An Improved Non-Interactive Zero-Knowledge Range Proof for Decentralized Applications

1st Ya-Che Tsai
Department of Computer Science
National Chengchi University
Taiwan
106753028@nccu.edu.tw

2nd Raylin Tso
Department of Computer Science
National Chengchi University
Taiwan
raylin@cs.nccu.edu.tw

3rd Zi-Yuan Liu
Department of Computer Science
National Chengchi University
Taiwan
105753036@nccu.edu.tw

4th Kung Chen
Department of Computer Science
Department of Management Information Systems
National Chengchi University
Taiwan
chenk@cs.nccu.edu.tw

***Abstract*—Blockchain is the core technology underlying the first decentralized cryptocurrency, Bitcoin, introduced by Nakamoto in 2008. Since then, blockchain technology has many more advancements that are being developed and experimented. In particular, recent blockchain platforms such as Ethereum offer general and executable scripts, namely smart contracts, that can be employed to develop decentralized applications (DApps) in many domains beyond payment. However, the transparency of blockchain data raises concerns for many applications that require high privacy level. Therefore, many privacy enhancing technologies have been applied to DApp development, including zero knowledge proof (ZKP). This paper focuses on a particular kind of ZKP, called zero knowledge range proof (ZKRP), that has been applied in blockchain-based payments for banks. ZKRP allows a user to convince other people that a secret value actually lies within an interval without revealing any information about the secret. Here we introduce a new ZKRP which has the following remarkable features: (1) Non-interactive: No communication is required between a user and a verifier during the proof. (2) Range-flexibility: There is no limitation on the lower bound and the upper bound of the range except that they are natural numbers. (3) Efficiency: Our scheme is modified from that of Pang et al. (2010), yet achieves better security and is more efficient than their scheme. We believe our new ZKRP can be beneficial to the development of DApps and can extend the application scope to more scenarios.**

***Index Terms*—Blockchain, Commitment scheme, Non-interactive zero-knowledge, Privacy protection, Range proof**

I. Introduction

Bitcoin is the first electronic money system that operates on a peer-to-peer network with no central authority yet secured by cryptographic techniques. The issuance of bitcoins and transactions management are collectively carried out by the network through a trustless consensus process. Thus bitcoin is generally referred to as a kind of decentralized cryptocurrency. The core technology supporting the running of bitcoin is blockchain, which maintains a distributed yet synchronized ledger that keeps track of all bitcoin transactions in an open and transparent but anonymized manner. Besides, by the application of cryptographic techniques, transactions recorded by blockchain are virtually immutable.

Decentralized applications (DApp) refer to applications running on top of blockchain in a decentralized peer-to-peer network. Due to the recent advancement of blockcahin technology with general executable scripts, namely smart contracts, there have been many interesting DApps developed in many domains. However, as data on blockchain are transparent and accessible to anyone, it is not practical to develop DApps that require a high privacy level without a proper data protection. Therefore, many privacy enhancing technologies have been applied to DApp development, including zero knowledge proof (ZKP). The goal is apparently to strike a balance between transparency and confidentiality when developing DApps.

Zero knowledge proof (ZKP) provides the ability to prove a secret without revealing it directly. It guarantees that a proof does not reveal more about private input and what cannot be inferred from the result of the computation. There have been several results published that apply ZKP to solve the privacy concern of blockchain in a general manner [11], [15], [21]. This paper focuses on a particular kind of ZKP, called zero knowledge range proof (ZKRP), that has been successfully applied to, among others, blockchain-based payments for banks. ZKRP provides the ability to convince other people that a secret value actually lies within an interval without revealing any information from its witness. This capability is useful for many kinds of DApp based sysems, such as e-cash, e-voting, and e-auctions system [9], [14], [15].

For instance, age is an essential requirement for the e-voting system. By comparing a person's real age number with that required by law, we can easily verify whether this person is a qualified voter. However, we may consider age as a kind of personal privacy and would like to hide the real age when doing the validation. In this situation, the characteristic of ZKRP is suitable to solve this problem. It allows the

978-1-7281-1264-0/19/$31.00 ©2019 IEEE
DOI 10.1109/DAPPCON.2019.00025

person to claim that his or her age is compliant with the law, without revealing the real age number. Regarding research on range proof schemes, Peng et al. have proposed a series of approaches [16]–[20] to ZKRP. Each of them has its own advantages and is suitable for different applications based on difference techniques. Among them, it has been implemented in the blockchain in recent work.

Koens et al. changed the range proof scheme [18] into non-interactive and employed smart contracts to implement it on Ethereum [10] in 2017. Although they successfully realized the range proof scheme, their approach has some drawbacks which cannot be ignored. Firstly, it has been discovered a potential security vulnerability by Madars Virza, Research Scientist MIT Media Lab[1]. More precisely, this range proof scheme has a parameter which is set up as a fixed bit length in practice. It allows the adversary have the ability to get a more accurate range of the secret value. Secondly, comparing the number of computation in modulo exponentiations of [2], [18], and our work. It is 40, 33, and 30 times for each scheme. Our work not only has the best efficient in this three scheme but does not have the potential security vulnerability. Finally, comparing to interactive zero-knowledge in [18], we found out that non-interactive zero-knowledge is more suitable for blockchain-based applications in practice.

Because non-interactive ZKRP is more suitable and better than interactive ZKRP to be used on blockchain in practice, there are many research results and applications of non-interactive ZKRP have been proposed [1], [5], [13], [23]. The famous work recently is by Bünz et al., which presents a range proof scheme for confidential transactions [3], [4]. In this protocol, the secret number is transformed into binary first, then the inner product of two polynomials is computed to obtain a zero knowledge proof. Both its performance and system size are better than other related results. However, this scheme still has a drawback. Their range must be a fixed form, that is $[0, \ldots, 2^n - 1]]$, where n is a bit number. Precisely, their lower bound must be zero, and the upper bound must be the number of an exponent of two. Of course, one may execute their protocol twice to prove a number in the difference range form, such as $[2^n - 1, 2^n, \ldots 2^{2n} - 1]$, but this range form is still fixed by this scheme.

A. Contribution

In this paper, we propose a new non-interactive ZKRP scheme, which provides substantial improvements from the previous schemes [10], [18]. We utilize the Fujisaki-Okamoto commitment, non-interactive zero-knowledge and computational bindingness through proof of knowledge in the cyclic group with secret order technique (CBPKCGSO) [18] in our protocol. The CBPKCGSO can prove that m is in a range $[a, b]$ by using $m - a$ and $b - m$ both bigger than 0. According to these techniques and new logical design, our new scheme maintains high flexible range form and solves the potential security in [10]. Even if the parameter is still being a fixed bit length, an adversary cannot utilize the publicly computable value to narrow down the given range in our new scheme. Besides, our new scheme satisfies three basic security properties of zero-knowledge proof: correctness, soundness, and zero-knowledge.

[1]Github, https://github.com/ing-bank/zkrangeproof, last accessed inSeptember 2018. But the new version replaces [18] with [2] to avoid this bug.

II. Preliminaries

A. Notation

We denote the set of natural numbers by $\mathbb{N}$, the set of integers by $\mathbb{Z}$, and the set of real numbers by $\mathbb{R}$. N is a large composite number which the factorization of N is unknown. $\mathbb{Z}_N^*$ is an integer group under multiplication modulo N without the factors of N. G is a subgroup of $\mathbb{Z}_N^*$ with a large order. We denote the range between a and b as $[a, b]$, where $a < b$, a is a lower bound and b is an upper bound for the given range. We define $a||b$ the concatenation of string a and string$b$. $X \xleftarrow{\$} Y(\cdot)$ means X is randomly chosen by Y which is a set up algorithm for choosing random number. Finally, we use *neg* to denote a negligible function.

B. Non-Interactive Zero-Knowledge

We present a general example based on [22] to introduce what an non-interactive zero-knowledge (*NIZK*) is. Firstly, we set up the system parameters p, q and g,where p, q are big prime numbers, and $g \in \mathbb{Z}_p^*$ is an element with order q ($g^q \ mod \ p = 1$). $H \subseteq G$ is a subgroup of order q generated by g. We denote $Hash(\cdot)$ be a secure hash function, r be a public identity of a user, and s be a private authenticator. Now, prover wants to prove the knowledge s which is hidden as $v = g^s \ mod \ p$. We simply discuss this non-interactive zero-knowledge as below.

- Prover:
  1) Pick $r \in \mathbb{Z}_p^*$ and computes $x = g^r \ mod \ p$
  2) Calculate $e = Hash(v)$
  3) Calculate $y = r + se \ mod \ q$
  4) Publish v, e, x, y
- Verifier: Accept if $x = g^y v^{-e} \ mod \ p$.

In this instance, we can see that prover do not interact with verifier and prover can convince the verifier that he/she knows s without revealing knowledge s.

C. Fujisaki-Okamoto commitment

Fujisaki-Okamoto commitment scheme was published by Fujisaki et al. [6]. It allows everyone to commit a chosen value while keeping it secret to others, and the prover has the ability to reveal the committed value later [7]. For the sake of simplicity, we let $E(x, r) = g^x h^r \ mod \ N$ to be the Fujisaki-Okamoto commitment with a secret x and a random number with bases (g, h). $N = pq$ is a large composite number where the prime factors p and q are unknown to anyone. g is an element in the group $\mathbb{Z}_N^*$ with a large order, and h is generated by g such that $h = g^L \ mod \ N$, where the relation $L \in \mathbb{Z}$ between g and h is unknown to anyone except the parameter generator.

Boudot asserted that Fujisaki-Okamoto commitment is a statically secure commitment scheme [2]. For example, we assume Alice utilizes Fujisaki-Okamoto commitment to commit two different values. She is unable to compute x_1, x_2, r_1, r_2, where $x_1 \neq x_2$ and $E(x_1, r_1) = E(x_2, r_2)$ due to the discrete logarithm problem as well as the factorization problem of N. Then, we assume Bob is trying to obtain the secret of the commitment generated by Alice. Because $E(x, r)$ is a statically secure commitment scheme, it reveals no information about x to Bob unless Alice publishes this secret.

D. The Secret Order Principle

The Secret Order Principle is based on the Integer Factorization Problem. This principle means that it is computationally infeasible to calculate any multiple of the order of a subgroup as long as the factorization of module N is intractable. Many papers [8], [10], [12], [18] have used this principle to prove that their privacy preserving protocols are secure. Moreover, the security of Fujisaki-Okamoto commitment is also based on this principle. Because of this property, it ensures that any adversary is unable to obtain the hidden secret from this commitment.

E. Knowledge of Discrete Logarithm in a Cyclic Group with a Secret Order (KDLCGSO)

KDLCGSO lets a party prove the knowledge of a secret m and a random number r such that $y = g^m h^r \ mod \ N$ without revealing this secret information. In [2], [12], [18], those papers use this KDLCGSO to prove that prover knows the secret in Fujisaki-Okamoto commitment. We denote P as a prover, and V as a verifier. P wants to convince V that he/she knows a secret $m \in \mathbb{Z}$. We simply discuss the process of KDLCGSO as follows.

- $P \rightarrow V$: P commits m as $y = g^m h^r \ mod \ N$ and makes another commitment $\alpha = g^{\chi} h^z \ mod \ N$, where $\chi, z \xleftarrow{\$} \mathbb{Z}$. Next, P publishes y and α to the verifier.
- $V \rightarrow P$: Verifier gives a challenge s to prover, where $s \xleftarrow{\$} \mathbb{Z}$.
- $P \rightarrow V$: Prover returns two responses $u = \chi - sm$ and $v = z - sr$ in $\mathbb{Z}$ to verifier
- Verification: V computes $g^u h^v c^s \ mod \ N$ and is convinced that P knows the secret value m if and only if $\alpha = g^u h^v c^s \ mod \ N$.

F. Two Commitments Hide the Same Secret Proof (EL Proof)

EL Proof was proposed by Boudot in 2000 [2]. This proof is used to validate that whether two commitment are hidden the same secret value or not. We follow the syntax in [18] and denote this proof as $EL(m, s, r|g, h_1, f, h_2|A, B)$. The EL function is a kind of zero-knowledge proof and is used to verify whether two commitments A and B where $A = g^m h_1^s \ mod \ N$ and $B = f^m h_2^r \ mod \ N$ hiding the same secret m or not. We simply review this protocol as below.

In the following protocol, (g, f, h_1, h_2, N) and a hash function $Hash$ can be regarded as public parameters. A prover and a verifier then do the following steps:

- Prover:
  1) Pick random integer numbers μ, υ_1, and υ_2 Then computes $C_1 = g^{\mu} h_1^{\upsilon_1} \ mod \ N$ and $C_2 = f^{\mu} h_2^{\upsilon_2} \ mod \ N$.
  2) Compute $H = Hash(C_1||C_2)$.
  3) Generate $X = \mu + Hm$, $X_1 = \upsilon_1 + Hs$, $X_2 = \upsilon_2 + Hr$
  4) Publish: (H, X, X_1, X_2).
- Verifier will check whether $Hash(g^X h_1^{X_1} A^{-H} \pmod N || f^X h_2^{X_2} B^{-H} \pmod N)$ is equal to H, $C_1 = g^X h_1^{X_1} A^{-H} \ mod \ N$, and $C_2 = f^X h_2^{X_2} B^{-H} \ mod \ N$.
  1) $C_1 = g^{\mu} h_1^{\upsilon_1} = g^{\mu + Hm} h_1^{\upsilon_1 + Hs} (g^m h_1^s)^{-H} = g^X h_1^{X_1} A^{-H} \ mod \ N$
  2) $C_2 = f^{\mu} h_2^{\upsilon_2} = f^{\mu + Hm} h_2^{\upsilon_2 + Hr} (f^m h_2^r)^{-H} N = f^X h_2^{X_2} B^{-H} \ mod \ N$
  3) $H = Hash(g^X h_1^{X_1} A^{-H} \pmod N || f^X h_2^{X_2} B^{-H} \pmod N) = Hash(C_1||C_2)$

If verifier can pass the above proof than verifier will believe that commitments A and B hide the same secret m.

G. Committed Number is a Square Proof (SQR Proof)

SQR Proof was proposed by Boudot in 2000 [2]. This proof is used to verify whether the secret number in commitment is a square number or not. We follow the syntax in [18] and denote this proof as $SQR(\alpha, r_1|g, h|E)$. The SQR function is a kind of zero-knowledge proof and is used to verify whether the commitment $E = g^{\alpha^2} h^{r_1} \ mod \ N$ hiding the square secret α^2 or not. We simply review this protocol as below.

In the following protocol, (g, h, E) and a hash function $Hash$ can be regarded as public parameters. A prover and a verifier then do the following steps:

- Prover:
  1) Pick a random number r_2 and compute $F = g^{\alpha} h^{r_2} \ mod \ N$.
  2) Compute $r_3 = r_1 - r_2 \alpha$ and $E' = F^{\alpha} h^{r_3} \ mod \ N$.
  3) Run the $EL(\alpha, r_2, r_3|g, h, F, h|F, E')$ protocol.
     a) Pick random numbers μ, υ_1, and υ_2 first and compute $C_1 = g^{\mu} h^{\upsilon_1} \ mod \ N$ and $C_2 = F^{\mu} h^{\upsilon_2} \ mod \ N$.
     b) Compute $H = Hash(C_1||C_2)$.
     c) Generate $X = \mu + H\alpha$, $X_1 = \upsilon_1 + Hr_2$, $X_2 = \upsilon_2 + Hr_3$.
  4) Finally, publish: (H, X, X_1, X_2, F, E').
- Verifier will check whether $Hash(g^X h^{X_1} F^{-H} \pmod N || F^X h^{X_2} E'^{-H} \bmod N)$ is equal to H, $C_1 = g^X h^{X_1} F^{-H} \ mod \ N$, and $C_2 = F^X h^{X_2} E'^{-H} \ mod \ N$.
  1) $C_1 = g^{\mu} h^{\upsilon_1} = g^{\mu + H\alpha} h^{\upsilon_1 + Hr_2} (g^{\alpha} h^{r_2})^{-H} = g^X h^{X_1} F^{-H} \ mod \ N$
  2) $C_2 = F^{\mu} h^{\upsilon_2} = F^{\mu + H\alpha} h^{\upsilon_2 + Hr_3} (F^{\alpha} h^{r_3})^{-H} = F^X h^{X_2} E'^{-H} \ mod \ N$
  3) $H = Hash(g^X h^{X_1} F^{-H} \pmod N || F^X h^{X_2} E'^{-H} \bmod N) = Hash(C_1||C_2)$

If verifier can pass the above proofs, then the verifier will believe the commitment F and E' hide the same secret α. It indirectly proves the commitment E hide a square secret α^2.

III. Non-Interactive Zero-Knowledge Range Proof

In this section, we provide formal definitions and the security notions for the non-interactive zero-knowledge range proof scheme.

Definition 1 (Non-interactive zero-knowledge range proof argument): A Non-interactive zero-knowledge range proof argument (NIRPA) is a tuple of algorithms $NIRPA = (Set, Pro, Ver)$ specified as follows.

- $p \xleftarrow{\$} Set(\lambda)$ The probabilistic algorithm Set which takes the security parameter λ as input, and outputs system parameter p.
- $\pi \xleftarrow{\$} Pro(p, m)$ The probabilistic algorithm Pro which takes p and secret value m and the range value $[a, b]$ as input, and outputs the proof π.
- $d \xleftarrow{\$} Ver(p, \pi)$ The probabilistic algorithm Ver which takes p and π as input, it returns a decision bit $d \in \{0, 1\}$ according to π. When $d = 1$, it means verfier accepts the proof π. Otherwise, it rejects the proof.

NIRPA typically satisfy three security properties: correctness, soundness, and zero-knowledge. We explain as below in more detail.

Correctness: The correctness property states that an honest prover can follow the protocol and pass all proof to convince a verifier that m is in the range $[a, b]$, where $a < b$.

Definition 2 (Correctness of NIPRA): Let $NIRPA = (Set, Pro, Ver)$ be a non-interactive zero-knowledge range proof argument. We say that $NIRPA = (Set, Pro, Ver)$ satisfies correctness property if for all security parameter λ, secure value m within the given range $[a, b]$, the following probabilistic is satisfied.

$$Pr\left[Ver(p, \pi) = 1 : \begin{array}{c} p \xleftarrow{\$} Set(\lambda); \\ \pi \xleftarrow{\$} Pro(p, m) \end{array} \right] \geq 1 - neg(\lambda)$$

Soundness: The soundness property states that if the proof is passed with a non-negligible probability, m must be within the range of $[a, b]$ and be committed by the prover.

Definition 3: Let $NIRPA = (Set, Pro, Ver)$ be a non-interactive zero-knowledge range proof argument. We say that $NIRPA = (Set, Pro, Ver)$ satisfies soundness if there exists a PPT simulator $\mathcal{S}$ and for all λ such that the following probabilistic is negligible.

$$Pr\left[Ver(p, \pi) = 1 \wedge m \notin [a, b] : \begin{array}{c} p \xleftarrow{\$} Pro(\lambda); \\ \pi \xleftarrow{\$} \mathcal{S}(p) \end{array} \right] \leq neg(\lambda)$$

Zero-knowledge: The zero-knowledge property states that a polynomially-bounded malicious verifier cannot obtain any information about the knowledge m. No one can get the secret value unless prover discloses it.

Definition 4: Let $NIRPA = (Set, Pro, Ver)$ be a non-interactive zero-knowledge range proof argument. We say that $NIRPA = (Set, Pro, Ver)$ satisfies Zero-knowledge if there exists a PPT simulator $\mathcal{S}$ and for all security parameter λ, adversaries $\mathcal{A}$, such that the following probabilistic is negligible.

$$Pr\left[b = b' : \begin{array}{c} p \xleftarrow{\$} Set(\lambda); \\ b \xleftarrow{\$} \{0, 1\}; m \xleftarrow{\$} \mathcal{A}(p); \\ \pi_1 \xleftarrow{\$} Pro(p, m); \pi_0 \xleftarrow{\$} \mathcal{S}(p); \\ b' \xleftarrow{\$} \mathcal{A}(p, \pi_b) \end{array} \right] - \frac{1}{2} \leq neg(\lambda)$$

IV. The New Non-interactive ZKRP Protocol

In this section, we introduce our new non-interactive range proof.

The core idea behind our protocol is that m lies within the range $[a, b]$ if and only if $(m - a + 1)(b - m + 1) > 0$, where a, b are two positive integers and is known to the verifier. If we directly use $(m-a+1)(b-m+1)$ in our protocol, it may leak the secret m with high probability. Alternatively, we compute $\omega^2(m - a + 1)(b - m + 1)$, where $\omega \xleftarrow{\$} \mathbb{Z}$. Therefore, when $\omega^2(m - a + 1)(b - m + 1)$ is positive, m must lie within the range $[a, b]$. To prove that $\omega^2(m-a+1)(b-m+1)$ is positive, we set M and R such that $M+R = \omega^2(m-a+1)(b-m+1)$. Here M is a square number (i.e. $M = \alpha^2$ for some integer α), and R is a positive integer. If M is a square, and $R > 0$, with overwhelmingly probability, $\omega^2(m - a + 1)(b - m + 1)$ is a positive integer.

Before executing our protocol, we assume that both prover and verifier know the range $[a, b]$ and the parameters (g, h, N) of Fujisaki-Okamoto commitment scheme. Fujisaki-Okamoto commitment scheme is used to commit the secret value m in form of $c = g^m h^r \ mod \ N$, where r is a big random integer. Therefore, to prove that the secret value in c lies within the range $[a, b]$, the prover executes the following steps to generate a proof with the commitment $c = g^m h^r \ mod \ N$.

1) The prover calculates,

$$c_1 = c/g^{a-1} \ mod \ N$$
$$c_2 = g^{b+1}/c \ mod \ N$$
$$c' = c_1^{b-m+1} h^{r'} \ mod \ N$$

where r' is randomly chooses by the prover

2) The prover utilizes c_2, c' to make a EL Proof,

$$EL(b - m + 1, -r, r' | g, h, c_1, h | c_2, c')$$

3) The prover randomly chooses two integers ω, r'', where ω is a big integer number except zero. With these random numbers, prover calculates,
$$c'' = c'^{\omega^2} h^{r''} \ mod \ N$$
4) The prover makes a SQR Proof.
$$SQR(\omega, r''|c', h|c'')$$
5) The prover randomly chooses integer α and calculates $M = \alpha^2$. If $M \geq \omega^2(m-a+1)(b-m+1)$ repeat step 5).
6) The prover calculates
$$R = \omega^2(m-a+1)(b-m+1) - M$$
7) The prover setes
$$r_1 + z = \omega^2((b-m+1)r + r') + r''$$
where r_1 and z are provsitive integers.
8) The prover commits M and R with r_1, z and publishes
$$c'_1 = g^M h^{r_1} \ mod \ N$$
$$c'_2 = g^R h^z \ mod \ N$$
9) The prover makes a SQR Proof.
$$SQR(\alpha, r_1|g, h|c'_1)$$
10) The prover publishes
$$\pi = \{c, c', c'', c'_1, c'_2, R, EL_1, SQR_1, SQR_2\}, where$$
$$EL_1 = EL(b-m+1, -r, r'|g, h, c_1, h|c_2, c'),$$
$$SQR_1 = SQR(\omega, r''|c', h|c''), \ and$$
$$SQR_2 = SQR(\alpha, r_1|g, h|c'_1)$$

To check the validaty of the proof π, a verifier does the following steps,
1) Calulate $c_1 = c/g^{a-1} \ mod \ N$
2) Calulate $c_2 = g^{b+1}/c \ mod \ N$
3) Verify $EL(b-m+1, -r, r'|g, h, c_1, h|c_2, c')$
4) Verify $SQR(\omega, r''|c', h|c'')$
5) Verify $c'' = c'_1 c'_2 \ mod \ N$
6) Verify $SQR(\alpha, r_1|g, h|c'_1)$
7) Verify $R > 0$

m is lying within the range $[a, b]$ if and only if step 3) to step 7) are passed.

For Step (5), $c'' = c'_1 c'_2 \ mod \ N$ because
$$\begin{aligned} c'' &= c'^{\omega^2} h^{r''} \ mod \ N \\ &= (c_1^{b-m+1} h^{r'})^{\omega^2} h^{r''} \ mod \ N \\ &= (c g^{(1-a)(b-m+1)} h^{r'})^{\omega^2} h^{r''} \ mod \ N \\ &= (g^{(m-a+1)(b-m+1)} h^{(b-m+1)r+r'})^{\omega^2} h^{r''} \ mod \ N \\ &= g^{\omega^2(m-a+1)(b-m+1)} h^{\omega^2((b-m+1)r+r')+r''} \ mod \ N \\ &= g^{M+R} h^{r_1+z} \ mod \ N \\ &= c'_1 c'_2 \ mod \ N \end{aligned}$$

For this protocol, If and only if all the conditions are satisfied, the verifier will accept this proof. Otherwise, it is regarded as failure.

V. Security Description

We discuss the security of our non-interactive ZKRP within three parts ; correctness, soundness, and zero-knowledge.

Correctness. As the secret value m lies in the range $[a, b]$, and the honest prover follows our protocol, the proof π can be accepted by the verifier in the following order of the checking list.
1) Calulate $c_1 = c/g^{a-1} \ mod \ N$
2) Calulate $c_2 = g^{b+1}/c \ mod \ N$
3) Verify $EL(b-m+1, -r, r'|g, h, c_1, h|c_2, c')$
4) Verify $SQR(\omega, r''|c', h|c'')$
5) Verify $c'' = c'_1 c'_2 \ mod \ N$
6) Verify $SQR(\alpha, r_1|g, h|c'_1)$
7) Verify $R > 0$

We explain our protocol has the property of correctness as below.
- If an honest prover followes the protocol, then $c_1 = c/g^{a-1}$, $c_2 = g^{b+1}/c$, and $R > 0$. Step 7) is correct.
- As $c_2 = g^{b-m+1} h^{-r}$ and $c' = c_1^{b-m+1} h^{r'}$ both commit the same secret. If the function EL is correct, step 3) is correct.
- As $c'' = c'^{\omega^2} h^{r''}$ and SQR are correct, step 4) is correct.
- As $c'' = g^{\omega^2(m-a+1)(b-m+1)} h^{\omega^2((b-m+1)r+r')+r''}$, $c'_1 = g^M h^{r_1}$, and $c'_2 = g^R h^z$ are correct, step 5) is correct
- As $c'_1 = g^M h^{r_1}$ and SQR are correct, step 6) is correct.
- As $SQR(\alpha, r_1|g, h|c'_1)$, $R > 0$, and $c'' = c'_1 c'_2$ are correct, a verifier can be convinced that $\omega^2(m-a+1)(b-m+1)$ is positive, and m is in $[a, b]$.

Because the proof π passes successfully, our protocol satisfy correctness property.

Soundness. In our protocol, if the proof π passes successfully, m must be in the given range $[a, b]$, and the prover knows m. Based on the difficulty of solving discrete logarithm problem and the integer factorization problem, Fujisaki-Okamoto commitment has the property of secret hiding. It means that after the prover publishes the commitment, the prover has negligible probability to change the secret number and to generate the same commitment. According to the secret hiding property, we take parameters of our protocol $c'_1 = g^M h^{r_1}$ to run the KDLCGSO protocol (*Section 2.4*) twice with difference challenge c and c'. We denote that P is prover and V is verifier.
- $P \rightarrow V : a = g^r h^s \quad r, s \xleftarrow{\$} \mathbb{N}$
- $V \rightarrow P : c$
- $P \rightarrow V : u = r - cM, \quad v = s - cr_1$

So we get the following result.
$$u = r - cM, \quad v = s - cr_1 \quad \rightarrow \quad a = g^u h^v c_1'^c \tag{1}$$
$$u' = r - c'M, \quad v' = s - c'r_1 \quad \rightarrow \quad a = g^{u'} h^{v'} c_1'^{c'} \tag{2}$$

And make (1)/(2),
$$1 = g^{u-u'} h^{v-v'} c_1'^{c-c'}$$

$$c_1' = g^{\frac{u-u'}{c'-c}} h^{\frac{s-s'}{c'-c}}$$

If M and r can be recovered by $\frac{u-u'}{c'-c}$ and $\frac{s-s'}{c'-c}$, prover must use M and r to generate this zero-knowledge proof. According to [18], $c' - c$ must be invertible, and the values of $\frac{u-u'}{c'-c}$, $\frac{s-s'}{c'-c}$ always exist and can be found. According to the above discussion, Prover knows M, r_1, R, z in our protocol.

$$c_1' = g^M h^{r_1} \ mod \ N$$
$$c_2' = g^R h^z \ mod \ N$$

If $c'' = c_1' c_2' = g^{M+R} h^{r_1+z}$, M is a square number, and $R > 0$, it can be explained that the prover not only knows the value hidden in c'' but also knows that the value is positive. Therefore, our protocol provides the property of soundness.

Zero-knowledge. During the whole protocol, adversary cannot get any information from the witness. Based on the binding property of Fujisaki-Okamoto commitment, our work has zero-knowledge property. For instance, we assume $c = g^m h^r \ mod \ N$ and $c^* = h^{r^*} \ mod \ N$ which is generated by simulator. Because of $h = g^L \ mod \ N$, for all r^* such that $c^* = h^{r^*} \ mod \ N$, there exists a r_0^* to make $c^* = g^m h^{r_0^*} \ mod \ N$. More precisely, c and c^* are viewed as generating from the same secret value m. Therefore, any verifier cannot ensure distinguish real proof and simulative proof. This proving process can be used to prove $\{c_1, c_2, c', c'', c_1', c_2', EL_1, SQR_1, SQR_2\}$ has the same property, therefore our protocol has Zero-knowledge property.

VI. Conclusion

We have proposed a new non-interactive zero-knowledge scheme and provided secure proof in the paper. Comparing to [3], our work provides an arbitrary range form for the non-interactive zero-knowledge range proof scheme. It is more flexible and suitable for being applied in a real environment. Besides, our work is more efficient and lighter than [10], [18] and solves the security vulnerability in [10]. We believe our new ZKRP can be beneficial to the development of DApps and can extend the application scope to more scenarios.

VII. Acknowledgment

This research was partially supported by the Ministry of Science and Technology, Taiwan (ROC), under Project Numbers MOST 107-2218-E-004-001, MOST 105-2221-E-004-001-MY3, and by Taiwan Information Security Center at National Sun Yat-sen University (TWISC@NSYSU).

Reference

[1] Shashank Agrawal, Chaya Ganesh, and Payman Mohassel. Non-interactive zero-knowledge proofs for composite statements. In *Annual International Cryptology Conference*, pages 643–673. Springer, 2018.

[2] Fabrice Boudot. Efficient proofs that a committed number lies in an interval. In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 431–444. Springer, 2000.

[3] Benedikt Bünz, Jonathan Bootle, Dan Boneh, Andrew Poelstra, Pieter Wuille, and Greg Maxwell. Bulletproofs: Efficient range proofs for confidential transactions. Technical report, Cryptology ePrint Archive, Report 2017/1066, 2017. https://eprint. iacr. org/2017/1066, 2017.

[4] Benedikt Bünz, Jonathan Bootle, Dan Boneh, Andrew Poelstra, Pieter Wuille, and Greg Maxwell. Bulletproofs: Short proofs for confidential transactions and more. In *Bulletproofs: Short Proofs for Confidential Transactions and More*, page 0. IEEE, 2018.

[5] Rafik Chaabouni, Helger Lipmaa, and Bingsheng Zhang. A non-interactive range proof with constant communication. In *International Conference on Financial Cryptography and Data Security*, pages 179–199. Springer, 2012.

[6] Eiichiro Fujisaki and Tatsuaki Okamoto. Statistical zero knowledge protocols to prove modular polynomial relations. In *Annual International Cryptology Conference*, pages 16–30. Springer, 1997.

[7] Oded Goldreich. *Foundations of Cryptography: Volume 1, Basic Tools*. Cambridge University Press, 2010.

[8] Jens Groth. Non-interactive zero-knowledge arguments for voting. In *International Conference on Applied Cryptography and Network Security*, pages 467–482. Springer, 2005.

[9] Adam Hahn, Rajveer Singh, Chen-Ching Liu, and Sijie Chen. Smart contract-based campus demonstration of decentralized transactive energy auctions. In *Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), 2017 IEEE*, pages 1–5. IEEE, 2017.

[10] Tommy Koens, Coen Ramaekers, and Cees van Wijk. Efficient zero-knowledge range proofs in ethereum. unpublished.

[11] Ahmed Kosba, Andrew Miller, Elaine Shi, Zikai Wen, and Charalampos Papamanthou. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In *2016 IEEE symposium on security and privacy (SP)*, pages 839–858. IEEE, 2016.

[12] Helger Lipmaa. On diophantine complexity and statistical zero-knowledge arguments. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 398–415. Springer, 2003.

[13] Helger Lipmaa. Progression-free sets and sublinear pairing-based non-interactive zero-knowledge arguments. In *Theory of Cryptography Conference*, pages 169–189. Springer, 2012.

[14] Patrick McCorry, Siamak F Shahandashti, and Feng Hao. A smart contract for boardroom voting with maximum voter privacy. In *International Conference on Financial Cryptography and Data Security*, pages 357–375. Springer, 2017.

[15] Ian Miers, Christina Garman, Matthew Green, and Aviel D Rubin. Zerocoin: Anonymous distributed e-cash from bitcoin. In *Security and Privacy (SP), 2013 IEEE Symposium on*, pages 397–411. IEEE, 2013.

[16] Kun Peng. A general, flexible and efficient proof of inclusion and exclusion. In *Cryptographers' Track at the RSA Conference*, pages 33–48. Springer, 2011.

[17] Kun Peng and Feng Bao. Batch range proof for practical small ranges. In *International Conference on Cryptology in Africa*, pages 114–130. Springer, 2010.

[18] Kun Peng and Feng Bao. An efficient range proof scheme. In *Social Computing (SocialCom), 2010 IEEE Second International Conference on*, pages 826–833. IEEE, 2010.

[19] Kun Peng, Colin Boyd, and Ed Dawson. Batch zero-knowledge proof and verification and its applications. *ACM Transactions on Information and System Security (TISSEC)*, 10(2):6, 2007.

[20] Kun Peng and Li Yi. Studying a range proof technique—exception and optimisation. In *International Conference on Cryptology in Africa*, pages 328–341. Springer, 2013.

[21] Eli Ben Sasson, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, and Madars Virza. Zerocash: Decentralized anonymous payments from bitcoin. In *2014 IEEE Symposium on Security and Privacy (SP)*, pages 459–474. IEEE, 2014.

[22] Claus-Peter Schnorr. Efficient identification and signatures for smart cards. In *Conference on the Theory and Application of Cryptology*, pages 239–252. Springer, 1989.

[23] Tsz Hon Yuen, Qiong Huang, Yi Mu, Willy Susilo, Duncan S Wong, and Guomin Yang. Efficient non-interactive range proof. In *International Computing and Combinatorics Conference*, pages 138–147. Springer, 2009.