LASEC

ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

Generic Homomorphic Undeniable Signature Scheme: Optimizations

Security and Cryptography Laboratory

A new undeniable signature scheme was proposed by LASEC. It allows to transform a private group homomorphism into a undeniable signature scheme. In 2004, a demonstrator for this scheme using the quartic residue symbol as a homomorphism has been implemented. The aim of this project was to optimize the existing implementation and to implement 3 additional homomorphisms (Jacobi symbol, discrete logarithm, RSA exponentiation) and compare them to each other.

Quartic residue and Jacobi symbol

By optimizing and reimplementing we achieved to reduce the running time of the existing implementation of the basic algorithm for the quartic residue symbol by half. Furthermore, we tried out Damgård's algorithm as well as a mixed algorithm, which lead to another gain in speed, and compared them to implementations of the Jacobi symbol, which is the equivalent of the quartic residue symbol in $\mathbb{Z}$.

Other homomorphisms

We implemented three versions of a homomorphism based on the discrete logarithm: the first using a hash table containing the precomputed values of the discrete logarithm, the second and the third implementing the Baby Step Giant Step (BSGS) and Pollard's Rho algorithm. We compared them to our implementation of the RSA exponentiation, the quartic residue symbol and the Jacobi symbol.

Results

Our implementations are written in C and use the GNU Multiple Precision Arithmetic Library (GMP) to handle large integers. We conducted our timing measurements with random numbers of the size a typical security level requires. All our results are average values.

Computation of one homomorphism	time in ms	iterations
Quartic: basic algorithm not optimized	62.79	249.27
Quartic: basic algorithm optimized	31.57	249.27
Quartic: Damgård's algorithm	50.63	766.12
Quartic: mixed algorithm	24.65	511.92
Jacobi: basic algorithm	1.26	187.71
Jacobi: binary algorithm (GMP)	0.12	
Discrete logarithm: precomputed table	9.66	
Discrete logarithm: BSGS	19.47	388.36
Discrete logarithm: Pollard's Rho	74.93	1037.49
RSA:	33.87	

Project produced by Yvonne Anne Oswald, Supervised by Jean Monnerat, February 2005.