Cryptology ePrint Archive: Report 2011/301

On the Amortized Complexity of Zero Knowledge Protocols for Multiplicative Relations

Ronald Cramer and Ivan Damgard and Valerio Pastro

Abstract: We present a protocol that allows to prove in zero-knowledge that committed values x_i, y_i, z_i, $i=1,\dots,l$ satisfy $x_iy_i=z_i$, where the values are taken from a finite field K, or are integers. The amortized communication complexity per instance proven is $O(\kappa + l)$ for an error probability of 2^{-l}, where κ is the size of a commitment. When the committed values are from a field of small constant size, this improves complexity of previous solutions by a factor of l. When the values are integers, we improve on security: whereas previous solutions with similar efficiency require the strong RSA assumption, we only need the assumption required by the commitment scheme itself, namely factoring. We generalize this to a protocol that verifies l instances of an algebraic circuit D over K with v inputs, in the following sense: given committed values $x_{i,j}$ and z_i, with $i=1,\dots,l$ and $j=1,\dots,v$, the prover shows that $D(x_{i,1},\dots,x_{i,v})= z_i$ for $i=1,\dots,l$. For circuits with small multiplicative depth, this approach is better than using our first protocol: in fact, the amortized cost may be asymptotically smaller than the number of multiplications in D.

Category / Keywords: cryptographic protocols /

Date: received 6 Jun 2011

Contact author: cramer at cwi nl, ivan@cs au dk, vpastro@cs au dk