A Remark on a Non-interactive Public-Key Distribution System

Ueli M. Maurer

Inst. for Theoretical Computer Science
ETH Zurich
CH-8092 Zurich, Switzerland

Yacov Yacobi

Bellcore
445 South St.
Morristown, NJ 07962

An identity-based non-interactive public key distribution system was presented by these authors at Eurocrypt '91 [2]. It is based on the observation that for an appropriate choice of m, computing discrete logarithms in $\mathbf{Z}_m^*$ is feasible if and only if the factorization of m is known. This observation allows one to set up an exponential key distribution system in which a user's (say Alice's) public key is equal to her identity I_A. A trusted authority who knows the factorization of m is required for computing (during registration) Alice's secret key S_A as the discrete logarithm of I_A to some base g, where g is an element of $\mathbf{Z}_m^*$ with maximal order.

Because in some applications the users' identities (e.g. their email address) can be assumed known to other users, the public keys of the above scheme need not be transmitted. Moreover, the public keys are self-authenticated and require no further authentication by certificates. One can therefore build a non-interactive public-key cryptosystem having, for example, applications for electronic mail where only a one-way, non-interactive communication takes place when messages are sent. When a user Bob (knowing I_A) wants to send a message to Alice, he computes the cipher key

$$K_{AB} = {I_A}^{S_B}$$

and encrypts the message using this key and a conventional cryptosystem. When receiving the cryptogram, Alice computes the same cipher key according to $K_{AB} = {I_B}^{S_A}$ and deciphers the message using this key.

R.A. Rueppel (Ed.): Advances in Cryptology - EUROCRYPT '92, LNCS 658, pp. 458-460, 1993.

One problem with the described approach is that the group $\mathbf{Z}_m^*$ is not cyclic and hence there exists no base g to which every element has a discrete logarithm. One solution to this problem is to transmit a small offset which, when added to the identity, results in an element of $\mathbf{Z}_m^*$ having a discrete logarithm to a public base. However, this solution requires interaction: the sender of a message must receive (either from the receiver or from a trusted server) the offset before encrypting a message.

A different solution was proposed in [2] where it was observed that every square modulo m has a discrete logarithm to a base g with maximal order in $\mathbf{Z}_m^*$. It was therefore suggested that the square modulo m of a user's identity, ${I_A}^2$, rather than the identity I_A itself be used as her public key, allowing to retain the non-interactive feature. Unfortunately, this solution is insecure [1] because a square root modulo m of the squared identity ${I_A}^2$ can be obtained when given the secret key $S_A = \log_g({I_A}^2)$ by computing $g^{S_A/2}$ (note that S_A is even). If for at least one of the prime factors p of m,

$$\log_g I_A \pmod{p} < (p-1)/2$$

while for at least some other prime factor q of m,

$$\log_g I_A \pmod{q} \geq (q-1)/2,$$

then the obtained square root of ${I_A}^2$ is different from I_A and $-I_A$ and thus allows one to find a non-trivial factor of m. This condition is satisfied by a fraction $1-2^{-r+1} \geq 1/2$ of all identities, where r is the number of distinct (odd) prime factors of m.

The purpose of this note is to point out the described weakness and to suggest a simple remedy. The trusted authority chooses once and for all a secret multiplier t randomly from $\mathbf{Z}_{\varphi(m)}^*$. Instead of issuing the discrete logarithms of squared identities as users' secret keys, the trusted authority conceals these logarithms by multiplying them with t before issuing them to users. Hence

$$S_A \equiv t \cdot \log_g({ID_A}^2) \pmod{\varphi(m)}.$$

This modification of the secret key generation requires no change of the communication phase because the mutual cipher key computed by both users is according to the above described formulas

$$K_{AB} = {I_A}^{2S_B} = g^{vS_AS_B} = {I_B}^{2S_A}$$

where $v \equiv t^{-1} \pmod{\varphi(m)}$.

An alternative solution presented in [2] to the problem of achieving the non-interactive feature is based on the observation that, if m is the product of two odd primes, $m = pq$, then the (efficiently computable) Jacobi symbol (x/m) of

an integer x is equal to 1 if and only if x has a discrete logarithm modulo m (to a base that is primitive both in $GF(p)$ and $GF(q)$). If $p \equiv 3 \pmod 8$ and $q \equiv 7 \pmod 8$ then $(2/m) = -1$ and Alice's modified identity can therefore be defined as

$$I'_A = \begin{cases} I_A & \text{if } (I_A/m) = 1 \\ 2I_A & \text{if } (I_A/m) = -1 \end{cases}$$

I'_A is obtained easily from I_A even without knowledge of the trapdoor and is guaranteed to have a discrete logarithm. However, this solution only works for the special case where m has only two prime factors. Note that for this choice computing discrete logarithms modulo p and q is feasible only when $p-1$ and $q-1$ are chosen to have only moderate prime factors [2].

When $m = p_1 \cdots p_r$ is the product of $r > 2$ prime factors (in which case general primes of appropriate size can be used), the following solution, which appears to be less attractive than the use of the secret multiplier t described above and is only briefly sketched, could alternatively be used. The trusted authority also publishes numbers $C_2, \ldots, C_r$, where C_i is a quadratic nonresidue modulo p_i but a quadratic residue modulo all the other prime factors of m. When Bob sends a message to Alice, he uses the secret key $K_{AB} = I_A{}^{s_B}$ and also sends $C_i^{S_B}$, $i = 2, \ldots, r$, to Alice. Alice knows for which primes her identity is a quadratic residue (non-residue), i.e., which of the C_i she must multiply her identity with to obtain an element with a discrete logarithm, which she obtained as her secret key. She can compute the cipher key K_{AB} by multiplying $I_B^{S_A}$ by an appropriate subset of the received $C_i^{S_B}$.

Acknowledgments

Some results presented in this paper were found independently by Pil Lee.

References

[1] A.J. Lenstra, private communication with Y. Yacobi.

[2] U.M. Maurer and Y. Yacobi, Non-interactive public-key cryptography, *Advances in Cryptology – EUROCRYPT '91*, D. Davies, Ed., Lecture Notes in Computer Science, vol. 547, pp. 498-507, Springer-Verlag, 1991.