Notes on Zero-Knowledge Range Proofs (ZKRPs)

Lizheng Wang 4th September 2025
lizhengwang1124@gmail.com

1 Introduction to Zero-Knowledge Range Proofs

A **Zero-Knowledge Range Proof (ZKRP)** is a cryptographic protocol that allows a prover to convince a verifier that a secret, committed value lies within a specific interval, without revealing the value itself. ZKRPs are a specialized form of zero-knowledge proofs and are essential building blocks in many privacy-preserving applications.

2 Core Concepts and Definitions

2.1 Commitment Schemes

A commitment scheme allows a party to commit to a value while keeping it hidden, with the ability to reveal it later. It consists of two algorithms:

- **Com(m, r):** Outputs a commitment c to a message m using randomness r.
- It must be **hiding**, meaning the commitment c reveals no information about m.
- It must be **binding**, meaning the committer cannot find two different messages that open to the same commitment.

A common choice for ZKRPs is the **Pedersen commitment**, which is computationally binding under the discrete logarithm assumption and is also homomorphic.

2.2 Zero-Knowledge Proofs (ZKPs)

A ZKP is an interactive protocol that allows a Prover to convince a Verifier of a statement's truth without revealing any information beyond the statement's validity. They must satisfy three properties:

- **Completeness:** An honest prover with a valid witness can always convince an honest verifier.
- **Soundness:** A malicious prover cannot convince the verifier of a false statement, except with negligible probability.
- **Zero-Knowledge:** The verifier learns nothing other than the fact that the statement is true.

2.3 Formal Definition of ZKRP

A ZKRP is a zero-knowledge proof of knowledge for the following relation, where Com is a commitment scheme:

$$RP_p = \{((y, u, v), (m, r)) : y = \mathrm{Com}(p, m, r) \wedge u \leq m \leq v\}$$

Here, the commitment y and the range [u, v] are public, while the message m and randomness r are the prover's secret witness.

3 General Construction Approaches

There are three primary techniques used to construct efficient ZKRPs. Most constructions focus on proving that a value lies in $[0, N-1]$, which can be generalized to an arbitrary range $[u, v]$ by proving that both $(z-u)$ and $(v-z)$ are non-negative.

3.1 Square Decomposition

This method is based on Lagrange's four-square theorem, which states that any non-negative integer z can be represented as the sum of four integer squares:

$$z = x_1^2 + x_2^2 + x_3^2 + x_4^2$$

To prove that a committed value z is non-negative, the prover shows they know four values x_1, x_2, x_3, x_4 that satisfy this equation. This approach requires special **integer commitments** that are binding over the integers $\mathbb{Z}$, not just a finite field, to prevent attacks that exploit modular arithmetic wrap-around.

Note

The classic integer commitment scheme employs hidden number groups, such as RSA group or class groups. If the prover knows the group order, they can find the mapping of negative values in the group, identifying corresponding x_1, x_2, x_3, x_4 values, thereby compromising the binding property.

Note

There is also an optimization for Square Decomposition. If the integer z satisfiesies the form $4n+1$, then it can be decomposed into three integer squares. So if we want to prove $z \in [0, B]$, then we can prove $4 \cdot z \cdot (B-z)$ can be represented as the sum of three integer squares.

3.2 n-ary Decomposition

In this approach, the prover represents the secret value z as a series of digits in a chosen base n (most commonly, base 2 for a binary decomposition).

$$z = \sum_{i=0}^{k-1} z_i \cdot n^i$$

The proof must then demonstrate two properties:

1. **Digit Validity:** Each digit z_i is valid for the chosen base (e.g., $z_i \in \{0, 1\}$ for base 2).
2. **Representativeness:** The committed digits correctly sum to the original committed value z.

Various tools are used to prove digit validity, including inner product arguments (used in Bulletproofs) and polynomial commitments (used in BFGW).

3.3 Hash Chains

This technique uses a one-way hash function H. A commitment to a value z is created by repeatedly applying the hash function z times to some initial random value r: $C_z = H^z(r)$. To prove that z is at least some threshold t, the prover provides $\pi = H^{z-t}(r)$. The verifier can then check this by computing $H^t(\pi)$ and confirming that it equals C_z. This method is very efficient but typically operates under a stronger trust model where a trusted authority distributes well-formed commitments.

References

- Christ, M., Baldimtsi, F., Chalkias, K. K., Maram, D., Roy, A., & Wang, J. (2024). SoK: Zero-Knowledge Range Proofs.