7-2016

One-round strong oblivious signature-based envelope

Rongmao CHEN

Yi MU

Willy SUSILO

Guomin YANG
Singapore Management University, gmyang@smu.edu.sg

Fuchun GUO

See next page for additional authors

Citation

CHEN, Rongmao; MU, Yi; SUSILO, Willy; YANG, Guomin; GUO, Fuchun; and ZHANG, Mingwu. One-round strong oblivious signature-based envelope. (2016). *Proceedings of the 21st Australasian Conference, Melbourne, Australia, 2016 July 4–6*. 9723, 3-20.
Available at: https://ink.library.smu.edu.sg/sis_research/7398

One-Round Strong Oblivious Signature-Based Envelope

Rongmao Chen[1,2(✉)], Yi Mu[1(✉)], Willy Susilo[1], Guomin Yang[1], Fuchun Guo[1], and Mingwu Zhang[3]

[1] Centre for Computer and Information Security Research School of Computing and Information Technology, University of Wollongong, Wollongong, Australia
{rc517,ymu,wsusilo,gyang,fuchun}@uow.edu.au
[2] College of Computer, National University of Defense Technology, Changsha, China
[3] School of Computers, Hubei University of Technology, Wuhan, China
csmwzhang@gmail.com

Abstract. Oblivious Signature-Based Envelope (OSBE) has been widely employed for anonymity-orient and privacy-preserving applications. The conventional OSBE execution relies on a secure communication channel to protect against eavesdroppers. In TCC 2012, Blazy, Pointcheval and Vergnaud proposed a framework of OSBE (BPV-OSBE) without requiring any secure channel by clarifying and enhancing the OSBE security notions. They showed how to generically build an OSBE scheme satisfying the new strong security in the standard model with a common-reference string. Their framework requires 2-round interactions and relies on the smooth projective hash function (SPHF) over special languages, i.e., languages from encryption of signatures. In this work, we investigate the study on the strong OSBE and make the following contributions. First, we propose a generic construction of *one-round yet strong* OSBE system. Compared to the 2-round BPV-OSBE, our one-round construction is more appealing, as its non-interactive setting accommodates more application scenarios in the real word. Moreover, our framework relies on the regular (identity-based) SPHF, which can be instantiated from extensive languages and hence is more general. Second, we also present an efficient instantiation, which is secure under the standard model from classical assumptions, DDH and DBDH, to illustrate the feasibility of our one-round framework. We remark that our construction is the first one-round OSBE with strong security.

Keywords: Oblivious signature-based envelope · Smooth projective hash function · Privacy

1 Introduction

In 2003, Li et al. [25] introduced a new primitive namely Oblivious Signature-Based Envelope (OSBE), which can be regarded as a nice way to ease the asymmetrical aspect of several authentication protocols. One motivating scenario for

J.K. Liu and R. Steinfeld (Eds.): ACISP 2016, Part II, LNCS 9723, pp. 3–20, 2016.
DOI: 10.1007/978-3-319-40367-0_1

OSBE is as follows: Alice is a regular entity without any specific affiliation. She wants to send a private message to another party (named Bob) if that party possesses certain credentials, e.g., a certificate produced by an authority. For example, Alice might be a potential informant and Bob might be an agent of Central Intelligence Agency (CIA). However, due to the sensitive nature of CIA, Bob is unwilling, or not allowed, to reveal his credentials. In this case, Alice and Bob are stuck and no session could be established. OSBE protocols can well deal with the aforementioned scenario since it allows Alice to send an envelope, which encapsulates her private message, to Bob in such a way that Bob will be able to open the envelope and obtain the private message if and only if Bob has possessed a credential, e.g., a signature on an agreed-upon message from CIA. In the process, Alice cannot determine whether Bob does really belong to CIA (*obliviousness*) and no other party learns anything about Alice's private message (*semantic security*).

Three OSBE protocols were presented in [25]: RSA-OSBE, Rabin-OSBE and BLS-OSBE. The last two protocols are one-round and derived from Identity-Based Encryption [8,17] while RSA-OSBE is 2-round with some interesting properties. Although these protocols satisfy the security requirements of the aforementioned scenario, they implicitly require a secure channel during the execution to protect against eavesdroppers. The reason is that an adversary may eavesdrop and replay a part of a previous interaction to impersonate a CIA agent. Particularly, the Certification Authority who has the signing key can reveal Alice's private message by eavesdropping on the communication between Alice and Bob. To eliminate the dependency on the secure channel for the OSBE, in TCC 2012, Blazy et al. [7] clarified and enhanced the security models of the OSBE by considering the security for both the sender and the receiver against the authority. Their new strong notion, namely *semantic security w.r.t. the authority*, requires that the authority who plays as the eavesdropper on the protocol, learns nothing about the private message of the sender. They showed how to generically build a 2-round OSBE scheme that can achieve the defined strong security in the standard model with a *common-reference string* (CRS), as well as an efficient instantiation (BPV-OSBE) in the standard model from the classical assumption.

Motivations. Although the work in [7] can achieve stronger security than the conventional OSBE protocols, we remark that their 2-round framework has some limitations as follows.

– From a practical point of view, the 2-round OSBE framework requires the receiver to send his obfuscated certificate/signature to the sender first and thereafter the sender sends its envelope to the receiver. Despite that this setting is reasonable in the interaction case, it might be unsuitable for some application scenarios. For example, in the aforementioned scenario, as an informant, Alice would prefer to send her envelope directly to the CIA agent, i.e., Bob, without contacting him in advance, as Alice might be also unwilling to reveal her identity. However, no one-round OSBE protocol with the strong security exists in the literature. It is thus desirable to propose an OSBE protocol that is *one-round* yet with strong security.

– Theoretically, the main idea of the generic construction in [7] is to use the smooth projective hash function (SPHF) on the *special* language defined by the encryption of valid signatures. Precisely, the framework requires the underlying encryption scheme to be semantically secure and the signature scheme to be existentially unforgeable. Although these schemes are quite common in reality, the framework does require them to be of some additional properties when it comes to instantiations. This is essentially due to the complex special language construction for the SPHF. For example, in the instantiation (BPV-OSBE) shown in [7], a linear encryption and a re-randomizable signature is used as the building blocks to achieve the strong security. Therefore, in some sense, the framework is somewhat not general due to the above instantiating limitation.

Based on the aforementioned observations, we can conclude that designing a *one-round* yet *general* OSBE framework with *strong security* is of practical and theoretical importance. In this paper, we are interested in such an OSBE protocol that is secure in the standard model from classical assumptions.

Table 1. Comparisons with existing OSBE protocols

Protocols	Round	Comp.	Comm.	Security			Assumptions
				O.A.	S.S.	S.S.A.	
RSA-OSBE [25]	2	4E+4M	$2\mathbb{Z}_N+P$	√	√	×*	R.O, CDH
Rabin-OSBE [25]	1	$4\|P\|\cdot$ E	$2\|P\|\cdot\mathbb{Z}_N$	√	√	×	R.O., QR
BLS-OSBE [25]	1	3E+2P	$\mathbb{G}_1+2P$	√	√	×	R.O., BDH
BPV-OSBE [7]	2	12E+8M+6P	$6\mathbb{G}_1+P$	√	√	√	CDH, DLin
Our protocol	1	5E+3M+2P	$2\mathbb{G}_1+3\mathbb{G}_T+P$	√	√	√	DDH, DBDH

[a] We use E to denote exponentiation, M the multiplication, P the pairing computation, P the private message.
[b] For the column of **Security**, O.A. denotes the security of *obliviousness w.r.t the authority*, S.S. denotes the security of *semantic security* and S.S.A. denotes the strong security of *semantic security w.r.t. the authority*.
[c] For the column of **Assumption**, R.O. denotes the *random oracle assumption*.

Our Contributions. In this work, we make the following contributions.

– *A Generic One-Round OSBE with Strong Security.* We propose a generic construction of one-round OSBE system of the strong security with a CRS. Compared to the 2-round framework in [7], our one-round construction is more appealing, as its non-interactive setting can accommodate more application scenarios in the real word. Moreover, our framework relies on the regular (IB-)SPHF, which can be instantiated from extensive languages and hence is more general than the work in [7] where special languages, i.e., languages from encryption of signatures are needed for instantiations.

– *An Efficient Instantiation from Classical Assumptions.* An efficient instantiation secure in the standard model from classical assumptions, DDH and DBDH, is presented to illustrate the feasibility of our generic construction. As shown in Table 1, our one-round protocol is of the same strong security as the BPV-OSBE [7] while the protocols in [25] are under the random oracle model and fail to achieve the *semantic security w.r.t. the authority*. It is worth noting that, as remarked in [7], the authority in the 2-round RSA-OSBE protocol can break the scheme by generating the RSA modulus $N = pq$ dishonestly. In terms of the efficiency, the communication complexity of our protocol is comparable to that of the BPV-OSBE [7] while our computation (include both the sender and the receiver) is much more efficient.

Technique Overview. Our central idea is to utilize the *conjunction* of an SPHF and an identity-based SPHF (IB-SPHF) for the protocol construction. The definition of an SPHF [19] requires the existence of a domain $\mathcal{X}$ and an underlying $\mathcal{NP}$ language $\mathcal{L}$, where elements of $\mathcal{L}$ form a subset of $\mathcal{X}$, i.e., $\mathcal{L} \subset \mathcal{X}$. The key property of SPHF is that the hash value of any word $W \in \mathcal{L}$ can be computed by using either a secret hashing key, or a public projection key with the witness to the fact that $W \in \mathcal{L}$ (*correctness*). However, the projection key gives almost no information about the hash value of any point in $\mathcal{X} \setminus \mathcal{L}$ (*smoothness*). Moreover, we say that the subset membership problem is hard if the distribution of $\mathcal{L}$ is computationally indistinguishable from $\mathcal{X} \setminus \mathcal{L}$. Similarly, an IB-SPHF [4,9] has the above properties except that its underlying language is usually associated with the identity which also acts as the public projection key. The secret (identity) hashing key is then derived based on the identity using a master secret key. The IB-SPHF system has formed the backbone of many IBE schemes [9,16,18,21,22], which, as shown in [8], give rise to the signature scheme. The master secret key plays as the signing key and each message is viewed as an identity. The signature is the private key corresponding to the identity.

Our construction deserves further interpretation. Precisely, the receiver owns a hashing key pair $(\mathsf{hk}, \mathsf{hp})$ belonging to the SPHF system while the authority has a master key pair $(\mathsf{msk}, \mathsf{mpk})$ belonging to the IB-SPHF system. The authority can use msk to issue the receiver a valid signature on any agreed-upon message (denoted as M), which is viewed as the identity in the IB-SPHF system. The CRS in our system contains both hp and mpk. To send a message P, the sender firstly samples two distinct words for the SPHF and the IB-SPHF respectively and derives the hash value of each word using hp and M (the identity) with their witnesses to conceal P into the envelope. The sender then sends the two words with the concealed P to the receiver. Upon receiving the message, the receiver uses hk and the valid signature (i.e., identity private key) of M to compute the hash value of the words and thereafter reveals P. One can note that the correctness of our framework relies on the correctness of the underlying SPHF and IB-SPHF. The obliviousness is clear in our one-round framework since the sender does not receive any information from the receiver. The semantic security is guaranteed by the smoothness and the hard subset membership problem of the IB-SPHF while the semantic security w.r.t. the authority is due to the underlying SPHF system.

Organization. The rest of this paper is organized as follows. We review some primitives, including the definition of SPHF and IB-SPHF in Sect. 2, and introduce a generic construction of one-round strong OSBE with formal security analysis in Sect. 3. An efficient instantiation of our framework is then given in Sect. 4. We then conclude our work in Sect. 5.

2 Preliminaries

2.1 Notations and Assumptions

Through this paper, ℓ denotes the security parameter. For a finite set Ω, $\omega \xleftarrow{\$} \Omega$ denotes that ω is selected uniformly from Ω while $\omega \xleftarrow{R} \Omega$ denotes that ω is picked randomly from Ω. Let X and Y be two random variables over a finite domain Ω, the *statistical distance* between X and Y is defined as $\mathsf{SD}(X,Y) = \frac{1}{2}\sum_{\omega\in\Omega} |\Pr[X=\omega] - \Pr[Y=\omega]|$. We say that X and Y are *ϵ-statistically indistinguishable* if $\mathsf{SD}(X,Y) \leq \epsilon$ and for simplicity we denote it by $X \overset{s}{\equiv} Y$.

Definition 1 (Decisional Diffie-Hellman (DDH) Assumption). *Let $\mathbb{G}$ be a general cyclic group of prime order p and $g_1, g_2 \in \mathbb{G}$ the generators of $\mathbb{G}$. Given (g_1, g_2), we say that the decisional Diffie-Hellman assumption holds on $\mathbb{G}$ if for any PPT adversary $\mathcal{A}$,*

$$\mathsf{Adv}^{\mathsf{DDH}}_{\mathcal{A}}(\ell) = |\Pr[\mathcal{A}(g_1^{r_1}, g_2^{r_1}) = 1] - \Pr[\mathcal{A}(g_1^{r_1}, g_2^{r_2}) = 1]| \leq \mathsf{negl}(\ell)$$

where the probability is taken over the random choices $r_1, r_2 \xleftarrow{R} \mathbb{Z}_p$ and the bits consumed by the adversary $\mathcal{A}$.

Let $\mathbb{G}_1, \mathbb{G}_T$ be two multiplicative groups with the same prime order p. Let g be the generator of $\mathbb{G}_1$ and I be the identity element of $\mathbb{G}_T$. A symmetric bilinear map is a map $e : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_T$ such that $e(u^a, v^b) = e(u,v)^{ab}$ for all $u, v \in \mathbb{G}_1$ and $a, b \in \mathbb{Z}_p$. It is worth noting that e can be efficiently computed and $e(g,g) \neq I$. We assume the existence of a group-generation algorithm $\mathcal{BG}(1^\ell)$ which takes as input 1^ℓ and outputs a tuple $(\mathbb{G}_1, \mathbb{G}_T, g, e(\cdot,\cdot), p)$ where $\mathbb{G}_1, \mathbb{G}_T$ are of prime order p.

Definition 2 (Decisional Bilinear Diffie-Hellman (DBDH) Assumption). *Let $(\mathbb{G}_1, \mathbb{G}_T,\ g, e(\cdot,\cdot), p) \leftarrow \mathcal{BG}(1^\ell)$. Given $D = (g, g^x, g^y, g^z)$, we say that the decisional bilinear Diffie-Hellman assumption holds on $\mathbb{G}$ if for any PPT adversary $\mathcal{A}$,*

$$\mathsf{Adv}^{\mathsf{DBDH}}_{\mathcal{A}}(\ell) = |\Pr[\mathcal{A}(D, e(g,g)^{xyz}) = 1] - \Pr[\mathcal{A}(D, e(g,g)^{r}) = 1]| \leq \mathsf{negl}(\ell)$$

where the probability is taken over the random choices $x, y, z, r \xleftarrow{R} \mathbb{Z}_p$ and the bits consumed by the adversary $\mathcal{A}$.

2.2 Smooth Projective Hash Functions

Smooth projective hash function (SPHF) is originally introduced by Cramer and Shoup [19] and extended for constructions of many cryptographic primitives [1–3,5,6,10,11,20,23,24]. We start with the original definition.

An SPHF is based on a domain $\mathcal{X}$ and an $\mathcal{NP}$ language $\mathcal{L}$, where $\mathcal{L}$ contains a subset of the elements of the domain $\mathcal{X}$, i.e., $\mathcal{L} \subset \mathcal{X}$. An SPHF system over a language $\mathcal{L} \subset \mathcal{X}$, onto a set $\mathcal{Y}$, is defined by the following five algorithms $(\mathsf{SPHFSetup}, \mathsf{HashKG}, \mathsf{ProjKG}, \mathsf{Hash}, \mathsf{ProjHash})$:

$(\mathsf{param}, \mathcal{L}) \leftarrow \mathsf{SPHFSetup}(1^\ell)$: The SPHFSetup algorithm takes as input a security parameter ℓ and generates the *global parameters* param and the description of an $\mathcal{NP}$ language $\mathcal{L}$. All other algorithms HashKG, ProjKG, Hash, ProjHash implicitly include $(\mathcal{L}, \mathsf{param})$ as input.

$\mathsf{hk} \leftarrow \mathsf{HashKG}$: The HashKG algorithm generates a *hashing key* hk;

$\mathsf{hp} \leftarrow \mathsf{ProjKG}(\mathsf{hk})$: The ProjKG algorithm derives the *projection key* hp from the hashing key hk;

$\mathsf{hv} \leftarrow \mathsf{Hash}(\mathsf{hk}, W)$: The Hash algorithm takes as input a word W and the hashing key hk, outputs the hash value $\mathsf{hv} \in \mathcal{Y}$;

$\mathsf{hv} \leftarrow \mathsf{ProjHash}(\mathsf{hp}, W, w)$: The ProjHash algorithm takes as input the projection key hp and a word W with the witness w to the fact that $W \in \mathcal{L}$, outputs the hash value $\mathsf{hv} \in \mathcal{Y}$.

An SPHF should satisfies the following properties.

Correctness. Formally, for any word $W \in \mathcal{L}$ with w the witness, we have $\mathsf{Hash}(\mathsf{hk}, W) = \mathsf{ProjHash}(\mathsf{hp}, W, w)$.

Smoothness. For any $W' \in \mathcal{X} \backslash \mathcal{L}$, the following two distributions are statistically indistinguishable, i.e.,$\mathcal{V}_1 \overset{\$}{\equiv} \mathcal{V}_2$, where $\mathcal{V}_1 = \{(\mathcal{L}, \mathsf{param}, W', \mathsf{hp}, \mathsf{hv}) | \mathsf{hv} = \mathsf{Hash}(\mathsf{hk}, W')\}$, and $\mathcal{V}_2 = \{(\mathcal{L}, \mathsf{param}, W', \mathsf{hp}, \mathsf{hv}) | \mathsf{hv} \overset{\$}{\leftarrow} \mathcal{Y}\}$. Precisely, the quantity of $\mathsf{Adv}^{\mathsf{smooth}}_{\mathsf{SPHF}}(\ell) = \sum_{v \in \mathcal{Y}} |\Pr_{\mathcal{V}_1}[\mathsf{hv} = v] - \Pr_{\mathcal{V}_2}[\mathsf{hv} = v]|$ is negligible.

For cryptographic purposes, we normally requires the $\mathcal{NP}$ language $\mathcal{L}$ to be membership indistinguishable, which is formally defined as follows.

Definition 3 (Hard SMP for SPHF). *The subset membership problem* (SMP) *is hard on* $(\mathcal{X}, \mathcal{L})$ *for an* SPHF *that consists of* (SPHFSetup, HashKG, ProjKG, Hash, ProjHash)*, if for any PPT adversary* $\mathcal{A}$*,*

$$\mathsf{Adv}^{\mathsf{SMP}}_{\mathcal{A},\mathsf{SPHF}}(\ell) = \Pr\left[b' = b : \begin{array}{l} (\mathsf{param}, \mathcal{L}) \leftarrow \mathsf{SPHFSetup}(1^\ell); \\ \mathsf{hk} \leftarrow \mathsf{HashKG}; \mathsf{hp} \leftarrow \mathsf{ProjKG}(\mathsf{hk}); \\ b \overset{R}{\leftarrow} \{0,1\}; \\ W_0 \overset{\$}{\leftarrow} \mathcal{X} \backslash \mathcal{L}; W_1 \overset{\$}{\leftarrow} \mathcal{L}; \\ b' \leftarrow \mathcal{A}(\mathsf{param}, \mathcal{L}, \mathsf{hk}, \mathsf{hp}, W_b) \end{array} \right] - \frac{1}{2} \leq \mathsf{negl}(\ell),$$

2.3 Identity-Based Smooth Projective Hash Function

The paradigm of IB-SPHF firstly appeared in [9], where the IB-SPHF is viewed as an SPHF with trapdoor. It was later shown as an identity-based key encapsulation mechanism (IB-KEM) with some special algebraic properties in [4]. IB-SPHF and its extensions have been well applied for cryptographic constructions [12–16].

It is worth noting that most, if not all, IB-SPHF systems require the underlying language $\mathcal{L}$ to depend on the projection key, i.e., the identity. To encompass a broad class of IB-SPHF systems, we associate the language to the identity and refer $\mathcal{L}_{\mathsf{ID}} \subset \mathcal{X}_{\mathsf{ID}}$ to the language for an identity ID. An IB-SPHF system over $\mathcal{L}_{\mathsf{ID}} \subset \mathcal{X}_{\mathsf{ID}}$, onto a set $\mathcal{Y}$, is defined by the following algorithms (IB-SPHFSetup, IB-HashKG, IB-Hash, IB-ProjHash):

$(\mathsf{param}, \mathcal{L}_{\mathsf{ID}}, (\mathsf{msk}, \mathsf{mpk})) \leftarrow \mathsf{IB\text{-}SPHFSetup}(1^\ell)$: The IB-SPHFSetup algorithm takes as input a security parameter ℓ and generates the *global parameters* param with the description of an $\mathcal{NP}$ language $\mathcal{L}_{\mathsf{ID}}$. It outputs the *master public key* mpk and the *master secret key* msk. The master public key defines an *identity set* $\mathcal{ID}$. All other algorithms IB-HashKG, IB-Hash, IB-ProjHash implicitly include $(\mathcal{L}_{\mathsf{ID}}, \mathsf{param}, \mathsf{mpk})$ as input.

$\mathsf{hk}_{\mathsf{ID}} \leftarrow \mathsf{IB\text{-}HashKG}(\mathsf{ID}, \mathsf{msk})$: For any identity $\mathsf{ID} \in \mathcal{ID}$, the IB-HashKG algorithm uses the master secret key msk to generates an *identity hashing key* $\mathsf{hk}_{\mathsf{ID}}$;

$\mathsf{hv} \leftarrow \mathsf{IB\text{-}Hash}(\mathsf{hk}_{\mathsf{ID}}, W)$: The IB-Hash algorithm takes as input a word W and the identity hashing key $\mathsf{hk}_{\mathsf{ID}}$, outputs the hash value $\mathsf{hv} \in \mathcal{Y}$;

$\mathsf{hv} \leftarrow \mathsf{IB\text{-}ProjHash}(\mathsf{ID}, W, w)$: The IB-ProjHash algorithm takes as input the identity ID and a word W with the witness w to the fact that $W \in \mathcal{L}_{\mathsf{ID}}$, outputs the hash value $\mathsf{hv} \in \mathcal{Y}$.

The properties of IB-SPHF are similar to that of an SPHF system, i.e.,

- *Correctness.* For any values of $\mathsf{msk}, \mathsf{mpk}$ produced by IB-SPHFSetup and $\mathsf{ID} \in \mathcal{ID}$ and word $W \in \mathcal{L}_{\mathsf{ID}}$ with w the witness, we have $\mathsf{IB\text{-}Hash}(\mathsf{hk}_{\mathsf{ID}}, W) = \mathsf{IB\text{-}ProjHash}\ (\mathsf{ID}, W, w)$.
- *Smoothness.* For any $\mathsf{ID} \in \mathcal{ID}$ and any $W' \in \mathcal{X}_{\mathsf{ID}} \backslash \mathcal{L}_{\mathsf{ID}}$, the following two distributions are statistically indistinguishable, i.e.,$\mathcal{V}_1 \overset{\$}{\equiv} \mathcal{V}_2$, where $\mathcal{V}_1 = \{(\mathcal{L}, \mathsf{param}, \mathsf{mpk},\ W', \mathsf{ID}, \mathbb{HK}, \mathsf{hv}_{\mathsf{ID}}) | \mathsf{hv}_{\mathsf{ID}} = \mathsf{IB\text{-}Hash}(\mathsf{hk}_{\mathsf{ID}}, W')\}$, and $\mathcal{V}_2 = \{(\mathcal{L}, \mathsf{param}, \mathsf{mpk}, W',\ \mathsf{ID}, \mathbb{HK}, \mathsf{hv}_{\mathsf{ID}}) | \mathsf{hv}_{\mathsf{ID}} \overset{\$}{\leftarrow} \mathcal{Y}\}$. Here $\mathbb{HK}$ is the set of identity hashing key for any identity $\mathsf{ID}' \in \mathcal{ID}$ and $\mathsf{ID}' \neq \mathsf{ID}$. Precisely, the quantity of $\mathsf{Adv}^{\mathsf{smooth}}_{\mathsf{IB\text{-}SPHF}}(\ell) = \sum_{v \in \mathcal{Y}} |\Pr_{\mathcal{V}_1}[\mathsf{hv} = v] - \Pr_{\mathcal{V}_2}[\mathsf{hv} = v]|$ is negligible.

Definition 4 (Hard SMP for IB-SPHF). *The subset membership problem* (SMP) *is hard on* $(\mathcal{X}_{\mathsf{ID}}, \mathcal{L}_{\mathsf{ID}})$ *for an* IB-SPHF *which consists of* (IB-SPHFSetup, IB-HashKG, IB-Hash, IB-ProjHash), *if for any PPT adversary* $\mathcal{A}$,

$$\mathsf{Adv}^{\mathsf{SMP}}_{\mathcal{A},\mathsf{IB\text{-}SPHF}}(\ell) = \Pr\left[b' = b : \begin{array}{l} \mathsf{hk}_{\mathsf{ID}} \leftarrow \mathsf{IB\text{-}HashKG}(\mathsf{ID}, \mathsf{msk}); \\ b \xleftarrow{R} \{0,1\}; \\ W_0 \xleftarrow{\$} \mathcal{L}_{\mathsf{ID}}; W_1 \xleftarrow{\$} \mathcal{X}_{\mathsf{ID}} \backslash \mathcal{L}_{\mathsf{ID}}; \\ b' \leftarrow \mathcal{A}^{\mathcal{O}_{\mathsf{reveal}}(\cdot)}(\mathsf{param}, \mathcal{L}_{\mathsf{ID}}, \mathsf{mpk}, \mathsf{ID}, W_b) \end{array}\right] - 1/2 \leq \mathsf{negl}(\ell),$$

where $\mathsf{msk}, \mathsf{mpk}$ *is produced by* IB-SPHFSetup *and* $\mathcal{O}_{\mathsf{reveal}}(\cdot)$ *is an oracle that on input of any* $\mathsf{id} \in \mathcal{ID}$*, returns* $\mathsf{hk}_{\mathsf{id}} \leftarrow \mathsf{IB\text{-}HashKG}(\mathsf{id}, \mathsf{msk})$.

3 A One-Round Framework for Strong OSBE

In this section, we first briefly introduce the Oblivious Signature-Based Envelope, as well as the formal security models. We then show the first generic construction of one-round OSBE with strong security.

3.1 Oblivious Signature-Based Envelope

An OSBE protocol involves two parties, i.e., a sender $\mathcal{S}$ and a recipient $\mathcal{R}$. $\mathcal{S}$ wants to send a private message P to the recipient $\mathcal{R}$ so that R can receive P if and only if he/she possesses a certificated/signature on a predefined message M. The formal definition is as follows. We mainly follow the definition in [25] to accommodate our generic one-round construction which is introduced in Sect. 3.2. We remark that the new framework captures all the required properties defined in [7,25].

Definition 5 (Oblivious Signature-Based Envelope). *An OSBE scheme is defined by an algorithm* OSBESetup *and an interactive protocol* OSBEProtocol $< \mathcal{S}, \mathcal{R} >$.

- $\mathsf{OSBESetup}(1^\ell)$: *The* OSBESetup *algorithm takes as input the security parameter* ℓ*, generates the global parameters* param*, and the master key pair* $(\mathsf{mpk}, \mathsf{msk})$ *for the authority. The receiver* $\mathcal{R}$ *is issued a certificate/signature* σ *on* M *by the authority.*
- OSBEProtocol $< \mathcal{S}(M, P), \mathcal{R}(M, \sigma) >$: *The* OSBEProtocol *is an interactive protocol between the sender* $\mathcal{S}$ *with a private message* P*, and the receiver* $\mathcal{R}$ *with a certificate/signature* σ*. At the end of the protocol,* $\mathcal{R}$ *receives* P *if* σ *is a valid certificate/signature on* M*, otherwise it learns nothing.*

The *correctness* of an OSBE scheme requires that at the end of OSBEProtocol, the authorized receiver $\mathcal{R}$ (who has a valid certificate/signature σ on M) can output P.

Security Notions for Strong OSBE. According to the original definition [25], in additional to the *correctness*, an OSBE scheme must satisfy *obliviousness* and *semantic security*. In this work, we are interested in the strong OSBE scheme

that should also satisfy another two security properties—*obliviousness w.r.t. the authority* and *semantic security w.r.t. the authority*, which are defined in [7].

Obliviousness (w.r.t. the Authority). Below we first briefly describe the notions of *obliviousness* and *obliviousness w.r.t the authority*. The *obliviousness* requires that the sender $\mathcal{S}$ should not be able to distinguish whether $\mathcal{R}$ uses a valid certificate/signature or not during the protocol execution. The *obliviousness w.r.t. the authority* requires that the above indistinguishability should also hold to the authority who plays as the sender or just eavesdrops on the protocol. One can easily notice that the latter notion is stronger than the former one and both of them can be trivially achieved in one-round OSBE schemes, since $\mathcal{S}$ receives no information from $\mathcal{R}$.

We now formally introduce the security notions of *semantic security* and *semantic security w.r.t. the authority*.

Semantic Security. This security is against the malicious receiver. Roughly speaking, it requires that at the end of the protocol, $\mathcal{R}$ learns nothing about the private input P of $\mathcal{S}$ if it does not use a valid certificate/signature on the predefined message M. The formal security game between the challenge $\mathcal{C}$ and the adversary $\mathcal{A}$ is defined as follows.

Setup. $\mathcal{C}$ runs $\mathsf{OSBESetup}(1^\ell)$ and sends $\mathcal{A}$ the global parameters param.

Query. $\mathcal{A}$ can issues the following two queries:

- $\mathsf{Sign\text{-}Query}$. On input of M, $\mathcal{C}$ returns the valid signature σ_M of M to $\mathcal{A}$.
- $\mathsf{Exec\text{-}Query}$. On input of (M, P), $\mathcal{C}$ first generates σ_M of M, runs $\mathsf{OSBEProtocol} < \mathcal{S}(M, P), \mathcal{R}(M, \sigma_M) >$ and returns the transcript to $\mathcal{A}$.

Challenge. $\mathcal{A}$ chooses a predefined message M^* which has not been queried for signature by $\mathcal{A}$, with two challenge message P_0, P_1 and sends them to $\mathcal{C}$. $\mathcal{C}$ randomly chooses a bit $b \xleftarrow{\$} \{0, 1\}$ and runs $\mathsf{OSBEProtocol} < \mathcal{S}(M^*, P_b), \mathcal{A} >$.

Query. $\mathcal{A}$ continues the query defined above, except that it cannot query M^* for signature.

Guess. Finally, $\mathcal{A}$ outputs b' as its guess on b and wins the game if $b' = b$.

We define the advantage of $\mathcal{A}$ in the above game as $\mathsf{Adv}^{\mathsf{SS}}_{\mathcal{A},\mathsf{OSBE}}(\ell) = \Pr[b = b'] - \frac{1}{2}$.

Semantic Security w.r.t. the Authority. This security is against the malicious authority. Roughly speaking, it requires that at the end of the protocol, the authority who plays as the eavesdropper on the protocol, learns nothing about the private input P of $\mathcal{S}$. The formal security game between the challenge $\mathcal{C}$ and the adversary $\mathcal{A}$ is defined as follows.

Setup. $\mathcal{C}$ runs $\mathsf{OSBESetup}(1^\ell)$ and sends $\mathcal{A}$ the global paramters param with the master secret key msk.

Query. $\mathcal{A}$ issues an Exec query with chosen input (M, P, σ_M). To answer this query, $\mathcal{C}$ runs $\mathsf{OSBEProtocol} < \mathcal{S}(M, P), \mathcal{R}(M, \sigma_M) >$ and returns the transcript to $\mathcal{A}$.

Challenge. $\mathcal{A}$ chooses a predefined message M^* with two challenge message P_0, P_1 and sends them to $\mathcal{C}$. $\mathcal{C}$ randomly chooses a bit $b \xleftarrow{\$} \{0, 1\}$ and runs $\mathsf{OSBEProtocol} < \mathcal{S}(M^*, P_b), \mathcal{R}(M^*, \sigma_{M^*}) >$ which $\mathcal{A}$ can access to its interaction transcript.

Query. $\mathcal{A}$ continues the Exec query as defined above.

Guess. Finally, $\mathcal{A}$ outputs b' as its guess on b and wins the game if $b' = b$.

We define the advantage of $\mathcal{A}$ in the above game as $\mathsf{Adv}^{\mathsf{SS\text{-}Authority}}_{\mathcal{A},\mathsf{OSBE}}(\ell) = \Pr[b = b'] - \frac{1}{2}$.

Definition 6 (Secure OSBE). *An OSBE scheme is secure if it is oblivious w.r.t. the authority and for any probabilistic polynomial-time adversaries $\mathcal{A}$, both $\mathsf{Adv}^{\mathsf{SS}}_{\mathcal{A},\mathsf{OSBE}}(\ell)$ and $\mathsf{Adv}^{\mathsf{SS\text{-}Authority}}_{\mathcal{A},\mathsf{OSBE}}(\ell)$ are negligible in ℓ.*

Remark. One may note that our security notions appear to be different from [7], where the adversary can access several queries in addition to the original models [25]. The reason is that our defined OSBE scheme follows the original one while the work in [7] revised the OSBE framework to accommodate its proposed construction. However, we insist that our models are essentially as strong as the notions defined in [7]. The *enhanced* semantic security (denoted sem) in [7] allows the adversary to obtain several interactions between the server and the receiver with a valid certificate/signature while the adversary in our notion is provided with the access to a so-called Exec oracle which returns the transcript of the honest interaction with adaptively chosen input (M, P) from the adversary. It is worth noting that we put no restriction on the Exec query input (M, P) from $\mathcal{A}$. In particular, $\mathcal{A}$ can make query with input the challenge messages, i.e., $M = M^*$ and $P = P_0/P_1$. Moreover, the Sign query through which $\mathcal{A}$ can obtain the signature of any non-challenge predefined message is also defined in both our model and the experiment in [7]. Similarly, the adversary in our defined notion of *semantic security w.r.t. the authority* can also query the Exec oracle for the transcripts of any specified interaction. We therefore remark that our defined models capture the same security properties as those do in [7].

3.2 The Proposed Generic Construction

We present a generic construction of OSBE from the conjunction of an SPHF and an $\mathsf{IB\text{-}SPHF}$. Let $\mathsf{SPHF} = (\mathsf{SPHFSetup}, \mathsf{HashKG}, \mathsf{ProjKG}, \mathsf{Hash}, \mathsf{ProjHash})$ be a smooth projective hash function over $\mathcal{L} \subset \mathcal{X}$ and $\mathsf{IB\text{-}SPHF} = (\mathsf{IB\text{-}SPHFSetup}, \mathsf{IB\text{-}HashKG}, \mathsf{IB\text{-}Hash}, \mathsf{IB\text{-}ProjHash})$ be an identity-based smooth

projective hash function over $\mathcal{L}_{\mathsf{ID}} \subset \mathcal{X}_{\mathsf{ID}}$. Suppose both systems are onto the same set $\mathcal{Y}$. We additionally use a key derivation function KDF for the generation of a pseudo-random bit-string as the encryption key for the private message. The generic construction of an one-round OSBE protocol on a predefined message M and a private message p is as follows.

- $\mathsf{OSBESetup}(1^\ell)$: The $\mathsf{OSBESetup}$ takes as input a security parameter ℓ.
  - It first generates the individual parameters as $\mathsf{SPHFSetup}(1^\ell) \rightarrow (\mathsf{param}_1, \mathcal{L}), \mathsf{IB\text{-}SPHFSetup}(1^\ell) \rightarrow (\mathsf{param}_2, \mathcal{L}_{\mathsf{ID}}, (\mathsf{msk}, \mathsf{mpk}))$. The master key pair $(\mathsf{msk}, \mathsf{mpk})$ is for the authority.
  - It generates a key pair $(\mathsf{hk}, \mathsf{hp})$ for the SPHF system as $\mathsf{HashKG} \rightarrow \mathsf{hk}, \mathsf{ProjKG}(\mathsf{hk}) \rightarrow \mathsf{hp}$. The hash key pair $(\mathsf{hk}, \mathsf{hp})$ is produced for the receiver.
  - The authority issues a signature $\sigma = \mathsf{hk}_M$ (by viewing M as the identity) as $\mathsf{IB\text{-}HashKG}(\mathsf{msk}, M) \rightarrow \mathsf{hk}_M$. A valid receiver is then given the signature σ.

  The output *global parameters* $\mathsf{param} = (\mathsf{param}_1, \mathsf{param}_2, \mathcal{L}, \mathcal{L}_{\mathsf{ID}}, \mathsf{mpk}, \mathsf{hp})$. All the algorithms involved in the protocol $\mathsf{OSBEProtocol}$ implicitly include param as input.
- $\mathsf{OSBEProtocol} < \mathcal{S}(M, P), \mathcal{R}(M, \sigma) >$: The $\mathsf{OSBEProtocol}$ executes as follows:
  - $\mathcal{S}$ picks $W_1 \leftarrow \mathcal{L}, W_2 \leftarrow \mathcal{L}_M$ with w_1, w_2 the witnesses respectively and computes

$$V = \mathsf{ProjHash}(\mathsf{hp}, W_1, w_1) \oplus \mathsf{IB\text{-}ProjHash}(M, W_2, w_2),$$

$$Q = P \oplus \mathsf{KDF}(V).$$

    $\mathcal{S}$ then sends (W_1, W_2, Q) to $\mathcal{R}$;
  - Upon receiving (W_1, W_2, Q), $\mathcal{R}$ computes,

$$V' = \mathsf{Hash}(\mathsf{hk}, W_1) \oplus \mathsf{IB\text{-}Hash}(\mathsf{hk}_M, W_2),$$

$$P' = Q \oplus \mathsf{KDF}(V').$$

3.3 Security Analysis

We show that the generic construction is secure under our defined models.

Theorem 1 (Correctness). *The generic OSBE construction is correct.*

Proof. Due to the correctness of SPHF and $\mathsf{IB\text{-}SPHF}$, we have that

$$\mathsf{ProjHash}(\mathsf{hp}, W_1, w_1) \oplus \mathsf{IB\text{-}ProjHash}(M, W_2, w_2) = \mathsf{Hash}(\mathsf{hk}, W_1) \oplus \mathsf{IB\text{-}Hash}(\mathsf{hk}_M, W_2),$$

i.e., $V = V'$ and thus $P' = P \oplus \mathsf{KDF}(V) \oplus \mathsf{KDF}(V') = P$.

Theorem 2 (Obliviousness w.r.t. the Authority). *The generic OSBE construction is oblivious w.r.t. the authority.*

Proof. This property is trivial since the protocol is one-round and the server $\mathcal{S}$ receives no information from the receiver $\mathcal{R}$ during the protocol execution.

Theorem 3 (Semantic Security). *The generic OSBE construction is semantically secure if the* SMP *is hard on* $(\mathcal{X}_M, \mathcal{L}_M)$ *for* IB-SPHF *(and under the pseudo-randomness of* KDF*).*

Proof. Let $\mathcal{A}$ be an adversary against the *semantic security* of our construction with advantage $\mathsf{Adv}^{\mathsf{SS}}_{\mathcal{A},\mathsf{OSBE}}(\ell)$. We define a sequence of games between the challenger $\mathcal{C}$ and $\mathcal{A}$ as follows.

Game $\mathcal{G}_0$. In this game, $\mathcal{C}$ simulates as follows.

- **Setup.** $\mathcal{C}$ runs $\mathsf{OSBESetup}(1^\ell)$ and outputs the global parameter param with the receiver secret key hk to $\mathcal{A}$. $\mathcal{C}$ keeps the master secret key msk itself.
- **Query.** $\mathcal{C}$ answers the query as follows.
  - Sign-Query. On input of M from $\mathcal{A}$, $\mathcal{C}$ computes $\mathsf{IB\text{-}HashKG}(\mathsf{msk}, M) \rightarrow \mathsf{hk}_M$, and then returns hk_M to $\mathcal{A}$;
  - Exec-Query. On input of (M, P) from $\mathcal{A}$, $\mathcal{C}$ randomly picks $W_1 \xleftarrow{\$} \mathcal{L}, W_2 \xleftarrow{\$} \mathcal{L}_M$ with w_1, w_2 the witnesses respectively. $\mathcal{C}$ then computes $V = \mathsf{ProjHash}(\mathsf{hp}, W_1, w_1) \oplus \mathsf{IB\text{-}ProjHash}(M, W_2, w_2), Q = P \oplus \mathsf{KDF}(V)$ and then sends (W_1, W_2, Q) to $\mathcal{A}$;
- **Challenge.** $\mathcal{A}$ chooses a predefined message M^* that is not issued to the Sign oracle, with two challenge message P_0, P_1 and sends them to $\mathcal{C}$. $\mathcal{C}$ randomly chooses a bit $b \xleftarrow{\$} \{0,1\}$ and picks $W_1^* \leftarrow \mathcal{L}, W_2^* \leftarrow \mathcal{L}_{M^*}$ with w_1^*, w_2^* the witnesses respectively and computes

  $$V^* = \mathsf{ProjHash}(\mathsf{hp}, W_1^*, w_1^*) \oplus \mathsf{IB\text{-}ProjHash}(M^*, W_2^*, w_2^*), Q^* = P_b \oplus \mathsf{KDF}(V^*).$$

  $\mathcal{C}$ then sends (W_1^*, W_2^*, Q^*) to $\mathcal{A}$;
- **Query.** $\mathcal{C}$ simulates as defined above.
- **Output.** Finally, $\mathcal{A}$ outputs b' as its guess on b.

We define the advantage of $\mathcal{A}$ in game $\mathcal{G}_0$ as $\mathsf{Adv}^{\mathcal{G}_0}_{\mathcal{A},\mathsf{OSBE}}(\ell)$. One can note the definition of game $\mathcal{G}_0$ is exactly the original model of semantic security and thus we have $\mathsf{Adv}^{\mathcal{G}_0}_{\mathcal{A},\mathsf{OSBE}}(\ell) = \mathsf{Adv}^{\mathsf{SS}}_{\mathcal{A},\mathsf{OSBE}}(\ell)$.

Game $\mathcal{G}_1$. Let game $\mathcal{G}_1$ be the same game as $\mathcal{G}_0$, except that in the challenge stage, instead of choosing $W_2^* \xleftarrow{\$} \mathcal{L}_{M^*}$, $\mathcal{C}$ chooses $W_2^* \xleftarrow{\$} \mathcal{X}_{M^*} \backslash \mathcal{L}_{M^*}$ and computes V^* as $V^* = \mathsf{ProjHash}(\mathsf{hp}, W_1^*, w_1^*) \oplus \mathsf{IB\text{-}Hash}(\mathsf{hk}_{M^*}, W_2^*)$. Due to the *hard subset membership problem* and the *correctness* of IB-SPHF, we have $|\mathsf{Adv}^{\mathcal{G}_1}_{\mathcal{A},\mathsf{OSBE}}(\ell) - \mathsf{Adv}^{\mathcal{G}_0}_{\mathcal{A},\mathsf{OSBE}}(\ell)| \leq \mathsf{Adv}^{\mathsf{SMP}}_{\mathcal{A},\mathsf{IB\text{-}SPHF}}(\ell)$.

Game $\mathcal{G}_2$. Let game $\mathcal{G}_2$ be the same game as $\mathcal{G}_1$, except that in the challenge stage, $\mathcal{C}$ computes V^* as $V^* = \mathsf{ProjHash}(\mathsf{hp}, W_1^*, w_1^*) \oplus r$, where $r \xleftarrow{\$} \mathcal{Y}$. Due to the *smoothness* of IB-SPHF, we have $|\mathsf{Adv}^{\mathcal{G}_2}_{\mathcal{A},\mathsf{OSBE}}(\ell) - \mathsf{Adv}^{\mathcal{G}_1}_{\mathcal{A},\mathsf{OSBE}}(\ell)| \leq \mathsf{Adv}^{\mathsf{smooth}}_{\mathsf{IB\text{-}SPHF}}(\ell)$.

Game $\mathcal{G}_3$. Let game $\mathcal{G}_3$ be the same game as $\mathcal{G}_2$, except that $\mathcal{C}$ computes $Q^* = P_b \oplus R$ where $R \xleftarrow{\$} \{0,1\}^l$. Due to the pseudo-randomness of KDF, we have $|\mathsf{Adv}^{\mathcal{G}_3}_{\mathcal{A},\mathsf{OSBE}}(\ell) - \mathsf{Adv}^{\mathcal{G}_2}_{\mathcal{A},\mathsf{OSBE}}(\ell)| \leq \mathsf{Adv}^{\mathsf{PR}}_{\mathcal{A},\mathsf{KDF}}(\ell)$.

Game $\mathcal{G}_4$. Let game $\mathcal{G}_4$ be the same game as $\mathcal{G}_3$, except that $\mathcal{C}$ computes $Q^* \xleftarrow{\$} \{0,1\}^l$. One can note that $\mathsf{Adv}^{\mathcal{G}_3}_{\mathcal{A},\mathsf{OSBE}}(\ell) = \mathsf{Adv}^{\mathcal{G}_4}_{\mathcal{A},\mathsf{OSBE}}(\ell)$. It is easy to see that $\mathcal{A}$ can only wins with probability at most $1/2$ as Q^* is independent of b and hence we have $\mathsf{Adv}^{\mathcal{G}_4}_{\mathcal{A},\mathsf{OSBE}}(\ell) = 0$.

Therefore, from game $\mathcal{G}_0, \mathcal{G}_1, \mathcal{G}_2, \mathcal{G}_3$ and $\mathcal{G}_4$, we have that $\mathsf{Adv}^{\mathsf{SS}}_{\mathcal{A},\mathsf{OSBE}}(\ell)$ is negligible, which completes the proof. □

Theorem 4 (Semantic Security w.r.t. the Authority). *The generic OSBE construction is semantically secure w.r.t. the authority if the* SMP *is hard on* $(\mathcal{X}, \mathcal{L})$ *for* SPHF *(and under the pseudo-randomness of* KDF*).*

Proof Let $\mathcal{A}$ be an adversary against the *semantic security w.r.t. the authority* of our construction with advantage $\mathsf{Adv}^{\mathsf{SS\text{–}Authority}}_{\mathcal{A},\mathsf{OSBE}}(\ell)$. We define a sequence of games between the challenger $\mathcal{C}$ and $\mathcal{A}$ as follows.
Game $\mathcal{G}_0$. In this game, $\mathcal{C}$ simulates as follows

- **Setup.** $\mathcal{C}$ runs $\mathsf{OSBESetup}(1^\ell)$ and outputs the global parameter param with the master secrete key msk to $\mathcal{A}$. $\mathcal{C}$ keeps the hashing key hk itself.
- **Query.** On input of (M, P, σ_M) from $\mathcal{A}$ for an Exec query, $\mathcal{C}$ randomly picks $W_1 \xleftarrow{\$} \mathcal{L}, W_2 \xleftarrow{\$} \mathcal{L}_M$ with w_1, w_2 the witnesses respectively and computes $V = \mathsf{ProjHash}(\mathsf{hp}, W_1, w_1) \oplus \mathsf{IB\text{-}ProjHash}(M, W_2, w_2), Q = P \oplus \mathsf{KDF}(V)$. $\mathcal{C}$ then sends (W_1, W_2, Q) to $\mathcal{A}$;
- **Challenge.** $\mathcal{A}$ chooses a predefined message M^* with two challenge message P_0, P_1 and sends them to $\mathcal{C}$. $\mathcal{C}$ randomly chooses a bit $b \xleftarrow{\$} \{0,1\}$ and picks $W_1^* \leftarrow \mathcal{L}, W_2^* \leftarrow \mathcal{L}_{M^*}$ with w_1^*, w_2^* the witnesses respectively, computes $V^* = \mathsf{ProjHash}\ (\mathsf{hp}, W_1^*, w_1^*) \oplus \mathsf{IB\text{-}ProjHash}(M^*, W_2^*, w_2^*), Q^* = P_b \oplus \mathsf{KDF}(V^*)$. $\mathcal{C}$ then sends (W_1^*, W_2^*, Q^*) to $\mathcal{A}$;
- **Query.** $\mathcal{C}$ simulates as defined above.
- **Output.** Finally, $\mathcal{A}$ outputs b' as its guess on b.

We define the advantage of $\mathcal{A}$ in game $\mathcal{G}_0$ as $\mathsf{Adv}^{\mathcal{G}_0}_{\mathcal{A},\mathsf{OSBE}}(\ell)$. One can note the definition of game $\mathcal{G}_0$ is exactly the original model of semantic security and thus we have $\mathsf{Adv}^{\mathcal{G}_0}_{\mathcal{A},\mathsf{OSBE}}(\ell) = \mathsf{Adv}^{\mathsf{SS\text{–}Authority}}_{\mathcal{A},\mathsf{OSBE}}(\ell)$.

Game $\mathcal{G}_1$. Let game $\mathcal{G}_1$ be the same game as $\mathcal{G}_0$, except that in the $\mathsf{challenge}$ stage, instead of choosing $W_1^* \xleftarrow{\$} \mathcal{L}$, $\mathcal{C}$ chooses $W_1^* \xleftarrow{\$} \mathcal{X} \backslash \mathcal{L}$ and computes $V^* = \mathsf{Hash}(\mathsf{hk}, W_1^*) \oplus \mathsf{IB\text{-}ProjHash}(M^*, W_2^*, w_2^*)$. Due to the *hard subset membership problem* and the *correctness* of SPHF, we have $|\mathsf{Adv}^{\mathcal{G}_1}_{\mathcal{A},\mathsf{OSBE}}(\ell) - \mathsf{Adv}^{\mathcal{G}_0}_{\mathcal{A},\mathsf{OSBE}}(\ell)| \leq \mathsf{Adv}^{\mathsf{SMP}}_{\mathcal{A},\mathsf{SPHF}}(\ell)$.

Game $\mathcal{G}_2$. Let game $\mathcal{G}_2$ be the same game as $\mathcal{G}_1$, except that in the $\mathsf{challenge}$ stage, $\mathcal{C}$ computes V^* as $V^* = r \oplus \mathsf{IB\text{-}ProjHash}(M^*, W_2^*, w_2^*)$, where $r \xleftarrow{\$} \mathcal{Y}$. Due to the *smoothness* of SPHF, we have $|\mathsf{Adv}^{\mathcal{G}_2}_{\mathcal{A},\mathsf{OSBE}}(\ell) - \mathsf{Adv}^{\mathcal{G}_1}_{\mathcal{A},\mathsf{OSBE}}(\ell)| \leq \mathsf{Adv}^{\mathsf{smooth}}_{\mathsf{SPHF}}(\ell)$.

Game $\mathcal{G}_3$. Let game $\mathcal{G}_3$ be the same game as $\mathcal{G}_2$, except that $\mathcal{C}$ computes $Q^* = P_b \oplus R$ where $R \xleftarrow{\$} \{0,1\}^l$. Due to the pseudo-randomness of KDF, we have $|\mathsf{Adv}^{\mathcal{G}_3}_{\mathcal{A},\mathsf{OSBE}}(\ell) - \mathsf{Adv}^{\mathcal{G}_2}_{\mathcal{A},\mathsf{OSBE}}(\ell)| \leq \mathsf{Adv}^{\mathsf{PR}}_{\mathcal{A},\mathsf{KDF}}(\ell)$.

Game $\mathcal{G}_4$. Let game $\mathcal{G}_4$ be the same game as $\mathcal{G}_3$, except that $\mathcal{C}$ computes $Q^* \xleftarrow{\$} \{0,1\}^l$. One can note that $\mathsf{Adv}^{\mathcal{G}_3}_{\mathcal{A},\mathsf{OSBE}}(\ell) = \mathsf{Adv}^{\mathcal{G}_4}_{\mathcal{A},\mathsf{OSBE}}(\ell)$. It is easy to see that $\mathcal{A}$ can only wins with probability at most $1/2$ as Q^* is independent of b and hence we have $\mathsf{Adv}^{\mathcal{G}_4}_{\mathcal{A},\mathsf{OSBE}}(\ell) = 0$.

Therefore, from game $\mathcal{G}_0, \mathcal{G}_1, \mathcal{G}_2, \mathcal{G}_3$ and $\mathcal{G}_4$, we have that $\mathsf{Adv}^{\mathsf{SS\text{-}Authority}}_{\mathcal{A},\mathsf{OSBE}}(\ell)$ is negligible, which completes the proof. □

Based on the results of **Theorems** 1, 2, 3 and 4, we then have the following conclusion.

Theorem 5. *The generic OSBE construction is secure if both* SPHF *and* IB-SPHF *are over hard subset membership problem (and under the pseudo-randomness of* KDF*).*

4 An Efficient Instantiation

In this section, we present a concrete OSBE protocol based on the DDH assumption and DBDH assumption.

4.1 Instantiating the Building Blocks

Due to the space limitation, we briefly describe the instantiations of SPHF and IB-SPHF from the DDH assumption and DBDH assumption respectively and refer the reader to the full version for more details.

DDH-*Based* SPHF. We first introduce the Diffie Hellman language $\mathcal{L}_{\mathsf{DH}}$ as follows. Let $\mathbb{G}$ be a group of prime order p and g_1, g_2 be the generators of $\mathbb{G}$.

$$\mathcal{L}_{\mathsf{DH}} = \{(u_1, u_2) | \exists r \in \mathbb{Z}_p, \text{s.t.}, u_1 = g_1^r, u_2 = g_2^r\}$$

One can see that the witness space of $\mathcal{L}_{\mathsf{DH}}$ is $\mathbb{Z}_p$ and $\mathcal{L}_{\mathsf{DH}} \subset \mathbb{G}^2$. Below we show an concrete SPHF (denoted by $\mathcal{SPHF}_{\mathsf{DH}}$) over the language $\mathcal{L}_{\mathsf{DH}} \subset \mathcal{X}_{\mathsf{DH}} = \mathbb{G}^2$ onto the group $\mathcal{Y} = \mathbb{G}$.

$\mathsf{SPHFSetup}(1^\ell)$: Set $\mathsf{param} = (\mathbb{G}, p, g_1, g_2)$;
HashKG : Pick $(\alpha_1, \alpha_2) \xleftarrow{\$} \mathbb{Z}_p^2$. Output $\mathsf{hk} = (\alpha_1, \alpha_2)$;
$\mathsf{ProjKG}(\mathsf{hk})$: Compute $\mathsf{hp} = g_1^{\alpha_1} g_2^{\alpha_2}$;
$\mathsf{Hash}(\mathsf{hk}, W)$: For a word $W = (u_1, u_2)$, output $\mathsf{hv} = u_1^{\alpha_1} u_2^{\alpha_2}$;
$\mathsf{ProjHash}(\mathsf{hp}, W, w)$: For a word $W = (g_1^r, g_2^r)$, output $\mathsf{hv} = \mathsf{hp}^r = (g_1^{\alpha_1} g_2^{\alpha_2})^r$.

DBDH-*Based* IB-SPHF. We introduce the language for our instantiated IB-SPHF, which can be viewed as the backbone of the IBE scheme in [16]. Let $(\mathbb{G}_1, \mathbb{G}_T, g, e(\cdot,\cdot), p) \leftarrow \mathcal{BG}(1^\ell)$, $u, h \in \mathbb{G}_1, \alpha, \beta \in \mathbb{Z}_p$. For any $\mathsf{ID} \in \mathcal{ID}$, the associated language $\mathcal{L}_{\mathsf{ID}} \subset \mathcal{X}_{\mathsf{ID}}$ are,

$$\mathcal{L}_{\mathsf{ID}} = \{(u_1, u_2, u_3) | \exists z \in \mathbb{Z}_p, \text{s.t.}, u_1 = g^z, u_2 = (u^{\mathsf{ID}} h)^z, u_3 = e(g,g)^{\beta z}\}$$
$$\mathcal{X}_{\mathsf{ID}} = \{(u_1, u_2, u_3) | \exists z_1, z_2 \in \mathbb{Z}_p, \text{s.t.}, u_1 = g^{z_1}, u_2 = (u^{\mathsf{ID}} h)^{z_1}, u_3 = e(g,g)^{\beta z_2}\}$$

One can see that the witness space is $\mathbb{Z}_p$ and $\mathcal{L}_{\mathsf{ID}} \subset \mathbb{G}_1 \times \mathbb{G}_1 \times \mathbb{G}_T$. Below we show the resulted IB-SPHF (denoted by $\mathcal{IB}\text{-}\mathcal{SPHF}$) over the language $\mathcal{L}_{\mathsf{ID}} \subset \mathcal{X}_{\mathsf{ID}}$ onto the group $\mathcal{Y} = \mathbb{G}_T$.

IB-SPHFSetup(1^ℓ) : Let $(\mathbb{G}_1, \mathbb{G}_T, g, e(\cdot,\cdot), p) \leftarrow \mathcal{BG}(1^\ell)$. Pick $u, h \xleftarrow{\$} \mathbb{G}_1, \alpha, \beta \xleftarrow{\$} \mathbb{Z}_p$, set $\mathsf{param} = (\mathbb{G}_1, \mathbb{G}_T, g, e(\cdot,\cdot), p, u, h)$, $\mathsf{msk} = (\alpha, \beta)$, $\mathsf{mpk} = (e(g,g)^\alpha, e(g,g)^\beta)$. The identity set is $\mathcal{ID} = \mathbb{Z}_p$.

IB-HashKG$(\mathsf{ID}, \mathsf{msk})$: For $\mathsf{ID} \in \mathbb{Z}_p$, choose $t, r \xleftarrow{\$} \mathbb{Z}_p$. Output $\mathsf{hk}_{\mathsf{ID}} = (sk_1, sk_2, sk_3) = (g^\alpha g^{-\beta t}(u^{\mathsf{ID}}h)^r, g^{-r}, t)$;

IB-Hash$(\mathsf{hk}_{\mathsf{ID}}, W)$: For a word $W = (u_1, u_2, u_3)$, output $\mathsf{hv}_{\mathsf{ID}} = e(u_1, sk_1)e(u_2, sk_2)u_3^{sk_3}$;

IB-ProjHash(ID, W, w) : For a word $W = (u_1, u_2, u_3) = (g^z, (u^{\mathsf{ID}}h)^z, e(g,g)^{\beta z})$, outputs $\mathsf{hv}_{\mathsf{ID}} = e(g,g)^{\alpha z}$.

4.2 Concrete OSBE Protocol

Using $\mathcal{SPHF}_{\mathsf{DH}}$ and $\mathcal{IB}\text{-}\mathcal{SPHF}$ as instantiation blocks, below we show the resulted OSBE protocol, where a sender $\mathcal{S}$ wants to send a private message $P \in \{0,1\}^l$ to a recipient R in possession of a signature (i.e., the identity hashing key) on a message M.

- OSBESetup(1^ℓ) : Let $\mathbb{G}$ be a group of prime order p and g_1, g_2 the generators of $\mathbb{G}$ and set $\mathsf{param}_1 = (\mathbb{G}, p, g_1, g_2)$. Let $(\mathbb{G}_1, \mathbb{G}_T, g, e(\cdot,\cdot), p) \leftarrow \mathcal{BG}(1^\ell)$, pick $u, h \xleftarrow{\$} \mathbb{G}_1, \alpha, \beta \xleftarrow{\$} \mathbb{Z}_p$, set $\mathsf{param}_2 = (\mathbb{G}_1, \mathbb{G}_T, g, e(\cdot,\cdot), p, u, h)$ and set $\mathsf{msk} = (\alpha, \beta)$, $\mathsf{mpk} = (e(g,g)^\alpha, e(g,g)^\beta)$.
  - Pick $(\alpha_1, \alpha_2) \xleftarrow{\$} \mathbb{Z}_p$, compute $\mathsf{hk} = (\alpha_1, \alpha_2)$, $\mathsf{hp} = g_1^{\alpha_1} g_2^{\alpha_2}$. Set $(\mathsf{hk}, \mathsf{hp})$ as the receiver key pair.
  - For any predefined message $M \in \mathbb{Z}_p$, choose $t, r \xleftarrow{\$} \mathbb{Z}_p$ and compute its signature as $\sigma = \mathsf{hk}_M = (sk_1, sk_2, sk_3) = (g^\alpha g^{-\beta t}(u^M h)^r, g^{-r}, t)$
- OSBEProtocol $< \mathcal{S}(M, P), \mathcal{R}(M, \sigma) >$:
  - $\mathcal{S}$ picks $W_1 = (\widehat{u_1}, \widehat{u_2}) = (g_1^r, g_2^r), W_2 = (u_1, u_2, u_3) = (g^z, (u^M h)^z, e(g,g)^{\beta z})$ and computes
$$V = (g_1^{\alpha_1} g_2^{\alpha_2})^r \cdot e(g,g)^{\alpha z}, Q = P \oplus \mathsf{KDF}(V).$$
$\mathcal{S}$ then sends (W_1, W_2, Q) to $\mathcal{R}$;
  - Upon receiving (W_1, W_2, Q), $\mathcal{R}$ computes,
$$V' = (\widehat{u_1}^{\alpha_1} \widehat{u_2}^{\alpha_2}) \cdot (e(u_1, sk_1)e(u_2, sk_2)u_3^{sk_3}),$$
$$P' = Q \oplus \mathsf{KDF}(V').$$

One should note that in the above concrete protocol, we requires the language used in our $\mathcal{SPHF}_{\mathsf{DH}}$ works on the $\mathbb{G}_T$, i.e., the DDH assumption is on $\mathbb{G} = \mathbb{G}_T$.

The *correctness* of the above protocol is guaranteed by the correctness of $\mathcal{SPHF}_{\mathsf{DH}}$ and $\mathcal{IB}$-$\mathcal{SPHF}$ while the *oblivious w.r.t. the authority* is clear due to the one-round execution. Based on the **Theorem** 5, we have the following conclusion.

Theorem 6. *The instantiated OSBE protocol is secure under the* DDH, DBDH *assumptions (and the pseudo-randomness of* KDF*).*

Efficiency. Our one-round protocol requires only one flow from the sender $\mathcal{S}$ during the execution. Precisely, in addition to the l-bit string (i.e., Q) for the masked $P \in \{0,1\}^l$, the communication in our protocol consists of 2 elements in $\mathbb{G}_1$ and 3 elements in $\mathbb{G}_T$ and hence is slightly higher than the BPV-OSBE protocol [7], where 6 elements in $\mathbb{G}_1$ are needed per execution. It is worth noting that by using a hash function $H : \mathbb{G} \rightarrow \mathbb{G}_T$ on the computation of V, i.e., letting $V = H((g_1^{\alpha_1} g_2^{\alpha_2})^r) \cdot e(g,g)^{\alpha z}$, we can reduce the communication cost of our protocol, as the language used by the $\mathcal{SPHF}_{\mathsf{DH}}$ is now on the smaller group $\mathbb{G}$, instead of $\mathbb{G}_T$. Regarding the computation cost, we remark that our protocol is much more efficient that the BPV-OSBE protocol. Particularly, our protocol mainly requires 5 exponentiation, 3 multiplication and only 2 pairing computation in total per execution while the BPV-OSBE protocol needs 12 exponentiation, 8 multiplication and 6 pairing computation.

5 Conclusion

In this work, we mainly improved the work from TCC 2012 [7] and presented a generic construction of one-round OSBE system that is strongly secure with a common reference string. Compared to the 2-round framework in [7], our one-round construction is more appealing due to the fact that its non-interactive setting accommodates more application scenarios in the real word. Moreover, our framework relies on the (IB-)SPHF, which can be instantiated from extensive languages and hence is more general than the work in [7] where special languages, i.e., languages of ciphertexts from signatures are needed for instantiations. An efficient instantiation, which is secure under the standard model from classical assumptions, DDH and DBDH, is also shown to illustrate the feasibility of our one-round framework.

Acknowledgements. We would like to thank the anonymous reviewers for their invaluable comments on a previous version of this paper. The work of Guomin Yang is supported by the Australian Research Council Discovery Early Career Researcher Award (Grant No. DE150101116) and the National Natural Science Foundation of China (Grant No. 61472308). The work of Mingwu Zhang is supported by the National Natural Science Foundation of China (Grant No. 61370224).

References

1. Abdalla, M., Benhamouda, F., Blazy, O., Chevalier, C., Pointcheval, D.: SPHF-friendly non-interactive commitments. In: Sako, K., Sarkar, P. (eds.) ASIACRYPT 2013, Part I. LNCS, vol. 8269, pp. 214–234. Springer, Heidelberg (2013)
2. Abdalla, M., Benhamouda, F., Pointcheval, D.: Disjunctions for hash proof systems: new constructions and applications. In: Oswald, E., Fischlin, M. (eds.) EUROCRYPT 2015. LNCS, vol. 9057, pp. 69–100. Springer, Heidelberg (2015)
3. Abdalla, M., Chevalier, C., Pointcheval, D.: Smooth projective hashing for conditionally extractable commitments. In: Halevi, S. (ed.) CRYPTO 2009. LNCS, vol. 5677, pp. 671–689. Springer, Heidelberg (2009)
4. Alwen, J., Dodis, Y., Naor, M., Segev, G., Walfish, S., Wichs, D.: Public-key encryption in the bounded-retrieval model. In: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 113–134. Springer, Heidelberg (2010)
5. Benhamouda, F., Blazy, O., Chevalier, C., Pointcheval, D., Vergnaud, D.: New techniques for SPHFs and efficient one-round PAKE protocols. In: Canetti, R., Garay, J.A. (eds.) CRYPTO 2013, Part I. LNCS, vol. 8042, pp. 449–475. Springer, Heidelberg (2013)
6. Blazy, O., Chevalier, C., Vergnaud, D.: Mitigating server breaches in password-based authentication: secure and efficient solutions. In: CT-RSA, pp. 3–18 (2016)
7. Blazy, O., Pointcheval, D., Vergnaud, D.: Round-optimal privacy-preserving protocols with smooth projective hash functions. In: Cramer, R. (ed.) TCC 2012. LNCS, vol. 7194, pp. 94–111. Springer, Heidelberg (2012)
8. Boneh, D., Franklin, M.: Identity-Based Encryption from the Weil Pairing. In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 213–229. Springer, Heidelberg (2001)
9. Boneh, D., Gentry, C., Hamburg, M.: Space-efficient identity based encryption without pairings. In: Proceedings of 48th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2007), October 20–23, 2007, Providence, RI, USA, pp. 647–657 (2007)
10. Chen, R., Mu, Y., Yang, G., Guo, F., Wang, X.: A new general framework for secure public key encryption with keyword search. In: Foo, E., Stebila, D. (eds.) ACISP 2015. LNCS, vol. 9144, pp. 59–76. Springer, Heidelberg (2015)
11. Chen, R., Mu, Y., Yang, G., Susilo, W., Guo, F.: Strongly leakage-resilient authenticated key exchange. In: CT-RSA, pp. 19–36 (2016)
12. Chen, Y., Zhang, Z., Lin, D., Cao, Z.: Anonymous identity-based hash proof system and its applications. In: Takagi, T., Wang, G., Qin, Z., Jiang, S., Yu, Y. (eds.) ProvSec 2012. LNCS, vol. 7496, pp. 143–160. Springer, Heidelberg (2012)
13. Chen, Y., Zhang, Z., Lin, D., Cao, Z.: Identity-based extractable hash proofs and their applications. In: Bao, F., Samarati, P., Zhou, J. (eds.) ACNS 2012. LNCS, vol. 7341, pp. 153–170. Springer, Heidelberg (2012)
14. Chen, Y., Zhang, Z., Lin, D., Cao, Z.: Generalized (identity-based) hash proof system and its applications. IACR Cryptology ePrint Archive 2013, 2 (2013)
15. Chen, Y., Zhang, Z., Lin, D., Cao, Z.: CCA-secure IB-KEM from identity-based extractable hash proof system. Comput. J. **57**(10), 1537–1556 (2014)
16. Chow, S.S.M., Dodis, Y., Rouselakis, Y., Waters, B.: Practical leakage-resilient identity-based encryption from simple assumptions. In: Proceedings of the 17th ACM Conference on Computer and Communications Security, CCS 2010, Chicago, Illinois, USA, 4–8 October 2010, pp. 152–161 (2010)

17. Cocks, C.: An identity based encryption scheme based on quadratic residues. In: Honary, B. (ed.) Cryptography and Coding 2001. LNCS, vol. 2260, pp. 360–363. Springer, Heidelberg (2001)
18. Coron, J.: A variant of Boneh-Franklin IBE with a tight reduction in the random oracle model. Des. Codes Crypt. **50**(1), 115–133 (2009)
19. Cramer, R., Shoup, V.: Universal hash proofs and a paradigm for adaptive chosen ciphertext secure public-key encryption. In: Knudsen, L.R. (ed.) EUROCRYPT 2002. LNCS, vol. 2332, pp. 45–64. Springer, Heidelberg (2002)
20. Gennaro, R., Lindell, Y.: A framework for password-based authenticated key exchange. In: EUROCRYPT, pp. 524–543 (2003)
21. Gentry, C.: Practical identity-based encryption without random oracles. In: Vaudenay, S. (ed.) EUROCRYPT 2006. LNCS, vol. 4004, pp. 445–464. Springer, Heidelberg (2006)
22. Gentry, C., Peikert, C., Vaikuntanathan, V.: Trapdoors for hard lattices and new cryptographic constructions. In: Proceedings of the 40th Annual ACM Symposium on Theory of Computing, Victoria, British Columbia, Canada, May 17–20, 2008, pp. 197–206 (2008)
23. Halevi, S., Kalai, Y.T.: Smooth projective hashing and two-message oblivious transfer. J. Cryptology **25**(1), 158–193 (2012)
24. Katz, J., Vaikuntanathan, V.: Round-optimal password-based authenticated key exchange. In: Ishai, Y. (ed.) TCC 2011. LNCS, vol. 6597, pp. 293–310. Springer, Heidelberg (2011)
25. Li, N., Du, W., Boneh, D.: Oblivious signature-based envelope. In: PODC, pp. 182–189 (2003)