Ring Signatures : Universally Composable Definitions and Constructions

[Extended Abstract]

Kazuki Yoneyama
The University of Electro-Communications
1-5-1 Chofugaoka Chofu-shi
Tokyo, Japan
yoneyama@ice.uec.ac.jp

Kazuo Ohta
The University of Electro-Communications
1-5-1 Chofugaoka Chofu-shi
Tokyo, Japan
ota@ice.uec.ac.jp

ABSTRACT

Though anonymity of ring signature schemes has been studied in many literatures for a long time, these papers showed different definitions and there is no consensus. Recently, Bender et al. proposed two new anonymity definitions of ring signature which is stronger than the traditional definition, that are called anonymity against attribution attacks/full key exposure. Also, ring signature schemes have two levels of unforgeability definitions, i.e., existential unforgeability (eUF) and strong existential unforgeability (sUF). In this paper, we will redefine anonymity and unforgeability definitions from the standpoint of universally composable (UC) security framework. First, we will formulate new ideal functionalities of ring signature schemes for each security levels separately. Next, we will show relations between cryptographic security definitions and our UC definitions. Finally, we will give another proof of the Bender et al.'s ring signature scheme following the UC secure definition by constructing a simulator to an adversary of sUF, which can be adaptable to the case of sUF under the assumption of a standard single sUF signature scheme.

Categories and Subject Descriptors

E.3 [**Data Encryption**]: Public key cryptosystems

General Terms

Security

Keywords

universal composability, ring signature, unforgeability, anonymity

1. INTRODUCTION

Recently, there are several digital signature schemes which require *anonymity* property, i.e., a verifier can be convinced that a signature is valid although he cannot identify the true signer among plural possible signers. The ring signature scheme is a sort of scheme which is suitable for this kind of situation. For any signed message, ring signature schemes hide the true signer of the message among more than one signer candidates. A ring signature is realized by letting the true signer to create the signature by using its own signing key and other member's verification keys who are the members of a group of signer candidates.

The formulation of ring signature in *universal composability* (UC) framework is firstly introduced by Yoneyama et al.[2]. The advantage of UC framework to traditional frameworks is that UC provides strong and robust secure composability, i.e., the security of a primitive (which is UC secure in a stand-alone manner) will always be preserved even when it is executed concurrently with other unbounded number of UC secure primitives in an adversarial controlled manner. They proposed an ideal functionality for the ring signature and proved that a protocol of a ring signature scheme securely realizes the functionality if and only if the scheme satisfies unforgeability and anonymity. However, their result isn't enough since the functionality only captures a kind of unforgeability and anonymity. Furthermore, though the strong cryptographic notion of anonymity is defined by Bender et al.[1], the strong notion in UC framework isn't given in [1]. In this paper, we will propose formulations of the ring signature functionality corresponding to strong cryptographic security notions, and a construction which actually satisfy UC-security.

1.1 Our contribution.

Universally composable definition. Previous definition of UC ring signature[2] only captures sUF and basic anonymity. Also, though stronger definitions of anonymity are studied in [1], they only gave cryptographic definitions, i.e., no UC definitions. In this paper, we formulate definitions of UC ring signature toward various security levels. Precisely, we propose an ideal ring signature functionality $\mathcal{F}_{\mathrm{rSIG}}^{(uf,anon)}$ which is convertible by a level of unforgeability *uf* and a level of anonymity *anon*. We are able to choose eUF or sUF as *uf*, and basic anonymity, anonymity against attribution attacks or anonymity against full key exposure as *anon*. So, our functionality can represent six kinds of security notions by combination of unforgeability and anonymity. This convertibility of $\mathcal{F}_{\mathrm{rSIG}}^{(uf,anon)}$ is useful in order to capture a necessary security property for analyzing a protocol. Moreover,

ASIACCS'07, March 20–22, 2007, Singapore.

Functionality $\mathcal{F}_{\text{rSIG}}^{(uf,anon)}$

Key Generation: On input ("KeyGen", sid) from party P_i, forward ("KeyGen", sid) to the adversary, obtain a ("Algorithms", $sid, \mathbf{RS}_i, \mathbf{RV}_i$) from the adversary, where $\mathbf{RS}_i$ is a description of a PPT ITM and $\mathbf{RV}_i$ is a description of a deterministic polytime ITM, output ("Verification Algorithms", $sid, \mathbf{RV}_i$) to P_i, record $L_{\text{all}} \leftarrow L_{\text{all}} \cup \{\mathbf{RV}_i\}$.

Signature Generation: On input ("Sign", sid, m, L) from P_i, check $(L \subseteq L_{\text{all}}) \wedge (\mathbf{RV}_i \in L)$. If not, ignore the input. Else, let $\sigma = \mathbf{RS}_i(m, L)$. If $\bigwedge_{\mathbf{RV}_j \in L} \mathbf{RV}_j(m, L, \sigma) = 1$, then record (m, L, σ, P_i) and output ("Signature", sid, m, L, σ). Else, output an error message.

Signature Verification: On input ("Verify", sid, m, L, σ) from some party P_k, output ("Verified", sid, m, f) where:

- Case of $uf =$ eUF
  - **Event 1.** If $L \subseteq L_{\text{all}}$, $(m, L, *, *)$ is not recorded and any party in G corresponding to L is not corrupted, then set $f = 0$.
  - **Event 2.** Else, set $f = \bigwedge_{\mathbf{RV}_j \in L} \mathbf{RV}_j(m, L, \sigma)$.
- Case of $uf =$ sUF
  - **Event 1.** If $L \subseteq L_{\text{all}}$, $(m, L, \sigma, *)$ is not recorded and any party in G corresponding to L is not corrupted, then set $f = 0$.
  - **Event 2.** Else, set $f = \bigwedge_{\mathbf{RV}_j \in L} \mathbf{RV}_j(m, L, \sigma)$.

Attribution: On input ("Attribute", sid, m, L, σ) from the adversary, check that there exists P_i s.t. (m, L, σ, P_i) is recorded. If not, ignore the input. Else, output a message to the adversary where:

- Case of $anon =$ basic
  - **Event 1.** If P_i is uncorrupted and there is the other one honest party in G corresponding to L, then output error message.
  - **Event 2.** Else, output ("Attributed", sid, m, σ, P_i).
- Case of $anon =$ attribution
  - **Event 1.** If there is honest party in G corresponding to L, then output error message.
  - **Event 2.** Else, output ("Attributed", sid, m, σ, P_i).
- Case of $anon =$ full-key

  Always output error message.

Figure 1: Ring signature functionality $\mathcal{F}_{\text{rSIG}}^{(uf,anon)}$

we show relations between cryptographic definitions and our functionality $\mathcal{F}_{\text{rSIG}}^{(uf,anon)}$ at all security levels. As a result, realizing $\mathcal{F}_{\text{rSIG}}^{(uf,anon)}$ is equivalent with ensuring traditional cryptographic security notions of ring signature. Therefore, our UC definitions of ring signature are well-designed.

Universally composable construction. In this paper, we also show concrete constructions which securely realizes our functionality $\mathcal{F}_{\text{rSIG}}^{(uf,anon)}$. We adapt [1](BKM scheme) which is secure without relying on the random oracle assumption.

2. RING SIGNATURE FUNCTIONALITY

In this section, we will introduce a new definition of ring signature schemes in UC framework, i.e., a new ideal ring signature functionality $\mathcal{F}_{\text{rSIG}}^{(uf,anon)}$. Figure 1 shows the functionality $\mathcal{F}_{\text{rSIG}}^{(uf,anon)}$.

$\mathcal{F}_{\text{rSIG}}^{(uf,anon)}$ receives three instructions for basic function of ring signature schemes(Key Generation, Signature Generation and Signature Verification requests) and one instruction for the adversary(Attribution request). $\mathcal{F}_{\text{rSIG}}^{(uf,anon)}$ covers six kinds of security levels, i.e., combination of two levels of unforgeability and three levels of anonymity. That is, $(uf, anon)$ represents a security level as uf is parameterized by eUF and sUF, and $anon$ is parameterized by basic anonymity, anonymity against attribution attacks and anonymity against full key exposure. From now on, on $anon$, we use basic as basic anonymity, attribution as anonymity against attribution attacks and full-key as anonymity against full key exposure for short. Specifically, Signature Verification request concerns unforgeability and Attribution request concerns anonymity. $\mathcal{F}_{\text{rSIG}}^{(uf,anon)}$ is the standard corruption functionality. If the adversary corrupts some party P_j and P_j finished Key Generation request, then $\mathcal{F}_{\text{rSIG}}^{(uf,anon)}$ outputs $\mathbf{RS}_j$ to the adversary. Also, we will show relations between cryptographic security notions.

Guaranteeing unforgeability. If an event corresponding to the condition of unforgeability occurs, $\mathcal{F}_{\text{rSIG}}^{(uf,anon)}$ outputs that the signature is invalid to Signature Verification request. Also, the difference of the condition between eUF and sUF appears at Signature Verification request since the difference of two notions is only the range of signatures which

should be deal with as forged signatures, i.e., $\mathcal{F}_{\mathrm{rSIG}}^{(uf,anon)}$ decides forged signatures. eUF requires that any adversary can't create a signature $\widetilde{\sigma}$ of never signed message $\widetilde{m}$ except with negligible probability, such that $\widetilde{\sigma}$ is verified as valid for $\widetilde{m}$ with respect to the correct verification key list. In addition to the requirement of eUF, sUF requires that any adversary can't even create a valid signature $\widetilde{\sigma}$ of already signed message $\widetilde{m}$ with respect to the verification list except with negligible probability.

Guaranteeing anonymity. The simulator obtain no information about linkage between identity of a signer and a generated signature at Signature Generation request since $\mathcal{F}_{\mathrm{rSIG}}^{(uf,anon)}$ generates the signature by using the signing algorithm **RS** without any interaction with the simulator. Therefore, as long as the simulator doesn't corrupt the signer, perfect anonymity is guaranteed about the signature. Intuitively, Attribution request represents the attribution attack by the adversary. For this attack, requirements of anonymity property differ by each definitions. In the case of basic anonymity, if there aren't at least two uncorrupted parties in the ring, then Event 2 at Attribution request in $\mathcal{F}_{\mathrm{rSIG}}^{(uf,anon)}$ occurs, i.e., the anonymity isn't guaranteed. Also, in the case of anonymity against attribution attacks, if all parties are corrupted, then Event 2 occurs. In the case of anonymity against full key exposure, the adversary can't obtain any information of the true signer even if all parties are corrupted.

Equivalence Relations between Cryptographic Notions and $\mathcal{F}_{\mathrm{rSIG}}^{(uf,anon)}$. Let Σ_r be a ring signature scheme and π_{Σ_r} be a generic protocol corresponding to Σ_r. Then, we obtain the following theorem.

THEOREM 1. *π_{Σ_r} securely realizes $\mathcal{F}_{\mathrm{rSIG}}^{(uf,anon)}$ if and only if Σ_r satisfies both unforgeability and anonymity according to uf and anon.*

3. UNIVERSALLY COMPOSABLE CONSTRUCTION WITHOUT RANDOM ORACLES

In this section, we show concrete constructions of ring signature which securely realizes $\mathcal{F}_{\mathrm{rSIG}}^{(uf,anon)}$. We adapt constructions of [1](BKM schemes). The security of BKM schemes are proved without relying on random oracle assumption.

3.1 BKM schemes

The basic one of BKM schemes is based on general assumptions, i.e., a semantically-secure public-key encryption scheme, an (standard) existentially unforgeable signature scheme and a zap which is a kind of witness-indistinguishable proofs. From now on, we call this scheme *BKM1 scheme*. BKM1 scheme uses the zap as a signature and adopts both perfect soundness and computational witness-indistinguishability of the zap for ensuring unforgeability and anonymity respectively. Under these assumptions, it was proved that BKM1 scheme satisfies eUF and anonymity against attribution attacks.

Moreover, it is shown that BKM1 scheme is able to modify in order to satisfy based on anonymity against full key exposure. We call this scheme *BKM2 scheme*. In this case, the additional assumption which is called a *simulatable* public-key encryption scheme is needed. Roughly speaking, a public-key encryption scheme is simulatable if, in addition to the normal key generation procedure, there is an algorithm to generate a public key without getting to know the corresponding secret key. It was proved that modified BKM2 scheme satisfies eUF and anonymity against full key exposure. However, it is an open problem whether BKM1 scheme and BKM2 scheme are universally composable or not. It seems that these schemes are able to be proved UC-security.

3.2 UC security of BKM schemes

In this section, we will show UC security of BKM schemes. Though BKM1 scheme and BKM2 scheme only satisfy eUF as unforgeability, furthermore, we will give a new modified BKM scheme which has sUF than original BKM schemes and prove UC-security of it similarly. We call this scheme *BKM3 scheme*.

We are able to prove that the protocol of BKM1 scheme securely realizes $\mathcal{F}_{\mathrm{rSIG}}^{(\mathsf{eUF},\mathsf{attribution})}$, i.e., eUF and anonymity against attribution attacks, by using Theorem 1.

THEOREM 2. *Assuming a semantically secure public-key encryption scheme, a existentially unforgeable standard signature scheme against adaptively chosen message attacks and a zap, BKM1 scheme securely realizes $\mathcal{F}_{\mathrm{rSIG}}^{(\mathsf{eUF},\mathsf{attribution})}$.*

Also, the protocol of BKM2 scheme satisfies UC-security, i.e., securely realizes $\mathcal{F}_{\mathrm{rSIG}}^{(\mathsf{eUF},\mathsf{full\text{-}key})}$, by assuming a simulatable public-key encryption scheme. Key Generation part is modified as using a oblivious key generator. We are able to prove that the protocol of BKM2 scheme securely realizes $\mathcal{F}_{\mathrm{rSIG}}^{(\mathsf{eUF},\mathsf{full\text{-}key})}$, i.e., eUF and anonymity against full key exposure, by using Theorem 1.

THEOREM 3. *Assuming a semantically secure simulatable public-key encryption scheme, a existentially unforgeable standard signature scheme against adaptively chosen message attacks and a zap, BKM2 scheme securely realizes $\mathcal{F}_{\mathrm{rSIG}}^{(\mathsf{eUF},\mathsf{full\text{-}key})}$.*

Also, we introduce a new modified BKM scheme, BKM3 scheme, which satisfies sUF and anonymity against full-key exposure. We prove it by showing that the protocol of BKM3 scheme securely realizes $\mathcal{F}_{\mathrm{rSIG}}^{(\mathsf{sUF},\mathsf{full\text{-}key})}$. We construct BKM3 scheme by replacing eUF standard signature to sUF standard signature in BKM2 scheme.

THEOREM 4. *Assuming a semantically secure simulatable public-key encryption scheme, a strong existentially unforgeable standard signature scheme against adaptively chosen message attacks and a zap, BKM3 scheme securely realizes $\mathcal{F}_{\mathrm{rSIG}}^{(\mathsf{sUF},\mathsf{full\text{-}key})}$.*

4. REFERENCES

[1] A. Bender, J. Katz, and R. Morselli. Ring Signatures: Stronger Definitions, and Constructions Without Random Oracles. In *TCC 2006*, pages 60–79, 2006.

[2] K. Yoneyama, Y. Hanatani, B. Santoso, and K. Ohta. Universally Composable Ring Signature. In *IWSEC2006*, 2006.