards Trustworthy Elections*, pp. 37–63, 2010.

[19] C. Guo W. Hu L. Yuan, M. Li and Z. Wang, "A verifiable e-voting scheme with secret sharing," *International Journal of Network Security*, vol. 19, no. 2, pp. 260–271, 2017.

[20] B. Lee, C. Boyd, Ed Dawson, K. Kim, J. Yang, and S. Yoo, "Providing receipt-freeness in mixnet-based voting protocols," in *Proceedings of the Information Security and Cryptology (ICISC'03)*, pp. 245–258, 2004.

[21] C. C. Lee, T. Y. Chen, S. C. Lin, and M. S. Hwang, "A new proxy electronic voting scheme based on proxy signatures," *Lecture Notes in Electrical Engineering*, vol. 164, pp. 3–12, 2012.

[22] C. C. Lee, M. S. Hwang, and W. P. Yang, "Untraceable blind signature schemes based on discrete logarithm problem," *Fundamenta Informaticae*, vol. 55, no. 3-4, pp. 307–320, 2003.

[23] C. C. Lee, M. S. Hwang, and W. P. Yang, "A new blind signature based on the discrete logarithm problem for untraceability," *Applied Mathematics and Computation*, vol. 164, no. 3, pp. 837–841, 2005.

[24] C. T. Li and M. S. Hwang, "A secure and anonymous electronic voting scheme based on key exchange protocol," *International Journal of Security and Its Applications*, vol. 7, no. 1, pp. 59–70, 2013.

[25] C. C. Lee M. S. Hwang and Y. C. Lai, "An untraceable blind signature scheme," *IEICE Transaction on Fundamentals*, vol. E86-A, no. 7, pp. 1902–1906, 2003.

[26] J. Chen M. Wu and R. Wang, "An enhanced anonymous password-based authenticated key agreement scheme with formal proof," *International Journal of Network Security*, vol. 19, no. 5, pp. 785–793, 2017.

[27] B. Riva and A. Ta-Shma, "Bare-handed electronic voting with pre-processing," *Proceedings of the USENIX/Accurate Electronic Voting Technology Workshop*, pp. 15, 2007.

[28] A. K. Md. Rokibul and S. Tamura, "Electronic voting: Scopes and limitations," in *Proceedings of International Conference on Informatics, Electronics & Vision (ICIEV12)*, pp. 525–529, May 2012.

[29] H. A. Haddad. N. Islam S. Tamura and A. K. Md. Rokibul, "An incoercible e-voting scheme based on revised simplified verifiable re-encryption mix-nets," *Information Security and Computer Fraud*, vol. 3, no. 2, pp. 32–38, 2015.

[30] D. Sandler, K. Derr, and D. S. Wallach, "Votebox: a tamper-evident verifiable electronic voting system," in *Proceedings of the 17th USENIX Security symposium*, pp. 349–364, 2008.

[31] B. Schneier, *Applied Cryptography*, John Wiley & Sons Inc., 2nd edition edition, 2008.

[32] Wen shenq Juang, Chin laung Lei, and Pei ling Yu, "A verifiable multi-authorities secret election allowing abstaining from voting," *Computer Journal*, vol. 45, no. 6, pp. 672–682, 2002.

[33] Shinsuke Tamura and Shuji Taniguchi, "Enhanced anonymous tag based credentials," *Information Security and Computer Fraud*, vol. 2, no. 1, pp. 10–20, 2014.

Biography

Kazi Md. Rokibul Alam is currently a professor in the Dept. of Computer Science and Engineering of Khulna University of Engineering & Technology. He received Dr. (Eng.) degree in System Design Engineering from University of Fukui, Japan, and M.Sc. and B. Sc. degrees both in Computer Science and Engineering from Bangladesh University of Engineering & Technology and Khulna University, Bangladesh in 2010, 2004 and 1999, respectively. His research interests include applied cryptography, information security and machine learning.

Adnan Maruf has received his B.Sc. Eng. degree in Computer Science & Engineering from Khulna University of Engineering & Technology in 2013. From 2013 to 2016, he worked as a Sr. Software Engineer in Samsung Research & Development Institute, Banglagesh. He is currently a PhD student at Florida International University, USA. His research interests include Computer Vision, Computational Geometry, and Computer Security.

Md. Rezaur Rahman Rakib is currently doing his MS in Computer Science at Technical University of Munich (TUM) in Germany. He received his bachelor degree in Computer Science and Engineering from Khulna University of Engineering & Technology, Bangladesh in 2013. In 2014, he joined in Samsung R&D Institute Bangladesh Ltd. (SRBD) as a software engineer. In 2016, he was promoted to senior software engineer in SRBD. His research interests include neural networks and artificial intelligence, machine learning, cognitive system, and deep learning.

G. G. Md. Nawaz Ali is currently a postdoctoral research fellow with the School of Electrical and Electronic Engineering, Nanyang Technological University (NTU), Singapore. He received his PhD in the Department of Computer Science, City University of Hong Kong in 2013. He received his B.Sc. degree in Computer Science and Engineering from Khulna University of Engineering & Technology, Bangladesh in 2006. He is a member of IEEE and IEEE VTS. His current research interests

include wireless broadcasting, mobile computing, network coding, and ad hoc networking with a focus on vehicular ad hoc networking.

Peter H. J. Chong is currently the Professor and Head of the Department of Electrical and Electronic Engineering, Auckland University of Technology, New Zealand. He received the B.Eng. (with distinction) in electrical engineering from the Technical University of Nova Scotia, Halifax, NS, Canada, in 1993, and the M.A.Sc. and Ph.D. degrees in electrical engineering from the University of British Columbia, Vancouver, BC, Canada, in 1996 and 2000, respectively. Between 2000 and 2001, he worked at Agilent Technologies Canada Inc., Canada. From 2001 to 2002, he was at Nokia Research Center, Helsinki, Finland. From May 2002 to 2016, he was with the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore as an Associate Professor (Tenured). He was an Assistant Head of Division of Communication Engineering between 2011 and 2013, since July 2013 to April 2016, he was the Director of Infinitus, Centre for Infocomm Technology in School of EEE. He has visited Tohoku University, Japan, as a Visiting Scientist in 2010 and Chinese University of Hong Kong (CUHK), Hong Kong, between 2011 and 2012. He is currently an Adjunct Professor of CUHK.

Yasuhiko Morimoto is a professor at Hiroshima University. He received his B.E., M.E. and Ph.D degrees from Hiroshima University in 1989, 1991 and 2002 respectively. From 1991 to 2002, he had been with IBM Tokyo Research Laboratory where he worked for data mining project and multimedia database project. Since 2002, he has been with Hiroshima University. His current research interest includes data mining, machine learning, geographic information system and privacy preserving information retrieval.