Masking Falcon Gaussian Sampler

Justine PAILLET

Hensoldt France SAS, Plaisir, France

Université Jean-Monnet Saint-Étienne, CNRS, Institut d'Optique Graduate School, Laboratoire Hubert Curien UMR 5516, F-42023, Saint-Étienne, France

Abstract

In the domain of cryptographic implementations, integer arithmetic is widely used because of its simplicity and efficiency. In the late 1990s, a countermeasure against side-channel attacks was introduced: masking. It involves randomly splitting sensitive data into multiple shares to mitigate most forms of leakage. Over the past 25 years, these techniques have improved significantly and have been extensively studied. They are now well-established in the field. Arithmetic and Boolean masking are the two most prominent examples and are particularly well suited to integers, in contrast to floating-point numbers. In 2023, Falcon was selected as a third-round finalist in the NIST post-quantum standardization process, and its main remaining challenge lies in the secure handling of floating point arithmetic.

This presentation focuses on the application of Boolean and arithmetic masking to floating-point numbers and to the Falcon signature scheme. It begins by analyzing key floating point operations—addition, multiplication, inversion, and the floor function—and explores how masking techniques can be applied in this context.

Building on the approach first proposed by Keng-Yu Chen and Jiun-Peng Chen in 2024, involving conversions between Boolean and arithmetic masking, this work also proposes a full implementation of the masking of Falcon's Gaussian Sampler.