Hardware Accelerated Post Quantum Cryptography

Graduate

Michael Schmid

Introduction: In the last decade, there has been a lot of research on quantum computers. Quantum computers are using quantum mechanical phenomena to solve various mathematical problems that are infeasible for traditional computers. In theory, those quantum computers could break many of the standard public key cryptosystems we are using today. This would compromise the confidentiality and integrity of nearly every form of digital communication. Post quantum cryptography is the term used for cryptographic algorithms which are resistant against attacks for both quantum and conventional computers. Small quantum computers are working in a non-commercial research environment, but to successfully attack cryptosystems, much larger quantum computers will need to be built. It is almost impossible to predict exactly when such quantum computers will be available. But it is considered certain that they will come one day.

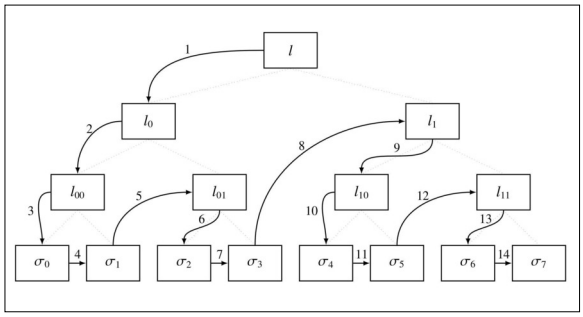
The National Institute of Standards and Technology of the United States of America (NIST) began the process of standardizing post-quantum cryptography in 2017. After three rounds, the first algorithms were selected for standardization in July 2022.

The hardware acceleration with Field Programmable Gate Arrays (FPGAs) has been done for all algorithms but one, namely Fast-Fourier Lattice-based Compact Signatures over NTRU (Falcon). For Falcon, only the signature verification has been accelerated. Due to the use of floating point operation and recursive functions the acceleration of the key generation and signature generation is still missing.

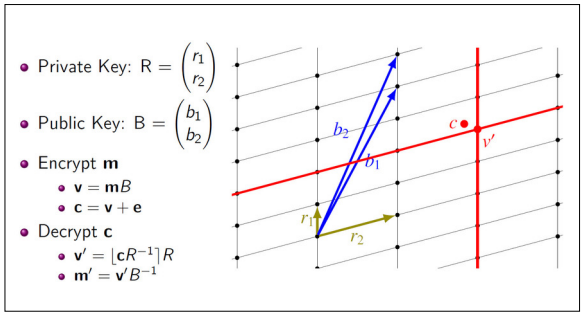
Approach: After a deeper understanding of the theory of the Falcon algorithm, the implementation on an FPGA could be started. For the implementation, the High Level Synthesis (HLS) was preferred over a traditional Hardware Description Language (HDL) like Verilog or Very High Speed Integrated Circuit Hardware Description Language (VHDL). The reference Implementation of the algorithm was written in the programming language C. HLS takes C code and translates into a Register Transfer Level (RTL) hardware description, therefore the reference implementation is directly used in HLS. Many minor modifications to the code had to be done in order to be compliant with HLS. The biggest and obvious changes were to rewrite all recursive functions into an iterative version.

Conclusion: All important parts of the Falcon algorithm could be implemented successfully on the FPGA. To the best of my knowledge, key generation and signature generation were implemented on an FPGA for the first time in this work. Due to the time-consuming implementation of such a large algorithm with HLS, there was not enough time for the originally planned optimizations for an FPGA. Therefore, further optimizations are necessary to improve both hardware utilization and performance.

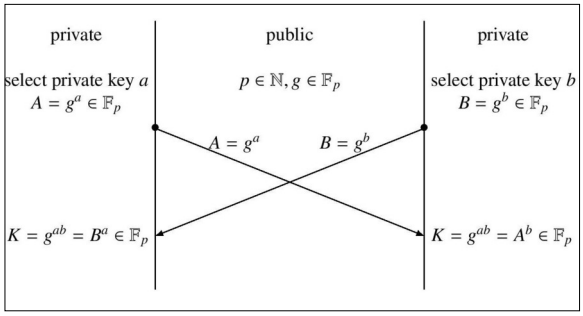
A faclon tree with its traversal. This was implemented with recursion and had to be rewritten into an iterative version.
Own presentment



The Goldreich-Goldwasser-Halevi lattice-based cryptosystem visualized in two dimensions.
Own presentment



Today's standard: Diffe-Hellman key exchange. This system could be attacked by a quantum computer.
Own presentment



Advisor
Prof. Dr. Paul Zbinden

Co-Examiner
Prof. Wei Tao, University of Rhode Island, College of Engineering, West Kingston

Subject Area
Electrical Engineering