Ling, San; **Nguyen, Khoa**; **Stehlé, Damien**; **Wang, Huaxiong**

Improved zero-knowledge proofs of knowledge for the ISIS problem, and applications. (English) Zbl 1314.94087

Kurosawa, Kaoru (ed.) et al., Public-key cryptography – PKC 2013. 16th international conference on practice and theory in public-key cryptography, Nara, Japan, February 26–March 1, 2013. Proceedings. Berlin: Springer (ISBN 978-3-642-36361-0/pbk). Lecture Notes in Computer Science 7778, 107-124 (2013).

Summary: In all existing efficient proofs of knowledge of a solution to the infinity norm inhomogeneous small integer solution (ISIS^{∞}) problem, the knowledge extractor outputs a solution vector that is only guaranteed to be $\widetilde{O}(n)$ times longer than the witness possessed by the prover. As a consequence, in many cryptographic schemes that use these proof systems as building blocks, there exists a gap between the hardness of solving the underlying ISIS^{∞} problem and the hardness underlying the security reductions. In this paper, we generalize Stern's protocol to obtain two statistical zero-knowledge proofs of knowledge for the ISIS^{∞} problem that remove this gap. Our result yields the potential of relying on weaker security assumptions for various lattice-based cryptographic constructions. As applications of our proof system, we introduce a concurrently secure identity-based identification scheme based on the worst-case hardness of the $\mathrm{SIVP}_{\widetilde{O}(n^{1.5})}$ problem (in the ℓ_2 norm) in general lattices in the random oracle model, and an efficient statistical zero-knowledge proof of plaintext knowledge with small constant gap factor for Regev's encryption scheme.

For the entire collection see [Zbl 1258.94004].

MSC:

94A60 Cryptography
68P25 Data encryption (aspects in computer science)

Full Text: DOI