RESEARCH ARTICLE

Non-interactive zero-knowledge proof scheme from RLWE-based key exchange

Shaofen Xie^{1,4,5}, Wang Yao^{2,4,5}, Faguo Wu^{3,4,5*}, Zhiming Zheng^{1,2,4,5}

1 School of Mathematical Sciences, Beihang University, and Key Laboratory of Mathematics, Informatics and Behavioral Semantics, Ministry of Education, Beijing, China, **2** Institute of Artificial Intelligence, Beihang University, and Key Laboratory of Mathematics, Informatics and Behavioral Semantics, Ministry of Education, Beijing, China, **3** Research Institute for Frontier Science, Beihang University, and Key Laboratory of Mathematics, Informatics and Behavioral Semantics, Ministry of Education, Beijing, China, **4** Peng Cheng Laboratory, Shenzhen, Guangdong, China, **5** Beijing Advanced Innovation Center for Big Data and Brain Computing, Beihang University, Beijing, China

* faguo@buaa.edu.cn

Abstract

Lattice-based non-interactive zero-knowledge proof has been widely used in one-way communication and can be effectively applied to resist quantum attacks. However, lattice-based non-interactive zero-knowledge proof schemes have long faced and paid more attention to some efficiency issues, such as proof size and verification time. In this paper, we propose the non-interactive zero-knowledge proof schemes from RLWE-based key exchange by making use of the Hash function and public-key encryption. We then show how to apply the proposed schemes to achieve the fixed proof size and rapid public verification. Compared with previous approaches, our schemes can realize better effectiveness in proof size and verification time. In addition, the proposed schemes are secure from completeness, soundness, and zero-knowledge.

OPEN ACCESS

Citation: Xie S, Yao W, Wu F, Zheng Z (2021) Non-interactive zero-knowledge proof scheme from RLWE-based key exchange. PLoS ONE 16(8): e0256372. <https://doi.org/10.1371/journal.pone.0256372>

Editor: Hua Wang, Victoria University, AUSTRALIA

Received: May 10, 2021

Accepted: August 4, 2021

Published: August 20, 2021

Copyright: © 2021 Xie et al. This is an open access article distributed under the terms of the [Creative Commons Attribution License](https://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

Data Availability Statement: All relevant data are within the manuscript and its [Supporting information](#) files.

Funding: This work was supported by the National Key Research and Development Program of China under Grant 2020YFB1005702 and the Science and Technology Innovation 2030-Key Project under Grant 2020AAA0108200. <https://service.most.gov.cn/>.

Competing interests: The authors have declared that no competing interests exist.

Introduction

With the development of information networks, the concern about privacy of personal data is growing. Users tend to communicate on the Internet without revealing individual data [1–7], such as users' passwords, personal assets information, personal health condition, and so on. According to cryptography theory, the zero-knowledge(ZK) proof [8] is an essential technique for preserving information protection. In the 1880s, Goldwasser et al. proposed the interactive zero-knowledge proof for the first time. Subsequently, Blum et al. [9] first proposed the non-interactive zero-knowledge proof, which is characterized by only one-time communication between the prover and the verifier. Andre et al. [10] designed the protocol which was based on the public-key cryptosystem RSA-encryption for the proof of ownership. Siamak et al. pointed that the significance of credential ownership proofs and gave the proof by the RSA signature scheme [11]. Over the past three decades, extensive research has been conducted on zero-knowledge proofs in terms of algorithm safety and operational efficiency [12–14]. And it is used in various fields such as authentication, ownership, etc. [15–17].

Since the non-interactive zero-knowledge proof is suitable for offline operations, it will have more application scenarios. Usually, there are two methods for interactive zero-knowledge proof to achieve non-interactive zero-knowledge proof: Fiat-Shamir heuristic and CRS (Common Reference Strings) model. For the Fiat-Shamir heuristic, it demands to include a random oracle to generate a uniformly random output. For the CRS model, it needs to rely on a trusted third-party or secure multi-party computing to obtain the common reference string. There has been a series of corresponding studies using the Fiat-Shamir heuristic. Lindell et al. [18] and Ciampi et al. [19] have redesigned the scheme to improve security and efficiency based on Fiat-Shamir transform. With the rapid application of cryptocurrency, after Groth [20] proposed the scheme of constant-size proofs, the first zero-knowledge succinct non-interactive argument of knowledge (ZK-SNARK) based on the assumption of a trusted third-party has also been widely studied. The zero-knowledge proof schemes of traditional encryption have been widely used. And they have made great contributions in efficiency, security, and so on. However, researchers have paid less attention to zero-knowledge proof schemes that can resist quantum attacks.

With the surprising development of quantum computers, a series of post-quantum cryptographic algorithms have been studied [21]. The lattice-based cryptographic algorithm could effectively resist quantum attacks. After Ajtai et al. [22] introduced lattice cryptography and gave strict proof from the average case to the worst case for the first time. Due to the security and applicability of lattice-based cryptographic algorithms, extensive research has been conducted. In 2010, RLWE(Ring Learning with Errors), proposed by Lyubashevsky et al. [23], significantly shortened the key length and improved the efficiency of the signature. Lattice-based cryptography theories have also begun extensive research and application. Subsequently, lattice-based zero-knowledge proofs have begun to develop gradually.

Related works

In 2012, Vadim Lyubashevsky used Fiat-Shamir with Aborts technology to design a zero-knowledge proof scheme [24], which proves that s satisfies $As = t \bmod q$ without revealing the secret value s . The signature size is 16500 bits which can be modified to shorten using the compression technique, where the scheme relies on SIS(Small Integer Solution) problem and LWE (Learning with Errors) problem. The scheme was then applied and extended by Vadim Lyubashevsky and Gregory Neven to a ciphertext-verifiable scheme [25]. At the same time, Fabrice Benhamouda et al. [26] used zero-knowledge to prove that the secret value s satisfies $p = as + e$ and was used in group signature authentication to protect the anonymity of group members. However, the security is based on a lattice-based assumption and the discrete-logarithm problem. Then we should consider how to construct an effective zero-knowledge proof system in terms of the proof size and the security to promote its application.

Most studies on commitment schemes are quite effective practice for zero-knowledge proof, such as [27–33]. Fabrice Benhamouda et al. [27] constructed a simple efficient string commitment scheme based on RLWE and the zero-knowledge proofs of knowledge for linear relations and multiplicative relations, where the communication complexity is $\mathcal{O}(Mn\log(q))$. In order to achieve a negligible soundness error, the protocol demands run M rounds. Vadim Lyubashevsky et al. [28] proposed splitting the polynomial into multiple factors. This method can improve the computation and more information will be hidden. Baum et al. [29] constructed a novel zero-knowledge proof of preimages scheme which would become a tool against malicious adversaries. Muhammed et al. [30] used the one-shot proof technique for non-linear polynomial relations to improve computing and communication performance. Baum et al. designed the zero-knowledge argument based on the short integer solution

assumption for specific languages. The communication complexity of this scheme is $\sqrt{m \log(m)}$, where m is the number of gates [31]. The proof size of Bootle et al. proposed scheme [32] is better than that of Stern type proof, but the efficiency of verification time still needs to be improved. Baum et al. [33] constructed a practical zero-knowledge proof of opening knowledge which is an improvement of the scheme of Fabrice Benhamouda et al. [27]. It has shown that prover does not need to send more proof for part of the calculation process. Obviously, the disadvantage of all these previous commitment schemes is that the commitments also consume calculation and communication in the interactive. Meanwhile, considering that the interactive property and the proof size, the commitment schemes are no longer suitable for the publicly-verifiable scheme. We would adopt non-interactive zero-knowledge proof to design a publicly-verifiable scheme with more short proof size and verification time.

Subsequently, related research has also improved in terms of efficiency and safety [34, 35]. Among them, Rafael et al. [34] proposed a scheme that could reduce the proof size. The main idea of this method is to reduce the number of equations in the protocol by increasing the running time of the proof. It is also an interactive scheme that is different from the non-interactive that we would discuss. The non-interactive zero-knowledge proof of LWE based on the SSP (Square Span Programs) in ZK-SNARKs was proposed by Rosario Gennaro et al. [35] and is considered post-quantum secure, and which would be used in the anonymous cryptocurrency Zerocash. The proof size of this scheme is constant which just consists of 5 LWE encodings. Rosario Gennaro et. al. mainly focused on designated-verifier proofs, but we would study the publicly-verifiable proofs. Ding has used the signal function from the RLWE key exchange to design an effective interactive zero-knowledge authentication protocol [36]. They pointed out that the design of the RLWE-based non-interactive zero-knowledge authentication scheme will be future work. Based on the above comparative analysis, we would construct the new non-interactive zero-knowledge proof protocols that can prove ownership with small proof size and high efficiency.

Motivation

Your protected private data can be used in a variety of scenarios, for example, you have a private key, or you have enough money to pay for the transaction, or you know the solution to the problem. In other words, prover should generate the proof for the verifier to prove the secret value for ownership, account balance, Sudoku, etc. Because of the convenience of one-time communication, we study the lattice-based non-interactive zero-knowledge proof against quantum attacks. Considering the wide application of scenarios, the scheme is extended from designated-verifier verification to publicly-verifiable. Because we do not completely trust the trusted third-party, and we want nobody to know our secret value. Therefore, we introduce the semi-trusted third-party assumption, that is, the third-party can only prove the secret value but know nothing about it. This assumption can further enhance the protection of the secret and ensure the security of the scheme.

Contributions

The main contributions in this paper are as follows:

1. We design a non-interactive zero-knowledge proof scheme to ensure that the proof size is constant for the designated-verifier. Then, we prove that this scheme is secure in terms of completeness, soundness, and zero-knowledge.

2. In order to satisfy the fixed proof size and improve verification efficiency, we combine public-key encryption with a semi-trusted third-party assumption to construct a publicly-verifiable scheme and prove the security of the scheme.
3. Compared with the previous scheme with efficiency advantage, we achieve better effectiveness schemes in zero-knowledge proof size and verification time.

Organization

The rest of this paper is organized as follows. In Section 2, we show the essential preliminary for the schemes. In Section 3, we construct a zero-knowledge proof scheme based on key-exchange in designated-verifier and provide the security analysis of the scheme. In Section 4, we construct the non-interactive zero-knowledge proof for publicly-verifiable and also give the security analysis. In Section 5, we compare the efficiency of our schemes with the previous existing protocols. In Section 6, we give a summary of this paper.

Preliminaries

Notations

Throughout the paper, following notations would be used in Table 1.

Non-interactive zero-knowledge proof

Definition 1 *Non-Interactive Zero-Knowledge Proof:* (P, V) is a non-Interactive zero-knowledge proof system for a language L , where s is secret value, should satisfy the following properties [9]:

Completeness. If the statement is true, the honest verifier will be convinced of this fact by an honest prover. That means, for $\forall x \in \mathcal{L}$, if the prover has the secret value s , then

$$\Pr [\pi \leftarrow P(x, s) : V(x, \pi) = 1] \geq 1 - 2^{-n}.$$

Soundness. If the statement is false, none prover as the adversary can convince the honest verifier that it is true, except with negligible probability. That means, for $\forall x \notin \mathcal{L}$, if the prover has no secret value s , then

$$\Pr [\pi \leftarrow P(x) : V(x, \pi) = 1] \leq 2^{-n}.$$

Table 1. Description of notations.

Notation	Description
n	security parameter, it's a power of 2
q	a positive integer
$\mathbb{Z}_q$	the ring $\mathbb{Z}/q\mathbb{Z}$
$x^n + 1$	irreducible polynomial
R_q	the ring $\mathbb{Z}_q[x]/(x^n + 1)$
$\{a_i\}_{i=0}^{n-1}$	any polynomial $a \in R_q$, using the coefficient vector $\{a_0, a_1, \dots, a_{n-1}\}$ in $\mathbb{Z}_q$ to represent a
M^T	the transpose of the matrix M
$\ s\ _\infty$	$\max s_i $ for a vector s
$\ s\ $	$\ s\ _q, (\sum_{i=0}^{n-1} v_i ^q)^{1/q}$ for a vector s
$\mathcal{D}$	the discrete Gaussian distribution on lattice

<https://doi.org/10.1371/journal.pone.0256372.t001>

Zero-knowledge. If the statement is true, the verifier will learn nothing about the secret but the fact that the statement is true.

That is, there is a polynomial-time simulator, for all $x \in \mathcal{L}$ and secret value s , the following two distributions are computationally indistinguishable, where $\text{Exp}_{\text{ZK-real}} = 1$ represents the algorithm of the real system and $[\text{Exp}_{\text{ZK-sim}} = 1]$ represents the algorithm of the simulation system.

$$\| \Pr [\text{Exp}_{\text{ZK-real}} = 1] - \Pr [\text{Exp}_{\text{ZK-sim}} = 1] \| \leq 2^{-n}.$$

Non-interactive. The prover only has one-way communication to the verifiers during the proof phase.

Ring learning with error

Here, we recall informally the Ring Learning with Error assumption, which is a classical hard problem on lattice defined by Regev [37]. And the security of our quantum-resistant schemes rely on the hardness assumption that has been previously used in the literature as follows.

Definition 2 Discrete Gaussian: For $\forall \sigma > 0, x \in \mathbb{Z}^N$, the center of Discrete Gaussian Distribution c , and defined $\rho_{\sigma,c}(x) = \left(\frac{1}{\sigma}\right)^N e^{-\frac{\pi\|x-c\|^2}{\sigma^2}}$ as the N -dimensional Gaussian function: Then the Discrete Gaussian Distribution can be defined as $\mathcal{D}_{\mathcal{L},\sigma,c} = \frac{\rho_{\sigma,c}(x)}{\rho_{\sigma,c}(\mathcal{L})}$.

Lemma 1 ([38]). Let $R = \mathbb{Z}[x]/(x^n + 1)$, for any $a, b \in R$, we have $\|a \cdot b\| \leq \sqrt{n} \cdot \|a\| \cdot \|b\|$ and $\|a \cdot b\|_{\infty} \leq \|a\|_{\infty} \cdot \|b\|_{\infty}$.

Lemma 2 ([39]). For any $\sigma \geq \omega(\sqrt{\log(n)})$, then we have

$$\Pr_{x \leftarrow \mathcal{D}_{\mathcal{L},\sigma,c}} [\|x\| > \sigma\sqrt{n}] \leq 2^{-n}.$$

Definition 3 RLWE Problem [36, 37]: Let $n \in \mathbb{Z}$ be a power of 2 and q be positive integers, and let χ_{α} be the Discrete Gaussian distribution on R_q . For a uniformly chosen element s of the polynomial ring R_q , let $\mathcal{A}_{s,\chi_{\alpha}}$ be the distribution of the pair $(a, as + 2e) \in R_q \times R_q$ where $a \leftarrow R_q$ is uniformly chosen and $e \leftarrow \chi_{\alpha}$ is independent of a . Then the $\mathcal{A}_{s,\chi_{\alpha}}$ is computationally indistinguishable from the uniform distribution on $R_q \times R_q$ for any probabilistic polynomial time (PPT).

Assumption 1 [36] The security of our schemes rely on the Ring-LWE assumption stating that the distribution of $(h_i, h_i s + e_i)$, where h_i is random in R_q and s, e_i are small polynomials, is indistinguishable from uniform. The search version of Ring-LWE is to modify the above definition by requiring the PPT algorithm to find s rather than distinguish the two distributions.

Signal function

Given $\mathbb{Z}_q$ is $\{-\frac{q-1}{2}, \dots, \frac{q-1}{2}\}$, we introduce the signal function [38] to eliminate the errors caused by Mod_2 function in R_q .

Definition 4 Signal Function Let $E_1 = [-\lfloor \frac{q}{4} \rfloor, \lfloor \frac{q}{4} \rfloor]$ and $E_2 = [-\lfloor \frac{q}{4} \rfloor + 1, \lfloor \frac{q}{4} \rfloor + 1]$, then the signal function $\text{Char} : \mathbb{Z}_q \rightarrow \{0, 1\}$ as the following:

$$\text{Char}(x) = \begin{cases} 0 & x \in E_1 \text{ or } x \in E_2 \\ 1 & \text{otherwise} \end{cases}.$$

Definition 5 The function $\text{Mod}_2 : \mathbb{Z}_q \times \{0, 1\} \rightarrow \{0, 1\}$ was defined as

$$\text{Mod}_2(x, a) = \left(x + a \cdot \frac{q-1}{2} \right) \text{Mod}_q \text{Mod}_2.$$

Lemma 3 ([40]). Let $q > 8$ and be an odd prime, $x, y \in \mathbb{Z}_q$ such that $\|x - y\|_\infty < \frac{q}{4}$ and $a = \text{Char}(x)$. Then

$$\text{Mod}_2(x, a) = \text{Mod}_2(y, a).$$

Proof 0.1 Known $\|x - y\|_\infty < \frac{q}{4}$, let $x = y + 2\epsilon$, $|2\epsilon| \leq \frac{q}{4} - 2$, Note that $(x + a \cdot \frac{q-1}{2}) \text{Mod}_q = (y + a \cdot \frac{q-1}{2} + 2\epsilon) \text{Mod}_q$. From the Char function as we defined, $|y + a \cdot \frac{q-1}{2}| < \frac{q}{4} + 1$, because $|y + a \cdot \frac{q-1}{2} + 2\epsilon| \leq |y + a \cdot \frac{q-1}{2}| + |2\epsilon| \leq \frac{q}{2} - 1$, $(y + a \cdot \frac{q-1}{2} + 2\epsilon) \text{Mod}_q = (y + a \cdot \frac{q-1}{2}) \text{Mod}_q + 2\epsilon$, Perform mod_2 on both sides of the above equation, then

$$\text{Mod}_2(x, a) = (x + a \cdot \frac{q-1}{2}) \text{Mod}_q \text{Mod}_2 = (y + a \cdot \frac{q-1}{2}) \text{Mod}_q \text{Mod}_2 = \text{Mod}_2(y, a).$$

Then, signal function and mod_2 function were extended to polynomial ring $x \in R_q$ by applying them for each coefficient $x_i \in \mathbb{Z}_q$. Clearly, the result in Lemma 3 still holds when extending to polynomial ring elements. In the following, we use the extend signal function and mod_2 function in the polynomial ring $R_q^{n \times n}$.

As far as we know, Ding et al. [41] in 2017 pointed out that signal function may leak the secret key when RLWE public-key is reused for the long term. But it does not mean that the signal function cannot be used forever. Gao et al. [42] used a key reuse mode by adding the user ID and a fresh public error against this attack in 2018.

Designated-verifier non-interactive zero-knowledge Proof based on RLWE key exchange

DVNIZK scheme

Firstly, we describe the designated-verifier non-interactive zero-knowledge proof scheme (DVNIZK) which is based on RLWE key exchange. As we know, only the designated-verifier can effectively check the proof in the DVNIZK scheme. This scheme is just a one-time proof. That is to say, a new session will be built for the different designated-verifier. At the same time, the prover will generate fresh errors for different verifiers. Therefore, this scheme can against signal function leakage attacks.

This scheme involves two objects: prover and verifier. Prover generates the proof for the verifier to prove the user of secret value for ownership, account balance, Sudoku, etc, which is illustrated in Fig 1.

In the first scheme, we provide the security model for the designated-verifier non-interactive zero-knowledge proof using the random oracle model, similar to the security model proposed in [36]. Our first scheme is composed of three algorithms: Setup, Proof, Verify. Specifically, we demonstrate it as follows, shown in Fig 2.

1. Setup:

- The public parameters q, n, α be generated, where $q > 8$ is prime.
- Let M be a uniformly random matrix $M \leftarrow R_q^{n \times n}$.
- Let $H: \{0, 1\}^{n \times n} \rightarrow \{0, 1\}^n$ be a random oracle.

Fig 1. The designated-verifier scheme architecture.

<https://doi.org/10.1371/journal.pone.0256372.g001>

- P has $P_A = M \cdot S_A + 2e_A \bmod q$ where S_A is secret information and $S_A, e_A \leftarrow \chi_\alpha$ are $n \times n$ dimensional. Namely, S_A consists of n elements in a polynomial ring (i.e. $S_A = (S_1, S_2, \dots, S_n)^T$, where $S_i = (s_{i1}, s_{i2}, \dots, s_{in}) \in R_q, s_{ij} \in \mathbb{Z}_q$, which i and j range from 1 to n). s_{ij} is sampled from the Discrete Gaussian distribution with parameter σ . Clearly, S_A can be expressed as a $n \times n$ dimensional matrix. And e_A is the same as above S_A . It is stated here that all the multiplication operations of the elements in the polynomial ring must undergo modulo q and modulo the irreducible polynomial $x^n + 1$ operations.
- V has $P_B = M \cdot S_B + 2e_B \bmod q$ where $S_B, e_B \leftarrow \chi_\alpha$ are also $n \times n$ dimensional. S_B and e_B are also same as above S_A .

2. Proof:

- Let $x = S_A^T \cdot P_B$, P computes $\omega = \text{Char}(x)$ and $W \leftarrow \text{Mod}_2(x, \omega)$ as the zero-knowledge proof.
- P computes $K = H(W)$.
- P sends K, ω to V.

3. Verify:

Fig 2. Designated-verifier non-interactive zero-knowledge based on RLWE key exchange.

<https://doi.org/10.1371/journal.pone.0256372.g002>

- Upon receiving K, ω , only verifier could do the following:
- Let $y = P_A^T \cdot S_B$, $\forall$ computes $J \leftarrow \text{Mod}_2(y, \omega)$ firstly.
- $\forall$ checks if $K \stackrel{?}{=} H(J)$. Accept if $K = H(J)$, otherwise reject.

Security analysis

Security is the most important factor of the zero-knowledge proof schemes. The first scheme for designated-verifier only can be used as the one-time proof. It satisfies the properties of the zero-knowledge proof: Completeness, Soundness, Zero-knowledge. We will supply a simple security analysis in the following.

Lemma 4 Let $q > 16\sigma^2 n^{\alpha_{3/2}}$, then $\text{Mod}_2(x, \omega) = \text{Mod}_2(y, \omega)$, except with negligible probability.

Proof 0.2 Firstly, we know that $x = S_A^T \cdot P_B$ and $y = P_A^T \cdot S_B$.

Considering that $x, y \in R_q^{n \times n}$, then we just show that $\|x_{i,j} - y_{i,j}\|_\infty < \frac{q}{4}$ by Lemma 3, where $i, j \in \{1, \dots, q\}$. After simplification, combining with Lemma 1 and Lemma 2, we have that

$$\|x_{i,j} - y_{i,j}\| = \|2(S_{A_{i,j}}^T \cdot e_{B_{i,j}} - e_{A_{i,j}}^T \cdot S_{B_{i,j}})\| < 4\sigma^2 n^{3/2}$$

By lemma 3, we obtain $\|x_{i,j} - y_{i,j}\|_\infty < 4\sigma^2 n^{3/2} < \frac{q}{4}$.

Then, $q > 16\sigma^2 n^{\alpha_{3/2}}$ with probability $1 - 2^{-n}$.

1) Completeness. The form of the proof is shown as follows:

As we know $K = H(W)$, where $W = \text{Mod}_2(x, \omega)$.

The verifier owns S_B, P_A, K, ω after receiving the proof, it will follow from straightforward calculations $H(J)$ where $J = \text{Mod}_2(y, \omega)$.

If S_A is true, by the lemma 4, $\text{Mod}_2(x, \omega) = \text{Mod}_2(y, \omega)$. That means $W = J$. Finally, $K = H(W)$ will be equal to $H(J)$. Then the verifier will be convinced that the prover owns the secret.

2) Soundness. Assuming that P would be an adversary and as an oracle that generate the valid proof for the honest verifier with non-negligible probability in the following.

Game₀: this game is the original scheme. According to the scheme, $P_A = M \cdot S_A + 2e_A \bmod q$, $P_B = M^T \cdot S_B + 2e_B \bmod q$, then W, ω, K, J is generated, and output b_d which is the determination of the verifier. Among which $b_d = 1$ means the verifier accepts and $b_d = 0$ respects he rejects.

Game₁: this game is equal to **Game₀** except that P_A is chosen uniformly. $\mathcal{A}$ cannot generate the valid proofs for the chosen uniform P_A with negligible probability.

Lemma 5 If prover as the adversary $\mathcal{A}$ who could generate a valid proof for $P_A = M \cdot S_A + 2e_A \bmod q$ without the secret of S_A to convince the honest verifier with non-negligible probability, then there is a distinguisher for P_A from uniform with the same probability.

Proof 0.3 Assuming that $\mathcal{B}$ be a RLWE distinguisher. Considering that interaction between $\mathcal{A}$ and $\mathcal{B}$ as the role of honest verifier. When $\mathcal{B}$ sends the challenge (M, P_A) from the RLWE challenger to $\mathcal{A}$, $\mathcal{A}$ would do the following. If $P_A = M \cdot S_A + 2e_A \bmod q$, the interaction between $\mathcal{A}$ and $\mathcal{B}$ is equal to **Game₀**, then $\mathcal{B}$ outputs 1. If P_A is chosen uniformly, the interaction between $\mathcal{A}$ and $\mathcal{B}$ is equal to **Game₁**, then $\mathcal{B}$ outputs 0.

Suppose $\mathcal{A}$ can generate a valid proof for the chosen uniform P_A with non-negligible probability, then $\mathcal{B}$ would not be successful from the above defined. That means the adversary can solve the search version of the Ring-LWE problem with the same probability. Suppose $\mathcal{A}$ can generate K and ω which are accepted by the honest verifier for P_A without the secret of S_A . In our first scheme, the crucial verify are $J = \text{Mod}_2(y, \omega)$. It means that the valid proof only could be obtained by guessed or correctly calculated $\text{Char}(y)$ and $\text{Mod}_2(y, \text{Char}(y))$.

On the one hand, the valid proof that the probability of being brutally guessed is negligible. On the other hand, the adversary wants to calculate $\text{Char}(y)$ and $\text{Mod}_2(y, \text{Char}(y))$ correctly. Considering that this scheme is used as a one-time proof, there is no sign function leakage attack that makes the secret value leak. Therefore, in order to calculate the correct $\text{Char}(y)$ and $\text{Mod}_2(y, \text{Char}(y))$, A needs to know the secret value S_B . However, if A knows the secret value S_B , it means that it can solve the search version of the Ring-LWE problem. In fact, the search version of Ring-LWE is to modify the above definition by requiring the PPT algorithm to find s rather than distinguish the two distributions in Assumption 1. Therefore, the adversary can generate a valid proof for the chosen uniform P_A and would be accepted by the designated-verifier with the same probability which can solve the search version of the Ring-LWE problem.

In summary, in DVNIZK-KE Scheme, the adversary cannot convince the verifier to believe him with negligible probability without knowing the secret value. Then the soundness error of our is negligible.

3) Honest-verifier zero-knowledge. **Lemma 6** Honest-verifier Zero-knowledge [26] means that there be a probabilistic polynomial-time simulator taking P_A and S'_B as input, that outputs (K', ω') is indistinguishable from an accepting protocol transcript generated by a real scheme run.

Proof 0.4 Then we assume a probabilistic polynomial-time simulator S would access to the random oracle $\mathcal{H}$. Then we construct $\text{Exp}_{\text{ZK-sim}}$ to make zero-knowledge proof in the random oracle model. Let $\text{Exp}_{\text{ZK-real}} = 1$ denotes the output of the interactive scheme between the real prover and the designated-verifier. $\text{Exp}_{\text{ZK-sim}} = 1$ means the simulator's output. The simulator S for our first scheme described in Fig 1 is constructed: query the random oracle $\mathcal{H}$ with input S'_B and output $K' = H(W') = H(\text{Mod}_2(P_A^T \cdot S'_B, \omega'))$ which $\omega' = \text{Char}(P_A^T \cdot S'_B)$.

According to the construction, we claim that the outputs from a probabilistic polynomial-time simulator are indistinguishable from an accepting protocol transcript generated by a real scheme run.

Considering the scheme of expandability, the prover would send $K = H(W)$ and ω encrypted with a symmetric key K_{PV} between prover and verifier. So no one can get the proof and the secret from the proof, except for the designated-verifier. At the same time, the verifier cannot obtain secret information except proof. We send $K = H(W)$ and ω with encryption in security communication for resisting the replay attack and man-in-the-middle attack.

Publicly-verifiable non-interactive zero-knowledge proof based on RLWE key exchange

Syntax

We consider zero-knowledge proof in publicly-verifiable scenario for ownership with three participants: the third-party(T) who is curious-but-honest, prover(P) who provides the proof without revealing the secret, verifier(V) who verifies the prove in Fig 3.

A non-interactive zero-knowledge scheme based key exchange from lattice includes a set of five polynomial-time algorithms(Setup, Register, Proof, Verify, Update). Then we briefly describe the process followed by five polynomial-time algorithms, shown in Fig 4.

1. **Setup** (1^p) $\rightarrow P$: The setup algorithms takes as the security parameters p , everyone could choose uniformly random matrix M and obtain the secret vector S which is satisfying Discrete Gaussian Distribution, and outputs the public key P .
2. **Register** (M, P_A, P_C) $\rightarrow (I, J)$: The register algorithm takes as input the parameters M , public key of P is P_A , public key of T for P is P_B , the corresponding public key P_C , signal function ω and v for eliminating the errors, and outputs I, W and J . T would save P_A, I, W and open P_A, J and ID_P which is the identity of prover.

Fig 3. The publicly-verifiable scheme architecture.

<https://doi.org/10.1371/journal.pone.0256372.g003>

3. **Proof** $(S_A, P_B, P_C, \omega) \rightarrow K$: Given S_A, P_B, P_C, ω , P would obtain the zero-knowledge proof K . Then P should send the public key P_A and the zero-knowledge proof K to verifier without encryption.
4. **Verify** $(K) \rightarrow \{0, 1\}$: After receiving the proof, V would find J by P_A from the third-party. Then V would verify if $H(K)$ is equal to J .
5. **Update** $J \rightarrow J, J_1$: Given the P_A, I_1, P_D, ω_1 , T should verify whether I_1 is equal to I or not firstly. If they were equal, then T would open P_A, J, J_1, ID_P and ID_{P_1} .

Security model

In this subsection, we provide the security model for the publicly-verifiable non-interactive zero-knowledge proof. Although the definition of non-interactive zero-knowledge remains unchanged, a semi-trusted third-party is introduced. Our security model is based on the curious-but-honest model and a random oracle model in federated learning [36, 43]. The semi-trusted third-party is curious-but-honest which means it does not deviate from the defined but tends to obtain all possible information from the legitimately received messages. In other words, the semi-trusted third-party only attempts to know the secret key of the prover, but he will not deceive other users with the proof he knows. Therefore, we can divide potential adversaries into the following:

1. An external adversary who is able to obtain public information. He attempts to give valid proof before the semi-trusted party issue.
2. The semi-trusted party as an internal adversary not only obtain the information from the phase of Register and Proof, but also possess the update key for all signers in the system.

Fig 4. Publicly-verifiable non-interactive zero-knowledge based on key exchange.

<https://doi.org/10.1371/journal.pone.0256372.g004>

In our second scheme, for the prover, he cannot forge an effective proof to deceive the semi-trusted third party and verifiers. For a semi-trusted third-party, he cannot obtain the secret key of the prover. For the verifier, he can neither obtain the secret key nor forge the proof of the secret value. Through the above analysis, it is clear that the security can be guaranteed if and only if the scheme satisfies the definition of zero-knowledge.

The scheme in detail

The system first generates the public parameters q, n, α , where $q > 8$ is an odd prime. Let M be a uniformly random matrix $M \leftarrow R_q^{n \times n}$. Let $H_1: \{0, 1\}^{n \times n} \rightarrow \{0, 1\}^n$ and $H_2: \{0, 1\}^{n \times n} \rightarrow \{0, 1\}^n$ be random oracles. The secret information owner P has $P_A = M \cdot S_A + 2e_A \bmod q$ where $S_A, e_A \leftarrow \chi_\alpha$ are $n \times n$ dimensional same as above mentioned and S_A is secret information. Meanwhile, its public key is $P_C = M \cdot S_C + 2e_C \bmod q$ where $S_C, e_C \leftarrow \chi_\alpha$ are $n \times n$ dimensional and S_B is its secret key. Similarly for the third-party T , its public key for P is $P_B = M^T \cdot S_B + 2e_B \bmod q$ while S_B is its secret key. $P_A, S_A, P_B, S_B, P_C, S_C$ are used to create the zero-knowledge proof for

verifiers V . Otherwise, T has a list for public and a symmetric key K_{PT} between prover and verifier.

The second scheme is composed of four algorithms except Setup algorithm: Register, Proof, Verify and Update. We specify it in full detail:

1. Register:

The secret information owner P does the following:

- Let $X = S_A^T \cdot P_B \cdot P_C$, $x = S_A^T \cdot P_B$, P computes $C \leftarrow E_{K_{PT}}(P_A, P_C, K, \omega, v)$, where $\omega = \text{Char}(x)$ and $v = \text{Char}(x)$.
- P sends C to T .

Upon receiving C , T does the following:

- T computes $(P_A, P_C, K, \omega, v) \leftarrow D_{K_{PT}}(C)$.
- T checks if $P_A \in \text{list}$, reject. If $P_A \notin \text{list}$ and P is a certified legal user by T , T adds it to the list.
- Let $Y = P_A^T \cdot S_B \cdot P_C$, $y = P_A^T \cdot S_B$, T computes $I \leftarrow \text{Mod}_2(y, v)$ and $W \leftarrow H_1(\text{Mod}_2(Y, \omega))$.
- T computes $J \leftarrow H_2(W)$.
- T saves (P_A, I, W) and opens (P_A, P_B, J, ID_P) Where ID_P is the identity of prover.

2. Proof:

- T computes $K \leftarrow H_1(\text{Mod}_2(X, \omega))$ as the zero-knowledge proof. In fact, $\text{Mod}_2(X, \omega)$ could be computed in the Register algorithm. The Proof algorithm only needs to calculate a hash operation.
- T opens (P_A, K) .

3. Verify:

Upon receiving (P_A, K, J) , everyone could do the following especially verifiers:

- After checking information is issued by ID_P , then it computes $H_2(K)$ firstly.
- V checks if $H_2(K) \stackrel{?}{=} J$. Accept if $H_2(K) = J$, otherwise reject.

4. Update:

The secret information owner P_1 does the following:

- P computes $I' \leftarrow \text{Mod}_2(x, v)$.
- P samples $S_D, e_D \leftarrow \chi_\alpha$ and computes $P_D = M \cdot S_D + 2e_D \bmod q$.
- Let $X_1 = S_A^T \cdot P_B \cdot P_D$, P computes $\omega_1 = \text{Char}(X_1)$ and $C_1 \leftarrow E_{K_{PT}}(P_A, I', P_D, \omega_1)$.
- P sends C_1 to T .

Upon receiving C_1 , T does the following:

- T computes $(P_A, I', P_D, \omega_1) \leftarrow D_{K_{PT}}(C_1)$.
- Let $Y_1 = P_A^T \cdot S_B \cdot P_D$, T checks if I' is equal to I . If they are equal, then it outputs $W_1 \leftarrow H_1(\text{Mod}_2(Y_1, \omega))$ and $J_1 \leftarrow H_2(W_1)$.
- T saves (P_A, I, W, W_1) and opens $(P_A, P_B, J, J_1, ID_P, ID_{P_1})$.

Security analysis

In this subsection, we prove that our zero-knowledge proof-based key exchange scheme is security over LWE in public under the hardness assumption from the following aspects.

Lemma 7 Let $R = \mathbb{Z}[x]/(x^n + 1)$, for any $a, b, c \in R$, we can easily obtain $\|a \cdot b \cdot c\| \leq n \cdot \|a\| \cdot \|b\| \cdot \|c\|$ and $\|a \cdot b \cdot c\|_\infty \leq \|a\|_\infty \cdot \|b\|_\infty \cdot \|c\|_\infty$ by Lemma 1.

Lemma 8 Let $q > 16\sigma^3 n^{\alpha/2}$, then $\text{Mod}_2(X, \omega) = \text{Mod}_2(Y, \omega)$, except with negligible probability.

Proof 0.5 Firstly, we know that $X = S_A^T \cdot P_B \cdot P_C$, $Y = P_A^T \cdot S_B \cdot P_C$.

$$\text{Then, } X - Y = (x - y) \cdot P_C$$

Prove similarly to Lemma 4, $X, Y \in R_q^{n \times n}$, then we just show that $\|X_{ij} - Y_{ij}\|_\infty < \frac{q}{4}$ by Lemma 3, where $i, j \in \{1, \dots, q\}$. After simplification, combining with Lemma 2 and Lemma 7, we have that

$$\begin{aligned} \|X_{ij} - Y_{ij}\| &\leq \|2[S_{A_{ij}}^T \cdot e_{B_{ij}} - e_{A_{ij}}^T \cdot S_{B_{ij}}]\| \cdot \|P_C\| \\ &< 4n \cdot (\sigma\sqrt{n})^3 \end{aligned}$$

By Lemma 3, we obtain $\|X_{ij} - Y_{ij}\|_\infty < 4\sigma^3 n^{5/2} < \frac{q}{4}$.

Then, $q > 16\sigma^3 n^{5/2}$ with probability $1 - 2^{-n}$.

1) Completeness. The proof from prover is as follows:

Since $K = H_1(\text{Mod}_2(X, \omega))$, $\text{Mod}_2(X, \omega)$ could be calculated in the previous Register algorithm, then K is only obtained by the hash operation as the proof for verifier.

The verifier gets the verification value J from the third-party and verifies K whether it is true or not by the hash function $J = H_2(K)$.

By Lemma 8, let $q > 16\sigma^3 n^{\alpha/2}$, if S_A^T is true, then

$$\text{Mod}_2(X, \omega) = \text{Mod}_2(Y, \omega).$$

except with negligible probability.

Then, we have that

$$K = H_1(\text{Mod}_2(X, \omega)) = H_1(\text{Mod}_2(Y, \omega)) = W$$

Finally, if K is true, $H_2(K)$ will be equal to J with probability $1 - 2^{-n}$, where $J = H_2(W)$. Then the verifier will be convinced that the prover owns the secret. That means, for $\forall P_A, P_B, P_C \in \mathcal{L}$, if the prover has the secret value S_A^T , then

$$\Pr [K \leftarrow P(S_A^T, P_A, P_B, P_C) : V(J_{(P_A, P_B, P_C)}, K) = 1] \geq 1 - 2^{-n}.$$

2) Soundness. Soundness means that the adversary has no secret value S_A and convinces the honest verifier that the secret value is true with negligible probability. In other words, if the prover has no secret value S_A , for $\exists P_A, P_B, P_C$, then

$$\Pr [K' \leftarrow P(P_A, P_B, P_C) : V(J_{(P_A, P_B, P_C)}, K') = 1] = \text{negl}.$$

Its analysis is similar to the soundness of the designated-verifier scheme in Fig 1. According to the second scheme in Fig 2, there are three participants: the third-party(T) who is curious-but-honest, prover(P), and verifier(V). Then we should consider this property from the third-party and the verifier.

- Between a malicious prover and the third-party.

Assume prover as the adversary that can register without the secret S_A with the non-negligible probability. This analysis is similar to the soundness of the designated-verifier scheme in Fig 1. According to Lemma 5, we can get the following Lemma 9 easily. Then the adversary cannot register successfully the verifier to believe him without knowing the secret value with negligible probability.

Lemma 9 *If prover as the adversary A who could register successfully using $P_A = M \cdot S_A + 2e_A \bmod q$ without the secret of S_A in the curious-but-honest third-party with non-negligible probability, then there is a distinguisher for P_A from uniform with the same probability.*

- Between a malicious prover and the verifiers.

Assume prover as the adversary that can make a valid proof K without the secret S_A with the non-negligible probability. According to the second scheme in Fig 2, the adversary only gets valid proof from P_A or J . Since the analysis of the above, we have already known that the prover is the adversary who only has P_A without S_A to convince the verifiers with negligible probability. Then the malicious prover only makes a valid proof from J . As the scheme described in Fig 2, we know that $J = H_2(K)$. That means the adversary can calculate the inverse of the hash function output J . However, one of the important hash function properties is that if H is collision-resistant, then $H(x)$ is hard to invert.

Lemma 10 *If prover as the adversary A who could generate a valid proof K for $P_A = M \cdot S_A + 2e_A \bmod q$ without the secret of S_A with non-negligible probability, then there is a distinguisher for P_A from uniform with the same probability, or the adversary can calculate the inverse of the hash function output.*

Above all considering, we believe that the adversary cannot successfully deceive the verifier without S_A , then we have that

$$\Pr [K \leftarrow \text{Adversary}(\cdot, P_A, P_B, P_C) : V(J_{(P_A, P_B, P_C)}, K) = 1] = \text{negl}.$$

3) Zero-knowledge. In the second scheme, S_A as the secret value, it must not be a leak in the whole process of proof. Because the proof can be verified by anyone especially the verifier, so we consider this property from the verifier and the third-party.

- For the verifier:

From the scheme beginning to the end, the verifier can only obtain P_A, K, J , where

$$P_A = M \cdot S_A + 2e_A \bmod q \quad (1)$$

$$K = H_1(\text{Mod}_2(X, \omega)) \quad (2)$$

$$J = H_2(W) = H_2(H_1(\text{Mod}_2(Y, \omega))) \quad (3)$$

From Eq (1), we can see that S_A will not be obtained from P_A under the Ring-LWE assumption. Since K and J are the results of hash function operation from equations Eqs (2) and (3), where K and J are n bits value, the secret value S_A will not be disclosed. According to the above analysis of soundness, the verifier can not get the secret value or a valid proof.

- For the third-party:

T, who is curious-but-honest, acts as the intermediary between the prover and the verifier. T has more values including $S_B, P_B, \omega, v, I, W$ except S_A .

$$\omega = \text{Char}(X) \quad v = \text{Char}(x) \quad (4)$$

$$I = \text{Mod}_2(y, v) \quad (5)$$

$$W = H_1(\text{Mod}_2(Y, \omega)) \quad (6)$$

In fact, the third-party has known the proof before the prover announced it. T is curious-but-honest means that T is eager to know the secret value of S_A and can not reveal any other values. From equations Eqs (4)–(6), we can make our second scheme is zero-knowledge for the third-party according to the above Lemma 6. Then this scheme is the honest-verifier zero-knowledge for the third-party.

Based on the above discussion, we can get the conclusion that there is no secret value leakage. Assume that there is a polynomial-time simulator, for all $P_A, P_B, P_C \in L$ and secret value S_A , the following two distributions are computationally indistinguishable

$$\|Pr [Exp_{ZK-real} = 1] - Pr [Exp_{ZK-sim} = 1]\| = \text{negl}.$$

The prover sends K with encryption in security communication for resisting the brute force attack and man-in-the-middle attack. In order to resist the replay attacks, the third-party opens ID_P except P_A, J .

Efficiency analysis

According to existing post-quantum schemes, we analyze the efficiency of the zero-knowledge proof schemes from the prover runtime, verification time, CRS size, and proof size [44]. Since the proof can be given off-line in advance, the prover's operation time is no longer considered here. Meanwhile, our schemes based on lattice key exchange do not involve CRS, so the size of CRS can be considered to be zero. Therefore, our proposed scheme is only compared with the previous study [27, 31–35] in verification time and proof size, which is described in more detail in Table 2.

In previous studies, the proof size in [27] is more than $4nM\log(q)$ bits, where n is a security parameter in the ring $\mathbb{Z}_q$ and M means the number of protocol rounds. And the $\text{poly}(n)$ means that the verification time is polynomial-time which is used in the following. In [31], the proof size is $\sqrt{m\log(m)}$ and the verification time is m , where m is the number of gates. In [32], the proof size is more than $1024t$ bits, where t means repeating the protocol times. The proof size

Table 2. Comparison the efficiency of related zero-knowledge proof schemes.

Scheme	Proof Size	Verification Time	Interactive	Untrusted-Setup	Assumptions
[27]	$4nM\log(q)$	$\text{poly}(n)$	YES	YES	RLWE
[31]	$\sqrt{m\log(m)}$	m	YES	YES	SIS
[32]	$1024t$	$\text{poly}(n)$	NO	YES	RSIS & RLWE
[33]	$c_2 n_2$	$\text{poly}(n)$	YES	YES	LWE
[34]	$512 + c_1 n_1$	$\text{poly}(n)$	NO	YES	SVP
[35]	k_1	l_1	NO	NO	q-PKE
Our scheme I	k_2	$\text{poly}(n)$	NO	YES	RLWE
Our scheme II	k_2	l_2	NO	SEMI	RLWE

<https://doi.org/10.1371/journal.pone.0256372.t002>

in [34] is larger than $512 + n_1(8\log(4\alpha n_1) + 2048\log(2\alpha))$ bits, where n_1 is the number of secrets, α is the security parameter. In Table 1, c_1 is used to represent a number greater than $8\log(4\alpha n_1) + 2048\log(2\alpha)$. The proof size and the verification time in [35] are constant. Here, $k_1 = 5(a+1)\log(q)$ represents the proof size, where a is the number of elements in the vector, which is also a security parameter. And l_1 represents the verification time. However, this scheme is based on ZK-SNARKs from SSP, the proof size is still large and the cost of computation is relatively expensive. At this time, the CRS size is more than $(3d+2)\log(q)$, where d is the degree of SSP. The proof size in [33] is $n_2 \cdot k \cdot \log(6\sigma) + n_2 \cdot \ell \cdot \log(q)$ which is replaced by $c_2 n_2$. Where n_2 and q are security parameters, n_2 is also the bit number of secrets, k is the width of the commitment matrices over R_q , σ is the standard deviation. The commitments are a guarantee condition sent by the prover to the verifier in commitment scheme [33]. when the width of the commitment matrices over R_q is equal to 1, the commitment size is $n_2 \cdot \log(q)$. Our schemes combine the key-exchange based on RLWE with the hash function so that proof size is only the output length of the hash function. k_2 represents the proof size of our schemes. Verification time is expressed as l_2 , which is a hash function operation for the publicly-verifiable scenario. Furthermore, Table 2 shows a comparison of other properties, including CRS or interactive, untrusted-Setup and assumptions, where q-PKE is the q-power knowledge of exponent assumption, (R)SIS is (Ring) short integer solution problem and SVP means shortest vector problem.

As shown in the result, our proof is the output of the hash function which its size does not change due to the size of secret values. In other words, the proof size does not become as large as the size of secret values increases. The commitment will be sent to the verifier along with the proof, as a condition for verification like a CRS. Therefore, we also give the corresponding commitment size in [33] and the CRS size in [35]. Given the security parameter is 1024, q is 2^{32} , d is 2^{15} , and the fixed output of the hash function is 512 bits. To intuitively show the performance of our second scheme, we compared the proof size of our second scheme, the optimal scheme of Baum et al. [33], and the scheme of [35] in Table 3 and in Fig 5. And the result indicates that our second scheme proof size is much smaller and constant.

For the verification time, our second scheme has only one hash operation time. However, the scheme of Baum et al. takes polynomial time to verify a matrix polynomial. For the scheme of [35], the verifier needs to encode several polynomials before calculating three polynomials during verification. Obviously, both of the above schemes take more time than our second scheme.

We have compared our second scheme with the related schemes in zero-knowledge proof size and verification time. Since the proof is the output of the hash function, our proof size is constant. So its size is smaller than that of other compared schemes in zero-knowledge proof size. In addition, the verifiers' runtime of our scheme for publicly-verifiable only involves the hash operation, so its computation is lower than that of other compared schemes in verification time.

Table 3. Approximate comparison.

Scheme	Other	Proof Size
Our scheme II	0	0.5KB
[33]	Commitment Size $\approx$ 8.1KB	6.6KB
[35]	CRS Size $\approx$ 3MB	160KB

<https://doi.org/10.1371/journal.pone.0256372.t003>

Fig 5. Impact of the secret value size on proof size.

<https://doi.org/10.1371/journal.pone.0256372.g005>

Conclusion

With the surprising development of quantum computers, it is an urgent requirement to construct efficient quantum-secure zero-knowledge proof schemes. In this paper, we have proposed a non-interactive zero-knowledge proof scheme for the designated-verifier to guarantee less proof size. We have also designed the scheme of RLWE-based key exchange from lattice for the publicly-verifiable scenario to ensure better effectiveness. Moreover, our schemes are secure from completeness, soundness, and zero-knowledge. Furthermore, compared with other previous schemes, we find that our schemes have more advantages in proof size and verification time. In the future, based on the abundant theoretical basis of lattice cryptography, we will design better performed zero-knowledge proof schemes for multiple applications.

Supporting information

S1 Table. The process of approximate comparison.
(XLSX)

S1 Fig. Impact of the secret value size on proof size.
(XLSX)

Author Contributions

Formal analysis: Shaofen Xie, Faguo Wu.

Methodology: Shaofen Xie, Wang Yao, Faguo Wu.

Supervision: Zhiming Zheng.

Writing – original draft: Shaofen Xie.

Writing – review & editing: Shaofen Xie, Faguo Wu, Zhiming Zheng.

References

1. Wang H, Sun L, Bertino E. Building access control policy model for privacy preserving and testing policy conflicting problems. *Journal of Computer and System Sciences*. 2014; 80(8):1493–1503. <https://doi.org/10.1016/j.jcss.2014.04.017>

2. Wang S, Zhang Q, Zhang Y, Sun J, Chen J, Sun X, et al. Improving the proof of "Privacy-preserving attribute-keyword based data publish-subscribe service on cloud platforms". PLoS ONE. 2019; 14(2). <https://doi.org/10.1371/journal.pone.0212761>
3. Ge YF, Yu WJ, Cao J, Wang H, Zhang J. Distributed Memetic Algorithm for Outsourced Database Fragmentation. IEEE Transactions on Cybernetics. 2020; PP(99):1–14.
4. Ge YF, Cao J, Wang H, Zhang Y, Chen Z. Distributed Differential Evolution for Anonymity-Driven Vertical Fragmentation in Outsourced Data Storage. In: International Conference on Web Information Systems Engineering. Springer; 2020. p. 213–226.
5. Wang H, Wang Y, Taleb T, Jiang X. Special issue on security and privacy in network computing. World Wide Web. 2020; 23(2):951–957. <https://doi.org/10.1007/s11280-019-00704-x>
6. Zhang F, Wang Y, Liu S, Wang H. Decision-based evasion attacks on tree ensemble classifiers. World Wide Web. 2020;(1-4).
7. Vimalachandran P, Liu H, Lin Y, Ji K, Wang H, Zhang Y. Improving accessibility of the Australian My Health Records while preserving privacy and security of the system. Health Information Science and Systems. 2020; 8(1):1–9.
8. Goldwasser S, Micali S, Rackoff C. The knowledge complexity of interactive proof systems. SIAM Journal on computing. 1989; 18(1):186–208. <https://doi.org/10.1137/0218012>
9. Blum M, Feldman P, Micali S. Non-interactive zero-knowledge and its applications. In: Proceedings of the twentieth annual ACM symposium on Theory of computing. ACM; 1988. p. 103–112.
10. Adelsbach A, Sadeghi AR. Zero-knowledge watermark detection and proof of ownership. In: International Workshop on Information Hiding. Springer; 2001. p. 273–288.
11. Shahandashti S, Safavi-Naini R, Baek J. Concurrently-secure credential ownership proofs. In: Proceedings of the 2nd ACM symposium on Information, computer and communications security. ACM; 2007. p. 161–172.
12. Dwork C, Naor M, Sahai A. Concurrent zero-knowledge. Journal of the ACM (JACM). 2004; 51(6):851–898. <https://doi.org/10.1145/1039488.1039489>
13. Ben-Sasson E, Chiesa A, Genkin D, Tromer E, Virza M. SNARKs for C: Verifying program executions succinctly and in zero knowledge. In: Annual Cryptology Conference. Springer; 2013. p. 90–108.
14. Unruh D. Non-interactive zero-knowledge proofs in the quantum random oracle model. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer; 2015. p. 755–784.
15. Peng K, Boyd C, Dawson E. Batch zero-knowledge proof and verification and its applications. ACM Transactions on Information and System Security (TISSEC). 2007; 10(2):6. <https://doi.org/10.1145/1237500.1237502>
16. Gentry C, Groth J, Ishai Y, Peikert C, Sahai A, Smith A. Using fully homomorphic hybrid encryption to minimize non-interactive zero-knowledge proofs. Journal of Cryptology. 2015; 28(4):820–843. <https://doi.org/10.1007/s00145-014-9184-y>
17. Chain K, Chang KH, Kuo WC, Yang JF. Enhancement authentication protocol using zero-knowledge proofs and chaotic maps. International Journal of Communication Systems. 2015; 30(1):e2945.1–e2945.17.
18. Lindell Y. An efficient transform from Sigma protocols to NIZK with a CRS and non-programmable random oracle. Springer; 2015. p. 93–109.
19. Ciampi M, Persiano G, Siniscalchi L, Visconti I. A Transform for NIZK Almost as Efficient and General as the Fiat-Shamir Transform Without Programmable Random Oracles. In: Theory of Cryptography—13th International Conference. vol. 9563 of Lecture Notes in Computer Science. Springer; 2016. p. 83–111.
20. Groth J. Short Pairing-based Non-interactive Zero-Knowledge Arguments. In: International Conference on the Theory and Application of Cryptology and Information Security. Springer; 2010. p. 321–340.
21. Chen L, Jordan S, Liu YK, Moody D, Peralta R, Perlner R, et al. Report on post-quantum cryptography. US Department of Commerce, National Institute of Standards and Technology; 2016.
22. Ajtai M. Generating hard instances of lattice problems(Extended Abstract). In: Proceedings of the twenty-eighth annual ACM symposium on Theory of computing. ACM; 1996. p. 99–108.
23. Lyubashevsky V, Peikert C, Regev O. On ideal lattices and learning with errors over rings. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer; 2010. p. 1–23.
24. Lyubashevsky V. Lattice signatures without trapdoors. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer; 2012. p. 738–755.

25. Lyubashevsky V, Neven G. One-shot verifiable encryption from lattices. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer; 2017. p. 293–323.
26. Benhamouda F, Camenisch J, Krenn S, Lyubashevsky V, Neven G. Better zero-knowledge proofs for lattice encryption and their application to group signatures. In: International Conference on the Theory and Application of Cryptology and Information Security. Springer; 2014. p. 551–572.
27. Benhamouda F, Krenn S, Lyubashevsky V, Pietrzak K. Efficient zero-knowledge proofs for commitments from learning with errors over rings. In: European symposium on research in computer security. Springer; 2015. p. 305–325.
28. Lyubashevsky V, Seiler G. Short, invertible elements in partially splitting cyclotomic rings and applications to lattice-based zero-knowledge proofs. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer; 2018. p. 204–224.
29. Baum C, Damgård I, Larsen KG, Nielsen M. How to prove knowledge of small secrets. In: Annual International Cryptology Conference. Springer; 2016. p. 478–498.
30. Esgin MF, Steinfeld R, Liu JK, Liu D. Lattice-based zero-knowledge proofs: new techniques for shorter and faster constructions and applications. In: Annual International Cryptology Conference. Springer; 2019. p. 115–146.
31. Baum C, Bootle J, Cerulli A, Del Pino R, Groth J, Lyubashevsky V. Sub-linear lattice-based zero-knowledge arguments for arithmetic circuits. In: Annual International Cryptology Conference. Springer; 2018. p. 669–699.
32. Bootle J, Lyubashevsky V, Seiler G. Algebraic techniques for short (er) exact lattice-based zero-knowledge proofs. In: Annual International Cryptology Conference. Springer; 2019. p. 176–202.
33. Baum C, Damgård I, Lyubashevsky V, Oechsner S, Peikert C. More efficient commitments from structured lattice assumptions. In: International Conference on Security and Cryptography for Networks. Springer; 2018. p. 368–385.
34. Del Pino R, Lyubashevsky V. Amortization with fewer equations for proving knowledge of small secrets. In: Annual International Cryptology Conference. Springer; 2017. p. 365–394.
35. Gennaro R, Minelli M, Nitulescu A, Orrù M. Lattice-based zk-snarks from square span programs. In: Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. ACM; 2018. p. 556–573.
36. Ding J, Saraswathy R, Alsayigh S, Clough C. How to validate the secret of a Ring Learning with Errors (RLWE) key. IACR Cryptology ePrint Archive. 2018; 2018:81.
37. Regev O. On lattices, learning with errors, random linear codes, and cryptography. *Journal of the ACM (JACM)*. 2009; 56(6):34.
38. Zhang J, Zhang Z, Ding J, Snook M, Dagdelen Ö. Authenticated key exchange from ideal lattices. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer; 2015. p. 719–751.
39. Micciancio D, Regev O. Worst-case to average-case reductions based on Gaussian measures. *SIAM Journal on Computing*. 2007; 37(1):267–302. <https://doi.org/10.1137/S0097539705447360>
40. Ding J, Xie X, Lin X. A Simple Provably Secure Key Exchange Scheme Based on the Learning with Errors Problem. IACR Cryptology ePrint Archive. 2012; 2012:688.
41. Ding J, Alsayigh S, Saraswathy R, Fluhrer S, Lin X. Leakage of signal function with reused keys in RLWE key exchange. In: 2017 IEEE International Conference on Communications (ICC). IEEE; 2017. p. 1–6.
42. Gao X, Ding J, Li L, Liu J. Practical randomized rlwe-based key exchange against signal leakage attack. *IEEE Transactions on Computers*. 2018; 67(11):1584–1593. <https://doi.org/10.1109/TC.2018.2808527>
43. Wu F, Yao W, Zhang X, Zheng Z. Lattice based signature with outsourced revocation for Multimedia Social Networks in cloud computing. *Multimedia Tools and Applications*. 2019; 78(3):3511–3528. <https://doi.org/10.1007/s11042-018-6330-9>
44. Maller M, Bowe S, Kohlweiss M, Meiklejohn S. Sonic: Zero-Knowledge SNARKs from Linear-Size Universal and Updateable Structured Reference Strings. IACR Cryptology ePrint Archive. 2019; 2019:99.