Cryptology ePrint Archive: Report 2011/510

On the Security of the Free-XOR Technique

Seung Geol Choi and Jonathan Katz and Ranjit Kumaresan and Hong-Sheng Zhou

Abstract: Yao's garbled-circuit approach enables constant-round secure two-party computation for any boolean circuit. In Yao's original construction, each gate in the circuit requires the parties to perform a constant number of encryptions/decryptions, and to send/receive a constant number of ciphertexts. Kolesnikov and Schneider (ICALP 2008) proposed an improvement that allows XOR gates in the circuit to be evaluated ``for free'', i.e., incurring no cryptographic operations and zero communication. Their ``free-XOR'' technique has proven very popular, and has been shown to improve performance of garbled-circuit protocols by up to a factor of~4.

Kolesnikov and Schneider proved security of their approach in the random oracle model, and claimed that (an unspecified variant of) correlation robustness would suffice; this claim has been repeated in subsequent work, and similar ideas have since been used (with the same claim about correlation robustness) in other contexts. We show that, in fact, the free-XOR technique cannot be proven secure based on correlation robustness alone: somewhat surprisingly, some form of circular security is also required. We propose an appropriate notion of security for hash functions capturing the necessary requirements, and prove security of the free-XOR approach when instantiated with any hash function satisfying our definition.

Our results do not impact the security of the free-XOR technique in practice, or imply an error in the free-XOR work, but instead pin down the assumptions needed to prove security.

Category / Keywords: cryptographic protocols /

Date: received 16 Sep 2011, last revised 5 Oct 2011

Contact author: jkatz at cs umd edu

Available formats: PDF | BibTeX Citation

Version: 20111005:145532 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]