Cryptology ePrint Archive: Report 2013/088

Secure Signatures and Chosen Ciphertext Security in a Post-Quantum World

Dan Boneh and Mark Zhandry

Abstract: We initiate the study of quantum-secure digital signatures and quantum chosen ciphertext security. In the case of signatures, we enhance the standard chosen message query model by allowing the adversary to issue quantum chosen message queries: given a superposition of messages, the adversary receives a superposition of signatures on those messages. Similarly, for encryption, we allow the adversary to issue quantum chosen ciphertext queries: given a superposition of ciphertexts, the adversary receives a superposition of their decryptions. These adversaries model a natural post-quantum environment where end-users sign messages and decrypt ciphertexts on a personal quantum computer.

We construct classical systems that remain secure when exposed to such quantum queries. For signatures we construct two compilers that convert classically secure signatures into signatures secure in the quantum setting and apply these compilers to existing post-quantum signatures. We also show that standard constructions such as Lamport one-time signatures and Merkle signatures remain secure under quantum chosen message attacks, thus giving signatures whose quantum security is based on generic assumptions. For encryption, we define security under quantum chosen ciphertext attacks and present both public-key and symmetric-key constructions.

Category / Keywords: foundations / Quantum computing, signatures, encryption, post-quantum security, chosen ciphertext security

Date: received 20 Feb 2013, last revised 20 Feb 2013

Contact author: mzhandry at stanford edu