

Blind Unanticipated RSA-Signature Schemes

Ildar M. Khamitov

Alkorsoft & Bank Tavrichesky

khamitov@paycash.ru

Andrey G. Moshonkin

Alkorsoft

agm@paycash.ru

Alexander L. Smirnov

Alkorsoft & Steklov Mathematical Institute

smirnov@paycash.ru

(contact author)

In the present paper we describe two blind unanticipated RSA-signature schemes. Each of these schemes admits a potentially unlimited number of kinds of signatures, does not need additional data growing with the number of kinds of signatures, and makes it possible to quickly obtain a blind signature at comparatively small resources.

Keywords: blind signature, RSA, Chaum scheme

1. Introduction

The concept of blind signature invented by D. Chaum [1] is of importance in providing privacy for the users of electronic service systems and, in particular for the users of payment systems.

In the general blind signature scheme a user presents the blinded form $M' = B(M, R)$ of the initial message M to the signer, where R is a randomized blinding key chosen by the user and B is a blinding function. In what follows M' is also called the blinded message. The signer returns the message S' to be unblinded to the user, and the user computes the signature S on the initial message M using an unblinding function U which takes S' and R as an input. In the schemes considered in the present paper S' is a signer's signature on M' . The first concrete realizations of the blind signature scheme are also suggested by D. Chaum [2, 3]. For other blind signature schemes see [4].

The Chaum schemes are extensions of the RSA scheme, i.e., S is an RSA-signature on M . This means that $S^E = M \pmod{N}$, where E is an exponent and N is the module of the public key to which the signature S corresponds. A detailed information concerning the RSA-signature scheme can be found in [4, 5]. In the present paper we deal only with the RSA-signature scheme. In the sequel we assume that the signer generates N as the product of two primes, P and Q , though in some cases N could have more prime factors.

In the Chaum blind signature scheme [2], which is unconditionally untraceable, the blinding and unblinding functions are given by the following formulas:

$$B(M, R) = R^E M \pmod{N}, \quad U(S', R) = R^{-1} S' \pmod{N}.$$

In some applications it is desirable to have several admissible kinds of signatures. Moreover, it is desirable that the kind of signature obtained by a user be determined after blinding. For example, in a payment system the kind of signature can be determined by the denomination of the digital token which is issued by a bank on customer's demand. This denomination can depend on the solvency of the customer's account or on the rate of exchange whose precise values might be unknown to the customer at the moment of the demand formation. In a timestamping system the kind of signature may depend on the time of the notary receiving the message; this time is also unknown when the message is created. In [3] the schemes in which the kind of signature is determined after blinding are called blind unanticipated signature schemes.

In the sequel we assume that the module N is fixed and that the kind of signature is determined by the public exponent. The Chaum blind signature [2] is not unanticipated one since the blinding function B depends on the public exponent E .

In the Chaum unanticipated blind signature scheme [3] the blinding and unblinding functions are defined by the formulas

$$B(M, R) = M \cdot g_1^{k_1} \cdot \dots \cdot g_u^{k_u} \pmod{N}, \quad U(i, S', R) = S' \cdot S_{1,i}^{-k_1} \cdot \dots \cdot S_{u,i}^{-k_u} \pmod{N}.$$

In these formulas (g_1, \dots, g_u) is a set of "generators", $R = (k_1, \dots, k_u)$, and $S_{i,j}$ is the signature on the generator g_j , corresponding to the public exponent E_i . The generators g_j and the signatures $S_{i,j}$ are published beforehand by the signer. A certain disadvantage of this method is that the set of data published increases with increase in the number of possible kinds of signatures; this fact potentially restricts the number of possible kinds of signatures. Furthermore, the untraceability in this scheme is ensured by special properties of the generators. A trusted representative of all users can ascertain that these properties hold by participating in the cut-and-choose protocol before publication. The disadvantage of this approach is that these properties cannot be checked by an individual user at a later moment of time and he is forced to trust the third party.

In the present paper we describe two blind unanticipated RSA-signature schemes denoted below as schemes 1 and 2. Each of these schemes admits a potentially unlimited number of kinds of signatures, does not need additional data growing with the number of kinds of signatures, and makes it possible to quickly obtain a blind signature at comparatively small resources.

In scheme 1 the blinding function is based on modular raising to a power. The advantage of scheme 1 is that the variety of admissible kinds of signatures is much wider than in the Chaum blind unanticipated signature scheme and in scheme 2 as well. Furthermore, version B of scheme 1 has the advantage over the Chaum blind unanticipated signature scheme that the properties of data ensuring the untraceability can be checked by an individual user (the signer can

convince him of that) at an arbitrary moment of time. In scheme 2, as in the Chaum blind signature scheme, the blinding function is based on modular multiplication. As the Chaum blind signature scheme, scheme 2 is unconditionally untraceable.

2. Scheme 1

In this scheme the blinding and unblinding functions are defined as follows:

$$B(M, R) \equiv M^R \pmod{N}, \quad U(S', R) \equiv (S')^A M^B \pmod{N},$$

where R is a randomized blinding key, E is the public exponent, and the integers A and B satisfy the relation $AR + BE = 1$. Such A and B can be found by the Euclidean algorithm.

The unblinding function can be calculated if $\text{GCD}(R, E) = 1$. This property is ensured by a user when choosing a specific blinding key R . To make this choice possible a set of admissible public exponents should be fixed in advance. For example, the set of admissible public exponents can be defined as the set of all products of basic public exponents E_1, \dots, E_k raised to arbitrary natural powers.

The blinding function $B(M, R)$ does not provide the untraceability of the signature since, e.g., there are the following two methods of linking the blinded message M' with the message M presented later.

Method 1. Let us assume that the message M turned out to be the L th power modulo P , where L divides $P - 1$, then the blinded message M' will also be the L th power modulo P . Thus, the signer gets linking information about the users who have obtained the signatures on messages that turned out to be the L th powers.

Method 2. Let $L = \text{GCD}(P - 1, Q - 1)$. There exist two independent homomorphisms $f, g : (\mathbf{Z}/N\mathbf{Z})^* \rightarrow \mathbf{Z}/L$, where f is the composition of the projection onto the group $(\mathbf{Z}/P\mathbf{Z})^*$ and the L th power residue symbol, which is defined on this group and takes values in the group of L th roots of 1 (which is identified with \mathbf{Z}/L). The homomorphism g is similarly defined with replacement of P by Q . We have $f(M')/g(M') = f(M)/g(M)$, which gives the linking information to the signer.

To ensure the untraceability in scheme 1, in particular, in order for the above-mentioned methods do not lead to linking, some steps should be taken. These steps are that the blinding key R is taken to be a multiple of the masking factor G whose properties are described below (conditions I and II). If R is divisible by G , then the blinded message belongs to the group

$$Z(G) = \{a^G \mid a \in (\mathbf{Z}/N\mathbf{Z})^*\}.$$

To evaluate the untraceability we use the quantity W called the blinding level and defined to be the probability that for a random variable X uniformly distributed in $(\mathbf{Z}/N\mathbf{Z})^*$ and for

independent random variables Y_1 and Y_2 uniformly distributed in $Z(G)$, the probability that Y_1 is obtained by blinding X coincides with the probability that Y_2 is obtained by blinding X .

If $W \approx 1$, then practically any blinded message can (with equal probability) correspond to practically any initial message. This implies almost complete untraceability of the signature. If, e.g., $W \approx 1/3$, then for a large number of initial messages, the signer, in general, can link the individual initial message with one of three sets of blinded messages. In each set all correspondences between the initial messages and blinded messages will be equiprobable. To what extent this level of untraceability is acceptable depends on a specific practical problem.

To ensure the untraceability, we take a masking factor G that is prime to any admissible public exponent and satisfies the following conditions:

- (I) G is divisible by $\text{GCD}(P - 1, Q - 1)$;
- (II) G is divisible by all $D < U$ such that D divides either $P - 1$ or $Q - 1$, where U is an appropriate bound.

Under assumption that the masking factor G satisfies conditions (I) and (II) we have the following estimate: $W > (1 - \text{Log}(N)/[U \cdot \text{Log}(U + 1)])^2$. This estimate is supported by the fact that $W \geq (1 - W_1)^2$, where W_1 is the probability that the set of all blinded forms of a random variable X uniformly distributed in $(\mathbf{Z}/N\mathbf{Z})^*$ (i.e., the set of invertible residues of the form $X^R \pmod{N}$, where R runs through the integers divisible by G) coincides with the group $Z(G)$. Furthermore, $W_1 \leq 1 - \prod(1 - L^{-1})$, where the product is taken over all primes L that divide $(P - 1) \cdot (Q - 1)$ and are greater than U . It can easily be shown that $W_1 < \text{Log}(N)/[U \cdot \text{Log}(U + 1)]$. For example, if the module N is of 1024 bits and $U = 10^8$, then $W > 1 - 4 \cdot 10^{-7}$.

In the versions A and B of scheme 1 the masking factor G satisfying conditions (I) and (II) is chosen differently.

Version A. In this case $G = 2$, and P and Q satisfy the conditions

- (A1) $P - 1$ does not have divisors D such that $2 < D < U$;
- (A2) $Q - 1$ does not have divisors D such that $2 < D < U$;
- (A3) $\text{GCD}(P - 1, Q - 1) = 2$.

The signer can use the cut-and-choose protocol to convince the users that the secret factors have the above properties.

Version B. In this case G is equal to the greatest divisor of $N - 1$ prime to each admissible public exponent, and

- (B1) N is a product of exactly two primes, say P and Q ;
- (B2) $P - 1$ does not have divisors D such that $2 < D < U$;
- (B3) $Q - 1$ does not have divisors D such that $2 < D < U$.

Note that in this version conditions (I) and (II) are fulfilled. Condition (I) follows from the fact that $\text{GCD}(P - 1, Q - 1)$ divides $N - 1$ (since $N - 1 = P(Q - 1) + (P - 1)$). Therefore, the fact that G is equal to the greatest divisor of $N - 1$ prime to each admissible public exponent and condition B1 imply that G is divisible by $\text{GCD}(P - 1, Q - 1)$, hence condition (I).

In version B, the properties of N , P , and Q can be tested by a user with the help of the signer as follows.

The test of condition (B1)

The signer publishes a pair (U, V) of residues such that the set $\{1, U, V, UV\}$ is a system of representatives for the group $(\mathbf{Z}/N\mathbf{Z})^*/\mathbf{Z}(2)$. After that an individual user presents a random challenge X to the signer, which responds with a Y such that $X \cdot Y^2 \pmod{N} \in \{1, U, V, UV\}$. In determining Y the signer must use such a procedure that prevents challengers from calculating essentially different square roots of a residue modulo N . Every such independent challenge reduces the probability that N is a product of more than two factors at least by half. To provide security for the signer, one can require that X be either prime that does not exceed a given bound, or be the image of some cryptographic hash-function of the number chosen by the user.

Moreover, if right responses to such challenges are received for all prime X less than a certain explicit bound T , then the user can be sure that N is a prime or a product of two primes. Indeed, if N is a product of at least three primes and for each odd prime $X < T$ there is a Y such that $X \cdot Y^2 \pmod{N}$ belongs to $\{1, U, V, UV\}$, then under the generalized Riemann hypothesis, which although is not proved mathematically but is tested experimentally to a great extent, we have $T < C[\text{Log}(N)]^2$, where the value of C can be calculated using the well-known estimates [7]. In particular, it is sufficient to take $C = 70$, and this estimate can be improved considerably if necessary.

The test of conditions (B2) and (B3)

It is sufficient to verify that $P - 1$ and $Q - 1$ are not divisible by L for any integer $L < U$, where L is either odd prime or $L = 4$. In the case of odd L , a user presents a challenge R to the signer who responds with $R^{1/L} \pmod{N}$. Every right response reduces the probability that $P - 1$ or $Q - 1$ is divisible by L in L times. To provide security for the signer, one can require that R be either sufficiently small or be the image of some cryptographic hash-function of the number chosen by the user.

Moreover, if right responses to such challenges are received for all prime R less than a certain explicit bound T , then the user can be sure that $P - 1$ and $Q - 1$ do not have odd prime divisors $L < U$. Indeed, if N is divisible by an odd prime P , $P - 1$ is divisible by an odd prime L , and for any $R < T$, there is a residue A such that $A^L \equiv R \pmod{N}$, then under the generalized Riemann hypothesis we have $T < D(\text{Log } N)^2$. An explicit value of D can be calculated using the well-known estimates [7]. In particular, it is sufficient to take $D = 70$, and this estimate can be improved if necessary.

Instead of checking that $P - 1$ and $Q - 1$ are not divisible by L for every particular L , it is sufficient to check this property for a set of numbers A_1, \dots, A_s such that any prime less than a given bound divides at least one of A_i .

There is the following way of verifying that $P - 1$ and $Q - 1$ are not divisible by $L=4$. First, after checking that $P - 1$ and $Q - 1$ are not divisible by 3, the user is sure that (-3) is not a square modulo P and modulo Q . Secondly, the signer convinces the user that 3 is a square modulo P and modulo Q by producing an integer R such that $R^2 \equiv 3 \pmod{N}$. Thus, a user convinces himself that the integer (-1) is a square neither modulo P nor modulo Q , and therefore $P - 1$ and $Q - 1$ are not divisible by 4.

Furthermore, knowing that $P - 1$ and $Q - 1$ are not divisible by 4, the user can verify that $P - 1$ and $Q - 1$ are not divisible by an odd prime L by checking that X is a square neither modulo P nor modulo Q , where $X = L$ if $L \equiv 1 \pmod{4}$ and $X = -L$ if $L \equiv 3 \pmod{4}$. The signer convinces the user of that by producing an integer R such that $R^2 \equiv -X \pmod{N}$. Such a verification is possible approximately for a half of odd L 's.

3. Scheme 2

In this scheme admissible public exponents have the form $E = E_1^{K_1} \cdot \dots \cdot E_k^{K_k}$, where K_1, \dots, K_k are nonnegative integers such that $K_i \leq L_i$ for $i = 1, \dots, k$. The limiting multiplicities L_1, \dots, L_k of the fixed basic public exponents E_1, \dots, E_k are either chosen by a user before applying the blinding function or fixed beforehand. The blinding and unblinding functions are given by the following formulas:

$$B(M, R) = R^U \cdot M \pmod{N}, \text{ where } U = E_1^{L_1} \cdot \dots \cdot E_k^{L_k},$$

$$U(S', R) = S' \cdot R^{-V} \pmod{N}, \text{ where } V = E_1^{L_1 - K_1} \cdot \dots \cdot E_k^{L_k - K_k}.$$

Here the multiplicities K_1, \dots, K_k are chosen by the signer, and V is determined by these multiplicities.

The degree of unanticipatability in this scheme, i.e., the number of admissible kinds of signatures, is determined by the number k of basic public exponents and by the limiting multiplicities. For example, if $k = 3$ and all limiting multiplicities are equal to 1000, then the number of admissible kinds of signatures is equal to 10^9 .

4. Additional remarks

Needless to say that various modifications of the schemes described above are possible. For example, in scheme 1 one can take P , Q , and G so that the masking factor G is either not divisible by $\text{GCD}(P - 1, Q - 1)$ or not divisible by divisors of $P - 1$ and $Q - 1$ that are less than a given bound. For example, one can choose $G = 1$. Although this choice do not allow one to make the blinding level arbitrarily close to 1, nevertheless, in some practical situations the untraceability achieved in this way may be acceptable.

References

- [1] D. Chaum, Blind signatures for untraceable payments, *Advanced in Cryptology—Proceedings of Crypto 82*, 1983, p. 199–203.
- [2] D. Chaum, Blind Signature Systems, U.S. Patent 4,759,063, 19 Jul 1988.
- [3] D. Chaum, Blind Unanticipated Signature Systems, U.S. Patent 4,759,064, 19 Jul 1988.
- [4] D. Pointcheval, J. Stern, Provably Secure Blind Signature, *Lectures Notes in Computer Science*, 1163, 1996, Springer, p. 252–265.

- [5] B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, John Wiley&Sons, New York, 2nd edition, 1996.
- [6] A. J. Menezes, P. C. Van Oorshot, S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1996.
- [7] J. Oesterle, Versions effectives du theoreme de Chebotarev sous l'hypothese de Riemann generalisee, *Soc. Math. De France, Asterisque* 61, 1979, p. 165–167.