Hardware Design Issues of Light-weight Crypto Algorithms for RFID

Jung-Tae Kim
Mokwon University

RFID의 경량화된 암호 알고리즘의 하드웨어적 설계의 문제점 분석

김정태
목원대학교
E-mail : jtkim5068@gmail.com

요 약

We analysed a hardware design issues, which is strong, compact and efficient. Due to its low area constraints, primitive based on hardware is especially suited for RFID (Radio Frequency Identification) devices. primitive is based on the classical DES (Data Encryption Standard) design. This approach makes it possible to considerably decrease chip size requirements.

Ⅰ. Introduction

Radio Frequency Identification (RFID) systems are expanding rapidly with their applications such as logistics, supply chain management, library item tracking, medical implants, road tolling (e.g. E-Z Pass), building access control, aviation security, and homeland security. These RFID systems often have customized requirements that are currently defined ad hoc. As a result, in most applications, RFID tag and reader hardware and software must be specifically designed for each particular application, and must be physically modified or re-designed every time the specification for the current application is adjusted[1]. An important security concern associated to the RFID technology is the privacy of the tag content. Indeed, it is very easy for anybody with technical skills to disintegrate a device for reading the tag content. To preserve user privacy, only authorized RFID readers should be enabled to access the tag content. An authentication protocol, which grants access to the tag content only to a legitimate reader, is therefore required. A few lightweight and ultra-lightweight authentication protocols have developed in the literature recently. RFID tags should be low-cost, which limit the computation power, the storage space, the communication capacity and the gates count.

II. Hardware Implementation of Cryptographic Primitives

In this section we focus on the implementation of the standardized cryptographic primitives SHA-256, SHA-1, MD5, AES-128, and ECC-192[2]. All implementations will be evaluated in respect to the metric defined. During the design of the hardware modules the main motivation was to reduce the power consumption and the chip area. A common method for reducing the power consumption is to reduce the clock frequency. This comes at the cost of . extended calculation times. Increasing the required number of clock cycles by serializing the algorithm also reduces the power consumptions but increases the calculation time too. Measures like pipelining and parallel processing which increase data throughput are counter-productive and should be avoided. On the register-transfer level, low-power design measures like clock gating and the elimination of glitching activity are extensively used. For the sake of briefness, details of the algorithms are not explained but references to appropriate literature are given. Only very specific features of the modules are presented. All modules were developed and tested using the same implementation platform that will be presented next.

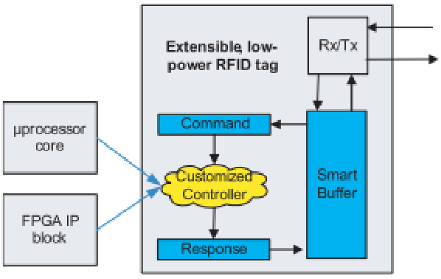

Figure 1. Extensible, low-power RFID tag

III. Comparison of Performance

The results and a comparison of the different hardware implementations can be seen in Table I. The chip area results are based on synthesis and are given in gate equivalents [GE]. For the used 0.35 □m CMOS process technology one gate equivalent compares to a NAND2 cell of 55 □m2. The mean current consumption in the third column is given in □A at a nominal clock frequency of 100 kHz and a supply voltage of 1.5 V. The current values were obtained by power simulations with NanoSim. The number of clock cycles also include IO for hashing (SHA-256, SHA-1, MD5), encrypting (AES-128), and an EC point multiplication over (ECC-192). It shows that public-key computations (ECC-192) take much longer. Moreover, ECC is in terms of power consumption and chip area more cost intensive. The implementation in a modern process technology could perhaps solve the problem in future. The comparison of the other algorithms shows that AES-128 is best suitable for implementation in passive RFID tags because it requires by far the smallest chip area. AES-128 also features the lowest power consumption. Additionally, the higher level of security (128 bits) in comparison to the competing algorithm MD5 puts the slightly higher 1,032 clock cycles into perspective. The comparison gives strong arguments for favoring AES. With the explosive growth of Internet-based applications like e-commerce, peer-to-peer networks and distributed gaming as well as embedded ones ranging from mobile over set-top boxes to automotive the demand for security in such systems has also grown dramatically. In these applications, asymmetric cryptography is used to achieve a large variety of security goals. However, asymmetric cryptographic algorithms are extremely arithmetic intensive since their security assumptions rely on computational problems which are considered to be hard in combination with parameters of significant bit sizes[3]. Some of authentication protocols use hash algorithm and symmetry key algorithms due to their simplicity compared to public key algorithms. However, they fail to satisfy the mentioned basic requirements of RFID systems. It is shown that a public key cryptographic algorithm is necessary to satisfy the required properties. We estimate the two primitives[4].

Recent work of Wolkerstorfer is the first to claim possible to have low power and compact implementation of ECC that meets the constraints imposed by the EPC standard]. We analyzed various standardized cryptographic algorithms which have a high level of security, optimized the implementation for application in passively powered RFID tags. This helps protocol designers to estimate costs more accurately. It explains the main features of the realized crypto modules SHA-256, SHA-1, MD5, AES-128, and ECC-192. It shows that public key computation (ECC-192) take much longer. Moreover, ECC is in terms of power consumption and chip area more cost intensive. The implementation in a modern process technology could solve in future. The comparison of the other algorithms shows that AES-128 is best suitable for implementation in passive RFID tags because it requires by far the smallest chip area. AES-128 also features the lowest power consumption. Additionally, the higher level of security (128 bits) in comparison to competing algorithm MD5 puts the slightly higher 1,032 clock cycles into perspective. The comparison gives strong arguments for favoring AES.

IV. Conclusion

RFID technology is becoming ubiquitous and security problem of these systems is much essential issues. In this paper, we analysed current issues on RFID privacy and security that are based on several consideration functions. A comparison on their security was made with consideration to a set of security and privacy properties that are relevant to the hardware based

References

[1] Alex K. Jones, Raymond R, "A Field Programmable RFID Tag and Associated Design Flow", 14th Annual IEEE Symposium on Field-Programmable Custom Computing Machines (FCCM'06), pp.100-104

[2] M. Feldhofer, S. Dominikus, and J. Wolkerstorfer, “Strong Authentication for RFID Systems using the AES Algorithm,” in Cryptographic Hardware and Embedded Systems CHES 2004, 6th International Workshop, Cambridge, MA, USA, August 11-13, 2004, Proceedings, ser. Lecture Notes in Computer Science, M. Joye and J.-J. Quisquater, Eds., vol. 3156. Springer, August 2004, pp. 357 370.

[3] Tim G˙uneysu and Christof Paar, "Ultra High Performance ECC over NIST Primes on Commercial FPGAs",CHES 2008, LNCS 5154, pp. 62 78, 2008.

[4] Martin Feldhofer, “Strong crypto for RFID Tag, - A comparison of low power hardware implementation”, 2007 IEEE, pp.1839-1842.

Acknowledgement

This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education, Science and Technology(grant number:2010-0024133)