

# Some trends for future research in distributed cryptography

Research Group on Mathematics Applied to Cryptography \*

Dept. Matemàtica Aplicada IV, Universitat Politècnica de Catalunya

C. Jordi Girona, 1-3, Mòdul C3, Campus Nord, 08034 Barcelona, Spain

<http://www-mat.upc.es/grup-de-cripto/>.

In general, it is not convenient that the security of a system relies on the behaviour of a single agent. Let us consider, for instance, the case of a certification authority, a trusted entity that certifies that a given public key corresponds to a given user. Clearly, a certification authority that is composed by several independent servers is more reliable than one that is formed by a single server.

*Distributed cryptography*, introduced in 1987, makes it possible to design cryptographic systems in which some operations require the collaboration of several users. Concretely, a *distributed cryptosystem* is a public key cryptosystem in which the secret key is shared among a set of users. Only some qualified subsets of users will be able to perform the operation related to the secret key (decrypting or signing). In this way, the security of the system is increased, because the loss or theft of several shares of the secret key does not necessarily break the system's security.

Several distributed cryptosystems have been proposed until now. Most of them have a threshold structure, that is, the sets of users that are able to execute the protocol are those having a certain number of elements. Due to this fact, distributed cryptography is called also in general *threshold cryptography*.

Distributed cryptography is currently a very active research field that is related to many different areas in cryptology. There are several open problems whose solution would lead to the construction of more efficient and versatile distributed cryptosystems. Many of these problems are related to the different cryptographic protocols that are used as pieces of a distributed cryptosystem.

Distributed cryptography is one of the main topics in which the Research Group in Mathematics Applied to Cryptography of the Technical University of Catalonia in Barcelona is currently involved.

We describe next some research subjects that, in our opinion, are important for their implications in the future development of distributed cryptography.

---

\*Professor Paz Morillo is the responsible of the Research Group on Mathematics Applied to Cryptography. The other members of the group are: Jaume Martí-Farré, Carles Padró, Jorge Luis Villar (Associate Professors), Mónica Breitman, Ignacio Gracia, Sebastià Martín, Germán Sáez, Magda Valls (Lecturers), Jorge Jiménez Urroz (Researcher), Vanesa Daza, David Galindo and Javier Herranz (PhD Students).

**Distributed cryptosystems with general structure** Most of the previous work on distributed cryptography and the related protocols has been done on a threshold basis. That is, both the sets of corrupted servers that must be tolerated by the system and the sets that are qualified to perform some action are determined by their cardinality. There exist many situations in which a non-threshold structure is required. Nevertheless, the design of distributed cryptosystems for non-threshold structures depends on some important and difficult problems that remain still unsolved.

**New public key cryptosystems** The efficiency of a distributed cryptosystem strongly depends on the characteristics of the public key cryptosystem on which it is based. Therefore, it is necessary to find new public key cryptosystems that are suitable to be efficiently distributed. For instance, many difficulties appear when using the currently known cryptosystems in the design of distributed cryptosystems for non-threshold structures. Besides, those new public key cryptosystems should fulfill the strongest security requirements.

**Secret sharing schemes** It is clear that secret sharing is a key point in the design of distributed cryptosystems. The optimization of the information rate, both for linear and general secret sharing schemes, is one of the questions that must be studied. Another important problem is to find efficient ways to construct verifiable and proactive secret sharing schemes.

**Multiparty computation** A multiparty computation protocol enables a group of users to jointly perform computations over secret data. They are one of the main components of distributed cryptosystems because in such a system a group of users must jointly decrypt or sign a message while the secret key must remain unknown to every single user. Therefore, the design of distributed cryptosystems with non-threshold access structure is closely related to the problem of performing multiparty computation on general access structures. The key point to solve this problem is to find efficient linear secret sharing schemes with the multiplicative property. Very little is known about multiplicative linear secret sharing schemes, specially if active adversaries are considered.

**Key distribution and key management systems** Whenever a group of users in a network need to securely communicate among them, they must have a common cryptographic key. The distribution of these keys should be jointly done by several servers instead of using a single central server to this end. Therefore, it is important to improve the efficiency of the previously proposed distributed key distribution systems. The amount of information that the servers have to deal with and the verifiability and proactivity of such systems are some important questions to be studied. Another application of distributed cryptosystems are the key escrow systems, which can be used to minimize the effects of the loss of a secret key as well as to provide the government or the court with some control on those keys.