Séminaire des doctorants en Théorie des Nombres
"Jouve-Pazuki"

Bordeaux, IMB - Jeudi 28 mars 2013 - Salle conférence- 14h-15h

High-Order Masking by Using Coding Theory

Soline Renner

Since the publication of Side Channel Analysis by Kocher at the end of the 90's, most of cryptosystems proved to be secure in theoretical point of view, become vulnerable against such attacks when implemented in embedded devices such as smart card. Nowadays to guarantee the security of a cryptographic scheme against such attacks, one needs to formally prove its leakage resilience. A relatively recent trend is to apply methods pertaining to the field of multi-party computation: in particular this means applying secret sharing techniques to design masking countermeasures. It is known besides that there is a strong connection between secret sharing schemes and error-correcting codes, namely every linear code gives rise to a (linear) secret sharing scheme. However, the schemes mostly used in practice are the so-called Boolean masking and Shamir's secret sharing scheme and it is widely thought that they are the most adapted to masking techniques because they correspond to so-called MDS codes that are in some sense optimal. In this talk, we will propose alternative masking techniques that rely on non-MDS linear codes: these codes are non-binary but have an underlying binary structure which is that of a self-dual binary code. Their being non-MDS is compensated by the fact that the distributed computation of squares comes at almost no cost. In protecting AES against high-order side channel analysis, this approach is competitive or even more efficient than previous methods, depending on the order.