10-2017

New framework of password-based authenticated key exchange from only-one lossy encryption

Haiyang XUE
Singapore Management University, haiyangxue@smu.edu.sg

Bao LI

Jingnan HE

Citation

XUE, Haiyang; LI, Bao; and HE, Jingnan. New framework of password-based authenticated key exchange from only-one lossy encryption. (2017). *Proceedings of the 11th International Conference, ProvSec 2017, Xi'an, China, October 23-25*. 188-198.

Available at: https://ink.library.smu.edu.sg/sis_research/9196

New Framework of Password-Based Authenticated Key Exchange from Only-One Lossy Encryption

Haiyang Xue[1,2](✉), Bao Li[1,2,3], and Jingnan He[1,2]

[1] Data Assurance and Communication Security Research Center,
Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China
[2] Science and Technology on Communication Security Laboratory, Chengdu, China
[3] University of Chinese Academy of Sciences, Beijing, China

Abstract. In this paper, we introduce a new framework of password-based key exchange (PAKE). Until now, most PAKEs are based on smooth projective hash function on secure encryption. Our PAKE does not rely on smooth projective hash function, and consists of a variate lossy encryption, called only-one lossy encryption, and indistinguishable plaintext checkable secure encryption. We also give construction of only-one lossy encryption based decisional Diffie Hellman (DDH) and learning with errors (LWE) assumptions. Although the instantiation based on DDH assumption does not improve efficiency of precious works, our framework provides more easier and elegant way to construct PAKE from LWE assumption.

Keywords: Password-based key exchange · Lossy encryption · DDH assumption · LWE assumption

1 Introduction

Password-based authenticated key exchange (PAKE) allows two users to mutually authenticate each other and agree on a high-entropy session key based on a shared low-entropy password. The challenge in designing such protocols is to prevent *off-line* dictionary attacks where an adversary exhaustively enumerates potential passwords, attempting to match the correct password. The secure goal of PAKE is to restrict the adversary's advantage to that of *online* dictionary attack. The seminal work in the area of PAKE was given by Bellovin and Merritt [4]. After that, Bellare et al. [6], and Boyko et al. [5] proposed formal security models for PAKE. Since then, a large number of constructions were presented in the random oracle model [1,5,6]. But the random oracle model is known to be not sound [8], we only consider standard model in this paper.

The first PAKE protocol to achieve security in standard model was given by Goldreich and Lindel [10]. There are several works to improve and simplify Goldreich and Lindel's scheme. Unfortunately, they are inefficient in terms of communication, computation and round complexity. Katz, Ostrovsky and Yung

T. Okamoto et al. (Eds.): ProvSec 2017, LNCS 10592, pp. 188–198, 2017.
https://doi.org/10.1007/978-3-319-68637-0_11

[16] demonstrated the first efficient PAKE (KOY) under DDH assumption with common reference string(CRS). On the ground of concrete construction of KOY protocol, a framework of PAKE (GL-PAKE) was abstracted by Gennaro and Lindell [11]. GL-PAKE consists of two smooth projective hash functions [7] (SPHF) on chosen ciphertext secure(IND-CCA) encryption. Following the work of KOY, Jiang and Gong [14] improved and gave a PAKE with mutual authentication under DDH assumption. Groce and Katz [12] abstracted the prototol of Jiang and Gong's protocol and give a framework of PAKE (GK-PAKE) by using of SPHF on IND-CPA secure encryption and IND-CCA secure encryption. Recently, Abdalla, Benhamouda and Pointcheval [2] pointed out that the underlying IND-CCA secure encryption in GL-PAKE and GK-PAKE once can be replaced by indistinguishable plaintext checkable secure (IND-PCA) scheme.

Both the GL-PAKE and GK-PAKE frameworks are based on SPHF over secure encryption. It seems that SPHF over encryption scheme is inevitable. Although SPHF supports efficient constructions based on DDH, QR and DCR [19] assumptions. The reliance on SPHF leads to limitations on resulting protocols: firstly, all SPHF are based on decisional assumptions which are generally weaker than computational assumptions. Secondly, When based on lattice assumptions, SPHF is unnatural and it is also an open problem to construct concrete SPHF based on lattice assumptions [17], making the SPHF based PAKE unsuitable in a possible upcoming post quantum world. We also note Katz and Vaikuntanathan [17] proposed an *approximate* SPHF over LWE-based IND-CCA secure encryption, and gave a LWE based PAKE by modifying GL-PAKE. But the protocol is inefficient and is more like a existence result.

One exception (that does not rely on SPHF) is the framework given by Canetti et al. [9] (CDVW-PAKE) based on oblivious transfer protocol and IND-CCA secure encryption. The CDVW-PAKE has the advantage of basing on computational assumption. But, the oblivious transfer protocol needs more communications (it needs 1 out of $|D|$ oblivious transfer, and $|D|$ commitments from the sender, where $|D|$ is the size of password space and the size of real-world password space $|D|$ is generally large [23]), the instantiations of CDVW-PAKE generally needs more communications (the commitments contains at least $|D|$ random string). Precisely, the communications is a linear function of password space.[1]

Thus, a new framework of PAKE, that does not rely on SPHF, has less communication independent with password space, and is more fitable to lattice assumption, is needed. We give such framework in this paper and propose its instantiations based on DDH and LWE assumptions.

1.1 Our Contributions

We propose a new framework of PAKE based on a variant of lossy encryption and IND-PCA secure encryption in this paper. This framework has the following

[1] Even optimizing the protocol by parse the password into bits, the communications still depends on the password space.

benefits: it does not rely on SPHF, making it possible to instantiate the framework on lattice assumptions; the communications is independent of the password space, and generally less then that based on oblivious transfer.

The basic tool is a strong variant of tag-based lossy encryption. Lossy encryption was proposed by Bellare *et al.* [3] by extending meaningful/meaningless encryption in [15]. The public key has two indistinguishable modes: in the normal mode, the cryptosystem behaves normally, and in the *lossy* mode, the ciphertext statistically loses information of the message.

We extend the lossy encryption to tag-based one to fits the application of PAKE. The tag-based encryption, called only-one lossy encryption, has the following properties: (1) The lossy encryption has a hidden branch in public key. Given public key it is difficult to find this branch; (2) only when tag is equal to this branch the encryption is normal and decryptable, in the other case the encryption of any two messages is statistically indistinguishable; (3) With a trapdoor, there is an algorithm to decide whether a tag is equal to the hidden branch in public key. At a first look, the tag-based encryption looks like All-But-One technique but it has essential difference. Take the general All-But-One lossy trapdoor function in [21] as example, in the All-But-One technique, the "one" is lossy and secure to prove the security, the others is invertible to provide inversion functionality. But the Only-one lossy encryption is that the one is decryptable to provide the functionality and the others is lossy and statistically secure to provide security.

Based on only-one lossy encryption and IND-PCA secure encryption, we propose a framework of PAKE, and prove its security in standard model. After that, we also give two instantiations based on DDH assumption and learning with errors (LWE) assumption.

1.2 Related Works

Peikert et al. proposed the notion of dual mode cryptosystem [20] aimming at universal composable secure oblivious transfer. In the dual mode cryptosystem, it requires two setup algorithms, and in one mode, there should be a algorithm to generate decryption key for ciphertext on all tag. We do not require this in only-one lossy encryption.

Canetti et al. [9] propose a framework of based on oblivious transfer protocol and IND-CCA secure encryption. The CDVW-PAKE has the advantage of basing on computational assumption. But, the oblivious transfer needs more communications (it needs $|D|$ commitment, where $|D|$ is the size of password space), the instantiations of CDVW-PAKE generally needs more communications (at least needs commitments of $|D|$ randomness).

2 Preliminaries

In this section, we give some notions and recall the definition of lossy encryption and the BPR secure mode of PAKE.

2.1 Notations

If S is a set, we denote by $|S|$ the cardinality of S, and denote by $x \leftarrow S$ the process of sampling x uniformly from S. A function is *negligible* (negl) if for every $c > 0$ there exists a λ_c such that $f(\lambda) < 1/\lambda^c$ for all $\lambda > \lambda_c$. If A and B are distributions, $A =_s B$ means that the statistical distance between A and B is negligible.

For any $s > 0$, and $\mathbf{c} \in \mathbb{R}^n$ define the Gaussian function: $\forall \mathbf{x} \in \mathbb{R}^n$, $\rho_{s,\mathbf{c}} = exp(-\pi \|\mathbf{x} - \mathbf{c}\|^2/s^2)$. For any $\mathbf{c} \in \mathbb{R}$, real $s > 0$, and n-dimensional lattice $\varLambda$, define the discrete Guassian distribution over $\varLambda$ as $\forall \mathbf{x} \in \varLambda, \mathcal{D}_{\varLambda,s,\mathbf{c}}(\mathbf{x}) = \frac{\rho_{s,\mathbf{c}}(\mathbf{x})}{\rho_{s,\mathbf{c}}(\varLambda)}$, where $\rho_{s,\mathbf{c}}(\varLambda) = \sum_{\mathbf{y} \in \varLambda} \rho_{s,\mathbf{c}}(\mathbf{y})$. we omit the parameter $\mathbf{c}$ when it is 0. For $\alpha \in \mathbb{R}^+$, $\varPsi_\alpha$ is defined to be the distribution on $\mathbb{R}/\mathbb{Z}$ of a mormal variable with mean 0 and standard deviation $\alpha/\sqrt{2\pi}$, reduced modulo 1. Let $\bar{\varPsi}_\alpha$ be the discrete distribution of the random variable $\lfloor q \cdot X \rceil \mod q$ where X has distribution $\varPsi_\alpha$.

2.2 Encryption

For formal definition of lossy encryption please refer citeBellare2009a. We first recall the definition of IND-PCA security given by Abdalla et al. [2], then give the definition of witness extractable encryption. Any (labeled) public-key encryption scheme is defined by three algorithms:

- $\mathsf{KeyGen}(1^\lambda)$ generates a key pair: a public key pk and a secret key sk;
- $\mathsf{Enc}(pk, \mathsf{label}, m, r)$ encrypts the message m under the key pk with label label, using the random coins r;
- $\mathsf{Dec}(sk, \mathsf{label}, C)$ decrypts the ciphertext C, using the secret key sk, label label. For any key pairs (pk, sk), any label label, any random coin r and any message m, it holds that $\mathsf{Dec}(sk, \mathsf{label}, \mathsf{Enc}(pk, \mathsf{label}, m, r)) = m$ with overwhelming probability.

Definition 1 (IND-PCA Security [2]**).** *A (labeled) public-key encryption scheme (KeyGen, Enc, Dec) is said to be indistinguishable plaintext checkable (IND-PCA) secure if the advantage of any PPT adversary A in the following interaction is negligible in the security parameter:*

1. *$\mathsf{KeyGen}(1^\lambda)$ outputs (pk, sk), A is given pk by the challenger.*
2. *A may adaptively query the decryption check oracle $\mathsf{DCheck}(\mathsf{label}, C, m)$, which answers whether the decryption of C under the label l is m.*
3. *At some point, A outputs a label label^* and two messages m_0 and m_1, and receives a challenge ciphertext $c^* = \mathsf{Enc}(pk, \mathsf{label}^*, m_b, r)$ for a uniformly chosen bit b.*
4. *A may continue to adaptively query the decryption check oracle $\mathsf{DCheck}(\mathsf{label}, C, m)$ with (label, C, m) such that $(\mathsf{label}, C) \neq (\mathsf{label}^*, C^*)$.*
5. *Finally, A outputs a bit b'. The advantage of A is denoted as $|Pr[b' = 1|b = 0] - Pr[b' = 1|b = 1]|$.*

2.3 Password-Based Authenticated Key Exchange

As the space limits, we omit the secure definition of BPR model [6] with mutual authentication which is added by [12]. For more details, please refer [12].

3 Only-One Lossy Encryption

As a basic tool of PAKE, we first propose the definition of only-one lossy encryption. And as a preparation of PAKE, we also give the instantiations based on DDH and LWE assumptions.

Informally, in the only-one lossy encryption, there is a branch hided in public key; With a trapdoor, there is a algorithm to decide which tag is equal to this branch; But without the trapdoor the branch is secure; If tag is equal to this branch the encryption works as normal and can decrypted with security key; If tag is not equal to this branch, the ciphertext of any two message is statistically indistinguishable. The following is the formal definition.

Definition 2 (Only-one lossy encryption). *The only-one lossy encryption consists a tuple of probability polynomial time (PPT) algorithms (*$\mathsf{NormSamp}$*,* KeyGen*,* Enc*,* Dec*,* Decide*).*

- $\mathsf{NormSamp}(\lambda)$*, given security parameters* λ*, outputs the public parameters* pp*, corresponding trapdoor* td *together with a normal branch* b *in tag space* D*.*
- $\mathsf{KeyGen}(b)$*, given the normal branch* b*, outputs* (pk, sk) *where* pk *is a public encryption key and* sk *is the corresponding decryption key on tag* b*.*
- $\mathsf{Enc}(pk, \mathsf{tag}, m, r)$*, given public key, and tag* $\mathsf{tag}\in D$*, message* $m \in \{0,1\}^l$ *and randomness* r*, outputs a ciphertext* c *of* m *on tag* tag*.*
- $\mathsf{Dec}(sk, c)$*, given a decryption key, ciphertext* c *on tag* b*, outputs a message* m *in* $\{0,1\}^l$*.*
- $\mathsf{Decide}(td, pk, \mathsf{tag})$*, given the trapdoor* td *generated by* $\mathsf{NormSamp}$*, public key with branch* b *and a tag* tag*, outputs* 1 *if* $\mathsf{tag} = b$*,* 0 *otherwise.*

Those algorithms satisfy the following secure requirements:

Correctness. *For all* $m \in \{0,1\}^l$ *and* pk *with normal branch* b*,*

$$Dec(sk, Enc(pk, b, m)) = m.$$

Lossiness. *For any* pk *with normal branch* b*, any tag* $\mathsf{tag} \neq b$*, and any pair of message* $m_0, m_1 \in \{0,1\}^l$*,there is*

$$\{Enc(pk, tag, m_0, r) | r \leftarrow \mathcal{R}\} =_s \{Enc(pk, tag, m_1, r) | r \in \mathcal{R}\}$$

Normal Branch Hidding. *For any the two distinct branches* (b, b^*) *in tag space, the two ensembles* $\{pk | (pk, sk) \leftarrow \mathsf{KeyGen}(b)\}$ *and* $\{pk | (pk, sk) \leftarrow \mathsf{KeyGen}(b^*)\}$ *are computational indistinguishable.*

Note that the only-one lossy encryptions has some property similar with dual mode cryptosystem given by [20], but has main differences. As their aim is universal composable secure oblivious transfer, in the dual mode cryptosystem, it requires two setup algorithms, and in one mode, there should be a algorithm to generate decryption key for ciphertext on all tag. We do not require this in only-one lossy encryption. There is another difference, the branch space in dual mode cryptosystem is $\{0, 1\}$, while in only-one lossy encryption the tag space is D.

In the following, we give the constructions based on DDH and LWE assumptions.

3.1 Only-One Lossy Encryption from DDH Assumption

Let $\mathbb{G}$ be a cyclic group of prime order p with a generator g. The DDH assumption is the following: for random generator $g, h \in \mathbb{G}$, and for independent $a, b, c \in Z_p$ the tuples (g, g^a, g^b, g^{ab}) abd (g, g^a, g^b, g^c) are computational indistinguishable. We now construct a only one lossy encryption scheme based on DDH assumption.

- $\mathsf{NormSamp}(\lambda)$, given security parameters λ, chooses $a \leftarrow Z_p$ and $b \leftarrow Z_p$, computes $h = g^a$. It outputs the public parameters $pp = (\mathbb{G}, g, h)$, corresponding trapdoor $td = a$ together with a normal branch b.
- $\mathsf{KeyGen}(b)$, given the normal branch b, chooses $r \leftarrow Z_p$, computes $g_1 = g^s, h_1 = h^s g^b$. It outputs $pk = (g_1, h_1)$ and $sk = s$.
- Enc, given public key (g_1, h_1), and tag $\mathsf{tag} \in Z_p$ and message $m \in Z_p$, chooses $r_1, r_2 \leftarrow Z_p$. It computes $c_1 = g^{r_1} h^{r_2}, c_2 = g_1^{r_1} (h_1/g^{\mathsf{tag}})^{r_2} \cdot m$, outputs a ciphertext $c = (c_1, c_2)$.
- Dec, given a decryption key s, ciphertext $c = (c_1, c_2)$ on tag b, outputs a message m by computing c_2/c_1^s.
- $\mathsf{Decide}(td, pk, \mathsf{tag})$, given the trapdoor $td = a$, public key with branch b and a tag tag, outputs 1 if $h_1/g_1^a = g^{\mathsf{tag}}$, 0 otherwise.

Theorem 1. *The above scheme is a only one lossy encryption under the DDH assumption on* $\mathbb{G}$.

As the space limit, we omit the formal proof.

3.2 Only-One Lossy Encryption from LWE Assumption

We recall the definition of LWE assumption.

Definition 3 (Learning With Errors (LWE)). *Let $m = m(n), q = q(n)$ be integers, and χ be a distribution on Z_q. Let $\boldsymbol{A} \leftarrow Z_q^{m \times n}$, $\boldsymbol{s} \leftarrow Z_q^n$, $\boldsymbol{e} \leftarrow \chi^m$, then LWE$(m, n, a, \chi)$ problem is to find $\boldsymbol{s}$, given $(\boldsymbol{A}, \boldsymbol{A}\boldsymbol{s}+\boldsymbol{e})$.*

This is the search version of the LWE problem. Regev [22] proved the security of LWE$(m, n, q, \mathcal{D}_{Z,\alpha q})$ when $m = poly(n)$ and $\alpha q \geq 2\sqrt{n}$.

Definition 4 (Decisional Learning With Errors (DLWE)). *Let $m = m(n), q = q(n)$ be integers, and χ be a distribution on Z_q. Let $\boldsymbol{A} \leftarrow Z_q^{m\times n}$, $\boldsymbol{s} \leftarrow Z_q^n$, $\boldsymbol{e} \leftarrow \chi^m$, then DLWE$(m, n, a, \chi)$ problem is that given $(\boldsymbol{A}, \boldsymbol{b})$, decide whether $\boldsymbol{b}$ is distributed by $\boldsymbol{As}+\boldsymbol{e}$ or chosen uniformly at random from $Z^n q$.*

The hardness of DLWE can be reduced to the hardness of the search version of LWE [22].

We now present the constructions of a only-one lossy encryption. This only-one lossy encryption is a modified and weaker version of dual-mode encryption based on LWE assumption proposed by Peikert et al. [20], which is also a Regev-like scheme [22]. The scheme uses Islossy algorithm in [13] to decide the normal branch.

- NormSamp(λ): chooses a random matrix $\mathbf{A} \leftarrow Z_q^{n\times m}$ uniformly random together with a trapdoor $t = \mathbf{S}$ as described by Gentry et al. [13]. It chooses k random vectors $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_k \leftarrow Z_q^m$. It generates a normal branch $b \in \{1, \cdots, k\}$ and outputs $(\mathbf{A}, \mathbf{v}_1, \cdots, \mathbf{v}_k)$ as CRS, $\mathbf{S}$ as trapdoor, and b as normal branch.
- KeyGen(b): given the normal branch $b \in \{1, \cdots, k\}$, it chooses a random $\mathbf{s} \in Z_q^n$ and errors vector $\mathbf{x} \leftarrow \chi^m$. It computes and outputs $pk = \mathbf{s}^T\mathbf{A} + \mathbf{x} + \mathbf{v}_b$.
- Enc(pk, tag, m): given public key, and tag $\mathsf{tag} \in \{1, \cdots, k\}$ and message $m \in \{0, 1\}$, it chooses a vector $\mathbf{e} \in Z^m$ according to $\mathcal{D}_{Z^m,r}$, where r is given in security analysis. It computes $\mathbf{u} = \mathbf{Ae}$ and $c = (pk - \mathbf{v}_{\mathsf{tag}})^T\mathbf{e} + m \cdot \lfloor 2/q \rfloor$ and outputs ciphertext $\mathbf{u}, c$.
- Dec$(sk, \mathbf{u}, c)$: given ciphertext $\mathbf{u}, c$, it computes $c - \mathbf{s}^T\mathbf{u}$ and outputs 0 if it is close to 0 than to $\lfloor q/2 \rfloor$, otherwise outputs 1.
- Decide$(\mathbf{S}, pk, \mathsf{tag})$: It computes $\mathbf{d} = pk - \mathbf{v}_{\mathsf{tag}}$. Run Islossy algorithm in [13] with input $(\mathbf{S}, \mathbf{A}, \mathbf{d})$, if Islossy outputs "lossy", tag is not the normal branch of pk, else it is.

The proof of the above only-one lossy encryption is implied by Lemmas 6.2, 6.3 and 6.6 in [13], and we just give sketch proof. The correctness of the decryption algorithm is guaranteed by Lemma 1. The correctness of the Decide algorithm is implied by Lemma 3. For any $\mathsf{tag} \neq b$, $pk - \mathbf{v}_{\mathsf{tag}} = \mathbf{s}^T\mathbf{A} + \mathbf{x} + \mathbf{v}_b - \mathbf{v}_{\mathsf{tag}}$. As both $\mathbf{v}_b$ and $\mathbf{v}_{\mathsf{tag}}$ are independent and randomly chosen, $\mathbf{v}_b - \mathbf{v}_{\mathsf{tag}}$ is randomly chosen, thus $\mathbf{s}^T\mathbf{A} + \mathbf{x} + \mathbf{v}_b - \mathbf{v}_{\mathsf{tag}}$ is randomly chosen. Take $\mathbf{s}^T\mathbf{A} + \mathbf{x} + \mathbf{v}_b - \mathbf{v}_{\mathsf{tag}}$ to be $\mathbf{p}$ in Lemma 2, we have the lossy property. At last, the normal branch hidding is implied by replacing $\mathbf{s}^T\mathbf{A} + \mathbf{x}$ with a random element.

4 New Framework of PAKE

We now present the new framework for PAKE from only-one lossy encryption and IND-PCA secure encryption scheme. In this construction, the following primitives are required: Let (NormSamp, KeyGen, Enc, Dec, Decide) be the only-one lossy encryption and $CENC$ = (CKeyGen, CEnc, CDec) be a lable-based IND-PCA secure encryption. (For more information of label-based IND-PCA

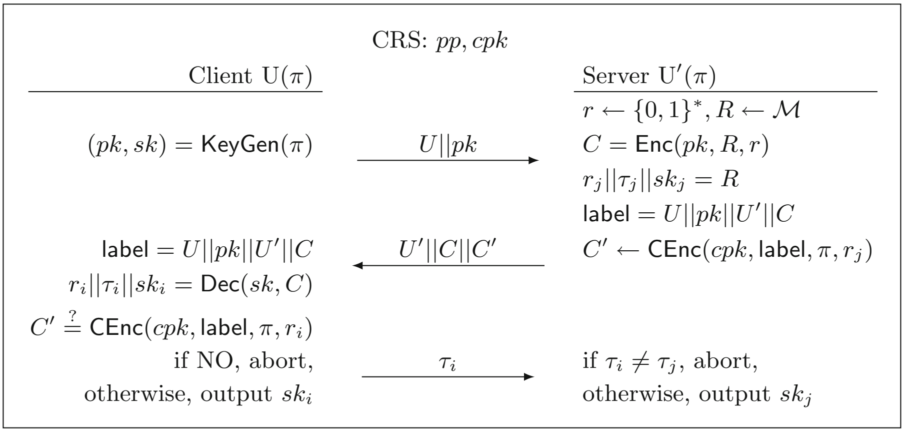
CRS: pp, cpk
Client U(π)
Server U$'$(π)
$r \leftarrow \{0,1\}^*, R \leftarrow \mathcal{M}$
$(pk, sk) = \mathsf{KeyGen}(\pi)$
$U||pk$
$C = \mathsf{Enc}(pk, R, r)$
$r_j||\tau_j||sk_j = R$
$\mathsf{label} = U||pk||U'||C$
$\mathsf{label} = U||pk||U'||C$
$U'||C||C'$
$C' \leftarrow \mathsf{CEnc}(cpk, \mathsf{label}, \pi, r_j)$
$r_i||\tau_i||sk_i = \mathsf{Dec}(sk, C)$
$C' \overset{?}{=} \mathsf{CEnc}(cpk, \mathsf{label}, \pi, r_i)$
if NO, abort,
τ_i
if $\tau_i \neq \tau_j$, abort,
otherwise, output sk_i
otherwise, output sk_j

Fig. 1. New framework of PAKE

secure encryption, please refer [2]) Let the branch space of lossy encryption be equal to the password space and they both do not include 0. The protocol is displayed in Fig. 1.

Initialization: The CRS consists of public parameters pp generated by $\mathsf{NormSamp}$, and the public keys cpk of IND-CPA secure encryption generated by $\mathsf{CKeyGen}$.

Protocol execution. Figure 1 demonstrates the execution of the protocol.

Stage 1: When a client U (holds π) wants to authenticate to the server U' (holds π), it generate the public key pk of only-one lossy encryption from $(pk, sk) \leftarrow \mathsf{KeyGen}(\pi)$, and sends $U||pk$ to U'.

Stage 2: On receiving the message $U||pk$, U' randomly chooses randomness r and a random message R in plaintext space $\mathcal{M}$, and computes ciphertext $C = \mathsf{Enc}(pk, R, r)$ with randomness r. It parse R into three bit strings r_j, τ_j, sk_j. It sets $\mathsf{label} = U||pk||U'||C$, encrypts π as $C' \leftarrow \mathsf{CEnc}(cpk, \mathsf{label}, \pi, r_j)$ with randomness r_j. Then U' sends $U'||C||C'$ to U.

Stage 3: On receiving the message $U'||C||C'$, user U decrypt C using sk and decomposes massage as $r_i||\tau_i||sk_i \leftarrow \mathrm{Dec}[sk, C]$. It sets $\mathsf{label} = (U||pk||U'||C)$ and checks $C' \overset{?}{=} \mathsf{CEnc}(cpk, \mathsf{label}, \pi, r_i)$. If no, aborts else sends τ_i to U' and outputs sk_i which means that U' has successfully authenticated to U.

Stage 4: On receiving the message τ_i, U' checks that if $\tau_i = \tau_j$ or not. If $\tau_i \neq \tau_j$, U' aborts, otherwise U has successfully authenticated to U' and U' outputs sk_j.

If both parties are honest and there is no adversarial interference, then it guarantees that $r_i||\tau_i||sk_i = r_j||\tau_j||sk_j$. Both parties will accept and output the same session key.

Theorem 2. *If the underling encryption scheme are only-one lossy encryption and IND-PCA secure encryption scheme, the PAKE in Fig. 1 is secure in the BPR model.*

As the space limit, we omit the proof. Please refre the full paper for the formal proof.

Instantiations. We instantiate the framework in Sect. 3 based on DDH assumption and LWE assumption. Although, in case of DDH, we get a scheme with communication complexity of 8 group elements which has one more groups than the scheme in [12]. Our framework can be instantiated based on LWE assumption, which the GK-PAKE can not be instantiated based on lattice assumptions. Based on LWE assumption, the only-one lossy encryption is the one give in Sect. 3.2, and the IND-PCA secure encryption can be that is IND-CCA secure given by Gentry et al. [13] or that given by Micciancio and Peikert [18].

5 Conclusion

We give a framework of PAKE, which consists of only-one lossy encryption and IND-PCA secure encryption. Our framework can be instantiated from lattice assumptions. Only-one lossy encryption can be constructed based DDH and LWE assumptions. Although the instantiation of our framework based on DDH assumption does not improve efficiency of precious works, our framework provides more easier and elegant way to construct PAKE from lattice assumptions.

Acaknowledgement. Haiyang Xue is supported by the Foundation of Science and Technology on Communication Security Laboratory (9140C110206150C11049), National Natural Science Foundation of China (No. 61602473, 61502480, 61672019) and National Cryptography Development Fund MMJJ20170116. Bao Li is supported by the Foundation of Science and Technology on Communication Security Laboratory (9140C110206150C11049) and the National Natural Science Foundation of China (No. 61379137).

References

1. Abdalla, M., Pointcheval, D.: Simple password-based encrypted key exchange protocols. In: Menezes, A. (ed.) CT-RSA 2005. LNCS, vol. 3376, pp. 191–208. Springer, Heidelberg (2005). doi:10.1007/978-3-540-30574-3_14
2. Abdalla, M., Benhamouda, F., Pointcheval, D.: Public-key encryption indistinguishable under plaintext-checkable attacks. In: Katz, J. (ed.) PKC 2015. LNCS, vol. 9020, pp. 332–352. Springer, Heidelberg (2015). doi:10.1007/978-3-662-46447-2_15
3. Bellare, M., Hofheinz, D., Yilek, S.: Possibility and impossibility results for encryption and commitment secure under selective opening. In: Joux, A. (ed.) EUROCRYPT 2009. LNCS, vol. 5479, pp. 1–35. Springer, Heidelberg (2009). doi:10.1007/978-3-642-01001-9_1

4. Bellovin, M., Merritt, M.: Encrypted key exchange: Password-based protocols secure against dictionary attacks. In: 1992 IEEE Symposium on Security and Privacy, pp. 72–84 (1992)
5. Boyko, V., MacKenzie, P., Patel, S.: Provably secure password-authenticated key exchange using Diffie-Hellman. In: Preneel, B. (ed.) EUROCRYPT 2000. LNCS, vol. 1807, pp. 156–171. Springer, Heidelberg (2000). doi:10.1007/3-540-45539-6_12
6. Bellare, M., Pointcheval, D., Rogaway, P.: Authenticated key exchange secure against dictionary attacks. In: Preneel, B. (ed.) EUROCRYPT 2000. LNCS, vol. 1807, pp. 139–155. Springer, Heidelberg (2000). doi:10.1007/3-540-45539-6_11
7. 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). doi:10.1007/3-540-46035-7_4
8. Canetti, R., Goldreich, O., Halevi, S.: The random oracle methodology, revisited. J. ACM **51**(4), 557–594 (2004)
9. Canetti, R., Dachman-Soled, D., Vaikuntanathan, V., Wee, H.: Efficient password authenticated key exchange via oblivious transfer. In: Fischlin, M., Buchmann, J., Manulis, M. (eds.) PKC 2012. LNCS, vol. 7293, pp. 449–466. Springer, Heidelberg (2012). doi:10.1007/978-3-642-30057-8_27
10. Goldreich, O., Lindell, Y.: Session-key generation using human passwords only. In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 408–432. Springer, Heidelberg (2001). doi:10.1007/3-540-44647-8_24
11. Gennaro, R., Lindell, Y.: A framework for password-based authenticated key exchange. In: Biham, E. (ed.) EUROCRYPT 2003. LNCS, vol. 2656, pp. 524–543. Springer, Heidelberg (2003). doi:10.1007/3-540-39200-9_33
12. Groce, A., Katz, J.: A new framework for efficient password-based authenticated key exchange. In: ACM Conference on Computer and Communications Security, pp. 516–525 (2010)
13. Gentry, C., Peikert, C., Vaikuntanathan, V.: Trapdoors for hard lattice and new cryptographic constructions. In: STOC, pp. 197–206 (2008)
14. Jiang, S., Gong, G.: Password based key exchange with mutual authentication. In: Handschuh, H., Hasan, M.A. (eds.) SAC 2004. LNCS, vol. 3357, pp. 267–279. Springer, Heidelberg (2004). doi:10.1007/978-3-540-30564-4_19
15. Kol, G., Naor, M.: Cryptography and game theory: designing protocols for exchanging information. In: Canetti, R. (ed.) TCC 2008. LNCS, vol. 4948, pp. 320–339. Springer, Heidelberg (2008). doi:10.1007/978-3-540-78524-8_18
16. Katz, J., Ostrovsky, R., Yung, M.: Efficient password-authenticated key exchange using human-memorable passwords. In: Pfitzmann, B. (ed.) EUROCRYPT 2001. LNCS, vol. 2045, pp. 475–494. Springer, Heidelberg (2001). doi:10.1007/3-540-44987-6_29
17. Katz, J., Vaikuntanathan, V.: Smooth projective hashing and password-based authenticated key exchange from lattices. In: Matsui, M. (ed.) ASIACRYPT 2009. LNCS, vol. 5912, pp. 636–652. Springer, Heidelberg (2009). doi:10.1007/978-3-642-10366-7_37
18. Micciancio, D., Peikert, C.: Trapdoors for lattices: simpler, tighter, faster, smaller. In: Pointcheval, D., Johansson, T. (eds.) EUROCRYPT 2012. LNCS, vol. 7237, pp. 700–718. Springer, Heidelberg (2012). doi:10.1007/978-3-642-29011-4_41
19. Paillier, P., Pointcheval, D.: Efficient public-key cryptosystems provably secure against active adversaries. In: Lam, K.-Y., Okamoto, E., Xing, C. (eds.) ASIACRYPT 1999. LNCS, vol. 1716, pp. 165–179. Springer, Heidelberg (1999). doi:10.1007/978-3-540-48000-6_14

20. Peikert, C., Vaikuntanathan, V., Waters, B.: A framework for efficient and composable oblivious transfer. In: Wagner, D. (ed.) CRYPTO 2008. LNCS, vol. 5157, pp. 554–571. Springer, Heidelberg (2008). doi:10.1007/978-3-540-85174-5_31
21. Peikert, C., Waters, B.: Lossy trapdoor functions and their applications. In: Ladner, R.E., Dwork, C. (eds) STOC 2008, pp. 187-196 (2008)
22. Rege, O.: On lattices, learning with errors, random linear codes, and cryptography. J. ACM **56**(6), 1–40 (2009)
23. Wang, D., Jian, G., Huang, X., Wang, P.: Zipfs law in passwords. ACM Trans. Info. Syst. Sec. **1**(1), 33 pages (2015). Article 1