CMSS – An Improved Merkle Signature Scheme

Johannes Buchmann[1], Luis Carlos Coronado García[2], Erik Dahmen[1], Martin Döring[1,⋆], and Elena Klintsevich[1]

[1] Technische Universität Darmstadt
Department of Computer Science
Hochschulstraße 10, 64289 Darmstadt, Germany
{buchmann, dahmen, doering, klintsev}@cdc.informatik.tu-darmstadt.de
http://www.sicari.de
[2] Banco de México
Av. 5 de Mayo No. 6, 5to piso
Col. Centro C.P. 06059, México, D.F.
coronado@banxico.org.mx

Abstract. The Merkle signature scheme (MSS) is an interesting alternative for well established signature schemes such as RSA, DSA, and ECDSA. The security of MSS only relies on the existence of cryptographically secure hash functions. MSS has a good chance of being quantum computer resistant. In this paper, we propose CMSS, a variant of MSS, with reduced private key size, key pair generation time, and signature generation time. We demonstrate that CMSS is competitive in practice by presenting a highly efficient implementation within the Java Cryptographic Service Provider FlexiProvider. We present extensive experimental results and show that our implementation can for example be used to sign messages in Microsoft Outlook.

Keywords: Java Cryptography Architecture, Merkle Signatures, One-Time-Signatures, Post-Quantum Signatures, Tree Authentication.

1 Introduction

Digital signatures have become a key technology for making the Internet and other IT infrastructures secure. Digital signatures provide authenticity, integrity, and support for non-repudiation of data. Digital signatures are widely used in identification and authentication protocols, for example for software downloads. Therefore, secure digital signature algorithms are crucial for maintaining IT security.

Commonly used digital signature schemes are RSA [RSA78], DSA [Elg85], and ECDSA [JM99]. The security of those schemes relies on the difficulty of factoring large composite integers and computing discrete logarithms. However, it is unclear whether those computational problems remain intractable in the

⋆ Author supported by SicAri, a project funded by the German Ministry for Education and Research (BMBF).

R. Barua and T. Lange (Eds.): INDOCRYPT 2006, LNCS 4329, pp. 349–363, 2006.

future. For example, Peter Shor [Sho94] proved that quantum computers can factor integers and can calculate discrete logarithms in the relevant groups in polynomial time. Also, in the past thirty years there has been significant progress in solving the integer factorization and discrete logarithm problem using classical computers (Lenstra and Verheul). It is therefore necessary to come up with new signature schemes which do not rely on the difficulty of factoring and computing discrete logarithms and which are even secure against quantum computer attacks. Such signature schemes are called post-quantum signature schemes.

A very interesting post-quantum signature candidate is the Merkle signature scheme (MSS) [Mer89]. Its security is based on the existence of cryptographic hash functions. In contrast to other popular signature schemes, MSS can only verify a bounded number of signatures using one public key. Also, MSS has efficiency problems (key pair generation, large secret keys and signatures) and was not used much in practice.

Our contribution. In this paper, we present CMSS, a variant of MSS, with reduced private key size, key pair generation time, and signature generation time. We show that CMSS is competitive in practice by presenting a highly efficient CMSS Java implementation in the Java Cryptographic Service Provider FlexiProvider [Flexi]. This implementation permits easy integration into applications that use the Java Cryptography Architecture [JCA02]. We present experiments that show: As long as no more that 2^{40} documents are signed, the CMSS key pair generation time is reasonable, and signature generation and verification times in CMSS are competitive or even superior compared to RSA and ECDSA. We also show that the CMSS implementation can be used to sign messages in Microsoft Outlook using our `FlexiS/MIME` plug-in [FOP03]. The paper specifies CMSS keys using Abstract Syntax Notation One (ASN.1) [Int02] which guarantees interoperability and permits efficient generation of X.509 certificates and PKCS#12 personal information exchange files. CMSS is based on the Thesis of Coronado [Cor05b] and incorporates the improvements of MSS from [Szy04, DSS05].

Related Work. Szydlo presents a method for the construction of authentication paths requiring logarithmic space and time in [Szy04]. Dods, Smart and Stam give the first complete treatment of practical implementations of hash based digital signature schemes in [DSS05]. In [NSW05], Naor et. al. propose a C implementation of MSS and give timings for up to 2^{20} signatures. A preliminary version of CMSS including security proofs appeared in the PhD thesis of Coronado [Cor05b] and in [Cor05a].

Organization. The rest of this paper is organized as follows: In Section 2, we describe the Winternitz one-time signature scheme and the Merkle signature scheme. In Section 3, we describe CMSS. Section 4 describes details of the CMSS implementation in the FlexiProvider and the ASN.1 specification of the keys. Section 5 presents experimental data including a comparison with standard signature schemes. Section 6 describes the integration of the CMSS implementation into Microsoft Outlook. Section 7 states our conclusions.