UNCOERCIBILITY IN E-VOTING AND E-AUCTIONING MECHANISMS USING DENIABLE ENCRYPTION

Jaydeep Howlader[1], Vivek Nair[1], Saikat Basu[2] and A. K. Mal[3]

[1]Department of Information Technology, National Institute of Technology, Durgapur, India
jaydeep.howlader@it.nitdgp.ac.in
[2]Department of Computer Science and Engineering, National Institute of Technology, Durgapur, India
deepbasu007@gmail.com
[3]Department of Electronics and Communication Engineering, National Institute of Technology, Durgapur, India
toakmal@gmail.com

ABSTRACT

The uncoercibility to prevent rigging in e-voting and e-auction have been studied in different literatures. It is realized that the notion of a virtual booth and untappable channel are required to prevent coerciveness. Virtual booth protects the candidates to cast their private values without being observed by the adversary/coercer. However the adversary can influence the candidates after their casting. Adversary used to acquire the encrypted votes/bids either from the colluded authorities (voting server, auctioneer) or by eavesdropping the communicating channel and coerces the candidates to disclose their private values with the private keys and verifies whether the ciphers are the encryption of the private values. In the prior literatures of e-voting and e-auctioning, threshold-encryption and receipt-free mechanism are used to prevent the coercion and collusion respectively. But they assumed untappable channel to restrict eavesdropping. However, practically untappable channel is difficult to achieve. It should be a dedicated trusted link or continuous fiber link to implement untappable channel. In this paper we present an alternative of untappable channel using deniable encryption. An encryption scheme is deniable if the sender can formulate 'fake random choice' that will make the cipher text 'look like' an encryption of a different plaintext, thus keeping the real plaintext private. Deniable encryption does not restrict the adversary to eavesdrop, but if the candidates are coerced, they are able to formulate a different value v_f and can convince the adversary that the ciphers are the encryption of v_f, without revealing the true private value v_r. Therefore, eavesdropping does not help the coercer, as he may be plausibly denied by the candidates. Our scheme is based on public key probabilistic encryption mechanism. We assume that the sender side (candidate) coercion is only applicable, that is, the coercer cannot coerce the receivers (authorities).

KEYWORDS

coercing, rigging, receipt-free, deniable encryption, probabilistic encryption

1. INTRODUCTION

The notions of uncoercibilety and receipt-freeness were first introduced by Benaloh and Tuinstra [1] to deal with *vote-selling* and *coercing* in electronic voting systems. They pointed out that, all the prior cryptographic electronic voting schemes were suffering from one common deficiency: the voters were allowed to encrypt their votes, but at the same time they were allowed to carry the *receipt* of their vote cast, which could be exploited to prove to a third party that a particular vote had been caste. This simple defect enables some serious problems like vote

selling and coercing. The problem was further studied in different electronic election literatures [2, 3, 14] and also in electronic sealed-bid auction literatures [4, 5, 13, 14, 16]. In this paper auction means sealed bid auction. The problem of vote-selling or bid-selling occurs when the voters/bidders are the adversary. A group of voters/bidders make a conspiracy and commit to cast their vote/bid to a certain value as decided by the colluded voters/bidders. This type of collusion is called a *ring* [14]. Generally secrecy and privacy is maintained in any voting/auctioning system. Therefore the votes/bids are generally in encrypted form. The voters/bidders have to prove their cast/bid to the ring to convince the other colluded members that he has not broken the collusion. The traditional election system discourages vote selling because of the voting booth. The voter promises to the ring to cast his vote in favour of a particular party, but within the privacy of the voting booth, he may cast the opposite vote without bring afraid of any further consequence. As the voting process does not issue any receipt/acknowledgment of the vote cast; there is no question of proving the private value (caste vote) to any third party, even the voter wants to (e.g. for exchange of bride). Similar protection is there for sealed-bid auction, where the bids are submitted in the sealed envelope and no receipts are issued. On the other hand, coercing is the problem where the adversary influences/threatens the voters/bides to cast a particular value. This is known as rigging. Due to the physical existence of booth, coercer is not able to control the voters during their vote casting. However, electronic mechanism does not provide such protection and coercing is possible. In fact coercing is a form a rigging and electronic voting or auction suffers from rigging in two different forms:

1. Rigging before casting: the candidates are rigged to cast their vote or bid as directed by the coercer.
2. Rigging after casting: the candidates are rigged to produce a proof of their casting to the coercer so that the coercer could verify whether they obey his order or not.

To overcome the rigging, different approaches were proposed. Multiple authority model with threshold-encryption [4, 5, 16] was used to overcome the collusion of the authorities. Generally, the secret value of the cast/bid was shared among the authorities in such a way that a subsequent number of authorities can reconstruct the secret. It was assumed that the adversary cannot collude the subsequent number of authorities. Whereas the problem of eavesdropping was overcame with the assumption of untappable channel. Untappable channel is a physical assumption, such that the adversary cannot eavesdrop the communication. This can be achieved either by dedicated private link or by peer to peer fiber link, which may not be feasible for many applications.

The implementation of secure electronic election/auction has seemed to be difficult with the two physical assumptions: virtual booth and untappable channel. This paper presents an alternative of the untappable channel. We propose a deniable encryption scheme using the public key, which may be used as a replacement of untappable channel. Our technique is well suited for electronic election and auction system. Deniable encryption was introduced by Canetti *et.al.* [17]. Deniable encryption allows an encrypted message to be decrypted to different sensible plaintexts, depending on the key used, or otherwise makes it impossible to prove the existence of the real message without the proper encryption key. This allows the sender to have plausible deniability if compelled to give up his or her encryption key.

1.1 Related works

The receipt-free incoercible protocols in [2, 5, 13, 14, 16] were based on two physical assumptions: bulletin/bidding booth and untappable channel. It is understood that without the untappable channel, uncoercibility can not be guaranteed. However, implementing the untappable channel might not be an easy task. In some literature [20, 21] tamper resistant smartcard were used to overcome the sender side coercing. The smartcard was used to generate the random inputs independently to encrypt the candidates' private values. The candidates had

no control over the randomness nor were they informed about the value of the randomness. Therefore, coercing at the sender side did not make any sense. However, the scheme is suitable for large scale election/auction mechanism and requires an infrastructure and deployment policy for smartcard distribution. The smartcard based systems restrict the unregistered candidates (those who were not having smartcards) to participate in the voting/auctioning. This may be applicable in large scale election, but not suitable for auctioning, where any bidder can participate in the process either pre-registered or un-registered. Further the untapability assumption has not been completely removed in [20]. Here the "channel" between the Voter and the Encryption Blackbox is still assumed to be untappable. This is because if the message is tapped even before it is encrypted in the Encryption Blackbox, the plaintext is revealed. A new approach of anonymous electronic voting was proposed in [24]. It described a *Generic Blind Signature Scheme with Dual Randomization* to achieve *uncoercibility* and *anonymity* in electronic voting systems. However, since it involves registration of all users so it cannot be used in the Electronic auction mechanisms where users are allowed to bid even if they are registered or not.

The present paper presents a deniable encryption scheme as an alternative of the untappable channel. The framework of deniable encryption was proposed by Canetti *et.al*, where they defined a *translucent* set $S \subset \{0,1\}^t$ for some large t and a trapdoor function d. The cardinality of *translucent* set S was relatively quite smaller than 2^t. It was easy to generate a random $x \subset_R S$ without the trapdoor *d*, but difficult to determine the membership of a given random $x \subset \{0,1\}^t$ without the trapdoor *d*. The sender-side deniable encryption scheme based on Quadratic Residuosity of Blum's composite modulus was proposed in [19]. The scheme is unplanned-deniable and is not secure as plan-ahead-deniable unless the coercer has no control on the sender's local randomness. It is also inefficient and difficult to fit in the election/auction protocol. In [22], a sender-side deniable encryption scheme was introduced, based on the intractability assumption of the Quadratic Residuosity Problem [18]. The scheme used one-time-padding technique to encrypt a message. The resultant cipher was two tuples (c, A), where c represented the padded message and A was a finite set of random elements $a \in \mathbf{Z}_n^*$ (n is the product of two distinct large primes) that represented a random string $r \subset \{0,1\}^*$ which was used in one-time-padding process. The receiver could reconstruct the string r with negligible error probability. In case of coercing, the sender could decode the random set A to some other string r_f and could conveniently disclose a different message m_f to prove that encryption of m_f and r_f resulted to the same cipher c.

The following is organized as follows: Section II describes the general methodology used in electronic voting and auctioning system, the method of coercing and the general techniques used to overcome the coercion. Section III describes the requirement of untappable channel to achieve the uncoerciveness and how deniable encryption can be used to replace the untappable channel. We present the technique to use deniable encryption with the existing protocols used in electronic voting and auctioning system.

2. ELECTRONIC CASTING SYSTEM AND COERCIVENESS

The general electronic casting systems consist of the following entities:

- A set of valid candidates, generally voters or bidders.
- The authorities of the casting system like vote counting machine of tallying machine.
- The adversary (coercer) may be a valid voter or bidder or may be an authority.
- The systems have a published list of nominees/items and the defined *rule* of the game (e.g. single candidate winning, the highest price winning auction).

The systems have the essential three phases:

- **Casting:** The candidates encrypt their private values with the authorities' public keys and the randomness to form conceals votes/bids and sends to the authorities.
- **Opening:** The authorities co-operate to open the encrypted casts.
- **Tallying:** After opening, the result has to be declared. The election protocol determines the winning nominee, not discloses the votes of the individuals. Whereas, the auction protocol determines the winning price, not the winner. The winner has to claim his victory with sufficient proof.

The coercer is the adversary in the system who wants to find the private values of some selected candidates. The coercer does the following:

- May coerces the candidates before or after their casting. Balloting/Bidding booth does not allow the coercing during the casting.
- Eavesdrop the communication link between the candidates and the authorities.
- Conspires with a set of colluded authorities. It is assumed that the coercer can not collude more then a certain number of authority.

The candidates must reveal any information if they are coerced. However, the candidates may plausibly deny or produce false information (fake message), provided that the coercer cannot verify the deniability or falseness.

2.1. How to get Uncoerciveness

Uncoerciveness can be achieved based on the three premises: booth, untappable channel, receipt-freeness. The existence of booth allows the candidates to cast their private values without being observed by the coercer [1, 3]. This allows the candidates to make promises to the adversary (coercer), buy within the privacy of the booth they can break the promises without being identified.

As the coercer cannot control the candidates during their casting, he taps the communication channel and acquires the encrypted values and coerces by forcing the candidates to revile their randomnesses and plaintexts and verifies whether the ciphers are the encryption of the plaintexts. All the prior electronic election and auctioning schemes ensure uncoerciveness based on the assumption of a physical untappable channel between the booths and the authorities. The untappable channel disallows the coercer to tap the communication and hence guaranties uncoerciveness.

The only way to coerce the candidates is to acquire the encrypted values from the colluded authorities. To overcome the problem of authorities collusion, receipt-free threshold encryption and anonymous voting/bidding scheme is used. Anonymous casting hides the candidates identity from their cast in such a way that the identity can be extracted in case of repudiation. any protocols use mixnet [6–8, 15] to get anonymous submission. With receipt-freeness the candidates should not be able to convince a third party of the values of their cast nor the coercer can demand the proof of the candidates' private cast values. A homomorphic public key encryption with randomness is used to get receiptfreeness [2, 5, 13, 16, 14]. The private key is shared among the authorities such that a certain number of authorities has to co-operate to decrypt ciphers [4, 5, 16]. Thus a threshold encryption [9–11] is used to overcome the collusion of the authorities.

3. UNTAPPABLE CHANNEL AND DENIABLE ENCRYPTION

The existence of untappable channel is essential to get uncoerciveness in electronic election and auction systems. However, untappable channel is difficult to achieve. Here we present a deniable encryption scheme as an alternative of the untappable channel. Let M is message set and $M \subset \mathbf{M}$ is the set of all sensible plaintexts. Any $m \in M$ is called valid message and M is the set of all valid messages. Generally the cardinality of the valid message set $|M|$ is

comparatively smaller then the cardinality of the message space $|\mathbf{M}|$. Let E is an probabilistic deniable encryption process that encrypts a message *m* with randomness *r*. If *c = E(m, r)* is a cipher of a valid message $m \in M$ and *r* is the randomness, then the plausible deniability allows the sender to find different plaintexts $m_f \in M$ and different randomness r_f easily such that the encryption $E(m_f, r_f)$ results to the same cipher *c*. The m_f and r_f is called the fake message and fake randomness respectively. It is obvious that the fake message should be the member of the valid message set so that the sender can easily convince the third party with the fake message by concealing the true message *m*.

Thus deniable encryption does not restrict the coercer to eavesdrop the communication, but if the coercer enforces the candidates to reveal the plaintexts and the randomness for their corresponding ciphers, they can easily find fake messages and fake randomness whose encryption looks like the same ciphers. Thus the candidates can confidently make a lie to the coercer without being afraid of being caught. Hence, eavesdropping does not provide any advantage to the coercer.

A. Prelimineries

The deniable encryption scheme proposed in this paper is based on the quadratic residue of a composite *n*, which is a product of two distinct primes. An integer $a \in \mathbf{Z}_n^*$ is a quadratic residue modulo n, if there exists some $x \in \mathbf{Z}_n^*$ such that $a \equiv x^2 \bmod n$. We denote $a \in \mathbf{Q}_n$. Otherwise a is quadratic nonresidue modulo n and denoted as $a \in \overline{\mathbf{Q}_n}$.

The properties of quadratic residues of composite:

Let $n \geq 3$ be odd number, the Jacobi symbol $\left(\frac{a}{n}\right)$ is defined as:

$$\left(\frac{a}{n}\right) = \begin{cases} -1 & a \in \bar{Q}_n \\ 1 & a \in Q_n \text{with probability } \alpha < 1 \\ 0 & gcd(a,n) > 1 \end{cases}$$

For n being a product of two large primes, given an element $a \in \mathbf{Z}_n^*$, if $\left(\frac{a}{n}\right) = 1$, it is hard to decide whether $a \in \mathbf{Q}_n$. Whereas, if $\left(\frac{a}{n}\right) = -1$, then it is sure that $a \in \overline{\mathbf{Q}_n}$. If $n = p \times q$ and the two primes factors of n are known then, given any $a \in \mathbf{Z}_n^*$, if $\left(\frac{a}{n}\right) = 1$, it is easy to determine whether $a \in \mathbf{Q}_n$. In that case $a \in \mathbf{Q}_n$ if both $\left(\frac{a}{p}\right) = 1$ and $\left(\frac{a}{q}\right) = 1$. On the other hand, if both $\left(\frac{a}{p}\right) = -1$ and $\left(\frac{a}{q}\right) = -1$, then $a \in \overline{\mathbf{Q}_n}$.

Let $n \geq 3$ be an odd composite number, $\mathbf{J}_n^+$ is the set of all pseudosquares and defined as

$$\mathbf{J}_n^+ = \{a \in \mathbf{Z}_n^* \mid \left(\frac{a}{n}\right) = 1\}.$$

$\mathbf{J}_n^-$ is the set of all quadratic nonresidues and defined as $\mathbf{J}_n^- = \{a \in \mathbf{Z}_n^* \mid \left(\frac{a}{n}\right) = -1\}$.

Let n be a product of two distinct primes. Then half of the elements in $\mathbf{J}_n^+$ are quadratic residues and the other half are quadratic nonresidues. That is, if a ϵ $\mathbf{J}_n^+$, then the probability of a ϵ $\mathbf{Q}_n$ is $\frac{1}{2}$.

B. Properties of Sender-Side Deniable Encryption Protocol

The sender-side deniable encryption mechanism:
A public-key encryption mechanism π is a sender-side deniable encryption if the following properties hold.

1. **Correctness:** The probability of the receiver's decryption differing from the sender's original message is negligible.
2. **Security:** For any two messages (m,m_f) the communications for transmitting m are computationally indistinguishable from the communications for transmitting m_f . We denote the indistinguishability as: $COM_\pi(m) \approx COM_\pi(m_f)$.
3. **Deniability:** Given a message m, a random input r and a communication protocol COM_π, the encryption mechanism results the cipher $c = COM_\pi(m, r)$. Then there exists a faking algorithm φ such that, φ takes the input parameters as the *true message m*, the *true random input r* and any fake randomness r_f and produces a fake message $m_f = \varphi(m, r, r_f)$ where the communication of the true message and the fake message are computationally indistinguishable, that is $COM_\pi(m, r) \approx COM_\pi(m_f, r_f)$.

The deniability provides a mechanism to derive a pair (m_f, r_f) such that, the encryption of message m with the random input r according to the communication protocol π is indistinguishable from the encryption of the message m_f with random input r_f . Thus the coercion can be overcome by hiding the true message m and disclosing the fake massage m_f with the random input r_f .

3.1 A Deniable Encryption Scheme

In [22] a sender-side deniable encryption scheme was proposed. Let n is a product of two distinct large primes (p and q) of equal size. The receiver's public key is n and the private key is (p, q). Let d : {0, 1} → $\mathbf{J}_n^*$ is a random trap-door function that randomly maps the binary set to an element in the set $\mathbf{J}_n^*$ is defined as follows:

$d(0) = a$ where $a \in_R \mathbf{J}_n^+$

$d(1) = a$ where $a \equiv x^2 \bmod n$, $x \in \mathbf{Z}_n^*$ and a $\in_R \mathbf{Q}_n$

The set $\mathbf{J}_n^+ \subset \mathbf{Z}_n^*$ denotes the set of all elements for which Jacobi symbol with respect to modulo n is 1 and $\mathbf{Q}_n \subset \mathbf{Z}_n^*$ is the set of all quadratic residue set of modulo n. With the trap-door information (that is p and q) it is easy to compute the inverse mapping of d;

$d^{-1}(a) = 0$ where $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) = -1$

$d^{-1}(a) = 1$ where $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) = 1$

But without knowing the value of p and q it is hard to compute the inverse of d.

Deniable Encryption by Sender One-time-padding is used as the encryption procedure. Let m is the message and r is a random string, the encrypted message is $c = m \oplus r$. The sender computes the cipher as a two tuple (c,A). The tuple A is a representation of r, such that, the receiver can decode the random string r from A with negligible error probability. Whereas, if the sender is coerced, sender can easily construct a different fake random string r_f for A and produce a fake message m_f to prove that the cipher c is the encryption of m_f and r_f. The tuple A is a $k \times t$ matrix of elements from J_n^+ and constructed as follows:
The i^{th} row of the A matrix is

$$A(i)[1...t] = d(0) \quad \text{if } b_r^i = 0$$
$$A(i)[1...t] = d(1) \quad \text{if } b_r^i = 1$$

That is, if the i^{th} bit of r (denoted as b_r^i) is 0, then the i^{th} row of A contains t random elements computed by the function d(0), otherwise, if $b_r^i = 1$, then the i^{th} row of A contains t random elements computed by the function $d(1)$. Sender sends (c,A) to the receiver.

Receiver Decryption Receiver first decodes A to the binary string r. The receiver's private key is (p, q). So receiver can easily compute the inverse of d. Receiver decodes the tuple A as follows:

$b_r^i = 0$ if $\exists$j = {1, 2, . . . t} where $d^{-1}(A[i][j]) = 0$
$b_r^i = 1$ if $\forall$j = {1, 2, . . . t} where $d^{-1}(A[i][j]) = 1$

After reconstructing r, the message is decrypted as $m = c \oplus r$. The probability of erroneous reconstruction of one 0 bit to 1 is $\left(\frac{1}{2}\right)^t$.

.

Dishonest Opening by the Sender If the sender is coerced; he dishonestly opens the random string to some fake string r_f and computes the fake message m_f to satisfy that the encryption of r_f and m_f results to c. Now, neither the sender nor the coercer knows the trap-door information (p, q). So, they do not compute the inverse of d. To open the random string r, sender has to disclose the values of x for the function $d(1)$. The sender discloses r as follows:

$b_r^i = 1$ when $x_{i,j} \subset \mathbf{Z}_n^*$ and $x_{i,j}^2 \equiv A[i][1 \ldots t] \bmod n$
$b_r^i = 0$ otherwise

That is, to open the i^{th} bit of r as 1, sender has to show the square roots of t elements of the i^{th} row of A. As the square root computation in modulo n is *hard*, neither the coercer nor the sender can explicitly compute the square root of any element $a \in A$. Hence, the coercer has to believe upon the sender, as he opens the random string. The sender can flip any bit from 1 to 0 by concealing the t square roots of a s in a particular row of A, but he cannot flip a 0 bit to 1.

3.2. A Valid Message Deniable Encryption Scheme

The scheme allows the sender to deny a true message m by producing the fake message m_f and the fake randomness r_f. But the fake message m_f is a function of the fake random string r_f, (that is, $m_f = c \oplus r_f$). As the valid message set M in electronic election and auction are comparatively

very small related to the message space M, the probability of $m_f \in M$ is very less. That is, if the sender randomly flips some bits of r to form r_f, then there may be very less possibility that m_f will be a valid message. So the sender has to determine the possible fake messages beforehand and then generates the random string r in such a way that he can produce the corresponding fake random strings r_f easily for which the encryption of m_f and r_f results to the cipher c. To do this the sender computes the message difference $m_d = m \oplus m_f$. The 1 bits in m_d implies that, if we flip the bits of m at that positions the result will be m_f. The encryption process works as follows:

1. Sender computes m_d
2. Sender generates the random string r by changing some 0 to 1 in the m_d
3. Sender encrypts the true message as $c = m \oplus r$
4. Sender computes the matrix A for the random string r

The random string r must be between m_d and [11 . . . 1]. If $r = m_d$ then the cipher c will be m_f and if r = [11 . . . 1] then the cipher c will be $\overline{m}$. During the dishonest opening, the sender flips only those positions of r where there are 1s in the m_d.

3.3. Implementation Constraints

Consider an election/auction protocol with the valid message set M. Let $m_1, m_2 \in M$ and m_1 is the true message and during dishonest opening, the sender would produce the fake message as m_2. Sender computes a random string r that contains the m_d (where $m_d = m_1 \oplus m_2$). In this scenario the following cases may happen:

$r = m_d$, then the cipher will equals to m_2.
$r = [11 \ldots 1]$, then the cipher will equals to $\overline{m}$.
$m_d \in r$, then cipher is a random string and deniability can be guaranteed.

But at the same time, according to the basic principle of the deniable encryption the string r must be a random string. So the sender cannot compute a string r which does not seem to be random (the distribution of 0s and 1s must be random). To ensure the above, we define a random mapping $I : M \rightarrow \mathbf{I}$, where I is called an indexing of the valid message m to an indexed message $\hat{m}$. The mapping I should follow the following properties:

1. All the indexed message $\hat{m} \in I$ are equal in size
2. All the indexed messages must be theoretically random
3. For any two indexed messages $\hat{m}_1$, $\hat{m}_2 \in I$, the message difference contain less numbers of 1s.

Now the sender computes the random string r properly. Sender generates a string r randomly and computes the randomness for one-time-padding as $r = r \oplus m_d$, where m_d is the message difference of $I(m)$ and $I(m_f)$ (m is the true message and m_f is the fake message). As $I(m)$ and $I(m_f)$ are equal in size and their difference contains less number of 1s, the OR operation of r and m_d does not lose the randomness of r. After decryption or dishonestly opening the cipher, the receiver/sender has to compute the inverse index function to get back the message.

The above is also useful to overcome the multiple coercing problem. If there are multiple coercers, those can coerce a candidate individually, then the candidate has to dishonestly open the same cipher to different fake messages in front of the individual coercer. Let m is the true message and $m_{f1}, m_{f2}, \ldots m_{ft}$ are the fake messages that the candidate would open during coerced by the coercer $C_1, C_2, \ldots, C_t$ respectively. In that case, the candidate generates r randomly and computes the random string for one-time-padding as

$r = r \vee m_{d1} \vee m_{d2} \vee ... \vee m_{dt}$, where $m_{di} = I(m) \oplus I(m_{fi})$. The mapping I ensures that m_{di}s do not contain many number of 1s. Therefore the successive OR operations with m_{di} lose less amount the randomness in r.

3.4. Existing Schemes without Untappable Channel

The existing election [2, 3, 14] and auction [5, 13, 16] schemes use encryption with randomness to secure the votes/bids form adversary. The encryption process produces the cipher which are random string over C, called cipher space. The cipher space C is sufficiently big and the ciphers are generally equal in size. But the bit differences among any two ciphers is also a random element in C. So, any pre-encryption mechanism results a random element over a sufficiently big set C which satisfy the first two properties of I function described in the previous section. However, the relaxation of the third property may not overcome the coercion by multiple coercions.

Fig 1 shows a simulation result for the estimation of the message difference string, where pre-encryption is used before the deniable encryption scheme. We vary the cipher space C from 128-bits to 1024-bits strings and calculate the number of 1s in the message-difference string for any randomly selected two ciphers from the cipher space C. The result shows that the distribution of 1s in the message-difference string are random and the count of occurrence of 1s are approximately half of the size of the ciphers.

To plausibly deny a true message m, the candidate first determines the fake message m_f. Then he computes the pre-encryption of m and m_f . Let c and c_f be the corresponding ciphers of m and m_f. Then the candidate computes $c_d = c \oplus c_f$ and computes the random string r by flipping some 0 bit of c_d to 1 randomly. The deniable encryption of c is $\hat{c} = c \oplus r$. During dishonest opening, the candidate flips the bits 1 to 0 of r where there is 1 in the c_d and produces r_f and c_f to the coercer. The candidate also opens the fake message m_f and proves that pre-encryption of m_f results to c_f . Thus the candidate conceals the true message m and conveniently convince the coercer with the fake message. Fig.2 describes the model of deniable encryption.

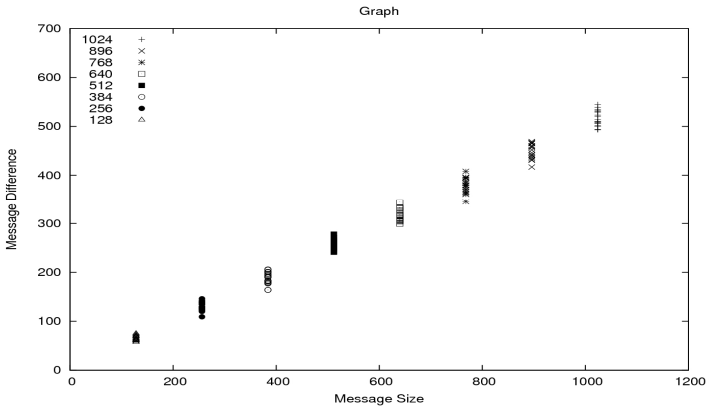

Figure 1. Average Message Difference Between to Random Messages

Cipher and Key Size in Deniable Encryption

The ciphers of the deniable encryption are relatively bigger then the plaintexts. Generally the pre-encryption proposed in different literatures [2, 3, 14] and [5, 13, 16] are mapping from $M \rightarrow C$, where $C = \mathbf{Z}_p$, p is large prime, then the plaintexts for the deniable encryption are $log_2 p$ bits.

Deniable encryption encrypts each bits of the plaintext to *t* random number in $\mathbf{Z}_n^*$, where the *A* matrix in the cipher has *t* columns. So the number of bits in the cipher are $t \times log_2 p \times log_2 n$.

Modern mainstay *ciphersystems* do not offer deniability because they all use a small key. If the key is as large as the message it may offer total deniability meaning that any plaintext the size of the *ciphertext* may be fitted with a proper key. For shorter keys the deniability is more limited. Hence modern *ciphersystems* where the key can grow in size without imposing a computational penalty do offer deniability. In the deniable encryption scheme proposed in this paper, the plaintext having $log_2 p$ bits are expanded to $t \times log_2 p \times log_2 n$ bits in the ciphertext. Thus substantial deniability is achieved without incurring subsequent computational penalty. Modern deniable encryption techniques exploit the *pseudorandom permutation* properties of existing *block ciphers*, making it cryptographically infeasible to prove that the *ciphertext* is not in fact random padding data generated by a *cryptographically secure pseudorandom number generator*.

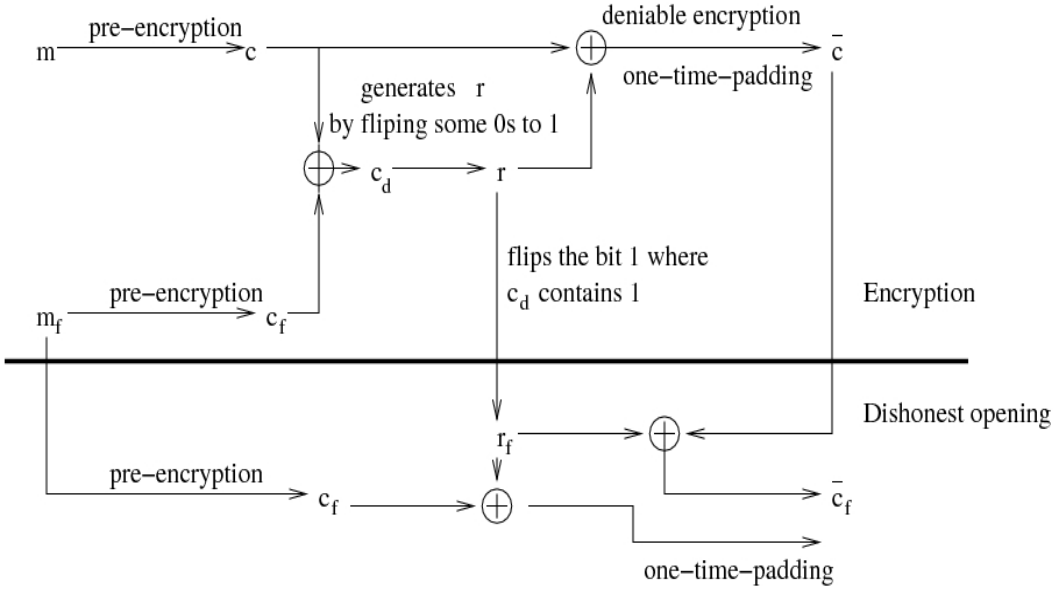

Figure 2. Deniable Encryption Model

5. DENIABILITY AND ANONYMITY

The deniable encryption mechanism described in this paper is used to overcome the coercing problem at the voter/bidder side. The situation would be worst if there are some authorities (vote tallying authority/auctioneer) who are colluded. The coercer may collect the encrypted votes/bids form the colluded authorities and will coerce the candidates. Neither the untappable channel nor the deniable encryption mechanism can prevent the coercer to coerce the candidates. To protect the candidates from coercing, in presence of colluded authorities, anonymous casting is proposed in different literatures [27]. Anonymity can be achieved by mixnet [25, 26]. Mixnet is the technique that uses cryptography and permutation to provide anonymity. A mixnet consists of sequence of server called mixes, each server receives a batch of input message and produces as output in a batch in permuted (mixed) order with a change of the appearance of the batch. The change of appearance and the random reordering of batch provide untracebility between the output batch and the input batches.

The deniable encryption mechanism can be redesign to provide a deniable mixnet between the candidates and the authorities. In that case, the private key of the deniable

encryption would be shared among the mixnet servers. The authorities will receive the anonymous encrypted private values from the candidates. It the coercer is provided the anonymous encrypted bids, he will not able to find the candidates to whom the encrypted bid belongs to; hence coercing is not feasible.

6. CONCLUSIONS

In this paper we have presented a technique that would replace the untappable channel used in election and auction protocol by deniable encryption. The adversary is allowed to tap the communication but if the adversary coerces the sender, then the sender can easily convince the coercer with a fake message that the cipher is the encryption of the fake message by concealing the true message. The deniable encryption scheme does not require any infrastructure and easy to deploy. The prior protocols which are based on public key cryptography and assume the existence of untappable channel are easily upgraded to a protocol without untappable channel without changing the basic encryption principle. However, deniable encryption has an expansion of the cipher size. Since, it does not use receipts and concepts of registration, so it can be effectively deployed in electronic auction mechanisms and is more secure as it does not assume untappable channels.

7. ACKNOWLEDGEMENT

Parts of the paper were published in ARTCom 2009, IEEE and NCS 2010, Bangalore. The authors would like to thank all the reviewers.

REFERENCES

[1] Josh Benaloh and Dwight Tuinstra: Receipt-Free Secter-Ballot Election (Extended Abstract). In Proc. 26th ACM Symposium on the Theory of Computing (STOC), 544-553. ACM, (1994).

[2] Martin Hirt and Kazue Sako: Efficient Receipt-Free Voting Based on Homomorphic Encryption. In Proc. EUROCRYPT 2000,539-556. LNCS 1807.

[3] Tatsuaki Okamoto: Receipt-Free Electronic Voting Schemes for Large Scale Elections. In Proc. Security Protocols Workshop, 1997,25-35. LNCS 1369.

[4] Matthew L. Franklin and Michael K. Reiter: The Design and Implementation of a Secure Auction Service. Trans. Software Engineering, IEEE, 1996, vol. 2, 302-312.

[5] Masayuki Abe and Koutarou Suzuki: Receipt-Free Sealed-Bid Auction. In Proc. ISC 2002, 191-199, LNCS 2433

[6] Masayuki Abe: Universally VerifiableMix-NetWith VerificationWork Independent of The Number of Mix Servers. In Proc. EUROCRYPT 1998, 437-447, LNCS 1403

[7] Michels Markus and Horster Patrick: Some Remarks on a Receipt-Free and Universally Verifiable Mix-Type Voting Scheme In Proc. ASIACRYPT '96 125-132, Springer-Verlag

[8] Olivier Baudron, Pierre-Alain Fouque, David Pointcheval, Jacques Stern and Guillaume Poupard: Practical Multi-Candidate Election System, In Proc. PODC 2001, 20th Annual ACM Symposium on Principles of Distributed Computing, 2001, 274-283, ACM

[9] Desmedt Yvo: Threshold Cryptography. Trans. on European Transaction on Telecommunications, Vol. 5, No. 4, 449-457

[10] Adi Shamir: How to Share a Secret. Trans. on Commun. ACM, 1979, Vol. 22 No. 11, 612-613, ACM

[11] Torben P. Pedersen: A Threshold Cryptosystem without a Trusted Party (Extended Abstract). In Proc. EUROCRYPT '91, 522-526, Springer

[12] Kazue Sako: An Auction Protocol Which Hides Bids of Losers. In Proc. Public Key Cryptography 2000, LNCS 1751, 422-432, Springer

[13] Xiaofeng Chen, Byoungcheon Lee and Kwangjo Kim: Receipt-Free Electronic Auction Scheme using Homomorphic Encryption. In Proc. ICISC 2003, 259-273, LNCS 2971

[14] M. Burmester, E. Magkos and V. Chrissikopoulos: Uncoercible e-Bidding Games. Trans. Electronic Commerce Research, Vol. 4, No. 1-2, 2004, 113-125, Kluwer Academic Publishers,Norwell, MA, USA

[15] Kazue Sako and Joe Kilian: Receipt-Free Mix-Type Voting Scheme - A Practical Solution to the Implementation of a Voting Booth. In Proc. EUROCRYPT '95, 393-403, Springer

[16] Jaydeep Howlader, Anushma Ghosh and Tandra Deb Roy: Secure Receipt-Free Sealed-Bid Electronic Auction. In Proc. IC3 2009, CCIS 40, Springer

[17] Ran Canetti, Cynthia Dwork, Moni Naor and Rafail Ostrovsky: Deniable Encryption In Proc. CRYPTO 97, LNCS 1294, 90-104, Springer

[18] S. Goldwasser and S. Micali: Probabilistic Encryption. Trans. on Journal of Computer and System Sciences, Vol. 28, 270-299, 1984.

[19] M. H. Ibrahim: A Method for Obtaining Deniable Public-Key Encryption. Trans. on International Journal of Network Security (IJNS), Vol. 8, No. 1, 1-9, Jan09

[20] Emmanouil Magkos, Mike Burmester and Vassilios Chrissikopoulos: Receipt-Freeness in Large-Scale Elections without Untappable Channels. In Proc. 1st IFIP Conference on E-Commerce, E-Business, E-Government 2001, 683-694, IFIP Conference Proceedings, Vol. 202

[21] Byoungcheon Lee Kwangjo: Receipt-Free Electronic Voting Scheme with a Tamper- Resistant Randomizer. In Proc. ICISC 2002 LNCS 2587, 389-406, Springer

[22] Jaydeep Howlader and Saikat Basu: Sender-Side Public Key Deniable Encryption Scheme. In Proc. ARTCom 2009, IEEE, 9-13

[23] Alfred J. Menezes and Paul C. van Oorschot and Scott A. Vanstone: Handbook of Applied Cryptography. 1996, ISBN 0849385237, CRC Press

[24] Chun-I Fan and Wei-Zhe Sun: Uncoercible Anonymous Electronic Voting. In Proc. JCIS 2006

[25] Byoungcheon Lee1, Colin Boyd, Ed Dawson1, Kwangjo Kim, Jeongmo Yang, and Seungjae Yoo: Providing Receipt-Freeness in Mixnet-Based Voting Protocols. In Proc. ICISC 2003, LNCS 2971, pp 245-258, 2004

[26] K. Sako and J. Kilian, "Receipt-free mix-type voting scheme – a practical solution to the implementation of a voting booth", *Advances in Cryptology – Eurocrypt'95*, LNCS 921, pp. 93–403, 1995.

[27] David Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. Communications of the ACM, 4(2), February 1982.

Authors

Jaydeep Howlader received the B.Tech. degree in Computer Science and Engineering from the Kalyani Government College, Nadia, India, and the M.Tech degree from National Institute of Technology, Durgapur, India in 2001 and 2009, respectively. He is currently working toward the Ph.D. degree at the National Institute of Technology, Durgapur, India. He is now working as an Assistant Professor in the Department of Information Technology at the National Institute of Technology,Durgapur. His research interests include cryptography and information security.

Vivek Nair received the B.Tech. degree in Computer Science and Engineering from Academy of Technology, India, in 2009 He is currently working toward the M.Tech. degree at the National Institute of Technology, Durgapur, India.. His research interests include Networking, Distributed System and Cryptography.

Saikat Basu is currently a final year undergraduate student in National Institute of Technology, Durgapur, India. His primary field of interests includes Cryptography,Network Security and Mobile Computing.

Ashis Kumar Mal received his Ph.D. in microelectronics and VLSI from the Indian Institute of Technology, Kharagpur, India, in 2009. He joined the Electronics and Communication Engineering Department, North Eastern Regional Institute of Science and Technology (NERIST), Itanagar, in 1993 as a Lecturer. In 2007, he joined the National Institute of Technology (NIT), Durgapur, and currently serves as an Associate Professor there. His research interests include mixed signal VLSI design, sampled analog circuits, interconnect modeling, and optical networking. Dr. Mal has coauthored more than 40 technical papers. He is a member of IEEE.