Area–Throughput Efficient Implementations of CRAFT Cipher For Internet of Vehicles

Jiahao Xiang[1,2] and Lang Li[1,2*]

[1*]College of Computer Science and Technology, Hengyang Normal University, Hengyang, 421002, China.
[2]Hunan Provincial Key Laboratory of Intelligent Information Processing and Application, Hengyang Normal University, Hengyang, 421002, China.

*Corresponding author(s). E-mail(s): lilang911@126.com;
Contributing authors: simple.xjh@qq.com;

Abstract

Purpose: With extraordinary growth in the Internet of Vehicles (IoV), the amount of data exchanged between IoV devices is growing at an unprecedented scale. Most of the IoV devices need instant response and real-time security to ensure the safety of users. The CRAFT cipher that is a lightweight block cipher for low-area can be used in IoV devices. In order to better adapt to these environment, the objective of this paper is to explore opportunities to optimize area and throughput for CRAFT cipher targeted for low-resource IoV devices. **Methods:** A novel compact CRAFT implementation is proposed in serialized fashion to achieve a small hardware footprint. We propose novel unrolled structure of CRAFT cipher for the high throughput feature. **Results:**The results on Artix-7 show that ... **Conclusion:** Hence, our works let CRAFT cipher more suitable for IoV devices.

Keywords: Lightweight block cipher, Internet of Vehicles, Field-programmable gate array(FPGA), Low-area, High-throughput

1 Introduction

Internet of Vehicles (IoV) is an emerging concept in intelligent transportation systems (ITS) to enhance the existing capabilities of VANETs by integrating with the Internet of Things (IoT) Sharma S (2019). As IoT technology continues to advance, IoV technology is also making great progress. But the same security issues that exist in IoT are also were introduced into IoV. At the some time, IoV involves a huge amount of dynamic real-time critical data so its security is a major concern.

Lightweight cryptography is a subfield of cryptography that aims to provide solutions tailored for resource-constrained devices Bassham L (2018). It can provides security with low resource consumption and low delay in IoV environment.

In this work, we propose the three architectures of FPGA implementations for the CRAFT Beierle C (2019), respectively Round based, Serial, and Loop unrolled. This allows IoV practitioners to select the architectures that best suit their needs. The contributions of this article can be summarized as follows.

1..... The rest of this article is organized as follows. Section 2 presents specification of CRAFT; the proposed the three architectures of FPGA implementations for the CRAFT are present in Section 3; Section 4 presents the implementation results, analysis, and comparison with other similar works; finally, the work is concluded in Section 5.

References

Bassham L MK (2018) Submission requirements and evaluation criteria for the lightweight cryptography standardization process. US National Institute of Standards and Technology

Beierle C MALeander G (2019) Craft: lightweight tweakable block cipher with efficient protection against dfa attacks. IACR Transactions on Symmetric Cryptology 1:5–45

Sharma S KB (2019) A survey on internet of vehicles: Applications, security issues & solutions. Vehicular Communications 20:100182