Two Efficient and Provably Secure Schemes for Server-Assisted Threshold Signatures

Shouhuai Xu[1,⋆] and Ravi Sandhu[2]

[1] Department of Information and Computer Science
University of California at Irvine
shxu@ics.uci.edu
[2] SingleSignOn.Net and Laboratory for Information Security Technology
George Mason University
sandhu@gmu.edu

Abstract. Secrecy of private signing keys is one of the most important issues in secure electronic commerce. A promising solution to this problem is to distribute the signing function among multiple parties. However, a threshold signature scheme typically assumes that the shared signing function can only be activated by a quorum number of parties, which is inappropriate in settings where a user employs some public servers for a threshold protection of her private signing function (therefore the name "server-assisted threshold signatures").
In this paper we present two efficient and provably secure schemes for server-assisted threshold signatures, where the signing function is activated by a user (but in certain enhanced way). The first one (we call `TPAKE-HTSig`) is tailored for the setting where a user has a networked device that is powerful enough to efficiently compute modular exponentiations. The second one (we call `LW-TSig`) is tailored for the setting where a user has a smart card without a cryptographic co-processor. Modular construction of the schemes ensures that any module can be substituted without weakening security of the resultant scheme, as long as the substitutive one satisfies certain security requirement. In addition to the two schemes, we also present a taxonomy of systems protecting private signing functions.

1 Introduction

Secrecy of private signing keys is one of the most important issues in secure electronic commerce. Threshold signatures enable us to achieve better security (i.e., compromise of certain number of participants does not expose the private key) and availability (i.e., a quorum number of participants suffice to sign messages). However, threshold signature schemes typically assume that the shared signing function can only be activated by a quorum number of participants; otherwise, the participant able to activate the function can always get signatures

⋆ Work mostly done while at the Laboratory for Information Security Technology, George Mason University.

M. Joye (Ed.): CT-RSA 2003, LNCS 2612, pp. 355–373, 2003.
© Springer-Verlag Berlin Heidelberg 2003

without compromising the private key. This assumption is relevant in certain settings (e.g., enterprise applications) but inappropriate in settings where a user employs some public servers (which perhaps provide service for economic incentives) to provide a threshold protection for her private signing function (therefore the name "server-assisted threshold signatures").

1.1 Our Contributions

We propose two efficient and provably secure schemes for server-assisted threshold signatures, where the signing function is activated by a user (but in certain enhanced way). The schemes are obtained via a *modular composition* approach, thereby any module can be substituted without weakening security of the resultant scheme, as long as the substitutive one (with, for instance, better performance) satisfies certain security requirements. The first scheme (we call `TPAKE-HTSig`) is tailored for the setting where a user has a networked device that is powerful enough to efficiently compute modular exponentiations. The second scheme (we call `LW-TSig`) is tailored for the setting where a user has a smart card with no cryptographic co-processor. In addition to the two schemes, we also present a taxonomy of systems protecting private signing functions.

Remark. Having said that our schemes allow the substitution of component modules as long as certain security requirement is satisfied, we stress that our approach is less general than the approach of Canetti [10].

Outline. In Section 2 we present certain cryptographic preliminaries. In Section 3 we present our first scheme `TPAKE-HTSig`, of which a formal security analysis is given in Appendix B. In Section 4 we present our second scheme `LW-TSig`. In Section 5, we present a taxonomy of systems for protecting private signing functions (including our schemes). We conclude in section 6. Due to space limitation, we eliminate from this version many discussions (including security analysis of `LW-TSig`), which will be found in the full version of this paper.

2 Cryptographic Preliminaries

Message Authentication Codes (MACs). A function family $\{f_k\}_k$, where $k \in \{0,1\}^\kappa$ for some security parameter κ, is a secure MAC family if any adversary $\mathcal{A}$ of probabilistic polynomial-time succeeds in the following game only with negligible probability. First a random key $k \in \{0,1\}^\kappa$ is chosen; then $\mathcal{A}$ adaptively chooses messages $m_1, \cdots, m_n$ and receives the corresponding MAC values $f_k(m_1), \cdots, f_k(m_n)$. $\mathcal{A}$ succeeds if it manages to generate a pair $\langle m, tag \rangle$, where $m \neq m_1, \cdots, m_n$ but $tag = f_k(m)$. We refer the reader to [2] for details.

Signature Schemes. A signature scheme `Sig` consists of three algorithms (`Sig.Init`, `Sig.Sig`, `Sig.Ver`). Taken as input a security parameter κ, the probabilistic key generation algorithm `Sig.Init` returns a pair of public and private keys (Y, X). Taken as input a message m and the private key X, the signing algorithm `Sig.Sig` outputs a signature σ. Taken as input a tag σ, the public key Y, and a message m, the verification algorithm `Sig.Ver` returns TRUE if σ is