An Efficient Range Proof Scheme

Kun Peng and Feng Bao
Institute for Infocomm Research, Singapore
dr.kun.peng@gmail.com

***Abstract*—A new range proof technique is proposed. It only needs a constant cost and is more efficient than the existing range proof schemes. In comparison with the existing range proof solutions with a constant cost or focusing on efficiency, security of the new scheme is based on the same widely accepted trade-offs and no weaker than theirs. In summary, it improves efficiency of range proof without further compromising security.**

I. Introduction

In cryptographic applications, it is often needed to test that a secret message is in a certain interval range [16], [17], [18], [19] When the secret message is known by a party, the party is often required to prove that he knows a secret integer in the interval range. The party chooses an integer from an interval range R, encrypts it or commits to it and publishes the ciphertext or commitment. Then he has to prove that the integer encrypted in the ciphertext or committed in the commitment is in R. The proof cannot reveal any information about the integer except that it is in the range. This proof operation is called range proof. The following security properties must be satisfied in a range proof protocol, while high efficiency is very important as well.

- Correctness: if the integer is in the range and the prover knows the integer and strictly follows the proof protocol, he can pass the verification in the protocol.
- Soundness: if the prover passes the verification in the protocol with a non-negligible probability, the integer is in the range.
- Privacy: no information about the integer is revealed in the proof except that it is in the range.

In satisfying the security properties and achieving high efficiency the existing solutions to range proof [7], [3], [14], [13], [4] have their drawbacks.

The most straightforward range proof technique is ZK (zero knowledge) proof of partial knowledge [7], which proves that the secret integer may be each integer in the range one by one and then link the multiple proofs with OR logic. This simple range proof can perform all the computations in a cyclic group with public order, so can easily achieve both formally provable soundness and formally provable privacy. Depending on the concrete application environment, an appropriate encryption algorithm or commitment function can be employed such that either soundness or privacy can be absolute in information-theoretic sense and the other is computational. So it supports various applications no matter whether information-theoretic soundness or information-theoretic privacy is required by them. However, this method has a drawback: the number of computations it needs is linear in the size of the range, which leads to very low efficiency.

It is well known that the straightforward method can be optimised in efficiency by sealing the secret integer bit by bit and proving that each commitment contains a bit. However, the optimised solution is still not efficient enough especially when the range size is large. This idea is extended in [4], which designs a special range proof technique for small ranges. It employs the **u**-base coding mechanism and proves that each **u**-base digit of the secret integer is in $\{0, 1, \ldots, \mathbf{u} - 1\}$. However, its improvement on efficiency is not great enough. Moreover, it has a special requirement: a separate instance of proof and verification is needed for each independent verifier, who must interactively run the proof and verification protocol separately with the prover. So the range proof technique in [4] is not general or universally verifiable. In addition, an additional computational assumption is needed in [4].

The range proof techniques in [3], [14], [13] improve efficiency by discarding the cyclic group with public order. They notice that a special setting is useful for efficient range proof, where the multiplication modulus is a large composite with secret factorization. A commitment function is designed in a large cyclic group modulo the composite modulus. As factorization of the modulus is hard, the order of the cyclic group is unknow. These techniques [3], [14], [13] implicitly and essentially depend on the following principle.

Definition 1: N is a large composite with unknown factorization and G is a cyclic subgroup of Z_N^* with a large order. It is hard to calculate any multiple of the order of G if factorization of N is hard.

It is called the *secret order principle* in this paper. With the secret order principle, a special proof technique can be employed: the prover proves that he knows a secret integer committed in the commitment, so that the committed integer is computationally binded and unique, otherwise the prover can calculate a multiple of the order of the cyclic group as the difference between two different integers committed in the same commitment and break the secret

978-0-7695-4211-9/10 $26.00 © 2010 IEEE
DOI 10.1109/SocialCom.2010.125

order principle[1]. In one word, the prover's knowledge of the secret integer and the secret order principle guarantees bindingness and uniqueness of the committed integer. After the committed integer has been fixed and cannot be changed, it is much easier to prove that it is non-negative. As a result, in [3], [14], [13] a range proof of integer m in a range $\{a, a+1, \ldots, b\}$ can be reduced to a proof that $m-a$ and $b-m$ are non-negative. This technique is called CBPKCGSO (computational bindingness through proof of knowledge in cyclic groups with secret order) in this paper. Using CBPKCGSO it is proved in [3] that each of $m-a$ and $b-m$ is the sum of a square and a non-negative integer, while in [14] it is proved that each of $m-a$ and $b-m$ is the sum of four squares. The design in [13] is a variant of [14] and discusses its application to various e-voting applications with different rules. In this paper, we focus on range proof itself and do not extend our discussion to its applications. So we regard [13] as a detailed variant of [14] with a concrete application environment and will not treat it separately. Without the secret order principle and the CBPKCGSO technique, the range proof in [3], [14], [13] cannot work as even if a negative integer is committed in a commitment, its value plus a multiple of the order of the cyclic group can be a positive integer to open the commitment. So the range proof techniques in [3], [14], [13] are only computationally sound. In addition, the secret order principle and the CBPKCGSO technique have another consequence to be detailed in Section II: complete and formally provable privacy is impossible and only statistical and intuitive privacy is achieved. Looser security requirements on soundness and privacy in [3], [14], [13] is a price to pay for higher efficiency.

We have an observation: even if the range proof techniques in [3], [14], [13] employ some trade-offs in security in comparison with the simple solution based on [7], like the secret order principle, the CBPKCGSO technique and weaker and less formal privacy, their advantage in efficiency over the simple solution is still not great enough. We believe that with the same trade-offs, higher efficiency can be achieved. So a new range proof scheme is proposed in this paper. It employs the same security trade-offs as [3], [14], [13] but uses different proof techniques to achieve higher efficiency than theirs. It is the most efficient range proof protocol.

II. Background

We are more interested in range proof schemes with higher efficiency like [3], [14], while their looser security requirements are regarded as inevitable trade-offs for the sake of efficiency. As mentioned before, [13] is not separately treated as it is regarded as a detailed variant of [14] with a concrete application environment. In [3], [14], the Fujisaki-Okamoto commitment function [10] or its variant [8] is employed. In [10], N is a large composite with unknown factorization and G is a cyclic subgroup of Z_N^* with a large order. According to the secret order principle the order of G is secret as the factorization problem is hard. Integers g and h are generators of G such that neither of $\log_g h$ and $\log_h g$ is known. A secret integer m is committed to in $c = g^m h^r \bmod N$ by a prover where r is randomly chosen from a certain large range. The prover has to publicly prove that m is in an interval range $\{a, a+1, \ldots, b\}$.

The most basic and important proof primitive in [3], [14] is KDLCGSO (knowledge of discrete logarithm in a cyclic group with secret order) proof, which enables a party to prove knowledge of integers x and z to satisfy $g^x h^z = y \bmod N$. In [3], three important building blocks, "Proof that two commitments hide the same secret" in Section 2.2, "proof that a committed number is a square" in Section 2.3 and "proof with tolerance $\delta = 1 + \epsilon$" in Section 3.1.1, all employ this primitive. In [14], proof that a committed number is a square employs this primitive as well and then is repeatedly employed to implement the range proof. KDLCGSO is necessary as prover's knowledge of the secret integer committed as a discrete logarithm must be guaranteed to apply the secret order principle and the CBPKCGSO technique to [3], [14] . Moreover, the proof must be performed in cyclic groups with secret orders. KDLCGSO is described in Figure 1 where P stands for prover and V stands for verifier.

1) $P \rightarrow V$: $a = g^r h^s \bmod N$
where r and s are randomly chosen from a large set of integers.

2) $V \rightarrow P$: c
where c is randomly chosen from a large set of integers.

3) $P \rightarrow V$: $u = r - c\chi$ in Z
$v = s - cz$ in Z

Verification: $a = g^u h^v y^c \bmod N$

Figure 1. Proof of knowledge of discrete logarithm in a cyclic group with secret order

As the order of G is unknown and u and v are calculated without any modulus, there are two side effects. Firstly, complete and formal proof of soundness in this setting is more difficult than when the order of G is public. It is easy to see that if the prover passes the verification with a non-negligible probability, it must be able to calculate in polynomial time two responses (u, v) and (u', v') to two different challenges c and c' to pass the verification with

[1]This deduction is reasonable as in [3], [14], [13] calculating two different integers committed in the same commitment the difference between which is not a multiple of the order of the cyclic group is hard due to difficulty of other hard problems like DL problem.

the same a[2]. Otherwise, the probability that it can pass the verification is negligible. More precisely, the prover must be able to calculate in polynomial time two responses (u, v) and (u', v') to two different challenges c and c' such that

$$a = g^u h^v y^c \bmod N \quad (1)$$

$$a = g^{u'} h^{v'} y^{c'} \bmod N \quad (2)$$

Now we wonder: from these two proof instances, can a polynomial extractor extract χ and z? Let us go on with the deduction and see.

(1) divided by (2) yields

$$1 = g^{u-u'} h^{v-v'} y^{c-c'} \bmod N$$

If the order of G, say q, is known, proof of soundness is easy as the extractor can always calculate $\mu = (u-u')/(c'-c) \bmod q$ and $\nu = (v-v')/(c'-c) \bmod q$ such that $y = g^\mu h^\nu \bmod N$ as explained in the following.

- If $GCD(q, c'-c) = 1$, then $(c'-c)^{-1} \bmod q$ always exists.
- If $GCD(q, c'-c) = \rho$ and $\rho > 1$, then q has a factor ρ but the order of $y^{c'-c}$ does not have a factor ρ. As $y \in G$, $u-u'$ and $v-v'$ must have a factor ρ. So $(u-u')/(c'-c) = ((u-u')/\rho)/((c'-c)/\rho) \bmod q$ and $(v-v')/(c'-c) = ((v-v')/\rho)/((c'-c)/\rho) \bmod q$ can be calculated as $((c'-c)/\rho)^{-1} \bmod q$ always exists.

Thus soundness is proved, which is similar to the case in Schnorr's proof protocol [21]. However, with the secret order principle, the prover does not know the order of G or its multiple. So he (using the extractor) can only calculate $(u-u')/(c'-c)$ and $(v-v')/(c'-c)$ when $u-u'$ and $v-v'$ are multiples of $c'-c$. If $u-u'$ or $v-v'$ is not a multiple of $c'-c$, it is not so simple to calculate $(u-u')/(c'-c)$ and $(v-v')/(c'-c)$. Soundness of KDLCGSO proof relies on Theorem 1.

Theorem 1: Even if the order of g and h are secret, there is still a polynomial algorithm to calculate integers χ and z to satisfy $g^\chi h^z = y \bmod N$ using (u, v) and (u', v') to satisfy (1) and (2).

Proof of Theorem 1 is quite complex. At first, it is attempted in [10] to give it a formal proof, but the same author [8] finds out that the analysis in [10] and its extended version is incomplete and soundness can only be formally proved when c is only 1 bit long. No formal proof of Theorem 1 is available until [9], which proves it in its Lemma 1. The polynomial algorithm to extract discrete logarithm without knowledge of the order of the cyclic group containing the bases and the exponentiations is proposed and its cost is estimated, both in details, in Lemma 1 in [9]. Due to space limit and complexity of the proof, proof of Theorem 1 is not repeated here and interested readers are referred to [9].

[2]This argument, especially the time analysis, is detailed in proof of Theorem 2.1 in [21].

In [3], "proof that two commitments hide the same secret" and "proof that a committed number is a square" are combinations of two KDLCGSO proofs sharing the same secret logarithms and "proof with tolerance $\delta = 1 + \epsilon$" employs one KDLCGSO proof with a special parameter setting and an additional test of the size of the response integer u. In [14], proof that a committed number is a square is the same as in [3] and employs two combined KDLCGSO proofs. Soundness of them all depends on Theorem 1. Proof that two commitments hide the same secret is denoted as $EL(\chi, r_1, r_2 |\ g_1, h_1, g_2, h_2 \mid y_1, y_2)$, which proves knowledge of secret integers χ, r_1 and r_2 such that $g_1^\chi h_1^{r_1} = y_1 \bmod N$ and $g_2^\chi h_2^{r_2} = y_2 \bmod N$. Proof that a committed number is a square is denoted as $SQR(\chi, r \mid g, h \mid y)$, which proves knowledge of integers χ and r such that $y = g^{\chi^2} h^r \bmod N$. Detailed implementation of the two proof protocols are not provided here due to place limit. They can be found in [3].

Another side effect of KDLCGSO is reducing privacy to statistical level, while its statistical privacy has not been formally proved so far to the best of our knowledge. Obviously, in KDLCGSO u is a monotone function of χ and v is a monotone function of z as calculations of u and v are carried out without any modulus. So some information about χ and z is always revealed from u and v although the amount of revealed information can be limited to a low level. The existing cryptographic schemes employing KDLCGSO including [3], [14] argue that the information revealed from u and v is statistically so trivial that the proof transcript can be simulated by a party without any knowledge of χ or z such that the simulating transcript generated by the party is statistically indistinguishable from the real proof transcript. However, none of them gives a formal proof to this argument. Although the formal definition of statistical indistinguishability between two distributions has been given in [12] and Lecture 7 of [15] as recalled in Definition 2, to the best of our knowledge none of the existing applications of KDLCGSO [10], [1], [5], [6], [11], [20], [2], [3], [14] tries to follow the formal definition and estimate (or calculate an upper bound of) the distance between the distribution of its real proof transcript and the distribution of a simulating transcript. So achievement of statistical indistinguishability in the existing cryptographic schemes employing KDLCGSO including [3], [14] is only an intuitive argument and has not been formally proved. Actually, to the best of our knowledge there is no existing formal proof of achievement of statistical privacy according to formal definition [12], [15] in any cryptographic scheme.

Definition 2: (Statistical indistinguishability). Let $L \in \{0,1\}^*$ be a language. Two families of random variables $\{U(\chi)\}$ and $\{V(\chi)\}$ are statistically indistinguishable on L

if the distance between them,

$$\sum_{\alpha\in\{0,1\}^*} |prob(U(\chi)=\alpha) - prob(V(\chi)=\alpha)|,$$

is negligible (or more precisely smaller than a negligible concrete upper bound) for all sufficiently long $\chi \in L$ where $prob(X)$ stands for the probability of an event X and $|Y|$ stands for absolute value of Y.

III. The New Range Proof Protocol

The main idea of the new range proof scheme is simple as follows.

- Like in [3], [14], [13], we employ the secret order principle and the CBPKCGSO technique to make the secret integer computationally binded and proof of non-negativity of an integer easier.
- An integer m is in a range $\{a, a+1, \ldots, b\}$ if and only if $(m-a+1)(b-m+1)$ is positive.
- If $w^2(m-a+1)(b-m+1)$ is positive, $(m-a+1)(b-m+1)$ is positive.
- To prove that $w^2(m-a+1)(b-m+1)$ is positive, it is divided into three shares m_1, m_2, m_3, whose sum is $w^2(m-a+1)(b-m+1)$. Moreover, m_3 is a square and thus non-negative. If both $sm_1+m_2+m_3$ and $m_1+tm_2+m_3$ are positive where s and t are random positive integers, then $w^2(m-a+1)(b-m+1)$ is positive with an overwhelmingly large probability.
- As the the information revealed from $sm_1+m_2+m_3$ and $m_1+tm_2+m_3$ about m is statistically negligible except showing that m is in the range $\{a, a+1, \ldots, b\}$, they can be published without compromising statistical privacy.
- Like in [3], [14], [13],
  - we show achievement of soundness in the new range proof scheme according to Theorem 1;
  - we intuitively argue that the revealed information in our range proof is so trivial that the proof transcript can be simulated by a party without any knowledge of any secret such that the simulating transcript generated by the party is statistically indistinguishable from the real proof transcript.

Like in [3], the Fujisaki-Okamoto commitment function is employed. We employ two large security parameters k_1 and k_2. k_1 is much smaller than k_2. However, k_1 is large enough such that $1/(k_1-1)$ is a negligible probability. A recommendation for their values is that k_1 is large but much smaller than the order of G (e.g. 160 bits long) and k_2 is larger than the order of G (e.g. longer than 1024 bits).

A secret integer m is committed to in $c = g^m h^r \bmod N$ where r is a random integer in Z_{k_2}. m is in an interval range $\{a, a+1, \ldots, b\}$. A party with knowledge of m and r has to prove that the message committed in c is in $\{a, a+1, \ldots, b\}$. The proof protocol and the corresponding verification are as follows.

1) The prover calculates and publishes $c_1 = c/g^{a-1} \bmod N$ and $c_2 = g^{b+1}/c \bmod N$.
2) He calculates and publishes $c' = c_1^{b-m+1} h^{r'} \bmod N$ and publicly gives a proof
$$EL(b-m+1, -r, r' \mid g, h, c_1, h \mid c_2, c'). \quad (3)$$
where r' is a random integer in Z_{k_2}.
3) He randomly chooses integers w and r'' respectively from $Z_{k_2} - \{0\}$ and Z_{k_2} and publishes
$$c'' = {c'}^{w^2} h^{r''} \bmod N.$$
He publicly gives a proof
$$SQR(w, r'' \mid c', h \mid c''). \quad (4)$$
4) He randomly chooses three non-negative integers m_1, m_2 and m_4 smaller than $w^2(m-a+1)(b-m+1)$ such that
$$m_1 + m_2 + m_3 = w^2(m-a+1)(b-m+1)$$
$$m_3 = m_4^2.$$
He randomly chooses r_1, r_2, r_3 to satisfy $r_1+r_2+r_3 = w^2((b-m+1)r + r') + r''$ and publishes
$$c_1' = g^{m_1} h^{r_1} \bmod N$$
$$c_2' = g^{m_2} h^{r_2} \bmod N$$
$$c_3' = c''/c_1' c_2' \bmod N.$$
He publicly gives a proof
$$SQR(m_4, r_3 \mid g, h \mid c_3'). \quad (5)$$
5) A verifier randomly chooses and publishes integers s and t in $Z_{k_1} - \{0\}$.
6) The prover randomly publishes
$$x = sm_1 + m_2 + m_3$$
$$y = m_1 + tm_2 + m_3$$
$$u = sr_1 + r_2 + r_3$$
$$v = r_1 + tr_2 + r_3$$
7) Besides verification of (3), (4) and (5) the following equations have to be publicly verified
$$c_1 = c/g^{a-1} \bmod N \quad (6)$$
$$c_2 = g^{b+1}/c \bmod N \quad (7)$$
$$c'' = c_1' c_2' c_3' \bmod N \quad (8)$$
$${c_1'}^s c_2' c_3' = g^x h^u \bmod N \quad (9)$$
$$c_1' {c_2'}^t c_3' = g^y h^v \bmod N \quad (10)$$
$$x > 0 \quad (11)$$
$$y > 0 \quad (12)$$

Any one can publicly perform the verification. Once all the integers involved in a verification equation are available, the equation is verified. If a verification fails, the proof protocol fails and stops. The proof protocol succeeds if and only if all the verification conditions are satisfied.

IV. Analysis

Security and efficiency of the new range proof scheme is analysed in this section. It is illustrated that the new scheme improves efficiency of range proof without further compromising security.

Theorem 2: If m is in $\{a, a+1, \ldots, b\}$, an honest prover can strictly follows the proof protocol and pass its verifications in (3), (4), (5), (6), (7), (8), (9), (10), (11) and (12).

Proof: Satisfaction of the verifications are as follows.

- As the prover strictly follows the proof protocol, (6) and (7) are immediately satisfied.
- As $c_2 = g^{b+1}/c \bmod N$, $c' = c_1^{b-m+1} h^{r'} \bmod N$ and $EL()$ is correct, (3) is satisfied.
- As $c'' = {c'}^{w^2} h^{r''} \bmod N$ and $SQR()$ is correct, (4) is satisfied.
- As $c_3' = g^{m_3} h^{r_3} \bmod N$, $m_3 = m_4^2$ and $SQR()$ is correct, (5) is satisfied.
- As

$$\begin{gathered} c'' = {c'}^{w^2} h^{r''} = (c_1^{b-m+1} h^{r'})^{w^2} h^{r''} \\ = ((c/g^{a-1})^{b-m+1} h^{r'})^{w^2} h^{r''} \\ = ((g^m h^r / g^{a-1})^{b-m+1} h^{r'})^{w^2} h^{r''} \\ = g^{w^2(m-a+1)(b-m+1)} h^{w^2((b-m+1)r+r')+r''} \\ \bmod N \\ c_1' = g^{m_1} h^{r_1} \bmod N \\ c_2' = g^{m_2} h^{r_2} \bmod N \\ c_3' = g^{m_3} h^{r_3}. \bmod N \\ m_1 + m_2 + m_3 = w^2(m-a+1)(b-m+1) \\ r_1 + r_2 + r_3 = w^2((b-m+1)r + r') + r'', \end{gathered}$$

  we have

$$\begin{gathered} c_1' c_2' c_3' = g^{m_1} h^{r_1} g^{m_2} h^{r_2} g^{m_3} h^{r_3} = g^{m_1+m_2+m_3} h^{r_1+r_2+r_3} \\ = g^{w^2(m-a+1)(b-m+1)} h^{w^2((b-m+1)r+r')+r''} = c'' \bmod N \end{gathered}$$

  and thus (8) is satisfied.
- As

$$\begin{gathered} x = sm_1 + m_2 + m_3 \\ y = m_1 + tm_2 + m_3 \\ u = sr_1 + r_2 + r_3 \\ v = r_1 + tr_2 + r_3 \end{gathered}$$

  we have

$$\begin{gathered} {c_1'}^s c_2' c_3' = g^{sm_1} h^{sr_1} g^{m_2} h^{r_2} g^{m_3} h^{r_3} \\ = g^{sm_1+m_2+m_3} h^{sr_1+r_2+r_3} = g^x h^u \bmod N \\ c_1' {c_2'}^t c_3' = g^{m_1} h^{r_1} g^{tm_2} h^{tr_2} g^{m_3} h^{r_3} \\ = g^{m_1+tm_2+m_3} h^{r_1+tr_2+r_3} = g^y h^v \bmod N \end{gathered}$$

  and thus (9) and (10) are satisfied.
- As $a \le m \le b$ and w is positive, we have $w^2(m-a+1)(b-m+1) > 0$. So it is feasible to find non-negative m_1, m_2 and m_3 to sum up $w^2(m-a+1)(b-m+1)$ such that $x = sm_1 + m_2 + m_3$ and $y = m_1 + tm_2 + m_3$ are positive. Therefore, (11) and (12) are satisfied.

□

Theorem 3: If the verifications in (3), (4), (5), (6), (7), (8), (9), (10), (11) and (12) are passed with a non-negligible probability, an integer in the range $\{a, a+1, \ldots, b\}$ is committed by the prover in c.

Before Theorem 3 can be proved, three lemmas have to be proved first.

Lemma 1: On the assumption that the factorization problem and discrete logarithm problem are hard, it is impossible for a polynomial prover to calculate integers α_1, α_2, β_1 and β_2 such that $\theta = g^{\alpha_1} h^{\beta_1} \bmod N$, $\theta = g^{\alpha_2} h^{\beta_2} \bmod N$ and $(\alpha_1, \beta_1) \neq (\alpha_2, \beta_2)$.

Proof: If a polynomial prover has calculated integers α_1, α_2, β_1 and β_2 such that $(\alpha_1, \beta_1) \neq (\alpha_2, \beta_2)$ and

$$\begin{gathered} \theta = g^{\alpha_1} h^{\beta_1} \bmod N \\ \theta = g^{\alpha_2} h^{\beta_2} \bmod N, \end{gathered}$$

then

$$g^{\alpha_1} h^{\beta_1} = g^{\alpha_2} h^{\beta_2} \bmod N.$$

Namely,

$$g^{\alpha_1 - \alpha_2} = h^{\beta_2 - \beta_1} \bmod N$$

So

$$(\alpha_1 - \alpha_2) = (\beta_2 - \beta_1) \log_g h \bmod order(G)$$

There are two possibilities: $\beta_2 - \beta_1 = 0 \bmod order(G)$ or $\beta_2 - \beta_1 \neq 0 \bmod order(G)$.

- If $\beta_2 - \beta_1 = 0 \bmod order(G)$, then $\alpha_1 - \alpha_2 = 0 \bmod order(G)$. So either $\beta_2 - \beta_1 = k \times order(G)$ or $\alpha_1 - \alpha_2 = k \times order(G)$ where $k \neq 0$, otherwise $(\alpha_1, \beta_1) = (\alpha_2, \beta_2)$. As $k \neq 0$, a multiple of the order of G is obtained, which is contradictory to the secret order principle as factorization of N is hard.
- If $\beta_2 - \beta_1 \neq 0 \bmod order(G)$, then

$$\log_g h = (\alpha_1 - \alpha_2)/(\beta_2 - \beta_1)$$

  can be calculated according to Theorem 1, which is contradictory to the assumption that discrete logarithm problem is hard.

As each possibility leads to a contradiction, the lemma is proved. □

Lemma 2: A prover passing the verifications of the new range proof protocol with a probability larger than $1/(k_1-1)$ must know integers m_1', m_2', m_3', r_1', r_2', r_3' such that $c_1' = g^{m_1'} h^{r_1'} \bmod N$, $c_2' = g^{m_2'} h^{r_2'} \bmod N$ and $c_3' = g^{m_3'} h^{r_3'} \bmod N$.

Proof: (9)/(10) yields a deduction: satisfaction of (9) and (10) with a probability larger than $1/(k_1-1)$ implies that the prover knows x, y, u and v such that

$$c_1'^{s-1} c_2'^{1-t} = g^{x-y} h^{u-v} \bmod N \tag{13}$$

with a probability larger than $1/(k_1-1)$. So among all the possible choices of s and t there must exist an s such that there are two different choices for t to satisfy (13). Otherwise, for each possible choice of s there is at most one choice of t among its all k_1-1 possible choices to satisfy (13) and the probability that (13) is satisfied is no larger than $1/(k_1-1)$, which is a contradiction. So there exist s_1, t_1 and t_2 in $Z_{k_1}-\{0\}$ such that the prover can calculate integers x_1, y_1, u_1, v_1 and x_2, y_2, u_2, v_2 to satisfy

$$c_1'^{s_1-1} c_2'^{1-t_1} = g^{x_1-y_1} h^{u_1-v_1} \bmod N \tag{14}$$
$$c_1'^{s_1-1} c_2'^{1-t_2} = g^{x_2-y_2} h^{u_2-v_2} \bmod N. \tag{15}$$

(14)/(15) yields

$$c_2'^{t_2-t_1} = g^{x_1-y_1-x_2+y_2} h^{u_1-v_1-u_2+v_2} \bmod N$$

As k_1 is smaller than the order of G and $t_1, t_2 \in Z_{k_1}-\{0\}$, $t_2 - t_1 \neq 0 \bmod order(G)$. So

$$c_2' = g^{(x_1-y_1-x_2+y_2)/(t_2-t_1)} h^{(u_1-v_1-u_2+v_2)/(t_2-t_1)} \bmod N$$

Therefore, according to Theorem 1, the prover knows m_2' and r_2' such that $c'_2 = g^{m_2'} h^{r_2'} \bmod N$. For the same reason, the prover knows m_1' and r_1' such that $c'_1 = g^{m_1'} h^{r_1'} \bmod N$. So (9) implies

$$(g^{m_1'} h^{r_1'})^s g^{m_2'} h^{r_2'} c_3' = g^x h^u \bmod N$$

and thus the prover knows $m_3' = x - sm_1' - m_2'$ and $r_3' = u - sr_1' - r_2'$ such that $c'_3 = g^{m_3'} h^{r_3'} \bmod N$. □

Lemma 3: Passing the verifications of the new range proof protocol with a non-negligible probability guarantees that the prover knows a positive integer committed in c''.

Proof: According to Lemma 2, the prover knows integers m_1', m_2', m_3', r_1', r_2', r_3' such that

$$c_1' = g^{m_1'} h^{r_1'} \bmod N$$
$$c_2' = g^{m_2'} h^{r_2'} \bmod N$$
$$c_3' = g^{m_3'} h^{r_3'} \bmod N,$$

as $1/(k_1-1)$ is a negligible probability. So satisfaction of (9) and (10) imply

$$(g^{m_1'} h^{r_1'})^s g^{m_2'} h^{r_2'} g^{m_3'} h^{r_3'} = g^x h^u \bmod N$$
$$g^{m_1'} h^{r_1'} (g^{m_2'} h^{r_2'})^t g^{m_3'} h^{r_3'} = g^y h^v \bmod N$$

Namely,

$$g^{sm_1'+m_2'+m_3'} h^{sr_1'+r_2'+r_3'} = g^x h^u \bmod N$$
$$g^{m_1'+tm_2'+m_3'} h^{r_1'+tr_2'+r_3'} = g^y h^v \bmod N$$

As the prover knows x, y, u and v, according to Lemma 1 and satisfaction of (11) and (12),

$$sm_1' + m_2' + m_3' = x > 0$$
$$m_1' + tm_2' + m_3' = y > 0$$

Note that (5) guarantees that the prover knows a square committed in c_3'. So according to Lemma 1, m_3' is the same square as he knows m_3'. So $m_3' \geq 0$. So $m_1' + m_2' + m_3'$ is always positive as

- if $m_1' \leq 0$, then $m_1'+m_2'+m_3' \geq sm_1'+m_2'+m_3' > 0$;
- if $m_2' \leq 0$, then $m_1'+m_2'+m_3' \geq m_1'+tm_2'+m_3' > 0$;
- if $m_1' > 0$ and $m_2' > 0$, $m_1'+m_2'+m_3' \geq m_1'+m_2' > 0$.

Therefore, as $c'' = c_1' c_2' c_3' \bmod N$, the prover commits a positive integer $m_1' + m_2' + m_3'$ in c''. □

Proof of Theorem 3:

(3), (6) and (7) imply that $(m'-a+1)(b-m'+1)$ is committed in c' where m' is an integer committed in c and known to the prover. (4) further implies that the prover knows an integer w' such that $w'^2(m'-a+1)(b-m'+1)$ is committed in c''. According to Lemma 3, the prover know's a positive integer m'' committed in c''. So,

$$w'^2(m'-a+1)(b-m'+1) = m'',$$

according to Lemma 1. Therefore,

$$w'^2(m'-a+1)(b-m'+1) > 0$$

and m', an integer committed in c and known to the prover, is in the range $\{a, a+1, \ldots, b\}$. □

Note that like in the existing range proof protocols [3], [14], [13] soundness of the new range proof protocol is proved through showing one or more committed integer is non-negative or positive and there is only one way to open the commitment as the prover knows the committed integer. Such a proof mechanism works through proof of the prover's knowledge and is based on hardness of factorization problem and discrete logarithm problem, the secret order principle and Theorem 1 in both the new scheme and [3], [14], [13]. With these assumptions, [3], [14], [13] and the new scheme guarantee soundness with an overwhelmingly large probability, whose exact value depends on the length of challenges from the verifiers (e.g. s and t in the new scheme and the challenges in the proof primitives in [3], [14], [13]). So soundness of the new scheme is as strong as that of the existing range proof schemes focusing on efficiency [3], [14], [13]. Moreover, its privacy has the same strength as theirs as it achieves intuitive statistical indistinguishability as well. An intuitive argument for statistical indistinguishability of the new range proof scheme is given in Theorem 4 and like in [3], [14], [13] it is not formally proved according to formal definition [12], [15]. Instead, we give an informal argument to show that privacy is no weaker in the new range

proof protocol than theirs. If their achievement of statistical indistinguishability (privacy) can be formally proved, ours can be formally proved as well.

Theorem 4: A polynomial algorithm without any access to the secret integer m can simulate the proof transcript of the new range proof protocol such that the simulating transcript generated by the algorithm is statistically indistinguishable from the real proof transcript.

Argument: In CBPKCGSO employed by the existing range proof schemes focusing on efficiency [3], [14], [13], c, u and v are published where two of them are functions of χ and z

$$\phi_1(\chi) = u = r - c\chi \text{ in } Z$$
$$\phi_2(z) = v = s - cz \text{ in } Z$$

and χ, z is the secret information. In our new range proof protocol, s, t and functions of the secret

$$\phi_3(m) = x = sm_1 + m_2 + m_3 \text{ in } Z$$
$$\phi_4(m) = y = m_1 + tm_2 + m_3 \text{ in } Z$$
$$\phi_5(r) = u = sr_1 + r_2 + r_3 \text{ in } Z$$
$$\phi_6(r) = v = r_1 + tr_2 + r_3 \text{ in } Z$$

are published where

$$m_1 + m_2 + m_3 = w^2(m - a + 1)(b - m + 1)$$
$$m_3 = m_4^2$$
$$r_1 + r_2 + r_3 = w^2((b - m + 1)r + r') + r''$$

and m is the secret information.

Obviously, $\phi_3(), \phi_4(), \phi_5(), \phi_6()$ are more complex functions than $\phi_1(), \phi_2()$. They employ more random integers and more scrambling operations to confuse and diffuse the secret information. As they employ more variables, they can make better use of parameter setting (e.g. setting some variable to be much larger than another variable) to strengthen the confusion and diffusion. Therefore, our new range proof protocol is no less private than the existing range proof schemes focusing on efficiency [3], [14], [13]. □

The new range proof scheme is compared with the existing range proof schemes in Table I. In analysis of computational cost, both the prover's and the verifier's operations are included and the number of modulo exponentiations are counted, while other costly operations like Rabin & Shallit algorithm is also mentioned. As application of [7] to range proof is not described in details in [7], we only discuss possibilities in its properties: either soundness or privacy can be IT (information-theoretic) secure and depending on the concrete commitment function only one of them is IT secure and the other is computational. IT secure soundness means soundness with an overwhelmingly large probability and without any computational assumption; while IT-secure privacy means absolutly no information about any secret is revealed. In [3], two proofs of non-negativity are employed and each is claimed to cost 20 exponentiations. Note that in [14] Rabin and Shallit algorithm is costly and cannot be ignored. As mentioned before, [13] is regarded as a variant of [14] with a concrete application environment, so is not separately treated. In [4], $\mathbf{u^l}$ is the size of the range. If an additional computational assumption is made for privacy like in [4], efficiency of our new scheme can be further improved by slightly modifying calculation of c'', r_1, r_2 and deleting r_3 as follows

$$c'' = {c'}^{w^2} \bmod N$$
randomly choosing r_1 andr_2 such that
$$r_1 + r_2 = w^2((b - m + 1)r + r')$$

where m_1, m_2 and m_3 still satisfy

$$m_1 + m_2 + m_3 = w^2(m - a + 1)(b - m + 1)$$
$$m_3 = m_4^2$$

and c_1', c_2' and c_3' are still calculated as

$$c_1' = g^{m_1} h^{r_1} \bmod N$$
$$c_2' = g^{m_2} h^{r_2} \bmod N$$
$$c_3' = c''/c_1' c_2'. \bmod N.$$

Consequently, the two $SQR()$ proofs become proof of knowledge of w and m_4 such that

$$c'' = {c'}^{w^2} \bmod N$$
$$c_3' = g^{m_4^2} \bmod N.$$

When w and m_4 are chosen from a large enough set, with this modification the variant of our new scheme can still achieve privacy with one additional computational assumption: the DL problem is hard. The comparison illustrates that the new scheme achieves high efficiency with some widely accepted trade-offs in security. It is more efficient than the existing range proof schemes.

V. Conclusion and Open Questions

The new range proof scheme proposed in this paper is more efficient than the existing range proof schemes. Its security is as strong as the existing solutions to range proof focusing on efficiency [3], [14], [13]. However the new scheme and [3], [14], [13] leave an open question: can their statistical privacy be formally proved following the formal security model in [12], [15] so that formally provable privacy can be achieved in them?

References

[1] G Ateniese, J Camenisch, M Joye and G Tsudik. A practical and provably secure coalition-resistant group signature scheme. In *CRYPTO '00*, pages 255–270.

Table I
COMPARISON OF RANGE PROOF SCHEMES

range proof	soundness	privacy	computation in modulo exponentiations	other comment
[7]	formally provable and can be IT secure	formally provable and can be IT secure	$6(b-a+1)$	either soundness or privacy is IT secure
[7] bit by bit	formally provable and can be IT secure	formally provable and can be IT secure	$6\log_2(b-a+1)$	either soundness or privacy is IT secure
[3]	computational asymptotical	statistical and intuitive	40	
[14]	computational	statistical and intuitive	74	additional costly Rabin & Shallit algorithm needed
[4]	computational	computational	$\mathbf{u}+23\mathbf{l}$+6	not general or universally verifiable
new	computational	statistical and intuitive	33	
new variant	computational	computational statistical and intuitive	25	

[2] F Boudot and J Traore. Efficient public verifiable secret sharing schemes with fast or delayed recovery. In *ICICS '99*, pages 87–102.

[3] F Boudot. Efficient proofs that a committed number lies in an interval. In *EUROCRYPT '00*, pages 431–444.

[4] J Camenisch, R Chaabouni and A Shelat. Efficient protocols for set membership and range proofs. In *ASIACRYPT '08*, pages 234–252.

[5] J Camenisch and M Michels. A group signature scheme with improved efficiency. In *ASIACRYPT '98*, pages 160–174.

[6] D Chaum, J Evertse and J Graaf. An improved protocol for demonstrating possession of discrete logarithms and some generations. In *EUROCRYPT '87*, pages 127–141.

[7] R Cramer, I Damgård and B Schoenmakers. Proofs of partial knowledge and simplified design of witness hiding protocols. In *CRYPTO '94*, pages 174–187.

[8] I Damgård and R Cramer. On $\sum$-protocols. *Cryptologic Protocol Theory*, 2002. Available as http://www.daimi.au.dk/~ivan/Sigma.ps.

[9] I Damgård and E Fujisaki. A statistically-hiding integer commitment scheme based on groups with hidden order. *ASICACRYPT '02*, pages 125–142.

[10] E Fujisaki and T Okamoto. Statistical zero knowledge protocols to prove modular polynomial relations. In *CRYPTO '97*, pages 16–30.

[11] M Girault. Self-certified public keys. In *EUROCRYPT '91*, pages 490–497.

[12] S Goldwasser, S Micali, and C Rackoff. The knowledge complexity of interactive proof systems. In *SIAM J Computer Vol 18*, pages 186–208, 1989.

[13] J Groth. Non-interactive zero-knowledge arguments for voting. In *ACNS '05*, pages 467–482.

[14] H. Lipmaa. On diophantine complexity and statistical zero-knowledge arguments. In *ASIACRYPT '03*, pages 398–415.

[15] M Luby. *Pseudorandomness and cryptographic applications*. Princeton University Press, 1996.

[16] K Peng, C Boyd, E Dawson and E Okamoto. A novel range test. In *ACISP '06*, *LNCS4058*, pages 247–258.

[17] K Peng and E Dawson. Range test secure in the active adversary model. In *ACM International Conference Proceeding Series; Vol. 249, AISW2007*, pages 159–162.

[18] K Peng, F Bao and E Dawson. Correct, private, flexible and efficient range test. In *Journal of Researchand Practice in Information Technology Volume 40, Issue 4, 2008*, pages 275–291.

[19] K Peng and F Bao. Practicalization of a range test and its application to e-auction. In *EuroPKI '09*, 2009.

[20] G Poupard and J Stern. Fair encryption of rsa keys. In *EUROCRYPT '00*, pages 172–189.

[21] C Schnorr. Efficient signature generation by smart cards. *Journal of Cryptology, 4, 1991*, pages 161–174, 1991.