Optimization of the MOVA Undeniable Signature Scheme

Jean Monnerat[1,⋆], Yvonne Anne Oswald[2], and Serge Vaudenay[1]

[1] EPFL, Switzerland
http://lasecwww.epfl.ch
[2] ETH Zürich, Switzerland

Abstract. This article presents optimization results on the MOVA undeniable signature scheme presented last year by Monnerat and Vaudenay at PKC '04 as well as its generalization proposed at Asiacrypt '04 which is based on a secret group homomorphism. The original MOVA scheme uses characters on $\mathbf{Z}_n^*$ and some additional candidate homomorphisms were proposed with its generalization. We give an overview of the expected performance of the MOVA scheme depending on the group homomorphism. Our optimizations focus on the quartic residue symbol and a homomorphism based on the computation of a discrete logarithm in a hidden subgroup of $\mathbf{Z}_n^*$. We demonstrate that the latter provides a signature generation which is three times faster than RSA.

Keywords: Undeniable signatures, optimization.

1 Introduction

Undeniable signatures, which have been introduced by Chaum and van Antwerpen in [1], differ from classical digital signatures in the verification process. Contrary to classical digital signatures, where anyone holding the public key of the signer is able to verify whether a given signature is valid or not, one has to interact with the signer to be convinced of the validity or the invalidity of the signature. This interaction enables the signer to control the distribution of the signature verification. An undeniable signature scheme therefore consists of a key setup algorithm and a signature generation algorithm, as well as an interactive verification protocol. This protocol is composed of a confirmation and a denial protocol which allow to prove the validity resp. the invalidity of the signature.

In March 2004, a new undeniable signature scheme called MOVA was proposed by Monnerat and Vaudenay [12]. More recently, the same authors generalized this scheme to the more general framework of group homomorphisms [13]. Namely, the MOVA scheme can be seen as the particular case where the underlying homomorphism is a character on $\mathbf{Z}_n^*$. When the choice of the homomorphism is adequate (as for MOVA), this signature scheme allows signatures to be arbitrarily short (typically around 20–30 bits), depending on the required security level.

⋆ Supported by a grant of the Swiss National Science Foundation, 200021-101453/1.

E. Dawson and S. Vaudenay (Eds.): Mycrypt 2005, LNCS 3715, pp. 196–209, 2005.

The goal of this paper is to optimize the signature generation algorithm of the generalized scheme based on group homomorphisms and to present a comparison of the signature generation efficiency between the group homomorphisms considered as potential candidates. In particular, we focus on the optimization of characters of order 4 which requires to deal with algorithms computing the quartic residue symbol. Moreover, one quartic residue symbol variant is of particular interest since it is the only homomorphism presenting the special property of having two levels of secret. We propose an application of this property where a delegate of a company needs to sign some pre-agreement of a transaction which will be finalized later by the company using an additional level of secret. We also analyze the case of a homomorphism proposed in [13] consisting of sending elements of $\mathbf{Z}_n^*$ to a cyclic subgroup followed by the computation of a discrete logarithm. We give details on an implementation using a precomputed table of discrete logarithms. A comparison with practical parameters (e.g., a modulus n of 1024 bits) with the Jacobi symbol as well as RSA using standard efficient methods is presented at the end of this article. Our implementations are done in C using the large numbers library GMP [6].

2 The MOVA Scheme

For the sake of simplicity, the generalized scheme [13] will be called MOVA as well. Below we review the main ideas and the signature generation algorithm of this undeniable signature scheme.

First, let us recall some basic definitions from [13] related to the interpolation of group homomorphisms.

Definition 1. *Let G and H be two Abelian groups.*

1. *Given $S := \{(x_1, y_1), \ldots, (x_s, y_s)\} \subseteq G \times H$, we say that the set of points S* interpolates in a group homomorphism *if there exists a group homomorphism $f : G \longrightarrow H$ such that $f(x_i) = y_i$ for $i = 1, \ldots, s$.*
2. *We say that a set of points $B \subseteq G \times H$* interpolates in a group homomorphism with another set of points *$A \subseteq G \times H$ if $A \cup B$ interpolates in a group homomorphism.*

The central idea of the generalized MOVA scheme is to consider a secret group homomorphism Hom between two publicly known Abelian groups Xgroup and Ygroup as the signer's secret key. The order of the group Ygroup is public and is denoted as d. The signer then chooses a set Skey $\subseteq$ Xgroup $\times$ Ygroup of Lkey points such that Skey interpolates in a unique homomorphism, namely Hom. The signer chooses Skey $:= \{(\mathrm{Xkey}_1, \mathrm{Ykey}_1), \ldots, (\mathrm{Xkey}_{\mathrm{Lkey}}, \mathrm{Ykey}_{\mathrm{Lkey}})\}$ in varying ways depending on the choice of one of the setup variants presented in [13]. The size of the parameter Lkey depends on the setup variant choice too. Then, to sign a given message m the signer computes Lsig values $\mathrm{Xsig}_1, \ldots, \mathrm{Xsig}_{\mathrm{Lsig}} \in$ Xgroup from m by using a random oracle and computes $\mathrm{Hom}(\mathrm{Xsig}_i) := \mathrm{Ysig}_i$