The ISC Int'l Journal of Information Security

January 2019, Volume 11, Number 1 (pp. 75–85)

http://www.isecure-journal.org

# A New Ring-Based SPHF and PAKE Protocol on Ideal Lattices

Amir Hassani Karbasi [1], Reza Ebrahimi Atani [2,*], and Shahabaddin Ebrahimi Atani [1]

[1] *Department of Mathematics, University of Guilan, Rasht, Iran*

[2] *Department of Computer Engineering, University of Guilan, Rasht, Iran*

ARTICLE INFO.

*Article history:*
**Received:** 10 December 2017
**Revised:** 9 December 2018
**Accepted:** 19 December 2018
**Published Online:** 30 January 2019

*Keywords:*
Lattice-based Cryptography, Ring-LWE, SPHF, PAKE.

ABSTRACT

*Smooth Projective Hash Functions* (SPHFs) as a specific pattern of zero knowledge proof system are fundamental tools to build many efficient cryptographic schemes and protocols. As an application of SPHFs, *Password-Based Authenticated Key Exchange* (PAKE) protocol is well-studied area in the last few years. In 2009, Katz and Vaikuntanathan described the first lattice-based PAKE using the Learning With Errors (LWE) problem. In this work, we present a new efficient *ring-based* smooth projective hash function "(Ring-SPHF)" using Lyubashevsky, Peikert, and Regev's dual-style cryptosystem based on the Learning With Errors over Rings (Ring-LWE) problem. Then, using our ring-SPHF, we propose an efficient password-based authenticated key exchange "(Ring-PAKE)" protocol over *rings* whose security relies on ideal lattice assumptions.



## 1 Introduction

During the past few years, lattice-based cryptography has been known for its numerous constructions and cryptographic protocols beside strong security proofs, resistance to quantum attacks, flexibility for fully homomorphic encryption [1] and efficiency with competitive performance among classical schemes which are established by *integer factoring problem* (IFP) and *discrete logarithm problem* (DLP). In particular, the learning with errors over rings (ring-LWE) [2, 3], as a lattice problem, is used for development of secure and efficient lattice-based primitives based on rings. However, there still has been little work on developing ring-based schemes and protocols in *real-word* applications using ideal lattices. In addition, the ring-LWE is the core of the security of cryptographic protocols on ideal lattices [1, 2, 18, 25, 36, 38]. Cramer and Shoup introduced a primitive, called "Smooth Projective Hash Function" (SPHF) [4], in order to obtain hash proof systems for IND-CCA security. Gennaro and Lindell proposed a generalized SPHF [5] for its many attractive properties and purposes such as implicit designated-verifier proofs of membership [6, 8]. On the other hand, there is a useful application of SPHF, called "Password-Based Authenticated Key Exchange" (PAKE) protocol. It was presented by Katz, Ostrovsky, and Yung [9] and also Gennaro and Lindell [5] which is known as the KOY-GL paradigm.

By a common password for the parties of a specific key exchange, a PAKE protocol is established. A PAKE provides security against *offline* dictionary attacks (formally, Bellare-Pointcheval-Rogaway (BPR) model [10]), and this setting, even with low-entropy passwords, prevents from users impersonation. Moreover, for a PAKE, a secure server equipped with password-based authentication can provide security against *online* dictionary attacks such that an attacker tries to impersonate a user using each possible pass-

* Corresponding author.
Email addresses: karbasi@phd.guilan.ac.ir (A. Hassani Karbasi), rebrahimi@guilan.ac.ir (R. Ebrahimi Atani), ebrahimi@guilan.ac.ir(S. Ebrahimi Atani)

ISSN: 2008-2045 

word. PAKE protocols, as a rare cryptographic primitive for real-word applications like the Internet, have been standardized [12] and widely deployed [13].

Recent advances in PAKE protocols, especially the improvement of password-based protocols, put them in a superior position for researchers. A *hybrid* model based on password and public keys is described in [14, 15]. A *password-only* model based on only a password with heuristic security is initiated in [16]. In particular, PAKEs with provable security in the random oracle model and formal models are shown in [10, 17, 19, 20]. The first *inefficient* PAKE in the standard model is presented in [19] and its improvement with weaker notion of security is shown in [21] but similarly it is impractical. The first *efficient* PAKE in the standard model with provable security is proposed in [9] and its variants are given in [22–24, 26, 27]. A *Common Reference String* (CRS) is needed for these protocols and a PAKE in the CRS model is presented in [28].

Lattice-based cryptography and its efficient protocols are appealing. The use of lattice assumptions and recognized worst-case to average-case connections between lattice problems for proof of security have put lattices in excellent position in practice. Until recently, constructing SPHF from lattice assumptions based on LWE and SIS problems has remained open. The only exception and the first PAKE using SPHFs in the standard model based on lattices is proposed in [29]. In this protocol, first, an approximate SPHF is constructed, and then, a PAKE is derived from it. The most technically effortful aspect of this protocol is the designing of a lattice-based IND-CCA encryption scheme with an associated approximate SPHF. However, this development has a critical downside: it only works for a specially appointed dialect of ciphertexts. Concretely, the corresponding decryption procedure needs to be tweaked, now requiring $q$ trapdoor inversion attempts, where $q$ is the modulus of theof the underlying Learning With Errors (LWE) problem [40]. In this paper, we have investigated this issue.

As we mentioned earlier, far less consideration has been paid to key exchange protocols for real-world communications from ideal lattice assumptions and as we can see almost all standards for cryptographic primitives are still designed around classical mechanisms such as RSA [30] and Diffie-Hellman [31]. However, some recent proposals such as [38–40], are promising. These methods are generally based on random oracles and standard proofs. Precisely, [38, 40] are based on standard model and [39] is based on ROM. The random oracle model is a heuristic approach that assumes the existence of a truly random function to which all parties involved in a protocol, good and bad alike, have access. Since in reality no such function exists, random oracles are instantiated with hash functions and one heuristically assumes that a hash function behaves good enough to be a replacement for random oracles. Random oracles are nice as they allow proving security of protocols while they are still practically efficient. Since there are theoretical results showing that there are protocols that are secure in the random oracle model but trivially insecure whenever the random oracle is instantiated with any hash function, standard model constructs, i.e., constructs that do not rely on random oracles, are nicer from a theoretical perspective. Standard model means that the protocols only rely on standard cryptographic assumptions (DDH, CDH, ...) in their proofs.

### 1.1 Our Contributions

To the best of our knowledge, by now building ring-based SPHF and ring-based PAKE based on the ring-LWE are open questions. Fortunately, in certain settings we can generalize existing classical schemes to lattice-based mechanisms without loss of security since lattice-based problems have very various mathematical properties than IFP and DLP. In this work, using ideas and modifications of [2–5, 7, 9, 11, 29], we give efficient ideal lattice-based schemes for fundamental asymmetric tasks such as ring-based smooth projective hash function (ring-SPHF) and password-based authenticated key exchange protocol (ring-PAKE) that are suitable for real-word applications like the Internet. Our proposals can all be proved secure (in the standard model) based on the believed difficulty of the ring-LWE problem.

### 1.2 Organization

The rest of this paper is formed as follows.

- In Section 2, we recall the necessary mathematical and cryptographic background and we give some supporting lemmas with respect to the ring-LWE problem.
- In Section 3, we propose the details of our new ring-SPHF from ideal lattices for constructing our ring-PAKE.
- In Section 4, we present and analyze our new secure 3-round ring-PAKE using our ring-SPHF.
- Section 5 concludes the paper.

## 2 Preliminaries

For $l \in \mathbb{Z}^+ \cup \{0\}$, we assume $[l]$ denote the set $\{0, 1, ..., l-1\}$. For $k \in \mathbb{R}$, we define $\lfloor k \rceil = \lfloor k+1/2 \rfloor \in \mathbb{Z}$. For an integer $q \geqslant 1$, we define by $\mathbb{Z}_q$ the quotient ring $\mathbb{Z}/q\mathbb{Z}$, that is, the ring of cosets $k + q\mathbb{Z}$ with the induced addition and multiplication operations. For any $\bar{x} \in \mathbb{R}/\mathbb{Z}$, we assume $[[\bar{x} \in \mathbb{R}]]$ denote the unique

representative $x \in (\bar{x} + \mathbb{Z}) \cap [-1/2, 1/2)$. Moreover, for $\bar{x} \in \mathbb{Z}_q$, we let $[[\bar{x}]]$ be the unique representative $x \in (\bar{x} + q\mathbb{Z}) \cap [-q/2, q/2)$. Furthermore, $[[.]]$ can be extended entrywise to vectors and matrices. By *rad(a)*, we denote the radical of a positive integer $a$, i.e., it is the product of all primes dividing $a$. For a vector $\boldsymbol{v}$ over $\mathbb{R}$ or $\mathbb{C}$, the $l_2$ norm is defined as $||\boldsymbol{v}||_2 = (\sum_i |v_i|^2)^{1/2}$, and the $l_\infty$ norm is defined as $||\boldsymbol{v}||_\infty = \max_i |v_i|$. The largest singular value and the smallest singular value for an $n$-by-$n$ matrix $M$ are shown by $s_1(M)$ and $s_n(M)$, respectively. Powerful basis, power basis, decoding basis, principal and fractional ideal are defined in [32].

### 2.1 Ring-LWE

The *learning with errors over rings* (ring-LWE) problem and its toolkit were introduced by Lyubashevsky, Peikert, and Regev in [2, 3], respectively as a generalization of the *learning with errors* (LWE) problem [32]. Here, we recall the discretized (normal) form of the ring-LWE probability distribution and decision/search version on ideal lattices, such that all elements are from the cyclotomic ring $R$ or $R_q = R/qR$, and the discretized error distribution is used for the secret sampling.

**Definition 1 (Ring-LWE Distribution, [33]).** For an $s \in R$ and a distribution $\chi$ over $R$, a sample from the *ring-LWE* distribution $A_{s,\chi}$ over $R_q \times R_q$ is generated by choosing $a \leftarrow R_q$ uniformly at random, choosing $e \leftarrow \chi$, and outputting $(a, b = a.s + e)$.

**Definition 2 (Decisional Ring-LWE, [33]).** In the "decision" version of the ring-LWE problem *(R-DLWE$_{q,\chi}$)* we want to distinguish independent samples between $A_{s,\chi}$, where $s \leftarrow \chi$ is sampled once and for all, and the same number of "uniformly random" independent samples from $R_q \times R_q$ with non-negligible advantage.

**Theorem 1** ([2]). *Let $R$ be the $m$th cyclotomic ring with dimension $n = \varphi(m)$. Let $\alpha = \alpha(n) < \sqrt{\log n}/n$, and let $q = q(n)$, $q = 1 \bmod m$ be a* Poly*(n)-bounded prime such that $\alpha q \geqslant \omega(\sqrt{\log n})$. There is a* Poly*(n)-time quantum reduction from $\tilde{O}(\sqrt{n}/\alpha)$-approximate* SIVP *(or* SVP*) on ideal lattices in $R$ to solving* R-DLWE$_{q,\chi}$ *given only $l - 1$ samples, where $\chi = \lfloor \psi \rceil$ and $\psi$ is the* Gaussian *distribution $(\hat{m}/g).D_{\zeta q}$ for $\zeta = \alpha.(nl/\log(nl))^{1/4}$.*

Notice that, there is the search (computational) version of the ring-LWE in order to better parameters in applications because it is hard for the fixed error distribution $\psi = (\hat{m}/g).D_{\alpha q}$, where $\alpha q \geqslant \omega(\sqrt{\log n})$. In the search problem we want to find the secret $s$ given arbitrary many ring-LWE samples [2].

In ideal lattice-based constructions, the behavior of *errors* is analyzed by the notion of *subgaussian* random variables [33]. For any $\gamma \geqslant 0$, a random variable $X$ (or its distribution) over $\mathbb{R}$ is said to be $\gamma$-subgaussian with parameter $r > 0$, if for all $y \in \mathbb{R}$, the (scaled) moment-generating function satisfies:

$$\mathbb{E}[\exp(2\pi y X)] \leqslant \exp(\gamma).\exp(\pi r^2 y^2).$$

For all $y \geqslant 0$, by Markov's inequality, $X$ has Gaussian tails:

$$\Pr[|X| \geqslant y] \leqslant 2\exp(\gamma - \pi y^2/r^2).$$

For $\mathbb{E}[X] = 0$ and $|X| \leqslant B$, $B$-bounded centered random variable $X$, we have $X$ as a 0-subgaussian with parameter $B\sqrt{2\pi}$.

The concept of subgaussianity can be extended to vectors. In particular, a random real vector $X$ is said to be $\gamma$-subgaussian with parameter $r$ if for all real unit vectors $u$, the random variable $< u, X > \in \mathbb{R}$ is $\gamma$-subgaussian with parameter $r$. In general, we can take $X$ and $u$ from any real inner product space.

We now present some technical lemmas and results with respect to the ring-LWE problem that will be used to prove correctness, smoothness, and security of our ring-SPHF and ring-PAKE. Notice that for a positive integer index $m$, $K = \mathbb{Q}(\zeta_m)$ and $R = \mathbb{Z}[\zeta_m] \subset K$ are the $m$th cyclotomic number field and ring, respectively where $\zeta_m$ is an abstract element with order $m$. (See [2] for more details about algebraic number theory background, special properties of cyclotomic number fields, and Gaussians on ideal lattices and ring-LWE problem.)

**Lemma 1** (Lemma 2.8 from [3]). *For any $n$-dimensional lattice $\boldsymbol{L}$ and $s > 0$, a point sampled from discrete Gaussian distribution $D_{\boldsymbol{L},s}$ has Euclidean norm at most $s\sqrt{n}$, except with probability at most $2^{-2n}$.*

**Lemma 2** (Lemma 2.9 from [3]). *There is an efficient algorithm that samples to within* negl(n) *statistical distance of $D_{\boldsymbol{L}+c,s}$, given $c \in H$, a basis $B$ of $\boldsymbol{L}$, and a parameter $s \geqslant \max_j ||\tilde{b}_j||.\omega(\sqrt{\log n})$, where $\tilde{B} = \{\tilde{b}_j\}$ is the* Gram-Schmidt *orthogonalization of $B$ and the subspace $H \subseteq \mathbb{R}^{s_1} \times \mathbb{C}^{2s_2}$ for some numbers $s_1 + 2s_2 = n$ is defined as:*

$$H = \{(x_1, ..., x_n) \in \mathbb{R}^{s_1} \times \mathbb{C}^{2s_2} : x_{s_1+s_2+j} = \bar{x}_{s_1+j}; \forall j \in [s_2]\} \subseteq \mathbb{C}^n.$$

*such that $H$ is isomorphic to $\mathbb{R}^n$ as an inner product space.*

**Lemma 3** (Lemma 2.23 from [3]). *Let $p$ and $q$ be positive coprime integers, and $\lfloor . \rceil$ be a valid discretization to (cosets of) $pR^\vee$, where $R^\vee \subset K$ is the dual ideal of the cyclotomic ring $R = \mathbb{Z}[X]/\phi_p(X)$ such that $pR^\vee \subseteq R \subseteq R^\vee$, with $pR^\vee \approx R$ for pth cyclotomic polynomial $\phi_p(X)$. There exists an optimal transformation that on*

*input $w \in R_p^\vee$ and a pair in $(a', b') \in R_q \times K_\mathbb{R}/qR^\vee$, outputs a pair $(a = pa' \bmod qR, b) \in R_q \times R_q^\vee$, where $K_\mathbb{R} = K \otimes_\mathbb{Q} \mathbb{R}$ is isomorphic to $H$, with the following guarantees: if the input pair is uniformly distributed then so is the output pair; and if the input pair is distributed according to the* ring-LWE *distribution $A_{s,\psi}$ for some (unknown) $s \in R^\vee$ and distribution $\psi$ over $K_\mathbb{R}$, then the output pair is distributed according to $A_{s,\chi}$, where $\chi = \lfloor p.\psi \rceil_{w+pR^\vee}$.*

**Lemma 4** (Lemma 2.24 from [3]). *Let $p$ and $q$ be positive coprime integers, $\lfloor . \rceil$ be a valid discretization to (cosets of) $pR^\vee$, and $w$ be an arbitrary element in $R_p^\vee$. If* R-DLWE$_{q,\psi}$ *is hard given some number $l$ of samples, then so is the variant of* R-DLWE$_{q,\psi}$ *in which the secret is sampled from $\chi := \lfloor p.\psi \rceil_{w+pR^\vee}$, given $l-1$ samples.*

**Claim 1** (Claim 4.2 from [3]). *The length of each element $p_j$ of $\overrightarrow{\boldsymbol{p}}$ in $l_\infty$ norm is $||p_j||_\infty = 1$, and in $l_2$ norm is $||p_j||_2 = \sqrt{\varphi(m)} = \sqrt{n}$, where $\overrightarrow{\boldsymbol{p}}$ is the* powerful $\mathbb{Z}$*-basis of $R$.*

**Lemma 5** (Lemma 6.2 from [3]). *The spectral norm of $\overrightarrow{\boldsymbol{d}}$ is $s_1(\overrightarrow{\boldsymbol{d}}) = \sqrt{rad(m)/m}$, where $\overrightarrow{\boldsymbol{d}}$ is the* decoding $\mathbb{Z}$*-basis of $R^\vee$.*

**Lemma 6** (Lemma 6.5 from [3]). *Let $I = (R^\vee)^k$ for some $k \geqslant 1$, let $a \in I$ and write $a =< \hat{m}^{1-k}\overrightarrow{\boldsymbol{d}}, \boldsymbol{a} >$ for some integral coefficient vector $\boldsymbol{a}$, and let $q \geqslant 1$ be an integer. If every coefficient $a_j \in [-q/2, q/2)$, then $[[a \bmod qI]] = a$. In particular, if every $a_j$ is $\gamma$-subgaussian with parameter $s$, then $[[a \bmod qI]] = a$ except with probability at most $2n.\exp(\gamma - \pi q^2/(2s)^2)$.*

**Lemma 7** (Lemma 6.6 from [3]). *Let $I = (R^\vee)^k$ for some $k \geqslant 1$, and let $a \in I$.*

- *Writing $a =< \hat{m}^{1-k}\overrightarrow{\boldsymbol{d}}, \boldsymbol{a} >$ for some integral vector $\boldsymbol{a}$, we have that every $|a_j| \leqslant \hat{m}^{k-1}\sqrt{n}.||a||_2$.*
- *If $a$ is $\gamma$-subgaussian with parameter $s$, and $b \in (R^\vee)^l$ for some $l \geqslant 0$ is arbitrary, then writing $a.b =< \hat{m}^{1-k-l}\overrightarrow{\boldsymbol{d}}, \boldsymbol{c} >$ for some integral vector $\boldsymbol{c}$, we have that every $c_j$ is $\gamma$-subgaussian with parameter $\hat{m}^{k+l-1}||b||_2.s$.*

**Corollary 1** (Leftover hash lemma, Corollary 7.5 from [3]). *Let $R$ be the ring of integers in the $m$th cyclotomic number field $K$ of degree $n$, and $q \geqslant 2$ an integer. For positive integers $k \leqslant l \leqslant \mathrm{Poly}(n)$, let $A = [I_{[k]}|\bar{A}] \in (R_q)^{[k]\times[l]}$, where $I_{[k]} \in (R_q)^{[k]\times[k]}$ is the identity matrix and $\bar{A} \in (R_q)^{[k]\times[l-k]}$ is uniformly random. Then, with probability $1 - 2^{-\Omega(n)}$ over the choice of $\bar{A}$, the distribution of $A\overrightarrow{\boldsymbol{x}} \in R_q^{[k]}$ where each coordinate of $\overrightarrow{\boldsymbol{x}} \in R_q^{[l]}$ is sampled from a discrete Gaussian distribution of parameter $r > 2n.q^{(k/l)+2/(nl)}$ over $R$, satisfies that the probability of each of the $q^{nk}$ possible outcomes is in the interval $(1 \pm 2^{-\Omega(n)})q^{-nk}$, and in particular, is within statistical distance $2^{-\Omega(n)}$ of uniform distribution over $R_q^{[k]}$.*

We assume the distance of a vector $z \in R_q$ from the lattice $\boldsymbol{L}(A)$ is denoted by $dist(z, \boldsymbol{L}(A))$. Lemma 8 shows that for most matrices $A \in R_q^{\{1,\dots,l\}}$, the fraction of vectors $z \in R_q$ that are *very close* to $\boldsymbol{L}(A)$ is *very small*. We give outline of the proof of Lemma 8 for arbitrary lattices and using Corollary 1 this lemma and its proof can be adapted quite well to the ring-LWE case.

**Lemma 8** (Adapted from [29]). *Let $n, q$, and $m$ be integers such that $m \geqslant n\log q$. Let $A \in \mathbb{Z}_q^{m\times n}$, $z \in \mathbb{Z}_q^m$, and $e \leftarrow D_{\mathbb{Z}^m,s}$. For all but a negligible portion of matrices $A$:*

$$\Pr_{z\leftarrow\mathbb{Z}_q^m}[dist(z, \boldsymbol{L}(A)) \leqslant \sqrt{q}/4] \leqslant q^{-(m+n)/2}.$$

*Proof.* Let $d$ be a free variable that will be optimized at the end of the proof. We want to find an upper bound for:

$$\Pr_{A,z}[dist(z, \boldsymbol{L}(A)) \leqslant d]$$

This may be re-written as:

$$\Pr_{A,z}[\exists s \in \mathbb{Z}_q^n, \exists e \in \mathbb{Z}^m \text{ with } ||e|| \leqslant d : z = A * s + e \bmod q].$$

By the union bound, this is smaller than:

$$\sum_s \sum_e \Pr_{A,z}[z = A * s + e \bmod q] =$$
$$\sum_s \sum_e q^{(-m)} \approx q^{(n-m)}.d^m/(\sqrt{m})^m.$$

In the last step, we use a bound on the number of integer points in the ball of radius $d$. This is indeed small for the $d$. □

Moreover, for a matrix $A \in R_q^{\{1,\dots,l\}}$ and a vector $z \in R_q$, we assume the statistical distance between the uniform distribution on $R_q$ and the distribution of $(\overrightarrow{\boldsymbol{e}}A, \overrightarrow{\boldsymbol{e}}z)$ is denoted by $\Delta_s(A, z)$, where $\overrightarrow{\boldsymbol{e}} = (e_1, ..., e_l) \in (R^\vee)^{\{1,\dots,l\}}$. Lemma 9 shows a converse statement of Lemma 8. That is, if $z$ and all its non-zero multiples are far from the ideal lattice $\boldsymbol{L}(A)$, then $\overrightarrow{\boldsymbol{e}}A$ does not reveal any information about $\overrightarrow{\boldsymbol{e}}z$. More generally, given $\overrightarrow{\boldsymbol{e}}A$, then $\overrightarrow{\boldsymbol{e}}z$ is statistically close to the random.

**Lemma 9.** *Let $R, n, q, k, l$, and $A$ be as in Corollary 1. For small enough $d$, if $z \in R_q$ is such that for all non-zero constant polynomial $a \in R_q$, $dist(az, \boldsymbol{L}(A)) \geqslant d$, then $\Delta_s(A, z) \leqslant$ negl(n).*

*Proof.* Let $B = [A|z]$, that is, we attach the vector $z$ and all its multiples to the ideal lattice $\boldsymbol{L}(A)$. By a generalization of Corollary 1, the distribution of $B\overrightarrow{\boldsymbol{x}} \in R_q$ is within statistical distance $2^{-\Omega(n)}$ of uniform over $R_q$, where each coordinate of $\overrightarrow{\boldsymbol{x}}$ is drawn from a discrete Gaussian distribution of parameter $s > 2n.q^{k/l+2/(nl)}$ over $R$, then $\Delta_s(A, z) \leqslant$ negl(n). □

### 2.2 Dual-Style Cryptosystem

The *dual* LWE encryption was first introduced in [34], and its ring-based variant is presented in [3] which is called *dual-style cryptosystem*. In these two dual systems, the public key is statistically close to uniform, whereas ciphertexts are only pseudorandom and have unique encryption randomness, i.e., the systems have dual properties to LWE-based cryptosystem [32]. We know by Claim 1 [32], the elements of $R$ with the powerful basis $\vec{\boldsymbol{p}}$ have maximum length $\sqrt{n}$, so we can use the algorithm from Lemma 2 for sampling, that is, the discrete Gaussian distribution $D_{R,r}$ for some $r \geqslant \sqrt{n}.\omega(\sqrt{\log n})$ is used in the key generation algorithm. Now let $l \geqslant 2$ and let principal and fractional ideal $(R^{\vee})^k =< t^{-k} >$, the dual-style cryptosystem is defined as follows.

- ***Gen*$(\mathbf{1^l})$:** choose $a_0 = -1 \in R_q$ and uniformly random and independent $a_1, ..., a_{l-1} \in R_q$, and independent $x_0, ..., x_{l-1} \leftarrow D_{R,r}$. Output $\vec{\boldsymbol{a}} = (a_1, ..., a_{l-1}, a_l = -\sum_{i\in[l]} a_i x_i) \in R_q^{\{1,...,l\}}$ as the public key, and $\vec{\boldsymbol{x}} = (x_1, ..., x_{l-1}, x_l = 1) \in R^{\{1,...,l\}}$ as the secret key.
- ***Enc*$_{\vec{\boldsymbol{a}}}(\boldsymbol{\mu\in R_p})$:** choose independent $e_0, ..., e_{l-1} \leftarrow \lfloor p.\psi \rceil_{pR^{\vee}}$, and $e_l \leftarrow \lfloor p.\psi \rceil_{t^{-1}\mu+pR^{\vee}}$. Let $\vec{\boldsymbol{e}} = (e_1, ..., e_l) \in (R^{\vee})^{\{1,...,l\}}$. Output ciphertext $\vec{\boldsymbol{c}} = e_0 * \vec{\boldsymbol{a}} + \vec{\boldsymbol{e}} \in (R_q^{\vee})^{\{1,...,l\}}$.
- ***Dec*$_{\vec{\boldsymbol{x}}}(\vec{\boldsymbol{c}})$:** compute $d = [[< \vec{\boldsymbol{c}}, \vec{\boldsymbol{x}} >]] \in R^{\vee}$, and output $\mu = t.d \bmod pR$.

**Lemma 10** (Lemma 8.1 from [3]). *If* $r > 2n.q^{1/l+2/(nl)}$, *then the* dual-style *cryptosystem is* IND-CPA *secure assuming the hardness of* R-DLWE$_{q,\psi}$ *given* $l + 1$ *samples.*

By Corollary 1, Lemma 3, and Lemma 4 the proof of Lemma 10 is obvious. We can refer to [3] for the full proof.

**Lemma 11** (Lemma 8.2 from [3]). *Suppose that for any* $c \in R_p^{\vee}$, $\lfloor p, \psi \rceil_{c+pR^{\vee}}$ *is* $\gamma$*-subgaussian with parameter* $s$ *for some* $\gamma = O(1/l)$, *and* $q \geqslant s\sqrt{(r^2l+1)n}.\omega(\sqrt{\log n})$. *Then decryption is correct with probability* $1 - \mathrm{negl(n)}$ *over all the randomness of key generation and encryption.*

The proof of Lemma 11 is obtained by Lemma 1, Lemma 5, Lemma 6, and Lemma 7. We can refer to [3] for the full proof.

### 2.3 Ring-Based Smooth Projective Hash Functions

Cramer and Shoup introduced smooth projective hash functions [4]; we improve and adapt the treatment of Katz and Vaikuntanathan [29], who extended the scheme of Gennaro and Lindell [5] based on lattices.

We assume there are sets $X, L \subset X$, and a subset $\bar{L} \subseteq L$; *approximate correctness* is guaranteed for $x \in \bar{L}$, while *smoothness* is guaranteed for $x \in X \backslash L$. Let $(Gen, Enc_{\vec{\boldsymbol{a}}}, Dec_{\vec{\boldsymbol{x}}})$ be a CPA-secure (*labeled*) dual-style encryption system and let $R_p$ be message space (dictionary of passwords in our application to ring-PAKE) that can be recognized efficiently. The dual-style cryptosystem defines a notion of *ciphertext validity* such that:

- By only $pk = \vec{\boldsymbol{a}}$, we can determine validity of a ciphertext with respect to $\vec{\boldsymbol{a}}$.
- All honestly created ciphertexts are valid.
- There is no decryption failure.

Let $(pk = \vec{\boldsymbol{a}}, sk = \vec{\boldsymbol{x}})$ be a key pair of $Gen(1^l)$ and let $C$ be the set of valid ciphertexts regard to $\vec{\boldsymbol{a}}$. The details of sets $X, \{\bar{L}_\mu\}_{\mu\in R_p}$, and $\bar{L}$ are as follows.

$$X = \{(label, \vec{\boldsymbol{c}}, \mu) : label \in R; \vec{\boldsymbol{c}} \in C; \mu \in R_p\},$$

$$\bar{L}_\mu = \{(label, Enc_{\vec{\boldsymbol{a}}}(label, \mu), \mu) : label \in R\} \subset X.$$

For $\mu \in R_p$, $\bar{L}_\mu$ is the set of honestly created encryptions of $\mu$ using any *label*, and $\bar{L} = \bigcup_{\mu\in R_p} \bar{L}_\mu$.

$$L_\mu = \{(label, \vec{\boldsymbol{c}}, \mu) : label \in R; Dec_{\vec{\boldsymbol{x}}}(label, \vec{\boldsymbol{c}}) = \mu\},$$

and set $L = \bigcup_{\mu\in R_p} L_\mu$. In addition, we have $\bar{L}_\mu \subseteq L_\mu$ for all $\mu$, and for any ciphertext $\vec{\boldsymbol{c}}$ and *label* $\in R$, we have at most one $\mu \in R_p$ for which $(label, \vec{\boldsymbol{c}}, \mu) \in L$.

Now we define a *ring-based* SPHF. A family of sets of keyed functions $\{H_k : X \to R^{\vee}\}_{k\in K}$, as well as a *projection function* $\alpha : K \times (pR^{\vee} \times C) \to S$ is called a "ring-based approximate smooth projective hash function" (ring-SPHF) with the following notions of (approximate) *correctness* and *smoothness*, where $H_k(y) = (r_0, r_1, ..., r_{n-1}) \in R^{\vee}$ for $y \in X$. Notice that based on the efficiency of ideal lattices, all operations can be performed in time $\tilde{O}(n)$ and the size of the digest is $\tilde{O}(n)$ [35]. Moreover, based on the structure of ideal lattices, $H_k$'s will be collision-resistance [35].

- **Approximate correctness** : As in [29], we require only approximate correctness for $y = (label, \vec{\boldsymbol{c}}, \mu) \in \bar{L}$, then the value of $H_k(y)$ is approximately obtained by $\alpha(k, label, \vec{\boldsymbol{c}})$ and $y$. In addition, the projection function $\alpha$ should be a function of *label*, $\vec{\boldsymbol{c}}$ only.
- **Smoothness** : Given $\alpha(k, label, \vec{\boldsymbol{c}})$ and $y$, if $y \in X \backslash L$ then, the value of $H_k(y)$ is statistically close to uniform (assume $k \in K$ is sampled uniformly).

Here, we give the formal definition of ring-based approximate smooth projective hash function by a sampling algorithm and given $\vec{\boldsymbol{a}}$.

**Definition 3.** We say that $(K, G, \mathbb{H} = \{H_k : X \to R^{\vee}\}_{k\in K}, S, \alpha : K \times (pR^{\vee} \times C) \to S)$ is a ring-SPHF such that:

- Using efficient algorithms in [2, 3]:

(1) we can compute $H_k(y)$ for all $y \in X$ and $k \in K$,
(2) we can sample a uniform $k \in K$, and
(3) we can compute $\alpha(k, label, \vec{c})$ for all $k \in K$ and $(label, \vec{c}) \in pR^\vee \times C$.

- For $y = (label, \vec{c}, \mu) \in \bar{L}$ we can compute the value of $H_k(y)$ approximately by $\alpha(k, label, \vec{c})$, relative to the statistical distance. In particular, let $\Delta(a, b)$ denote the statistical distance of two variables $a, b$ as vectors in $R^\vee$, then we have an efficient algorithm $H'$ that takes as input $s = (k, label, \vec{c})$ and $y' = (label, \vec{c}, \mu, r)$ for which $\vec{c} = Enc_{\vec{a}}(label, \mu, r)$ and satisfies:

$$\Delta(H_k(y), H'(y', s)) \leqslant negl(n).$$

- For any $y = (label, \vec{c}, \mu) \in X \backslash L$, the following two distributions have statistical distance negligible in $n$:

$$\{k \leftarrow K; s = \alpha(k, label, \vec{c}) : (s, H_k(y))\},$$

and

$$\{k \leftarrow K; s = \alpha(k, label, \vec{c}); v \leftarrow R^\vee : (s, v)\}.$$

## 3 Ring-SPHF Using Ideal Lattices

Now we explain our main results for constructing of a SPH system over rings (ring-SPHF) using ring-LWE problem on ideal lattices.

Assume a public key $A = \vec{a} = [I_{[k]}|\bar{A}] \in R_q^{\{1,...,l\}}$ is chosen for the system such that $k = 1$ and $\bar{A} \in R_q^{\{1,...,l-1\}}$. Let $R_p$ be a dictionary. Let sets $X, \bar{L}_\mu$, and $L_\mu$ be as defined in Section 2.3, and let $r$ be such that $\sqrt{n}.\omega(\sqrt{\log n}) \leqslant r$.

A key for the ring-SPHF is $\vec{x} = (x_1, ..., x_l) \in R^{\{1,...,l\}}$ where each $x_i \leftarrow D_{R,r}$ is drawn independently.

- We know the projection set $S = R_q$. The projection is $\alpha(\vec{x}) = \alpha(x_1, ..., x_l) = a_l \in R_q$ for a key $\vec{x} = (x_1, ..., x_l) \in R^{\{1,...,l\}}$, where $a_l = A\vec{x}$.
- Now, the ring-SPHF $\mathbb{H} = \{H_k\}_{k \in K}$ is defined. We have a key $\vec{x} = (x_1, ..., x_l) \in R^{\{1,...,l\}} = K$ and a ciphertext $y = (label, \vec{c}, \mu)$ as input, the hash function is given as follows:

$$h = H_k(y) = [[< y, \vec{x} >]] \in R^\vee,$$

where $h = (a_0, a_1, ..., a_{n-1}) \in R^\vee$ as a vector.
- On input a projected key $a_l \in S$, a ciphertext $y = (label, \vec{c}, \mu)$ and a witness $e_0 \in R_q$ for the ciphertext, the hash function is executed as follows:

$$h' = H'_{a_l}(y, e_0) = [[a_l * e_0 + e_l]] \in R^\vee,$$

where $h' = (b_0, b_1, ..., b_{n-1}) \in R^\vee$ as a vector.

**Theorem 2.** *Let the parameters $n, l, q, p$, and $r$ be as defined in Section 2. Then, $\mathbb{H} = \{H_k\}_{k \in K}$ is a ring-based approximate smooth projective hash system (ring-SPHF).*

*Proof.* Clearly, using ring-LWE toolkit [3], the following processes can all be done in polynomial time:

- A uniform key for the hash function $\vec{x} = (x_1, ..., x_l) \leftarrow D_{R,r}$ is sampled.
- The hash function $H$ on input the key $\vec{x} = (x_1, ..., x_l)$ and a ciphertext $y$ is computed.
- The projected key $A\vec{x} = \alpha(x_1, ..., x_l)$ is computed.
- Using the projected key $a_l$, a ciphertext $y$, and a witness $e_0$ for the ciphertext $y$, the hash function is computed.

Now, approximate correctness is shown. We have any $(label, \vec{c}, \mu) \in \bar{L}$, where on input the message $\mu$, the dual-style cryptosystem gives a ciphertext $\vec{c}$, i.e., $\vec{c} = e_0 * \vec{a} + \vec{e} \in R_q^{\{1,...,l\}}$ where according to Lemma 1, $||x_i||_2 \leqslant r\sqrt{n}$ and $||x_l||_2 = ||1||_2 = \sqrt{n}$.

We first show that the values $h$ (performed using the key) and $h'$ (performed using the projected key) are *close*, that is, $h$ and $h'$ have statistical distance negligible in $n$. More precisely, we show that the values $h$ and $h'$ are statistically indistinguishable from uniform, i.e.

$$\Delta(h, \mathcal{U}) \leqslant \text{negl(n) and } \Delta(h', \mathcal{U}) \leqslant \text{negl(n)},$$

then,

$$\Delta(h, h') \leqslant \text{negl(n)}.$$

Based on Corollary 1 (leftover hash lemma) and Lemma 10, $a_l = A\vec{x}$ is statistically indistinguishable from uniform, so clearly $h' = [[a_l * e_0 + e_l]]$ is statistically close to the uniform.

On the other hand, according to Lemma 2, $\vec{x}$ is statistically indistinguishable from uniform and according to Lemma 3 and Lemma 4, $\vec{c}$ is statistically indistinguishable from uniform, so clearly $h = [[< y, \vec{x} >]]$ is close to the uniform. Therefore, $\Delta(H_k(y), H'_{a_l}(y, e_0)) \leqslant \text{negl(n)}$. This shows approximate correctness ($h = h'$).

We now show smoothness. Recall each coefficient of polynomials $h$ and $h'$ is in $\mathbb{Z}$, so we can show $h$ and $h'$ as vectors in $\mathbb{Z}$. Consider any $y = (label, \vec{c}, \mu) \in X \backslash L$. By definition of $L$, this reveals that the decryption process on input $(label, \vec{c}, \mu)$ and any possible secret key $sk = \vec{x}$, outputs either $\perp$, or a message $\mu' \neq \mu$. We explain the two cases:

- The decryption algorithm gives $\perp$. This reflects that for the constant polynomial $a \in R_q$, the vector $az$ is far from the ideal lattice $\boldsymbol{L}(B)$. So, $az$ must be close to the ideal lattice $\boldsymbol{L}(B)$.
- The decryption algorithm gives a message $\mu' \neq \mu$. This could occur only if there is an $a' \in R_q$

**Table 1**. Parallel comparison between the SPHF on arbitrary lattices and ring-SPHF on ideal lattices.

| Scheme | HashKey(K) | ProjectedKey(S) | Hashing | ProjectiveHashing |
|---|---|---|---|---|
| SPHF[29] | $\mathbf{k} = (e_1, ..., e_k)$ $\in (\mathbb{Z}_q^m)^k$, $e_i \leftarrow D_{\mathbb{Z}^m, r}$ | $\mathbf{s} = \alpha(e_1, ..., e_k)$ $= (u_1, ..., u_k)$, $u_i = B^T e_i$, $A = [B\|U]$ | $H_k = b_i = \begin{cases} 0 \text{ if } z_i < 0 \\ 1 \text{ if } z_i > 0 \end{cases}$, $i = 1, ..., k$ $z_i = e_i^T[y - U.\begin{pmatrix} 1 \\ m \end{pmatrix}]$ $\in \mathbb{Z}_q$, $c = (label, y, m)$ | $H' = b_i = \begin{cases} 0 \text{ if } u_i^T s < 0 \\ 1 \text{ if } u_i^T s > 0 \end{cases}$, $i = 1, ..., k$ $(u_1, ..., u_k) \in S$, witness $s \in \mathbb{Z}_q^n$ |
| Ring-SPHF | $k = \overrightarrow{\boldsymbol{x}} = (x_1, ..., x_l)$ $\in R^{\{1,...,l\}}$, $x_i \leftarrow D_{R,r}$ | $s = \alpha(\overrightarrow{\boldsymbol{x}})$ $= \alpha(x_1, ..., x_l)$ $= a_l \in R_q$, $a_l = A\overrightarrow{\boldsymbol{x}}$, $A = \overrightarrow{\boldsymbol{a}} = [I\|\bar{A}]$ | $H_k = [[< y, \overrightarrow{\boldsymbol{x}} >]]$ $\in R^\vee$, $y = (label, \overrightarrow{\boldsymbol{c}}, \mu)$ | $H' = [[a_l * e_0 + e_l]]$ $\in R^\vee$, $a_l \in S$, witness $e_0 \in R_q$ |

such that $a'z'$ is close to the ideal lattice $\boldsymbol{L}(B)$. So, $a'z'$ must be far from the ideal lattice $\boldsymbol{L}(B)$.

Note that, according to an application of Lemma 8 and Lemma 9, $az$ and $a'z'$ are uniformly random and independent, because we utilize two honest CPA and CCA-secure cryptosystems with meaningful decryption algorithm. □

In Table 1, we summarize Katz and Vaikuntanathan's SPHF [29] over arbitrary lattices based on the LWE problem and our ring-SPHF over ideal lattices based on the ring-LWE problem.

## 4 Ring-PAKE Using Ring-SPHF

In this section, a new efficient password-based authenticated key exchange protocol over rings (ring-PAKE) on ideal lattices from ring-SPHF is presented that its structure is a modification and improvement of the Katz and Vaikuntanathan's framework [29] and its security is defined based on the standard definition of security for PAKE [19, 22, 27, 29]. Here, we describe the details of the protocol and we show a high-level overview of the 3-round ring-PAKE protocol as well.

The ring-based dual-style cryptosystem $\sum'$ with associated ring-SPHF is used and an ideal lattice-based CCA-secure encryption system such as [33] is denoted by $\sum$. In the ring-PAKE, there is a common reference string (CRS) containing of public keys $\overrightarrow{\boldsymbol{a}}, \overrightarrow{\boldsymbol{a'}}$ for $\sum, \sum'$, respectively. Moreover, as we know, the ring-SPHF associated with $\overrightarrow{\boldsymbol{a'}}$ is shown by:

$(K, G, \mathbb{H} = \{H_k : X \to R^\vee\}_{k \in K}, S, \alpha : K \times (pR^\vee \times C) \to S)$.

For authenticating of a client instance to a server instance, at first, a random string $r$ is chosen by the client and then it executes an encryption $\overrightarrow{\boldsymbol{c'}} = Enc_{\overrightarrow{\boldsymbol{a'}}}(w, r)$ of the shared password $w$. Then, a random hash key $k' \leftarrow K$ is sampled by the client and it selects the projected key $s' = \alpha(k', label', \overrightarrow{\boldsymbol{c'}})$. The client now sends "Client$\|\overrightarrow{\boldsymbol{c'}}\|s'$" to the server.

After receiving the message "Client$\|\overrightarrow{\boldsymbol{c'}}\|s'$", two random hash keys $k, k^* \leftarrow K$ are sampled by the server and it computes the projected keys $s = \alpha(k, label', \overrightarrow{\boldsymbol{c'}})$ and $s^* = \alpha(k^*, label', \overrightarrow{\boldsymbol{c'}})$. Then, hash values $H_k(\overrightarrow{\boldsymbol{c'}}, w) \in R^\vee$ and $H_{k^*}(\overrightarrow{\boldsymbol{c'}}, w) \in R^\vee$ using the ciphertext $\overrightarrow{\boldsymbol{c'}}$ and the password $w$ are computed by the server. The value $H_{k^*}(\overrightarrow{\boldsymbol{c'}}, w)$ is parsed as a sequence of three bit strings $r_j^*, \zeta_j^*$, and $SK_j^*$ where $r_j^*$ will be used as the random string for an encryption. Here, the server sets "$label$ = Client$\|$Server$\|\overrightarrow{\boldsymbol{c'}}\|s$", and encrypts the shared password $w$ as $\overrightarrow{\boldsymbol{c}} = Enc_{\overrightarrow{\boldsymbol{a}}}(label, w, r_j^*)$. Then, the hash value $H(s', \overrightarrow{\boldsymbol{c}})$ using the client's projected key $s'$ is performed by the server, and it computes a temporary session key $tk = H_k(\overrightarrow{\boldsymbol{c'}}, w) \oplus H(s', \overrightarrow{\boldsymbol{c}})$. In addition, it computes $\Delta = \text{Ecc}(H_{k^*}(\overrightarrow{\boldsymbol{c'}}, w)) \oplus tk$ where $\text{Ecc} : \{0,1\}^n \to \{0,1\}^m$, $n < m$ is an appropriate error-correcting code. Finally, the message "Server$\|\overrightarrow{\boldsymbol{c}}\|s\|s^*\|\Delta$" is sent to the client by the server.

After receiving the message "Server$\|\overrightarrow{\boldsymbol{c}}\|s\|s^*\|\Delta$", first, hash values $H_{k'}(\overrightarrow{\boldsymbol{c}}, w)$ and $H(s, \overrightarrow{\boldsymbol{c'}})$ using the server's projected key $s$ and encryption value $\overrightarrow{\boldsymbol{c}}$ are computed by the client such that $k'$ is created in the first round. Furthermore, the client computes $H(s^*, \overrightarrow{\boldsymbol{c'}})$ using the server's projected key $s^*$. Next, it computes:

$$tk' = H_{k'}(\overrightarrow{\boldsymbol{c}}, w) \oplus H(s, \overrightarrow{\boldsymbol{c'}}),$$

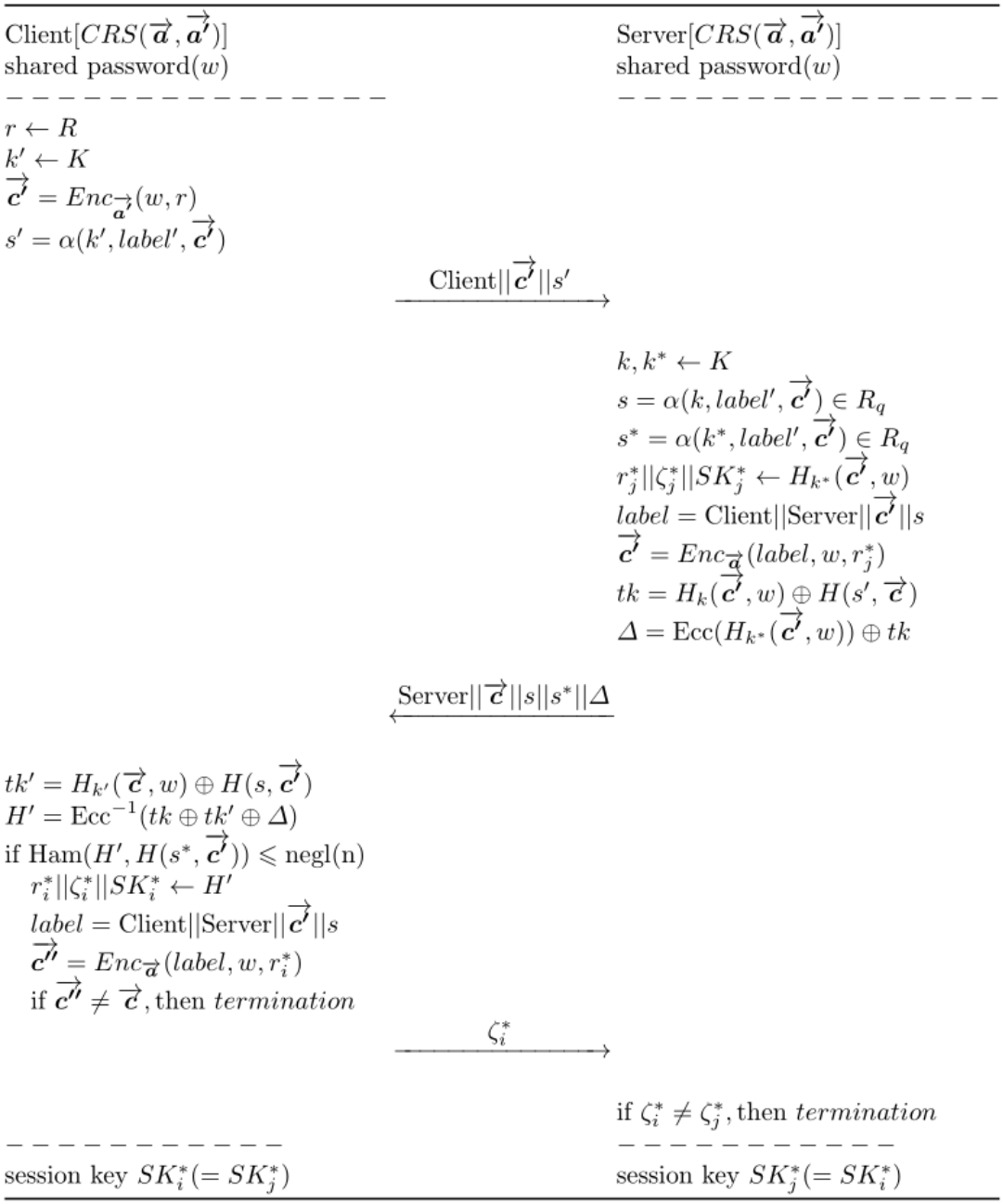



**Figure 1**. The proposed scheme.

and

$$H' = \text{Ecc}^{-1}(tk \oplus tk' \oplus \Delta).$$

Then, the client verifies the Hamming distance:

$$\text{Ham}(H', H(s^*, \vec{c'})) \leqslant \text{negl(n)},$$

if not, the client *terminates*. Otherwise, it parse $H'$ to $r_i^*, \zeta_i^*$, and $SK_i^*$ and computes $\vec{c''} = Enc_{\vec{a}}(label, w, r_i^*)$. Next, the client verifies $\vec{c''} = \vec{c}$ such that $\vec{c}$ is generated in the second round, if it is the case, the server is authenticated to the client, and the client make a connection and sends $\zeta_i^*$ to the server, hence outputs the session key $SK_i^*$, otherwise, the client *terminates*.

After receiving the massage $\zeta_i^*$ in the third round, the server verifies $\zeta_i^* = \zeta_j^*$, if it is the case, the client is authenticated to the server, and the server accepts and outputs the session key $SK_j^*$, otherwise, the server *terminates*.

**Correctness**. In an honest execution of the ring-PAKE and without adversarial interference, we show that the client and server's session keys are match and common. We have:

$$H' = \mathrm{Ecc}^{-1}(tk \oplus tk' \oplus \Delta)$$

where

$$tk = H_k(\overrightarrow{\boldsymbol{c'}}, w) \oplus H(s', \overrightarrow{\boldsymbol{c}}),$$

$$tk' = H_{k'}(\overrightarrow{\boldsymbol{c}}, w) \oplus H(s, \overrightarrow{\boldsymbol{c'}}),$$

and

$$\Delta = \mathrm{Ecc}(H_{k^*}(\overrightarrow{\boldsymbol{c'}}, w)) \oplus tk.$$

Approximate correctness of the ring-SPHF (Theorem 2), implies that:

$$\mathrm{Ecc}^{-1}(tk \oplus tk' \oplus \Delta) = H_{k^*}(\overrightarrow{\boldsymbol{c'}}, w),$$

so it holds that $r_i^* = r_j^*$, $\zeta_i^* = \zeta_j^*$. Thus, the same session key $SK_i^* = SK_j^*$ is obtained for the client and server. The security analysis of the ring-PAKE is based on the main ideas of [22, 27, 29, 37] as follows.

**Theorem 3.** *The Ring-PAKE provides session key security based on the Ring-SPHF.*

*Proof.* As we know, in the ring-PAKE protocol, we use the dual-style cryptosystem which is associated with the ring-SPHF, a CCA-secure cryptosystem, and an Ecc as an appropriate error-correcting code.

For an adversary that observes interactions between the client and server (passive attack), the shared session key is statistically indistinguishable from uniform (pseudorandom). Clearly, this is because a CPA-secure encryptions of the password $w$ and the projected keys of the ring-SPHF are used for the transcript of each interaction. For attackers that manipulate the messages in interactions between the client and server (active attack) such as man-in-the-middle, assume an adversary and a client have interactions with a password $w$.

- By the GK framework, if a ciphertext is sent from the adversary to the client that does not decrypt to the client's password $w$, then according to adversary's view, the client's session key is statistically close to uniform. Therefore, based on smoothness of the ring-SPHF (Theorem 2), this condition holds.
- By a CCA-secure encryption scheme that we use in the protocol, the probability that the attacker can generate a new ciphertext that decrypts to the client's password $w$ is at most $Att./|R_p|$+negl(n), where $Att.$ is the number of online attacks and $R_p$ is the password dictionary. Hence, based on the cyclotomic ring $R$ and parameter $p$ on ideal lattices, this probability is negligible in $n$.

□

## 5 Conclusion

In this work, we first presented a new efficient construction of a ring-based smooth projective hash function (ring-SPHF) on ideal lattices using ring-LWE problem based on ideas of Katz and Vaikuntanathan's SPHF on arbitrary lattices using LWE problem. Namely, we built an improvement of the lattice-based SPHF and analyzed its security based on ideal lattice assumptions.

Then, we proposed the first efficient password-based authenticated key exchange (ring-PAKE) protocol over rings using our ideal lattice-based ring-SPHF and described its security.

**Acknowledgments.**

We would like to thanks Prof. Jonathan Katz and Prof. Vadim Lyubashevsky for helpful discussions and useful suggestions while writing this paper. Special thanks to Prof. Damien Stehlé and Prof. Chris Peikert for their invaluable contributions in proving Lemma 8 and 9.

## References

[1] Gentry, C.: Fully homomorphic encryption using ideal lattices. In: 41st ACM STOC, pp. 169–178. ACM Press, Bethesda, Maryland (2009)

[2] Lyubashevsky, V., Peikert, C., Regev, O.: On ideal lattices and learning with errors over rings. Journal of the ACM. 60(6), 43:1–43:35 (2013)

[3] Lyubashevsky, V., Peikert, C., and Regev, O.: A toolkit for ring-LWE cryptography. In T. Johansson and P. Q. Nguyen, editors, EUROCRYPT 2013, volume 7881 of LNCS, pages 35–54. Springer, May (2013). Archive: https://eprint.iacr.org/2013/293

[4] Cramer, R., Shoup., V.: Universal hash proofs and a paradigm for adaptive chosen ciphertext secure public-key encryption. In: EUROCRYPT, pp. 45–64. Springer Press, Amsterdam (2002)

[5] Gennaro, R., Lindell, Y.: A framework for password-based authenticated key exchange. In: EUROCRYPT, pp. 524–543. Springer press, Warsaw (2003)

[6] Abdalla, M., Chevalier, C., Pointcheval, D.: Smooth projective hashing for conditionally extractable commitments. In: CRYPTO, pp. 671–689. Springer press, Santa Barbara, CA (2009)

[7] Reza Ebrahimi Atani, Shahabaddin Ebrahimi Atani, Amir Hassani Karbasi, NETRU: A Non-commutative and Secure Variant of CTRU Cryptosystem, The ISC International Journal of Information Security (ISeCure), Volume 10, Issue 1, Winter and Spring 2018, Page 45-53

[8] Blazy, O., Pointcheval, D., Vergnaud, D.:

Round-optimal privacy-preserving protocols with smooth projective hash functions. In: TCC, pp. 94–111. Springer press, Taormina, Sicily (2012)
[9] Katz, J., Ostrovsky, R., Yung, M.: Efficient password-authenticated key exchange using human-memorable passwords. In: EUROCRYPT, pp. 475–494. Springer press, Innsbruck (2001)
[10] Bellare, M., Pointcheval, D., Rogaway, P.: Authenticated key exchange secure against dictionary attacks. In: EUROCRYPT, pp. 139–155. Springer press, Bruges (2000)
[11] Amir Hassani Karbasi, Reza Ebrahimi Atani, Shahabaddin Ebrahimi Atani, PairTRU: Pairwise Non-commutative Extension of The NTRU Public key Cryptosystem, International Journal of Information Security Science, Volume 7, Issue 1, 2018, Page 11-19.
[12] SPEKE: RFC5931, RFC6617, IEEE P1363.2, U.S. Patent 6,226,383
[13] J-PAKE: Implemented in OPENSSL, NSS, used by FIREFOX-SYNC, https://wiki.mozilla.org/Services/KeyExchange
[14] Gong, L., Lomas, T.M.A., Needham, R.M., Saltzer, J.H.: Protecting poorly chosen secrets from guessing attacks. IEEE Journal of Selected Areas in Communications. 11(5), 648–656 (1993)
[15] Halevi, S., Krawczyk, H.: Public-key cryptography and password protocols. ACM Trans. Information and System Security. 2(3), 230–268 (1999)
[16] Bellovin, S.M., Merritt, M.: Encrypted key exchange: Password-based protocols secure against dictionary attacks. In: IEEE Symposium on Security and Privacy, pp. 72–84. IEEE press (1992)
[17] MacKenzie, P.D., Patel, S., Swaminathan, R.: Password-authenticated key exchange based on RSA. In: Asiacrypt, pp. 599–613. Springer press (2000)
[18] Reza Ebrahimi Atani, Shahabaddin Ebrahimi Atani, Amir Hassani Karbasi, A Provably Secure Variant of ETRU Based on Extended Ideal Lattices Over Direct Product of Dedekind domains, To appear in the Journal of Computing and Security, (2018).
[19] Goldreich, O., Lindell, Y.: Session-key generation using human passwords only. Journal of Cryptology. 19(3), 241–340 (2006)
[20] Boyko, V., MacKenzie, P.D., Patel, S.: Provably secure password-authenticated key exchange using Diffie-Hellman. In: Eurocrypt, pp. 156–171. Springer press (2000)
[21] Nguyen, M.H., Vadhan, S.: Simpler session-key generation from short random passwords. Journal of Cryptology. 21(1), 52–96 (2008)
[22] Benhamouda, F., Blazy, O., Chevalier, C., Pointcheval, D., Vergnaud, D.: New techniques for SPHFs and efficient one-round PAKE protocols. In: CRYPTO, pp. 449–475. Springer press, Santa Barbara, CA (2013)
[23] Gennaro, R.: Faster and shorter password-authenticated key exchange. In: TCC, pp. 589–606. Springer press (2008)
[24] Katz, J., MacKenzie, P.D., Taban, G., Gligor, V.D.: Two-server password-only authenticated key exchange. In: 3rd International Conference on Applied Cryptography and Network Security (ACNS), pp. 1–16. Springer press (2005)
[25] Amir Hassani Karbasi, Reza Ebrahimi Atani, IL-TRU: An NTRU-Like Public Key Cryptosystem Over Ideal Lattices, IACR Cryptology ePrint Archive, 2015.
[26] Canetti, R., Halevi, S., Katz, J., Lindell, Y., MacKenzie, P.D.: Universally composable password-based key exchange. In: Eurocrypt, pp. 404–421. Springer press (2005)
[27] Gennaro, R., Lindell, Y.: A framework for password-based authenticated key exchange. ACM Trans. Information and System Security. 9(2), 181–234 (2006)
[28] Jiang, S., Gong, G.: Password based key exchange with mutual authentication. In: 11th Annual International Workshop on Selected Areas in Cryptography (SAC), pp. 267–279. Springer press (2004)
[29] Katz, J., Vaikuntanathan, V.: Smooth projective hashing and password-based authenticated key exchange from lattices. In: ASIACRYPT, pp. 636–652. Springer press, Tokyo, Japan (2009)
[30] Rivest, R.L., Shamir, A., Adleman, L.M.: A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM. 21(2), 120–126 (1978)
[31] Diffie, W., Hellman, M.E.: New directions in cryptography. IEEE Transactions on Information Theory, IT-22(6), 644–654 (1976)
[32] Regev, O.: On lattices, learning with errors, random linear codes, and cryptography. In: 37th Annual ACM Symposium on Theory of Computing (STOC), pp. 84–93. ACM press (2005)
[33] Peikert, C.: Lattice Cryptography for the Internet. In: Post-Quantum Cryptography - 6th International Workshop, PQCrypto, pp. 197–219. Springer press, Waterloo, ON (2014)
[34] Gentry, C., Peikert, C., Vaikuntanathan, V.: Trapdoors for hard lattices and new cryptographic constructions. In: STOC, pp. 197–206. (2008)
[35] Lyubashevsky, V., Micciancio, D., Peikert, C., Rosen, A.: SWIFFT: A modest proposal for FFT hashing. In: FSE, pp. 54–72. (2008)
[36] Reza Ebrahimi Atani, Shahabaddin Ebrahimi Atani, Amir Hassani Karbasi, EEH: AGGH-like public key cryptosystem over the eisenstein integers using polynomial representations, The ISC

International Journal of Information Security (ISeCure), Volume 7, Issue 2, Summer and Autumn 2015, Page 115-126.

[37] Groce, A., Katz, J.: A New Framework For Efficient Password-based Authenticated Key Exchange. In: 17th ACM Conf. on Computer and Communications Security, pp. 516525. ACM Press, New York, (2010)

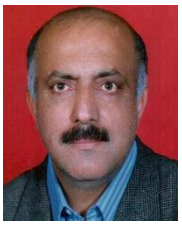
[38] Zhang, J., Zhang, Z., Ding, J., Snook, M., Dagdelen, O.: Authenticated key exchange from ideal lattices. In: Oswald, E., Fischlin, M. (eds.) EUROCRYPT 2015. LNCS, vol. 9057, pp. 719–751. Springer, Berlin (2015). DOI: 10.1007/ 978–3–662–46803–624.

[39] Jintai Ding, Saed Alsayigh, Jean Lancrenon, Provably Secure Password Authenticated Key Exchange Based on RLWE for the Post-Quantum World, CT-RSA (2017), pp. 183–204, 2017. DOI: 10.1007/978–3–319–52153–411.

[40] Fabrice Benhamouda, Olivier Blazy, Lo Ducas, Willy Quach, Hash Proof Systems over Lattices Revisited, Public-Key Cryptography–PKC (2018), pp. 644–674.

**Amir Hassani Karbasi** studied his B.S. in applied mathematics at the University of Tabriz in Tabriz, Iran. He received his B.S. degree in 2010. He received his M.S. in computer networks in 2013 from University of Guilan. He received his Ph.D. in 2018 from University of Guilan (Elite Entrance Students to Ph.D.) and has worked on "Design and security analysis of lattice-based cryptographic structures". Now, he is a part-time faculty member at some Universities and information security specialist at some companies. His main research interests include lattice-based cryptography, digital signatures, network security, rings and semi-ring theory and pullback of rings.

**Reza Ebrahimi Atani** studied electronics engineering at the University of Guilan, Rasht, Iran and got his B.S. degree in 2002. He followed his masters and Ph.D. studies at Iran University of Science & Technology (IUST) in Tehran, and received Ph.D. degree in 2010. He is now holding an associated professor position in the department of computer engineering at the University of Guilan. His research interests focuses on design and implementation of cryptographic algorithms and protocols as well as their applications to computer and network security and mobile communications. He is a member of IEEE and IACR.



**Shahabaddin Ebrahimi Atani** got his B.S. and M.S. in Mathematics. In 1996, he graduated from a Ph.D. program of mathematical science department of University of Manchester, England. He is now a professor at faculty of mathematical sciences of the University of Guilan. His research interests include rings and semi-ring theory and pullback of rings.