Jasmin Implementation of the ARIA Block Cipher

A Formally Verified Secure Implementation of the ARIA Block Cipher

Utilizing Jasmin for Verified, High-Performance Cryptographic Primitives

Ji, Yong-hyeon

hacker3740@kookmin.ac.kr

Department of Cyber Security
Kookmin University

April 19, 2025

Contents

Chapter 1

The ARIA Block Cipher

1.1 Introduction

Table 1.1: ARIA Block Cipher Specification

Parameter	Value
Block size	128 bits
Key sizes	128, 192, 256 bits
Number of rounds	12 (128-bit key) 14 (192-bit key) 16 (256-bit key)
Structure	Substitution–Permutation Network (SPN)
S-boxes	Four 8×8 S-boxes $S_1, S_2, S_3 = S_1^{-1}, S_4 = S_2^{-1}$
Diffusion layer	Involutive linear maps M_0, M_1
Round key size	128 bits
Round keys per cipher	$N_r + 1$ (whitening + rounds)
Key schedule	Derives whitening and round keys via M_0, M_1
Standardization	ISO/IEC 18033-3:2010
Designer	Korean Information Security Agency (KISA)

ARIA is a symmetric-key block cipher standardized as KS X 1213 (2004) and ISO/IEC 18033-3 (2010). It features a 128-bit block size, variable key lengths (128/192/256 bits), and an involutive SPN structure that unifies encryption and decryption routines. This manual details its specification, design rationale, and implementation guidelines.

ARIA is a substitution–permutation network (SPN) block cipher operating on 128-bit blocks with key sizes of 128, 192, and 256 bits, using 12, 14, or 16 rounds respectively.

1.2 History

The design phase of ARIA began in late 2003 by a consortium led by KISA, and the algorithm was published as KS X 1213 in 2004 and ratified as ISO/IEC 18033-3 in 2010.

1.3 Features

- **Block size:** 128 bits
- **Key lengths:** 128, 192, 256 bits
- **Rounds:** 12, 14, 16 (depending on key size)
- **Structure:** Involutional Substitution–Permutation Network
- **S-boxes:** Two 8×8 involutive S-boxes (S_1, S_2) and inverses (S_3=S_1^{-1}, S_4=S_2^{-1})
- **Diffusion:** 16×16 involutive binary matrix with branch number 8
- **Key schedule:** 3-round, 256-bit Feistel network with constants from $1/\pi$
- **Whitening:** Initial and final AddRoundKey stages
- **Security:** Strong against differential, linear, and side-channel attacks

1.4 Structure

An ARIA encryption operation consists of:

1. Initial AddRoundKey (whitening)
2. N_r full rounds (Substitution → Diffusion → AddRoundKey)
3. Final AddRoundKey (whitening)

1.4.1 Substitution Layer

Each byte of the 128-bit state passes through one of four 8×8 involutive S-boxes defined by

$$S_1(x) = B\,x^{-1} \oplus b,$$
$$S_2(x) = C\,x^{-1} \oplus c,$$

where B, C are invertible 8×8 matrices and b, c are 8×1 vectors over GF(2^8).

1.4.2 Diffusion Layer

The diffusion layer applies

$$y = A\,x, \quad A^2 = I,$$

with A a 16×16 involutive binary matrix of branch number 8, ensuring full branch diffusion within two rounds.

1.4.3 Key Expansion / AddRoundKey

1. Pad the master key MK to 256 bits (KLKR).
2. Compute $\{W_0, \ldots, W_3\}$ via a 3-round Feistel network F using constants C_1 = `0x517cc1b7...`, C_2 = `0x6db14acc...`, C_3 = `0xdb92371d...`.
3. Derive encryption keys ek_i by rotations ($\lll 19$, $\lll 31$, $\lll 61$) and XORs of the W words.
4. Obtain decryption keys dk_i by reversing and applying A to the ek_i.