사물인터넷 통신을 위한 경량 암호기술 동향 분석

김정태

목원대학교

Analyses of Light-weight Cryptography Technology for Internet of Things

Jung Tae Kim

Mokwon University

E-mail : jtkim3050@mokwon.ac.kr

Abstract

With the development of the Internet, the popularization of internet has become the new trend and enormously changed the way of human communication. There is a strong need for security. The following research will provide the definition and purpose of IoT and examine its security concerns, In this paper, we surveyed at energy consumption of lightweight block ciphers implemented in reconfigurable devices, and we analyze d the effects that round unrolling might have on the energy consumed during the encryption.

Keyword

Security, IoT, Gateway, Privacy, WSN

Ⅰ. Introduction

An ever-increasing number of these devices contain transceivers for WiFi, Bluetooth, Zigbee, or other wireless networking technologies, which allows them to communicate with each other or establish a connection to the Internet. Security and privacy issues pose a significant challenge to the further expansion of the IoT and the end-user acceptance of many IoT-based applications and services. Similar to the "ordinary" Internet, Public-Key Cryptography can play a valuable role in the IoT to overcome these challenges by providing such services as encryption, authentication, and key establishment. Many techniques to reduce the nodes' energy consumption were proposed and can be categorized into two groups, namely communication and computation based approach. Communication-based approaches include routing protocol, polling mechanism, node selection algorithm and others. Whereas computation-based approaches include architecture-level optimization, logic design, circuit design, and process technology [1].

Ⅱ. Reduced Hardware Architecture

An reduced hardware architecture system-on-chip targeting digital block design was proposed higher energy efficiency. The design has been verified by synthesizing into FPGA and implemented in silicon based on Silterra 180nm process. Results show that the proposed design achieved reduction up to 24% of leakage power and 15% of dynamic power reduction over reference design [2]. Security in reconfigurable devices has been extensively explored by the scientific community. Works proposed so far range from low cost implementation of standard algorithms [3], to high performance devices dedicated to cryptanalysis [4]. Researchers have also dedicated significant amount of effort in

realizing FPGA designs which are robust against physical attacks. Batina et al. [5] explored area, power, and energy consumption of several recently-developed lightweight block ciphers and compared it with the AES algorithm, considering also possible optimizations for the non linear transformation. However, no possible optimization was considered for other transformations, and effects of other design choices, such as serialization. A comparison of the energy consumptions of fully and partially unrolled circuits with respect to the latency in the circuit was also carried out in [6]. Typically in loT configuration, data from the nodes are immediately send to loT gateway devices wirelessly, where gateway devices aggregate data from multiple nodes and process these data before sending to the cloud through network means. Different loT sensor node platforms are available, developed either for commercial or academia purposes [7].

Ⅲ. Encryption Method

In most case, the sensing node of IoT uses wireless communication way to avoid the inconvenience brought by the laying cable. Sensitive data often needed to be transmitted between the nodes in practical applications. Sensitive data is referred to as key, ID, node authentication information and control command etc. which are related to system security and stable operation. However in the open wireless communication, these sensitive data can be gotten illegally by some special technologies, thus the security of the IoT application system will be under threat[1,2]. The designed encryption node can manage the access permission and implement the user authentication. The software and hardware design methods of the encryption node are presented. The data transmission experiments between the nodes are carried out. The results show that the encryption nodes can achieve wireless encryption transmission for the node's data, so its security can be ensured [8].

Ⅳ. Conclusion

We analyzed presented work proposes the prototyping of an FPGA-based edge device for IoT, focusing on the connectivity space problem in this paper. It is described the planned implementation for an IoT protocol stack under a cost-effective SoC FPGA.

Acknowledgments. This research was supported by Basic Science Research Program through the National Re-search Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (grant number: 2015R1D1A09061435)

Reference

[1] Md. Mahmud Hossain, Maziar Fotouhi, and Ragib Hasan, "Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things", 2015 IEEE World Congress on Services, 2015, pp.21-28.

[2] Erich Wenger and Johann Großschadl, "An 8-bit AVR-Based Elliptic Curve Cryptographic RISC Processor for the Internet of Things", 2012 45th Annual IEEE/ACM International Symposium on Microarchitecture Workshops, pp.39-46

[3] P. Chodowiec and K. Gaj, "Very compact fpga implementation of the aes algorithm," in Cryptographic Hardware and Embedded Systems-CHES 2003. Springer, 2003, pp. 319–333.

[4] S. Kumar, C. Paar, J. Pelzl, G. Pfeiffer, and M. Schimmler, "Breaking ciphers with copacobana–a cost-optimized parallel code breaker," in Proceedings of the 8th international conference on Cryptographic Hardware and Embedded Systems. Springer-Verlag, 2006, pp. 101118.

[5] L. Batina, A. Das, B. Ege, E. B. Kavun, N. Mentens, C. Paar, I. Verbauwhede, and T. Yalc¸ın, "Dietary recommendations for lightweight block ciphers: Power, energy and area analysis of recently developed architectures," in Radio Frequency Identification. Springer, 2013, pp.103–112.

[6] S. Banik, A. Bogdanov, and F. Regazzoni, "Exploring energy efficiency of lightweight block ciphers," in Selected Areas in Cryptography–SAC2015. Springer, 2015.

[7] Y.W. Lim "Reduced Hardware Architecture for Energy-Efficient loT Healthcare Sensor Nodes", 2015 IEEE International Circuits and Systems Symposium (ICSyS), pp.90-95

[8] Zeng Bohan, Wang Xu and Zhou Kaili, "Encryption Node Design in Internet of Things Based on Fingerprint Features and CC2530", 2013 IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber,Physical and Social Computing, pp.1454-1457