Workshop on Fault Diagnosis and Tolerance in Cryptography

Luca Breveglieri
Dipartimento di Elettronica e Informazione
Politecnico di Milano, Milano, Italy - breveglieri@elet.polimi.it

Israel Koren
Department of Electrical and Computer Engineering
University of Massachusetts, Amherst, MA, USA - koren@ecs.umass.edu

Abstract

Cryptographic devices are becoming increasingly ubiquitous and complex, making reliability an important design objective. Moreover, the diffusion of mobile, low-price consumer electronic equipment containing cryptographic components makes them more vulnerable to attack procedures, in particular to those based on injection of faults. This workshop aims at providing researchers in both the dependability and cryptography communities an opportunity to start bridging the gap between fault diagnosis and tolerance techniques, and cryptography.

1. Motivation

In recent years applied cryptography has developed considerably, to satisfy the increasing security requirements of various information technology disciplines, e.g., telecommunication, networking, data base systems and mobile applications. In the past, cryptography relied mainly on a small number of standard crypto-systems (or algorithms), e.g., DES (private key) and RSA (public key). In the last years, however, numerous novel cryptographic systems have been developed, e.g.: AES (Advanced Encryption Standard) as a replacement of DES; the emerging ECC (Elliptic Curve Cryptosystems) technology for wireless network applications, which aims at possibly replacing the widespread RSA; and many others.

Crypto-systems are inherently computationally complex, and in order to satisfy the high throughput requirements of many applications, they are often implemented by means of either VLSI devices (crypto-accelerators) or highly optimized software routines (crypto-libraries) and are used via suitable (network) protocols.

The high complexity of such implementations raises concerns regarding their reliability. Research is therefore needed to develop methodologies and techniques for designing robust cryptographic systems (both hardware and software).

Moreover, new attack procedures are emerging, including those based on injection of faults in order to extract sensitive information (e.g., the secret key). Research is therefore needed to protect cryptographic devices against both accidental faults and intentional intrusions and attacks, in particular those based on malicious injection of faults.

2. Contents

The papers presented in the workshop cover several aspects of the outlined topic, including theoretical research results and practical case studies. In particular, the following aspects are dealt with: modeling the reliability of cryptographic systems; reliable cryptographic systems and algorithms; fault models for cryptographic devices; reliability-based attack procedures on cryptographic devices; adapting classical fault diagnosis and tolerance techniques to cryptography; novel fault diagnosis and tolerance techniques for cryptography; case studies of attacks, fault diagnosis and tolerance techniques in cryptography. The workshop starts with a tutorial reviewing the basics of cryptography and classifying the known attacks.

3. Participation

The speakers at the workshop come from both academia and industry. The workshop's goal is to present the currently available results and challenges, encourage collaboration among the current researchers, and possibly enlarge the community of researchers in this field by advertising this research topic to both the cryptography and fault tolerance research communities.