Control and Cybernetics

vol. **42** (2013) No. 4

Lightweight digital signature with secretly embedded warning*†

by

Mirosław Kutyłowski and Przemysław Kubiak

Institute of Mathematics and Computer Science
Wrocław University of Technology
ul. Wybrzeże Wyspiańskiego 27, 50-370 Wrocław, Poland
{miroslaw.kutylowski; przemyslaw.kubiak}@pwr.wroc.pl

Abstract: We show how a signatory can indicate coercion by embedding a secret message into the signature. Our scheme is practical and applies to standard signature schemes unlike the recent construction of Durnoga et al. (2013). The construction follows directly from kleptographic techniques due to Moti Yung and Adam Young.

Keywords: coercion, digital signature, kleptography, funkspiel

1. Introduction

We address the problem of coercing an owner of a *signature creation device* to sign a document. The idea is that the owner uses a *coercion PIN* and the device creates a signature, which is indistinguishable from the regular one – at least from the point of view of the coercer, but at the same time contains a secret warning.

A scheme satisfying these requirements has been proposed in Durnoga et al. (2013). However, this scheme is quite inefficient in terms of computational complexity and incompatible with the signature schemes used in practice.

In this note we propose a fairly simple solution to the same problem based on techniques from Young and Yung (1997) (also related to the *funkspiel* techniques, Håstad et al., 2000). It applies to any signature scheme based on the Discrete Logarithm Problem, where we compute $r := g^k$ for a k chosen at random, and either r is explicitly given or can be reconstructed from the final signature. Examples of such schemes are ElGamal, Schnorr, DSA, ECDSA, Nyberg-Rueppel. (RSA does not fall into this category, however a similar solution is possible for RSA-PSS encoding, see RSA Laboratories, 2005.)

*Submitted: September 2013; Accepted: September 2013

†This paper was partly supported by the grant S30028/I-18 from the Institute of Mathematics and Computer Science, Wrocław Uniwersity of Technology.

2. Efficient signatures with a warning

2.1. The scheme

In order to embed a warning we use a signature creation device such that there are different PIN numbers which lead to signatures with embedded warning and signatures without warning. Which PIN is which is known only to the device owner. Moreover, there could be more than two PINs where only one is without warning. So, coercing the owner to reveal the PIN or PINs may lead to exposure of all PINs but the "no warning" PIN and the coercer cannot see that an incomplete set of PINs has been revealed.

For a PIN with warning the following signing procedure is executed by the signing device:

PROCEDURE 1: creating a signature with a warning

1. choose k at random,
2. compute $w = Y^k$, where Y is the public key of the authority to be warned
3. if $Hash(M, w)$ has the last bit equal to 0, then return to point 1 and choose k again
4. compute $r = g^k$ and proceed with the standard signature algorithm.

For a PIN with no warning the following signing procedure is executed by the signing device:

PROCEDURE 2: creating a signature with no warning

1. choose k at random,
2. compute $w = Y^k$, where Y is the public key of the authority to be warned
3. if $Hash(M, w)$ has the last bit equal to 1, then return to point 1 and choose k again
4. compute $r = g^k$ and proceed with the standard signature algorithm.

2.2. Properties

Note the following properties of the scheme:

- A trusted authority knowing secret y such that $Y = g^y$ can easily recover w as $w = Y^k = g^{yk} = r^y$, and thereby compute $Hash(M, w)$.
- For the coercer it is infeasible to read the warning: even if a candidate for the value w is given, then without y it is infeasible to check whether $w = Y^k$. Indeed, (g, g^k, g^y, w) is a case of the Decisional Diffie Hellman Problem.
- The only way to learn the warning is to reverse engineer the signing device and recover the signing key x. It is known that in this case the ephemeral values k can be recovered from the signatures. Consequently, we may compute the warning as well. However, the scheme of Durnoga et al. (2013) also reveals the warning if all secrets of the signers are revealed. On the other hand, if we are using a signature creation device, then we strongly believe that it is infeasible to retrieve the secret keys stored in the device.

References

Durnoga, K., Pomykała, J. and Trabszys, T. (2013) Digital signature with secretly embedded warning. *Control and Cybernetics*, in this issue, 805–824

Håstad, J., Jonsson, J., Juels, A. and Yung, M. (2000) Funkspiel schemes: an alternative to conventional tamper resistance. In D. Gritzalis, S. Jajodia, and P. Samarati, eds.: *ACM Conference on Computer and Communications Security*. ACM, 125–133.

Young, A.L. and Yung, M. (1997) Kleptography: Using cryptography against cryptography. In W. Fumy, ed.: *EUROCRYPT*. LNCS **123**, Springer, 62–74.

RSA Laboratories (2005) PKCS#1 v2.1 – RSA Cryptography Standard + Errata.