Efficient Protocols based on Probabilistic Encryption using Composite Degree Residue Classes

Ivan Damgård, Mads Jurik
Aarhus University, Dept. of Computer Science
Ny Munkegade
DK 8000 Aarhus C
Denmark
Tel. +45 89 42 33 80
Email: ivan@daimi.au.dk

27 April 2000

Keywords: Voting Schemes, Threshold Cryptosystems, Zero-Knowledge.

We study various applications and variants of Paillier's probabilistic encryption scheme. First, we propose a threshold variant of the scheme, and then zero-knowledge protocols for proving that a given ciphertext encodes a given plaintext, and for verifying multiplication of encrypted values.

We then show how these building blocks can be used for applying the scheme to efficient electronic voting. This leads to a voting scheme which is as efficient for the voters as the previously best known solutions, but which reduces dramatically the work needed to compute the final result of an election. To the best of our knowledge, this is the first voting scheme that scales well to elections with a large number of voters and candidates.

We show how the basic scheme for a yes/no vote can be easily adapted to casting a vote for up to t out of L candidates. The same basic building blocks can also be adapted to provide receipt-free elections, under appropriate physical assumptions. The scheme for 1 out of L elections can be optimised such that for a certain range of parameter values, a ballot has size only $O(\log L)$ bits.

Finally, we propose a variant of the encryption scheme, that allows reducing the expansion factor of Paillier's scheme from 2 to almost 1.

A technical report describing our results in more detail can be found at http://www.brics.dk (under "publications")