Practical Fair Anonymous Undeniable Signatures

Song Han, Elizabeth Chang, Xiaotie Deng, Li Gao and Winson Yeung

Abstract—We present a new model for undeniable signatures: fair-anonymous undeniable signatures. This protocol can not only preserve the privacy of the signer (i.e. anonymity) but also track the illegal utilization of the valid signatures. In addition, our model prevents the trusted centre from forging a valid signature for any signer.

Keywords—Cryptography, Fair Anonymity, Information Security, RSA Signatures, Undeniable Signatures.

I. Introduction

As the Information Technology's presence gets larger and more pronounced, we can expect to see some changes. Many of those changes have already started to happen. The most attractive characteristics for those changes are: Multi-user electronic commerce is more and more concerning the issue of security and privacy. Various solutions were proposed for this issue, for example, encryption technique, digital signature technique (including general signature scheme, blind signature scheme, undeniable signature scheme, group signature scheme, etc.), and other cryptographic techniques [16], as well as steganography techniques. Anonymity and fair anonymity are one of the important goals achieved by some of these techniques.

Undeniable signatures are one of the techniques, which can help to achieve anonymity and fair anonymity. Undeniable signatures, first devised by David Chaum and Hans van Antwerpen [4], are non self-authenticating (i.e. non universal verifiability) signature schemes, where signatures can only be verified with the consent of the signer (e.g. a company). However, if a signature is only verifiable with the aid of a signer, a dishonest signer may refuse to authenticate a genuine document. Undeniable signatures solve this problem by adding a new component called the denial protocol in addition to the normal components of signature and verification. That is, undeniable signatures have two distinctive features:

1. The verification process is interactive, so the signer can limit who (e.g. payee) can verify their signature.
2. A disavowal protocol, that is a cryptographic protocol which will allow them to prove that a given signature is a forgery.

The first property means that a signer can allow only those who are authorized to access the document to verify their signature. If the document were to be leaked to a third party, the third party would be unable to verify that the signature is genuine. However because of this property it means that the signer may deny a signature which was valid. To prevent this we have the second property, a method to prove that a given signature is a forgery.

The protection of signatures from being verified without the permission of the signer is not only justified by confidentiality and privacy concerns but it also opens a wide range of applications where verifying a signature is a valuable operation by itself. A typical scenario is the case of a software company that uses signature confirmation as a means to provide a proof of authenticity of their software to authorized (e.g., paying) customers only. This example illustrates the core observation on which the notion of undeniable signatures stands: *verification of signatures, and not only their generation, is a valuable resource to be protected.*

So far, various undeniable signatures have been created, [2]-[5], [7], [9], [11]-[13], [15], [17]. Those schemes provided undeniability analysis (including completeness, soundness, and zero-knowledge). However, it will be more interesting if anonymity for undeniable signatures are proposed in today's electronic commerce. Galbraith and Mao [7] constructed such a scheme and provided the anonymity analysis. However, their scheme only proposed perfect anonymity. That is, their scheme always preserves the *privacy* of signers in any case and the signers have *perfect privacy*. Therefore, users may ask such an interesting problem: how can we identify the signer who did anything illegal by taking advantage of the undeniable signature scheme.

In this paper, we solve the above problem. Moreover, the proposed undeniable signature scheme has the significant properties of undeniability and fair anonymity, simultaneously. In addition, we also have improved the result reported in [18]. In our scheme, a *trusted center* is involved. In practical scenario, a bank or a government will play the role

Manuscript received November 3, 2004. This work was supported in part by a research fellowship and ARC funding at CEEBI and Curtin, and a research funding of Hong Kong Research Grant Council.

Song Han is with the School of Information Systems and the Department of Computing, Curtin University of Technology (e-mail: hans@cs.curtin.edu.au). He will join the Centre for Extended Enterprises and Business Intelligence.

Elizabeth Chang is with the School of Information Systems, Curtin University of Technology.

Winson Yeung, Xiaotie Deng are with the Department of Computer Science, City University of Hong Kong .

Li Gao is currently with the College of Applied Science, Beijing University of Technology.

of a *trusted center.* From some point of view, they act as the authorized organizations.

The organization of the rest of this paper is as follows. In section 2, we first provide the definition of fair anonymous undeniable signature. In section 3, the fair-anonymous undeniable signature scheme is proposed. In section 4, the analysis and proofs are provided, mainly including unforgeabiligy and undeniability, as well as fair anonymity – a very important property for a practical undeniable signature scheme. The performance analysis and the conclusions appear in section 5 and section 6, respectively.

II. Definition of Fair-Anonymous Undeniable Signatures

In this section, we will provide the definition of fair anonymous undeniable signatures (or fair AUS).

A fair anonymous undeniable signature (fair AUS) scheme consists of four algorithms, namely Setup, Key, Sign and DelAnonymity, and two protocols, namely Confirmation and Denial protocols. For every choice of the security parameter *k* there is a public-key space $\underline{K}$, a message space $\underline{M}$ and a signature space $\underline{S}$. For our applications we stress that the space $\underline{S}$ must depend only on the security parameter *k* and not on a specific public key.

Setup is a probabilistic polynomial time algorithm which takes as input a security parameter *k* and outputs a family of system parameters.

Key is a probabilistic polynomial time algorithm which is executed by a trusted centre and the signers. The input contains system parameters, as well as random parameters which are chosen by the trusted centre and the signers. The output includes a public key $pk \in \underline{K}$ and a corresponding secret key *sk*.

Sign is a probabilistic polynomial time algorithm, which takes as input a secret key *sk* and a message $m \in \underline{M}$ and outputs a signature $Sig_{sk} \in \underline{S}$. In general, there are many valid signatures for any pair $(m, pk) \in \underline{M} \times \underline{K}$.

Confirmation is a deterministic polynomial time protocol between a signer and a verifier (e.g. a payee). The input contains a message $m \in \underline{M}$, a signature $s \in \underline{S}$ and a (certified) public key *pk*. This protocol permits the signer to prove to a verifier that the signature *s* is valid on the message *m* and the public key *pk*. If the verifier has a suitable public key then the proof may be taken to be a non-interactive, designated-verifier proof.

Denial is a deterministic polynomial time protocol. The public input includes $m \in \underline{M}$, $s \in \underline{S}$ and $pk \in \underline{K}$. This protocol makes a signer prove to a verifier that the given signature is not valid for the message and that public key.

DelAnonymity is a deterministic polynomial time algorithm, which is executed only by the trusted centre. The input includes $m \in \underline{M}$, $s \in \underline{S}$ and some system parameters. The output is the identity of the originator for the signature $s \in \underline{S}$.

Remark 1 For some undeniable signature schemes, the denial protocol may be the same as the confirmation protocol from the point of the initial state of the protocol.

III. Theoretical Foundation of Fair AUS

The proposed scheme consists of the following algorithms: *Setup*, *Key*, *Sign*, *Confirm*, *Deny*, *DelAnonymity*. Details of them are described as follows:

We first present the setup for the proposed fair anonymous undeniable signature scheme. Afterwards, the main steps of the protocol are provided.

A. Setup Algorithm

The *Setup algorithm* is a probabilistic polynomial algorithm. It is carried out by a trusted center.

(1) The trusted center chooses N pairs of primes $\{p_i, q_i\}$ $(1 \le i \le N)$, where $p_i \equiv q_i \equiv 3 (\mathrm{mod}\, 4)$, and all prime factors of $(p_i - 1)/2$ and $(q_i - 1)/2$ are greater than a soundness bound B as in [9].

(2) She computes $n_i \leftarrow p_i q_i$ and chooses $e_i, d_i \xleftarrow{R} \square_{n_i}^{*}$ such that $e_i d_i \equiv 1 (\mathrm{mod}\, \varphi(n_i))$ where $\varphi(\cdot)$ is Euler phi function.

(3) The family $\{(n_i, p_i, q_i, e_i, d_i) \mid 1 \le i \le N\}$ forms the database of the trusted center.

(4) She sends the ciphertext of $\{n_i, e_i, d_i\}$ to $signer_i$ for $1 \le i \le N$; here the trusted center uses the Cramer-Shoup public key encryption system [6] to encrypt $\{n_i, e_i, d_i\}$.

(5) Let $D = \{0,1\}^*$ be the document space, in which the messages will be signed.

B. Key Algorithm

The *Key algorithm* is a probabilistic polynomial time algorithm, which is executed by the signers.

(1) For any $1 \le i \le N$, the $signer_i$ gets the ciphertext of $\{n_i, e_i, d_i\}$ from the trusted center, and then decrypts it.

(2) He chooses $x_i, y_i \xleftarrow{R} \square_{n_i}^{*}$ and computes $g_i = (x_i y_i)^2 \left(\mathrm{mod}\, n_i\right)$ and $h_i = g_i^{e_i} (\mathrm{mod}\, n_i)$.

(3) Finally he gets $SK_i \leftarrow \{n_i, e_i, d_i, x_i, y_i\}$ as the private key, and $PK_i \leftarrow \{n_i, g_i, h_i\}$ as the public key.

C. Sign Algorithm

The *Sign algorithm* is still a probabilistic polynomial time algorithm. Given any message $M \in D$, and $SK_i \leftarrow \{n_i, e_i, d_i, x_i, y_i\}$ and $PK_i \leftarrow \{n_i, g_i, h_i\}$ respectively being the private key and public key of $signer_i$.

(1) To sign a message M, $signer_i$ first chooses $r \xleftarrow{R} \square_{n_i}^{*}$, and computes $s_1 \leftarrow x_i H(M \| r)^{(g_i - r) d_i} (\mathrm{mod}\, n_i)$ and $s_2 \leftarrow y_i H(M \| r)^{rd_i} (\mathrm{mod}\, n_i)$.

(2) He then calculates $s_c^{'} = s_c + b_c n_i$ for $c \in \{1, 2\}$, where b_c are chosen so that $|s_c^{'}| \le k$.

(3) He then obtains a signature $\{s_1^{'}, s_2^{'}, H(M \| r)\}$ for M.

D. Confirm or Deny Algorithm

The *Confirm or Deny algorithm* is a deterministic polynomial time algorithm. They are the interactive algorithms between the signers and the verifiers. To confirm or deny an alleged undeniable signature $\{s_1', s_2', H(M\|r)\}$, the $signer_i$ executes the non-interactive, designated verifier versions of the proofs ([14]) which prove the two relationships:

1. $g_i \equiv h_i^{d_i} \pmod{n_i}$
2. $(s_1' s_2' \pmod{n_i})^{2e_i} \stackrel{?}{\equiv} h_i H(M\|r)^{2g_i} \pmod{n_i}$

E. DelAnonymity Algorithm

The *DelAnonymity algorithm* is also a deterministic polynomial time algorithm. The executing of this algorithm is only titled to the trusted center.

(1) When certain emergence case appears, the trusted center will quickly be "on-line" and search her database.

(2) For $i=1$ to N, the trusted center checks whether

$$(s_1' s_2' \pmod{n_i})^{2e_i} \equiv h_i H(M\|r)^{2g_i} \pmod{n_i} \quad (1)$$

If there exists an I such that

$$(s_1' s_2' \pmod{n_I})^{2e_I} \equiv h_I H(M\|r)^{2g_I} \pmod{n_I} \quad (2)$$

then the trusted center will tell us that it is just the $signer_I$ who has signed the signature $\{s_1', s_2', H(M\|r)\}$.

Prior to going further, we give the following remarks.

Remark 2: The proposed fair anonymous undeniable signature scheme can be used to sign various messages, including short messages and long messages. That is, there is no limit on the length of messages to be signed.

IV. Theorem Proof and Case Studies against Attack

This section we will analyze our undeniable signature scheme and come up with all the proofs of the scheme. We will prove that our scheme has the significant properties: unforgeability, undeniability and fair anonymity.

A. Unforgeability

Unforgeability means that illegal entity can not create a valid undeniable signature which can successfully pass the check of the *Confirmation* protocol and the *Denial* protocol. By comparision, the trusted center should have higher probability than an outside adversary in forging a valid signature successfully, since she knows more secret information about the signers than an adversary does. So it would be much convincible if we can prove that *even the trusted center is not able to impersonate any legal singer to forge a valid signature*.

Theorem 1 The trusted center is not able to impersonate any legal signer to forge a valid signature.

We can prove this theorem by considering two cases of attack made by the center:

Case 1: The trusted center cannot reveal the private key from the public key or her database for any signer. Since x_i, y_i are only known by each $signer_i$ and even if the trusted center knows the factorization of n_i, it does not help to recover x_i and y_i from $g_i = (x_i y_i)^2 \pmod{n_i}$.

Lemma 1 Given the factorization of n_i, for reasonably large number g_i, the probability of the trusted center recovering x_i and y_i from $g_i = (x_i y_i)^2 \pmod{n_i}$ is negligible with respect to the fair anonymous undeniable signature scheme.

Proof Since n_i is a composite number, by the number theory, for large number g_i, $g_i \pmod{n_i}$ has four different square roots corresponding to the equation $g_i = (x_i y_i)^2 \pmod{n_i}$. Let these roots be respectively:

$X_1 \pmod{n_i}$, $X_2 \pmod{n_i}$, $X_3 \pmod{n_i}$, $X_4 \pmod{n_i}$.

For each case, $X_j = x_i y_i \pmod{n_i}$ (for $1 \le j \le 4$) is an uncertain equation with two different unknown elements. Suppose it has α_j pairs of solutions, i.e.

$$\begin{Bmatrix} x_{l_1} \\ y_{l_1} \end{Bmatrix}, \begin{Bmatrix} x_{l_2} \\ y_{l_2} \end{Bmatrix}, \begin{Bmatrix} x_{l_3} \\ y_{l_3} \end{Bmatrix}, \ldots, \begin{Bmatrix} x_{l_{\alpha_j}} \\ y_{l_{\alpha_j}} \end{Bmatrix}$$

Then, the equation $g_i = (x_i y_i)^2 \pmod{n_i}$ with x_i and y_i being the unknown elements has

$\gamma = \alpha_1 + \alpha_2 + \alpha_3 + \alpha_4$ different pairs of solutions.

Therefore, the probability ε of the trusted center recovering x_i and y_i from $g_i = (x_i y_i)^2 \pmod{n_i}$ for the fair anonymous undeniable signature scheme is $\frac{100}{\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4}\%$. By the property of Z_{n_i}, with certain high probability we know that $\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 \ge [g_i/2]$, where $[g_i/2]$ is the least integer greater than or equal to $g_i/2$. Therefore, the above probability is negligible.

Case 2: The trusted center cannot forge valid signatures by making adaptive queries to the scheme. We can prove this point according to the unforgeability security of our scheme.

Theorem 2 *The proposed scheme is secure against chosen message attack under the condition that the underlying RSA signature is unforgeable against chosen message attack.*

Proof We first investigate the plain RSA signature:

Message: M

Signature: $s = M^d \pmod{n}$

It is well known that the plain RSA signature is not unforgeable against the adaptive chosen message attack. Hence some researchers for example Bellare and Rogaway [1] suggest using the padding scheme for the plain RSA signature in order to make it unforgeable against the adaptive chosen message attack. Therefore, the regular RSA signature has the following formulas:

Message: M

Signature: $s = E(M)^d \bmod n$

In the above signature, $E(M)$ is the encapsulation of the message M [16]. For example, M can be hashed by a padding scheme $H(M\square r)$, where $H(\cdot)$ is a collision-free hash function, and r is chosen randomly from $\square_n^*$. By the report in [1], we know that the regular RSA signature is unforgeable against chosen message attack.

Now let us return to our undeniable signature: Suppose $\{s_1', s_2', H(M \| r)\}$ is a valid signature for a message M; Then

$$s_1' = x_i H(M \| r)^{(g_i - r)d_i} \pmod{n_i} \quad (3)$$

$$s_2' = y_i H(M \| r)^{rd_i} \pmod{n_i} \quad (4)$$

We will transform s_1' and s_2' as follows:

$$\begin{aligned} s_1' &= x_i H(M \| r)^{(g_i - r)d_i} \pmod{n_i} \\ &= \left(x_i^{\frac{1}{d_i}} \right)^{d_i} H(M \| r)^{(g_i - r)d_i} \pmod{n_i} \\ &= \left(x_i^{\frac{1}{d_i}} H(M \| r)^{(g_i - r)} \right)^{d_i} \pmod{n_i} \\ &= \left(x_i^{e_i} H(M \| r)^{(g_i - r)} \right)^{d_i} \pmod{n_i} \end{aligned} \quad (5)$$

and

$$\begin{aligned} s_2' &= y_i H(M \| r)^{rd_i} \pmod{n_i} \\ &= \left(y_i^{\frac{1}{d_i}} \right)^{d_i} H(M \| r)^{rd_i} \pmod{n_i} \\ &= \left(y_i^{\frac{1}{d_i}} H(M \| r)^{r} \right)^{d_i} \pmod{n_i} \\ &= \left(y_i^{e_i} H(M \| r)^{r} \right)^{d_i} \pmod{n_i} \end{aligned} \quad (6)$$

By the underlying scheme, only $signer_i$ knows the values of e_i, x_i and y_i. Naturally we can view $x_i^{e_i} H(M \| r)^{(g_i - r)}$ and $y_i^{e_i} H(M \| r)^{r}$ as the encapsulation of M. Therefore, the new undeniable signature is equivalent to its underlying regular RSA signature. However, the regular RSA signature is secure against chosen message attack [1]. Hence, our scheme is also secure against chosen message attack.

B. Undeniability

Undeniability means that the proposed scheme has the completeness, soundness, and zero-knowledge for both the *Confirmation* and Denial protocol. In order to prove the new scheme has the undeniability property, we have to respectively transform the *Confirm or Deny* algorithm of the scheme into the *confirmation protocol* and the *denial protocol* that are designated verifier proofs.

Here we assume the designated verifier Bob is honest in the protocol. In fact, because of the trapdoor commitment scheme we use in the following, the verifier is permitted to be dishonest.

Confirmation Protocol: Given an alleged signature $\{s_1', s_2', H(M \| r)\}$ on message M.

1. Bob chooses $t_1, t_2 \in \square_n^*$ randomly, finds $C_1 \equiv h^{t_1} \pmod{n}$ and $C_2 \equiv (s_1' s_2')^{t_2} \pmod{n}$, and sends them to the signer.
2. The signer computes $R_1 = C_1^{\,d} \pmod{n}$ and $R_2 = C_2^{\,2e} \pmod{n}$, and then computes the commitment $W_1 = Commit(R_1)$ and $W_2 = Commit(R_2)$ to R_1 and R_2 respectively, where $Commit(\cdot)$ is a trapdoor commitment scheme [16]. Finally she sends W_1 and W_2 to Bob.
3. After receiving W_1 and W_2, Bob sends t_1 and t_2 to the singer. The signer checks that C_1 and C_2 are correctly formed, then opens W_1 and W_2 for Bob. Finally Bob gets R_1 and R_2.
4. The verifier Bob will be verifying that:

$$R_1 = g^{t_1} \pmod{n} \quad \text{and} \quad R_2 = hH(M \| r)^{2gt_2} \pmod{n}.$$

If this is the case, Bob accepts the signature to be valid. Otherwise, the invalidity of the signature is "undetermined".

Theorem 3 *The confirmation protocol derived from the Confirm or Deny algorithm has the following properties.*

Completeness: If $\{s_1', s_2', H(M \| r)\}$ on message M is computed correctly, then Bob will accept the proof of the signer.

Soundness: If $\{s_1', s_2', H(M \| r)\}$ is an invalid signature on M, then signer, even computationally unbounded, cannot convince Bob to accept her proof with probability better than $1/B$.

Zero-knowledge: When the signer behaves correctly in the protocol, Bob gains no useful information except the validity of the proof.

Proof *Completeness:* If $\{s_1', s_2', H(M \| r)\}$ on message M has been formed correctly and the signer executes the protocol honestly, then it is easy to see Bob will accept the signer's proof. Therefore, the completeness comes here.

Soundness: Let $\{s_1', s_2', H(M \| r)\}$ be an invalid signature on message *M*. Now the signer will try to convince the verifier that the signature is valid. In order to estimate the cheating probability of the signer, we can assume that this is in the worst case for the verifier, and the best case for the signer. Without lost of generality, we may assume in the confirmation protocol all the first three steps have passed the verifier's check successfully. Therefore, the signer's cheating probability (i.e. to convince the verifier Bob to accept the proof) is maximized by choosing the two responses R_1 and R_2 that pass the verifier's test with maximum probability in step 2 and step 4 in the confirmation protocol. Note that the signer has the private key *d* and *e*, so R_1 will definitely pass the check. Hence, the signer will choose a proper and tricky R_2 in order to pass the test.

By the description above, we can write s_1 and s_2 as

$$s_1 = aH(M \| r)^{(g-r)d} \pmod{n} \quad (7)$$

$$s_2 = bH(M \| r)^{rd} \pmod{n}. \quad (8)$$

Here $a \neq x$ and $b \neq y$. Certainly, the values of *a* and *b* are not known to the signer. Now $C_2 = (s_1' s_2')^{t_2} \pmod{n}$, where t_2 is chosen by the verifier randomly. Note that the signer has to

come up with R_2 before getting t_2. The verifier checks whether:

$$R_2 = C_2^{2e} \pmod n = hH(M \| r)^{2gt_2} \pmod n; \quad (9)$$

$$(ab)^{2et_2} z^{2gt_2} \pmod n = hH(M \| r)^{2gt_2} \pmod n. \quad (10)$$

Therefore, $h = (ab)^{2gt_2} \pmod n$.

Note that a, b and t_2 are information theoretically hidden with respect to the signer. Hence, if the signer wants to cheat successfully (i.e. pass the test), she will have no better strategy than guessing the value of t_2 in the response R_2. Also, note that the order of $\square_n^*$ is $\varphi(n) = (p_i - 1)(q_i - 1)$, and all the prime factors of $(p_i - 1)/2$ and $(q_i - 1)/2$ are greater than B, the probability of the signer selecting t_2 from $\square_n^*$ successfully pass the test is not greater than $1/B$. Hence, the soundness in the theorem is proved.

Zero-knowledge: When the signer behaves correctly and the input $\{s_1', s_2', H(M \| r)\}$ to the confirmation protocol is a valid undeniable signature on message *M*, there is a simulator that can simulate all the transcripts of the protocol. Therefore, the protocol is easily simulatable. Hence, it has the zero-knowledge property. In fact, we construct the simulator as follows:

1. The simulator chooses $\alpha, \beta \in \square_n^*$ randomly;
2. Computes $C_1 = h^\alpha \pmod n$ and $C_2 = (s_1' s_2')^\beta \pmod n$;
3. Rewinds the verifier;
4. Compute $R_1 = g^\alpha \pmod n$ and $R_2 = hH(M \| r)^{2g\beta} \pmod n$;
5. Commits to R_1 and R_2 respectively: $W_1 = Commit(R_1)$ and $W_2 = Commit(R_2)$.

Hence, by the construction of the simulator, the protocol can be simulated successfully.

Lemma 2 We can derive a denial protocol from the Confirm or Deny algorithm of the new scheme and the derived denial protocol has the completeness, soundness and zero-knowledge properties.

Proof The proof is similar to that for **Theorem 3**.

Theorem 4 The proposed undeniable signature scheme has the undeniability property.

Proof By the proving of Theorem 3 and Lemma 2, it is known that the undeniable signature scheme has the undeniability.

C. Fair Anonymity

In this section we prove that our new scheme has the fair anonymity.

Lemma 3 In the random oracle model, our new undeniable signature scheme has the anonymity property under the assumption that the special composite decision Diffir-Hellman problem is hard and the trusted center is trusted.

Proof The proof of the lemma is omitted here since it is similar to Theorem 5 and Corollary 1 in [8] (pp. 90-91).

Lemma 4 The trusted center is able to revoke the anonymity of any signer from the undeniable signature scheme if there is some emergence case.

Proof By the construction of the new scheme we know the trusted center has a database. If some emergence case appears, for example, some $signer_i$ does not use the scheme legally and that results a dispute. Then the trusted center will run the DelAnonymouity algorithm to revoke the anonymity of $signer_i$. Therefore, relevant participants can know who signed the signature $\{s_1', s_2', H(M \| r)\}$. In fact, the center will search her database. For *i=1* to *N*, she checks whether

$$(s_1' s_2' \pmod{n_i})^{2e_i} \equiv h_i H(M \| r)^{2g_i} \pmod{n_i}$$

If there exists an I such that

$$(s_1' s_2' \pmod{n_I})^{2e_I} \equiv h_I H(M \| r)^{2g_I} \pmod{n_I},$$

then the trusted center will tell us that it is just the $signer_I$ who has signed the signature. Therefore, the trusted center is able to revoke the anonymity of any signer from the undeniable signature scheme.

Theorem 5 *The new undeniable signature scheme has the fair anonymity property.*

Proof By Lemma 3 and Lemma 4, we achieved the correctness of the theorem.

V. Performance Analysis

The performance of our scheme is dominated by the calculations of exponentiation mod n operations as well as the Cramer-Shoup encryption/decryption of keys. Suppose that the times for performing multiplication and addition mod n operations could be ignored, then total computation cost of key generation and signing algorithm for each signer requires O(k3) exponentiation mod n operations.

For the next steps, we will implement our scheme by JAVA or C.

VI. Conclusions

In this paper, we presented a new model for the undeniable signature scheme, i.e. the fair anonymous undeniable signature scheme. Our work mainly focuses on how to realize the fair anonymity (when it is needed) under the condition of preserving the anonymity of the signers. At the same time, we proved the new undeniable signature scheme has the undeniability property.

Acknowledgment

The first author thanks Sonya Carter (who is with the Curtin Business School, Curtin University of Technology) for the helpful comments and discussion on this paper. The authors thank the anonymous referees for helpful comments about this work. The first author gives thanks to the director at CEEBI for the invaluable help and support.

References

[1] M. Bellare and P. Rogaway, "*The exact security of digital signature*{how *to sign with RSA and Rabin}*, " EUROCRYPT 1996, LNCS 1070, Springer, pp. 399-416, 1996.

[2] J. Boyar, D. Chaum, I. Damgard and T. Pedersen, "*Convertible undeniable signatures*," Advances in Cryptology - Crypto '90, LNCS 537, pp. 189-205, Springer, 1990.

[3] C. Boyd and E. Foo, "Off-line fair payment protocols using convertible signatures," in K. Ohta et al (eds.), ASIACRYPT '98, Springer LNCS 1514 (1998) 271-285.

[4] D. Chaum, and Hans van Antwerpen, "*Undeniable signatures*," CRYPTO 1989, LNCS 435, Springer, pp. 212-216, 1990.

[5] D. Chaum, "*Zero-knowledge undeniable signatures*," EUROCRYPT 1990, LNCS 473, Springer, pp. 458-464, 1991.

[6] R. Cramer and V. Shoup, "A *practical public key cryptosystem provably secure against adaptive chosen ciphertext attack*," CRYPTO 1998, LNCS 1462, Springer, 13-25, 1998.

[7] I. Damgard and T. P. Pedersen, "*New convertible undeniable signature scheme*," EUROCRYPT 1996, LNCS 1070, Springer, pp. 372-386, 1996.

[8] S. D. Galbraith and W. Mao. "*Invisibility and anonymity of undeniable and confirmer signatures*," In: *CT-RSA 2003*, LNCS 2612, pp. 80–97. Springer-Verlag, 2003.

[9] S. D. Galbraith, Wenbo Mao, and Kenneth G. Paterson, "*RSA-based undeniable signatures for general moduli*," CT-RSA 2002. LNCS 2271, Springer, pp. 200-217, 2002.

[10] R. Gennaro, H. Krawczyk and Tal Rabin, "*RSA-based undeniable signatures*," Journal of Cryptology (2000) 13: 397-416.

[11] S. Han, K.Y. Yeung and J. Wang, *"Identity based confirmer signatures from pairings over elliptic curves*," Proceedings of ACM conference on Electronic commerce, pp. 262-263, 2003.

[12] S. S. M. Chow, L. C. K. Hui, S. M. Yiu, K. P. Chow, "*A secure modified id-based undeniable signature scheme based on Han et al.'s scheme against Zhang et al.'s attacks*," Cryptology ePrint Archive, Report 2003/262.

[13] L. Jongkook, R. Shiryong, K. Jeungseop and Y. Keeyoung, "*A new undeniable signature scheme using smart cards*," IMA 2001. LNCS 2260, Springer, 387-394, 2001.

[14] M. Jakobsson, K. Sako and R. Impagliazzo, "Designated verifier proofs and their applications," in U. Maurer (ed.) EUROCRYPT '96, Springer LNCS 1070 (1996) pp. 143–154.

[15] B. Libert and Jean-Jacques Quisquater. "*Identity based undeniable signatures*," In: *Topics in Cryptology - CT-RSA 2004*, LNCS 2964, pp. 112-125. Springer-Verlag, 2004.

[16] W. Mao, "*Modern* c*ryptography: theory and practice,*" Prentice-Hall, PTR, USA, ISBN 0-13-066943-1, 2004.

[17] Jean Monnerat and S. Vaudenay, "*Undeniable signatures based on characters: how to sign with one bit*," Advances in Cryptology PKC'04, Singapore, Lecture Notes in Computer Science, No. 2947, pp. 69-85, Springer-Verlag, 2004.

[18] Winson K. Y. Yeung and S. Han, "*Revocable anonymity of undeniable signature schem*." Intelligent Data Engineering and Automated, Learning, IDEAL 2003, Lecture Notes in Computer Science, 2690, Springer.

