Post-Quantum Cryptography on FPGAs: The Niederreiter Cryptosystem

Extended Abstract

Wen Wang
Yale University
New Haven, CT, USA
wen.wang.ww349@yale.edu

Jakub Szefer
Yale University
New Haven, CT, USA
jakub.szefer@yale.edu

Ruben Niederhagen
Fraunhofer SIT
Darmstadt, Germany
ruben@polycephaly.org

ABSTRACT

Our invited presentation will give an introduction to major hardware building blocks needed to implement code-based cryptographic systems. We will present details of a modern, FPGA-based, constant-time implementation of the Niederreiter cryptosystem using binary Goppa codes, including modules for encryption, decryption, and key generation. The presentation will also include a brief summary of other existing implementations of code-based cryptographic systems and it will present research challenges for implementing such systems efficiently.

Currently, there are five promising classes of post-quantum cryptographic algorithms: hash-based, code-based, lattice-based, multivariate, and isogeny-based cryptography. Our work focuses on code-base cryptography, specifically the Niederreiter cryptosystem using binary Goppa codes. The main design challenge within code-based cryptosystems is the tension between cryptographic parameters (i.e., security level) and practical aspects, e.g., the size of keys and computation speed, resulting from the chosen parameters.

The core of the presentation will focus on the FPGA implementation of our binary Goppa code-based Niederreiter cryptosystem, including modules for encryption, decryption, and key generation [2, 3]. We will show how to make the design constant-time in order to protect against timing side-channel analysis and how to make the design fully parameterized in order to support a wide range of parameter choices for security, including binary field size, the degree of the Goppa polynomial, and the code length. The parameterized design also allows users to choose design parameters for time-area trade-offs in order to support a large variety of applications ranging from smart cards to server accelerators. For parameters that are considered to provide "128-bit post-quantum security" (i.e., the cost of an attack on a quantum computer is assumed to be at least 2^{128} quantum operations), our time-optimized implementation requires 966,400 cycles for the generation of both public and private portions of a key and 14,291 cycles to decrypt a ciphertext. The time-optimized design uses only 121,806 ALMs (52% of the available logic) and 961 RAM blocks (38% of the available memory), and results in a design that runs at about 250 MHz on a medium-size Stratix V FPGA (5SGXEA7N).

To achieve this efficient design, a number of building blocks were needed: Gaussian systemizers for matrix systemizations [1], Gao-Mateer additive FFT for polynomial evaluations, a merge-sort module for generating uniformly distributed permutations, and a constant-time Berlekamp-Massey module for decoding [2, 3]. Reasons for making these design choices will be covered in the presentation as well.

Given the increasing interest in code-based cryptography, a number of projects have been focusing on the hardware implementation of the Niederreiter cryptosystem. We will present the performance of our entire Niederreiter cryptosystem with "128-bit post-quantum security" and compare our design with other existing FPGA-based implementations. Prior works have not reached the security level of our design, and this presentation will highlight design choices which allow for achieving a high-security design, while maintaining efficiency. Our current work is the fastest design to date, beating prior FPGA work and optimized CPU-based implementations on recent processors. Based on insights from our work, the presentation will show how to design flexible hardware cores that can be easily configured for different security levels and performance targets.

KEYWORDS

Post-Quantum Cryptography, Code-Based Cryptography, Niederreiter Cryptosystem, FPGA, Hardware Implementation.

ACM Reference Format:
Wen Wang, Jakub Szefer, and Ruben Niederhagen. 2018. Post-Quantum Cryptography on FPGAs: The Niederreiter Cryptosystem: Extended Abstract. In *GLSVLSI '18: 2018 Great Lakes Symposium on VLSI, May 23–25, 2018, Chicago, IL, USA.* ACM, New York, NY, USA, 1 page. https://doi.org/10.1145/3194554.3194617

ACKNOWLEDGMENTS

This work was supported in part by United States' National Science Foundation grant 1716541.

REFERENCES

[1] Wen Wang, Jakub Szefer, and Ruben Niederhagen. 2016. Solving Large Systems of Linear Equations over GF(2) on FPGAs. In *Reconfigurable Computing and FPGAs – ReConFig 2016.* IEEE, 1–7.
[2] Wen Wang, Jakub Szefer, and Ruben Niederhagen. 2017. FPGA-based Key Generator for the Niederreiter Cryptosystem Using Binary Goppa Codes. In *CHES 2017 (LNCS)*, Wieland Fischer and Naofumi Homma (Eds.), Vol. 10529. Springer, Heidelberg, 253–274.
[3] Wen Wang, Jakub Szefer, and Ruben Niederhagen. 2018. FPGA-based Niederreiter Cryptosystem using Binary Goppa Codes. In *International Workshop on Post-Quantum Cryptography – PQCrypto 2018.*

GLSVLSI '18, May 23–25, 2018, Chicago, IL, USA

ACM ISBN 978-1-4503-5724-1/18/05…$15.00
https://doi.org/10.1145/3194554.3194617