Cryptology ePrint Archive: Report 2011/421

Superposition Attacks on Cryptographic Protocols

Ivan Damg{\aa}rd and Jakob Funder and Jesper Buus Nielsen and Louis Salvail

Abstract: Attacks on cryptographic protocols are usually modeled by allowing an adversary to ask queries to an oracle. Security is then defined by requiring that as long as the queries satisfy some constraint, there is some problem the adversary cannot solve, such as compute a certain piece of information. Even if the protocol is quantum, the queries are typically classical, such as a choice of subset of players to corrupt. In this paper, we introduce a fundamentally new model of quantum attacks on protocols, where the adversary is allowed to ask several classical queries in quantum superposition. This is a strictly stronger attack than the standard one, and we consider the security of several primitives in this model. We show that a secret-sharing scheme that is secure with threshold t in the standard model is secure against superposition attacks if and only if the threshold is lowered to $t/2$. This holds for all classical as well as a large class of quantum secret sharing schemes. We then consider zero-knowledge and first show that known protocols are not, in general, secure in our model by designing a superposition attack on the well-known zero-knowledge protocol for graph isomorphism. We then use our secret-sharing result to design zero-knowledge proofs for all of NP in the common reference string model. While our protocol is classical, it is sound against a cheating unbounded quantum prover and computational zero-knowledge even if the verifier is allowed a superposition attack. Finally, we consider multiparty computation and give a characterization of a class of protocols that can be shown secure, though not necessarily with efficient simulation. We show that this class contains non-trivial protocols that cannot be shown secure by running a classical simulator in superposition.

Category / Keywords: cryptographic protocols / quantum, protocols, superposition attacks

Date: received 4 Aug 2011, last revised 7 Mar 2012

Contact author: ivan at cs au dk