Full hardware implementation of the Post-Quantum Public-Key Cryptography Scheme Round5

Michal Andrzejczak*, Farnoud Farahmand†, and Kris Gaj†
*Military University of Technology, Warsaw, Poland
{michal.andrzejczak}@wat.edu.pl
†Department of Electrical and Computer Engineering, George Mason University, Fairfax, VA, U.S.A.
{ffarahma, kgaj}@gmu.edu

***Abstract*—We describe a generic high-speed hardware architecture for the lattice-based post-quantum cryptosystem Round5. This architecture supports both public-key encryption (PKE) and a key encapsulation mechanism (KEM). Due to several hardware-friendly features, Round5 can achieve very high performance when implemented in modern FPGAs.**

***Index Terms*—Post-Quantum Cryptography, lattice-based, KEM, polynomial multiplier, FPGA**

I. Introduction

Due to the recent progress in the development of full-scale quantum computers, there is a strong need to develop secure post-quantum cryptography (PQC) standards [1]. In case of similar security strength of multiple candidates, software and hardware performance are likely to break a tie. In this paper, we examine one of the lattice-based PQC candidates – Round5 [2] – from the point of view of its efficiency when implemented in FPGAs. This submission supports a public-key encryption scheme with indistinguishability under chosen-ciphertext attack (IND-CCA PKE) and a key encapsulation mechanism (KEM) with indistinguishability under chosen-plaintext attack (IND-CPA KEM). A total of 18 major parameter sets are described in the specification of Round5 [2]. In this paper, we focus on the implementation and benchmarking of six of them, namely, ring parameter sets without error correction, denoted by R5ND_*_0d.

II. Hardware architecture of Round5

The top-level block diagram of our design is shown in Fig. 1. cSHAKE and *r5_cpa_enc* are used in the implementations of both investigated schemes. AES-GCM is used only by the IND-CCA PKE. cSHAKE is used for seed expansion, and AES-GCM is used as a data encapsulation mechanism (DEM).

The block diagram of the datapath of *r5_cpa_enc* is shown in Fig. 2. The controller selects proper input and output values for functions computed in arithmetic units: Poly_Mul and Rounding. The degree of the polynomials and the coefficient bit lengths are determined by the parameter set, which is selected during the synthesis time.

The most time-consuming operation of Round5 is polynomial multiplication, which is used twice in encryption and once in decryption. Before this multiplication begins, one of the input polynomials must be lifted to the proper polynomial ring. The result is unlifted back to the original ring. The NTRU polynomial multiplier (NTRU_Poly_Mul) is the biggest module in terms of logic requirements. This module also offers the highest acceleration in terms of the total execution time, compared to the software implementations.

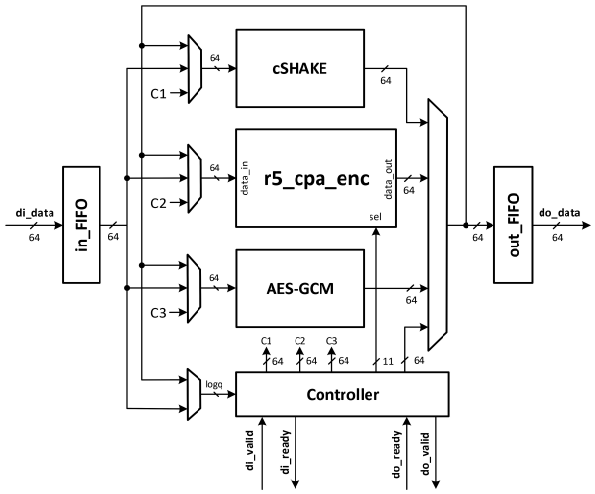

Fig. 1. Top-level block diagram of Round5

Multiplication in Round5 is simplified by always using a ternary polynomial as one of its arguments. In such polynomials, coefficients have only values from the set $\{-1, 0, 1\}$. As a result, the entire multiplication can be performed very efficiently using additions and subtractions.

III. Results

Taking into account our optimization goal – high-speed, differences among FPGA families, and the availability of general-purpose development boards supporting specific FPGAs, we decided to generate results for the high-performance Xilinx Virtex UltraScale XCVU440-FLGA2892-3-e FPGA device, manufactured in the 20 nm technology. The results for the IND-CPA KEM and the IND-CCA PKE are shown in Table I. For PKE, the size of the message is assumed to be 128 bits.

Our design can perform fast computations for both types of schemes. The total execution time varies between 5.5μs and 36.4μs. For the IND-CPA KEM, it is longer for encapsulation, which requires one more multiplication than decapsulation. For the IND-CCA PKE, it is longer for decryption due to

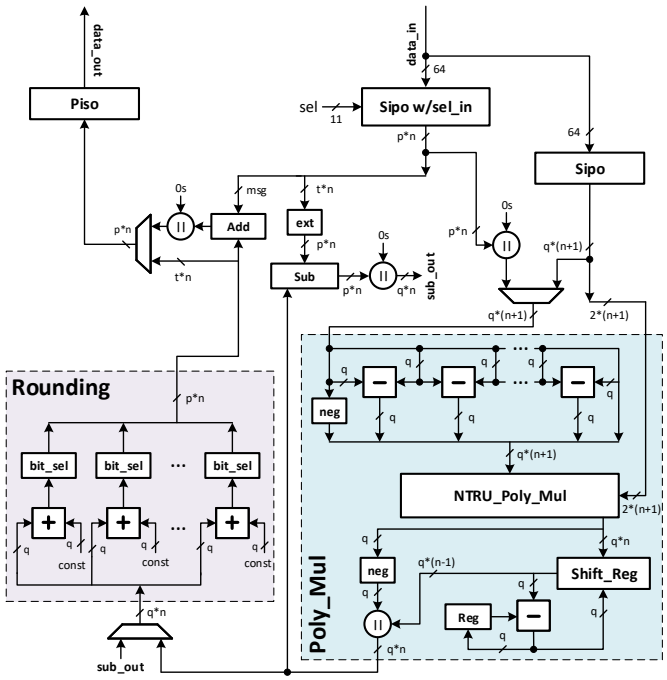

Fig. 2. Block diagram of the datapath of r5_cpa_enc. q, p, and t represent $log_2(q)$, $log_2(p)$ and $log_2(t)$, respectively.

the Round5 construction. The IND-CCA PKE uses KEM, and its decryption requires both encapsulation and decapsulation, while in encryption, only the encapsulation is performed. The design area is greater for the IND-CCA PKE than for IND-CPA KEM, because of the need for the AES-GCM unit. The number of LUTs increases quite substantially with the increase in security level, reaching about 102,000 for the PKE at the security level 5. Most of the area is used by the polynomial multiplier. Despite many multiplications in Round5, the proposed design does not require (and cannot take advantage of) any DSP blocks.

IV. Conclusions

From the hardware perspective, Round5 has many advantages. Its major operations are easy to implement efficiently in hardware. All used moduli are powers of two, so the modular reduction does not require any additional logic. The polynomial multiplication can be performed using a simple addition or subtraction due to the ternary form of one of the input polynomials. These two factors have a significant impact on logic requirements and overall performance. Taking into account all the aforementioned factors, Round5 seems to be a good candidate for a hardware-efficient post-quantum cryptosystem.

References

[1] "Post-Quantum Cryptography Standardization," 2019. [Online]. Available: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Post-Quantum-Cryptography-Standardization

[2] Round5 Submission Team, "Round 2 Submissions - Round5 candidate submission package," Apr. 2019. [Online]. Available: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-2-Submissions

TABLE I
Results obtained for the IND-CPA KEM and the IND-CCA PKE. * — in bytes; ** — in clock cycles. Enc denotes Encapsulation for KEM, and Encryption for PKE. Dec denotes Decapsulation for KEM, and Decryption for PKE. Other notation: PK - Public Key, SK - Secret Key, CT - Ciphertext.

Parameter	*IND-CPA KEM*	*IND-CCA PKE*
Security level: 1		
Parameter set	R5ND_1KEM_0d	R5ND_1PKE_0d
PK size*	634	676
SK size*	16	708
CT size*	682	754
Enc latency**	2,994	3,110
Dec latency**	1,488	4,120
LUTs	45,451	55,442
Slices	10,032	14,307
BRAMs	2	3
Max freq.	260 MHz	260 MHz
Enc time	11.5 μs	11.9 μs
Dec time	5.5 μs	15.8 μs
Security level: 3		
Parameter set	R5ND_3KEM_0d	R5ND_3PKE_0d
PK size*	909	983
SK size*	24	1,031
CT size*	981	1,119
Enc latency**	3,817	4,406
Dec latency**	1,909	5,856
LUTs	66,413	73,881
Slices	12,985	14,307
BRAMs	2	3
Max freq.	240 MHz	249 MHz
Enc time	15.9 μs	17.6 μs
Dec time	7.9 μs	23.5 μs
Security level: 5		
Parameter set	R5ND_5KEM_0d	R5ND_5PKE_0d
PK size*	1,176	1,349
SK size*	32	1,413
CT size*	1,274	1,525
Enc latency**	5,040	6,040
Dec latency**	2,458	8,016
LUTs	98,063	102,092
Slices	17,561	18,167
BRAMs	2	3
Max freq.	220 MHz	220 MHz
Enc time	22.9 μs	27.4 μs
Dec time	11.1 μs	36.4 μs