Undeniable Signatures

David Chaum
Hans van Antwerpen

Centre for Mathematics and Computer Science
Kruislaan 413 1098 SJ Amsterdam

Introduction & Motivation

Digital signatures [DH]—unlike handwritten signatures and banknote printing—are easily copied exactly. This property can be advantageous for some uses, such as dissemination of announcements and public keys, where the more copies distributed the better. But it is unsuitable for many other applications. Consider electronic replacements for all the written or oral commitments that are to some extent personally or commercially sensitive. In such cases the proliferation of certified copies could facilitate improper uses like blackmail or industrial espionage. The recipient of such a commitment should of course be able to ensure that the issuer cannot later disavow it—but the recipient should also be unable to show the commitment to anyone else without the issuer's consent.

Undeniable signatures are well suited to such applications. An undeniable signature, like a digital signature, is a number issued by a signer that depends on the signer's public key and the message signed. Unlike a digital signature, however, an undeniable signature cannot be verified without the signer's cooperation.

The validity of an undeniable signature can be ascertained by anyone issuing a challenge to the signer and testing the signer's response. If the test is successful, there is an exponentially high probability that the signature is valid. If the test fails, there are two cases: (a) the signature is not valid; or (b) the signer is giving improper responses, presumably in an effort to falsely deny a valid signature. But even if the signer has infinite computing power, the challenger can

G. Brassard (Ed.): Advances in Cryptology - CRYPTO '89, LNCS 435, pp. 212-216, 1990.

distinguish case (a) from case (b), with exponentially high certainty, by means of a second challenge.

Quite efficient and practical undeniable signature protocols based on the "discrete log" problem [DH] are presented below. Since all signers can use the same group, signatures created by different signers commute with each other—a useful property [CE] that has not yet been achieved for digital signatures. Furthermore, a new type of "blinding" [C] can be applied in the signing as well as in the challenge and response.

CRYPTOGRAPHIC SETTING

Consider using the group of known prime order p: All values transmitted between the participants are elements of this group, the multiplicatively denoted group operation is easily computed by all participants, and taking the discrete log in the group is assumed to be computationally infeasible.

One potentially suitable representation is the multiplicative group of the field GF(2^n), where $p = 2^n\text{-}1$ is prime. A second is the group of squares modulo prime q, where $q\text{-}1 = 2p$. (Notice that such choices rule out the Pohlig-Hellman attack on discrete log [PH].) An attractive variation on the second approach represents group elements by the integers 1 to p; the group operation is the same, except that all results are normalized by taking the additive inverse exactly when this yields a smaller least positive representative.

PROTOCOL

A suitable group of prime order p and a primitive element g are initially established and made public for use by a set of signers. Consider a particular signer S having a private key x and a corresponding public key g^x. A message m ($\neq 1$) is signed by S to form signature z, which should be equal to m^x. Someone receiving z from S may wish to establish its validity immediately; the challenge/response protocol used to establish this, though, is the same for any later verifier V.

The initial challenge is of the form $z^a(g^x)^b$, where V chooses a and b independently and uniformly from the group elements. The response should be formed by S raising the challenge to the multiplicative inverse of x modulo p. When V computes $m^a g^b$ and finds it equal to the response, then V knows (by Theorem 1 below) that, even if S were to have infinite computing power, the probability of z being unequal m^x (and hence invalid) is at most p^{-1}.

When the value V computes is unequal to the response, the challenge/response protocol should be repeated with independently chosen c and d replacing a and b, respectively. Then V can use the two responses r_1 and r_2 to test whether $(r_1 g^{-b})^c = (r_2 g^{-d})^a$. Equality means that S is answering consistently and z is invalid, with the same high probability as for signature validity; inequality means that S is answering improperly (Theorem 2).

UNDENIABILITY

Two essential points can be proved:

Theorem 1: Even with infinite computing power S cannot with probability exceeding p^{-1} provide a valid response for an invalid signature.

Proof: First notice that each challenge value corresponds to p pairs (a,b), as a simple consequence of the group structure. It is sufficient to show that if the signature is not m^x, then each pair corresponding to a challenge value requires a different response. Suppose $z = m^{x'}$, with $x \neq x'$. If two pairs (a,b) and (a',b') yield the same challenge, then

$$m^{x'a} g^{xb} = m^{x'a'} g^{xb'}$$
$$m^{x'(a-a')} = g^{x(b'-b)}.$$

Assuming, by way of contradiction, that the same response is accepted for both pairs gives

$$m^{a} g^{b} = m^{a'} g^{b'}$$
$$m^{(a-a')} = g^{(b'-b)}.$$

But $x \neq x'$. Q.E.D.

Theorem 2: Even with infinite computing power S cannot with probability exceeding p^{-1} avoid detection of inconsistency between two invalid responses to a valid signature.

Proof: It suffices to show that, after a first invalid response, the ability of S to show consistency of the second invalid response contradicts Theorem 1. After the first invalid response, a, b, and m may in the worst case be assumed known to S. The consistency test $(r_1 g^{-b})^c = (r_2 g^{-d})^a$ can be written as $r_2 = (r_1^{1/a} g^{-b/a})^c g^d$. But since $r_1^{1/a} g^{-b/a}$ may be regarded as a known constant at this point, being able to satisfy this test implies an ability to establish the validity of an invalid signature. Q.E.D.

UNFORGEABILITY

Computing the private key from the public key is clearly no more difficult than breaking Diffie-Hellman key exchange. But an open question remains: Can the oracle for inverse roots provided by the signer help a forger? In view of the fact that minimum disclosure versions of these protocols are now known (and will appear in subsequent work), the example shown here is only proposed as a cryptosystem predicated on this open question being answered in the negative.

BLINDING

Of the two blinding techniques appearing in the literature, one of them, called blinding for "unanticipated" signatures [C], can be applied to the present protocols. The blinding party first chooses r independently and uniformly at random, forms the blinding factor g^r, and computes the signature of the blinding factor as $(g^x)^r$. To blind a message before it is signed, the message is multiplied by the blinding factor; unblinding entails multiplying by the multiplicative inverse of the signed form of the blinding factor. The challenge/response protocol requires V to show m to S, but V may blind m in the challenge and use the signed form of m and the blinding factor in verifying the response.

A previously unpublished blinding technique, which may be called "exponential" blinding, can also be used. A message is blinded by raising it to an independently and uniformly chosen random power; unblinding is by raising to the multiplicative inverse of the random power.

CONCLUSION

Undeniable signatures are better suited for many applications and are efficient.

ACKNOWLEDGEMENTS

It is a pleasure to thank Jan-Hendrik Evertse, Bert den Boer, and Gilles Brassard for their interest and comments.

REFERENCES

[BCC] Brassard, G., D. Chaum, and C. Crépeau, "Minimum disclosure proofs of knowledge," *Journal of Computer and System Sciences*, vol. 37, 1988, pp. 156–189.

[C] Chaum, D., "Blinding for unanticipated signatures," Advances in Cryptology—EUROCRYPT '87, D. Chaum & W.L. Price Eds., Springer Verlag, 1987, pp. 227–233.

[CE] Chaum, D. and J.-H. Evertse, "A secure and privacy-protecting protocol for transmitting personal information between organizations," Advances in Cryptology—CRYPTO '86, A.M. Odlyzko Ed., Springer Verlag, 1987, pp. 118–167.

[DH] Diffie, W. and M.E. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, Vol. IT-22, 1976, pp. 644–654.

[EG] ElGamal, T., "A public key cryptosystem and a signature scheme based on discrete logarithm," *IEEE Transactions on Information Theory*, vol. IT-31, 1985, pp. 469–472.

[PH] Pohlig, S. and M.E. Hellman, "An improved algorithm for computing logarithms over GF(p) and its cryptographic significance," *IEEE Transactions on Information Theory*, vol. IT-24, 1978, pp. 106–110.