SHOT: Lightweight block cipher for legacy-compatible secure storage in bounded-lifetime IoT deployments

Journal of King Saud University - Computer and Information Sciences • Article • *Open Access* • 2026 • DOI: 10.1007/s44443-026-00956-4

Lestari, Andriani Adi [a] ; MT, Suryadi [b] ; Ramli, Kalamullah [a] ; Gunawan, Teddy Surya [c] ; Agustina, Esti Rahmawati [d] ; +3 authors

[a] Department of Electrical Engineering, Faculty of Engineering, Universitas Indonesia, Depok, Indonesia

Abstract

Many deployed internet of things (IoT) devices used for medical sensor logging, industrial telemetry, and smart metering require block-cipher-based random-access encrypted storage on 8-bit microcontrollers. Conventional 128-bit block ciphers impose significant flash and random-access memory (RAM) overhead on 8-bit platforms, introducing up to 100% padding overhead for short sensor records, while modern authenticated encryption with associated data (AEAD) schemes built from sponge permutations do not support constant-time random-access decryption due to their sequential structure. This work introduces SHOT (Substitution-rotation Hybrid Optimized Transform), an 80-bit block cipher tailored for 8-bit devices and co-designed with the storage format. SHOT integrates a 5-bit nonlinear substitution layer (S-box) and a linear layer inspired by the

Ascon permutation into a 32-round Feistel network with a 160-bit key, enabling standard cipher block chaining (CBC) and counter (CTR) modes. Mixed-integer linear programming (MILP) analysis indicates estimated security margins of 17 and 20 rounds for differential and linear cryptanalysis, respectively, within our search limits. A fully unrolled SHOT assembly implementation on an AVR-class microcontroller achieves 384.7 cycles per byte and an energy cost of 330.6 nJ per bit, while a compact field-programmable gate array (FPGA) design sustains 251 Mbps using about 1,013 lookup tables. In a continuous glucose monitoring scenario, SHOT reduces padding overhead for per-record encryption and extends flash logging capacity on the same hardware partition. © The Author(s) 2026.

Author keywords

Data encryption; Embedded systems; Feistel network design; Internet of Things security; Lightweight block cipher; Resource-constrained cryptography

Corresponding authors

Corresponding author	K. Ramli
Affiliation	Department of Electrical Engineering, Faculty of Engineering, Universitas Indonesia, Depok, Indonesia
Email address	kalamullah.ramli@ui.ac.id

About Scopus

Scopus blog

Scopus API

Privacy matters

Language

日本語版を表示する

查看简体中文版本

查看繁體中文版本

Просмотр версии на русском языке

Customer Service

Help

Tutorials

Contact us

ELSEVIER