Response to the Reviews

Title: Efficient Implementations of CRAFT Cipher For Internet of Things

Manuscript Reference Number:
COMPELECENG-D-24-00145

Authors:
Jiahao Xiang
Lang Li

Date: February 20, 2024

Message from the Authors

Dear Editors and Reviewers,

We appreciate your constructive comments, which have significantly enhanced our manuscript. Each comment has been addressed, and your valuable suggestions have been included in the revised manuscript. The manuscript has been updated accordingly. All updates have been colored in blue to distinguish them from the original content.
We have addressed each comment individually in the detailed response that follows. Please note that all page and reference numbers in our response correspond to the revised manuscript, unless stated otherwise. The page and reference numbers in the reviewers' comments remain as they were in the original manuscript. We eagerly await your feedback and hope that our revisions meet your satisfaction.

Sincerely,
Jiahao Xiang and Lang Li.

Response To Reviewer #1

Overall Comments

Good paper. Talk briefly about side channel attacks. Address the comments below for another revision.

Authors Response

We greatly value your detailed feedback and careful review. In response to your suggestions, we have expanded our discussion on side channel attacks. Additionally, we have included relevant references to support this new content.

Reviewer Comment

A) References are not uniformly formatted.

Authors Response

We have meticulously reviewed the .bib file and the references, and made the necessary adjustments to ensure uniform formatting.

Reviewer Comment

B) Please add comparisons in a table (or subsection) so that one could fairly compare your work with similar previous works.

Authors Response

In response, we've conducted a fair comparison with similar previous works, specifically the Iterative architecture of CRAFT proposed in the original paper. We've updated our manuscript to include a description of the three architectures in Table 4, and a comparison in Tables 5-7.

Reviewer Comment

C) Papers related to crypto need to consider this: With the advent of post-quantum cryptography, it is better to add some relevant papers including the followings to make sure you cover that topic too. When PQC replaces ECC/RSA every security application from smart phones to block chains will be affected. So mention about PQC and its threats adding these 4 papers:

**High-performance fault diagnosis schemes for efficient hash algorithm blake, 2019 IEEE 10th Latin American Symposium on Circuits & Systems (LASCAS).

** CRC-oriented error detection architectures of post-quantum cryptography niederreiter key generator on FPGA, 2022 IEEE Nordic Circuits and Systems Conference (NorCAS), 2022.

**Error Detection Schemes Assessed in FPGA for Multipliers in Lattice-Based Key Encapsulation Mechanisms in post-quantum cryptography, IEEE Transactions on Emerging Topics in Computing, 2022.

**Hardware Constructions for Error Detection in WG-29 Stream Cipher Benchmarked on FPGA, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2023, to appear.

Authors Response

As a result, we've addressed the significant topic of post-quantum cryptography in the Introduction section of our revised manuscript. To support this new content, we've also included pertinent references. The detailed revisions are as follows:

In response to these fault attacks, several countermeasures have been suggested. For example, [18] introduced a scheme for error detection. In the realm of Post-Quantum Cryptography, [19] proposed specific error detection methods.

[18] J. Kaur, A. C. Canto, M. M. Kermani, R. Azarderakhsh, Hardware constructions for error detection in wg-29 stream cipher benchmarked on fpga, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (2024) 1-1doi:10.1109/tcad.2023.3338108.

[19] A. C. Canto, A. Sarker, J. Kaur, M. M. Kermani, R. Azarderakhsh, Error detection schemes assessed on fpga for multipliers in lattice-based key encapsulation mechanisms in post-quantum cryptography, IEEE Transactions on Emerging Topics in Computing 11 (3) (2023) 791-797. doi:10.1109/tetc.2022.3217006.

Reviewer Comment

D) Again, any crypto paper needs to address this: Also add some previous works on side-channel attacks and lightweight cryptography or PQC. These attacks are critical when you want to implement your security and privacy usage model, mention these works:

**Education and Research Integration of Emerging Multidisciplinary Medical Devices Security, American Society for Engineering Education (ASEE), 2016.

**Multidisciplinary Approaches and Challenges in Integrating Emerging Medical Devices Security Research and Education, American Society for Engineering Education (ASEE), 2016.

**Fault Detection Schemes for High Performance VLSI Implementations of the Advanced Encryption Standard, The University of Western Ontario, 2007.

Authors Response

In response, we have expanded our discussion to include previous works on side-channel attacks and have added relevant references to support this content. The detailed revisions are as follows:

Differential fault analysis, which is a type of side channel attack, was first introduced by [16]. This concept was later elaborated in more detail by [17]. In response to these fault attacks, several countermeasures have been suggested. For example, [18] introduced a scheme for error detection. In the realm of Post-Quantum Cryptography, [19] proposed specific error detection methods.

[16] E. Biham, A. Shamir, Differential fault analysis of secret key cryptosystems, Springer Berlin Heidelberg, 1997, pp. 513-525. doi:10.1007/bfb0052259.

[17] M. M. Kermani, R. Azarderakhsh, M. Mirakhorli, Multidisciplinary approaches and challenges in integrating emerging medical devices security research and education (2016). doi:10.18260/p.25761.

[18] J. Kaur, A. C. Canto, M. M. Kermani, R. Azarderakhsh, Hardware constructions for error detection in wg-29 stream cipher benchmarked on fpga, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (2024) 1-1doi:10.1109/tcad.2023.3338108.

[19] A. C. Canto, A. Sarker, J. Kaur, M. M. Kermani, R. Azarderakhsh, Error detection schemes assessed on fpga for multipliers in lattice-based key encapsulation mechanisms in post-quantum cryptography, IEEE Transactions on Emerging Topics in Computing 11 (3) (2023) 791-797. doi:10.1109/tetc.2022.3217006.

Reviewer Comment

E) You could add a subsection for Discussions

Authors Response

In response, we have added a Discussions section to improve the quality of our manuscript. The detailed revisions are as follows:

This section discusses the performance of three different architectures of CRAFT: the serial architecture, the unrolled architecture, and the iterative architecture. These architectures are compared and analyzed to determine which one is best suited for different environments.

The serial architecture of CRAFT is designed to minimize area consumption. It has the lowest area consumption among the three architectures, which results in it having the lowest dynamic power. Additionally, it boasts the highest frequency among the three architectures. However, it has a high latency, leading to the lowest maximum throughput among the three architectures. The serial architecture is suitable for resource-limited environments where high throughput is not a requirement.

The unrolled architecture of CRAFT aims to maximize throughput. It boasts the lowest latency among the three architectures, which contributes to its highest maximum throughput, despite having the lowest maximum frequency. This architecture is also energy-efficient, offering the lowest energy per bit among the three architectures. However, it does have the highest area consumption. The unrolled architecture is best suited for environments where high throughput and low energy are priorities, and low area is not a requirement.

The iterative architecture of CRAFT is designed to strike a balance between area consumption and throughput. While it doesn't have the lowest area consumption, the highest frequency, the lowest latency, the highest maximum throughput, or the lowest energy per bit among the three architectures, it does have the highest throughput per slice. The iterative architecture is suitable for environments where moderate throughput is required at the lowest possible area cost.

Reviewer Comment

F) Please add one or more future works for enhancing your presentation

Authors Response

In response, we have included a discussion of potential future work in the Conclusion section to enhance the quality of our manuscript. The detailed revisions are as follows:

Future work could extend the proposed architectures to other lightweight ciphers and examine their performance. Additionally, these lightweight ciphers could be implemented in a way that makes them resistant to side channel attacks.

Reviewer Comment

G) Moreover, some works missing on lightweight cryptography LWC and building blocks. Implementations need to be low-energy and low-power, so it is essential to mention about such efficient ways to pursue with implementations using these 4 references:

** Optimized architectures for elliptic curve cryptography over Curve448, Cryptology ePrint Archive, 2020.

**Reliable architectures for finite field multipliers using cyclic codes on FPGA utilized in classic and post-quantum cryptography, IEEE Transactions on Very Large Scale Integration (VLSI) Systems 31 (1), 2022.

**Work-in-progress: Hyflex hands-on hardware security education during covid-19, 2022 IEEE World Engineering Education Conference (EDUNINE). arXiv preprint arXiv:2306.08178

**Guest Editorial: Introduction to the Special Section on Emerging Security Trends for Biomedical Computations, Devices, and Infrastructures, IEEE/ACM Transactions on Computational Biology and Bioinformatics, 2016.

Authors Response

The similar works we have talk in the introduction, and we have added relevant references to support this content. The detailed contents are as follows:

Lara-Nino et al. [20] introduced a 16-bit datapath architecture for the PRESENT cipher, which resulted in reduced area and power consumption. Similarly, Pandey et al. [21] suggested an optimized key schedule for the same cipher, leading to a smaller area. Shahbazi et al. [22] put forth an 8-bit serial architecture for AES, which also reduces area and power consumption. Li et al. [23] presented unrolled architectures and a low-cost architecture for PRINCE, optimizing both throughput and area separately.

[20] C. A. Lara-Nino, A. Diaz-Perez, M. Morales-Sandoval, Lightweight hardware architectures for the present cipher in FPGA, IEEE Trans. Circuits Syst. I Regul. Pap. 64-I (9) (2017) 2544-2555. doi:10.1109/TCSI.2017.2686783.

[21] J. G. Pandey, T. Goel, A. Karmakar, Hardware architectures for PRESENT block cipher and their FPGA implementations, IET Circuits Devices Syst. 13 (7) (2019) 958-969. doi:10.1049/IET-CDS.2018.5273.

[22] K. Shahbazi, S. Ko, Area-efficient nano-aes implementation for internet-of-things devices, IEEE Trans. Very Large Scale Integr. Syst. 29 (1) (2021) 136-148. doi:10.1109/TVLSI.2020.3033928.

[23] L. Li, J. Feng, B. Liu, Y. Guo, Q. Li, Implementation of PRINCE with resource-efficient structures based on fpgas, Frontiers Inf. Technol. Electron. Eng. 22 (11) (2021) 1505–1516. doi:10.1631/FITEE.2000688.

Reviewer Comment

- With the advent of post-quantum cryptography (PQC), it is better to add some relevant works to make sure you cover that topic too. This is the hottest topic in cryptography now. With PQC, add a paper on each of these six topics separately: (a) Curve448 and Ed448 on Cortex-M4, (b) SIKE on Cortex-M4, (c) SIKE Round 3 on ARM Cortex-M4, (d) Kyber on 64-Bit ARM Cortex-A, (e) Cryptographic accelerators on Ed25519, (f) Supersingular isogeny Diffie-Hellman key exchange on 64-bit ARM.

Authors Response

Our paper's primary focus is on hardware implementation, which is why we did not include the suggested papers on software implementation. In response to your feedback, we have expanded the Introduction section of our revised manuscript. This expansion includes a discussion on post-quantum cryptography, backed by relevant references. The detailed revisions are as follows:

In response to these fault attacks, several countermeasures have been suggested. For example, [18] introduced a scheme for error detection. In the realm of Post-Quantum Cryptography, [19] proposed specific error detection methods.

[18] J. Kaur, A. C. Canto, M. M. Kermani, R. Azarderakhsh, Hardware constructions for error detection in wg-29 stream cipher benchmarked on fpga, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (2024) 1-1doi:10.1109/tcad.2023.3338108.

[19] A. C. Canto, A. Sarker, J. Kaur, M. M. Kermani, R. Azarderakhsh, Error detection schemes assessed on fpga for multipliers in lattice-based key encapsulation mechanisms in post-quantum cryptography, IEEE Transactions on Emerging Topics in Computing 11 (3) (2023) 791-797. doi:10.1109/tetc.2022.3217006.

Reviewer Comment

- NIST lightweight standardization was finalized in Feb. 2023. Also mention fault attacks as side-channel attacks, these topics to explore and add a reference on each of these separately: (a) Error Detection in Lightweight Welch-Gong (WG)-Oriented Streamcipher WAGE, (b) error detection reliable architectures of Camellia block cipher, (c) fault diagnosis of low-energy Midori cipher, (d) block cipher QARMA with error detection mechanisms.

Authors Response

In response, we have broadened our discussion in the Introduction section to include fault attacks as a type of side-channel attack. We've also added relevant references to support this new content. The detailed revisions are as follows:

Differential fault analysis, which is a type of side channel attack, was first introduced by [16]. This concept was later elaborated in more detail by [17]. In response to these fault attacks, several countermeasures have been suggested. For example, [18] introduced a scheme for error detection. In the realm of Post-Quantum Cryptography, [19] proposed specific error detection methods. It's important to note that these methods do increase the hardware consumption of the cipher system. The CRAFT cipher was designed with resistance to fault attacks in mind. However, it currently lacks efficient implementations. To make it suitable for use in more constrained environments, development of more efficient implementations is necessary.

[16] E. Biham, A. Shamir, Differential fault analysis of secret key cryptosystems, Springer Berlin Heidelberg, 1997, pp. 513-525. doi:10.1007/bfb0052259.

[17] M. M. Kermani, R. Azarderakhsh, M. Mirakhorli, Multidisciplinary approaches and challenges in integrating emerging medical devices security research and education (2016). doi:10.18260/p.25761.

[18] J. Kaur, A. C. Canto, M. M. Kermani, R. Azarderakhsh, Hardware constructions for error detection in wg-29 stream cipher benchmarked on fpga, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (2024) 1-1doi:10.1109/tcad.2023.3338108.

[19] A. C. Canto, A. Sarker, J. Kaur, M. M. Kermani, R. Azarderakhsh, Error detection schemes assessed on fpga for multipliers in lattice-based key encapsulation mechanisms in post-

quantum cryptography, IEEE Transactions on Emerging Topics in Computing 11 (3) (2023) 791-797. doi:10.1109/tetc.2022.3217006.

Response To Reviewer #2

Overall Comments

The authors present two serial and unrolled architectures of CRAFT and effectively reduce area resources by optimizing the S-box and Mix-Columns of CRAFT. Overall, the quality of the paper is good.

Response

We are grateful for the reviewer's positive feedback. It serves as a significant motivation for us to enhance the quality of our work.

Response To Reviewer #3

Overall Comments

This work implemented the CRAFT block cipher with two architectures proposed, the Serial architecture and the Unrolled architecture. Then, the efficiency of the implementations is tested on three FPGA platforms. The implementations proposed in this paper are interesting for the practical applications of CRAFT in IoT.

Response

We sincerely appreciate the time and effort you've invested in reviewing our paper. Your valuable suggestions are greatly appreciated and will undoubtedly enhance the quality of our work. In the subsequent section, we will address each of your comments individually.

Reviewer Comment

1. The reference format should be consistent with equations, such as, 'as shown in Equation 1' $->$ 'as shown in Equation (1)'.

Response

We have revised the manuscript to ensure that the reference format is consistent with the equations.

Reviewer Comment

2. The description of IA is not necessary to occupy a single subsection (Subsection 3.3). It is better to move it to Preliminaries. Meanwhile, the comparison between the IA, SA, and UA is not sufficient.

Response

We remove the subsection 3.3 IA and remove it to the Preliminaries (Section 2). We also add the discussion of the comparison between the IA, SA, and UA on the discussion section. The details are as follows:

This section discusses the performance of three different architectures of CRAFT: the serial architecture, the unrolled architecture, and the iterative architecture. These architectures are compared and analyzed to determine which one is best suited for different environments.

The serial architecture of CRAFT is designed to minimize area consumption. It has the lowest area consumption among the three architectures, which results in it having the lowest dynamic power. Additionally, it boasts the highest frequency among the three architectures. However, it has a high latency, leading to the lowest maximum throughput among the three architectures. The serial architecture is suitable for resource-limited environments where high throughput is not a requirement.

The unrolled architecture of CRAFT aims to maximize throughput. It boasts the lowest latency among the three architectures, which contributes to its highest maximum throughput, despite

having the lowest maximum frequency. This architecture is also energy-efficient, offering the lowest energy per bit among the three architectures. However, it does have the highest area consumption. The unrolled architecture is best suited for environments where high throughput and low energy are priorities, and low area is not a requirement.

The iterative architecture of CRAFT is designed to strike a balance between area consumption and throughput. While it doesn't have the lowest area consumption, the highest frequency, the lowest latency, the highest maximum throughput, or the lowest energy per bit among the three architectures, it does have the highest throughput per slice. The iterative architecture is suitable for environments where moderate throughput is required at the lowest possible area cost.

Reviewer Comment

3. The definitions of SA and UA are not explicit, especially the implementation under UA. It is necessary to highlight their innovativeness in relation to previous architectures.

Response

To clarify, we have added the definitions of SA and UA in the headers of Subsections 3.1 and 3.2, respectively. Additionally, we have emphasized their innovative aspects compared to the architectures proposed in the original CRAFT article. The details are as follows:

The purpose of the serial architecture is to reduce the datapath, which represents the number of bits dealt with in one cycle. For instance, the CRAFT cipher has a 64-bit block size, meaning it can process 64-bit data in one cycle when using the iterative architecture. In contrast, the serial architecture reduces the datapath from 64-bit to 4-bit, meaning it can only process 4-bit data in one cycle. Despite this limitation, serial architectures can significantly reduce area usage by reusing components, making them a viable alternative to iterative architectures.

The unrolled architecture allows for the execution of more than one round function in a single cycle. In contrast, the iterative architecture of the CRAFT cipher only runs one round function per cycle. This approach can significantly reduce the latency of the encryption process. It does this by reducing the number of cycles needed to encrypt one block size plaintext, thereby improving the throughput rate.

Reviewer Comment

4. Can CRAFT be implemented under the Iterative architecture? If so, do implementations under UA or SA still have advantages over IA? On the other hand, can UA or SA be applied to other ciphers, such as PRESENT, and bring efficiency improvements?

Response

We have addressed them individually.

1. In response to your query about implementing CRAFT under the Iterative architecture: Yes, the Iterative architecture can indeed be applied to the CRAFT cipher, as suggested in the original CRAFT paper. However, the paper does not provide performance data for FPGA platforms. To address this, we have included the Iterative architecture in our experimental setup, obtained results, and compared these with the SA and UA.

2. On the advantages of the SA and UA over the IA on the CRAFT cipher: The SA and UA still maintain advantages over the IA on the CRAFT cipher.

3. On whether SA and UA can be applied to other ciphers, such as PRESENT, for efficiency improvements: Yes, the SA and UA can be applied to the PRESENT cipher to enhance efficiency. The challenge lies in implementing the architecture within the cipher. For instance, we optimized the Mix-Columns component of CRAFT for the SA, but PRESENT does not have this component. This means the same method cannot be used for PRESENT with the SA. The task ahead of us is to determine how to make the new component of the cipher work with the SA or UA. This includes the non-linear component (e.g., S-box) and the linear component (e.g., Mix-Columns, PermuteNibbles).

We apologize for any misunderstanding. We have conducted a fair comparison of the three architectures on the CRAFT cipher and updated the online repository on GitHub. We have also added a discussion of the comparison between the IA, SA, and UA in the new Section 5: Discussion. We hope this response is satisfactory.

Reviewer Comment

5. It is better to combine the Section 4 with Section 5 in my opinion.

Response

To enhance the readability of the manuscript, we have merged Sections 4 and 5 into a new Section 4 titled "Experiment Results". The previous Section 5 has been transformed into Subsection 4.5.

Reviewer Comment

6. The data in Figure 9-13 is also demonstrated in Table 5-7, one approach is enough to compare the results.

Response

The data from Figures 9-13 is also presented in Tables 5-7. The graphical representation in the figures is considered to provide an intuitive understanding. As a result, both the figures and tables are retained in the manuscript.