DESIGN OF FINITE FIELD MULTIPLIERS WITH CRC-BASED ERROR DETECTION CONSTRUCTIONS IN CRYPTOGRAPHY APPLICATIONS

[1] YALAGANDHULA EESWARASAI, [2] Mr. G. BABU
[1]PG Scholar, Dept.of ECE, Vaagdevi College of Engineering, Warangal, Telangana, India.
[2] Assistant professor, Dept.of ECE, Vaagdevi College of Engineering, Warangal, Telangana, India.
[1] eeswarasaiy@gmail.com, [2] babugundlapally@gmail.com

***Abstract*—** In this paper Finite-field multiplication has received prominent attention in the literature with applications in cryptography and error-detecting codes. For many cryptographic algorithms, this arithmetic operation is a complex, costly, and time-consuming task that may require millions of gates. In this work, we propose efficient hardware architectures based on cyclic redundancy check (CRC) as error-detection schemes for post quantum cryptography (PQC) with case studies for the Luov cryptographic algorithm. Luov was submitted for the National Institute of Standards and Technology (NIST) PQC standardization competition and was advanced to the second round. The CRC polynomials selected are in-line with the required error-detection capabilities and with the field sizes as well. We have developed verification codes through which software implementations of the proposed schemes are performed to verify the derivations of the formulations. Additionally, hardware implementations of the original multipliers with the proposed error-detection schemes are performed over a Xilinx field-programmable gate array (FPGA), verifying that the proposed schemes achieve high error coverage with acceptable overhead.

***Keywords*—** Cyclic redundancy check (CRC), fault detection, field-programmable gate array (FPGA), finite-field multiplication.

I. INTRODUCTION

Many modern, sensitive applications and systems use finite-field operations in their schemes, among which finite-field multiplication has received prominent attention. Finite-field multipliers perform multiplication modulo, an irreducible polynomial used to define the finite field. For post quantum cryptography (PQC), the inputs can be very large, and the finite-field multipliers may require millions of logic gates. Therefore, it is a complex task to implement such architectures resilient to natural and malicious faults; consequently, research has focused on ways to eliminate errors and obtain more reliability with acceptable overhead [1]–[6]. Moreover, there has been previous work on countering fault attacks and providing reliability for PQC. Sarker et al. [7] used error-detection schemes of number theoretic transform (NTT) to detect both permanent and transient faults. Mozaffari-Kermani et al. [8] performed fault detection for stateless hash-based PQC signatures. Additionally, error-detection hash trees for stateless hash-based signatures are proposed in [9] to make such schemes more reliable against natural faults and help protecting them against malicious faults. In [10], algorithm-oblivious constructions are proposed through recomputing with swapped cipher text and additional authenticated blocks, which can be applied to the Galois counter mode (GCM) architectures using different finite-field multipliers in G F(2128). Several countermeasures based on error-detection checksum codes and spatial/temporal redundancies for the NTRU encryption algorithm have been presented in [11].

Our proposed error-detection architectures are adapted to the Luov cryptographic algorithm [12]; however, they can be applied to different PQC algorithms that use finite-field multipliers. The Luov algorithm was submitted for National Institute of Standards and Technology (NIST) standardization competition [13] and was advanced to the second round [14]. Cyclic redundancy check (CRC) error-detection schemes are applied in our proposed hardware constructions to make sure that they are overhead-aware with high error coverage. Our contributions in this brief are summarized as follows.

1) Error-detection schemes for the finite-field multipliers G F(2m) with m > 1 used in the Luov cryptographic algorithm are proposed. These error-detection architectures are based on CRC-5. Additionally, we explore and study both primitive and standardized generator

polynomials for CRC-5, comparing their complexity.

2) We derive new formulations for the error-detection schemes of Luov's algorithm, performing software implementations for the sake of verifications. We note that such derivation covers a wide range of applications and security levels. Nevertheless, the presented schemes are not confined to these case studies.

3) The proposed error-detection architectures are embedded into the original finite-field multipliers. We perform the implementations using Xilinx field-programmable gate array (FPGA) family Kintex Ultrascale+ for device xcku5p-ffvd900-1-i to confirm that the schemes are overhead-aware and that they provide high error coverage.

II. RELATED WORK

a) Reliable hardware architectures for the third-round sha-3 finalist grostl benchmarked on fpga platform:

The third round of competition for the SHA-3 candidates is ongoing to select the winning function in 2012. Although much attention has been devoted to the performance and security of these candidates, the approaches for increasing their reliability have not been presented to date. In this paper, for the first time, we propose a high-performance scheme for fault detection of the SHA-3 round-three candidate Grostl which is inspired by the Advanced Encryption Standard (AES). We propose a low-overhead fault detection scheme by presenting closed formulations for the predicted signatures of different transformations of this SHA-3 third-round finalist. These signatures are derived to achieve low overhead and include one or multi-bit parities and byte/word-wide predicted signatures. The proposed reliable hardware architectures for Grostl are implemented on Xilinx Virtex-6 FPGA family to benchmark their hardware and timing characteristics. The results of our evaluations show high error coverage and acceptable overhead for the proposed scheme.

b) Reliable hardware architectures for cryptographic block ciphers led and height:

Cryptographic architectures provide different security properties to sensitive usage models. However, unless reliability of architectures is guaranteed, such security properties can be undermined through natural or malicious faults. In this paper, two underlying block ciphers which can be used in authenticated encryption algorithms are considered, i.e., light encryption device and high security and lightweight block ciphers. The former is of the Advanced Encryption Standard type and has been considered area-efficient, while the latter constitutes a Feistel network structure and is suitable for low-complexity and low-power embedded security applications. In this paper, we propose efficient error detection architectures including variants of recomputing with encoded operands and signature-based schemes to detect both transient and permanent faults. Authenticated encryption is applied in cryptography to provide confidentiality, integrity, and authenticity simultaneously to the message sent in a communication channel. In this paper, we show that the proposed schemes are applicable to the case study of simple lightweight CFB for providing authenticated encryption with associated data. The error simulations are performed using Xilinx Integrated Synthesis Environment tool and the results are benchmarked for the Xilinx FPGA family Virtex-7 to assess the reliability capability and efficiency of the proposed architectures.

III. CYCLIC REDUNDANCY CHECK

The cyclic redundancy check, or CRC, is a technique for detecting errors in digital data, but not for making corrections when errors are detected. It is used primarily in data transmission. In the CRC method, a certain number of check bits, often called a checksum, are appended to the message being transmitted. The receiver can determine whether or not the check bits agree with the data, to ascertain with a certain degree of probability whether or not an error occurred in transmission. If an error occurred, the receiver sends a "negative acknowledgement" (NAK) back to the sender, requesting that the message be retransmitted.

The technique is also sometimes applied to data storage devices, such as a disk drive. In this situation each block on the disk would have check bits, and the hardware might automatically initiate a reread of the block when an error is detected, or it might report the error to software.

The material that follows speaks in terms of a "sender" and a "receiver" of a "message," but it should be understood that it applies to storage writing and reading as well.

IV. PROPOSED SYSTEM

The proposed system are five popular PQC algorithm classes: code-based, hash-based, isogeny-based, lattice-based, and multivariate-quadratic equation-based cryptosystems [15]. Code-based cryptography differs from others in that its security relies on the hardness of decoding in a linear error-correcting code. Hash-based cryptography creates signature algorithms based on the security of a selected cryptographic hash function. The security of isogeny-based cryptography is based on the hard problem to find an isogeny between two given super singular elliptic curves. Lattice-based cryptography is capable of creating a public-key cryptosystem based on lattices. Lastly, the security of multivariate-quadratic-equation-based cryptography depends on the difficulty of solving a system of multivariate polynomials over a finite field. Such cryptographic schemes use large field sizes to provide the needed security levels.

Luov is a multivariate public key cryptosystem and an adaptation of the unbalanced oil and vinegar (UOV) signature scheme, but there is a restriction on the coefficients of the public key. Instead, the scheme uses two finite fields: one is the binary field of two elements, whereas the other is its extension of degree m. F2 is the binary field and F2m is its extension of degree m. The central map F: Fn 2m → Fo 2m is a quadratic map, where o and v satisfy n = o + v, αi,j,k , βi,k and γk are chosen from the base field F2, and whose components f1,..., fo are in the form f k(x) = v i=1 n j=i αi,j,k xi x j +n i=1 βi,k xi +γk.

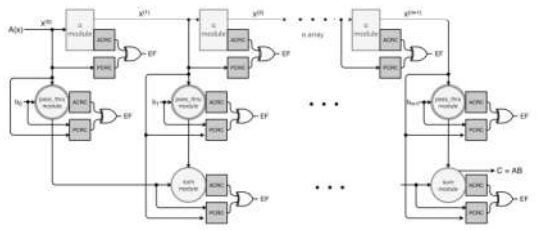

Figure-1: Finite-field multiplier with the proposed error-detection schemes based on CRC

These finite-field multiplications are very complex and require large-area footprint. Therefore, it is a complex task to implement such architectures resilient to natural and malicious faults. The aim of this work is to provide countermeasures against natural faults and fault injections for the finite-field multipliers used in cryptosystems such as the Luov algorithm as a case study, noting that the proposed error-detection schemes can be adapted to other applications and cryptographic algorithms whose building blocks need finite-field multiplications. Readers who are interested in knowing more details about the Luov's cryptographic algorithm are encouraged to refer to [12].

a) Proposed fault-detection architectures

The multiplication of any two elements A and B of G F(2m), following the approach in [16], can be presented as A· B mod f (x) = m−1 i=0 bi · ((Aαi) mod f (x)) = m−1 i=0 bi · X(i), where the set of αi's is the polynomial basis of element A, the set of bi's is the B coefficients, f (x) is the field polynomial, X(i) = α·X(i−1) mod f (x), and X(0) = A. To perform finite-field multiplication, three different modules are needed: sum, α, and pass-thru modules. The sum module adds two elements in G F(2m) using m two-input XOR gates, the α module multiplies an element of G F(2m) by α and then reduces the result modulo f (x), and lastly, the pass-thru module multiplies a G F(2m) element by a G F(2) element. One finite-field multiplication uses a total of m − 1 sum modules, m − 1 α modules, and m pass-thru modules to get the output. Fault injection can occur in any of these modules, and formulations for parity signatures in G F(2m) are derived in [16]. Parity signatures provide an error flag (EF) on each module. The major drawback of parity signatures is that their error coverage is approximately 50%, that is, if the number of faults is even, the approach would not be able to detect the faults. This highly predictable countermeasure can be circumvented by intelligent fault injection.

In this work, our aim is the derivation of error-detection schemes that provide a broader and higher error coverage than parity signatures and explore the application of such schemes to the

Luov algorithm. Thus, we derive and apply CRC signatures [17] to the finite-field multipliers used in Luov algorithm. This would be a step forward toward detecting natural and malicious intelligent faults, especially and as discussed in this brief, considering both primitive and standardized CRCs with different fault multiplicity coverage. CRC was first proposed in 1961 and it is based on the theory

of cyclic error-correcting codes. To implement CRC, a generator polynomial g(x) is required. The message becomes as the dividend, the quotient is discarded, and the remainder produces the result. In CRC, a fixed number of check bits are appended to the data and these check bits are inspected when the output is received to detect any errors. The entire finite-field multiplier with our error-detection schemes is shown in Fig. 1, where actual CRC (ACRC) and predicted CRC (PCRC) stand for ACRC signatures and PCRC signatures, respectively. In Fig. 1, only one EF is shown for clarity; however, for CRC-5, which is the case study proposed in this brief, 5 EFs are computed on each module.

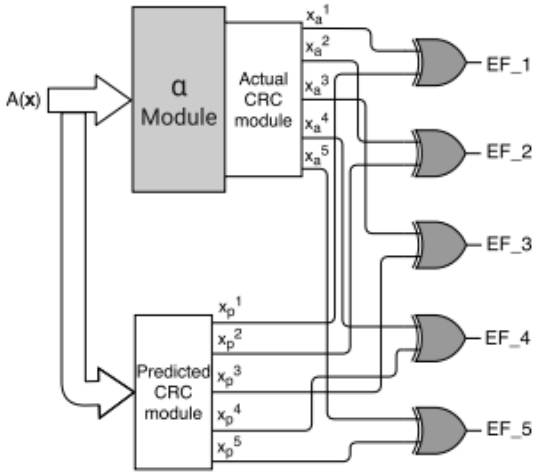

Figure-2: Proposed error-detection constructions for α module.

with its respective one to produce five EFs, which are represented as E F1–E F5. As an example, to obtain E F1, x1 p (or a15 + a13 + a12 + a10 + a9 + a8 + a6 + a4 for g0(x)) is XORed with x1 a (or γ14 + γ13 + γ11 + γ10 + γ9 + γ7 + γ5 + γ0 for g0(x)), which are calculated in (4) and (6), respectively. For our case study, the outputs are divided into five groups since we use CRC-5; however, if any other CRC-n is used, there will be n EFs and the actual and predicted outputs will be divided into n groups. In Table I, the CRC signatures for the different primitive polynomials are shown. We note that the choice of the utilized CRC can be tailored based on the reliability requirements and the overhead to be tolerated. In other words, for applications such as game consoles in which performance is critical (and power consumption is not because these are plugged in), one can increase the size of CRC. However, for deeply embedded systems such as implantable and wearable medical devices, smaller CRC is preferred.

V. RESULTS

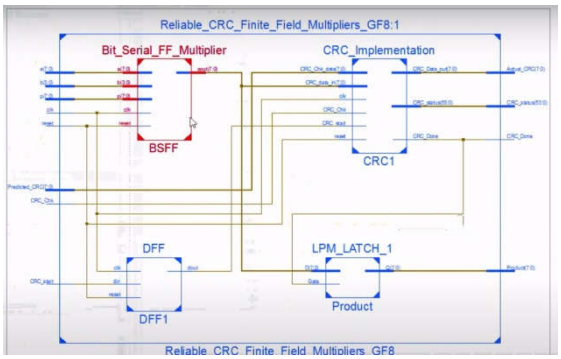

Figure-3: Proposed System

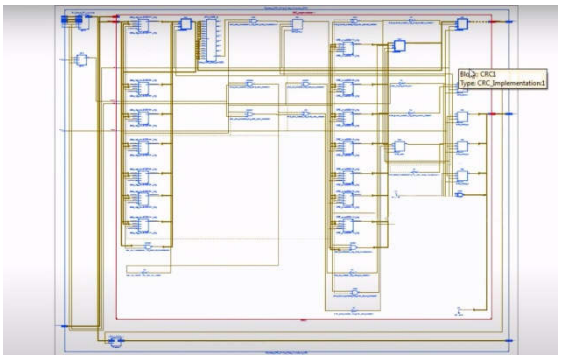

Figure-4: Schematic

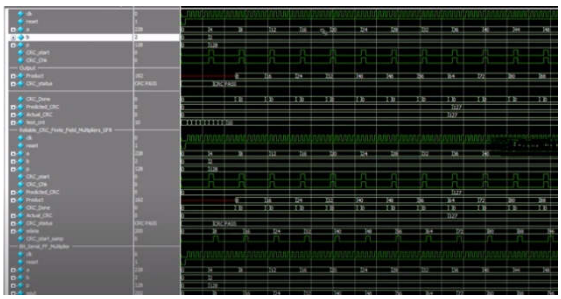

Figure-5: Output Wave forms

Table-1: Device Utilization Summary

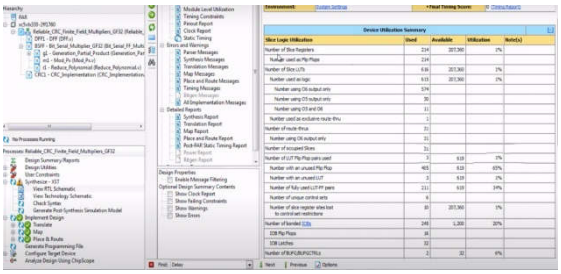

Table-2: Comparison of CRC – Based Error Constructions for Finite Field Multipliers

	Comparisons of Reliable CRC-Based Error Detection Constructions for Finite Field Multipliers	
	GF8 - CRC	GF32 CRC
Number of Slice Registers	56	214
Number of Slice LUTs	140	616
Number of Occupied Slices	43	229
IOBs	113	245
Delay (ns)	3.102	3.665
Power (W)	3.296	3.300

VI. CONCLUSION

In this work, we have derived error-detection schemes for the finite-field multipliers used in post quantum cryptographic algorithms such as Luov, noting that the proposed error-detection schemes can be adapted to other applications and cryptographic algorithms whose building blocks need finite-field multiplications. The error-detection architectures proposed in this work are based on CRC-5 signatures and we have performed software implementations for the sake of verification. Additionally, we have explored and studied both primitive and standardized generator polynomials for CRC-5, comparing the complexity for each of them. We have embedded the proposed error-detection schemes into the original finite-field multipliers of the Luov's algorithm, obtaining high error coverage with acceptable overhead.

REFERENCES

[1] J. L. Danger et al., "On the performance and security of multiplication in G F(2N)," Cryptography, vol. 2, no. 3, pp. 25–46, 2018.

[2] M. Mozaffari-Kermani and A. Reyhani-Masoleh, "Reliable hardware architectures for the third-round SHA-3 finalist Grostl benchmarked on FPGA platform," in Proc. DFT, Oct. 2011, pp. 325–331.

[3] M. Mozaffari-Kermani and A. Reyhani-Masoleh, "A low-cost S-box for the advanced encryption standard using normal basis," in Proc. IEEE Int. Conf. Electro/Inf. Technol., Jun. 2009, pp. 52–55.

[4] M. Yasin, B. Mazumdar, S. S. Ali, and O. Sinanoglu, "Security analysis of logic encryption against the most effective side-channel attack: DPA," in Proc. IEEE Int. Symp. Defect Fault Tolerance VLSI Nanotechnol. Syst. (DFTS), Oct. 2015, pp. 97–102.

[5] M Mozaffari-Kermani, R. Azarderakhsh, A. Sarker, and A. Jalali, "Efficient and reliable error detection architectures of hash-counter-hash tweakable enciphering schemes," ACM Trans. Embedded Comput. Syst., vol. 17, no. 2, pp. 54:1–54:19, May 2018.

[6] M. Mozaffari-Kermani, R. Azarderakhsh, and A. Aghaie, "Reliable and error detection architectures of Pomaranch for false-alarm-sensitive cryptographic applications," IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 23, no. 12, pp. 2804–2812, Dec. 2015.

[7] A. Sarker, M. Mozaffari-Kermani, and R. Azarderakhsh, "Hardware constructions for error detection of number-theoretic transform utilized in secure cryptographic architectures," IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 27, no. 3, pp. 738–741, Mar. 2019.

[8] M. Mozaffari-Kermani, R. Azarderakhsh, and A. Aghaie, "Fault detection architectures for post-quantum cryptographic stateless hash-based secure signatures benchmarked on ASIC," ACM Trans. Embedded Comput. Syst., vol. 16, no. 2, pp. 59:1–59:19, Dec. 2016.

[9] M. Mozaffari-Kermani and R. Azarderakhsh, "Reliable hash trees for post-quantum stateless cryptographic hash-based signatures," in Proc. IEEE Int. Symp. Defect Fault Tolerance VLSI Nanotechnol. Syst. (DFTS), Oct. 2015, pp. 103–108.

[10] M. M. Kermani and R. Azarderakhsh, "Reliable architecture-oblivious error detection schemes for secure cryptographic GCM structures," IEEE Trans. Rel., vol. 68, no. 4, pp. 1347–1355, Dec. 2019.

[11] A. A. Kamal and A. M. Youssef, "Strengthening hardware implementations of NTRUEncrypt against fault analysis attacks," J. Cryptograph. Eng., vol. 3, no. 4, pp. 227–240, Nov. 2013.

[12] A. Kipnis, J. Patarin, and L. Goubin, "Unbalanced oil and vinegar signature schemes," in

Proc. Int. Conf. Theory Appl. Cryptograph. Techn. Berlin, Germany: Springer, 1999, pp. 206–222.

[13] D. Moody, “Post-quantum cryptography: NIST’s plan for the future,” Tech. Rep., Feb. 2016. [Online]. Available: https://csrc.nist.gov/csrc/media/projects/post-quantum-cryptography/documents/pqcrypto-2016-presentation.pdf

[14] D. Moody, “Post-quantum cryptography: Round 2 submissions,” Tech. Rep., Mar. 2019. [Online]. Available: https://csrc.nist.gov/CSRC/media/Presentations/Round-2-of-the-NIST-PQC-Competition-Whatwas-NIST/images-media/pqcrypto-may2019-moody.pdf

[15] D. J. Bernstein, “Post-quantum cryptography,” in Encyclopedia of Cryptography and Security, H. C. A. van Tilborg and S. Jajodia, Eds. Boston, MA, USA: Springer, 2011, pp. 949–950, doi: 10.1007/978-1-4419-5906- 5_386.

[16] A. Reyhani-Masoleh and M. A. Hasan, “Error detection in polynomial basis multipliers over binary extension fields,” in Proc. CHES, 2002, pp. 515–528.

[17] EPC Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz 960 MHz, EPC Global, Brussels, Belgium, Version 1.0.23, 2008.

[18] T. V. Ramabadran and S. S. Gaitonde, “A tutorial on CRC computations,” IEEE Micro, vol. 8, no. 4, pp. 62–75, Aug. 1988.

[19] S. Subramanian, M. Mozaffari-Kermani, R. Azarderakhsh, and M. Nojoumian, “Reliable hardware architectures for cryptographic block ciphers LED and HIGHT,” IEEE Trans. Comput.-Aided Design Integr. Circuits Syst., vol. 36, no. 10, pp. 1750–1758, Oct. 2017.