Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 6, June : 2023

DESIGN OF AN EFFICENT CRC BASED FINITE FIELD MULTIPLIERS USED IN CRYPTOGRAPHY

V.Lakshmk Sraddha[1], M.Surekha

[1]PG Scholar, Dept of ECE, PBR VITS, Kavali, AP, India

[2]Associate Professor, Dept of ECE, PBR VITS, Kavali, AP, India

Abstract

Finite-field multiplication has gotten a lot of attention recently because of its potential use in encryption and error detection codes. Complex, expensive, and time-consuming, it may take millions of gates to perform this arithmetic function in many cryptographic algorithms. With the Luov cryptography algorithm as a case study, we offer efficient equipment important in the design upon cyclic redundancy checks (CRC) error-detection algorithms. Luov made it to the next stage of both the National Institute of Standards & Technology's (NIST) PQC challenge. CRC polynomials have been chosen based on their ability to detect errors as well as their field widths. Software implementations of proposed systems are tested to verify the formulations' derivations using our verification codes. It is further shown that, in hardware implementations of a Xilinx ground gated arrays (FPGA), the suggested error detection algorithms produce high error coverage with acceptable overhead for the original multipliers.

Key words: Cyclic redundancy check (CRC), fault detection, field-programmable gate array (FPGA), finite-field multiplication.

1.Introduction

The standard finite-field multiplication has become an important part of many current and sensitive applications and systems. Multiplying modulo, the irreducible polynomial required to determine the finite field, is performed using finite field multipliers. An infinite-field multiplier may requires billions of logic gates for post quantum cryptography (PQC). Due to the difficulty of developing systems that are impervious to errors caused by both natural and intentional causes, research has concentrated on finding strategies to reduce errors while simultaneously increasing overall system reliability. PQC's reliability and security have already been addressed in past work. NTT-based error-detection techniques were utilised perfectly to identify both long-term and short-term problems. Connectionless hash-based PQC signatures were the focus of a defect detection study by Mozaffari-Kermani et al. To further improve the robustness of stateless hash-based signatures against both natural and intentional errors, a new class of error-detection hash trees has been developed. Recomputing with flipped cipher text and added authentication blocks is used in to suggest algorithm oblivious constructions that can be extended to the Galois cryptography (GCM) designs utilizing alternative finite-field multipliers in. Checksum codes and spatial/temporal

redundancy for the NTRU cryptographic algorithms have been proposed as possible defences. Our proposed error-detection structures are tailored to the Luov encrypting algorithm. These methods can, however, be applied to many PQC algorithms that utilize finite-field multipliers. Luov's algorithm was accepted as a finalist in NIST's standards competition and will now go to the next phase. We use CRC error detection algorithms to ensure that our hardware designs are overhead-aware and have a high level of error coverage. The following is a summary of our work in this brief.

2.Literature survey

Cryptographic hash functions have been extensively studied in the past, see Preneel [8] for an excellent survey. Message Authentication Codes (MACs) have also been thoroughly investigated, see Simmons for a comprehensive review [9]. Security of several types of MACs have been formally evaluated, including HMAC [10], CBC-MAC [11] and XOR-MAC [12]. Unconditionally secure message authentication codes were pioneered by Gilbert et. al. [13] and the theoretical basis was laid by Simmons [14]. The idea of constructing authentication codes through hash functions belongs to Carter and Wegman [15]. They were first to show how to combine hash functions with one-time pads in order to construct strong and efficient authentication algorithms. Their approach was further investigated and refined by Brassed [16], Desmond [17] and Krawczyk [6].

Stinson introduced a formal definition of ”almost strongly universal hash families” [18] which made possible considerably reducing the key length of unconditionally secure MACs. For more details on universal hashing, see his influential paper [19]. Black et al. described how universal hash families can be applied to construct efficient computationally secure MACs, e.g. UMAC [20].

A number of methods for cryptographic checksums and MACs based on stream ciphers were proposed, including Lai et. al. [21], Taylor [22], Johansson [23] and [24]. In these methods, a new representative of a hash family is generated for each message by using the pseudo-random generator of a stream cipher. In our case, as well as in the case of [6], the same hash function can be re-used for multiple messages. Only the random pad which is used for encrypting the hash values has to be updated for each message.

Rabin [25] first proposed the use of CRCs in the cryptographic context, namely for fingerprinting information (where the fingerprint is kept secret). However, his construction does not shift the message by n bit positions before the polynomial division. For this reason, it is nonsecure for message authentication even if the fingerprint is encrypted using a perfect one-time pad. For example, if we complement some of the n least significant bits of the message as well as the corresponding bits in the encrypted authentication tag, such a modification will not be detected by the fingerprint [6].

Krawczyk [6] has shown that, if the multiplication by x n factor is added to Rabin’s scheme [25], then the scheme becomes secure for message authentication

provided that the tag is encrypted using one-time pad. He has also presented another interesting family of hash functions employing Toeplitz hashing where the columns of the matrix are formed from the consecutive states on an LFSR [6]. Such a construction has a bit lower hashing and authentication strength as the construction based on a random matrix, but its implementation cost is considerably smaller.

Apart from using CRCs in cryptographic context, there is another line of work focusing on message authentication codes capable of detecting, correcting or tolerating random errors [26]–[29]. MACs based on BCH and Reed Solomon error-correcting codes have been presented in [26]. Several classes of approximate MACs designed of tolerate a small number of errors in a message have been developed, including [28], [29]. The idea of re-using a cryptographic MAC for detecting random errors in resource-constrained applications, such as Wireless Sensor Networks (WSN), has been proposed in [27].

3.Proposed system

Any two GF(2m) items A and B can be multiplied using the following approach: There are two sets of coefficients in B, one for the A coefficients and the other for B coefficients, and they are called ai and bi. f (x) is indeed the fields polynomial. Each of the summation, _, and pass-thru modules is required in order to carry out finite-field multiplications. The sum module uses m two-input XOR gates to add two GF(2m) elements, the _module multiply a GF(2m) element by and then decreases the output modulo f (x), and the pass-through subsystem multiply a GF(2m) component by a GF(2) component. The entire sum, minus, and pass-thru modules in one finite-field multiplication are used to generate the result. Equations for parity signs in GF(2m) have been derived for all of these modules. The error flag (EF) provided by parity signatures is unique to each module. While parity signatures may be able to detect defects when there are an equal number of them, their error detection is only about half as high as it could be. Intelligent fault injection can get beyond this extremely foreseeable countermeasure. Error detection techniques that span a wider and greater error range than parity signatures are the focus of this research. We will examine the Luov algorithm's use of such schemes in this work, as well. As a result, we have generated and applied CRC signatures to the Luov algorithm's finite-field multipliers. Detection of natural and malevolent intelligent faults would be aided by using both primitive and standardised CRCs with varying fault multiplicity coverage, as stated in this brief. First suggested in 1961, CRC is based on the idea of cyclic error correction codes. g(x) is needed in order to implement CRC. We take a quotient and throw it out; what's left is what we call the dividend. To detect any problems, the output of a CRC algorithm is checked against a set of check bits that are attached to the data. There are two types of CRC signatures: ACRC signatures (ACRC) and PCRC signatures (PCRC) for the full finite-field multiplier using our error detection algorithms. There are only two EFs depicted in this brief because the case

study recommended in this brief uses five EFs for CRC-5.

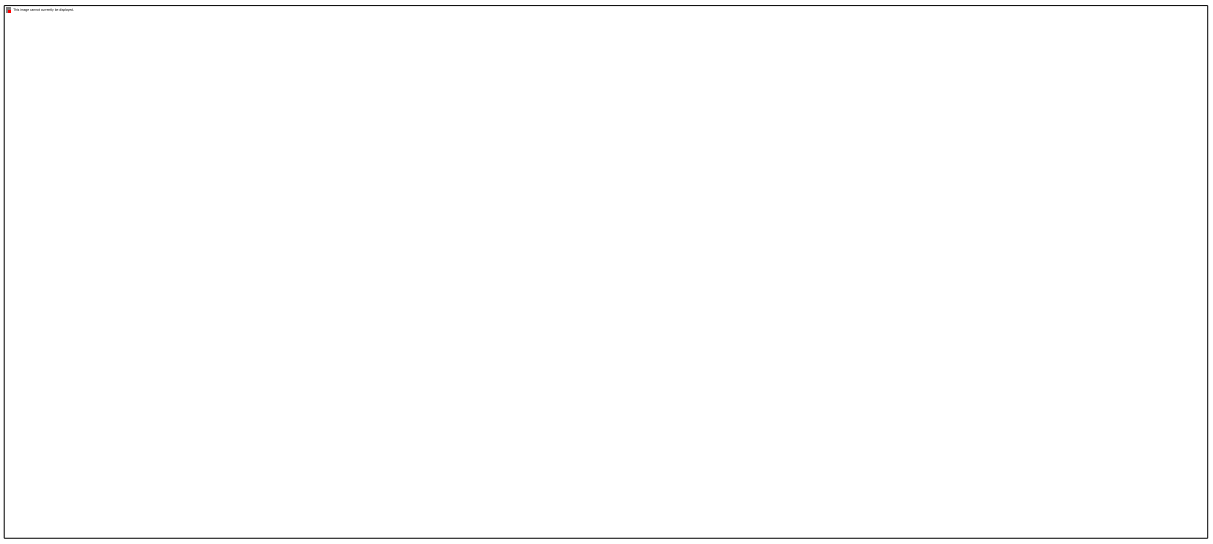

Figure 1: Finite-field multiplier with the proposed error-detection schemes based on CRC.

In order to obtain an efficient CED scheme for the purpose of detecting errors in the output of the finite field multipliers the modular inversion algorithm has been incorporated into the error detecting scheme. This technique has been proved to have better power and area efficiency when compared to the time redundancy scheme. The modular inversion technique also performed in two steps.

The multiplication array block performs bit serial, digit serial or bit parallel multiplication in finite field. The 2-to-1 Mux block selects one of the inputs for multiplication based on the select signal 'S'. The error detection process is performed using the block diagram by multiplying two inputs A(x) and B(x). Instead of modular multiplication in time redundancy technique here modular inversion is used to detect the errors. In this technique also exact error bit position can be detected and it can detect multiple errors.

The data flow for the CED scheme using modular inversion in the block diagram is explained in two steps as follows: During the first step the two inputs (A(x), B(x)) are multiplied using the Montgomery multiplication algorithms (Bit serial, Digit serial or Bit Parallel). The output of the Montgomery multiplication array (C(x)) is further taken as input into the modular inversion block where the inversion algorithm is performed and the output C'(x) is generated.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 6, June : 2023

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

4.Results

Figure 3: Simulation result of the 128 bit encryption

Figure 4: Simulation result of the 128 bit decryption

5.Conclusion

This form of error detection method for the Luov's finite-field multipliers has never been done before, as far as we can find out. In order to make sure that the costs are reasonable, we'll look at several examples. 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. As long as the original architecture can still detect natural or deliberate errors, these degradations are acceptable.

REFERENCES

[1] T.-B. Pei and C. Zukowski, "High-speed parallel CRC circuits in VLSI," IEEE Transactions on Communications, vol. 40, pp. 653 –657, Apr. 1992.

[2] T. Ramabadran and S. Gaitonde, "A tutorial on CRC computations," Micro, IEEE, vol. 8, pp. 62 –75, Aug. 1988.

[3] W. Peterson and D. Brown, "Cyclic codes for error detection," Proceedings of the IRE, vol. 49, pp. 228 –235, Jan. 1961.

[4] S. Golomb, Shift Register Sequences. Aegean Park Press, 1982.

[5] M. Bellare, R. Canetti, and H. Krawczyk, "Keying hash functions for message authentication," in Advances in Cryptology - CRYPTO 96 (N. Koblitz, ed.), vol. 1109 of Lecture Notes in Computer Science, pp. 1–15, Springer Berlin Heidelberg, 1996.

[6] H. Krawczyk, "LFSR-based hashing and authentication," in Proceedings of the 14th Annual International Cryptology Conference on Advances in Cryptology, CRYPTO '94, (London, UK, UK), pp. 129–139, Springer-Verlag, 1994.

[7] S. Gao and D. Panario, "Tests and constructions of irreducible polynomials over finite fields," in Foundations of Computational Mathematics (F. Cucker and M. Shub, eds.), pp. 346–361, Springer Berlin Heidelberg, 1997.

[8] B. Preneel, "The state of cryptographic hash functions," in Lectures on Data Security, Modern Cryptology in Theory and Practice, Summer School, Aarhus, Denmark, July 1998, (London, UK), pp. 158–182, Springer-Verlag, 1999.

[9] G. Simmons, "A survey of information authentication," Proceedings of the IEEE, vol. 76, pp. 603–620, May 1988.

[10] M. Bellare, R. Canetti, and H. Krawczyk, "Keying hash functions for message authentication," in Proceedings of the 16th Annual International Cryptology Conference on Advances in Cryptology, CRYPTO '96, (London, UK), pp. 1–15, Springer-Verlag, 1996.

[11] M. Bellare, J. Kilian, and P. Rogaway, "The security of cipher block chaining," in Advances in Cryptology CRYPTO 94 (Y. Desmedt, ed.), vol. 839 of Lecture Notes in Computer Science, pp. 341–358, Springer Berlin Heidelberg, 1994.

[12] M. Bellare, R. Guerin, and P. Rogaway, "Xor macs: New methods for message authentication using finite pseudorandom functions," in ´ Proceedings of the 15th Annual International Cryptology Conference on Advances in Cryptology, CRYPTO '95, (London, UK, UK), pp. 15–28, Springer-Verlag, 1995.

Author's Profiles

V.LAKSHMI SRADDHA, M. Tech student with Specialization of VLSI DESIGN in PBR Visvodaya Institute Of Technology And Science, Kavali.

M.SUREKHA, Graduate in Electronics & Communication Engg.Later Worked as Asst.Professor in the Dept.of ECE, PBRVITS, Kavali. Currently working as Associate professor in the Dept.of ECE, PBRVITS, kavali.