# How to Sign with One Bit

## Abstract

Jean Monnerat and Serge Vaudenay

EPFL

An undeniable signature scheme is similar to a classical digital signature except that the recipient of a message cannot verify its validity by itself: he needs also to interact with the signer in order to be convinced of the validity of the signature. This opposes to the so called universal verifiability of classical digital signatures where anybody knowing the signer's public key is able to verify the signature at any time. In some applications such as signing a contract it is desirable to keep the signer's privacy by limiting the ability to verify this signature. However, an undeniable signature does not abandon the non repudiation property. Indeed, in the case of a dispute the signer could be compelled by an authority to prove the invalidity of a signature, otherwise this would be considered as an attempt of denying a valid signature. An undeniable signature scheme is composed of a signature generation algorithm, a confirmation protocol to prove the validity of a signature and a denial protocol in order to prove the invalidity of an alleged non signature. These two protocols often consist of an interactive proof.

Since the invention of the first undeniable signature scheme proposed by Chaum and van Antwerpen [5], a certain amount of work has been dedicated to its development and different improvements [2,3,4,6,7]. Until the proposition of an undeniable signature scheme based on RSA by Gennaro et al. [8], all the other undeniable signatures were based on the discrete logarithm problem. More recently, three undeniable signatures based on different problems have been proposed. The first one is based on pairings [9], the second one is based on a quadratic field [1] and the third one (MOVA) is based on characters [10].

In traditional digital signature schemes, the security collapses when the signature is too short because of universal verifiability: an attacker can try to guess a signature until it is valid in order to forge it. One advantage of undeniable signatures is that the security smoothly decreases with the signature length. As an example, we can think about 20-bit signatures which cannot be forged but with a probability of success of $2^{-20}$. This probability can be increased in an on-line attack which can easily be detected. So, undeniable signatures could in principle be arbitrarily small e.g. as small as a MAC, although no such signatures were proposed so far except MOVA signatures. We can even consider a 1-bit signature.

We introduce a new computational problem related to the interpolation of group homomorphisms. Many famous cryptographic problems including discrete logarithm, Diffie-Hellman, RSA are at most as hard as special instances of this problem. As a principal application, we propose a generic undeniable signature

scheme which generalizes the recent MOVA schemes. Our scheme is generic in the sense that we transform a private group homomorphism from a public input group to a public output group (whose order is also public) into an undeniable signature scheme. It is provably secure in the random oracle model and it offers the advantage of making signature size arbitrarily short (depending on a security level). We (im)prove some security results from MOVA. We also propose an example with complexity similar to RSA and with 3-byte signatures whose complexity cost is similar to RSA [11]. We hope that this example will be completed by some various additional settings since group homomorphisms are common objects in cryptography.

## References


1. I. Biehl, S. Paulus and T. Takagi, *Efficient Undeniable Signature Schemes based on Ideal Arithmetic in Quadratic Orders*, Conference on The Mathematics of Public-Key Cryptography, Toronto, 1999.
2. J. Boyar, D. Chaum, I. Damgård and T. Pedersen, *Convertible Undeniable Signatures*, Advances in Cryptology - Crypto '90, LNCS **537**, pp. 189-205, Springer, 1990.
3. D. Chaum, *Zero-Knowledge Undeniable Signatures*, Advances in Cryptology - Eurocrypt '90, LNCS **473**, pp. 458-464, Springer, 1990.
4. D. Chaum, *Designated Confirmer Signatures*, Advances in Cryptology - Eurocrypt '94, LNCS **950**, pp. 86-91, Springer, 1994.
5. D. Chaum and H. van Antwerpen, *Undeniable Signatures*, Advances in Cryptology - Crypto '89, LNCS **435**, pp. 212-217, Springer, 1989.
6. I. Dåmgard and T. Pedersen, *New Convertible Undeniable Signatures Schemes*, Advances in Cryptology - Eurocrypt '96, LNCS **1070**, pp. 372-386, Springer, 1996.
7. Y. Desmedt and M. Yung, *Weaknesses of Undeniable Signature Schemes*, Advances in Cryptology - Crypto '91, LNCS **576**, pp. 205-220, Springer, 1991.
8. R. Gennaro, T. Rabin and H. Krawczyk, *RSA-Based Undeniable Signatures*, Journal of Cryptology, **13**, pp. 397-416, Springer, 2000.
9. B. Libert and J.-J. Quisquater, *Identity Based Undeniable Signatures*, Cryptology ePrint Archive, Report 2003/206, 2003, `http://eprint.iacr.org`.
10. J. Monnerat and S. Vaudenay, *Undeniable Signatures Based on Characters: How to Sign with One Bit.*, PKC '04, LNCS **2947**, pp. 69–85, Springer, 2004.
11. R. L. Rivest, A. Shamir and L. M. Adleman, *A Method for Obtaining Digital Signatures and Public-key Cryptosystem*, Communications of the ACM, vol. 21, pp. 120-126, 1978.