Invitation à la soutenance publique de thèse
pour l’obtention du doctorat en Sciences de l'Ingénieur

François MACE
Ingénieur civil électricien

Physical Design of Cryptographic Applications:
Constrained Environments and Power Analysis Resistance

Modern cryptography responds to the need for security that has arisen with the emergence of communication appliances. However, its adapted integration in the wide variety of existing communication systems has opened new design challenges. Amongst them, this thesis addresses two in particular, related to hardware integration of cryptographic algorithms: constrained environments and side-channel security.

In the context of constrained environments, we propose to study the interest of the Scalable Encryption Algorithm SEA for constrained hardware applications. We investigate both the FPGA and ASIC contexts and illustrate, using practical implementation results, the interest of this algorithm. Indeed, we demonstrate how hardware implementations can keep its high scalability properties while achieving interesting implementation figures in comparison to conventional algorithms such as the AES.

Next, we deal with three complementary aspects related to side-channel resistance.

We first propose a new class of dynamic and differential logic families achieving low-power performance with matched leakage of information to state-of-the-art countermeasures.

We then discuss a power consumption model for these logic styles and apply it to DyCML implementations. It is based on the use of the isomorphism existing between the gate structures of the implemented functions and the binary decision diagrams describing them. Using this model, we are not only able to predict the power consumption, and therefore attack such implementations, but also to efficiently choose the gate structures achieving the best resistance against this model.

We finally study a methodology for the security evaluation of cryptographic applications all along their design and test phases. We illustrate the interest of such a methodology at different design steps and with different circuit complexity, using either simulations or power consumption measurements.

Membres du jury :
Promoteur : Monsieur J.J. QUISQUATER (ELEC),
Promoteur : Monsieur J.D. LEGAT (DICE),
Monsieur W. FISCHER (Infineon Tech, Allemagne)
Monsieur I. VERBAUWHEDE (KUL)
Monsieur F.-X. STANDAERT (DICE)

Président : Monsieur L. VANDENDORPE (ELEC).

Monsieur J.D. LEGAT, Doyen sera le président de la cérémonie.