Batch Range Proof For Practical Small Ranges

Kun Peng and Feng Bao

dr.kun.peng@gmail.com

Institute for Inforcomm Research (I^{2}R), Singapore

Agenda

1. Introduction
2. Range proof
3. Batch proof
4. Extended batch proof and verification
5. Application to range proof
6. Conclusion

Range Proof

- Knowledge of a secret integer m in an interval range R.
- Sealed in a ciphertext or commitment.
- Proof to show that it is in the range.
- No other information is revealed.
- Frequently needed in cryptographic applications.

Security Properties

- 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, the integer is guaranteed with an overwhelmingly large probability to be in the range.
- Privacy: no information about the integer is revealed in the proof except that it is in the range.

ZK Proof of Partial Knowledge

- Proposed by Cramer et al at 1994.
- Prove that the committed integer may be each integer in the range one by one.
- Link the multiple proofs with OR logic.
- Almost perfect in security.
- Drawback: its cost is linear in the size of the range.

Higher Asymptotic Efficiency

- Respectively proposed by Boudot in 2000, Lipmaa in 2003 and Groth in 2005.
- Employing cyclic groups with secret orders and computations in Z.
- Asymptotically high efficiency.
- But actual cost is not so satisfying, especially for small ranges.
- Depending on the factorization problem.
- Computations in Z weakens privacy.

Small Ranges

- The most recent and advanced range proof by Camenisch et al in 2008.
- In most practical applications the ranges are not large.
- Asymptotic efficiency is not so important.
- More efficient for small ranges.
- Depends on hardness of ($\log_k$)-Strong Diffie Hellman assumption.

Our Motivations

- Solutions with high security is inefficient.
- Asymptotically efficient solutions weaken security.
- Only one solution for practically small ranges.
- Higher efficiency is desired, especially in small ranges.
- High security should be maintained.

Batch Proof and Verification

- Firstly proposed by Bellare et al in 1998.
- Developed by Gennaro et al and Peng et al.
- Batching multiple proofs into one instance.
- Employing small exponents to save cost.
- A kind of trade-off between efficiency and security.

Batch Proof and Verification by Chida and Yamamoto 1

- p, q are primes such that $q|p-1$.
- G is the cyclic subgroup with order q of Z_p^*.
- g and $y_{i,1},\ y_{i,2}$ for $i = 1, 2, \ldots, n$ are in G.
- The prover knows $b_i \in \{0, 1\}$ and s_{i,b_i} such that $y_{i,b_i} = g^{s_{i,b_i}}$.

Batch Proof and Verification by Chida and Yamamoto 2

The prover selects $r, v, c_{i,\bar{b}_i} \in_R Z/qZ$ and computes

$$R_0 = g^r \prod_{\{i|b_i=1\}} y_{i,0}^{c_{i,0}}$$

$$R_1 = g^v \prod_{\{i|b_i=0\}} y_{i,1}^{c_{i,1}}$$

$$c_i = H(CI||c_{i-1}||c_{i-1,0})$$

$$c_{i,b_i} = c_i - c_{i,\bar{b}_i} \bmod q$$

$$z_0 = r - \sum_{\{i|b_i=0\}} c_{i,0} s_{i,0} \bmod q$$

$$z_1 = v - \sum_{\{i|b_i=1\}} c_{i,1} s_{i,1} \bmod q$$

where $c_0 = R_0$ and $c_{0,0} = R_1$.

Batch Proof and Verification by Chida and Yamamoto 3

1. The prover sends $(z_0, z_1, c_1, c_{1,0}, \ldots, c_{n,0})$ to the verifier
2. The verifier computes

$$c_{i,1} = c_i - c_{i,0} \bmod q$$
$$c_{i+1} = H(CI||c_i||c_{i,0})$$

   and verifies

$$c_1 = H(CI||g^{z_0} \prod_{i=1}^{n} y_{i,0}^{c_{i,0}}||g^{z_1} \prod_{i=1}^{n} y_{i,1}^{c_{i,1}})$$

Our Extension 1

- The parameters are the same.
- The number of possible discrete logarithms in each case is extended from 2 to k.
- g and $y_{i,j}$ for $i = 1, 2, \ldots, n$ and $j = 1, 2, \ldots, k$ are in G.
- The prover knows $b_i \in \{1, 2, \ldots, k\}$ and s_{i,b_i} such that $y_{i,b_i} = g^{s_{i,b_i}} \bmod p$ for $i = 1, 2, \ldots, n$.

Our Extension 2

The prover selects $r_1, r_2, \ldots, r_k$ from Z_q and $c_{i,j}$ for $i = 1, 2, \ldots, n$ and $j \in S_i$ from Z_{2^L} and computes

$$R_1 = g^{r_1} \prod_{1 \le i \le n,\ b_i = 1} \prod_{j \in S_i} y_{i,j}^{c_{i,j}} \bmod p$$

$$R_2 = g^{r_2} \prod_{1 \le i \le n,\ b_i = 2} \prod_{j \in S_i} y_{i,j}^{c_{i,j}} \bmod p$$

$$\ldots\ldots$$

$$\ldots\ldots$$

$$R_k = g^{r_k} \prod_{1 \le i \le n,\ b_i = k} \prod_{j \in S_i} y_{i,j}^{c_{i,j}} \bmod p$$

Our Extension 3

The prover calculates

$$c_i = H(CI||c_{i-1}||c_{i-1,1}||c_{i-1,2}||\ldots||c_{i-1,k-1})$$

$$c_{i,b_i} = c_i - \sum_{j \in S_i} c_{i,j} \bmod q$$

$$z_1 = r_1 - \sum_{\{i|b_i=1\}} c_{i,1} s_{i,1} \bmod q$$

$$z_2 = r_2 - \sum_{\{i|b_i=2\}} c_{i,2} s_{i,2} \bmod q$$

$$\ldots\ldots$$

$$\ldots\ldots$$

$$z_k = r_k - \sum_{\{i|b_i=k\}} c_{i,k} s_{i,k} \bmod q$$

where $c_0 = R_0$ and $c_{0,0} = R_1$.

Our Extension 4

1. The prover sends $(z_1, z_2, \ldots, z_k, c_1, c_{1,1}, c_{1,2} \ldots, c_{1,k-1}, c_{2,1}, c_{2,2} \ldots, c_{2,k-1}, \ldots \ldots \cdot_{n,1}, c_{n,2} \ldots, c_{n,k-1})$ to the verifier
2. The verifier computes

$$c_{i,k} = c_i - \sum_{j=1}^{k-1} c_{i,j} \bmod 2^L$$

$$c_i = H(CI||c_{i-1}||c_{i-1,1}||c_{i-1,2}|| \ldots ||c_{i-1,k-1})$$

and verifies

$$c_1 = H(CI||g^{z_1} \prod_{i=1}^{n} y_{i,1}^{c_{i,1}} \bmod p||g^{z_2} \prod_{i=1}^{n} y_{i,2}^{c_{i,2}} \bmod p|| \ldots ||g^{z_k} \prod_{i=1}^{n} y_{i,k}^{c_{i,k}} \bmod p)$$

The New Range Proof Protocol

- Representing the secret integer x in a base-k system.
- Range proof reduced to $\log_k(b-a)$ instances of proof that each digit of the base-k representation of $x-a$ is in Z_k.
- The $\log_k(b-a)$ instances of proof can be batched using the extended batch proof and verification technique.
- Efficiency can be improved.

How to Prove

1. $c = g^x h^r \bmod p$ where h is a generator of G and $\log_g h$ is unknown.
2. $c' = c/g^a \bmod p$.
3. The prover calculates representation of $x - a$ in the base-k system $(x_1, x_2, \ldots, x_n)$.
4. He randomly chooses $r_1, r_2, \ldots, r_n$ in Z_q and publishes $e_i = g^{x_i} h^{r_i} \bmod p$ for $i = 1, 2, \ldots, n$.
5. He proves knowledge of
   $r' = \sum_{i=1}^{n} r_i k^{i-1} - r \bmod q$ such that
   $h^{r'} c' = \prod_{i=1}^{n} e_i^{k^{i-1}} \bmod p$.

How to Prove Cont

6. The range proof is reduced to n smaller-scale ranges proofs

$$KN(\log_h e_i) \vee KN(\log_h e_i/g) \vee KN(\log_h e_i/g^2) \vee \cdots \vee KN(\log_h e_i/g^{k-1}) \text{ for } i = 1, 2, \ldots, n$$

where $KN(z)$ denotes knowledge of z.

7. The proof can be implemented through batch proof and verification of knowledge of 1-out-of-k discrete logarithms.

Conclusion

- The batch proof and verification technique by Chida and Yamamoto is extended.
- The new batch proof and verification technique proposed in this paper is more general and can save more cost.
- The new technique is employed to improve efficiency and security of range proof in practical small ranges.

Questions?