

SOME TRENDS FOR FUTURE RESEARCH IN DISTRIBUTED CRYPTOGRAPHY

Research Group on
Mathematics Applied to Cryptography

Departament de Matemàtica Aplicada IV
Universitat Politècnica de Catalunya

DISTRIBUTED CRYPTOGRAPHY

The secret key is shared

Only some groups of users can decrypt or sign

Useful in some situations: actions requiring the agreement of several people

The security increases

A very active research field

Many open problems related to the protocols that are used in a distributed cryptosystem

DISTRIBUTED CRYPTOSYSTEMS WITH GENERAL ACCESS STRUCTURE

Most distributed cryptosystems until now are threshold cryptosystems

The use of more general access structures is interesting for its applications

Nevertheless, there are important open problems

NEW PUBLIC KEY CRYPTOSYSTEMS

Suitable to be distributed

Strongest security requirements

SECRET SHARING AND MULTIPARTY COMPUTATION

Information rate

Verifiability and proactivity

Multiplicative linear secret sharing schemes

Secret sharing and multiparty computation over
the integers and other rings

KEY DISTRIBUTION AND KEY MANAGEMENT SYSTEMS

Distributed key distribution centers

Verifiability and proactivity

Key escrow systems