Hardware implementation of the ARIA block cipher with six modes of operation

Chi Trung Ngo, Van Khanh Pham, Sang Tran, Jong-Phil Hong

School of Electrical Engineering, Chungbuk National University

trung@cbnu.ac.kr, pvkhanh@cbnu.ac.kr, sang@cbnu.ac.kr,
jphong@cbnu.ac.kr

여섯 가지 작동 모드를 갖춘 ARIA 블록 암호의 하드웨어 구현

오치충, 팜반카인, 트랑상, 홍종필
충북대학교 전기공학부

요 약

In this work, we propose a hardware architecture for the ARIA block cipher supporting six standard modes of operation. The proposed design is synthesized using a 180-nm CMOS process and operates at a clock frequency of 40 MHz. The place and route area overhead is 94 kGE for ECB mode, 115 kGE for CBC mode, 98 kGE for CFB mode, 101 kGE for CTR mode, 105 kGE for OFB mode, and 284 kGE for GCM mode

Ⅰ. Introduction

ARIA is a Korean symmetric-key block cipher included in the validation scope of the Korean Cryptographic Module Validation Program (KCMVP). It adopts a substitution–permutation network (SPN) structure and shares architectural similarities with the Advanced Encryption Standard (AES), as its design was guided by AES design principles. A block cipher mode of operation defines a method for processing arbitrarily long data streams using a single secret key, thereby enabling cryptographic functionalities such as confidentiality, authentication, and authenticated encryption. In this work, we present a hardware implementation of ARIA supporting six block cipher modes of operation, namely Electronic Codebook (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB), Counter (CTR), Output Feedback (OFB), and Galois/Counter Mode (GCM).

Ⅱ. Method

ARIA employs a 128-bit block size for both input and output and supports key lengths of 128, 192, and 256 bits, corresponding to 12, 14, and 16 encryption rounds, respectively, as summarized in Table~I.

	Plaintext(bit)	Key(bit)	Round
ARIA128	128	128	12
ARIA192	128	192	14
ARIA256	128	256	16

Table I Parameter of ARIA.

The encryption scheme of ARIA, including both the encryption flow and the associated key schedule, is illustrated in Fig. 1. The encryption algorithm follows a SPN structure and consists of an initial round key addition, a sequence of round transformations, and a final round. The intermediate rounds are composed of two alternating round functions, denoted as FO and FE. Each round comprises a nonlinear substitution layer implemented using S-boxes, a diffusion layer that provides byte-wise permutation, and a round key addition operation. The selection of the round function is determined by the S-box type employed: rounds utilizing Type-I S-boxes correspond to the FO function, whereas rounds employing Type-II S-boxes implement the FE function.

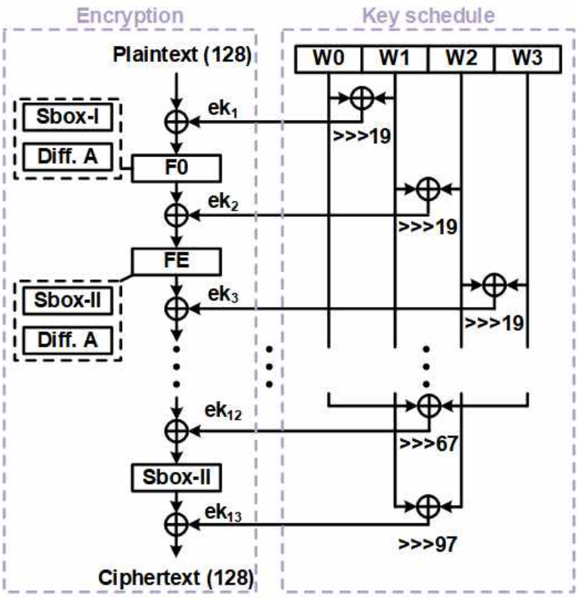

Fig. 1 ARIA Encryption scheme.

The ARIA key schedule expands the master key into a set of round keys for encryption and decryption through a sequence of hardware-friendly nonlinear and linear transformations. Specifically, S-box substitution and diffusion operations are applied in combination with predefined constants (W_0, W_1, W_2, and W_3) to generate round-dependent subkeys, as defined in the original ARIA specification [1]. This structure enables efficient hardware realization with regular datapath reuse while ensuring sufficient diffusion of the master key across all round keys, thereby improving resistance to related-key and differential attacks.

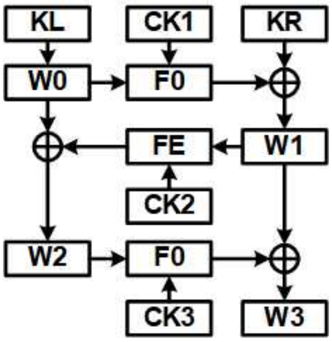

Fig. 3 Initial setup for key schedule parameter.

During the initialization phase, four 128-bit intermediate values, denoted as W0, W1, W2, and W3, are derived from the master key (MK) using a three-round 256-bit Feistel cipher. The master key may have a length of 128, 192, or 256 bits. To accommodate variable key lengths, the 128-bit value KL is first populated with the most significant bits of the master key, while any remaining bits are assigned to the 128-bit value KR. If the master key length is less than 256 bits, the unused bits in KR are padded with zeros, such that the concatenation of KL and KR equals the master key followed by zero padding. The value CKi is a fixed constant defined in the original specification of ARIA [1]

In accordance with the recommendations specified in NIST Special Publication 800-38A and 800-38D, ARIA can be operated under multiple block cipher modes of operation to support diverse security services and application requirements. In this work, ARIA is implemented with six standardized modes, namely ECB, CBC, CFB, CTR, OFB, and GCM. The modes defined in NIST SP 800-38A [2] primarily provide data confidentiality through different feedback, chaining, and counter-based mechanisms, each offering distinct trade-offs in terms of error propagation, latency, and implementation complexity.

		This work
Technology		180
Frequency (MHz)		40
Area (kGE)	ECB mode	94
	CBC mode	115
	CFB mode	98
	CTR mode	101
	OFB mode	105
	GCM mode	284

Table II Performance summary of the proposed system..

In particular, feedback-based modes such as CBC and CFB introduce inter-block dependencies, whereas counter-based modes such as CTR and OFB enable parallelizable encryption and decryption, which is advantageous for high-throughput and low-latency hardware implementations. In contrast, GCM, specified in NIST SP 800-38D [3], extends the CTR mode by incorporating a Galois field-based authentication mechanism, thereby supporting authenticated encryption with associated data (AEAD) and simultaneously ensuring both data confidentiality and integrity.

Table II summarizes the hardware performance of the ARIA implementation. The proposed design has been functionally validated and synthesized using a 180-nm CMOS process technology and operates at a clock frequency of 40 MHz. The implementation occupies 94 kGE for ECB mode, 115 kGE for CBC mode, 98 kGE for CFB mode, 101 kGE for CTR mode, and 105 kGE for OFB mode. In contrast, the GCM implementation requires 284 kGE, reflecting the additional hardware overhead introduced by the Galois field multiplication and authentication logic necessary to support authenticated encryption.

Ⅲ. Conclusion

This paper presented a hardware implementation of the ARIA block cipher supporting six standardized modes of operation in compliance with NIST SP 800-38A and SP 800-38D. The proposed design integrates ECB, CBC, CFB, CTR, OFB, and GCM, enabling both data confidentiality and authenticated encryption with associated data. Synthesized using a 180-nm CMOS process and operating at 40 MHz. Overall, the results confirm that the proposed ARIA implementation provides a flexible and standards-compliant suitable for security-critical embedded and industrial applications.

ACKNOWLEDGMENT

This work was partly supported by Innovative Human Resource Development for Local Intellectualization program through the Institute of Information & Communications Technology Planning & Evaluation(IITP) grant funded by the Korea government(MSIT) (IITP-2025-RS-2020-II201462). Basic Science Research Program through the National Research Foundation of Korea(NRF) grant funded by the Ministry of Education(RS-2020-NR049604).

참고문헌

[1] Kwon, D. et al. (2004). New Block Cipher: ARIA. In: Lim, JI., Lee, DH. (eds) Information Security and Cryptology - ICISC 2003. ICISC 2003. Lecture Notes in Computer Science, vol 2971. Springer, Berlin, Heidelberg.

[2] National Institute of Standards and Technology (NIST). Recommendation for Block Cipher Modes of Operation: Methods and Techniques. NIST Special Publication 800-38A, 2001.

[3] National Institute of Standards and Technology (NIST). Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC. NIST Special Publication 800-38D, 2007.