Efficient ID-Based Non-Malleable Trapdoor Commitments Based on RSA and Factoring

Chunhui Wu[1], Qin Li[2], and Dongyang Long[3]
[1] Department of Computer Science, Guangdong University of Finance, Guangzhou 510521, P.R.China
[2] College of Information Engineering, Xiangtan University, Xiangtan 411105, P.R.China
[3] Department of Computer Science, Sun Yat-sen University, Guangzhou 510275, P.R.China
Email: {chunhuiwu, liqin805}@163.com; issldy@mail.sysu.edu.cn

Abstract—Non-malleability is an important property in commitment schemes. It can resist to the person-in-the-middle (PIM) attacks within the interaction. In this paper, we focus on the non-malleability in ID-based trapdoor commitments. We first give two constructions of (full) ID-based trapdoor commitment schemes based on RSA and Factoring assumptions respectively and then extend them to non-malleable schemes. The formal proofs show that our proposed schemes satisfy all the desired security properties.

Index Terms—Trapdoor commitment, ID-based, non-malleable

I. Introduction

Commitment is an important cryptographic primitive, it provides two basic properties as hiding and binding. A commitment scheme is an interactive protocol between two parties, the sender *S* who holds a message, and the receiver *R*. It can be divided into two phases as commitment phase and opening phase. In the commitment phase, the sender gives some jumbled information about the message to the receiver such that, on one hand, even a malicious receiver $\mathcal{R}^*$ cannot gain any information about the message (hiding), and on the other hand, a malicious sender $\mathcal{S}^*$ cannot ambiguously open a commitment given to *R* (binding). In the opening phase, the sender transmit the original message and some evidence that the commitment really jumbles this message. Due to the computation power of the adversary, these two properties can either be perfect (statistical) or computational. But a scheme cannot be perfect (statistical) hiding and perfect (statistical) binding at the same time [1], so we mainly have two types of commitment schemes, one type is perfect (statistical) hiding and another type is perfect (statistical) binding, with the other property only computational. A scheme is perfect (statistical) hiding and computational binding if the distribution of the commitments of any message are identical (statistical close) for any arbitrary powerful malicious $\mathcal{R}^*$, and opening a valid commitment ambiguously contradicts the hardness of some cryptographic assumption. A scheme is perfect (statistical) binding and computational hiding if a valid commitment can be opened ambiguously with probability zero (negligible) for any arbitrary powerful malicious $\mathcal{S}^*$, and two commitments are computationally indistinguishable for any probably polynomial time (PPT) malicious $\mathcal{R}^*$.

Trapdoor commitment is a commitment scheme with special properties, that is, one with the trapdoor key can open his commitment in different ways. Trapdoor commitment is also called equivocable commitment or chameleon commitment. It has many applications in modern cryptography. One important application is in constructing zero-knowledge proof [2], [3]. Additionally, trapdoor commitments play an important role for the construction of secure signature schemes. They have been helpful in the design of secure signature schemes without relying on the strong random oracle assumption [4]. Also, they turn out to be quite useful for the construction of chameleon signatures [5] and on-line/off-line signatures [6]. Further applications of trapdoor commitment include design of universally composable commitment schemes [7], [8], which can be securely composed with other secure protocols, and schemes in E-commerce, such as receiptfree voting and auction schemes [9], [10], where receiptfreeness can be achieved by changing the committed value using the trapdoor.

Shamir [11] firstly introduced the notion of ID-based cryptosystem, where a trusted authority, called the private key generation center (PKG), is responsible for the generation of private key after user authentication. Private key generation, also known as Extract( ) algorithm, applies the PKG's master secret key MSK to the user's identity. For security, the adversary is allowed to query the Extract( ) oracle polynomial many times on inputting id_i, and obtain the corresponding secret keys sk_{id_i}, while keeping *MSK* secret. But in some previous definitions and schemes of ID-based trapdoor commitment [1], the public parameters are generated w.r.t. a specific identity, where compromising of two users exposes the *MSK* and breaks the binding property for other users. So it cannot satisfy the requirement of ID-

Manuscript received January 26, 2015; revised May 13, 2015.
This work is supported by Foundation for Distinguished Young Talents in Higher Education of Guangdong, China (No. LYM11093), Start-up Research Funds of Guangdong University of Finance (No. 2012RCYJ012), and National Natural Science Foundation of China (No. 61202398).
Corresponding author email: chunhuiwu@163.com.
doi:10.12720/jcm.10.5.330-338

based cryptosystem and we call them partial ID-based trapdoor commitment [12].

The concept of non-malleability has been introduced by Dolev *et al*. [13]. They present a non-malleable public-key encryption scheme (based on any trapdoor permutation) and a non-malleable commitment scheme with logarithmically many rounds based on any one-way function. Yet, their solutions involve cumbersome non-interactive and interactive zero-knowledge proofs, respectively. Di Crescenzo *et al*. [14] present a non-interactive and nonmalleable commitment scheme based on any one-way function in the common random string model. Though being non-interactive, their system is rather theoretical as it excessively applies an ordinary commitment scheme to non-malleably commit to a single bit. Fischlin *et al*. [15] present efficient interactive non-malleable commitment schemes based on standard assumptions, such as Discrete- Logarithm (DL) and RSA assumptions, in the common reference string model. Wu *et al*. [12] firstly propose two ID-based non-malleable trapdoor commitment schemes based on DL system with/without random oracles respectively, while no efficient schemes based on RSA and Factoring are constructed.

Our Contribution. In this paper, we focus on the nonmalleability in ID-based trapdoor commitment based on RSA and Factoring. We first give two concrete constructions of (full) ID-based trapdoor commitment based on RSA and Factoring assumption respectively, and extend them to non-malleable commitments. The formal proofs show that our proposed schemes satisfy all the desired security properties.

Organization. The rest of the paper is organized as follows: Some definitions and analysis of different notions of non-malleability are given in Section II. The proposed ID-based non-malleable trapdoor commitment based on RSA and its security proofs are given in Section III. Another scheme based on Factoring is given in Section IV. Finally, conclusions are made in Section V.

II. Preliminaries

In this section, we first introduce the notion of (full) IDbased trapdoor commitment compared to the partial IDbased trapdoor commitment, then discuss the relationship between different definitions of non-malleable commitments.

A. Full ID-Based Trapdoor Commitment

Wu *et al*. [12] pointed out the weaknesses in the definition of *partial* ID-based trapdoor commitment proposed by Fischlin [1]. The partial ID-based trapdoor commitment cannot simulate the Extract( ) oracle required in ID-based cryptosystem, and an adversary can get the master secret key by corrupting several identities and break the binding property of other identities. We briefly review Fischlin's DL-based scheme and give an analysis as follows.

Let $\mathbb{G}$ be a group with a prime order q and $g_1, g_2, g_3 \in \mathbb{G}$ be three generators of $\mathbb{G}$. To commit to a message $m \in \mathbb{Z}_q$ with $id \in \mathbb{Z}_q$, the sender picks $r \in_R \mathbb{Z}_q$, computes and sends

$$C = (g_1^{id} g_2)^m g_3^r$$

to the receiver. To setup the ID-based trapdoor, the simulator chooses $\mathbb{G}$ and g_1, g_3 at random. Given the specific identity $id_0 \in \mathbb{Z}_q$ the simulator selects $x \in_R \mathbb{Z}_q$ and computes g_2 as $g_2 = g_1^{-id_0} g_3^x$. With the trapdoor key $x = \log_{g_3}(g_1^{id_0} g_2)$, the commitment with id_0 can be opened to any message m':

$$r' = r + x(m - m') \mod q$$

while it is still binding for $C = (g_1^{id} g_2)^m g_3^r$, $id \neq id_0$.

We now show that if adversary gets two trapdoor keys w.r.t. id_1 and id_2 then he can compute the trapdoor w.r.t. id_3. Denote the trapdoor key w.r.t. id_i as $x_i = \log_{g_3}(g_1^{id_i} g_2)$. We divide the two equations

$$g_1^{id_1} g_2 = g_3^{x_1}$$
$$g_1^{id_2} g_2 = g_3^{x_2}$$

and get $g_1^{id_1 - id_2} = g_3^{x_1 - x_2}$, so we can compute the discrete logarithm of g_3 w.r.t. g_1 as

$$k_3 = \log_{g_1} g_3 = (id_1 - id_2)(x_1 - x_2)^{-1}$$

Then by $g_1^{id_1} g_2 = g_3^{x_1} = g_1^{k_3 x_1}$, we can compute the discrete logarithm of g_2 w.r.t. g_1 as

$$k_2 = \log_{g_1} g_2 = k_3 x_1 - id_1$$

In summary, we get master secret key (k_2, k_3), and the trapdoor for any other identity id_3 can be computed as

$$x_3 = \log_{g_3}(g_1^{id_3} g_2) = (id_3 + k_2) k_3^{-1}$$

which break the binding property of other identities.

Based on the first definition of (full) ID-based trapdoor commitment proposed by Canetti *et al*. [7], Wu *et al*. [12] gave another formal definition in the interactive settings where perfect (statistical) and computational simulative are defined. It is more suitable for the discussion of non-malleability. The notion follows the zero-knowledge approach: there is a simulator whose description of the commitment is indistinguishable from executions with honest parties, yet this simulator is also able to output additional ID-based trapdoor which enables to open the commitment for any messages. We omit the formal definition here, please refer to [12] for the details.

B. On Definitions of Non-Malleable Commitment

The notion of non-malleability can be divided into non-malleable w.r.t. commitment and non-malleable w.r.t. opening. According to the definition of Di Crescenzo *et al*. [14], a scheme is non-malleable w.r.t. opening if the adversary cannot construct a commitment from a given

one, such that after having seen the opening of the original commitment, the adversary is able to correctly open his commitment with a related message. But the definition of Dolev *et al*. [13] demands more: if there is a one-to-one correspondence between the commitment and the message (say, if the commitment binds unconditionally), then they define that such a scheme is non-malleable if one cannot even generate a commitment of a related message. We call such schemes non-malleable w.r.t. commitment. For these schemes to contradict non-malleability it only suffices to come up with a commitment such that there exists a related opening. From an intuitive view, non-malleable w.r.t. commitment is a stronger notion than non-malleable w.r.t. opening, i.e., a scheme non-malleable w.r.t. commitment is non-malleable w.r.t. opening (it is infeasible to generate a commitment, not to say open it), but we cannot give a proof for this, even for perfectly binding commitments; but in the other way, it is proved that non-malleable w.r.t. opening cannot imply non-malleable w.r.t. commitment. Fischlin [1] gives such a example, which satisfies non-malleable w.r.t. opening but is not non-malleable w.r.t. commitment. In the meantime, they give another definition of non-malleability, which we call strong non-malleable w.r.t. commitment, and it can imply both non-malleable w.r.t. commitment and w.r.t. opening.

The definition on non-malleable commitments follows the well-known idea of defining secure encryption, namely, we will demand that for any adversary $\mathcal{A}$ transforming the sender's commitment successfully, there should be an adversary $\mathcal{A}'$ that sends a commitment to a related message with almost the same probability as $\mathcal{A}$ but without the sender's help.

We follow the notations of [1] and describe the attack in details. First, the public parameters PubPar are generated by a trusted party according to a publicly known, efficiently samplable distribution. On input PubPar the adversary $\mathcal{A}$ then picks the adversarial parameters AdvPar for the message space *M* and relation *R*. The sender *S* is initialized with $m \in_R \mathsf{M}(\mathrm{AdvPar})$. Now $\mathcal{A}$, given some prior information $\mathsf{Hist}(m)$, mounts a PIM (person-in-themiddle) attack with $\mathcal{S}(m)$ and *R*. Let $\pi_{\mathsf{com}}(\mathcal{A}, \mathsf{M}, \mathcal{R})$ denote the probability that, at the end of the commitment phase, the protocol execution between $\mathcal{A}$ and *R* constitutes a valid commitment for some message m^* satisfying $\mathsf{R}(\mathrm{AdvPar}, \mathsf{Hist}(m), m, m^*)$. Let $\pi_{\mathsf{open}}(\mathcal{A}, \mathsf{M}, \mathcal{R})$ denote the probability that $\mathcal{A}$ is also able to successfully open the commitment after *S* has decommitted.

In a second experiment, a simulator $\mathcal{A}'$ tries to commit to a related message without the help of the sender. That is, $\mathcal{A}'$ gets as input random public parameters PubPar, generates adversarial parameters AdvPar' and then, given $\mathsf{Hist}(m)$ for some $(m, \mathsf{Hist}(m)) \in_R \mathsf{M}(\mathrm{AdvPar}')$, it commits to *R* without interacting with $\mathcal{S}(m)$. Let $\pi'_{\mathsf{com}}(\mathcal{A}', \mathsf{M}, \mathcal{R})$ denote the probability that this is a valid commitment to some related message m' under public parameters PubPar w.r.t. relation $\mathsf{R}(\mathrm{AdvPar}', \mathsf{Hist}(m), \cdot, \cdot)$. By $\pi'_{\mathsf{com}}(\mathcal{A}', \mathsf{M}, \mathcal{R})$ we denote the probability that $\mathcal{A}'$ simply outputs a related message (without reference to public parameters, commitment and decommitment).

Definition 1: A commitment scheme is called

1) S*trong non-malleable w.r.t. commitment* if for every adversary $\mathcal{A}$ there exists a simulator $\mathcal{A}'$ s.t. for anymessage space *M* and any interesting relation *R* the difference $\pi_{com}(\mathcal{A}, \mathsf{M}, \mathcal{R}) - \pi'_{open}(\mathcal{A}', \mathsf{M}, \mathcal{R})$ is negligible.
2) *Non-malleable w.r.t. commitment* if for every adversary $\mathcal{A}$ there exists a simulator $\mathcal{A}'$ s.t. for any message space *M* and any interesting relation *R* the difference $\pi_{com}(\mathcal{A}, \mathsf{M}, \mathcal{R}) - \pi'_{com}(\mathcal{A}', \mathsf{M}, \mathcal{R})$ is negligible.
3) *Non-malleable w.r.t. opening* if for every adversary $\mathcal{A}$ there exists a simulator $\mathcal{A}'$ s.t. for any message space *M* and any interesting relation *R* the difference $\pi_{open}(\mathcal{A}, \mathsf{M}, \mathcal{R}) - \pi'_{open}(\mathcal{A}', \mathsf{M}, \mathcal{R})$ is negligible.

By defining strong non-malleable w.r.t. commitment, we can show that $1) \Rightarrow 2)$ and $1) \Rightarrow 3)$. Since $\pi'_{com}(\mathcal{A}', \mathsf{M}, \mathcal{R}) > \pi'_{open}(\mathcal{A}', \mathsf{M}, \mathcal{R})$ by their definitions, we have

$$\pi_{com}(\mathcal{A}, \mathsf{M}, \mathcal{R}) - \pi'_{open}(\mathcal{A}', \mathsf{M}, \mathcal{R}) > \pi_{com}(\mathcal{A}, \mathsf{M}, \mathcal{R}) - \pi'_{com}(\mathcal{A}', \mathsf{M}, \mathcal{R})$$

the former is negligible so is the latter and $1) \Rightarrow 2)$.

In the same way, $\pi_{com}(\mathcal{A}, \mathsf{M}, \mathcal{R}) > \pi_{open}(\mathcal{A}, \mathsf{M}, \mathcal{R})$, so

$$\pi_{com}(\mathcal{A}, \mathsf{M}, \mathcal{R}) - \pi'_{open}(\mathcal{A}', \mathsf{M}, \mathcal{R}) > \pi_{open}(\mathcal{A}, \mathsf{M}, \mathcal{R}) - \pi'_{open}(\mathcal{A}', \mathsf{M}, \mathcal{R})$$

and $1) \Rightarrow 3)$. The notions of $2)$ and $3)$ are not equal, Fischlin [1] gives an example showing that $3) \not\Rightarrow 2)$; but otherwise, the relation is not sure.

For perfect (statistic) hiding commitment schemes, it is proper to consider non-malleability w.r.t. opening. Since for these schemes, any commitment can be openable with any message, and an arbitrary chosen commitment can have related decommitments, which *trivially* breaks nonmalleability w.r.t. commitment, but we do not consider this as truly breaking non-malleability.

Another notion closely related to non-malleability is simulation-soundness, refer to [16] for the detailed analysis of their relations. Recently, linearly homomorphic *structure-preserving* signatures[1] [17] are used to construct simulation-sound trapdoor commitments to group elements [18].

[1]A signature scheme is structure-preserving if messages, signature components and public keys live in the bilinear group $\mathbb{G}$

III. ID-Based Non-Malleable Trapdoor Commitment Based on RSA

In this section, we first introduce an efficient (full) ID-based trapdoor commitment scheme based on RSA assumption in the random oracle model, following the idea of key-exposure free chameleon hash [19], then extend it to non-malleable commitment and prove its security.

A. Full ID-Based Trapdoor Commitment Based on RSA

Let $N = pq$ be an *n*-bit RSA modulus and $e \geq 2^{n+1}$ be a random prime integer; by this choice, the exponent *e* is relatively prime to $\varphi(N) < 2^{n+1}$ and this fact is publicly verifiable without knowledge of the factorization of *N*. The secret key *d* is computed such that $ed = 1 \bmod \varphi(N)$. Let $H : \{0,1\}^* \rightarrow \mathbb{Z}_N^*$ be a full-domain collision resistant hash function. The public key is (N, e) and the secret key is (p, q, d).

In commitment phase, the sender chooses $r \in_R \mathbb{Z}_N^*$ randomly, and computes the commitment for message $m \in \mathbb{Z}_e$ under identity *id*:

$$M = G^m r^e \mod N$$

where $G = H(id)$.

In opening phase, the sender outputs the opening (*m*, *r*) of commitment *M*. The receiver checks

$$G^m r^e \stackrel{?}{=} M$$

outputs accept if the equation satisfied.

The trapdoor for *id* can be extracted as $TK_{id} = G^d$, where $G = H(id)$. With this trapdoor, a commitment $M = G^m r^e$ can be opened to any message m' for *id* by computing

$$r' = rG^{d(m-m')}$$

Note that

$$Com(id, m', r') = G^{m'} r'^e = G^{m'} (rG^{d(m-m')})^e = G^m r^e$$

Theorem 1: The ID-based trapdoor commitment scheme described above is perfectly simulative and computationally binding under RSA assumption in random oracle model.

Proof 1: The scheme is perfectly simulative. The simulator can generate the public parameters as described above, and a commitment $M = G^m r^e$ can be opened to any message m' under identity *id* with the trapdoor $TK_{id} = G^d$ by computing r'. Moreover, if *r* distributes randomly then also r'. So the simulator's behavior is identical to the one of the honest parties.

The scheme is computationally binding. Assume there is a PPT adversary $\mathcal{A}$ that breaks the binding property with non-negligible probability. Then we get a pair of collision (*m*, *r*) and (m', r') for the target identity id_t, i.e.

$$\mathsf{Com}(id_t, m, r) = \mathsf{Com}(id_t, m', r')$$

that is

$$G_t^m r^e = G_t^{m'} r'^e$$

then

$$G_t^{m-m'} = (r'/r)^e$$

where $G_t = H(id_t)$ and *H* is treated as random oracle. Since $m \in \mathbb{Z}_e$, it follows that $gcd(m - m', e) = 1$. Using the extended Euclidean algorithm, one computes α and β s.t.

$$\alpha(m - m') + \beta e = 1$$

So

$$G_t = G_t^{\alpha(m-m')+\beta e} = ((r'/r)^\alpha G_t^\beta)^e$$

and the RSA signature on message id_t can now be extracted as

$$G_t^d = (r'/r)^\alpha G_t^\beta$$

this contradicts the fact that RSA signature is existential unforgeable under adaptive chosen message attack (UFACMA) in random oracle model. In the mean time, $\mathcal{A}$ is allowed to query Extract( ) oracle polynomial many times and gets the RSA signatures G_i^d on id_i, where $id_i \neq id_t,\ i = 1, 2, \cdots, q(n)$. We can simulate the Extract( ) oracle as simulating RSA signature. To sum up, the scheme is computationally binding under RSA assumption in random oracle model.

Unfortunately, non-malleable is not achieved by commitment schemes in general, because ordinary schemes are only designated to hide the secret. Even worse, most known commitment schemes are in fact provably malleable. The above scheme is malleability w.r.t. opening because the adversary can change the commitment $M = G^m r^e \mod N$ to $M^* = GM$, and open M^* to $m + 1$ after the sender opens *M* to *m*.

B. The Proposed ID-Based Non-Malleable Trapdoor Commitment

In this section, we extend the scheme in Section IIIA to a non-malleable scheme. The main idea to achieve non-malleability is to add a three round efficient zeroknowledge proof after committing to a message using the malleable ID-based trapdoor commitment. The zeroknowledge proof ensures that the adversary knows a related message, which contradict the hiding property of the original scheme. However, if using zero-knowledge proof directly, the scheme is still malleable because the zero-knowledge proof may be malleable itself. The coin flipping protocol comes to rescue. We let the challenge in the zero-knowledge proof be determined by such a coinflipping protocol. The ideas come from [15], and similar as [13]. Our scheme is described in Fig. 1.

Theorem 2: The scheme in Fig. 1 is perfectly hiding and computationally binding under RSA assumption in

random oracle model.

Proof 2: For the proof of binding property, please refer to Theorem 1. In the mean time, the scheme is perfectly hiding, because the additional proof of knowledge for m is witness independent (aka. perfect witness indistinguishable), i.e., for any challenge *c* the transmitted values *S*, *v*, *w* are distributed independently of the actual message.

Theorem 3: The scheme in Fig.1 is non-malleable w.r.t. opening under RSA assumption.

A rough idea why our scheme is non-malleable can be described as follows. Given a commitment *M* of some unknown message *m* (together with a witness independent proof of knowledge described by *S*, *c*, *v*, *w*) w.r.t. parameters *N*, *e*, *g*, we show how to employ the PIM adversary $\mathcal{A}$ to derive some information about *m*. Namely, if we are able to learn the related message m^* of the adversary by extracting it via his "self-employed" proof of knowledge, then we know that *m* is related to m^* for the relation R. This, of course, contradicts the perfect secrecy of the commitment *M*. We remark that the formal proof of non-malleability requires to come up with a simulator generating a related message without the help of the sender. However, as we will show, the essential part of the simulator is made out of such an extraction procedure.

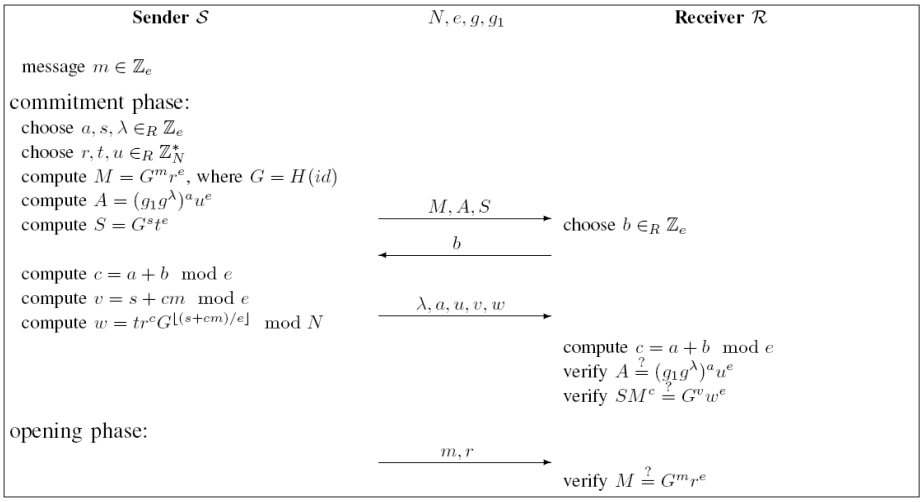


Fig. 1. ID-based Non-malleable trapdoor commitment scheme based on RSA.

Follow the proof of [15], we first construct the extraction algorithm w.r.t. restricted attacks, and then w.r.t. fullfledged attacks. Finally, we discuss that the required nonmalleability simulator can be derived from the extraction procedure.

1) Outline of the extraction procedure

We make some simplifications of the adversary: first, we assume that the PIM adversary always catches up concerning the order of the transmissions, i.e., sends his first message after learning the first message of *S* and answers to *S* after having seen *R*'s response etc. Second, let the adversary always successfully commit and decommit to a related message, rather than with small probability. Third, we presume that the target identity id_t is given beforehand instead of choosing adaptively, similar to the "selective-ID assumption" in ID-based cryptsystems. The first and second restriction will be removed in the following passages, while removing the third restriction is a challenge.

To learn the adversary's message m^* we use the proof of knowledge in our commitment protocol. Intuitively, a proof of knowledge guarantees that the prover knows the message, i.e., one can extract the message by running experiments with the prover. For the setting of parameters please refer to Fig. 2 of a pictorial description of the experiments.

We play the rest of the commitment phase twice by rewinding it to the step where the receiver chooses *b* and sends it to the adversary $\mathcal{A}$ To distinguish the values in both repetitions we add the number of the loop as subscript and write a_1, a_1^*, a_2, a_2^* etc.

In the first time, the adversary upon receiving b_1 passes some b_1^* to the (simulated) sender *S*, and expects *S* to open the commitment for a_1 and supplement the proof of knowledge for *M* w.r.t. the challenge $(a_1 + b_1^*)$ mod *e*. We choose a_1 s.t. $(a_1 + b_1^*)$ mod e equals the given value *c*. Hence, *v* and *w* are proper values to complement the proof of knowledge for *M*. We can open *A* with a_1 by the trapdoor property of the commitment scheme since we know $(g_1 g^\lambda)^{1/e} = X$ Finally, the adversary answers with the decommitment a_1^*, u_1^* for A^* and the rest of the proof of knowledge for M^* w.r.t. challenge $(a_1^* + b_1)$ mod *e*.

Now we rewind the execution and select another random challenge b_2. The adversary then decides upon his value b_2^* (possibly different from his previous choice b_1^* and hands it to *S*. Again, we open *A* with a_2 such that $c = (a_2 + b_2^*)$ mod *e*. The adversary finishes his commitment with a_2^*, u_2^* as opening for A^* and the missing values for the proof of knowledge.

The fundamental proof of knowledge paradigm [20] says that we can extract the message m^* if we learn two valid executions between $\mathcal{A}$ and *R* with the same commitment M^*, A^*, S^* but different challenges. Hence, if the adversary's decommitments satisfy $a_1^* = a_2^*$ and we have $b_1 \neq b_2$ (which happens with probability $1 - 1/e$), then this yields different challenges $a_1^* + b_1$, $a_2^* + b_2$ in the executions between $\mathcal{A}$ and *R* and we get to know the message m^*. We are therefore interested in the event that the adversary is able to "cheat" by presenting different openings $a_1^* \neq a_2^*$. We prove that the adversary cannot find different openings for commitment A^* too often, else we would derive a contradiction to the intractability of the RSA problem. Hence, under the RSA assumption this event hardly occurs and we extract m^* with sufficiently high probability.

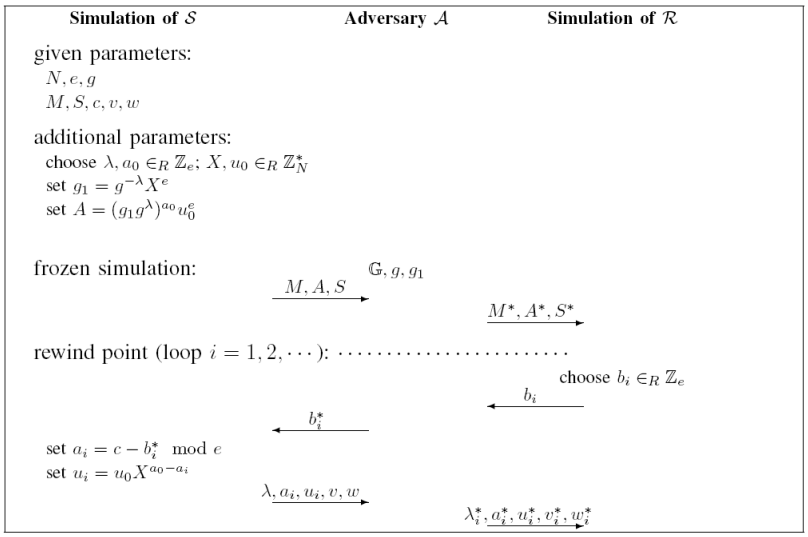


Fig. 2. Knowledge extraction.

2) Extraction w.r.t. restricted attacks

In the restricted attacks, first, we too adopt the convention that the adversary $\mathcal{A}$ does not "mix" the order of messages but rather catches up. Second, we also presume that the target id_t is given beforehand instead of choosing adaptively.

An important modification of the knowledge extractor in comparison to the one in [20] is that, once having entered the loop phase, not only does our extractor stop in case of success; it also aborts with no output if in some repetitions *i*, *j* the adversary both times opens A^* with distinct values $a_i^* \neq a_j^*$. We say that $\mathcal{A}$ wins if this happens. In this case, the extractor fails to extract a message.

To analyze the success probability of our extractor let π denote the probability of $\mathcal{A}$ completing the commitment phase with *R* successfully. The basic extraction paradigm says that we are able to extract with probability $\pi - 1/e - \epsilon(n)$, where $\epsilon(n)$ denotes the probability that $\mathcal{A}$ wins (*n* is the security parameter).

We would like to prove that we extract with probability approximately to the adversary's success probability $\pi_{open}(\mathcal{A})$. We first prove that $\epsilon(n)$ roughly equals $\pi - \pi_{open}(\mathcal{A})$, or put differently, that $\delta(n) = \epsilon(n) - (\pi - \pi_{open}(\mathcal{A}))$ is negligible. One may think of the difference $\pi - \pi_{open}(\mathcal{A})$ describing the probability of executions in which $\mathcal{A}$ successfully commits but never finds a related, valid opening. Thus, the extractor succeed with probability $\pi - 1/e - \epsilon(n) = \pi_{open}(\mathcal{A}) - 1/e - \delta(n)$.

The following lemma shows that $\delta(n)$ is negligible under RSA assumption.

Lemma 1: $\delta(n) = \epsilon(n) - (\pi - \pi_{open}(\mathcal{A}))$ is negligible under RSA assumption.

Proof 3: Assume that $\delta(n)$ is noticeable, then the probability of $\mathcal{A}$ wins $\epsilon(n) = \delta(n) + (\pi - \pi_{open}(\mathcal{A}))$ is also noticeable. We show how to use $\mathcal{A}$ to solve RSA problem, that is, given $g_0 \in_R \mathbb{Z}_N^*$, we can compute $g_0^{1/e}$.

Randomly choose $\lambda \in_R \mathbb{Z}_e$ and $X \in_R \mathbb{Z}_N^*$, we set the parameters as follows:

$$g = g_0, g_1 = g^{-\lambda} X^e$$

Since $g_1 g^\lambda = g^{-\lambda} X^e g^\lambda = X^e$, we have $(g_1 g^\lambda)^{1/e} = X$, and we can open the commitment *A* to proper values such that the coin flipping protocol always yields the same challenge *c* in the rewinding phase.

Next we emulate $\mathcal{A}$ on values $\mathbb{Z}_N^*, e, g, g_1$ and *M*, *A*, *S* by running the extraction procedure above.

Given that $\mathcal{A}$ wins with probability $\epsilon(n) = \delta(n) + (\pi - \pi_{open}(\mathcal{A}))$, i.e., $\mathcal{A}$ finds some $a_i^* \neq a_j^*$ for two accepting executions *i*, *j* with noticeable probability. We have:

$$(g_1 g^{\lambda_i^*})^{a_i^*} u_i^{*e} = A^* = (g_1 g^{\lambda_j^*})^{a_j^*} u_j^{*e}$$

and therefore

$$(u_i^*/u_j^*)^e = (g_1 g^{\lambda_j^*})^{a_j^*}/(g_1 g^{\lambda_i^*})^{a_i^*}$$

Since $g = g_0, g_1 = g^{-\lambda}X^e$ we can transform this into

$$(u_i^*/u_j^* \cdot X^{a_i^*-a_j^*})^e = g^{(\lambda_j^*-\lambda)a_j^*-(\lambda_i^*-\lambda)a_i^*}$$

So we solve the RSA problem $g_0^{1/e}$.

In summary, with probability $\pi_{open}(\mathcal{A}) - 1/e - \delta(n)$ (which is negligibly close to the adversary's success probability $\pi_{open}(\mathcal{A})$) we extract some message m'. The final step is to show that indeed m' equals the adversary's decommitment m^* except with negligible probability (or, more precisely, that m' is at least an appropriate substitution for m^* insofar as it also satisfies *R* often enough). Denote by $\pi_{open}(\varepsilon)$ the probability that the extraction procedure returns m' that is related to *m* under *R*.

Lemma 2: The probabilities $\pi_{open}(\varepsilon)$ and $\pi_{open}(\mathcal{A}) - 1/e - \delta(n)$ are negligible close under RSA assumption in random oracle model, i.e., the probability that the extraction procedure returns m' s.t. $\mathsf{R}(m, m')$ is negligible close to the adversary's success probability $\pi_{open}(\mathcal{A})$.

Proof 4: If this were not the case we could solve the RSA problem, i.e., given $G_0 \in \mathbb{Z}_N^*$, we could compute $G_0^{1/e}$.

Set $G = G_0$ for the target identity id_t[2], randomly choose $m \in_R \mathbb{Z}_e$, $r \in_R \mathbb{Z}_N^*$, set $M = G^m r^e$; randomly choose $X \in_R \mathbb{Z}_N^*$, $\lambda \in_R \mathbb{Z}_e$, set $g_1 = g^{-\lambda}X^e$. Run the extraction procedure.

Suppose that $\pi_{open}(\mathcal{A}) - 1/e - \delta(n)$ and $\pi_{open}(\varepsilon)$ have noticeable difference, i.e., the message m' extracted with probability $\pi_{open}(\mathcal{A}) - 1/e - \delta(n)$ doesn't satisfy the relation *R*. In particular, since m^*satisfies the relation *R*, we have $m' \neq m^*$, in other words, we have got a pair of collision (m^*, r^*) and (m', r') with noticeable probability. By

$$G^{m^*} r^{*e} = G^{m'} r'^e$$

we get

$$(r^*/r')^e = G^{m'-m^*}$$

and solve the RSA problem $G^{1/e} = G_0^{1/e}$.

3) Extraction w.r.t. full-fledged attacks

We observe that the order of the messages in the PIM attack does not violate any of the discussions above. This is quite easy to see since any message on the sender's side can be predetermined at the outset of the knowledge extraction procedure.

4) Extraction implies non-malleability

Finally, we construct a non-malleable simulator $\mathcal{A}'$ from the extract procedure. $\mathcal{A}'$ prepares the public parameters as required for the extraction procedure. $\mathcal{A}'$ also has to prepare a commitment *M* of *m* together with a proof of knowledge *S*, *c*, *v*, *w*, but without actually knowing the secret message *m* of the sender. We let $\mathcal{A}'$ simply take an arbitrary message $m_0 \in \mathsf{M}$ and compute *M*, *S*, *c*, *v*, *w* from this message m_0 instead. Since the commitment *M* is perfectly secret and *S*, *c*, *v*, *w* are distributed independently of m_0, these values are equivalent to genuine values.

Finally, the simulator $\mathcal{A}'$ outputs the message it extracts from the PIM adversary. The results about the extraction procedure in the previous sections show that the success probability of $\mathcal{A}'$ is at most negligibly smaller than the probability of the PIM adversary. This completes the proof.

IV. ID-Based Non-Malleable Trapdoor Commitment Based on Factoring

Let $N = pq$ be a Blum integer, where *p* and *q* are two random primes such that $p = q = 3 \bmod 4$. Define a cryptographic hash function $H : \{0,1\}^* \to \mathbb{Z}_N^*[+1]$, where $\mathbb{Z}_N^*[+1] = \{a | a \in \mathbb{Z}_N^*, \left(\frac{a}{N}\right) = +1\}$ is the set of elements of $\mathbb{Z}_N^*$ with Jacobi symbol +1. We restrict the considered message space of the commitment to be $\{0,1\}^{f(k)}$ where *k* is the security parameter and *f*(*k*) is super-logarithmic in *k*, i.e., $0 \leq m \leq 2^{f(k)} - 1$. Trivially, the case of the message space of $\{0,1\}^*$ can be easily extended by using a collision-resistant hash function from $\{0,1\}^*$to $\{0,1\}^{f(k)}$. The proposed scheme is described in Fig. 3. The idea comes from the key-exposure free chameleon hash in [21].

Theorem 4: The ID-based trapdoor commitment scheme in Fig. 3 is perfectly hiding, and computationally binding under Factoring assumption in random oracle model.

Proof 5: The commitment scheme in Fig. 3 is perfectly hiding. The simulator can generate the public parameters as described above, and a commitment $M = zG^m r^{2^{f(k)}} \bmod N$ can be opened to any message m' under identity id with the trapdoor $TK_{id} = |G|^{\frac{1}{2^{f(k)}}} \bmod N$, $G = H(id)$, here $|G| = G$ if $G \in QR_N$ (QR_N denotes the group of all quadratic residue modulo *N*); $|G| = -G$ otherwise. Then the corresponding random string can be computed as

$$r' = rTK_{id}^{m-m'} \mod N$$

$$z' = \begin{cases} z, & if\ G \in QR_N \\ z(-1)^{m-m'}, & otherwise \end{cases}$$

One can easily verify that $Com(id, m, r, z) = Com(id, m', r', z')$. In the mean time, the additional proof

[2]We can set $G = G_0$ because we are in random oracle model.

of knowledge for m is witness independent (aka. Perfect witness indistinguishable), i.e., for any challenge *c* the transmitted values *S*, *v*, *w* are distributed independently of the actual message.

The scheme is computationally binding. Assume there is a PPT adversary $\mathcal{A}$ that break the binding property with non-negligible probability. Then we get a pair of collision (m, r) and (m', r') for the target identity id_t, s.t.

$$\mathsf{Com}(id_t, m, r, z) = \mathsf{Com}(id_t, m', r', z')$$

that is

$$zG_t^m r^{2^{f(k)}} = z' G_t^{m'} r'^{2^{f(k)}}$$

where $G_t = H(id_t)$ and *H* is treated as random oracle. It follows that

$$|G_t|^{m-m'} = (r'/r)^{2^{f(k)}}$$

Let

$$2^\gamma = gcd(m - m', 2^{f(k)}), \text{ where } 0 \le \gamma < f(k)$$

Compute $\alpha, \beta \in \mathbb{Z}$ s.t.

$$\alpha(m - m') + \beta 2^{f(k)} = 2^\gamma$$

then

$$|G_t|^{2^\gamma} = |G_t|^{\alpha(m-m')+\beta 2^{f(k)}} = (r'/r)^{\alpha 2^{f(k)}} |G_t|^{\beta 2^{f(k)}} = ((r'/r)^\alpha |G_t|^\beta)^{2^{f(k)}}$$

We can compute

$$|G_t|^{\frac{1}{2}} = ((r'/r)^\alpha |G_t|^\beta)^{2^{f(k)-\gamma-1}}$$

which is a Rabin signature on message id_t, this contradicts the fact that Rabin signature is existential unforgeable under the factoring assumption in random oracle model. In the mean time, $\mathcal{A}$ is allowed to query Extract( ) oracle polynomial many times and gets the Rabin signatures $|G_i|^{\frac{1}{2}}$ on id_i, where $id_i \neq id_t$, $i = 1, 2, \cdots, q(n)$. We can simulate the Extract( ) oracle as simulating Rabin signature. To sum up, the scheme is computationally binding under factoring assumption in random oracle model.

Theorem 5: The ID-based trapdoor commitment scheme in Fig. 3 is non-malleable w.r.t. opening under Factoring assumption.

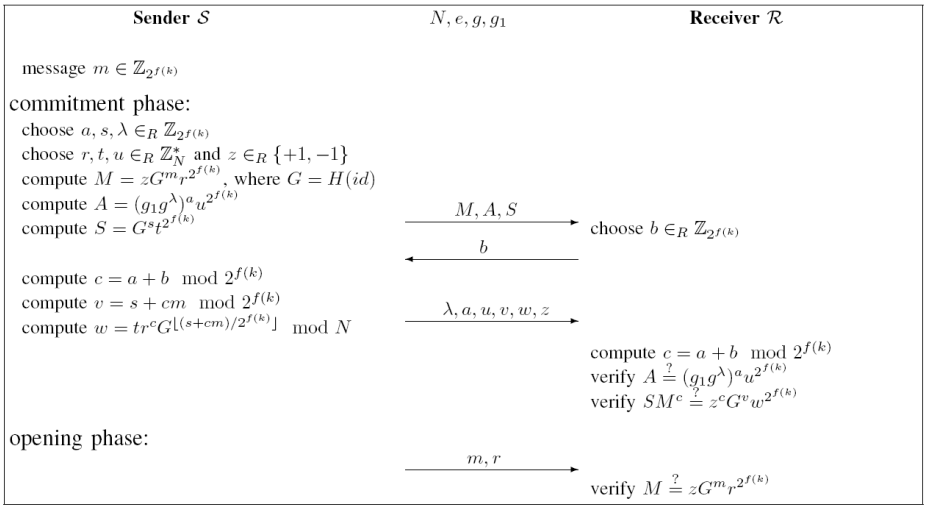


Fig. 3. ID-based Non-malleable trapdoor commitment scheme based on factoring.

Proof 6: The proof is similar to Theorem 3. We omit the detailed proof to avoid the redundance here.

V. Conclusion

In this paper, we focused on the non-malleability in ID-based trapdoor commitment. Wu et al. proposed two efficient ID-based non-malleable trapdoor commitment schemes based on DL system with/without random oracle respectively, while no schemes are known based on RSA and Factoring assumption. We introduced two (full) IDbased trapdoor commitments based on RSA and Factoring assumption respectively, improved the weakness in Fischlin's partial ID-based schemes [1]. We also analysed the different definitions of non-malleable commitment, and extended the two schemes to non-malleable schemes. The formal proofs showed that they satisfy all the desired security properties. The future work is to construct efficient non-malleable schemes in the non-interactive setting and without random oracle.

References

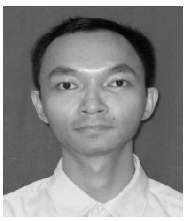
[1] M. Fischlin, "Trapdoor commitment schemes and their applications," Ph.D. Thesis, Johann Wolfgang Goethe-University, 2001.

[2] G. Brassard, D. Chaum, and C. Crepeau, "Minimum disclosure proofs of knowledge," *Journal of Computer and Systems Science*, vol. 37, no. 2, pp. 156–189, 1988.

[3] J. Groth, "Efficient zero-knowledge arguments from two-tiered homomorphic commitments," in *Advances in Cryptology-Asiacrypt 2011*, Springer- Verlag, 2011, vol. 7073, pp. 431–448.

[4] R. Gennaro, S. Halevi, and T. Rabin, "Secure hashand-sign signatures without the random oracle," in *Advances in Cryptology-Eurocrypt'99*, Springer-Verlag, 1999, vol. 1592, pp. 123–139.

[5] X. Chen *et al*., "Discrete logarithm based chameleon hashing and signatures without key exposure," *Computers and Electrical Engineering*, vol. 37, no. 4, pp. 614–623, 2011.
[6] X. Chen *et al*., "Efficient generic on-line/off-line (threshold) signatures without key exposure," *Information Sciences*, vol. 178, no. 21, pp. 4192–4203, 2008.
[7] R. Canetti *et al*., "Universally composable security with global setup," in *TCC 2007*, Springer- Verlag, 2007, vol. 4392, pp. 61–85.
[8] M. Fischlin, B. Libert, and M. Manulis, "Non-interactive and Re-usable universally composable string commitments with adaptive security," in *Advances in Cryptology-Asiacrypto 2011*, Springer-Verlag, 2011, vol. 7073, pp. 468–485.
[9] M. Abe and K. Suzuki, "Receipt-free sealed-bid auction," in *ISC 2002*, Springer-Verlag, 2002, vol. 2433, pp. 191–199.
[10] T. Okamoto, "Receipt-free electronic voting schemes for large scale elections," in *5th Security Protocols*, Springer-Verlag, 1997, vol. 1361, pp. 25–35.
[11] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Advances in Cryptology-Crypto 1984*, Springer-Verlag, 1985, vol. 196, pp. 47–53.
[12] C. Wu *et al*., "Efficient ID-based non-malleable trapdoor commitment," Computers and Electrical Engineering, vol. 38, no. 6, pp. 1647–1657, 2012.
[13] D. Dolev, C. Dwork, and M. Naor, "Non-malleable cryptography," *SIAM Jornal on Computing*, vol. 30, no. 2, pp. 391–437, 2000.
[14] G. D. Crescenzo, Y. Ishai, and R. Ostrovsky, "Non interactive and non-malleable commitment," in *Proc. 30th Annual ACM Symposium on Theory of Computing*, ACM Press, 1998, pp. 141–150.
[15] M. Fischlin and R. Fischlin, "Efficient non-malleable commitment schemes," *Journal of Cryptology*, vol. 22, no. 4, pp. 530–571, 2009.
[16] P. MacKenzie and K. Yang, "On simulation-sound trapdoor commitments," in *Advances in Cryptology EUROCRYPT 2004*, Springer-Verlag, 2004, vol. 3027, pp. 382–400.
[17] M. Abe *et al*., "Constant-size structure-preserving signatures: Generic constructions and simple assumptions," in *Advances in Cryptology-Asiacrypt 2012*, Springer-Verlag, 2012, vol. 7658, pp. 4–24.
[18] B. Libert *et al*., "Linearly homomorphic structure-preserving signatures and their applications," in *Advances in Cryptology-CRYPTO 2013*, Springer-Verlag, 2013, vol. 8043, pp. 289–307.
[19] G. Ateniese and B. de Medeiros, "On the key exposure problem in chameleon hashes," in *SCN 2004*, Springer-Verlag, 2005, vol. 3352, pp. 165–179.
[20] U. Feige and A. Shamir, "Zero-knowledge proofs in two rounds," in *Advances in Cryptology-Crypto 1989*, Springer-Verlag, 1990, vol. 435, pp. 526–544.
[21] X. Chen *et al*., "Comments and Improvements on keyexposure free chameleon hashing based on factoring," in *Inscrypt 2010*, Springer-Verlag, 2011, vol. 6584, pp. 415–426.



Chunhui Wu received his Ph.D. degree in Computer Science from Sun Yat-sen University, Guangzhou, China in 2010. He is a lecturer in the Department of Computer Science, Guangdong University of Finance, China. His research interests include design and analysis of public key cryptography schemes, anonymity and privacy, and financial cryptography.

Qin Li received her Ph.D. degree in Computer Science from Sun Yat-sen University, Guangzhou, China in 2010. She is an associate professor in the College of Information Engineering, Xiangtan University, China. Her research interests include quantum cryptography and classical cryptography.

Dongyang Long is a professor and Ph.D. supervisor in the Department of Computer Science at Sun Yat-sen University, Guangzhou, China. His research interests include information security, quantum information, and network coding