УДК 004.056.5

LATTICE-BASED ZERO-KNOWLEDGE PROOF FOR MULTIPLICATIVE RELATION BETWEEN COMMITTED VALUES

Нгуен В. Ч (Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО»)

Научный руководитель – **Давыдов В. В.** (Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО»)

In this work a practical lattice-based zero-knowledge proof for multiplicative relation between committed values is constructed. The existing protocol uses many garbage commitments for random masking polynomials which leads to the large proof size. Another approach was used which needs only one additional commitment to a garbage term and achieves smaller proof size and clearer intuition.

Commitment schemes form an important part in the construction of generalized ZKPs and advanced cryptographic constructions. An important feature that often desirable is being able to prove algebraic relationships among committed values. For lattice-based cryptographic schemes it is natural to build proof systems with lattice techniques. Such approach gives simpler implementations and helps to avoid additional hardness assumptions for the schemes.

In this work, we construct a lattice-based solution for zero-knowledge proving multiplicative relations between committed values, which has decent complexity and relatively small proof size.

For proving multiplicative relation between 3 committed values in the existing protocol, beside 3 commitments for those values, the Prover needs to send a large commitment to 5 masking polynomials together with an opening proof for it, and 3 uniform masked openings. This approach requires the proof size to be more than twice the size of commitments to the actual values.

To reduce the proof size, in this work we use another approach which uses only one additional commitment to a garbage term. We let the Verifier compute additional necessary values based on 3 commitments to 3 actual values, 1 commitment to a garbage term and one helper value received from the Prover. Then the Verifier can check the verification equation and decide that the proof is accepted or rejected.

The protocol is constructed following the Sigma protocol ($\sum$-protocol). The Prover commits to a small-coefficient masking vector from a discrete Gaussian distribution. The Verifier then sends back a short challenge polynomial. The Prover calculate a short vector from the opening to values commitments, the short masking vector, and the challenge polynomial. Here a technique called Rejection Sampling is used to make the distribution of the calculated value independent from the opening to values commitments.

The constructed protocol is very technically natural and straight forwards. It uses only one garbage commitment, so the size of the proof is significantly reduced in comparison to existing techniques. The protocol has negligible soundness error which could be resolved by repeating the protocol. Mitigating this soundness error without repeating the protocol will be the goal of the future work.

Нгуен В. Ч. (автор) Подпись

Давыдов В. В. (научный руководитель) Подпись