Side-channel Information Leakage of the Syndrome Computation in Code-Based Cryptography
(Work in progress)

Tania Richmond¹,₄, Benoît Gérard²,₄, Annelie Heuser³,₄ and Axel Legay¹,₄

¹ Inria Rennes - Bretagne Atlantique, France
² DGA.MI, France
³ CNRS, France
⁴ IRISA, Rennes, France

Abstract. Public-key cryptography (PKC) used in practical real-world application is about to change. The nowadays used PKC schemes based on number theory (like integer factorization or discrete logarithm problems) will not be secure in the quantum area [Sho97]. However, recently proposed schemes are based on problems for which no classical or quantum algorithm exist to solve them in polynomial time. So-called post-quantum cryptography (PQC) is mainly classified into code-based cryptography (CBC), lattices-, hash-, multivariate- and isogeny-based cryptography.

In this work we focus on CBC. The first PKC based on error-correcting codes was proposed by McEliece in 1978 using binary Goppa codes [McE78]. A dual version was then proposed by Niederreiter in 1986 using generalized Reed-Solomon (GRS) codes [Nie86]. Since then, many variants using different families of codes were proposed until 2013. But, all including GRS codes except two were cryptanalyzed because they are too structured. The first exception is for QC-MDPC codes, proposed by Misoczki et al. in [MTSB13]. The second one is for LRPC codes, proposed by Gaborit et al. in [GMRZ13]. LRPC codes are equivalent in Rank metric to QC-MDPC codes in Hamming metric.

Considering Hamming metric, there is always a syndrome computation to do regardless the chosen code. There are different possible methods to compute the syndrome:
- vector-matrix product;
- Fast Fourier Transform (FFT) [Choi77];
- XOR of rotations [Choi16];
- multiplications in a polynomial ring;
- lookup table (and additions) [BS08].

Depending on the chosen method, particular information leakage appears. In this work, we analyze the side-channel resilience of each method. The current state-of-the-art in side-channel analysis of the syndrome computation is given in Table 1.

Keywords: Code-based cryptography, side-channel analysis, syndrome computation
Methods | Attacks
--- | ---
vector-matrix product | [HMP10][PRD⁺15][PRD⁺16]
Fast Fourier Transform (FFT) |  
XOR of rotations | [RHM17]
multiplications in a polynomial ring |  
lookup table (and additions) |  

Table 1: SCAs of the syndrome computation

References


