A Simple and Secure Way to Show the Validity of Your Public Key.

Jeroen van de Graaf
Centrum voor Wiskunde en Informatica
Amsterdam

René Peralta
Facultad de Matemáticas
Universidad Católica de Chile

ABSTRACT

We present a protocol for convincing an opponent that an integer N is of the form P^rQ^s, with P and Q primes congruent to 3 modulo 4 and with r and s odd. Our protocol is provably secure in the sense that it does not reveal the factors of N. The protocol is very fast and therefore can be used in practice.

1. Introduction.

Many protocols in the literature assume that the parties involved have previously agreed that their respective public keys are Blum integers. That is, composites of the form $N = P^rQ^s$, with P and Q primes congruent to 3 modulo 4 and with r and s odd. This agreement must of course be achieved through a protocol which does not compromise the secrecy of the keys.

Blum integers are characterized by the following three conditions:

i) $N \equiv 1 \bmod 4$.

ii) There exists a quadratic residue modulo N with square roots with opposite Jacobi symbol.

iii) N has at most two prime factors.

C. Pomerance (Ed.): Advances in Cryptology - CRYPTO '87, LNCS 293, pp. 128-134, 1988.

There is no known efficient algorithm to verify conditions ii) and iii). Interactive protocols are used for this purpose: A convinces B that ii) and iii) hold. The protocol for verifying condition ii), due to Manuel Blum [Blum82], requires the interchange of roughly 100 integers modulo N, and thus is very fast. The bottleneck in the published protocols (see [BKP85] [GHY85]) is in showing that N has exactly two distinct prime factors. The protocols are based on an observation due to Adleman. He suggested using the fact that if N has exactly two prime factors then 1/4 of the elements of $\mathbf{Z}_N{}^*$ are quadratic residues. If N has more than two prime factors then at most 1/8 of the elements of $\mathbf{Z}_N{}^*$ are quadratic residues. Thus, a binomial experiment can be used to distinguish between the two cases. Ommiting details, the standard solution is to jointly generate M random numbers in $\mathbf{Z}_N{}^*$ with Jacobi symbol +1 and have the owner of the public key N produce square roots modulo N for approximately half of the numbers. In [BKP85] it is shown that the error probability is minimized by having the prover show square roots for a fraction $(\sqrt{21} - 1)/20$ of the M numbers, giving a probability of error asymptotically bounded by $e^{-(M/75)}$ above and $e^{-(M/74)}$ below. Thus M must be in the thousands in order to achieve truly negligible probability of error. An additional undesirable property of this solution is that the error is two-sided. It is possible that A may fail to convince B that N has exactly two prime factors when in fact it does, and it is possible that A can convince B that N has exactly two prime factors when in fact it doesn't.

We present a much faster protocol that solves this problem and which has only one-sided error probability : with exponentially small probability, A can convince B that N has exactly two prime factors when in fact it has more.

We assume the existence of a mutually trusted source of random bits. This imposes no restriction on our protocol since any of a number of cryptographic techniques can be used to generate mutually trusted random bits.

In the next section we recall the number theoretic definitions and theorems needed for the protocol. Section 3 gives the actual protocol, together with a proofs of correctness and security.

2. Number Theoretic Background.

We denote by $\mathbf{Z}_N^*(+1)$ the set of elements in $\mathbf{Z}_N^*$ with Jacobi symbol +1. If N is a Blum integer then $N \equiv 1 \bmod 4$. This implies the Jacobi symbol modulo N of -1 is +1, a fact we will use. We assume B checks that $N \equiv 1 \bmod 4$, not a square and not a power of a prime.

The set of n-tuples $S_n = [\ \{1,-1\}^n\ ]$ endowed with ordinary component-wise integer multiplication is a group with identity $\mathbf{1} = (1, \ldots ,1)$. Let $P_1^{r1} P_2^{r2} \ldots P_n^{rn}$ be the factorization of N with the P_i's distinct primes. We define the function $\sigma_N : \mathbf{Z}_N^* \longrightarrow S_n$ as follows : the i'th component of $\sigma_N(x)$ is 1 if x is a quadratic residue modulo P_i and -1 otherwise. Notice that σ_N is a homomorphism with kernel the quadratic residues in $\mathbf{Z}_N^*$. If P is a prime or the power of a prime then exactly half the elements of $\mathbf{Z}_P^*$ are quadratic residues. Thus, if x is random in $\mathbf{Z}_N^*$ then, by the Chinese Remainder Theorem, $\sigma_N(x)$ is a random element of S_n. Notice also that if N is a Blum integer then $\sigma_N(-1) = (-1,-1)$.

If the prime powers appearing in the factorization of N all have odd exponents then we say N is **free of squares**. Let N = VW with W the part of N which is free of squares. That is (V,W) = 1 , V is a square, and W is free of squares. Notice that W > 1 by assumption. Since V and N are congruent to 1 mod 4, it follows that W is congruent to 1 mod 4. If x is a random element in $\mathbf{Z}_N^*(+1)$ then, by the Chinese Remainder Theorem, x mod V is a random element in $\mathbf{Z}_V^*$ (provided V > 1) and x mod W is a random element in $\mathbf{Z}_W^*(+1)$. From now on we denote by w the number of distinct prime factors of W and by v the number of distinct prime factors of V. Since $W \equiv 1 \bmod 4$ and free of squares, it follows that an even number of prime factors of W is congruent to 3 mod 4. This implies that $\sigma_W(-1)$ has an even (possibly 0) number of negative entries. Another number-theory fact we will use is that a random number x in $\mathbf{Z}_W^*(+1)$ has probability $(1/2)^{w-1}$ of being a quadratic residue. Similarly, a random number x in $\mathbf{Z}_V^*$ has probability $(1/2)^v$ of being a quadratic residue. It follows, by the Chinese Remainder Theorem, that a random number x in $\mathbf{Z}_N^*(+1)$ has probability $(1/2)^{v+w-1}$ of being a quadratic residue. If x is random in $\mathbf{Z}_N^*(+1)$ and $-1 \in \mathbf{Z}_N^*(+1)$ then -x is also a random element in $\mathbf{Z}_N^*(+1)$. Thus the probability that at least one of x or -x is a quadratic residue is less than or equal to $2(1/2)^{v+w-1} = (1/2)^{v+w-2}$ We have shown the following theorem:

Theorem 1: Suppose $N \equiv 1$ modulo 4 and has more than two distinct prime factors. If x is a random element in $\mathbf{Z}_N^*(+1)$ then the probability that at least one of x or -x is a quadratic residue modulo N is less than or equal to (1/2).

Another class of numbers will appear throughout this paper. These are composites of the form $N = P^{2r}Q^{s}$ with P and Q prime, $P \equiv 3$ mod 4, $Q \equiv 1$ mod 4, and s odd. For lack of a better name we call these numbers "class II" composites.

Theorem 2: Suppose N is a Blum integer or of class II. Let x be a random number in $\mathbf{Z}_N^*(+1)$. Then either x or -x is a quadratic residue modulo N.

<u>Proof</u>: If N is a Blum integer then $\sigma_N(x) \in \{(1,1),(-1,-1)\}$. Thus x is not a quadratic residue if and only if $\sigma_N(x) = (-1,-1)$. But then $\sigma_N(-x) = \sigma_N(-1)\,\sigma_N(x) = (-1,-1)\,(-1,-1) = (1,1)$ and so -x is a quadratic residue.

If N is of class II then $\sigma_N(-1) = (-1,1)$ and $\sigma_N(x) \in \{(1,1),(-1,1)\}$. Thus if x is not a quadratic residue then $\sigma_N(x) = (-1,1)$ and so $\sigma_N(-x) = \sigma_N(-1)\,\sigma_N(x) = (-1,1)(-1,1) = (1,1)$. $\square$

Theorem 3 : Assume $N \equiv 1$ mod 4, N is not a square and not a power of a prime. Let x be a random element in $\mathbf{Z}_N^*(+1)$. If N is not a Blum integer and not a class II composite, then the probability ρ that one or both of x and -x are quadratic residues modulo N is less than or equal to (1/2).

Proof : If N has more than 2 distinct prime factors then, by theorem 1, $\rho \le (1/2)$. So we may assume N has exactly 2 prime factors P and Q.

If $P \equiv Q \equiv 3$ mod 4 with $N = P^{r}Q^{s}$ then, since $N \equiv 1$ mod 4, r and s must have the same parity. Since N is not a square it follows that r and s are odd and therefore N is a Blum integer.

If $P \equiv 3$ mod 4 and $Q \equiv 1$ mod 4 then N must be of the form $P^{2r}Q^{s}$ with s odd (since N is not a square and is congruent to 1 mod 4) and therefore is of class II.

The only remaining case is when $P \equiv Q \equiv 1 \bmod 4$. In this case x is a quadratic residue if and only if $-x$ is a quadratic residue. If N is of the form $P^{2r}Q^s$ with s odd then $\rho = (1/2)$ because x must be a quadratic residue modulo Q^s but is random modulo P^{2r}. Finally, if N is of the form P^rQ^s with r and s odd, then $\sigma(x)$ is either $(1,1)$ or $(-1,-1)$, each with equal probability. Therefore in this last case ρ is also $(1/2)$.$\square$

We will also need the following facts:

Lemma 1 : If $N = P^rQ^s$ is a Blum integer, x a quadratic residue modulo N, and b is 1 or -1, then x has a square root modulo N with Jacobi symbol b.

Proof. By the Chinese Remainder theorem, $\mathbf{Z}_N$ is isomorphic to $\mathbf{Z}_{P^r} \times \mathbf{Z}_{Q^s}$. Let ψ be the isomorphism mapping $\mathbf{Z}_N$ to $\mathbf{Z}_{P^r} \times \mathbf{Z}_{Q^s}$. Let u be a square root of x modulo N, and let $\psi(u) = (\alpha, \beta)$. Then $v = \psi^{-1}((-\alpha, \beta))$ is also a square root of x modulo N. Recall that the Jacobi symbol of u modulo N is equal to the Jacobi symbol of α modulo P^r multiplied by the Jacobi symbol of β modulo Q^s . Since $P^r \equiv 3 \bmod 4$, the Jacobi symbol of α and $-\alpha$ modulo P^r have opposite sign. Therefore u and v have opposite Jacobi symbol.$\square$

Lemma 2 : Suppose $N = P^{2r}Q^s$ is of class II. Let x be a quadratic residue modulo N. Then all square roots of x modulo N have the same Jacobi symbol.

Proof. Using the notation of lemma 1 the four square roots of x are $\psi^{-1}((\pm\alpha, \pm\beta))$ for some α and β. Now $+\alpha$ and $-\alpha$ have Jacobi symbol 1 mod P^{2r}, and $+\beta$ and $-\beta$ have the same Jacobi symbol modulo Q^s since $Q \equiv 1 \bmod 4$. Thus all square roots of x have the same Jacobi symbol.$\square$

3. How to Convince an Opponent that N is a Blum Integer.

Assume N is not a square, not the power of a prime, and is congruent to 1 mod 4. The following protocol will convince B that N is a Blum integer.

PROTOCOL:

(1) A and B use the mutually trusted source of randomness to obtain 100 random numbers $\{x_i : i = 1, \ldots, 100\}$ in $\mathbf{Z}_N^*(+1)$ and 100 random signs $\{b_i : i = 1, \ldots, 100\}$ with $b_i \in \{1, -1\}$.

(2) for i = 1 to 100 A displays a square root r_i of x_i or of $-x_i$ modulo N with Jacobi symbol equal to b_i.

Proof of correctness: If N is a Blum integer then, by theorem 2 and lemma 1, A can produce all the square roots required at step (2). If N is not a Blum integer or of class II then, by theorem 3, the probability that A can produce all the square roots required at step (2) is at most $(1/2)^{100}$. But if N is of class II then, by lemma 2, the probability that A can produce all the roots with the required Jacobi symbol is $(1/2)^{100}$ Thus, unless N is a Blum integer, A will get caught cheating with probability $1 - (1/2)^{100}$.$\square$

Proof of security: We must show that if N is a Blum integer then no information is released by A other than this fact. Notice that B simply observes the mutually trusted source of random bits and A's messages. In the terminology of [CEGP86], this is a verifier-passive protocol. It is shown in [CEGP86] that to prove security of verifier-passive protocols we only need to produce a machine S, with input N a Blum integer, which can generate random bits and simulated messages which have the same joint probability distribution as the mutually trusted random bits and the messages sent by A. The simulator S can be constructed as follows:

PROGRAM FOR SIMULATOR S.

i) Generate 100 random elements $r_i \in \mathbf{Z}_N^*$ $\{i = 1, \ldots, 100\}$.

ii) Let b_i be the Jacobi symbol of r_i modulo N.

iii) For each i let $x_i = r_i^2 \bmod N$ or $x_i = -(r_i^2) \bmod N$ with equal probability.

It is a trivial matter to check that the r_i's, the b_i's, and the x_i's have the same joint probability distribution as those generated by A if A is honest.$\square$

Acknowledgements :

We thank Ivan Damgård for helping with an early draft of this paper.

References.

[BKP85] - Berger,Kannan,Peralta, "A Framework For The Study Of Cryptographic Protocols". Proceedings of Crypto85.

[Blum82] - Manuel Blum, "Coin Flipping By Phone". COMPCON. IEEE, February 1982.

[CEGP86] - Chaum, Evertse, van de Graaf, Peralta, "Demonstrating Possession of a Discrete Logarithm Without Revealing It". Proceedings of Crypto86.

[GHY85] - Galil,Haber, Yung, "A Private Interactive Test of a Boolean Predicate and Minimum-Knowledge Public-Key Cryptosystems". 26th. FOCS, 1985.