Power Analysis Resistance of Lattice-based Cryptosystems

Francesco Regazzoni, Felipe Valencia
ALaRI - USI
Lugano, Switzerland

Abstract

The security of cryptographic schemes is based in the difficulty of solving specific mathematical problems. Also, the nature of the basement problems drives some features of the cryptographic primitive implementations, for instance, memory and execution time. Until today, the most well established schemes are based on integer factorization and discrete logarithm problems. This trend is changing because these problems can be solved in polynomial time by quantum computers. Cryptographic schemes based on lattice problems (Lattice-based cryptography) standout because they can not be solved efficiently by quantum computers and its performance is comparable with current cryptosystems (i.e. RSA).

Despite the theoretic security of any cryptographic scheme, for the implementation, it is necessary to take into account physical attacks, which are attacks that take advantage of the implementation vulnerabilities, overpassing the mathematical hardness. These attacks can recover the secret information exploiting the correlation of physical variables - such as power, time and electromagnetic radiation - with the processed data. To destroy this correlation hiding and masking techniques are applied but it implies an overhead in the resource consumption. In this talk we will summarize state of the art protection against power analysis for lattice based cryptography and we will highlight potential research directions.