SECRET DISTRIBUTION OF KEYS FOR PUBLIC-KEY SYSTEMS

Jean-Jacques Quisquater

Philips Research Laboratory Brussels
Avenue Van Becelaere, 2
B-1170 Brussels, Belgium

Extended abstract

Abstract

This paper proposes new public-key cryptosystems systems the security of which is based on the tamperfreeness of a device and the existence of secret key cryptosystems instead of the computational complexity of a *trapdoor* one-way function (RSA).

1 Introduction

This paper is an extension of ideas presented by Desmedt and Quisquater at CRYPTO '86 in [2]. In that presentation, the first identity-based cryptosystem (a nice idea proposed by Adi Shamir [3]) to protect privacy was presented. This cryptosystem is based on the existence of secret-key cryptosystems, of tamperfree devices, using an authority (a trusted center) and the key generation specific to the identity-based systems. An important open problem was set:

> *Does there exist an identity-based cryptosystem to protect privacy which security is based on tamperfree devices and computational complexity and which use* different *supersecret keys s for different users?*

We give here an explicit construction of such a cryptosystem. The involved concepts can be used to improve a signature scheme of Davies using smart cards (where there was the same problem for the unique supersecret key): Our solution allows to avoid the illegal creation of any new (false) identity in the system. A related construction permits to strongly limit the subliminal use of protocols where the exchange of random numbers is essential. We introduce in this context the concept of *certified random*.

2 Key generation for identity-based systems

The figure 1 recalls the principle of key generations for public-key cryptosystems (a) and for identity-based cryptosystems (b). The figure 2 gives a first implementation of a public-key cryptosystem where the (unique) supersecret key of the authority is s. The secret-key cryptosystems are based on the cryptographic functions E' (the "inverse" of which is D') and D''. More explanations are given in [2].

C. Pomerance (Ed.): Advances in Cryptology - CRYPTO '87, LNCS 293, pp. 203-208, 1988.

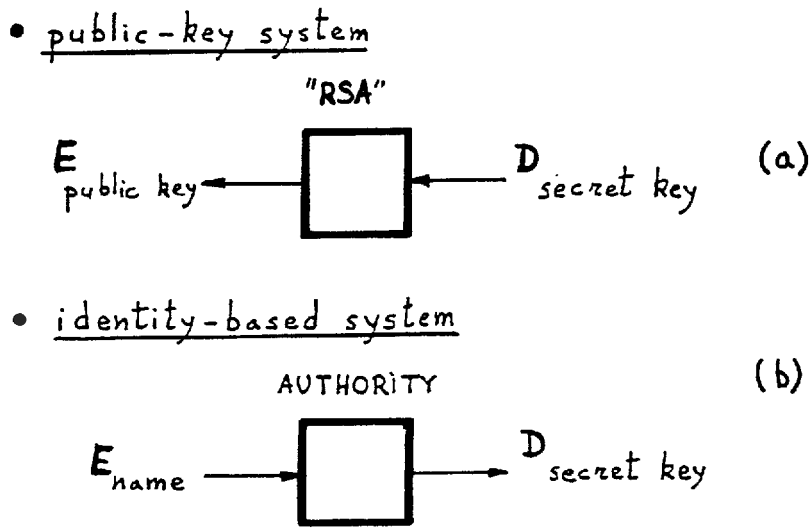


Figure 1: Key generation for public-key and identity-based systems

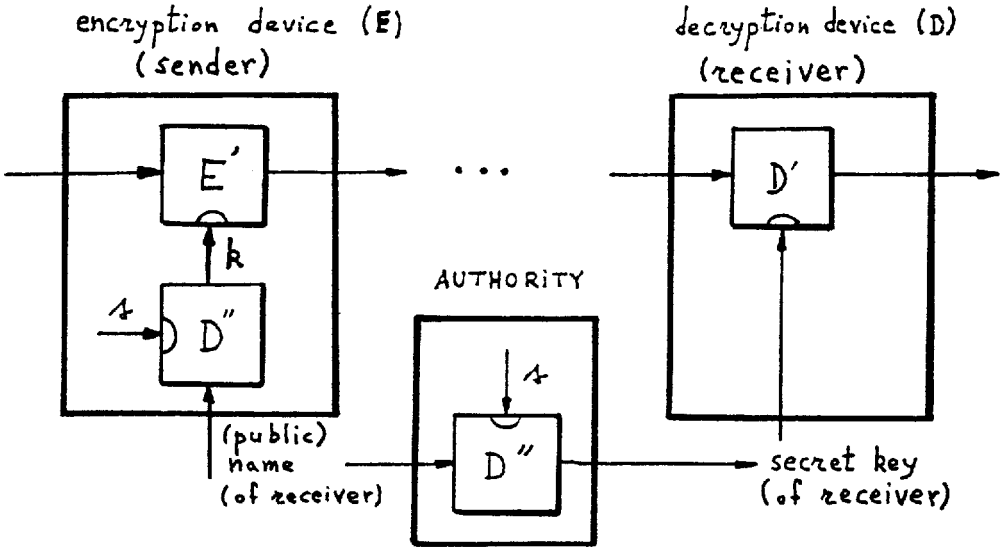


Figure 2: The first identity-based system to protect privacy

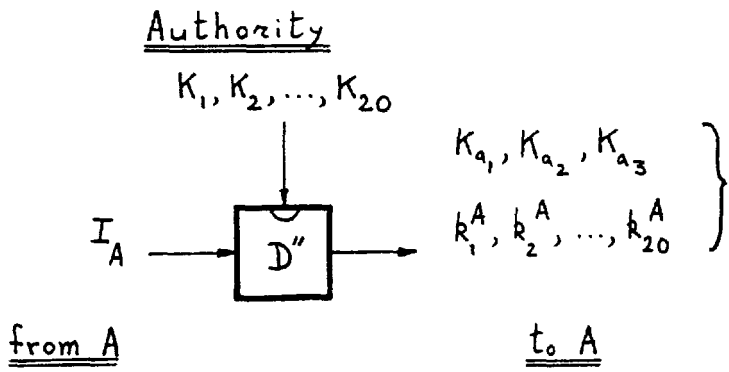


Figure 3: The new key generation

3 The main idea

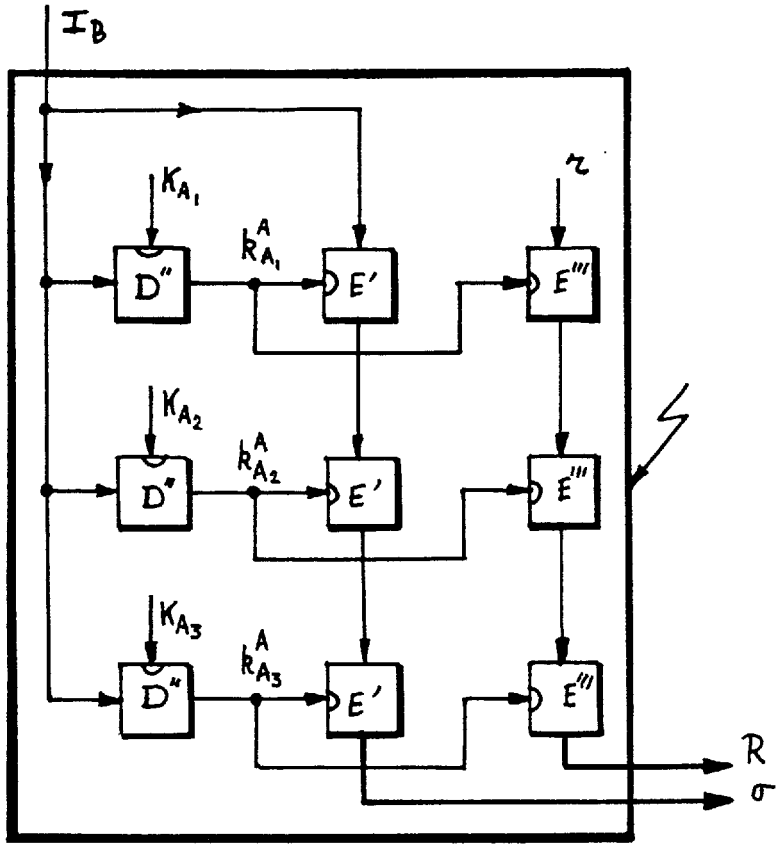
3.1 Sketch

The main idea here is that the authority has many supersecret keys (for instance, 20) but distributes only few keys to each user (for instance, 3 keys). This set of 3 keys is unique for each user (there is thus a limit for the number of users in the system, in this version) and nobody knows if he/her has one or two keys in common with a given user. The authority retains secret the distribution of keys. Each user receives also the encrypted form of his/her identity by the 20 supersecret keys. Another idea is that if one knows some *useful* information about the used keys one can avoid an exhaustive search of keys (concept of *indicator*).

Another possible and useful idea is to have two or more authorities. It will be described in the full paper.

3.2 The new key generation

The new key generation in given in figure 3. The supersecret keys of the authority are K_1, K_2, K_3, ..., K_{20}, the identity of some user A is denoted by I_A, the elements of the subset α of supersecret keys given to the user A (inside his tamperproof device) are K_{A_1}, K_{A_2} and K_{A_3} where A_1, A_2 and A_3 are ordered values chosen from $\{1, 2, 3, ..., 20\}$ by the authority in such a way that only this user has these three keys. The encrypted forms of the identity I_A by the supersecret keys are k_1^A, k_2^A, k_3^A, ..., k_{20}^A also enclosed in the tamperproof device of A.



I_B: (public) identity of B;

R: enciphered version of the session key r chosen by A;

σ: indicator of the subset α;

K_{A_1}, K_{A_2} and K_{A_3}: the 3 supersecret keys specific to the user A;

$k^A_{A_1}$, $k^A_{A_2}$, $k^A_{A_3}$: computed values, "protected" by the tamperproof device of A and also known (because it was given by the authority) by the tamperproof device of B.

Figure 4: Transmission of the session key R from A to B

3.3 The new scheme

These two combined ideas (several supersecret keys and the use of the indicator) give the scheme briefly described in figure 4. This scheme shows the transmission of a secret session key r from the user A to the user B. The sender A uses the public identity I_B of the user B as input to his tamperproof device which computes two values, transmitted to the user B;

- the enciphered session key R: the common secret key session being r;
- the indicator σ of the subset α from $\{1, 2, 3, ..., 20\}$;

Only the tamperproof device of B is able to recover the values r and α. After a maximum of $\binom{20}{3}$ computations (a practical value), the device of B recovers A_1, A_2 and A_3, using the *indicator*, that is, a value giving some indications about the used supersecret keys but useful only to him. Some collision is possible (two sets of keys give the same indicator) but it is very improbable in a well designed system and can be avoided. Some precomputations are possible to accelerate the process. Then, the device of B deciphers R using the function D''' (the inverse of E''') and the values $k^A_{A_1}$, $k^A_{A_2}$, $k^A_{A_3}$, known thanks to the indicator. The secret common key r is now transmitted.

4 Access control

Here the problem is to avoid the possibility of fraud, that is the illegal creation of certified identities (without the use of the trusted authority). We only give the main idea without detail. The context of tamperproof devices is here implicit, that is, the sensible informations are always inside such devices.

The authority has, for instance, 100 secret functions (an one-way function and 100 keys). The output of these functions can be small, one bit for instance. To each correct identity I the authority gives the 100 outputs, corresponding to these functions. Each verifier (terminal) receives only some of these functions (depending on the level of security). These functions permit to verify, with some degree of confidence, but not to create new certified identities. Again the distribution of keys by the authority is secret. So an opponent will have many problems to recover all keys in view of creating new certified identities.

5 The concept of certified random

The concept of subliminal channel was introduced by G. Simmons [4]. In fact, each protocol using random numbers has possibilities of subliminal channels. Indeed, each random number is, maybe, an encrypted message by a secret function (unknown to somebody among the parties of the protocol). How to avoid that problem? The sender of the random number has to prove to everybody the correct use of some intermediary (see the concept of warden in the paper of Y. Desmedt). That is, for instance, given a random number r, the sender computes $f(r) = R$ and sends R. Now the sender has to prove the

use of f (without repeated tests to choose a "good" R). This intermediary can be a tamperproof device computing $f(r)$ and certifying this computation with the technique of the last section about access control. The verifier has some keys from the authority to verify the certificate. More details will be given in the full paper. Other techniques are possible using some concepts related to zero-knowledge protocols (with only one interaction).

Acknowledgement. The author is most grateful to Andrew Odlyzko and Carl Pomerance for warm encouragements.

References

[1] George Davida and Brian Matt, "*Arbitration in tamper proof systems*", *in* These proceedings, 1987.

[2] Yvo Desmedt and Jean-Jacques Quisquater, "*Public-key systems based on the difficulty of tampering (Is there a difference between DES and RSA?)*, *In* Proceedings of CRYPTO '86, Springer-Verlag, Berlin, 1987.

[3] Adi Shamir, "*Identity-based cryptosystems and signature schemes*", *in* Proceedings of CRYPTO '84, Springer-Verlag, Berlin, 1985, pp. 46-53.

[4] Gustavus J. Simmons, "*The prisoner's problem and the subliminal channel*, *in* Proceedings of CRYPTO '83, Plenum Press, New York, 1984, pp. 51–67.