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 16, 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. For clarity, 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. Each comment we received is boxed for clarity, with our responses written immediately after. 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

> Reviewer # 1 - Good paper. Talk briefly about side channel attacks. Address the comments below for another revision.

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. We trust that these revisions satisfactorily address your concerns.

Reviewer Comment

> Reviewer # 1.1 - References are not uniformly formatted

Response

We appreciate your feedback. We have meticulously reviewed the .bib file and the references, and made the necessary adjustments to ensure uniform formatting. We believe these revisions adequately address the concerns.

Reviewer Comment

> Reviewer # 1.2 - Please add comparisons in a table (or subsection) so that one could fairly compare your work with similar previous works.

Response

Thank you for your suggestion. In response, we have added a new table in the Results section of our revised manuscript. This table offers a comprehensive comparison between our work and similar previous studies. We trust that this addition effectively addresses your concerns. The detailed revisions are as follows:

add compare table in here

Reviewer Comment

> Reviewer # 1.3 - 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.

Response

We appreciate your feedback. 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. We believe these modifications adequately address your concerns. The detailed revisions are as follows:

To counter these fault attacks, various schemes have been proposed. For instance, [18] proposed a fault diagnosis scheme, while [19] introduced an error detection scheme. Additionally, [20] and [21] have suggested error detection methods specifically for Post-Quantum Cryptography.

[18] M. M. Kermani, S. B. Sarmadi, A. E. Ackie, R. Azarderakhsh, High-performance fault diagnosis schemes for efficient hash algorithm BLAKE, in: R. S. Murphy (Ed.), 10th IEEE Latin American Symposium on Circuits & Systems, LASCAS 2019, Armenia, Colombia, February 24-27, 2019, IEEE, 2019, pp. 201-204. doi:10.1109/LASCAS.2019.8667597.

[19] 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.

[20] A. Cintas-Canto, M. Mozaffari-Kermani, R. Azarderakhsh, K. Gaj, Crc-oriented error detection architectures of post-quantum cryptography niederreiter key generator on fpga (2022). doi:10.1109/norcas57515.2022.9934378.

[21] 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

Reviewer # 1.4 - Again, any crypto paper needs to address this: Also add some previous works on side-channel attacks and lightweight cryptography or PQC.

Response

We appreciate your expert suggestion. In response, we have expanded our discussion to include previous works on side-channel attacks and have added relevant references to support this content. We trust that these modifications adequately address your concerns. The detailed revisions are as follows:

Differential fault analysis, a type of side channel attack, was first proposed by [16] and further discussed in [17]. To counter these fault attacks, various schemes have been proposed. For instance, [18] proposed a fault diagnosis scheme, while [19] introduced an error detection scheme. Additionally, [20] and [21] have suggested error detection methods specifically for Post-Quantum Cryptography.

[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] M. M. Kermani, S. B. Sarmadi, A. E. Ackie, R. Azarderakhsh, High-performance fault diagnosis schemes for efficient hash algorithm BLAKE, in: R. S. Murphy (Ed.), 10th IEEE Latin American Symposium on Circuits & Systems, LASCAS 2019, Armenia, Colombia, February 24-27, 2019, IEEE, 2019, pp. 201-204. doi:10.1109/LASCAS.2019.8667597.

[19] 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.

[20] A. Cintas-Canto, M. Mozaffari-Kermani, R. Azarderakhsh, K. Gaj, Crc-oriented error detection architectures of post-quantum cryptography niederreiter key generator on fpga (2022). doi:10.1109/norcas57515.2022.9934378.

[21] 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

Reviewer # 1.5 - You could add a subsection for Discussions.

Response

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

section of discussion

Reviewer Comment

Reviewer # 1.6 - Please add one or more future works for enhancing your presentation

Response

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

future work, section of discussion

Reviewer Comment

Reviewer # 1.7 - Moreover, some works missing on lightweight cryptography LWC and building blocks.

Response

We value your insightful suggestion. In response, we have included the previously missing implementation work and added the necessary references to support this addition. The detailed revisions are as follows:

In the context of other ciphers, Bisheh Niasar et al. [24] proposed a design for Curve448. Shahbazi et al. [25] put forth an 8-bit serial architecture for AES, which also reduces area and power consumption. Li et al. [26] presented unrolled architectures and a low-cost architecture for PRINCE, optimizing both throughput and area separately. Cintas Canto et al. [27] discussed finite field multipliers using cyclic codes, a technique that can be optimized as all ciphers need finite field multipliers.

[24] M. Bisheh-Niasar, R. Azarderakhsh, M. M. Kermani, Optimized architectures for elliptic curve cryptography over curve448, IACR Cryptol. ePrint Arch. (2020) 1338.

[25] 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.

[26] 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.

[27] A. Cintas-Canto, M. M. Kermani, R. Azarderakhsh, 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) (2023) 157-161. doi:10.1109/tvlsi.2022.3224357.

Reviewer Comment

> Reviewer # 1.8 - 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.

Response

We appreciate your expert suggestion. However, 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. We trust that these modifications adequately address your concerns. The detailed revisions are as follows:

introduction with PQC discussion

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

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

[xx] 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.

[xx] 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.

Reviewer Comment

> Reviewer # 1.9 - 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.

Response

We appreciate your expert suggestion. 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. We believe these modifications adequately address your concerns. The detailed revisions are as follows:

detailed content of SCA in Introduction

Response To Reviewer #2

Overall Comments

> Reviewer # 2 - 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

> Reviewer # 3 - 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

> Reviewer # 3.1 - The reference format should be consistent with equations, such as, ’as shown in Equation 1’ $->$ ’as shown in Equation (1)’.

Response

Thank you for your suggestion. We have revised the manuscript to ensure that the reference format is consistent with the equations.

Reviewer Comment

> Reviewer # 3.2 - 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

todo for Response to Reviewer # 3.2

1. remove subsection 3.3 IA ?
2. add the discussion of the comparison between the IA, SA, and UA on discussion section

---

Reviewer Comment

> Reviewer # 3.3 - The definitions of SA and UA are not explicit, especially the im-

plementation under UA. It is necessary to highlight their innovativeness in relation to previous architectures.

Response

todo for Response to Reviewer # 3.3

in the 3.1 and 3.2 header, we will add the definition of SA and UA, and highlight their innovativeness in relation to previous architectures.

Reviewer Comment

> Reviewer # 3.4 - 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

todo for Response to Reviewer # 3.4, it want a fair compare, give it a reason.

logic answer:

The CRAFT can be implemented under the Iterative architecture, but the UA and SA still have advantages over IA. The UA and SA can also be applied to other ciphers, such as PRESENT, to bring efficiency improvements. However, since different ciphers have different linear and non-linear operations, enabling the new components to work together poses a challenge under a common strategy.

Reviewer Comment

> Reviewer # 3.5 - It is better to combine the Section 4 with Section 5 in my opinion.

Response

todo for Response to Reviewer # 3.5

Combine Section 4 and Section 5 into one section named ”Experiment Results”

Reviewer Comment

> Reviewer # 3.6 - The data in Figure 9-13 is also demonstrated in Table 5-7, one approach is enough to compare the results.

Response

todo for Response to Reviewer # 3.6

add a horizontal comparison Table, not use the Figure 9-13.