Cryptology ePrint Archive: Report 2011/001

Practical Frameworks For h-Out-Of-n Oblivious Transfer With Security Against Covert and Malicious Adversaries

Zeng Bing and Tang Xueming and Xu Peng and Jing Jiandu

Abstract: We present two practical frameworks for h-out-of-n oblivious transfer (OT^{n}_{h}). The first one is secure against covert adversaries who are not always willing to cheat at any price. The security is proven under the ideal/real simulation paradigm (call such security fully simulatable security). The second one is secure against malicious adversaries who are always willing to cheat. It provides fully simulatable security and privacy respectively for the sender and the receiver (call such security one-sided simulatable security). The two frameworks can be implemented from the decisional Diffie-Hellman (DDH) assumption, the decisional N-th residuosity assumption, the decisional quadratic residuosity assumption and so on.

The DDH-based instantiation of our first framework costs the minimum communication rounds and the minimum computational overhead, compared with existing practical protocols for oblivious transfer with fully simulatable security against covert adversaries or malicious adversaries.

Though our second framework is not efficient, compared with existing practical protocols with one-sided simulatable security against malicious adversaries. However, it first provides a way to deal with general OT^{n}_{h} on this security level. What is more, its DDH-based instantiation is more efficient than the existing practical protocols for oblivious transfer with fully simulatable security against malicious adversaries.

Category / Keywords: cryptographic protocols / oblivious transfer, secure two-party computation

Date: received 31 Dec 2010, last revised 4 Jan 2011

Contact author: zeng bing zb at gmail com