7-2009

Efficient non-interactive range proof

Tsz Hon YUEN

Qiong HUANG

Yi MU

Willy SUSILO

Duncan S. WONG

See next page for additional authors

Citation

YUEN, Tsz Hon; HUANG, Qiong; MU, Yi; SUSILO, Willy; WONG, Duncan S.; and YANG, Guomin. Efficient non-interactive range proof. (2009). *Proceedings of the 15thAnnual International Conference, Niagara Falls, USA, 2009 July 13-15*. 138-147.

Available at: https://ink.library.smu.edu.sg/sis_research/7380

Author

Tsz Hon YUEN, Qiong HUANG, Yi MU, Willy SUSILO, Duncan S. WONG, and Guomin YANG

Efficient Non-interactive Range Proof

Tsz Hon Yuen[1], Qiong Huang[2], Yi Mu[1], Willy Susilo[1],
Duncan S. Wong[2], and Guomin Yang[2]

[1] University of Wollongong, Australia
{thy738,ymu,wsusilo}@uow.edu.au
[2] City University of Hong Kong, China
{csqhuang@student.,duncan@,csyanggm@cs.}cityu.edu.hk

Abstract. We propose the first constant size non-interactive range proof which is not based on the heuristic Fiat-Shamir transformation and whose security does not rely on the random oracle assumption. The proof consists of a constant number of group elements. Compared with the most efficient constant-size range proof available in the literature, our scheme has significantly reduced the proof size. We showed that our scheme achieves perfect completeness, perfect soundness and composable zero-knowledge under a conventional number-theoretic assumption, namely the Subgroup Decision Problem.

1 Introduction

Proving in zero-knowledge that a committed value lies within a specified integer range is called *range proof*. Consider the following scenario: suppose that there is a firewall which grants the access of some private network only to users from a specific range of IP addresses, say with the same class A IP prefix "10.*.*.*". Each user when accessing the private network has to prove to the firewall that he has a valid credential corresponding to his IP address, while he does not want to reveal his actual IP address to the firewall due to some privacy concern. Suppose that the user's IP address is 10.168.0.1 and he is holding an anonymous credential for his corresponding IP value $178782209 = 10 \times 256^3 + 168 \times 256^2 + 1$. The user can prove to the firewall, using the *range proof*, that his IP value lies in the range $[10 \times 256^3, 10 \times 256^3 + 255 \times 256^2 + 255 \times 256 + 255]$, without revealing exactly what his IP address is.

Range proof has many other applications. For example, in some anonymous credential system [20] and e-cash system, [7], a prover can show that he is old enough (e.g. age ≥ 18) to access some sensible information; or show that the sequence number of an e-cash lies within a specified range, respectively.

In the literature, there are a number of range proof schemes available [5, 9, 18, 4, 17, 12, 6]. Most of the schemes are interactive and have to use the Fiat-Shamir transformation [13] for converting to their non-interactive versions. The security of the transformation relies on the random oracle [1] assumption, which is considered to be heuristic. The security may not preserve when the random oracle is replaced by a hash function, even if the security of a scheme is

H.Q. Ngo (Ed.): COCOON 2009, LNCS 5609, pp. 138–147, 2009.

reduced to some complexity (or number-theoretic) assumptions [8]. In addition to this, each of the schemes has a number of additional limitations (see Sec. 1.2 for details). Some of them may be inefficient: the proof size is linear to that of either some desirable security level ([5]) or the range ([18, 12, 6]). At the security aspect, some schemes do not achieve perfect completeness ([9, 4, 12]), perfect soundness ([18, 5, 9, 4, 17, 12, 6]), or only have statistical zero-knowledge ([9, 4, 17, 6]).

A natural question which remains unanswered is whether it is possible to build a non-interactive range proof scheme which does not rely on the random oracle assumption, while at the same time, is efficient (i.e. constant size) and achieves perfect completeness, perfect soundness and desirably a stronger notion of zero-knowledge.

1.1 Our Results and Techniques Used

In this paper, we answer this question affirmatively, by proposing a constant size non-interactive range proof scheme. The scheme is not based on the Fiat-Shamir transformation and its security does not rely on the random oracle assumption. To the best of our knowledge, our scheme is the first constant size non-interactive range proof without relying on the random oracle assumption. In addition to this, the proof contains a constant number of group elements and is more efficient than all the comparable schemes.On the security, the scheme achieves perfect completeness, perfect soundness and by far, one of the strongest zero-knowledge notions, namely the composable zero-knowledge (which implies unbounded zero-knowledge) [15].

Regarding the techniques used in our constructions, we have borrowed ideas from some of the previous range proof schemes and also made use of some techniques from other types of zero-knowledge proof systems, but putting them together in an interesting way for achieving those desirable properties mentioned above. In particular, our scheme follows the typical approach for range proof: suppose a prover P wants to prove that a committed secret μ is in some integer interval $[a, b]$. P will show that both $\mu – a$ and $b – \mu$ are non-negative. To do so, the scheme first applies the classic Lagrange's theorem that any positive integer can be written as the sum of four squares, which can be found using the Rabin-Shallit algorithm [19]. Then, we borrow some of the techniques from Groth and Sahai's non-interactive witness-indistinguishable (NIWI) proof for bilinear groups [16] and turn it into the final non-interactive range proof scheme. The security proof of our scheme is done in the traditional common reference string model. The number theoretic assumption that our scheme relies on is the Subgroup Decision Problem, which was first proposed by Boneh, Goh and Nissim [3].

1.2 Related Work

Below is a brief review of the related range proof schemes. In the description, we use P and V to denote a prover and a verifier, respectively. If P proves that a committed secret μ falls in an interval I while V is convinced that μ belongs to an interval $J \supseteq I$, then we say that the *expansion rate* of the range proof scheme is $|J|/|I|$.

In 1987, Brickell *et al.* [5] proposed the BCDG range proof that prove a committed secret lying in $[0, B]$ for some positive integer B. The scheme has perfect completeness and perfect zero-knowledge. It achieves "computational" soundness, that is, the probability that a cheating prover can succeed is bounded by 2^{-t} where t is the number of times that the proof is iterated. The expansion rate of the scheme is three and the proof size is proportional to the value of t.

In 1998, Chan, Frankel and Tsiounis [9] improved the BCDG range proof. We call this scheme as CFT range proof. CFT range proof range achieves "computational" completeness with probability greater than $1 - 2^l$ for some security parameter $l \in \mathbb{N}$. The soundness achieved is also computational, where a cheating prover can succeed with probability bounded by 2^{-t}. Regarding zero-knowledge, the scheme achieves honest-verifier statistic zero-knowledge (HVSZK). The expansion rate is 2^{t+l+1}. The CFT range proof improves the BCDG range proof by having the proof size independent of the value of t.

With similar range structure to that of BCDG and CFT range proofs, Mao [18] proposed a range proof in 1998 for ranges in the form of $[0, 2^k - 1]$ where $k \in \mathbb{N}$. Mao's proof size is proportional to the size of the range. The scheme has perfect completeness, perfect zero-knowledge, and "computational" soundness.

The first range proof scheme for the general range $[a, b]$ was proposed by Boudot in 2000 [4]. In addition, its expansion rate is exactly one. In other words, it is the first range proof which solves the expansion rate problem. The scheme has "computational" completeness and soundness, and the level of HVSZK with respect to zero-knowledge.

In 2003, Lipmaa [17] propose a range proof for committed secrets lying in $[0, B]$ where B is some positive integer. In Lipmaa's proof, the following classic Lagrange's theorem from the year 1770 was employed.

Theorem 1. *For an integer μ, there exist (efficiently computable) integers ω_1, ω_2, ω_3, ω_4 such that $\mu = \omega_1^2 + \omega_2^2 + \omega_3^2 + \omega_4^2$, if and only if $\mu \geq 0$.*

For finding the four squares in the theorem, Rabin and Shallit's algorithm [19] can be used. Lipmaa's scheme has perfect completeness, while the soundness is "computational" and the zero-knowledge is HVSZK.

Di Crescenzo, Herranz and Sáez [12] proposed a non-interactive range proof without random oracles in 2004. We call this scheme as DHS range proof. The DHS range proof decomposes the committed number using Mao's method, and uses the NIZK proof for Blum integers and quadratic residue [11]. The DHS range proof has perfect zero-knowledge, while the completeness and the soundness are "computational". The disadvantage of this scheme is that the communication complexity is proportional to the size of the range.

Groth [14] proposed a variation of Lipmaa's method in 2005. It is based on an observation from number theory that the only numbers that cannot be written as the sum of three squares are of the form $4^m(8k + 7)$ for some integers m and

k. Specifically, $4\mu + 1$ can be written as a sum of three squares, which implies μ to be non-negative.

Recently in [6], Camenisch, Chaabouni and shelat proposed a new range proof. Their scheme is constructed from a set membership proof which is based on the Boneh-Boyen signature scheme [2]. This also implies that their scheme's security relies on the q-Strong Diffie-Hellman assumption, while the other range proofs are generally relying on the strong RSA assumption. Furthermore, their scheme has perfect completeness while having HVSZK in zero-knowledge and "computational" soundness. The proof size also depends on the size of the range.

2 Definitions and Number-Theoretic Assumption

2.1 Non-interactive Proof System

We review the definition for non-interactive proof based on the one given by Groth and Sahai recently in [16]. Let R be an efficiently computable ternary relation. For triplets $(gk, x, w) \in R$ we call gk the setup, x the statement and w the witness. Let L_R be the language such that

$$L_R(gk) \doteq \{x \mid (\exists w)[(gk, x, w) \in R]\}.$$

The standard definition of an NP-language often has gk omitted. In [16] and in this paper, gk is the description of a bilinear group.

A non-interactive proof system for R consists of four probabilistic polynomial time algorithms: a setup algorithm $\mathcal{G}$, a common reference string (CRS) generation algorithm K, a prover P and a verifier V. $\mathcal{G}$ takes as input the security parameter 1^k, and outputs a setup gk. It may also output some auxiliary information sk, for example, the factorization of a group order. Note that sk can simply be an empty string, meaning that the proof system is built upon a group without knowledge of any trapdoor. The CRS generation algorithm K takes (gk, sk) as input and produces a common reference string σ. P takes as input (gk, σ, x, w) and produces a proof π, while V takes as input (gk, σ, x, π) and outputs 1 for accepting the proof, or 0 for rejecting the proof. We call $(\mathcal{G}, K, \mathsf{P}, \mathsf{V})$ a non-interactive proof system for R if it has the following properties.

Perfect Completeness. For all adversaries $\mathcal{A}$, we have

$$\Pr[(gk, sk) \leftarrow \mathcal{G}(1^k); \sigma \leftarrow K(gk, sk); (x, w) \leftarrow \mathcal{A}(gk, \sigma); \pi \leftarrow \mathsf{P}(gk, \sigma, x, w) : \\ \mathsf{V}(gk, \sigma, x, \pi) = 1 \text{ if } (gk, x, w) \in R] = 1.$$

Perfect Soundness. For all adversaries $\mathcal{A}$, we have

$$\Pr[(gk, sk) \leftarrow \mathcal{G}(1^k); \sigma \leftarrow K(gk, sk); (x, \pi) \leftarrow \mathcal{A}(gk, \sigma) : \\ \mathsf{V}(gk, \sigma, x, \pi) = 0 \text{ if } x \notin L_R(gk)] = 1.$$

Composable Zero-Knowledge.[1] For this notion of zero-knowledge, there are two aspects: first, an adversary should not be able to distinguish a real CRS from

[1] Composable zero-knowledge was first proposed by Groth [15]. In [15], Groth also showed that composable zero-knowledge implies unbounded zero-knowledge.

a simulated CRS; second, the adversary should not be able to distinguish real proofs on a simulated CRS from simulated proofs, even if he gets access to the secret simulation key τ. In other words, there exists a polynomial time simulator (S_1, S_2) that for all non-uniform polynomial time adversaries $\mathcal{A}$, we have

$$\begin{aligned}&\Pr[(gk, sk) \leftarrow \mathcal{G}(1^k); \sigma \leftarrow K(gk, sk) : \mathcal{A}(gk, \sigma) = 1]\\ \approx\, &\Pr[(gk, sk) \leftarrow \mathcal{G}(1^k); (\sigma, \tau) \leftarrow S_1(gk, sk) : \mathcal{A}(gk, \sigma) = 1],\end{aligned}$$

and

$$\begin{aligned}&\Pr[(gk, sk) \leftarrow \mathcal{G}(1^k); (\sigma, \tau) \leftarrow S_1(gk, sk); (x, w) \leftarrow \mathcal{A}(gk, \sigma, \tau);\\ &\quad \pi \leftarrow \mathsf{P}(gk, \sigma, x, w) : \mathcal{A}(\pi) = 1]\\ =\, &\Pr[(gk, sk) \leftarrow \mathcal{G}(1^k); (\sigma, \tau) \leftarrow S_1(gk, sk); (x, w) \leftarrow \mathcal{A}(gk, \sigma, \tau);\\ &\quad \pi \leftarrow S_2(gk, \sigma, \tau, x) : \mathcal{A}(\pi) = 1],\end{aligned}$$

where $(gk, x, w) \in R$.

2.2 Pairing and Intractability Problem

Let $\mathbb{G}, \mathbb{G}_T$ be multiplicative groups of order $n = pq$, where p and q are prime. Let g be the generator of $\mathbb{G}$. We denote $\mathbb{G}_q$ as the subgroup of $\mathbb{G}$ with order q.

Definition 1. *A map $\hat{e} : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ is called a pairing if, for all $g \in \mathbb{G}$ and $a, b \in \mathbb{Z}_n$, we have $\hat{e}(g^a, g^b) = \hat{e}(g, g)^{ab}$, and if g is the generator of $\mathbb{G}$, then $\hat{e}(g, g)$ generates $\mathbb{G}_T$.*

Definition 2 (Subgroup Decision Problem). *Given $(n, \mathbb{G}, \mathbb{G}_T, \hat{e})$ and a random element $u \in \mathbb{G}$, output '1' if the order of u is q and output '0' otherwise.*

The advantage of an algorithm $\mathcal{A}$ in solving the problem is defined as:

$$\begin{aligned}Adv_{\mathcal{A}}(k) = \Big|\, &\Pr\Big[\mathcal{A}(n, \mathbb{G}, \mathbb{G}_T, \hat{e}, u) = 1 : \begin{array}{c}(p, q, \mathbb{G}, \mathbb{G}_T, \hat{e}) \leftarrow \mathcal{G}(1^k)\\ n = pq, u \leftarrow \mathbb{G}.\end{array}\\ &- \Pr[\mathcal{A}(n, \mathbb{G}, \mathbb{G}_T, \hat{e}, u) = 1 : \begin{array}{c}(p, q, \mathbb{G}, \mathbb{G}_T, \hat{e}) \leftarrow \mathcal{G}(1^k)\\ n = pq, u \leftarrow \mathbb{G}_q.\end{array}\Big]\ \Big|.\end{aligned}$$

The subgroup decision assumption assumes that for any polynomial time algorithm $\mathcal{A}$, $Adv_{\mathcal{A}}(k)$ is a negligible function in k. This assumption was first proposed by Boneh, Goh and Nissim [3].

3 Our Range Proof Scheme

As mentioned in Sec. 1.1, our approach is to prove that both $\mu_1 = \mu - a$ and $\mu_2 = b - \mu$ are non-negative for a committed secret μ which lies in $[a, b]$. To do this, P applies Theorem 1 and represents $\mu_i = \omega_{i,1}^2 + \omega_{i,2}^2 + \omega_{i,3}^2 + \omega_{i,4}^2$ for $i = 1, 2$, using the Rabin and Shallit algorithm [19]. Then, P performs a proof for the statement

$$\mu_1 = \sum_{j=1}^{4} \omega_{1,j}^2 \quad \wedge \quad \mu_2 = \sum_{j=1}^{4} \omega_{2,j}^2. \tag{1}$$

using the witness $(\{\omega_{i,j}\}_{1\leq i\leq 2;1\leq j\leq 4}, \mu)$. We borrow some of the techniques from Groth and Sahai's NIWI proof [16] and turn it into the final non-interactive range proof. In particular, we borrow the technique of commitment for pairings from [16] that is based on the subgroup decision assumption.

We follow the notations for pairings denoted in Sec. 2.2. Let u be either a generator of $\mathbb{G}$ or that of $\mathbb{G}_q$. We commit to $w \in \mathbb{Z}_p$, by choosing $\rho \in \mathbb{Z}_n$ at random and setting $T_w := g^w u^\rho$. If u's order is q, w is uniquely determined in $\mathbb{Z}_p$, since $T_w^q = g^{wq}$; but if u's order is n, then we have a perfectly hiding commitment to w. Under the subgroup decision assumption, the two types of commitments are computationally indistinguishable.

3.1 The Construction and Its Security

Suppose that $|b-a| \leq p$, the non-interactive range proof scheme is as follows:

- $\mathcal{G}(1^k)$: We define $\mathcal{G}$ such that it generates $gk = (n, \mathbb{G}, \mathbb{G}_T, \hat{e})$ and $sk = (p,q)$, where p and q are two random k-bit primes, $n = pq$, and $\hat{e}$ the pairing as described in Def. 1.
- $K(gk, sk)$: The CRS generation algorithm K takes as input $gk = (n, \mathbb{G}, \mathbb{G}_T, \hat{e})$ and $sk = (p,q)$, randomly selects a generator g of $\mathbb{G}$ and a generator u of $\mathbb{G}_q$, and outputs $\sigma = (g,u)$.
- $\mathsf{P}(gk, \sigma, x, w)$: The prover P takes as input $gk = (n, \mathbb{G}, \mathbb{G}_T, \hat{e})$, $\sigma = (g,u)$, x the statement (which is equation (1)) and w the witness of equation (1), and carries out the following: for $i = 1,2, j = 1,\ldots,4$, P randomly chooses $r_{i,j} \in_R \mathbb{Z}_n$ and computes $T_{i,j} = g^{\omega_{i,j}} u^{r_{i,j}}$. Then P randomly picks $r_w \in_R \mathbb{Z}_n$ and computes $T_w = g^w u^{r_w}$. P calculates:

$$\phi_1 = g^{-r_w + 2\sum_{j=1}^{4} r_{1,j}\omega_{1,j}} u^{\sum_{j=1}^{4} r_{1,j}^2},$$
$$\phi_2 = g^{r_w + 2\sum_{j=1}^{4} r_{2,j}\omega_{2,j}} u^{\sum_{j=1}^{4} r_{2,j}^2}.$$

  P sends the proof $\pi = (\{T_{1,j}, T_{2,j}\}_{j\in[4]}, T_w, \phi_1, \phi_2)$ to the verifier V.
- $\mathsf{V}(gk, \sigma, x, \pi)$: The verifier V takes as input $gk = (n, \mathbb{G}, \mathbb{G}_T, \hat{e})$, $\sigma = (g,u)$, x the statement (which is equation (1)) and $\pi = (\{T_{1,j}, T_{2,j}\}_{j\in[4]}, T_w, \phi_1, \phi_2)$ the proof, and checks if

$$\hat{e}(g^a T_w^{-1}, g) \cdot \prod_{j=1}^{4} \hat{e}(T_{1,j}, T_{1,j}) = e(u, \phi_1),$$
$$\hat{e}(T_w g^{-b}, g) \cdot \prod_{j=1}^{4} \hat{e}(T_{2,j}, T_{2,j}) = e(u, \phi_2).$$

  V outputs 1 if the equations hold; otherwise, outputs 0.

Our proof scheme described above can also be adapted to prove logical relations of ranges. Groth and Sahai [16] mentioned that logical operations like AND and OR are easy to encode into their framework using standard techniques in arithmetization. Therefore we can use our system to prove that $x \in [a, b] \vee x \in [c, d]$.

Theorem 2. *The range proof scheme described above is a non-interactive proof system satisfying perfect completeness, perfect soundness and composable zero-knowledge if the subgroup decision assumption holds.*

Proof. Perfect Completeness.

$$\begin{aligned}
&\hat{e}(g^a T_w^{-1}, g) \cdot \prod_{j=1}^{4} \hat{e}(T_{1,j}, T_{1,j}) \\
&= \hat{e}(g^{a-w} u^{-r_w}, g) \cdot \prod_{j=1}^{4} \left(\hat{e}(g,g)^{\omega_{1,j}^2} \cdot \hat{e}(u,g)^{2r_{1,j}\omega_{1,j}} \cdot \hat{e}(u, u^{r_{1,j}^2}) \right) \\
&= \hat{e}(g,g)^{\sum_{j=1}^4 \omega_{1,j}^2 + a - w} \cdot \hat{e}(u, g^{-r_w + \sum_{j=1}^4 2r_{1,j}\omega_{1,j}} u^{\sum_{j=1}^4 r_{1,j}^2}) \\
&= \hat{e}(u, \phi_1), \\
&\hat{e}(T_w g^{-b}, g) \cdot \prod_{j=1}^{4} \hat{e}(T_{2,j}, T_{2,j}) \\
&= \hat{e}(g^{w-b} u^{r_w}, g) \cdot \prod_{j=1}^{4} \left(\hat{e}(g,g)^{\omega_{2,j}^2} \cdot \hat{e}(u,g)^{2r_{2,j}\omega_{2,j}} \cdot \hat{e}(u, u^{r_{2,j}^2}) \right) \\
&= \hat{e}(g,g)^{\sum_{j=1}^4 \omega_{2,j}^2 + w - b} \cdot \hat{e}(u, g^{r_w + \sum_{j=1}^4 2r_{2,j}\omega_{2,j}} u^{\sum_{j=1}^4 r_{2,j}^2}) \\
&= \hat{e}(u, \phi_2).
\end{aligned}$$

Perfect Soundness. Notice that u is in $\mathbb{G}_q$. Therefore when we try to power q from both sides of the verification equations, the equations become:

$$\hat{e}(g^a T_w^{-1}, g)^q \cdot \prod_{j=1}^{4} \hat{e}(T_{1,j}, T_{1,j})^q = (\hat{e}(g^{a-w}, g) \cdot \prod_{j=1}^{4} \hat{e}(g,g)^{\omega_{1,j}^2})^q = 1,$$
$$\hat{e}(T_w g^{-b}, g)^q \cdot \prod_{j=1}^{4} \hat{e}(T_{2,j}, T_{2,j})^q = (\hat{e}(g^{w-b}, g) \cdot \prod_{j=1}^{4} \hat{e}(g,g)^{\omega_{2,j}^2})^q = 1.$$

If $x \notin L$, then we have either $\mu_1 = \mu - a$ or $\mu_2 = b - \mu$ is negative. Theorem 1 states that if μ_i is negative, then we cannot represent μ_i as $\sum_{j=1}^4 \omega_{i,j}^2$. Therefore we have either $\mu - a \neq \sum_{j=1}^4 \omega_{1,j}^2$ or $b - \mu \neq \sum_{j=1}^4 \omega_{2,j}^2$. Therefore the proof cannot pass the verification.

Composable Zero-Knowledge. First, we prove that a PPT adversary cannot distinguish a real CRS from a simulated CRS. The simulated CRS is generated as follows. Suppose the simulator S_1 takes as input $gk = (n, \mathbb{G}, \mathbb{G}_T, \hat{e})$ and $sk = (p, q)$. The simulator S_1 is also given u from the subgroup decision problem. S_1 randomly selects a generator g of $\mathbb{G}$. S_1 outputs the simulated CRS $\sigma = (g, u)$ and the secret simulation key $\tau = (p, q)$. If a PPT adversary $\mathcal{A}_1$ can distinguish a real CRS from σ, then $\mathcal{S}_1$ answers 0 to the subgroup decision problem. By the subgroup decision assumption, no PPT adversary can distinguish a real CRS generated by K from a simulated CRS generated by S_1.

Second, we prove that a PPT adversary cannot distinguish real proofs on a simulated CRS from simulated proofs, even if he gets access to the secret simulation key τ. Suppose the simulator S_2 takes as input $gk = (n, \mathbb{G}, \mathbb{G}_T, \hat{e})$, $\sigma = (g, u)$, $\tau = (p, q)$ and x is the proof statement. S_2 picks a random w_r from the range $[a, b]$. By theorem 1, S_2 can also represent $w_r - a$ and $b - w_r$ as sum of four squares. Therefore S_2 can calculate simulated commitments and proofs with this randomly chosen witness w_r.

Suppose there is a PPT adversary $\mathcal{A}_2$ can distinguish this simulated proof and the real proof with witness $(\{\omega_{1,j}, \omega_{2,j}\}_{j\in[4]}, w)$. The commitments $(\{T_{1,j}, T_{2,j}\}_{j\in[4]}, T_x)$ are perfect hiding if u is the generator of $\mathbb{G}$. They have the same distribution no matter we use the witness $(\{\omega_{1,j}, \omega_{2,j}\}_{j\in[4]}, w)$ or the randomly chosen witness $(\ldots, w_r)$. Therefore $\mathcal{A}_2$ cannot distinguish from the commitment only.

Therefore $\mathcal{A}_2$ can only distinguish from the proofs (ϕ_1, ϕ_2) given the commitment. Theorem 3 of [16] tells us that the proofs (ϕ_1, ϕ_2) made with either one of the above witnesses are uniformly distributed over all possible choices of the corresponding domain. Contradiction occurs. □

3.2 Comparison

We now compare our range proof with the existing ones found in the literature. During the comparison, we consider the security level comparable to 80-bit symmetric or 1024-bit RSA.

Suppose that the underlying pairing with composite order is constructed from a supersingular curve with embedding degree 2. The proof size (i.e. communication overhead) of our scheme is

$$11\mathbb{G} = 11 \times 1025 = 11275 \text{ bits}.$$

If we restrict the witness to have the form $4v + 1$ for some integer v, then we can have further reduce the proof size. For example, in the case of voting, we can represent candidate A as number 1, candidate B as number 5 and so on. Then we can represent the number of any candidate as the sum of three squares (Sec. 1.2) and the proof size will be reduced to 9 $\mathbb{G}$ = 9216 bits, which is 18% less than the original one.

Recently, Camenisch, Chaabouni and shelat [6] proposed a range proof without relying on the strong RSA assumption. If the range is $< k - 1$ bits, then the proof size is $O(\frac{k}{\log k - \log\log k})$. Using the example in their paper, a prover wants to show that the committed secret lies between $[347184000, 599644800)$. Cheon [10] proved that the security of the ℓ-SDH problem on an abelian group of order p can be reduced up to $O(\log p \cdot p^{1/3})$ (resp. $O(\log p \cdot p^{1/3})$) for large ℓ if $p-1$ (resp. $p+1$) has a divisor $d = O(p^{1/2})$ (resp. $d = O(p^{1/3})$). Because of this, Cheon suggested to use 220-bit prime p for 80-bit symmetric security level. Suppose that we use a pairing with embedding degree 6. The proof size[2] is

$$5\mathbb{G} + 8\mathbb{G}_T + 20\mathbb{Z}_p = 5 \times 221 + 8 \times 1321 + 20 \times 220 = 16073 \text{ bits}.$$

Our scheme has the proof size 30% less than that of Camenisch *et al.*'s scheme. It is not hard to see that our scheme saves even more bandwidth if the range is larger.

It is more natural to compare our scheme with the existing constant size range proofs whose expansion rate equals to 1. We use the 1024-bit RSA security level for communication complexity comparison. The proof size of our scheme is about 42% less than that of existing schemes.

Table 1. Comparison of range proofs with expansion rate equals to 1. Complexity stands for the proof size. We omit the figure for Camenisch *et al.* [6] since it is not a constant size range proof. PC stands for perfect completeness. PS stands for perfect soundness. ZK stands for zero-knowledge. NI stands for non-interactive.

Scheme	Complexity	PC	PS	ZK	Assumption	Proof System
Boudot	23544 bits	×	×	HVSZK	strong RSA	interactive
Lipmaa	19536 bits	√	×	HVSZK	strong RSA	interactive
Camenisch *et al.*	-	√	×	HVSZK	ℓ-SDH	interactive
This paper	11275 bits	√	√	composable ZK	subgroup decision	NI

4 Conclusion

We proposed an efficient non-interactive range proof. To the best of our knowledge, this is the first constant size range proof which is not based on the Fiat-Shamir transformation and whose security does not rely on the random oracle assumption. The proof consists of constant number of group elements and is the most efficient range proof scheme in the literature. We showed that our scheme achieves perfect completeness, perfect soundness and composable zero-knowledge under the Subgroup Decision Problem.

References

1. Bellare, M., Rogaway, P.: Random oracles are practical: A paradigm for designing efficient protocols. In: CCS 1993, pp. 62–73. ACM Press, New York (1993)
2. Boneh, D., Boyen, X.: Short Signatures Without Random Oracles. In: Cachin, C., Camenisch, J.L. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 56–73. Springer, Heidelberg (2004)

[2] Camenisch *et al.* [6] used 3072-bit RSA security level for comparison. However, they used a pairing of embedding degree 12 which has no known efficient implementation. They did not take into account of the attack on the ℓ-SDH problem by Cheon [10].

3. Boneh, D., Goh, E.-J., Nissim, K.: Evaluating 2-DNF Formulas on Ciphertexts. In: Kilian, J. (ed.) TCC 2005. LNCS, vol. 3378, pp. 325–341. Springer, Heidelberg (2005)
4. Boudot, F.: Efficient Proofs that a Committed Number Lies in an Interval. In: Preneel, B. (ed.) EUROCRYPT 2000. LNCS, vol. 1807, pp. 431–444. Springer, Heidelberg (2000)
5. Brickell, E.F., Chaum, D., Damgård, I., van de Graaf, J.: Gradual and verifiable release of a secret. In: Pomerance, C. (ed.) CRYPTO 1987. LNCS, vol. 293, pp. 156–166. Springer, Heidelberg (1988)
6. Camenisch, J., Chaabouni, R., Shelat, A.: Efficient protocols for set membership and range proofs. In: Pieprzyk, J. (ed.) ASIACRYPT 2008. LNCS, vol. 5350, pp. 234–252. Springer, Heidelberg (2008)
7. Camenisch, J., Hohenberger, S., Lysyanskaya, A.: Compact e-cash. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 302–321. Springer, Heidelberg (2005)
8. Canetti, R., Goldreich, O., Halevi, S.: The random oracle methodology, revisited. J. ACM 51(4), 557–594 (2004)
9. Chan, A.H., Frankel, Y., Tsiounis, Y.: Easy come - easy go divisible cash. In: Nyberg, K. (ed.) EUROCRYPT 1998. LNCS, vol. 1403, pp. 561–575. Springer, Heidelberg (1998)
10. Cheon, J.H.: Security analysis of the strong diffie-hellman problem. In: Vaudenay, S. (ed.) EUROCRYPT 2006. LNCS, vol. 4004, pp. 1–11. Springer, Heidelberg (2006)
11. De Santis, A., Di Crescenzo, G., Persiano, G.: The knowledge complexity of quadratic residuosity languages. Theor. Comput. Sci. 132(2), 291–317 (1994)
12. Di Crescenzo, G., Herranz, J., Sáez, G.: Reducing server trust in private proxy auctions. In: Katsikas, S.K., López, J., Pernul, G. (eds.) TrustBus 2004. LNCS, vol. 3184, pp. 80–89. Springer, Heidelberg (2004)
13. Fiat, A., Shamir, A.: How to Prove Yourself: Practical Solutions to Identification and Signature Problems. In: Odlyzko, A.M. (ed.) CRYPTO 1986. LNCS, vol. 263, pp. 186–194. Springer, Heidelberg (1987)
14. Groth, J.: Non-interactive Zero-Knowledge Arguments for Voting. In: Ioannidis, J., Keromytis, A.D., Yung, M. (eds.) ACNS 2005. LNCS, vol. 3531, pp. 467–482. Springer, Heidelberg (2005)
15. Groth, J.: Simulation-sound NIZK proofs for a practical language and constant size group signatures. In: Lai, X., Chen, K. (eds.) ASIACRYPT 2006. LNCS, vol. 4284, pp. 444–459. Springer, Heidelberg (2006)
16. Groth, J., Sahai, A.: Efficient non-interactive proof systems for bilinear groups. In: Smart, N.P. (ed.) EUROCRYPT 2008. LNCS, vol. 4965, pp. 415–432. Springer, Heidelberg (2008)
17. Lipmaa, H.: On diophantine complexity and statistical zero-knowledge arguments. In: Laih, C.-S. (ed.) ASIACRYPT 2003. LNCS, vol. 2894, pp. 398–415. Springer, Heidelberg (2003)
18. Mao, W.: Guaranteed correct sharing of integer factorization with off-line shareholders. In: Imai, H., Zheng, Y. (eds.) PKC 1998. LNCS, vol. 1431, pp. 60–71. Springer, Heidelberg (1998)
19. Rabin, M., Shallit, J.: Randomized algorithms in number theory. Communications in Pure and Applied Mathematics 39, 239–256 (1986)
20. Teranishi, I., Furukawa, J., Sako, K.: k-times anonymous authentication (Extended abstract). In: Lee, P.J. (ed.) ASIACRYPT 2004. LNCS, vol. 3329, pp. 308–322. Springer, Heidelberg (2004)