Jain, Abhishek; **Krenn, Stephan**; **Pietrzak, Krzysztof**; **Tentes, Aris**

Commitments and efficient zero-knowledge proofs from learning parity with noise. (English)

Zbl 1292.94082

Wang, Xiaoyun (ed.) et al., Advances in cryptology – ASIACRYPT 2012. 18th international conference on the theory and application of cryptology and information security, Beijing, China, December 2–6, 2012. Proceedings. Berlin: Springer (ISBN 978-3-642-34960-7/pbk). Lecture Notes in Computer Science 7658, 663-680 (2012).

Summary: We construct a perfectly binding string commitment scheme whose security is based on the learning parity with noise (LPN) assumption, or equivalently, the hardness of decoding random linear codes. Our scheme not only allows for a simple and efficient zero-knowledge proof of knowledge for committed values (essentially a Σ-protocol), but also for such proofs showing any kind of relation amongst committed values, i.e., proving that messages $m_0, \ldots, m_u$, are such that $m_0 = C(m_1, \ldots, m_u)$ for any circuit C.

To get soundness which is exponentially small in a security parameter t, and when the zero-knowledge property relies on the LPN problem with secrets of length ℓ, our 3 round protocol has communication complexity $O(t|C|\ell \log(\ell))$ and computational complexity of $O(t|C|\ell)$ bit operations. The hidden constants are small, and the computation consists mostly of computing inner products of bit-vectors.

For the entire collection see [Zbl 1258.94006].

MSC:

94A60 Cryptography

Full Text: DOI