A Subliminal-Free Variant of ECDSA

Jens-Matthias Bohli[1], María Isabel González Vasco[2], and Rainer Steinwandt[3]

[1] Institut für Algorithmen und Kognitive Systeme, Universität Karlsruhe, 76128 Karlsruhe, Germany
bohli@ira.uka.de
[2] Departamento de Matemática Aplicada, Universidad Rey Juan Carlos, c/ Tulipán, s/n, 28933 Madrid, Spain
mariaisabel.vasco@urjc.es
[3] Center for Cryptology and Information Security, Dept. of Mathematical Sciences, Florida Atlantic University, 777 Glades Road, Boca Raton, FL 33431, USA
rsteinwa@fau.edu

Abstract. A mode of operation of the Elliptic Curve Digital Signature Algorithm (ECDSA) is presented which provably excludes subliminal communication through ECDSA signatures. For this, the notion of a signature scheme that is *subliminal-free with proof* is introduced which can be seen as generalizing *subliminal-free signatures* and being intermediate to the established concepts of *invariant* and *unique signatures*.

Motivated by the proposed use of ECDSA for signing passports, our focus is not on proving the mere existence of a subliminal-free ECDSA mode of operation, but on demonstrating its practical potential. The proposed construction relies on the availability of a party acting as warden and on a reasonably-sized non-interactive proof of subliminal-freeness. For instance, in the passport scenario, the passport holder plays the role of the warden, and we show that a suitable combination of the pseudo random function of Naor and Reingold with bit commitments and non-interactive zero-knowledge proofs can be used for accomplishing the required proof of subliminal-freeness with acceptable efficiency.

Keywords: subliminal communication, digital signature, ECDSA.

1 Introduction

It is a well-known phenomenon that cryptographic schemes can also be used for purposes or in a way they have not been designed for (cf., for instance, [DGB87, Des88a, Des88b, YY04]). One well-explored example of this is the use of *subliminal channels* in signature schemes: Subliminal channels in signature schemes were introduced by Simmons in [Sim84] as a solution to the prisoner's problem: two prisoners are allowed to exchange signed messages, but their communication is monitored by a warden. The prisoners want to exchange a secret message unnoticeable to the warden and hide the message in a signature of a "harmless" cover message. In contrast, the warden is interested in implementing a subliminal-free signature scheme that prevents any subliminal communication.

J. Camenisch et al. (Eds.): IH 2006, LNCS 4437, pp. 375–387, 2007.

Of course, this scenario does not address the use of steganographic techniques for embedding information, and is mainly of interest if the signer has no or only limited control over the messages to be signed.

However, already developing a general formalization of subliminal communication is quite an ambitious goal. In the context of interactive zero-knowledge proofs for languages, a formalization of subliminal-freeness has been put forward by Burmester et al. in [BDI+99]. For the specific case of subliminal communication through digital signatures such a formalization has been proposed in [BS05]. Specifically, [BS05] provides a definition of a (non-interactive) *subliminal-free signature scheme* and proves the well-established RSA-PSS scheme to be subliminal-free in this sense (if being used in deterministic mode along with a precautious key generation).

However, for the common family of Digital Signature Algorithm (DSA)-like signatures no subliminal-free variant is known[Sim94]. Simmons [Sim93] gives an interactive signing procedure between the signer and the warden for generating DSA signatures, but as pointed out by Desmedt in [Des96], this scheme contains a subliminal channel, if the signer can reject some protocol runs and start anew. While the warden in an interactive protocol could take some precautions against this, it makes a transformation into a non-interactive signing procedure where the signer uses a pseudo random generator to simulate the warden's input impossible—the signer can reject the signing process privately and unnoticeably.

A cryptographic primitive that turns out to be closely related to subliminal-free signature schemes is known as *invariant signature schemes* [GO93]. A special type of *invariant signature schemes* are *unique signature schemes*, defined by [Lys02] as those schemes for which only one valid signature is provided for each message and verification key. Unique signature schemes are subliminal-free in the sense of [BS05], but in most scenarios where subliminal channels matter, signatures do not need to be unique w. r. t. the verification, as long as the warden is convinced that the signing algorithm has been used "in a unique manner". We will refer to signatures, where the warden can be convinced of such uniqueness, as *subliminal-free with proof* and show that they lie between invariant and unique signatures.

Within our new framework a subliminal-free usage of ECDSA is possible in the following sense: If the proof delivered along with the signature is correct, the warden can be sure that the signature does not contain suspicious information (and delete the proof). Note that we do not care about subliminal information embedded in the proof: We aim at preventing communication between signer and verifier through signatures, not at preventing communication between signer and warden. A scenario where the availability of a warden is quite natural is in the context of digitally signed passports: e. g., Germany considers using ECDSA for signing passports [Bun05]. Thus, one may ask whether it is possible to produce ECDSA signatures where the owner of a passport (who is taking the role of the warden here) can be sure that the signature contains no subliminal compromising information.