Error-Correcting Codes for Lattice-Based Key Exchange

Tim Fritzmann*
* Technical University of Munich
Munich
Germany

The fast progress in the development of quantum computers is leading to an increasing concern about the security of current communication systems. Practical quantum computing algorithms will be able to break most of the public-key cryptosystems in use, including RSA and elliptic curve cryptography. In contrast to traditional cryptography, lattice-based cryptography is believed to be secure against quantum attacks. In 2016, a key exchange mechanism called NewHope Simple [1], which is related to worst-case lattice problems, was proposed. This protocol draws a lot of attention and has good chances to become standardized. However, more analysis is required to allow an optimization of the protocol. We analyzed the failure rate, security, communication overhead and the different error-correcting alternatives. The analysis of the failure rate provides the basis for a performance evaluation of the additive threshold encoding that is currently used in NewHope Simple. It also helps to evaluate error-correcting codes that are more powerful than the one used in NewHope Simple. To improve the error-correcting capability of the protocol, we present four different error-correcting options: i) BCH code; ii) combination of BCH code and additive threshold encoding; iii) LDPC code; and iv) combination of BCH and LDPC code. Test results have shown that all options lead to a significant improvement of the error-correcting capability, whereby their respective benefits and drawbacks vary. The advantage of modern codes, such as LDPC codes, is that they can get close to the channel capacity. In comparison to the applied BCH code, the applied LDPC code gets 3.8 dB closer to the channel capacity at a bit error rate of 10^{-6}. The disadvantage of LDPC codes is that the error floor limits their performance at low error rates. Therefore, classical codes, such as BCH codes, have to be used to achieve very low error rates. Combining a BCH code with an additive threshold encoding leads to a reduction of the time complexity. However, the error-correcting capability is weaker compared to a pure BCH implementation. With the concatenation of the BCH and LDPC code, we combine the advantages of classical and modern codes, achieving a quasi-error-free communication, increasing the security against quantum attacks by 20.39% and decreasing the communication overhead by 12.8%. This enables the development of a key exchange mechanism secure against chosen-ciphertext attacks.

References

[1] Alkim, Erdem and Ducas, Léo and Pöppelmann, Thomas and Schwabe, Peter. NewHope without reconciliation. *IACR Cryptology ePrint*, Archive, 2016, 1157.

crypto day matters 28 (2018)
Beiträge vom 28. Kryptotag, 07.-08.06.2018, Kirchheim.
doi:10.18420/cdm-2018-28-12