IEICE TRANS. INF. & SYST., VOL.E105–D, NO.11 NOVEMBER 2022

INVITED PAPER *Special Section on Next-generation Security Applications and Practice*

Generic Construction of 1-out-of-*n* Oblivious Signatures

Yu ZHOU[†,††a)], **Shengli LIU**[†,††,†††b)], ***and*** **Shuai HAN**[†c)], ***Nonmembers***

SUMMARY In a 1-out-of-*n* oblivious signature scheme, a user provides a set of messages to a signer for signatures but he/she can only obtain a valid signature for a specific message chosen from the message set. There are two security requirements for 1-out-of-*n* oblivious signature. The first is ambiguity, which requires that the signer is not aware which message among the set is signed. The other one is unforgeability which requires that the user is not able to derive any other valid signature for any messages beyond the one that he/she has chosen. In this paper, we provide a generic construction of 1-out-of-*n* oblivious signature. Our generic construction consists of two building blocks, a commitment scheme and a standard signature scheme. Our construction is round efficient since it only asks one interaction (i.e., two rounds) between the user and signer. Meanwhile, in our construction, the ambiguity of the 1-out-of-*n* oblivious signature scheme is based on the hiding property of the underlying commitment, while the unforgeability is based on the binding property of the underlying commitment scheme and the unforgeability of the underlying signature scheme. Moreover, our construction can also enjoy strong unforgeability as long as the underlying building blocks have strong binding property and strong unforgeability respectively. Given the fact that commitment and digital signature are well-studied topics in cryptography and numerous concrete schemes have been proposed in the standard model, our generic construction immediately yields a bunch of instantiations in the standard model based on well-known assumptions, including not only traditional assumptions like Decision Diffie-Hellman (DDH), Decision Composite Residue (DCR), etc., but also some post-quantum assumption like Learning with Errors (LWE). As far as we know, our construction admits the first 1-out-of-*n* oblivious signature schemes based on the standard model.

key words: *oblivious signature, ambiguity, unforgeability*

1. Introduction

Digital signature is one of the essential cryptographic primitives in modern cryptography. Generally speaking, a signature scheme allows a signer to generate a pair of verification key and signing key $(\mathsf{vk}, \mathsf{sk})$ and use the signing key sk to sign messages m to obtain signatures σ via a signing algorithm. Given the publicly issued verficition key vk, anyone is able to verify the validity of the signature w.r.t. the message. The unforgeability requires that a probabilistic polynomial-time (PPT) adversary is unable to forge a signature for a new message, even if he can obtain signatures for messages of its choices. Digital signature provides authenticity of the signer, data integrity of the message and undeniability of issuing the signatures.

An important application of digital signature is issuing certificates by authorities. For example, a certificate authority (CA) is responsible for issuing public key certificates for users, and by binding and signing the user's identity and his/her public key in the user's public key certificate, CA transfers the trustworthiness to user's public key. Another example is protection of intellectual property via digital signature. For example, when a user buys a software, the seller may bind the software with the identity of the user to declare the legacy of their products, and the software works only if it is signed by the seller.

In the era of big data, mass data are produced, proceeded and exchanged. The dissemination of information is surprisingly rapid and it provides great convenience to people's lives. However, the side effect of big data is the offence of people's privacy. Analysis of data related to a person might be able to trace his track, derive his hobby, even predict his behavior. Therefore, nowadays there is a serious call on privacy protection from the public. As for digital signatures which are issued by some authorities or companies to users, the messages submitted by the users are completely exposed to the signer, and no privacy is guaranteed for the users. A possible way to this problem is 1-out-of-*n* oblivious signature.

1.1 1-out-of-*n* Oblivious Signature (OS_1^n) Scheme

The concept of oblivious signatures was proposed by Chen in 1994 [1]. In a 1-out-of-*n* oblivious signature scheme OS_1^n, the user prepares a set of n messages, and chooses one message from the set. Then the user interacts with the signer in a polynomial number of rounds, where the user knows the message set $\mathcal{M}$, the chosen message $m \in \mathcal{M}$ and the verification key vk of the signer, and the signer knows its signing key sk and the message set $\mathcal{M}$. In the protocol, the signer interacts with the user and provides oblivious signature σ for the n messages. Finally the user extracts a final signature Σ for his/her chosen message m from the oblivious signature σ.

OS_1^n is able to provide privacy protection for the users while preserving the functionality of signature. This is reflected by two security requirements: *ambiguity* and *un-*

Manuscript received February 17, 2022.
Manuscript revised May 20, 2022.
Manuscript publicized July 15, 2022.

[†]The authors are with the Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai 200240, China.
[††]The authors are with the State Key Laboratory of Cryptology, P.O. Box 5159, Beijing 100878, China.
[†††]The author is with the Westone Cryptologic Research Center, Beijing 100070, China.
a) E-mail: zhouyusjtu2019@sjtu.edu.cn
b) E-mail: slliu@sjtu.edu.cn (Corresponding author)
c) E-mail: dalen17@sjtu.edu.cn (Corresponding author)
DOI: 10.1587/transinf.2022NGI0001

forgeability.

- *Ambiguity.* It requires that the signer is not able to learn which message is chosen by the user for signature from the interactions between the signer and the user. Clearly, the ambiguity of OS_1^n provides privacy protection for the user.
- *Unforgeability.* It deals with malicious users. If the user interacts with the signer honestly, it is able to obtain a valid signature $\Sigma^{(\ell)}$ for one message $m^{(\ell)}$ that he/she has chosen during one execution of the interaction protocol. Unforgeability requires that a malicious user can not forge a valid signature Σ^* for a new message that is different from the messages $m^{(\ell)}$, i.e., $m^* \notin \{m^{(\ell)}\}$.
- *Strong Unforgeability.* We can similarly define *strong unforgeability*, which asks the impossibility of a new valid message-signature pair $(m^*, \Sigma^*) \notin \{(m^{(\ell)}, \Sigma^{(\ell)})\}$.

Let us go back to the application of the software sale. A user wants to buy a software but does not like the seller learn his interest. Then the user can choose n different products and implement 1-out-of-n oblivious signature scheme. The seller does not know which software is bought by the user, and the user can only obtain the very product that he chose and nothing else.

1.2 Related Work

In 1994, Chen [1] proposed two oblivious signature schemes. The schemes are based on a 3-move protocol proposed in [5] and their security are proved in the random oracle model.

In 2008, Tso et al. [2] presented a formal syntax and security model for 1-out-of-n oblivious signature with n messages. They also proposed an efficient scheme based on the Schnorr signature scheme [6] and proved its security in the random oracle model. Compared with [1], their scheme has less communication overhead and less computation cost.

In 2018, Chiou and Chen [3] proposed a t-out-of-n oblivious signature scheme based on the RSA assumption, which achieves strong unforgeability in the random oracle model. However, it needs 3 rounds of communications in the interaction between the signer and the user.

Recently, Tso [4] proposed a new definition called two-in-one oblivious signature system which integrates the oblivious signature w.r.t. n_1 keys and the oblivious signature w.r.t. n_2 messages into one scheme $\mathsf{OS}_1^{(n_1,n_2)}$. This new oblivious signature scheme allows a user to ask for a signature of a message under one of the n_1 signing keys and the message is one of the n_2 messages. The author presented two schemes of two-in-one oblivious signature, which are built from the Schnorr signature scheme [6] and the ELGamal-variant signature scheme. The securities of these schemes were also proved in the random oracle model.

Over the years, some related topics were developed from 1-out-of-n oblivious signatures. In [7], a so-called oblivious signature-based envelop was proposed to solve a secure two-party computation problem. Meanwhile, an efficient envelop scheme was constructed from the RSA signature scheme [8]. In [9], Song et al. proposed an electronic voting protocol based on oblivious signature scheme. In [10], Li et al. constructed a secure obfuscation scheme which implements obfuscation for a special functionality of oblivious signature. Most recently, Chiou and He [11] combined the oblivious signature with proxy signature [12] to yield a t-out-of-n proxy blind signature protocol.

1.3 Our Contributions

As far as we know, there does not exist a good generic construction of oblivious signature scheme in the literature, and almost all the available oblivious signature schemes rely on random oracles for the security proofs. This leads us to consider the following questions.

Is it possible to find a simple generic construction of 1-out-of-n oblivious signatures? Can we build 1-out-of-n oblivious signature schemes in the standard model?

In this paper, we give an affirmative answer to the questions.

- We give a generic construction of 1-out-of-n oblivious signature OS_1^n from two building blocks: a signature scheme and a commitment scheme. Our construction of OS_1^n only involves a 2-round interaction, hence is round efficient. Meanwhile, the ambiguity of OS_1^n is guaranteed by the hiding property of the commitment scheme, and the unforgeability of OS_1^n is guaranteed by the binding property of the commitment scheme and the unforgeability of the signature scheme.
- Moreover, our OS_1^n also enjoys strong unforgeability as long as the underlying building blocks have strong binding property and strong unforgeability respectively.
- Given abundant choices for the commitment and signature schemes in the standard model, we immediately obtain numerous concrete OS_1^n schemes in the standard model, including the ones based on the DL,

Table 1 Comparison of existing oblivious signature schemes. Here "#Round" denotes the number of rounds in the interactive protocol; "/" denotes "or"; "RO" denotes the random oracle model; "Standard" denotes the standard model; "DL" denotes the discrete logarithm assumption; "RSA" denotes the RSA assumption; "CDH" denotes the computational Diffie-Hellman assumption; "DDH" denotes the decisional Diffie-Hellman assumption; "DCR" denotes the deciding composite residuosity assumption; "LWE" denotes the learning with errors assumption; "FAC" denotes the factoring assumption.

Schemes	#Round	Security models	Assumptions
Chen [1]	2	RO	DL
Tso et al. [2]	2	RO	DL
Chiou et al. [3]	3	RO	RSA
Tso [4]	2	RO	DL/CDH
Ours	2	Standard	DDH/DCR /RSA/LWE /FAC

RSA, DCR, FAC assumptions and the post-quantum ones based on the LWE assumption.

A comparison of existing oblivious signatures schemes and our schemes is shown in Table 1.

1.4 Organization

The rest of the paper is organized as follows. Section 2 includes the notations and related definitions. Then we present the generic construction of 1-out-of-n oblivious signature in Sect. 3. In Sect. 4, we give suggestions on instantiations of our construction in the standard model. Finally, Sect. 5 concludes this paper.

2. Preliminaries

Notation. We denote the set of all positive integers up to n as $[n] := \{1, \cdots, n\}$. For a set $\mathcal{X}$, we use $x \xleftarrow{\$} \mathcal{X}$ to denote the process of sampling x from $\mathcal{X}$ uniformly. For a distribution $\mathcal{X}$, $x \leftarrow \mathcal{X}$ denotes the process of sampling x according to $\mathcal{X}$. Let λ denote the security parameter. If an algorithm (or a function) $\mathcal{A}$ is probabilistic, we use the semicolon when we wish to make the randomness explicit: i.e., we denote by $\mathcal{A}(x; r)$ the result of computing $\mathcal{A}$ on input x with randomness r. We use $y \in \mathcal{A}(x)$ to indicate that y lies in the support of $\mathcal{A}(x)$.

2.1 Digital Signatures

Definition 1: A signature scheme $\mathsf{SIG} = (\mathsf{KeyGen}, \mathsf{Sign}, \mathsf{Vrfy})$ consists of a triple of PPT algorithms which are defined below.

- $(\mathsf{vk}, \mathsf{sk}) \leftarrow \mathsf{KeyGen}(1^\lambda)$: Algorithm KeyGen takes a security parameter 1^λ as input and outputs a verification key vk and a secret key sk.
- $\sigma \leftarrow \mathsf{Sign}(\mathsf{sk}, m)$: Algorithm Sign takes a secret key sk and a message m as input and outputs a signature σ.
- $1/0 \leftarrow \mathsf{Vrfy}(\mathsf{vk}, m, \sigma)$: Algorithm Vrfy takes as input a verification key vk, a message m and a signature σ, and outputs 1 or 0 to indicate the validity or invalidity of the signature.

A signature scheme SIG is *existentially unforgeable against chosen message attack* (i.e., *euf-cma* secure) if it has correctness and unforgeability. Similarly, SIG is *strongly euf-cma* secure if it has correctness and strong unforgeability.

- ***Correctness.*** For any message m, there exists a negligible function $\mathsf{negl}(\lambda)$ such that:

$$\Pr\left[\mathsf{Vrfy}(\mathsf{vk}, m, \sigma) = 1 : \begin{array}{c}(\mathsf{vk}, \mathsf{sk}) \leftarrow \mathsf{KeyGen}(1^\lambda), \\ \sigma \leftarrow \mathsf{Sign}(\mathsf{sk}, m)\end{array}\right] \geq 1 - \mathsf{negl}(\lambda).$$

- ***Unforgeability.*** For any PPT adversary $\mathcal{A}$, there exists a negligible function $\mathsf{negl}(\lambda)$ such that:

$$\Pr\left[\begin{array}{c}\mathsf{Vrfy}(\mathsf{vk}, m^*, \sigma^*) = 1 \\ \wedge\ m^* \notin Q_m\end{array} : \begin{array}{c}(\mathsf{vk}, \mathsf{sk}) \leftarrow \mathsf{KeyGen}(1^\lambda), \\ (m^*, \sigma^*) \leftarrow \mathcal{A}^{\mathsf{Sign}(\mathsf{sk}, \cdot)}(\mathsf{vk})\end{array}\right] \leq \mathsf{negl}(\lambda),$$

where $\mathsf{Sign}(\mathsf{sk}, \cdot)$ is the signing oracle and Q_m is a set recording the messages queried to the Sign oracle by $\mathcal{A}$. Note that $m^* \notin Q_m$ means m^* must be a new message.

- ***Strong Unforgeability.*** For any PPT adversary $\mathcal{A}$, there exists a negligible function $\mathsf{negl}(\lambda)$ such that:

$$\Pr\left[\begin{array}{c}\mathsf{Vrfy}(\mathsf{vk}, m^*, \sigma^*) = 1 \\ \wedge\ (m^*, \sigma^*) \notin Q\end{array} : \begin{array}{c}(\mathsf{vk}, \mathsf{sk}) \leftarrow \mathsf{KeyGen}(1^\lambda), \\ (m^*, \sigma^*) \leftarrow \mathcal{A}^{\mathsf{Sign}(\mathsf{sk}, \cdot)}(\mathsf{vk})\end{array}\right] \leq \mathsf{negl}(\lambda),$$

where $Q = \{m_i, \sigma_i\}_{i \in [Q]}$ records all the Q messages $\{m_i\}_{i \in [Q]}$ queried by $\mathcal{A}$ and the corresponding signatures $\{\sigma_i\}_{i \in [Q]}$ replied by the Sign oracle.

2.2 1-out-of-n Oblivious Signatures

We recall the notion of 1-out-of-n oblivious signature scheme and the security requirements for it. The following definition is adapted from [2] and it only considers a two-round protocol between the signer $\mathcal{S}$ and the receiver $\mathcal{R}$.

Definition 2 ([2]): A 1-out-of-n oblivious signature scheme $\mathsf{OS}_1^n = (\mathsf{OKeyGen}, \mathsf{OSign}(\mathcal{S} \rightleftharpoons \mathcal{R}), \mathsf{OVrfy})$ consists of two PPT algorithms and a two-round interactive protocol, which are defined below.

- $(\mathsf{vk}, \mathsf{sk}) \leftarrow \mathsf{OKeyGen}(1^\lambda)$: Algorithm $\mathsf{OKeyGen}$ takes a security parameter 1^λ as input and outputs a verification key vk and a secret key sk.
- $\Sigma/\perp \leftarrow \mathsf{OSign}(\mathcal{S} \rightleftharpoons \mathcal{R})$: OSign is an interactive protocol executed by a signer $\mathcal{S}$ and a receiver $\mathcal{R}$, as shown in Fig. 1. The protocol is made up of the following three algorithms $\mathsf{OSend}\mathcal{R}$, $\mathsf{OSign}\mathcal{S}$, and $\mathsf{OSign}\mathcal{R}$.
  - $(\delta, \mathsf{st}) \leftarrow \mathsf{OSend}\mathcal{R}(\mathsf{vk}, \mathcal{M} = \{m_i\}_{i \in [n]}, j)$: It takes an index $j \in [n]$ and a set of messages $\mathcal{M} = \{m_i\}_{i \in [n]}$ as input and outputs a helper parameter δ and a state st.
  - $\sigma \leftarrow \mathsf{OSign}\mathcal{S}(\mathsf{sk}, \mathcal{M} = \{m_i\}_{i \in [n]}, \delta)$: It takes a secret key sk, a set of messages $\mathcal{M}$ and a helper parameter δ as inputs and outputs an oblivious signature

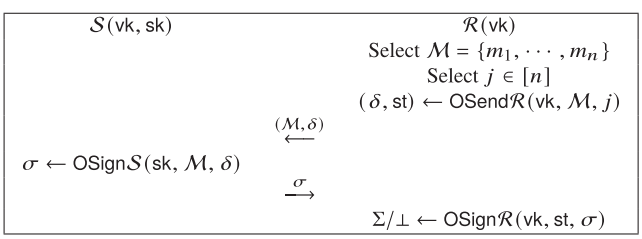

Fig. 1 The interactive protocol $\mathsf{OSign}(\mathcal{S} \rightleftharpoons \mathcal{R})$.

σ.

- $\Sigma/\perp \leftarrow \mathsf{OSign}\mathcal{R}(\mathsf{vk}, \mathsf{st}, \sigma)$: It takes a verification key vk, a state st and an oblivious signature σ as inputs and outputs Σ or $\perp$, where Σ is a signature of m_j.

In practice (see Fig. 1), the protocol is executed in the following way. The receiver $\mathcal{R}$ chooses an n-message set $\mathcal{M} = \{m_i\}_{i\in[n]}$ and selects a message $m_j \in \mathcal{M}$ by specifying the index j, then invokes $(\delta, \mathsf{st}) \leftarrow \mathsf{OSend}\mathcal{R}(\mathsf{vk}, \mathcal{M} = \{m_i\}_{i\in[n]}, j)$ to obtain the help parameter δ. Then $\mathcal{R}$ sends the message set $\mathcal{M}$ together with the help parameter δ to signer $\mathcal{S}$. Next, $\mathcal{S}$ invokes $\sigma \leftarrow \mathsf{OSign}\mathcal{S}(\mathsf{sk}, \mathcal{M}, \delta)$ to generate an oblivious signature σ and then sends σ to $\mathcal{R}$. Finally, $\mathcal{R}$ generates the final signature Σ for m_j with the help of the oblivious signature σ by invoking $\Sigma/\perp \leftarrow \mathsf{OSign}\mathcal{R}(\mathsf{vk}, \mathsf{st}, \sigma)$.

- $1/0 \leftarrow \mathsf{OVrfy}(\mathsf{vk}, m, \Sigma)$: Algorithm OVrfy takes as input a verification key vk, a message m and a signature Σ, and outputs 1 or 0 to indicate the validity or invalidity of the signature.

The 1-out-of-n oblivious signature scheme OS_1^n is *secure* if it has correctness, unforgeability and ambiguity. Similarly, OS_1^n is *strongly secure* if it has correctness, strong unforgeability and ambiguity.

- ***Correctness.*** For any message set $\mathcal{M} = \{m_i\}_{i\in[n]}$ and any $j \in [n]$, there exists a negligible function $\mathsf{negl}(\lambda)$ such that:

$$\Pr\left[\mathsf{OVrfy}(\mathsf{vk}, m_j, \Sigma) = 1 : \begin{array}{c}(\mathsf{vk}, \mathsf{sk}) \leftarrow \mathsf{OKeyGen}(1^\lambda),\\ (\delta, \mathsf{st}) \leftarrow \mathsf{OSend}\mathcal{R}(\mathsf{vk}, \mathcal{M}, j),\\ \sigma \leftarrow \mathsf{OSign}\mathcal{S}(\mathsf{sk}, \mathcal{M}, \delta),\\ \Sigma \leftarrow \mathsf{OSign}\mathcal{R}(\mathsf{vk}, \mathsf{st}, \sigma)\end{array}\right]$$
$$\geq 1 - \mathsf{negl}(\lambda).$$

- ***Unforgeability.*** For any PPT adversary $\mathcal{A}$, there exists a negligible function $\mathsf{negl}(\lambda)$ such that:

$$\Pr\left[\begin{array}{c}\mathsf{OVrfy}(\mathsf{vk}, m^*, \Sigma^*) = 1\\ \wedge\ m^* \notin Q_m^{\mathsf{OS}}\end{array} : \begin{array}{c}(\mathsf{vk}, \mathsf{sk}) \leftarrow \mathsf{OKeyGen}(1^\lambda),\\ (m^*, \Sigma^*) \leftarrow \mathcal{A}^{\mathsf{OSign}\mathcal{S}(\mathsf{sk},\cdot,\cdot)}(\mathsf{vk})\end{array}\right]$$
$$\leq \mathsf{negl}(\lambda).$$

The set Q_m^{OS} records the messages for which $\mathcal{A}$ can obtain valid signatures via querying the $\mathsf{OSign}\mathcal{S}(\mathsf{sk}, \cdot, \cdot)$ oracle. More precisely, for each query $(\mathcal{M} = \{m_i\}_{i\in[n]}, \delta)$ from $\mathcal{A}$, if δ (along with some state st) is an output of $\mathsf{OSend}\mathcal{R}(\mathsf{vk}, \mathcal{M}, j)$ for some $j \in [n]$ and oracle $\mathsf{OSign}\mathcal{S}(\mathsf{sk}, \mathcal{M}, \delta)$ replies σ to $\mathcal{A}$, then $\mathcal{A}$ may learn a signature Σ of m_j by invoking $\Sigma \leftarrow \mathsf{OSign}\mathcal{R}(\mathsf{vk}, \mathsf{st}, \sigma)$, and in this case, the message m_j is recorded in Q_m^{OS} (if there are multiple choices for j, only one m_j is recorded).

- ***Strong Unforgeability.*** For any PPT adversary $\mathcal{A}$, there exists a negligible function $\mathsf{negl}(\lambda)$ such that:

$$\Pr\left[\begin{array}{c}\mathsf{OVrfy}(\mathsf{vk}, m^*, \Sigma^*) = 1\\ \wedge\ (m^*, \Sigma^*) \notin Q^{\mathsf{OS}}\end{array} : \begin{array}{c}(\mathsf{vk}, \mathsf{sk}) \leftarrow \mathsf{OKeyGen}(1^\lambda),\\ (m^*, \Sigma^*) \leftarrow \mathcal{A}^{\mathsf{OSign}\mathcal{S}(\mathsf{sk},\cdot,\cdot)}(\mathsf{vk})\end{array}\right]$$
$$\leq \mathsf{negl}(\lambda).$$

The set Q^{OS} records the valid message-signature pairs that $\mathcal{A}$ can obtain via querying the $\mathsf{OSign}\mathcal{S}(\mathsf{sk}, \cdot, \cdot)$ oracle. More precisely, for each query $(\mathcal{M} = \{m_i\}_{i\in[n]}, \delta)$ from $\mathcal{A}$, if δ (along with some state st) is an output of $\mathsf{OSend}\mathcal{R}(\mathsf{vk}, \mathcal{M}, j)$ for some $j \in [n]$ and oracle $\mathsf{OSign}\mathcal{S}(\mathsf{sk}, \mathcal{M}, \delta)$ replies σ to $\mathcal{A}$, then $\mathcal{A}$ may learn a signature Σ of m_j by invoking $\Sigma \leftarrow \mathsf{OSign}\mathcal{R}(\mathsf{vk}, \mathsf{st}, \sigma)$, and in this case, the message-signature pair (m_j, Σ) is recorded in Q^{OS} (if there are multiple choices for j, only one pair (m_j, Σ) is recorded).

- ***Ambiguity.*** For any PPT adversary $\mathcal{A}$, there exists a negligible function $\mathsf{negl}(\lambda)$ such that:

$$\left|\Pr\left[j^* = j : \begin{array}{c}(\mathsf{vk}, \mathsf{sk}) \leftarrow \mathsf{OKeyGen}(1^\lambda),\\ \mathcal{M} = \{m_1, m_2, \ldots, m_n\} \leftarrow \mathcal{A}(\mathsf{vk}, \mathsf{sk}),\\ j \xleftarrow{\$} [n], (\delta, \mathsf{st}) \leftarrow \mathsf{OSend}\mathcal{R}(\mathsf{vk}, \mathcal{M}, j),\\ j^* \leftarrow \mathcal{A}(\delta)\end{array}\right] - \frac{1}{n}\right|$$
$$\leq \mathsf{negl}(\lambda).$$

2.3 Commitment

Definition 3: A commitment scheme $\mathsf{Commit} = (\mathsf{Com}, \mathsf{Ver})$ consists of two PPT algorithms which are defined below.

- $(\mathsf{c}, \mathsf{r}) \leftarrow \mathsf{Com}(m)$: Algorithm Com takes a message m as input, and outputs a commitment-opening pair (c, r).
- $1/0 \leftarrow \mathsf{Ver}(m, \mathsf{c}, \mathsf{r})$: Algorithm Ver takes a message m, a commitment c and an opening r as input, and outputs 1 or 0 to indicate the validity or invalidity of the opening.

The following properties are required:

- ***Correctness.*** For any message m, there exists a negligible function $\mathsf{negl}(\lambda)$ such that:

$$\Pr\left[\mathsf{Ver}(m, \mathsf{c}, \mathsf{r}) = 1 : (\mathsf{c}, \mathsf{r}) \leftarrow \mathsf{Com}(m)\right] \geq 1 - \mathsf{negl}(\lambda).$$

- ***Soundness.*** For any message m, for all $(\mathsf{c}, \mathsf{r}) \notin \mathsf{Com}(m)$, it always holds that $\mathsf{Ver}(m, \mathsf{c}, \mathsf{r}) = 0$.
- ***Statistical binding.*** For any commitment c, there exists a negligible function $\mathsf{negl}(\lambda)$ such that:

$$\Pr\left[\begin{array}{c}\exists(m, \mathsf{r}), (m', \mathsf{r}')\ s.t.\ m \neq m'\\ \wedge\ \mathsf{Ver}(m, \mathsf{c}, \mathsf{r}) = 1\ \wedge\ \mathsf{Ver}(m', \mathsf{c}, \mathsf{r}') = 1\end{array}\right] \leq \mathsf{negl}(\lambda).$$

- ***Strong statistical binding.*** For any commitment c, there exists a negligible function $\mathsf{negl}(\lambda)$ such that:

$$\Pr\left[\begin{array}{c}\exists(m, \mathsf{r}), (m', \mathsf{r}')\ s.t.\ (m, \mathsf{r}) \neq (m', \mathsf{r}')\\ \wedge\ \mathsf{Ver}(m, \mathsf{c}, \mathsf{r}) = 1\ \wedge\ \mathsf{Ver}(m', \mathsf{c}, \mathsf{r}') = 1\end{array}\right] \leq \mathsf{negl}(\lambda).$$

- ***Computational hiding.*** For any PPT adversary $\mathcal{A}$, there exists a negligible function $\mathsf{negl}(\lambda)$ such that:

$$\Big|\Pr\left[\mathcal{A}(\mathsf{c}) = 1 : (m_0, m_1) \leftarrow \mathcal{A}(1^\lambda), (\mathsf{c}, \mathsf{r}) \leftarrow \mathsf{Com}(m_0)\right]$$
$$- \Pr\left[\mathcal{A}(\mathsf{c}) = 1 : (m_0, m_1) \leftarrow \mathcal{A}(1^\lambda), (\mathsf{c}, \mathsf{r}) \leftarrow \mathsf{Com}(m_1)\right]\Big|$$
$$\leq \mathsf{negl}(\lambda).$$

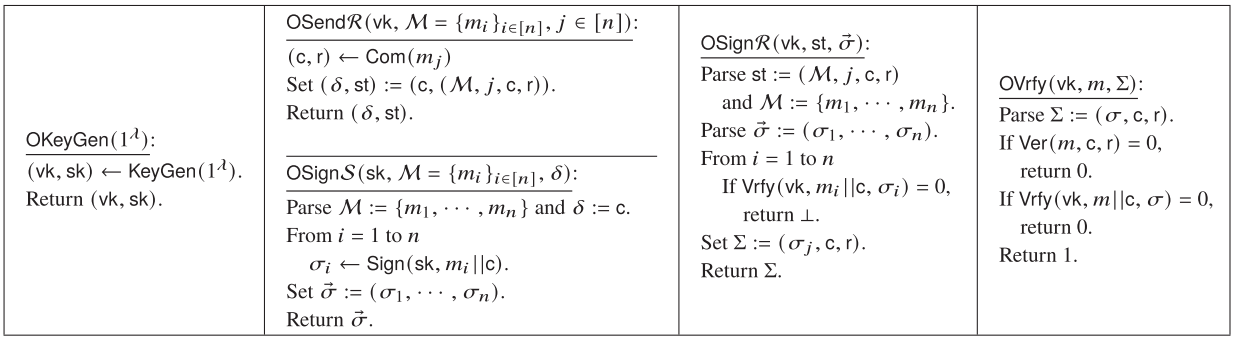

Fig. 2 Generic construction of 1-out-of-n oblivious signature OS_1^n.

3. Generic Construction of 1-out-of-n Oblivious Signature

In this section, we present our generic construction of 1-out-of-n oblivious signature and prove its (strong) unforgeability and ambiguity.

3.1 Generic Construction

Our generic construction of 1-out-of-n oblivious signature scheme OS_1^n is shown in Fig. 2 and it consists of the following two building blocks.

- A signature scheme $\mathsf{SIG} = (\mathsf{KeyGen}, \mathsf{Sign}, \mathsf{Vrfy})$ (as defined in Definition 1).
- A commitment scheme $\mathsf{Commit} = (\mathsf{Com}, \mathsf{Ver})$ (as defined in Definition 3).

The correctness of the 1-out-of-n oblivious signature scheme OS_1^n follows directly from the correctness of SIG and the correctness of Commit.

Remark 1: In the construction of OS_1^n in Fig. 2, it is possible for $\mathsf{OSign}\mathcal{R}$ to check $\mathsf{Vrfy}(\mathsf{vk}, m_j||\mathsf{c}, \sigma_j)$ only for the specific $j \in \mathsf{st}$ and neglect all $i \in [n] \setminus \{j\}$. This modification will lead to better efficiency and there is no affection on the security proofs. However, we recommend to check $\mathsf{Vrfy}(\mathsf{vk}, m_i||\mathsf{c}, \sigma_i)$ for all $i \in [n]$, since this can guarantee the authenticity and integrity of $\vec{\sigma}$ sent from $\mathcal{S}$.

3.2 Security Proofs

In this subsection, we provide Theorem 1 and Theorem 3 to show the unforgeability and ambiguity of OS_1^n with security proofs. In Theorem 2, we also show that OS_1^n can achieve strong unforgeability, as long as Commit has the strong statistical binding property and SIG has strong unforgeability.

Theorem 1 (Unforgeability): Suppose that $\mathsf{SIG} = (\mathsf{KeyGen}, \mathsf{Sign}, \mathsf{Vrfy})$ is a signature scheme which satisfies unforgeability, and $\mathsf{Commit} = (\mathsf{Com}, \mathsf{Ver})$ is a commitment scheme which satisfies statistical binding, then the 1-out-of-n oblivious signature scheme OS_1^n in Fig. 2 satisfies unforgeability.

Proof of Theorem 1: Assume, towards a contradiction, there exists a PPT adversary $\mathcal{A}$ that can break the unforgeability of the 1-out-of-n oblivious signature scheme OS_1^n, with a non-negligible probability. Then we construct a PPT adversary $\mathcal{B}_{\mathsf{SIG}}$ against the unforgeability of SIG.

$\mathcal{B}_{\mathsf{SIG}}$ is constructed by invoking $\mathcal{A}$ and simulating the unforgeability game of OS_1^n for $\mathcal{A}$.

- Firstly, $\mathcal{B}_{\mathsf{SIG}}$ receives a verification key vk from its own challenger. $\mathcal{B}_{\mathsf{SIG}}$ sends vk to $\mathcal{A}$.
- $\mathcal{B}_{\mathsf{SIG}}$ simulates the $\mathsf{OSign}\mathcal{S}(\mathsf{sk}, \cdot, \cdot)$ oracle for $\mathcal{A}$. Note that $\mathcal{B}_{\mathsf{SIG}}$ does not have the secret key sk, and instead, $\mathcal{B}_{\mathsf{SIG}}$ will resort to its own $\mathsf{Sign}(\mathsf{sk}, \cdot)$ oracle (provided in the unforgeability game of SIG) to accomplish the simulation.

  Suppose that $\mathcal{A}$ makes Q queries to the $\mathsf{OSign}\mathcal{S}$ oracle for some polynomial Q. When answering the η-th ($\eta \in [Q]$) $\mathsf{OSign}\mathcal{S}$ query ($\mathcal{M}^{(\eta)} = \{m_1^{(\eta)}, \cdots, m_n^{(\eta)}\}, \delta^{(\eta)} = \mathsf{c}^{(\eta)}$) made by $\mathcal{A}$, $\mathcal{B}_{\mathsf{SIG}}$ makes n queries $m_1^{(\eta)}||\mathsf{c}^{(\eta)}, \cdots, m_n^{(\eta)}||\mathsf{c}^{(\eta)}$ to its own Sign oracle, and receives n signatures $\sigma_1^{(\eta)}, \cdots, \sigma_n^{(\eta)}$ from its own challenger. $\mathcal{B}_{\mathsf{SIG}}$ sends $\vec{\sigma}^{(\eta)} := (\sigma_1^{(\eta)}, \cdots, \sigma_n^{(\eta)})$ to $\mathcal{A}$ as the response of the $\mathsf{OSign}\mathcal{S}$ query.
- Finally, $\mathcal{B}_{\mathsf{SIG}}$ receives a forgery $(m^*, \Sigma^* = (\sigma^*, \mathsf{c}^*, \mathsf{r}^*))$ from $\mathcal{A}$. $\mathcal{B}_{\mathsf{SIG}}$ returns $(m^*||\mathsf{c}^*, \sigma^*)$ to its own challenger as its forgery.

It is clear to see that $\mathcal{B}_{\mathsf{SIG}}$ simulates the unforgeability game of OS_1^n perfectly for $\mathcal{A}$.

For each $\mathsf{OSign}\mathcal{S}$ query $(\mathcal{M}^{(\eta)} = \{m_1^{(\eta)}, \cdots, m_n^{(\eta)}\}, \mathsf{c}^{(\eta)})$ made by $\mathcal{A}$, where $\eta \in [Q]$, we call it a *good* or *bad* query according to the following rule:

– It is called a *good* query, if $\mathsf{c}^{(\eta)}$ is generated honestly by $\mathcal{A}$'s invoking of $\mathsf{OSend}\mathcal{R}$, i.e., $\mathsf{c}^{(\eta)} \in \mathsf{OSend}\mathcal{R}(\mathsf{vk}, \mathcal{M}^{(\eta)}, j)$ for some $j \in [n]$. By our construction in Fig. 2, this means that $\mathsf{c}^{(\eta)}$ is a commitment of $m_j^{(\eta)}$, i.e., $(\mathsf{c}^{(\eta)}, \mathsf{r}^{(\eta)}) \in \mathsf{Com}(m_j^{(\eta)})$ with some opening $\mathsf{r}^{(\eta)}$. By the correctness of Commit, it follows that $\mathsf{Ver}(m_j^{(\eta)}, \mathsf{c}^{(\eta)}, \mathsf{r}^{(\eta)}) = 1$, except with a negligible probability.

  Consequently, for a good query, $\Sigma^{(\eta)} = (\sigma_j^{(\eta)}, \mathsf{c}^{(\eta)}, \mathsf{r}^{(\eta)})$ is a valid signature of $m_j^{(\eta)}$ that $\mathcal{A}$ may obtain. We

record $m_j^{(\eta)}$ in set Q_m^{OS} (the set of messages that $\mathcal{A}$ may know a signature) and record $(m_j^{(\eta)}, \Sigma^{(\eta)} = (\sigma_j^{(\eta)}, \mathsf{c}^{(\eta)}, \mathsf{r}^{(\eta)}))$ in set Q^{OS} (the corresponding set of message-signature pairs).
– It is called a *bad* query, if $\mathsf{c}^{(\eta)}$ is not generated according to $\mathsf{OSend}\mathcal{R}$, i.e., $\mathsf{c}^{(\eta)} \notin \mathsf{OSend}\mathcal{R}(\mathsf{vk}, \mathcal{M}^{(\eta)}, j)$ for all $j \in [n]$. By our construction in Fig. 2, this means that $\mathsf{c}^{(\eta)}$ is not a commitment of any $m_j^{(\eta)}$ in $\mathcal{M}^{(\eta)}$. In other words, for any $j \in [n]$ and any opening $\mathsf{r}^{(\eta)}$, it holds that $(\mathsf{c}^{(\eta)}, \mathsf{r}^{(\eta)}) \notin \mathsf{Com}(m_j^{(\eta)})$, which further implies that $\mathsf{Ver}(m_j^{(\eta)}, \mathsf{c}^{(\eta)}, \mathsf{r}^{(\eta)}) = 0$ by the soundness of Commit.

  According to the security model, Q_m^{OS} and Q^{OS} remains unchanged for a bad query.

We define the events that $\mathcal{B}_{\mathsf{SIG}}$ succeeds and $\mathcal{A}$ succeeds as follows, respectively.

– Let $\mathcal{B}_{\mathsf{SIG}}$-$\mathsf{Wins}$ denote the event that $\mathcal{B}_{\mathsf{SIG}}$'s output $(m^*\|\mathsf{c}^*, \sigma^*)$ is a successful forgery of SIG, i.e., $m^*\|\mathsf{c}^* \notin Q_m := \{m_i^{(\eta)}\|\mathsf{c}^{(\eta)}\}_{i\in[n],\eta\in[Q]}$ (the set of messages that $\mathcal{B}_{\mathsf{SIG}}$ queried to its own Sign oracle) but $\mathsf{Vrfy}(\mathsf{vk}, m^*\|\mathsf{c}^*, \sigma^*) = 1$.
– Let $\mathcal{A}$-Wins denote the event that $\mathcal{A}$'s output $(m^*, \Sigma^* = (\sigma^*, \mathsf{c}^*, \mathsf{r}^*))$ is a successful forgery of OS_1^n, i.e., $m^* \notin Q_m^{\mathsf{OS}}$ (the set of messages that $\mathcal{A}$ knows a signature) but $\mathsf{OVrfy}(\mathsf{vk}, m^*, \Sigma^*) = 1$, where $\mathsf{OVrfy}(\mathsf{vk}, m^*, \Sigma^*) = 1$ means $\mathsf{Ver}(m^*, \mathsf{c}^*, \mathsf{r}^*) = 1$ and $\mathsf{Vrfy}(\mathsf{vk}, m^*\|\mathsf{c}^*, \sigma^*) = 1$.

For ease of analysis, we consider three cases regarding the c^* contained in $\mathcal{A}$'s forgery.

– Let $\mathsf{FreshCom}$ denote the event that $\mathsf{c}^* \notin \{\mathsf{c}^{(\eta)}\}_{\eta\in[Q]}$.
– Let $\mathsf{ExistGood}$ denote the event that there exists a good query, say the η_0-th query $(\mathcal{M}^{(\eta_0)}, \mathsf{c}^{(\eta_0)})$, such that $\mathsf{c}^* = \mathsf{c}^{(\eta_0)}$.
– Let AllBad denote the event that all queries $(\mathcal{M}^{(\eta)}, \mathsf{c}^{(\eta)})$ satisfying $\mathsf{c}^* = \mathsf{c}^{(\eta)}$ are bad queries.

To analyze $\mathcal{B}_{\mathsf{SIG}}$'s advantage $\Pr[\mathcal{B}_{\mathsf{SIG}}\text{-}\mathsf{Wins}]$, we have the following three claims.

Claim 1: $\Pr[\mathcal{A}\text{-}\mathsf{Wins}] = \mathsf{non\text{-}negl}(\lambda)$.

Proof of Claim 1. This is due to the fact that the game that $\mathcal{B}_{\mathsf{SIG}}$ simulates for $\mathcal{A}$ is identical to the unforgeability game of OS_1^n. Thus, by our assumption that $\mathcal{A}$'s advantage is non-negligible, Claim 1 holds. ∎

Claim 2: $\Pr[\mathcal{B}_{\mathsf{SIG}}\text{-}\mathsf{Wins}] \geq \Pr[\mathcal{A}\text{-}\mathsf{Wins} \wedge (\mathsf{FreshCom} \vee \mathsf{AllBad})]$.

Proof of Claim 2. Suppose that $\mathcal{A}$-Wins occurs and $(\mathsf{FreshCom} \vee \mathsf{AllBad})$ occurs, we want to show that $\mathcal{B}_{\mathsf{SIG}}$'s output $(m^*\|\mathsf{c}^*, \sigma^*)$ is a successful forgery of SIG, i.e., $m^*\|\mathsf{c}^* \notin Q_m$ but $\mathsf{Vrfy}(\mathsf{vk}, m^*\|\mathsf{c}^*, \sigma^*) = 1$.

Since $\mathcal{A}$-Wins implies that $\mathcal{A}$'s output $(m^*, \Sigma^* = (\sigma^*, \mathsf{c}^*, \mathsf{r}^*))$ satisfies $\mathsf{Vrfy}(\mathsf{vk}, m^*\|\mathsf{c}^*, \sigma^*) = 1$, it remains to show that $m^*\|\mathsf{c}^* \notin Q_m$ holds, i.e., $m^*\|\mathsf{c}^*$ is a fresh message that has not been queried by $\mathcal{B}_{\mathsf{SIG}}$.

Note that $\mathcal{B}_{\mathsf{SIG}}$ queried $Q_m := \{m_i^{(\eta)}\|\mathsf{c}^{(\eta)}\}_{i\in[n],\eta\in[Q]}$ to its own Sign oracle. We divide $[Q]$ into two subsets:

$$\mathcal{I}_1 := \{\eta \in [Q] \mid \mathsf{c}^* \neq \mathsf{c}^{(\eta)}\},$$
$$\mathcal{I}_2 := \{\eta \in [Q] \mid \mathsf{c}^* = \mathsf{c}^{(\eta)}\},$$

and accordingly, we divide Q_m into two subsets:

$$Q_{m,1} := \{m_i^{(\eta)}\|\mathsf{c}^{(\eta)}\}_{i\in[n],\eta\in\mathcal{I}_1},$$
$$Q_{m,2} := \{m_i^{(\eta)}\|\mathsf{c}^{(\eta)}\}_{i\in[n],\eta\in\mathcal{I}_2}.$$

It is clearly that $m^*\|\mathsf{c}^* \notin Q_{m,1}$. Next we show that $m^*\|\mathsf{c}^* \notin Q_{m,2}$ as well.

- In the case that $\mathsf{FreshCom}$ occurs, $\mathcal{I}_2$ is the empty set, so is $Q_{m,2}$. Thus $m^*\|\mathsf{c}^* \notin Q_{m,2}$ trivially holds.
- In the case that AllBad occurs, we have that for every $\eta \in \mathcal{I}_2$, query $(\mathcal{M}^{(\eta)}, \mathsf{c}^{(\eta)})$ satisfying $\mathsf{c}^* = \mathsf{c}^{(\eta)}$ is a bad query. By the definition of bad query, it follows that $\mathsf{c}^* = \mathsf{c}^{(\eta)}$ is not a commitment of any $m_i^{(\eta)}$ in $\mathcal{M}^{(\eta)}$, so that $\mathsf{Ver}(m_i^{(\eta)}, \mathsf{c}^{(\eta)}, \mathsf{r}^{(\eta)}) = 0$ holds for any $i \in [n]$ and any opening $\mathsf{r}^{(\eta)}$. On the other hand, $\mathcal{A}$-Wins implies that $\mathcal{A}$'s output $(m^*, \Sigma^* = (\sigma^*, \mathsf{c}^*, \mathsf{r}^*))$ satisfies $\mathsf{Ver}(m^*, \mathsf{c}^*, \mathsf{r}^*) = 1$, i.e., c^* is a commitment of m^*. Therefore, it must hold that $m^* \neq m_i^{(\eta)}$ for all $i \in [n]$ and $\eta \in \mathcal{I}_2$, and consequently, $m^*\|\mathsf{c}^* \notin Q_{m,2}$.

Overall, we have $m^*\|\mathsf{c}^* \notin Q_{m,2}$ in either case, and consequently $m^*\|\mathsf{c}^* \notin Q_m = Q_{m,1} \cup Q_{m,2}$. This shows the freshness of $m^*\|\mathsf{c}^*$, and completes the proof of Claim 2. ∎

Claim 3: $\Pr[\mathcal{A}\text{-}\mathsf{Wins} \wedge \mathsf{ExistGood}] \leq \mathsf{negl}(\lambda)$.

Proof of Claim 3. In the case $\mathsf{ExistGood}$, there exists a good query $(\mathcal{M}^{(\eta_0)}, \mathsf{c}^{(\eta_0)})$ such that $\mathsf{c}^* = \mathsf{c}^{(\eta_0)}$. By the definition of good query, there exists a valid signature $\Sigma^{(\eta_0)} = (\sigma_j^{(\eta_0)}, \mathsf{c}^{(\eta_0)}, \mathsf{r}^{(\eta_0)})$ of some $m_j^{(\eta_0)}$ in $\mathcal{M}^{(\eta_0)}$, so that $\mathsf{Ver}(m_j^{(\eta_0)}, \mathsf{c}^{(\eta_0)}, \mathsf{r}^{(\eta_0)}) = 1$ holds, and the corresponding $m_j^{(\eta_0)}$ was recorded in Q_m^{OS}.

Moreover, $\mathcal{A}$-Wins implies that $\mathcal{A}$'s output $(m^*, \Sigma^* = (\sigma^*, \mathsf{c}^*, \mathsf{r}^*))$ satisfies $m^* \notin Q_m^{\mathsf{OS}}$ but $\mathsf{Ver}(m^*, \mathsf{c}^*, \mathsf{r}^*) = 1$.

Therefore, $\mathcal{A}$-$\mathsf{Wins} \wedge \mathsf{ExistGood}$ implies the existence of (m^*, r^*) and $(m_j^{(\eta_0)}, \mathsf{r}^{(\eta_0)})$ such that

$$\mathsf{c}^* = \mathsf{c}^{(\eta_0)} \wedge m^* \neq m_j^{(\eta_0)} \in Q_m^{\mathsf{OS}}$$
$$\wedge\ \mathsf{Ver}(m^*, \mathsf{c}^*, \mathsf{r}^*) = 1 \wedge \mathsf{Ver}(m_j^{(\eta_0)}, \mathsf{c}^{(\eta_0)}, \mathsf{r}^{(\eta_0)}) = 1,$$

which can happen with at most a negligible probability, by the statistical binding property of Commit. This completes the proof of Claim 3. ∎

Finally, by taking Claims 1–3 together, we have

$$\begin{aligned}
&\Pr[\mathcal{B}_{\mathsf{SIG}}\text{-}\mathsf{Wins}] \geq \Pr[\mathcal{A}\text{-}\mathsf{Wins} \wedge (\mathsf{FreshCom} \vee \mathsf{AllBad})] \\
&= \Pr[\mathcal{A}\text{-}\mathsf{Wins}] - \Pr[\mathcal{A}\text{-}\mathsf{Wins} \wedge \mathsf{ExistGood}] \\
&\geq \mathsf{non\text{-}negl}(\lambda) - \mathsf{negl}(\lambda),
\end{aligned}$$

which is still non-negligible in λ. This shows that $\mathcal{B}_{\mathsf{SIG}}$ breaks the unforgeability of SIG successfully, leading to a

contradiction. This completes the proof of the non-strong version of Theorem 1. □

Theorem 2 (Strong Unforgeability): Suppose that $\mathsf{SIG} = (\mathsf{KeyGen}, \mathsf{Sign}, \mathsf{Vrfy})$ is a signature scheme which satisfies strong unforgeability, and $\mathsf{Commit} = (\mathsf{Com}, \mathsf{Ver})$ is a commitment scheme which satisfies strong statistical binding, then the 1-out-of-n oblivious signature scheme OS_1^n shown in Fig. 2 satisfies strong unforgeability.

The proof of Theorem 2 is similar to that of Theorem 1, except that strong unforgeability of SIG and strong statistical binding property of Commit are needed. Due to space limitations, we omit the details of the proof.

Theorem 3 (Ambiguity): Suppose that the scheme $\mathsf{SIG} = (\mathsf{KeyGen}, \mathsf{Sign}, \mathsf{Vrfy})$ is a signature scheme, and $\mathsf{Commit} = (\mathsf{Setup}, \mathsf{Com}, \mathsf{Ver})$ is a commitment scheme which satisfies computational hiding, then the 1-out-of-n oblivious signature scheme OS_1^n shown in Fig. 2 satisfies ambiguity.

Proof of Theorem 3: Assume, towards a contradiction, there exists a PPT adversary $\mathcal{A}$ that can break the ambiguity of the 1-out-of-n oblivious signature scheme OS_1^n, with a non-negligible probability. Then we construct a PPT adversary $\mathcal{B}_{\mathsf{Commit}}$ against the computational hiding property of Commit.

$\mathcal{B}_{\mathsf{Commit}}$ is constructed by invoking $\mathcal{A}$ and simulating the ambiguity game of OS_1^n for $\mathcal{A}$.

- Firstly, $\mathcal{B}_{\mathsf{Commit}}$ invokes $(\mathsf{vk}, \mathsf{sk}) \leftarrow \mathsf{OKeyGen}(1^\lambda)$ by itself. $\mathcal{B}_{\mathsf{Commit}}$ sends $(\mathsf{vk}, \mathsf{sk})$ to $\mathcal{A}$, and receives a set of messages $\mathcal{M} = \{m_1, m_2, \ldots, m_n\}$ from $\mathcal{A}$.
- Then $\mathcal{B}_{\mathsf{Commit}}$ samples an index $j \xleftarrow{\$} [n]$ uniformly, sets $m'_0 := m_j$ and samples a message m'_1 uniformly from the message space. $\mathcal{B}_{\mathsf{Commit}}$ sends (m'_0, m'_1) to its own challenger, and receives a challenger c^* from its own challenger, where c^* is either a commitment of m'_0 or a commitment of m'_1. $\mathcal{B}_{\mathsf{Commit}}$ aims to guess which case it is.
- Finally, $\mathcal{B}_{\mathsf{Commit}}$ returns $\delta := \mathsf{c}^*$ to $\mathcal{A}$, and receives j^* from $\mathcal{A}$ as the guessing of j. $\mathcal{B}_{\mathsf{Commit}}$ returns 1 to its own challenger if and only if $j^* = j$.

Now we analyze $\mathcal{B}_{\mathsf{Commit}}$'s advantage against the computational hiding property of Commit.

– In the case that c^* is a commitment of m'_0, δ $(= \mathsf{c}^*)$ is a commitment of m_j $(= m'_0)$. By our construction in Fig. 2, δ follows from $\mathsf{OSend}\mathcal{R}(\mathsf{vk}, \mathcal{M}, j)$, thus the above game that $\mathcal{B}_{\mathsf{Commit}}$ simulates for $\mathcal{A}$ is identical to the ambiguity game of OS_1^n. Therefore, $\mathcal{A}$'s output j^* equals j with probability $1/n \pm \mathsf{non\text{-}negl}(\lambda)$ for some $\mathsf{non\text{-}negl}(\lambda)$, and consequently, $\mathcal{B}_{\mathsf{Commit}}$ returns 1 to its own challenger with the same probability $1/n \pm \mathsf{non\text{-}negl}(\lambda)$ as well.
– In the case that c^* is a commitment of m'_1, δ $(= \mathsf{c}^*)$ is a commitment of m'_1, which is a uniformly chosen message and is independent of j. Therefore, j is completely hidden to $\mathcal{A}$, and $\mathcal{A}$'s output j^* equals j with probability exactly $1/n$. Consequently, $\mathcal{B}_{\mathsf{Commit}}$ returns 1 to its own challenger with the same probability $1/n$.

Overall, $\mathcal{B}_{\mathsf{Commit}}$'s advantage equals $|(1/n \pm \mathsf{non\text{-}negl}(\lambda)) - 1/n| = \mathsf{non\text{-}negl}(\lambda)$. This shows that $\mathcal{B}_{\mathsf{Commit}}$ breaks the computational hiding property of Commit with a non-negligible probability, leading to a contradiction. This completes the proof of Theorem 3. □

4. Instantiations of Our Generic OS_1^n Construction

In this section, we present the instantiations of our generic construction OS_1^n. To this end, all we have to do is to instantiate the two building blocks.

As for the commitment scheme $\mathsf{Commit} = (\mathsf{Com}, \mathsf{Ver})$, we can instantiate it from any public key encryption scheme $\mathsf{PKE} = (\mathsf{KGen}, \mathsf{Enc}, \mathsf{Dec})$ as follows:

- The public key pk generated by $\mathsf{KGen}(1^\lambda)$ serves as the public parameter of Commit.
- The algorithm $\mathsf{Com}(m; \mathsf{r})$ invokes $\mathsf{c} \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m; \mathsf{r})$, and returns (c, r).
- The algorithm $\mathsf{Ver}(m, \mathsf{c}, \mathsf{r})$ invokes the $\mathsf{c}^* \leftarrow \mathsf{Enc}_{\mathsf{pk}}(m; \mathsf{r})$. Then it outputs 1 if $\mathsf{c}^* = \mathsf{c}$, and outputs 0 otherwise.

When PKE satisfies correctness and IND-CPA security, the commitment scheme Commit constructed as above could satisfy those requirements as defined in Definition 3 because:

- The perfect correctness of Commit is due to the fact that $\mathsf{Enc}_{\mathsf{pk}}(\cdot\,;\cdot)$ is a deterministic function.
- The perfect soundness of Commit follows from the fact that $\mathsf{Ver}(m, \mathsf{c}, \mathsf{r}) = 1$ iff $\mathsf{c} = \mathsf{Enc}_{\mathsf{pk}}(m; \mathsf{r})$ and the fact if $\mathsf{c} = \mathsf{Enc}_{\mathsf{pk}}(m; \mathsf{r})$ then $(\mathsf{c}, \mathsf{r}) \in \mathsf{Com}(m)$.
- The statistical binding of Commit follows from the correctness of PKE.
- The computational hiding of Commit follows from the IND-CPA security of PKE.

There are lots of PKE schemes with IND-CPA security in the standard model. Meanwhile, many PKE schemes yield Commit schemes with strong statistical binding property. For example, the ElGamal scheme [13] based on the Decisional Diffie-Hellman (DDH) assumption, the Paillier scheme [14] based on the Deciding Composite Residuosity (DCR) assumption, the Regev scheme [15] based on the LWE assumption and the Rabin scheme [16] based on the QR assumption which is equivalent to the Factoring (FAC) assumption.

As for the signature scheme $\mathsf{SIG} = (\mathsf{KeyGen}, \mathsf{Sign}, \mathsf{Vrfy})$ with euf-cma security, there are many proposals in the standard model. For example, the SIG schemes [17]–[20] based on the RSA, DDH, DCR, LIN, SIS, LWE assumptions. Moreover, all these schemes can be converted into signature schemes with strong unforgeability via generic transforms in [17], [21].

By integrating those instantiations via our generic construction, we obtain numerous OS_1^n schemes in the standard

Table 2 Performances of several OS_1^n schemes. Here "$|\mathsf{vk}|$" denotes the bit length of the verification key, "$|\mathsf{sk}|$" denotes the bit length of the signing key, "$|\delta|$" denotes the bit length of the helper parameter, "$|\vec{\sigma}|$" denotes the bit length of the oblivious signature and "$|\Sigma|$" denotes the bit length of final signature.

OS_1^n Scheme	$\lvert\mathsf{vk}\rvert$	$\lvert\mathsf{sk}\rvert$	$\lvert\delta\rvert$	$\lvert\vec{\sigma}\rvert$	$\lvert\Sigma\rvert$	Assumption(s)	Standard model
Scheme 1	$O(\lambda)$	$O(\lambda)$	$O(\lambda)$	$O(n\lambda)$	$O(\lambda)$	DDH	✓
Scheme 2	$O(\lambda)$	$O(\lambda)$	$O(\lambda)$	$O(n\lambda)$	$O(\lambda)$	DCR	✓
Scheme 3	$O(\mathsf{poly}(\lambda))$	$O(\mathsf{poly}(\lambda))$	$O(\lambda \log \lambda)$	$O(n\mathsf{poly}(\lambda))$	$O(\mathsf{poly}(\lambda))$	ring-LWE + LWE	✓

- Scheme 1 is instantiated via ELGamal encryption scheme and signature scheme in [19].
- Scheme 2 is instantiated via Pailler encryption scheme and signature scheme in [19].
- Scheme 3 is instantiated via Regev encryption scheme and signature scheme in [20].

model. Note that we can also use those SIG and Commit schemes in the RO model to admit more OS_1^n schemes in the RO model.

Finally, we stress that our OS_1^n construction can be easily extended to construct t-out-of-n oblivious signature schemes: the output δ of $\mathsf{OSend}\mathcal{R}$ consists of commitments $(\mathsf{c}_1, \cdots, \mathsf{c}_t)$ of t messages, while $\mathsf{OSign}\mathcal{S}$ outputs the partial signature $\sigma := \{\sigma_{i,j}\}_{i\in[n],j\in[t]}$ where $\sigma_{i,j} \leftarrow \mathsf{Sign}(\mathsf{sk}, m_i \| \mathsf{c}_j)$.

In Table 2, we present performances of OS_1^n instantiations based on the DDH, DCR and ring-LWE assumptions respectively. We list the sizes of the verification keys, the signing keys, the helper parameters, oblivious signatures, the final signatures and the assumptions in the three OS_1^n schemes.

5. Conclusion

We present a generic construction of 1-out-of-n oblivious signature based on a commitment scheme and a standard signature scheme. Our construction can be easily instantiated, since there are abundant choices for secure commitment schemes and signature schemes with euf-cma security. Compared with the previous 1-out-of-n oblivious signature schemes, our construction is generic and can be instantiated to obtain specific schemes not only in the random oracle model, but also in the standard model. The performances of our 1-out-of-n oblivious signature schemes are determined directly by the two underlying building blocks. Meanwhile, any advances in more efficient signature and commitment schemes will directly lead to more efficient 1-out-of-n oblivious signature schemes.

Acknowledgments

This work is partially supported by National Natural Science Foundation of China (No. 61925207) and Guangdong Major Project of Basic and Applied Basic Research (2019B030302008).

References

[1] L. Chen, "Oblivious signatures," Computer Security - ESORICS 94, Third European Symposium on Research in Computer Security, Brighton, UK, Nov. 7-9, 1994, Proceedings, ed. D. Gollmann, Lecture Notes in Computer Science, vol.875, pp.161–172, Springer, 1994.

[2] R. Tso, T. Okamoto, and E. Okamoto, "1-out-of-n oblivious signatures," International Conference on Information Security Practice and Experience, pp.45–55, 2008.

[3] S. Chiou and J. Chen, "Design and implementation of a multiple-choice e-voting scheme on mobile system using novel t-out-of-n oblivious signature," J. Inf. Sci. Eng., vol.34, no.1, pp.135–154, 2018.

[4] R. Tso, "Two-in-one oblivious signatures," Future Gener. Comput. Syst., vol.101, pp.467–475, 2019.

[5] D. Chaum and T.P. Pedersen, "Wallet databases with observers," ed. E.F. Brickell, Lecture Notes in Computer Science, vol.740, pp.89–105, Springer, 1992.

[6] C.P. Schnorr, "Efficient signature generation by smart cards," J. Cryptol., vol.4, no.3, pp.161–174, 1991.

[7] N. Li, W. Du, and D. Boneh, "Oblivious signature-based envelope," Proceedings of the Twenty-Second ACM Symposium on Principles of Distributed Computing, PODC 2003, Boston, Massachusetts, USA, July 13–16, 2003, ed. E. Borowsky and S. Rajsbaum, pp.182–189, ACM, 2003.

[8] R.L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems (reprint)," Commun. ACM, vol.26, no.1, pp.96–99, 1983.

[9] C. Song, X. Yin, and Y. Liu, "A practical electronic voting protocol based upon oblivious signature scheme," 2008 International Conference on Computational Intelligence and Security, pp.381–384, IEEE, 2008.

[10] C. Li, Z. Yuan, and M. Mao, "Secure obfuscation of a two-step oblivious signature," International Conference on Network Computing and Information Security, vol.345, pp.680–688, Springer, 2012.

[11] S.-Y. Chiou and Y.-X. He, "Generalized proxy oblivious signature and its mobile application," Secur. Commun. Networks, vol.2021, pp.5531505:1–5531505:16, 2021.

[12] M. Mambo, K. Usuda, and E. Okamoto, "Proxy signatures: Delegation of the power to sign messages," IEICE Trans. Fundamentals, vol.E79-A, no.9, pp.1338–1354, 1996.

[13] T.E. Gamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," ed. G.R. Blakley and D. Chaum, Lecture Notes in Computer Science, vol.196, pp.10–18, Springer, 1984.

[14] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," ed. J. Stern, Lecture Notes in Computer Science, vol.1592, pp.223–238, Springer, 1999.

[15] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," Proceedings of the 37th Annual ACM Symposium on Theory of Computing, Baltimore, MD, USA, May 22–24, 2005, ed. H.N. Gabow and R. Fagin, pp.84–93, ACM, 2005.

[16] M.O. Rabin, "Digitalized signatures and public-key functions as intractable as factorization," Tech. Rep., Massachusetts Inst. of Tech. Cambridge Lab for Computer Science, 1979.

[17] J. Katz, Digital Signatures, Springer, 2010.

[18] O. Blazy, S.A. Kakvi, E. Kiltz, and J. Pan, "Tightly-secure signatures from chameleon hash functions," Public-Key Cryptography - PKC 2015 - 18th IACR International Conference on Practice and Theory in Public-Key Cryptography, Gaithersburg, MD, USA,

March 30 - April 1, 2015, Proceedings, ed. J. Katz, Lecture Notes in Computer Science, vol.9020, pp.256–279, Springer, 2015.

[19] X. Zhang, S. Liu, D. Gu, and J.K. Liu, "A generic construction of tightly secure signatures in the multi-user setting," Theor. Comput. Sci., vol.775, pp.32–52, 2019.

[20] X. Zhang, S. Liu, J. Pan, and D. Gu, "Tightly secure signature schemes from the LWE and subset sum assumptions," Theor. Comput. Sci., vol.795, pp.326–344, 2019.

[21] R. Steinfeld, J. Pieprzyk, and H. Wang, "How to strengthen any weakly unforgeable signature into a strongly unforgeable signature," Topics in Cryptology - CT-RSA 2007, The Cryptographers' Track at the RSA Conference 2007, San Francisco, CA, USA, Feb. 5–9, 2007, Proceedings, ed. M. Abe, Lecture Notes in Computer Science, vol.4377, pp.357–371, Springer, 2007.

Yu Zhou received the BS degree from South-east University of School of Mathematics, in2019. He is working toward the PhD degree inShanghai Jiao Tong University. His researchinterests include fuzzy extractor, MPC andindistinguishability obfuscation.

Shengli Liu received the Ph.D. degree in cryptography from XidianUniversity, in 2000 and another Ph.D. degreefrom Eindhoven University of Technology, in2002. She is a professor in Shanghai Jiao TongUniversity. Her research interests include cryp-tography and information security.

Shuai Han received the Ph.D. degree in cryptography from Shanghai Jiao Tong University in 2017. He is an assistant professor in Shanghai Jiao Tong University. His research interests include cryptography and information security.