How to improve signature schemes

Gilles BRASSARD †

Département IRO
Université de Montréal
C.P. 6128, Succursale "A"
Montréal (Québec)
CANADA H3C 3J7

ABSTRACT

Bellare and Micali have shown how to build strong signature schemes from the mere assumption that trapdoor permutation generators exist. Subsequently, Naor and Yung have shown how to weaken the assumption under which a strong signature scheme can be built: it is enough to start from permutations that are one-way rather than trapdoor. In this paper, which is independent from and orthogonal to the work of Naor and Yung, we weaken in a different way the assumption under which a strong signature scheme can be built: it is enough to start from what we call a weak signature scheme (defined below). Weak signature schemes are trapdoor in nature, but they need not be based on permutations. As an application, the Guillou–Quisquater–Simmons signature scheme (a variant on Williams' and Rabin's schemes, also defined below) can be used to build a strong signature scheme, whereas it is not clear that it gives rise directly to an efficient trapdoor (or even one-way) permutation generator.

1. Introduction

In a very nice paper [BM], Bellare and Micali have shown how to build a strong signature scheme from the mere assumption that trapdoor *permutation* generators exist (trapdoor *functions* are not shown to suffice, despite the title of [BM]). Here, "strong" means "non existentially forgeable under an adaptive chosen message attack". Refer to [GMR] for a precise definition of this concept. This was a significant improvement over [GMR], which needed the (possibly) stronger assumption that claw-free pairs exist in order to build strong signature schemes.

This result of Bellare and Micali can be extended in several directions. One such extension was worked out by Naor and Yung, who showed that it is enough to start from permutations that are one-way rather than trapdoor [NY].

† Supported in part by Canada NSERC grant A4107.

In this paper, which is independent from the work of Naor and Yung, we extend the result of Bellare and Micali in an orthogonal direction: in order to build strong signature schemes, it suffices to start with a signature scheme that is "randomly simulatable", but "non randomly forgeable under a key-only attack", which we shall refer to as a "weak signature scheme" (a precise definition is given in Section 2). This generalization is not achieved through a more clever construction, but rather through the observation that the original construction of Bellare and Micali works just as well under our weaker assumption. Following [GMR], a "key-only attack" is an attack in which the enemy knows only the legitimate signer's public key. A "random forgery" is the ability to forge a signature for a message selected at random, with non-negligible probability of success. (This is somewhere between existential and universal forgery, in the terminology of [GMR].) In contrast, the scheme is "randomly simulatable" if knowledge of the public key suffices to produce pairs (m, s) of signed messages whose probability distribution is the same as if message m had been chosen randomly and signature s had been provided by the legitimate signer. The difference between these notions is best grasped if one thinks of the RSA signature scheme [RSA], which is randomly simulatable and conjectured not to be randomly forgeable.

It is clear that a trapdoor permutation generator such as those used as building block in [BM] can be used to obtain a weak signature scheme, but the converse may not hold. In order to build a weak signature scheme from a trapdoor permutation generator, generate a pair (x, y) such that $E(x, \bullet)$ and $I(y, \bullet)$ are permutations that are inverses of each other (refer to [BM] for the notation, not needed for the remainder of this paper), and write down x in the public directory. In order to sign message m, use the secret information y to compute signature $s = I(y, m)$. In order to verify that signature s is valid for message m, use the public information x to verify that $E(x, s) = m$. Moreover, this signature scheme is randomly simulatable provided that knowledge of x is sufficient to draw randomly and uniformly in the domain of $E(x, \bullet)$.

Thus, it has been common practice since Diffie and Hellman [DH] to think of the signing process as computing a trapdoor permutation in the hard direction (the direction that requires knowledge of the trapdoor), whereas the verification process corresponds to computing the trapdoor permutation in the easy direction. However, this perspective is unnecessarily restrictive for the following reasons:

1) The public verification procedure is given both the message and its purported signature. In general, it could compute on both of them in order to decide whether the signature is valid — rather than computing on the signature alone and then using the message merely for the purpose of a final comparison. In fact, it would make perfect sense to have a signature scheme such that, given a signature, no one — perhaps not even the legitimate signer — could figure out which message is (or which messages are) actually signed by this signature, yet given a message and its signature, everyone could verify the validity of the signature.

2) A signature scheme could be secure even if some (or all) messages had more than one valid signature. In terms of trapdoor permutations, this would translate into allowing the function $E(x,\bullet)$ not to be one-one, thus the "function" $I(y,\bullet)$ would be multi-valued (hence not a function).

3) A signature scheme could be secure even if some (or all) signatures were valid for more than one message. In terms of trapdoor permutations, this would translate into allowing the function $I(y,\bullet)$ not to be one-one, thus the "function" $E(x,\bullet)$ would be multi-valued (hence not a function).

4) The space of messages and the space of signatures need not be the same, and they could even have different cardinalities (which is clearly not allowed in the trapdoor *permutation* setting). Moreover, the set of signatures could be different from one instance of a signature scheme to another even if the set of messages to be signed were the same. (As pointed out in [BM], a cross product construction due to Yao [Ya] can be used to bypass this difficulty. Nevertheless, from a practical point of view, it is preferable if Yao's construction can be avoided.)

After defining formally the notion of weak signature scheme in Section 2 and sketching how to transform any one of them into a strong signature scheme in Section 3, we conclude this paper in Section 4 with a discussion of a signature scheme due independently to Guillou and Quisquater [GQ] and to Simmons [S], which we shall refer to as the GQS signature scheme. This signature scheme is based on the scheme of Williams [Wi] — and thus also similar to Rabin's [Ra]. Notice that all these schemes, including the GQS scheme, are totally broken under a directed chosen-message attack. Nevertheless, the GQS signature scheme fits our definition of a weak signature scheme, hence it can be used directly to build a strong signature scheme. Transforming the GQS signature scheme into an efficient trapdoor (or even one-way) permutation generator, on the other hand, would be difficult because of problems (2), (3) and (4) above.

2. Definition of a weak signature scheme

Let X be a finite set. Denote by $ps[X]$ the set of functions f from X to the real interval $[0,1]$ such that $\sum_{x\in X} f(x)=1$. (Think of "$ps[X]$" as the set of all probability distributions over X.)

Let k be an integer parameter. Consider the set $M=\{0,1\}^k$ of length k messages, a set S of signatures (arbitrary for now), and two functions $sig: M \to ps[S]$ and $ver: M\times S \to \{true, false\}$ such that for all $m\in M$ and $s\in S$, $ver(m,s)=true$ if and only if $(sig(m))(s)>0$. Intuitively, this means that the verification function should accept s as a valid signature for m precisely when the probability that the signing process on m would produce s is nonzero. A *weak signature pair* (with parameter k) is a pair of (possibly probabilistic) efficient algorithms *SIG* and *VER* such that *VER*

computes the function *ver* and such that the probability that *SIG* on input m returns s is precisely $(sig(m))(s)$ for all m and s. Furthermore, we require that:

- *The signature scheme is non randomly forgeable under a key-only attack*: given a randomly chosen $m \in M$, knowledge of the algorithm *VER* does not enable one (in feasible time) to find even one $s \in S$ such that $ver(m,s) = true$ (except with negligible probability).
- *The signature scheme is randomly simulatable*: knowledge of the algorithm *VER* does enable one to come up efficiently with pairs (m,s) such that
  - $ver(m,s) = true$;
  - the marginal probability on the m thus generated is uniform on M ; and
  - no matter which m is generated, the conditional probability on s is given by $sig(m)$.

In other words, knowledge of VER does not enable one to forge signatures for randomly chosen messages, but enables one to forge pairs (m,s) that look just like what the legitimate signer would produce where she to choose a random message and sign it.

A *weak signature scheme* is a generator of weak signature pairs. More precisely, it is a probabilistic algorithm G that outputs such a pair on input 1^k. The description of algorithms *SIG* and *VER* produced by G must be of a length polynomially related to k. The set S may be different from pair to pair, but the set M must always be $\{0,1\}^k$. We require that every pair $<SIG, VER>$ thus generated be randomly simulatable. However, we only require that it be non randomly forgeable in a probabilistic and uniform sense: given any (possibly probabilistic) polynomial-time algorithm A, any polynomial p, and any sufficiently large integer k, the probability that $VER(m, A(k, VER, m)) = true$ is less than $1/p(k)$, where *VER* is obtained by a call on $G(1^k)$ and m is a random element of $\{0,1\}^k$. (The probabilities are taken over all random choices of G and A, and over the random choice of m.)

3. How to improve weak signature schemes

Assume the existence of a weak signature scheme. A strong signature scheme can be obtained with the techniques of Bellare and Micali [BM]. The only modification is that algorithms for trapdoor permutations are replaced by the *SIG* algorithms and, similarly, the inverse of the trapdoor permutations are replaced in the obvious way by the application of the *VER* algorithms. For the sake of completeness, here is a brief sketch of the construction of Bellare and Micali, adapted for our purpose.

Let k be an integer safety parameter and let l be the maximum length of the description of *VER* that can be produced by a call on $G(1^k)$. In order to set up a strong signature capability, each user obtains one weak signature pair $<SIG, VER>$ by a call on $G(1^k)$. The user also chooses $l+1$ pairs $(x_0, y_0), (x_1, y_1), \ldots, (x_l, y_l)$ of

elements drawn uniformly at random among $\{0,1\}^k$. These $l+1$ pairs are made public, together with the description of algorithm VER. In order to sign a first bit b, the user exhibits $SIG(x_0)$ if $b=0$ or $SIG(y_0)$ if $b=1$. Furthermore, the user calls $G(1^k)$ again, thus producing a new pair $<SIG_1, VER_1>$. The pairs $(x_1, y_1), \ldots, (x_l, y_l)$ are used to sign the description of VER_1 bit-by-bit, much the same way that (x_0, y_0) had been used to sign bit b. At this point, a second bit can be signed by producing either $SIG_1(x_0)$ or $SIG_1(y_0)$, depending on the value of the bit to be signed. This process is continued in order to sign an arbitrary (polynomial in k) number of bits.

The process by which such a signature can be verified should be clear. The reader is referred to [BM] for more detail, in particular for the various ways in which more than one message can be signed. The proof that this scheme is non existentially forgeable under an adaptive chosen message attack [GMR] (assuming that the underlying signature scheme is weakly secure) follows the lines of the proof given in [BM] and is not repeated here.

4. The GQS signature scheme and how to use it

Our main motivation for this work was to be able to use a simple, elegant and natural variant on Williams' signature scheme as basis for the construction of Bellare and Micali [BM]. This work was necessary since this signature scheme does not yield a trapdoor permutation generator, because of difficulties (2) and (3) mentioned in Section 1, and because the removal of difficulty (4) through Yao's construction would be expensive in practice

Williams' key observation [Wi] is that if $n=pq$ where p and q are primes congruent to 3 and 7 modulo 8, respectively, then -1 is a quadratic non-residue modulo n with Jacobi symbol $+1$, whereas 2 has Jacobi symbol -1. Such an integer is called a Williams' integer. In his paper, Williams uses this property to remove a difficulty found in Rabin's previously proposed scheme [Ra]: without using the secret factorization of n, Williams transforms any element of $\mathbb{Z}_n^*$ between 1 and $n/8$ (or "any odd number between 1 and $n/4$" [Wi]) into an element of $\mathbb{Z}_n^*$ that can be signed directly and deterministically (with knowledge of the factors of n) by a scheme as hard to break as it is to factor n (under a key-only attack). (Recall that $\mathbb{Z}_n$ denotes the set of integers modulo n, whereas $\mathbb{Z}_n^*$ denotes the subset of $\mathbb{Z}_n$ consisting of those integers relatively prime with n. For simplicity, we confuse a residue class with its smallest non-negative representative, so that it makes sense to talk about an odd element of $\mathbb{Z}_n^*$.)

In the opinion of the current author, Williams' observation could have been used in a much simpler way: if n is of the form proposed by Williams and if $x \in \mathbb{Z}_n^*$, then exactly one among $\{x, -x, 2x, -2x\}$ (modulo n) is a quadratic residue, and whichever it is can be signed by providing one of its square roots modulo n. This idea was discovered independently by Guillou and Quisquater [GQ] and by Simmons [S]

(see also [SP]). (In a personal communication, Quisquater has given credit to Goldwasser for the observation that there exists exactly one quadratic residue among $\{x, -x, 2x, -2x\}$ modulo a Williams' integer.) We refer to the resulting scheme and its immediate variants as the Guillou–Quisquater–Simmons (or GQS) signature scheme. We now describe in more detail a version of this scheme that is well suited for our purpose.

Let k be an integer parameter. In order to build a weak signature pair, randomly choose two distinct primes p and q of binary length $1+\lfloor k/2 \rfloor$ and $1+\lceil k/2 \rceil$, respectively, such that $p \equiv 3 \pmod 8$ and $q \equiv 7 \pmod 8$. Compute $n = pq$. Note that $2^k < n < 4 \times 2^k$. For any $x \in \mathbb{Z}_n^*$, let $\sqrt{x}$ denote the (possibly empty) set $\{y \in \mathbb{Z}_n^* \mid x \equiv y^2 \pmod n\}$, and let $car(x)$ stand for the unique element of $\{x, -x, 2x, -2x\}$ (modulo n) that is a quadratic residue. If X is a non-empty finite set, let $unif(X)$ denote an element of X chosen randomly with uniform distribution.

The weak signature pair corresponding to n is defined by the following algorithms, where $M = \{0,1\}^k$ will be confused with the set of integers between 0 and $2^k - 1$, and $S = \mathbb{Z}_n$:

- $SIG(m) = \begin{cases} m & \text{if } \gcd(m,n) \neq 1 \\ unif(\sqrt{car(m)}) & \text{otherwise,} \end{cases}$

- $VER(m,s) = \begin{cases} true & \text{if } \gcd(m,n) \neq 1 \text{ and } m = s \\ true & \text{if } \gcd(m,n) = 1 \text{ and } s^2 \in \{m, -m, 2m, -2m\} \pmod n \\ false & \text{otherwise.} \end{cases}$

The signing process is well-defined because $n > 2^k$, hence $M \subseteq \mathbb{Z}_n$. The reader can verify that all the desired properties of a weak signature scheme are fulfilled under the conjecture that factoring Williams' integers is hard. (It is easy to see that it is non randomly forgeable under a key-only attack assuming the factoring conjecture; it is a bit more subtle to show that it is randomly simulatable — and the fact that $n \in O(2^k)$ is important here.) Therefore, this weak signature scheme can serve as basis for the construction of Bellare and Micali in order to obtain a strong signature scheme.

It should be pointed out that the version of the GQS signature scheme described above should *not* be used directly. Not only is it totally breakable under a chosen message attack, but it could even be broken under a known message attack [GMR] if the same message is ever signed twice by the legitimate signer! For this reason, Simmons [S] suggests that only one of the four elements of $\sqrt{car(m)}$ should be returned for any given m (for instance, we suggest that it be the one that is simultaneously odd and whose Jacobi symbol is +1 — this defines a unique signature because both prime factors of n are congruent to 3 modulo 4). Nevertheless, this safeguard is not necessary if the basic scheme is used only as building block in the construction of Bellare and Micali in order to obtain a strong signature scheme.

ACKNOWLEDGEMENTS

The author is very grateful to Gus Simmons, who presented this paper on his behalf at EUROCRYPT '89 when his newborn daughter Alice was too young for him to travel.

BIBLIOGRAPHY

[BM] Bellare, M. and Micali, M., "How to sign given any trapdoor function", *Proceedings of the 20th ACM Symposium on Theory of Computing*, 1988, pp. 32–42. (Also presented at *CRYPTO '88*.)

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

[GMR] Goldwasser, S., Micali, S. and Rivest, R. L., "A digital signature scheme secure against adaptive chosen-message attacks", *SIAM Journal on Computing*, vol. 17, no. 2, April 1988, pp. 281–308.

[GQ] Guillou, L. and Quisquater, J.–J., "Efficient digital public-key signatures with shadow", *Advances in Cryptology — CRYPTO '87 Proceedings*, Springer-Verlag, 1988, p. 223.

[NY] Naor, M. and Yung, M., "Universal one-way hash functions and their cryptographic applications", *Proceedings of the 21st ACM Symposium on Theory of Computing*, 1989, pp. 33–43.

[Ra] Rabin, M. O., "Digital signatures and public-key functions as intractable as factorization", Technical Report MIT/LCS/TR-212, M.I.T., 1979.

[RSA] Rivest, R. L., Shamir, A. and Adleman, L. M., "A method for obtaining digital signatures and public-key cryptosystems", *Communications of the ACM*, vol. 21, 1978, pp. 120–126.

[S] Simmons, G. J., "A protocol to provide verifiable proof of identity and unforgeable transaction receipts", *IEEE Journal on Selected Areas of Communications*, vol. 7, no. 4, May 1989, pp. 435–447.

[SP] Simmons, G. J. and Purdy, G. B., "Zero-knowledge proofs of identity and veracity of transactions receipts", *Advances in Cryptology — EUROCRYPT '88 Proceedings*, Springer-Verlag, 1988, pp. 35–49.

[Wi] Williams, H. C., "A modification of the RSA public-key encryption procedure", *IEEE Transactions on Information Theory*, vol. IT-26, 1980, pp. 726–729.

[Ya] Yao, A. C.-C., "Theory and applications of trapdoor functions", *Proceedings of the 23rd IEEE Symposium on Foundations of Computer Science*, 1982, pp. 80–91.