Machine-Checked Proofs for AES: High-Assurance Security

v 1.0

Ji, Yong-hyeon

(hacker3740@kookmin.ac.kr)

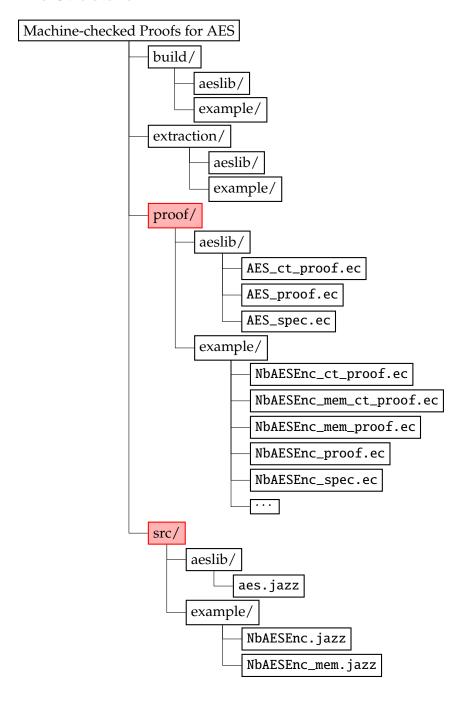
Department of Information Security, Cryptology, and Mathematics

College of Science and Technology

Kookmin University



File Structure



Copyright

© 2024 Crypto and Security Engineering Lab All rights reserved.

This document and its content are the intellectual property of "Ji, Yong-hyeon". No part of this document may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the author, except in the case of brief quotations embodied in critical reviews and certain other noncommercial uses permitted by copyright law. For permission requests, write to the author at the e-mail.

Changelog

v1.0 2024-12-24

Initial release:

Contents

1	Block Cipher	2
	1.1 Formal Definition	2

1 Block Cipher

1.1 Formal Definition

Pseudo-Random Permutation (PRP)

Definition 1. Consider a mapping

$$f: \{0,1\}^m \times \{0,1\}^n \to \{0,1\}^n$$
, i.e., $f: \{0,1\}^m \to \text{Perm}(\{0,1\}^n)$.

Let

$$\mathcal{F} := \left\{ f_k \right\}_{k \in \left\{0,1\right\}^m} \text{ where } f_k \in \text{Perm}(\left\{0,1\right\}^n)$$

be a family of permutations, where n is the block length and m is key length. The family \mathcal{F} is said to be a **pseudo-random permutation** (PRP) if it satisfies the following properties:

(i) **Permutation Property**: For every $k \in \{0, 1\}^m$, the function $f_k : \{0, 1\}^n \to \{0, 1\}^n$ is a bijection. That is,

$$f_k^{-1}(f_k(x)) = x$$
 and $f_k(f_k^{-1}(y)) = y$, $\forall x, y \in \{0, 1\}^n$.

(ii) **Indistinguishability from Random Permutation**: Define the advantage of an adversary $\mathcal A$ as

$$\operatorname{Adv}_{\mathcal{F}}^{\operatorname{PRP}}(\mathcal{A}) := \left| \operatorname{Pr}[\mathcal{A}^{f_k, f_k^{-1}} = 1] - \operatorname{Pr}[\mathcal{A}^{P, P^{-1}} = 1] \right|,$$

where

- $k \stackrel{\$}{\leftarrow} \{0,1\}^m$ (uniformly sampled)
- $P \stackrel{\$}{\leftarrow} \text{Perm} (\{0,1\}^n)$ (a uniformly random permutation)
- $\mathcal{A}^{f_k,f_k^{-1}}$ is the adversary \mathcal{A} interacting with the oracle for f_k and f_k^{-1} , while
- $\mathcal{A}^{P,P^{-1}}$ is the adversary \mathcal{A} interacting with the oracle for P and P^{-1} .
- (iii) **Efficiency**: The functions f_k and f_k^{-1} must be efficiently computable, meaning there exits deterministic algorithms that compute $f_k(x)$ and $f_k^{-1}(y)$ in time polynomial in n and m.

Remark 1 (Secure PRP). The family \mathcal{F} is a **secure PRP** if, for all probabilistic polynomial-

time (PPT) adversary \mathcal{A} , the advantage $\mathrm{Adv}^{\mathrm{PRP}}_{\mathcal{F}}(\mathcal{A})$ is negligible in m, i.e.,

$$Adv_{\mathcal{F}}^{PRP}(\mathcal{A}) \leq negl(m).$$

Block Cipher

Definition 2. A **block cipher** is defined as a family of functions

$$\{E_k: \{0,1\}^n \to \{0,1\}^n\}_{k \in \{0,1\}^k},$$

where:

• Each function E_k is a bijection over $\{0,1\}^n$, meaning there exists a corresponding decryption function D_k such that

$$D_k(E_k(x)) = x, \quad \forall x \in \{0,1\}^n.$$

- The family of functions satisfies the *secure pseudo-random permutation (PRP)* property: for a uniformly chosen $k \in \{0,1\}^k$, no computationally bounded adversary can distinguish E_k from a truly random permutation $P : \{0,1\}^n \to \{0,1\}^n$ with non-negligible advantage.
- The block cipher operates on fixed-length input blocks of size n, and the key k is sampled uniformly from the key space $\{0,1\}^k$.

In summary, a block cipher is a deterministic, key-dependent, reversible function family over fixed-length input blocks, which achieves the properties of a secure pseudo-random permutation when the key is secret.

References