An identity-based identification scheme based on discrete logarithms modulo a composite number

Marc Girault
Service d'Etudes communes des Postes et Télécommunications (SEPT)
42 rue des Coutures, Caen, France

Abstract. *We first describe a modification of Schnorr's identification scheme, in which the modulus is composite (instead of prime). This modification has some similarity with Brickell-McCurley's one, presented at the same conference. Then, by establishing a new set-up, we derive the first identity-based identification scheme based on discrete logarithms. More precisely, it is based on discrete logarithm modulo a composite number, a problem known to be harder than factorization problem. This scheme has interesting and somewhat paradoxical features. In particular, any user can choose his own secret, and, provided the parameters have convenient sizes, even the trusted center is unable to retrieve it from the public key (contrary to any identity-based scheme known until now).*

1. Introduction

At CRYPTO'90 conference, Schnorr presented a new identification scheme [Sc], the security of which is based on the difficulty of discrete logarithm problem modulo a prime.

The set-up of Schnorr's scheme is as follows. A trusted center (or KAC : "Key Authentication Center") generates two primes p and f such that f divides p-1, and an integer b of order f modulo p (i.e. f is the smallest integer such that $b^f = 1$ [mod p]). The integers p, f and b are published by the center. Each user chooses a secret s, smaller than f, and his public key is $P = b^{-s}$ (mod p). Now, the center signs a message composed of user's identity I, his public key P and other parameters such as validity dates. This signed message will be called certificate, in accordance with ISO/CCITT vocabulary. Any signature scheme (including the one derived from this identification scheme) can be used to produce this certificate.

I.B. Damgard (Ed.): Advances in Cryptology - EUROCRYPT '90, LNCS 473, pp. 481-486, 1991.

Compared to other identification schemes, Schnorr's one has some advantages but also some drawbacks. One of these drawbacks is the necessity for the center to produce certificates, and for the verifier to check them. This drawback does not exist in identity-based schemes [Sh], in which a user's public key is nothing but his identity I.

Conversely, one important drawback of identity-based schemes is the fact that not only a user cannot choose his secret key, but this key is calculated by the center and can be calculated again by it at any moment during its period of validity.

In this paper, we present the first identity-based identification scheme in which every user can choose himself his secret key, the center being unable to retrieve it from the public key. To achieve this goal, we first design a Schnorr-like identification scheme using a composite modulus instead of a prime one (section 3), then we modify the set-up of the scheme in order to render it identity-based (section 4). Beforehand, we briefly recall what Schnorr's identification protocol is (section 2).

Because we are limited in space, only the security of the set-up of these schemes will be discussed. The security of the protocols themselves (in particular their zero-knowledgeness) will not be addressed.

Before starting, we inform the reader that a very closely related paper has been presented at ESORICS'90 conference [GP] in October 1990.

2. Schnorr's identification scheme

The set-up of Schnorr's scheme has been described in the introduction. The typical sizes of the parameters are 512 bits for p, and 140 bits for f.

When Alice wants to prove to Bob she is Alice, the two partners use the following protocol :

1) Alice picks a random integer r in the interval [0, f-1], calculates $x = b^r \pmod p$ and sends it to Bob along with her certificate.

2) Bob checks the certificate, picks a random integer c in the interval $[0, 2^t-1]$ (where, typically, t lies between 20 and 70) and sends it to Alice.

3) Alice calculates $y = r + sc \pmod f$ and sends it to Bob.

4) Bob checks that $b^y P^c = x \pmod p$.

It can be proven that a fraudor (somebody who wants to impersonate Alice but

does not know s), has only one chance over 2^t not to be detected, and that this protocol is zero-knowledge provided discrete logarithm modulo a prime is a hard problem. Some optimizations features of the scheme, though important, are not considered here for short.

3. A Schnorr-like scheme with a composite modulus

Description

We now describe a modification of Schnorr's scheme. Let n be the product of two primes p and q such that $p = 2fp' + 1$ and $q = 2fq' + 1$, where f, p' and q' are distinct primes. In the basic version, f is 200 bit-long, p' and q' are 300-bit long, so n is a 1000-bit integer. In a variant, f is 140-bit long, p' and q' are 210-bit long, so n is 700-bit long (this should be the minimal length of n). The difference of security between both versions will be discussed later.

Let b be an integer of order f both modulo p and modulo q. Therefore the order of b modulo n is f and we have : $b^f = 1 \pmod n$. Note that all these parameters can be easily generated by the center (we omit the details). Now, the integers n, f and b are made public, whilst p and q are kept secret.

The rest of the scheme is exactly the same as in Schnorr's scheme except that we replace every occurrence of *p* by *n*. To be explicit, each user chooses a secret s, smaller than f, and his public key is $P = b^{-s} \pmod n$. The certificate is calculated by the authority as shown in the introduction and the identification protocol is as follows :

1) Alice picks a random integer r in the interval [0, f-1], calculates $x = b^r \pmod n$ and sends it to Bob along with her certificate.

2) Bob checks the certificate, picks a random integer c in the interval $[0, 2^t-1]$ and sends it to Alice.

3) Alice calculates $y = r + sc \pmod f$ and sends it to Bob.

4) Bob checks that $b^y P^c = x \pmod n$.

Note that Schnorr introduced the parameter f, a small divisor of p-1, only in order to optimize the performances of this scheme. The security of his scheme is not compromised if f is equal to p-1, since p is public. On the contrary, choosing f as a

very small divisor of p-1 and q-1 is crucial for the security of our modification, since p and q are secret.

Security of the scheme

Generally speaking, the security of the scheme lies on the difficulty of computing a discrete logarithm modulo a composite number. This problem is known to be harder than factorization problem. More precisely, factorization problem can be reduced to general discrete logarithm problem in probabilistic polynomial time [W]. Recently, Schrift and Shamir [SS] proved that almost all bits of the discrete logarithm modulo a Blum integer were individually secure (and the right half of them simultaneously secure) provided factorization of Blum integers is hard.

Now, the moduli we use are Blum integers, but of a very special form. Moreover, some side information on factors of n is revealed, since a divisor f of (p-1)(q-1), the Euler function of n, is made public, as well as an integer b of order f modulo n. The security of the scheme therefore lies on a very specific assumption, namely the difficulty of finding s, given b^{-s} (mod n) and all this knowledge about n.

However, as far as we know, even factoring n seems to be hard. The only attack we found, apart from existing factorization algorithms, costs $2^{|p'+q'|/|f|}$ operations, where |u| denotes the number of bits of u. This is why we chose |p'+q'|/|f| at least equal to 2^{70}.

Note that, in the basic version, factoring n is not enough to retrieving s from P, since the enemy still has to compute discrete logarithms modulo p and q, which are 500-bit primes. In fact, as long as factoring (our special) n *or* discrete logarithm modulo (our special) p is hard, then our scheme is secure. This is an interesting similarity with Brickell and McCurley's scheme [BC], reported in these proceedings. This last scheme also is a modification of Schnorr's scheme, designed so as to preserve its security even if either factorization or discrete logarithm modulo a prime (but not both) became no more infeasible.

Of course, the property that the scheme remains secure even if n is factorized does not subsist if n is a 700-bit number (and p, q 350-bit numbers) since existing algorithms may compute discrete logarithms for primes of this size. Nonetheless, if this property is not specifically required, then these sizes of parameters can be chosen.

4. A "paradoxical" identity-based scheme

Description

We now come to our final scheme. Let n, f, b be as in the previous section, e be a public exponent coprime with p-1 and q-1 (where, typically, the length of e lies between 20 and 70 bits) and d be the inverse of e modulo l.c.m. (p-1, q-1). The integers n, f, b and e are published by the authority, whilst p, q and d are kept secret.

Alice chooses her secret key s as before, calculates b^{-s} (mod n) and gives it to the center. Then, the center calculates $P = I^{-d}b^{-s}$ (mod n), and P will be Alice's public key . This public key is somewhat particular in that it depends both on user's identity I and on his secret s. Note that I and P are connected by the equation : $P^eIh^s = 1$ (mod n), where $h = b^e$ (mod n). A similar set-up can be found in [TO].

The protocol is as follows :

1) Alice picks a random integer r in the interval [0, f-1], calculates $x = h^r$ (mod n) and sends it to Bob along with her certificate.

2) Bob checks the certificate, picks a random integer c in the interval [0, e-1] and sends it to Alice.

3) Alice calculates y = r + sc (mod f) and sends it to Bob.

4) Bob checks that $h^y(P^eI)^c = x$ (mod n).

Security of the scheme

Two distinct questions have to be discussed. First, what is the level of difficulty to impersonate a user (by finding his secret s) ? Second, what is the level of difficulty to impersonate the trusted center (by finding his secret d) ?

In non-identity-based schemes, as Schnorr's scheme, the second question is irrelevant since the answer only depends on the signature scheme which is used to produce certificates. And this signature scheme may be completely independent of the identification scheme itself.

In usual identity-based schemes, the two questions become only one, because s is calculated from I using d, and finding d seems to be the only way to find s.

In our scheme, the two questions are separate since, as already mentioned, d is not sufficient to calculate s. Factoring n is enough to impersonate the trusted center whilst calculating a discrete logarithm modulo n (a harder problem, see previous section) is required to impersonate a user.

Other topic

The set-up of this scheme also provides material for identity-based key-exchange. The whole package has been exposed in [GP].

Acknowledgements

Many thanks to Brigitte Vallée, who improved the security of the scheme. Also thanks to K. Ohta, C. Schnorr and G. Robin, who listened to me exposing it.

Bibliography

[BC] E. F. Brickell and K. S. McCurley, "An interactive identification scheme based on discrete logarithms and factoring", EUROCRYPT'90, these proceedings.

[GP] M. Girault and J. C. Paillès, "An identity-based scheme providing zero-knowledge authentication and authenticated key-exchange", Proc. of ESORICS'90, 24-26 oct. 90.

[Sc] C. P. Schnorr, "Efficient identification and signatures for smart cards", Advances in Cryptology, Proc. of CRYPTO'89, Springer-Verlag.

[Sh] A. Shamir, "Identity-based cryptosystems and signature schemes", Advances in Cryptology, Proc. of CRYPTO'84, LNCS 196, Springer-Verlag, 1985, pp.47-53.

[SS] A. Schrift and A. Shamir, "The discrete log is very discreet", presented at 1st Oberwolfach Conference on Cryptography, 24-30 sept. 89.

[TO] K. Tanaka and E. Okamoto, "Key distribution system using ID-related information directory suitable for mail systems", Proc. of SECURICOM'90, pp.115-122.

[W] H. Woll, "Reductions among number theoretic problems", Information and Computation 72, pp.167-179, 1987.