IDENTITY-BASED CRYPTOSYSTEMS AND SIGNATURE SCHEMES

Adi Shamir

Department of Applied Mathematics
The Weizmann Institute of Science
Rehovot, 76100 Israel

THE IDEA

In this paper we introduce a novel type of cryptographic scheme, which enables any pair of users to communicate securely and to verify each other's signatures without exchanging private or public keys, without keeping key directories, and without using the services of a third party. The scheme assumes the existence of trusted key generation centers, whose sole purpose is to give each user a personalized smart card when he first joins the network. The information embedded in this card enables the user to sign and encrypt the messages he sends and to decrypt and verify the messages he receives in a totally independent way, regardless of the identity of the other party. Previously issued cards do not have to be updated when new users join the network, and the various centers do not have to coordinate their activities or even to keep a user list. The centers can be closed after all the cards are issued, and the network can continue to function in a completely decentralized way for an indefinite period.

The scheme is ideal for closed groups of users such as the executives of a multinational company or the branches of a large bank, since the headquarters of the corporation can serve as a key generation center that everyone trusts. The scheme remains practical even on a nationwide scale with hundreds of key generation centers and millions of users, and it can be the basis for a new type of personal identification card with which everyone can electronically sign checks, credit card slips, legal documents, and electronic mail.

The scheme is based on a public key cryptosystem with an extra twist: Instead of generating a random pair of public/secret keys and publishing one of these keys, the user chooses his name and network address as his public key. Any combination of name, social security number, street address, office number or telephone number can be used (depending on the context) provided that it uniquely identifies the user in a way he cannot later deny, and that it is readily available to the

Copyright (c) 1998, Springer-Verlag

other party. The corresponding secret key is computed by a key generation center and issued to the user in the form of smart card when he first joins the network. The card contains a microprocessor, an I/O port, a RAM, a ROM with the secret key, and programs for message encryption/decryption and signature generation/verification.

An identity-based scheme resembles an ideal mail system: If you know somebody's name and address you can send him messages that only he can read, and you can verify the signatures that only he could have produced. It makes the cryptographic aspects of the communication almost transparent to the user, and it can be used effectively even by laymen who know nothing about keys or protocols.

When user A wants to send a message to user B, he signs it with the secret key in his smart card, encrypts the result by using B's name and network address, adds his own name and network address to the message, and sends it to B. When B receives the message, he decrypts it using the secret key in his smart card, and then verifies the signature by using the sender's name and network address as a verification key.

The secret keys must be computed by a key generation center rather than by the users, since there is nothing special about a user's identity: If user A could compute the secret key that corresponds to the public key "A", he could also compute the secret keys that correspond to the public keys "B", "C", etc., and the scheme would not be secure. The key generation center can be in a privileged position by knowing some secret information (such as the factorization of a large number) which enables it to compute the secret keys of all the users in the network.

The overall security of the scheme depends on the following points: (a) The security of the underlying cryptographic functions. (b) The secrecy of the priveleged information stored at the key generation centers. (c) The thoroughness of the identity checks performed by the centers before they issue cards to users. (d) The precautions taken by users to prevent the loss, duplication, or unauthorized use of their cards.

The cryptographic scheme effectively ties the message with the identification information i, and the ownership of the card effectively ties i with the physical user. Like any other agency that issues ID cards, the center must carefully screen requests for cards to prevent misrepresentations, and must carefully protect its "stamps" to prevent forgeries. Users can protect themselves against unauthorized use of their cards via a password system or by memorizing part of the key.

The differences between private-key, public-key, and identity-based cryptosystems are summarized in Fig. 1. In all these schemes, the mes-

Copyright (c) 1998, Springer-Verlag

sage m is encrypted under key ke, transmitted as ciphertext c through the exposed channel, and decrypted under key kd. The choice of keys is based on a truly random seed k. In private-key schemes, ke = kd = k, and the separate key channel (which is usually a courier) must preserve both the secrecy and the authenticity of the key. In public-key schemes, the encryption and decryption keys are derived from k via two different functions ke = fe(k) and kd = fd(k), and the separate key channel (which is usually a directory) must preserve only the authenticity of the key. In identity-based schemes, the encryption key is the user's identity ke = i, and the decryption key is derived from i and k via kd = f(i,k). The separate key channel between the users is completely eliminated, and is replaced by a single interaction with the key generation center when the recipient first joins the network.

Public-key and identity-based signature schemes are mirror images of the corresponding cryptosystems, as depicted in Fig. 2. The message m is signed with the signature generation key kg, tranmitted along with its signature s and sender identity i, and verified with the signature verification key kv. The rest of the diagram should be self-evident.

THE IMPLEMENTATION

To implement the idea described in the previous section, we need a public-key scheme with two additional properties: (a) When the seed k is known, secret keys can be easily computed for a non-negligible fraction of the possible public keys. (b) The problem of computing the seed k from specific public/secret key pairs generated with this k is intractable.

Unfortunately, the RSA scheme cannot be used in a way that satisfies these conditions simultaneously: (a) If the modulus n is a pseudo-random function of the user's identity, even the key generation center cannot factor this n and cannot compute the decryption exponent d from the encryption exponent e. (b) If the modulus n is universal and the seed is its secret factorization, then anyone who knows an encryption exponent e and its corresponding decryption exponent d can compute the seed.

At this stage we have concrete implementation proposals only for identity-based signature schemes, but we conjecture that identity-based cryptosystems exist as well and we encourage the reader to look for such systems. This situation is reminiscent of the 1976 period, when public key cryptosystems were defined and their potential applications were

Copyright (c) 1998, Springer-Verlag

investigated even though the first concrete implementations were published only in 1978.

The signature scheme is based on the verification condition

$$s^e = i \cdot t^{f(t,m)} \pmod{n}$$

where

- m is the message
- s,t is the signature
- i is the user's identity
- n is the product of two large primes
- e is a large prime which is relatively prime to $\varphi(n)$
- f is a one way function.

The parameters n,e and the function f are chosen by the key generation center, and all the users have the same n,e and the same algorithmic description of f stored in their smart cards. These values can be made public, but the factorization of n should be known only to the key generation center. The only difference between users is the value of i, and the secret key which corresponds to i is the (unique) number g such that

$$g^e = i \pmod{n}.$$

This g can be easily computed by the key generation center, but if the RSA scheme is secure no one else can extract e-th roots mod n.

Each message m has a large number of possible (s,t) signatures, but their density is so low that a random search is extremely unlikely to discover any one of them. Any attempt to set one of (s,t) to a random value and solve for the other variable requires the extraction of modular roots, which is believed to be an exceedingly difficult computational task. However, when g is known, there is a very simple way to generate any number of signatures of any message even when the factorization of n is unknown.

To sign the message m, the user chooses a random number r and computes

$$t = r^e \pmod{n}.$$

The verification condition can be rewritten as

$$s^e = g^e \cdot r^{ef(t,m)} \pmod{n}.$$

Since e is relatively prime to $\varphi(n)$, we can eliminate the common factor e from the exponents

$$s = g \cdot r^{f(t,m)} \pmod{n}$$

Copyright (c) 1998, Springer-Verlag

and thus s can be computed without any root extraction.

To prevent attacks based on multiplicative relationships between the identities (and thus also the g values) of different users, it is advisable to expand the string that describes the user's identity into a long pseudo-random string via a universal one way function, and use the expanded form as i in the verification condition. Since everyone in thenetwork knows how to apply this function, the scheme retains its identity-based flavour even though the signature verification key is not strictly equal to the user's identity.

The security of the scheme depends on the inability of the cryptanalyst to isolate g by analysing a large number of valid signatures of messages of his choice. If the gcd of f and e is $c \neq 1$, it is possible to extract the c-th root of i by manipulating the verification condition, and thus it is essential to make e a sufficiently large prime and f a sufficiently strong one way function so that this case will never arise in practice. The value of r should never be reused or revealed, since g is protected in any concrete signature by its randomness and secrecy.

The variants of the verification condition in which one of the two occurrences of t is eliminated (e.g., by replacing it with a constant) are insecure. It is thus important to use a one way function that mixes t and m thoroughly (preferably via non-arithmetic and non-invertible operations) and which has a large range of possible values.

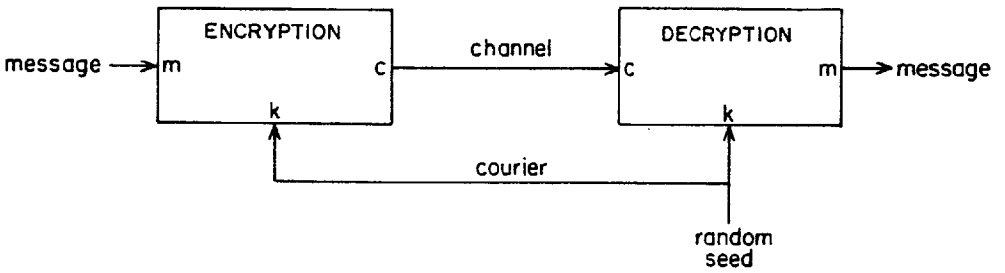
We believe that with a proper choice of parameters this scheme can be made very secure, but we cannot prove that breaking it is equivalent to solving some well known computational problem. Its main purpose is didactic, to serve as the first existence proof for identity based schemes. The Ong-Schnorr-Shamir signature scheme (described elsewhere in these proceedings) can also be used as an identity-based scheme, but its security is still an open problem in light of Pollard's successful attacks against its earlier verisons. As always, we do not recommend to use this scheme right away, before the cryptographic community had ample time to assess its security.

ACKNOWLEDGEMENTS

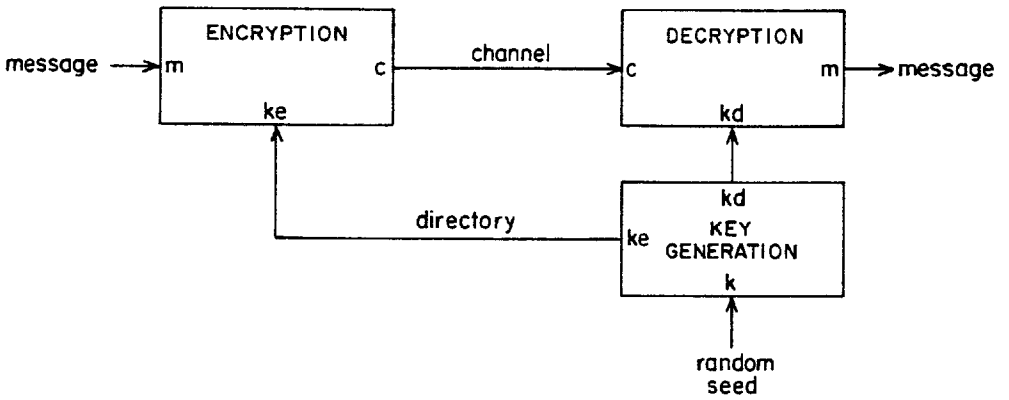
I would like to thank Amos Fiat, Heidroon Ong and Claus Schnorr for very helpful discussions.

Copyright (c) 1998, Springer-Verlag

PRIVATE-KEY CRYPTOSYSTEM :



PUBLIC-KEY CRYPTOSYSTEM :



IDENTITY-BASED CRYPTOSYSTEM :

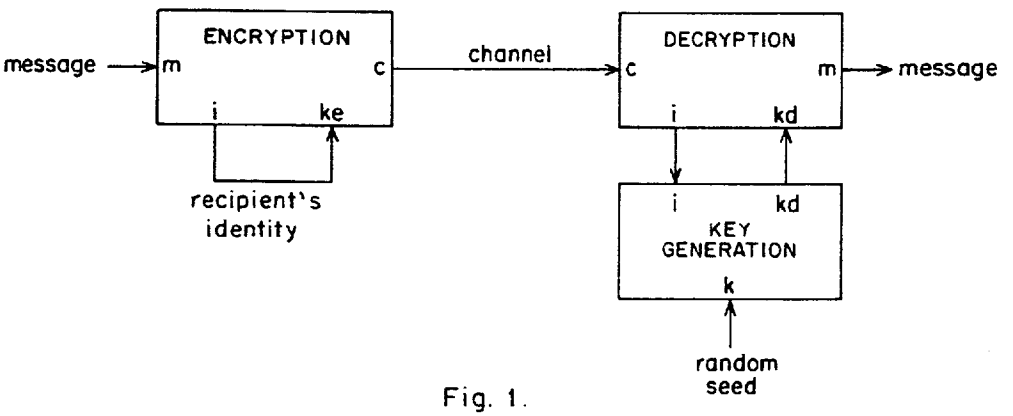
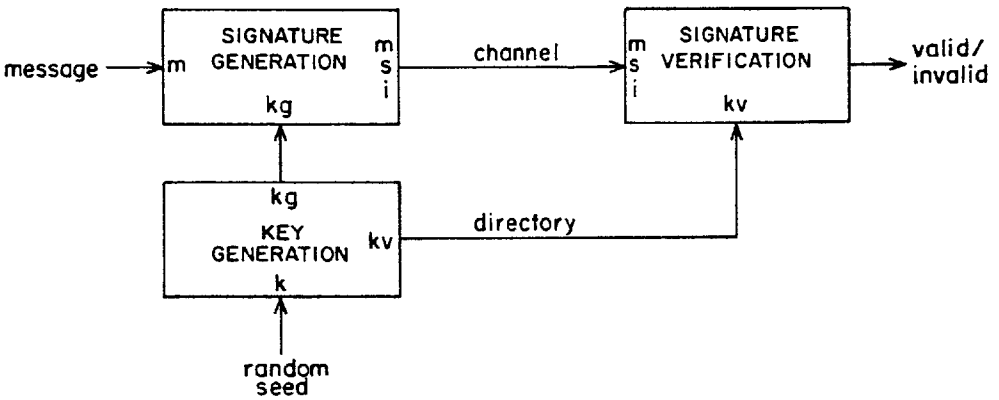


Fig. 1.

Copyright (c) 1998, Springer-Verlag

PUBLIC-KEY SIGNATURE SCHEME :



IDENTITY-BASED SIGNATURE SCHEME :

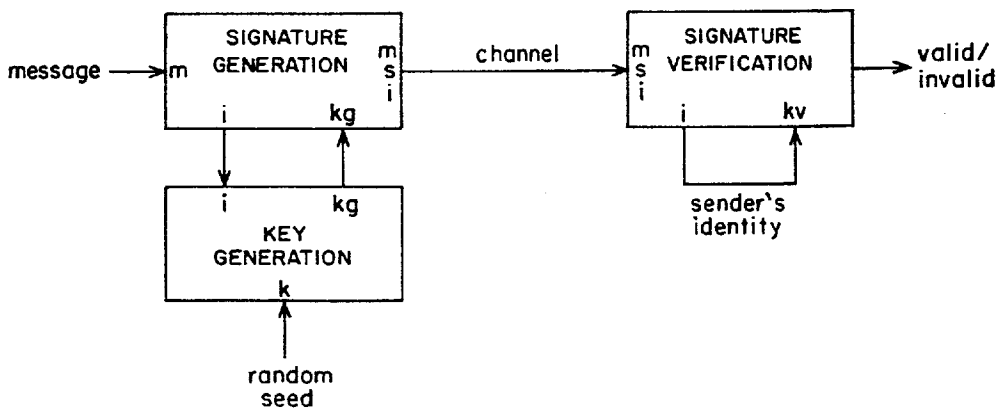


Fig. 2.

Copyright (c) 1998, Springer-Verlag