On the Rabin signature

Michele Elia; \footnote{Politecnico di Torino, Italy} Davide Schipani \footnote{University of Zurich, Switzerland}  

November 26, 2011

Abstract

Some classical Rabin signature schemes are exposed to forgery attacks. We propose some variants to counter this weakness.

Keywords: Rabin signature, Rabin cryptosystem.

Mathematics Subject Classification (2010): 94A60, 11T71, 14G50

1 Introduction

In [1] the Rabin scheme was revisited, considering its use both as a cryptosystem for the exchange of secret messages and as a signature. In particular, a new variant of the classical Rabin signature (cf. [3]) was proposed using a deterministic padding mechanism. This Rabin signature is briefly described in the following.

Suppose all operations are done in $\mathbb{Z}_N$, the residue ring modulo $N$, which is a product of two primes $p$ and $q$ known only by the signer. The signature of a message $m$ is a triple $(m, U, S)$, where $U$ is a pad (found either randomly or deterministically as in [1]) such that the equation $x^2 = mU$ is solvable, and $S$ is one of its solutions. Verification is performed by comparing $mU$ with $S^2$.

This simple scheme is plainly vulnerable to forgery attacks: it is immediate to compute $S^2$, choose any message $m'$, compute $U' = S^2 m'^{-1}$, and forge the signature as $(m', U', S)$ without knowing the factorization of $N$. In some variants $S$ is a solution of $x^2 = H(mU)$, with $H$ a hash function, but this does not help against the above forgery attack.

However, another signature, which also relies on the difficulty of finding square roots, the Rabin-Williams signature (cf. [2, 4]), avoids the forgery vulnerability: the signature is a four-tuple $[m, e, f, S]$, where $e \in \{1, -1\}$ and $f \in \{1, 2\}$ are chosen to make the equation $efS^2 = m$ solvable; the scheme is limited to pair of primes, where one is congruent 3 and the other 7 modulo 8.

The non-forgeability is based on the limited set of multipliers $e$ and $f$. However, the Rabin-Williams scheme requires the use of two primes respectively congruent 3 and 7 modulo 8, while the above scheme works with every pair of primes.
We show here that it is possible to devise a Rabin signature that avoids forgery and works for every pair of primes. We consider that a valid signature of a message \( m \) cannot be forged if it does not allow us to derive a valid signature for another given message \( m' \) without knowing the factorization of \( N \).

## 2 Schemes

### 2.1 A general scheme

Every signer determines a set of four padding factors \( \mathcal{U} \) which is made public. The set \( \mathcal{U} \) has the property that, for any given \( m \in \mathbb{Z}_N^* \), there exists a multiplier \( u \in \mathcal{U} \) that makes the equation \( x^2 = um \) solvable. In fact, it is sufficient to find 4 numbers \( a_1, a_2, b_1, b_2 \), such that

\[
\left( \frac{a_1}{p} \right) = 1, \quad \left( \frac{a_2}{p} \right) = -1, \quad \left( \frac{b_1}{q} \right) = 1 \quad \text{and} \quad \left( \frac{b_2}{q} \right) = -1,
\]

and form the set

\[
\mathcal{U} = \{ r_1^2(a_1 \psi_1 + b_1 \psi_2), r_2^2(a_1 \psi_1 + b_2 \psi_2), r_3^2(a_2 \psi_1 + b_1 \psi_2), r_4^2(a_2 \psi_1 + b_2 \psi_2) \},
\]

where \( r_1, r_2, r_3, \) and \( r_4 \) are four random different numbers in \( \mathbb{Z}_N^* \) (to prevent an easy factorization of \( N \)), and \( \psi_1 \) and \( \psi_2 \) are the constants determined by the Chinese Remainder Theorem as in [1]: by the generalized Euclidean algorithm, two integer numbers, \( \lambda_1, \lambda_2 \in \mathbb{Z} \), such that \( \lambda_1 p + \lambda_2 q = 1 \), are computed; thus, setting \( \psi_1 = \lambda_2 q \) and \( \psi_2 = \lambda_1 p \), we have the following properties:

\[
\begin{align*}
\psi_1 + \psi_2 &= 1 \\
\psi_1 \psi_2 &= 0 \mod N \\
\psi_1^2 &= \psi_1 \mod N \\
\psi_2^2 &= \psi_2 \mod N \\
\psi_1 &= 1 \mod p, \quad \psi_1 = 0 \mod q \\
\psi_2 &= 0 \mod p, \quad \psi_2 = 1 \mod q
\end{align*}
\]

(1)

Given the properties above, by writing \( m \) as \( m_1 \psi_1 + m_2 \psi_2 \), one can easily find the suitable padding factor \( u \in \mathcal{U} \) such that the conditions \( \left( \frac{um}{p} \right) = \left( \frac{um}{q} \right) = 1 \) are satisfied. Specifically the signer chooses \( a_i \) and \( b_i \) so that \( \left( \frac{a_i}{p} \right) = \left( \frac{m_1}{p} \right) \) and \( \left( \frac{b_i}{q} \right) = \left( \frac{m_2}{q} \right) \).

The following signature is forgery resistant, thanks to the small number of possible padding factors.

**Public-key:** \( N \) and the finite set \( \mathcal{U} \)

**Signed message:** \([m, u, S]\), where \( u \) is the padding factor in \( \mathcal{U} \) which makes the equation \( x^2 = mu \) solvable, and \( S \) is any solution of this equation.

**Verification:** Check that \( u \) belongs to \( \mathcal{U} \); compute \( mu \) and \( S^2 \); the signature is valid if and only if these two numbers are equal.

The verification cost is two squares and two products.
2.2  Blum primes

If the Rabin scheme is restricted to Blum primes, then it is possible to avoid the use of the set of multipliers \( U \) in at least two ways.

In Variant I, the cost to pay is a further parameter in the signature, which consists of a four-tuple \([m, U, S, T]\).

The padding parameter \( U \) can be chosen deterministically as in [1] as \( U = R^2 \left[ f_1 \psi_1 + f_2 \psi_2 \right] \), where \( R \) is a random number, \( f_1 = \left( \frac{m_1}{p} \right) \) and \( f_2 = \left( \frac{m_2}{q} \right) \). In fact, writing \( m = m_1 \psi_1 + m_2 \psi_2 \), the equation

\[
x^2 = (m_1 \psi_1 + m_2 \psi_2)(f_1 \psi_1 + f_2 \psi_2) = m_1 f_1 \psi_1 + m_2 f_2 \psi_2
\]

is always solvable modulo \( N \), because \( m_1 f_1 \) and \( m_2 f_2 \) are clearly quadratic residues modulo \( p \) and modulo \( q \), respectively, since \( \left( \frac{m_1}{p} \right) = \left( \frac{f_1}{p} \right) \), \( \left( \frac{m_2}{q} \right) = \left( \frac{f_2}{q} \right) \), so that

\[
\left( \frac{m_1 f_1}{p} \right) = \left( \frac{m_1}{p} \right) \left( \frac{f_1}{p} \right) = 1, \quad \left( \frac{m_2 f_2}{q} \right) = \left( \frac{m_2}{q} \right) \left( \frac{f_2}{q} \right) = 1.
\]

Then \( S \) is chosen among the roots of the equation \( x^2 = mU \) with the further constraint that the equation \( y^2 = (U + 1)S \) is solvable. This is always possible because in the case of Blum primes the four roots of a quadratic equation form a set \( \Omega \) of padding factors as above. Lastly, \( T \) is a root of \( y^2 = (U + 1)S \).

In Variant II, the padding factor is a square root of unity, but is not a public element of the signature. In this case a triple will be sufficient to define a signature that is resistant to forgery.

Variant I.

Public-key: \( N \)

Signed message: \([m, U, S, T]\), where \( U \) is a padding factor which makes the equation \( x^2 = mU \) solvable, and \( S \) is a root of this equation such that the equation \( y^2 = (U + 1)S \) is solvable, then \( T \) is any root of this equation.

Verification: Check whether \( T^2 = (U + 1)S \), then check whether \( S^2 = mU \); the signature is valid if and only if both equalities hold.

 Forgery is not possible because given \( m' \) and computing \( U' = S^2/m' \), the second equation to be verified would be

\[
(U' + 1)S = T^2 = (U + 1)S,
\]

which is true if and only if \( U = U' \), that is if and only if \( m' = m \).

In this case the verification cost is two squares and two products.

Note that, if \( U \) is chosen deterministically as above, it is possible to make different signatures of the same message. Clearly, \( U \) should not be \( \psi_1 - \psi_2 \) or \(-\psi_1 + \psi_2 \), because these square roots of unity would unveil the factorization of \( N \); in fact adding 1 to either of them gives a multiple of \( p \) or a multiple of \( q \).
Variant II.

Public-key: $N$

Signed message: $[m, F, R^3]$, where $R$ is a secret random number, $S$ is a root of the equation $x^2 = mU$, where the padding factor $U$ is chosen as $U = \left( \frac{m}{p} \right) \psi_1 + \left( \frac{m}{q} \right) \psi_2$ and $F = RS$.

Verification: Compute $R^{12}m^6$ and $F^{12}$; the signature is valid if and only if these two numbers are equal.

The algorithm works because $U^2 = 1$, thus $F^4 = R^4m^2$.

Forgery is not possible because, given $m_1$ and $F_1$, only a number $K$ such that $Km_1^6 = F_1^{12}$ can be found, but not a fourth root of it. Note that using $R^2$ in the signature instead of $R^3$ would expose $U$, which would unveil the factorization of $N$ if $U$ is not $\pm 1$, but one of the other two roots of unity.

In this case the verification cost is seven squares and three products.

Here it is possible to make different signatures of the same message by choosing different random numbers $R$.

3 Acknowledgments

The research was supported in part by the Swiss National Science Foundation under grant No. 132256.

References


