Cryptology ePrint Archive: Report 2011/539

Sign Modules in Secure Arithmetic Circuits

Ching-Hua Yu

Abstract: In this paper, we study the complexity of secure multiparty computation using only the secure arithmetic black-box of a finite field, counting the cost by the number of secure multiplications. We observe that a specific type of quadratic patterns exists in all finite fields, and the existence of these patterns can be utilized to improve the efficiency of secure computation to a remarkable extent.

We define \emph{sign modules} as partial functions that %distinguish a specific character. simulate integer signs in an effective range using a polynomial number of arithmetic operations on a finite field. Let ℓ denote the bit-length of a finite field size. We show the existence of $\ell/5$-``effective" sign modules in any finite field that has a sufficiently large characteristic. When $\ell$ is decided first, we further show the existence of prime fields that contain an $\Omega(\ell\log \ell)$-``effective" sign module and we propose an efficient probabilistic algorithm that finds concrete instances of sign modules.

Let $\Z_p$ be any odd prime field. Then, based on the existence of effective sign modules and providing a binary-expressed random number in $\Z_p$, prepared in the offline phase, we show that the computation of bitwise less-than can be improved from the best known result of $O(\ell)$ to $O(\sqrt{\frac{\ell}{\log \ell}})$ (with $O(1)$ rounds) in the online phase using only the $\Z_p$-arithmetic black-box. Accompanied by several related improvements, secure computation involving integer comparisons and modulo reductions can be improved from the best known result $O(\ell)$ to $O(\sqrt{\frac{\ell}{\log \ell}})$ (with $O(1)$ rounds), and a (deterministic) zero test can be improved from $O(\ell)$ to $O(1)$ in the online phase. Additionally, a tight-bound complexity of bit-decomposition is also obtained.

Category / Keywords: cryptographic protocols / multi-party computation, arithmetic black-box, unconditional security

Date: received 1 Oct 2011, last revised 22 Nov 2011

Contact author: chinghua yu at gmail com

Available formats: PDF | BibTeX Citation

Version: 20111122:100937 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]