DANIEL PANARIO, Carleton University

Towards constant-time probabilistic root finding for code-based cryptography

In code-based cryptography, deterministic algorithms are used in the root-finding step of the decryption process. However, probabilistic algorithms are, in general, more time efficient than deterministic ones for large fields. These algorithms can be useful for long-term security where larger parameters are relevant. Still, current probabilistic root-finding algorithms suffer from time variations making them susceptible to timing side-channel attacks. To prevent these attacks, we propose a countermeasure to a probabilistic root-finding algorithm so that its execution time does not depend on the degree of the input polynomial but on the cryptosystem parameters. We compare the performance of our proposed algorithm to other root-finding algorithms already used in code-based cryptography. In general, our method is faster than the straightforward algorithm in Classic McEliece. The results also show the range of degrees in larger finite fields where our proposed algorithm is faster than the Additive Fast Fourier Transform algorithm also used in code-based cryptosystems.

Joint work with Dunia Marchiori, Ricardo Custodio and Lucia Moura.