



Results for SHOT: LIGHTWE... >

SHOT: Lightweight block cipher for legacy-compatible secure storage in bo...



Export ▾

Add To Marked List

< 1 of 1 >

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

By [Lestari, AA](#) (Lestari, Andriani Adi) ^[1] ; [Suryadi, MT](#) (Suryadi, M. T.) ^[2] ; [Ramli, K](#) (Ramli, Kalamullah) ^[1] ; [Gunawan, TS](#) (Gunawan, Teddy Surya) ^[3] ; [Agustina, ER](#) (Agustina, Esti Rahmawati) ^[4] ; [Windarta, S](#) (Windarta, Susila) ^[5] ; [Wildan, W](#) (Wildan, Wildan) ^[4] ; [Triputra, FR](#) (Triputra, Fadjar Rahino) ^[6]

Are you this author?

Source [JOURNAL OF KING SAUD UNIVERSITY COMPUTER AND INFORMATION SCIENCES](#)

← [View Journal Impact](#)

Volume: 38 Issue: 6
DOI: 10.1007/s44443-026-00956-4

Article Number 556

Published JUN 29 2026

Indexed 2026-08-14

Document Type Article

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.

Keywords

Author Keywords: [Data encryption](#); [Embedded systems](#); [Feistel network design](#); [Internet of Things security](#); [Lightweight block cipher](#); [Resource-constrained cryptography](#)

Keywords Plus: [CRYPTANALYSIS](#); [INTERNET](#); [DEVICES](#)

Author Information

Corresponding Address Ramli, (corresponding
: Kalamullah author)

▼ Univ Indonesia, Fac Engr, Dept Elect Engr, Depok, Indonesia

E-mail Addresses :

kalamullah.ramli@ui.ac.id

Addresses :

- ▼ ¹ Univ Indonesia, Fac Engn, Dept Elect Engn, Depok, Indonesia
- ▼ ² Univ Indonesia, Fac Math & Nat Sci, Dept Math, Depok, Indonesia
- ▼ ³ Int Islamic Univ Malaysia, Dept Elect & Comp Engn, Kuala Lumpur, Malaysia
- ⁴ Natl Cyber & Crypto Agcy, Depok, Indonesia
- ⁵ Politeknik Siber & Sandi Negara, Dept Cybersecur, Bogor, Indonesia

[...more addresses](#)

E-mail Addresses :

andriani.adi@ui.ac.id; yadi.mt@sci.ui.ac.id;
kalamullah.ramli@ui.ac.id; tsgunawan@iium.edu.my;
esti.rahmawati@bssn.go.id; susila.windarta@poltekssn.ac.id;
wildan@bssn.go.id; fadjar.rahino.triputra@brin.go.id

Data availability statement

No datasets were generated or analysed during the current study.

Conflict of interest statement

The authors declare no conflict of interest.

Categories/ Classification

Research Areas: Computer Science

Web of Science Categories

[Computer Science, Information Systems](#)

Funding

View funding text

Funding agency	Grant number
University of Indonesia through the Hibah Publikasi Terindeks Internasional (PUTI) Q1 Scheme	PKS-252/UN2.RST/HKP.05.00/2025
Lembaga Pengelola Dana Pendidikan (LPDP), Ministry of Finance of the Republic of Indonesia	SKPB-4400/LPDP/LPDP.3/2023

+ See more data fields

Journal information

JOURNAL OF KING SAUD UNIVERSITY COMPUTER AND INFORMATION SCIENCES

View Journal Impact

ISSN	1319-1578
eISSN	2213-1248
Current Publisher	SPRINGER NATURE, CAMPUS, 4 CRINAN ST, LONDON N1 9XW, ENGLAND
Table of Contents	Current Contents Connect
Research Areas	Computer Science
Web of Science Categories	Computer Science, Information Systems

6.4

Journal Impact Factor™ (2025)



1.47

Journal Citation Indicator™ (2025)



In Web of Science Core Collection

0 Citations

 Create citation alert

0

Last 180 Days

0

Since 2013

[Learn more →](#)

77
Cited References

[→ View Related Records](#)

This record is from:

Web of Science Core Collection

- Science Citation Index Expanded (SCI-EXPANDED)



© 2026 Clarivate. All rights reserved.

[← Open comparison metrics panel](#)

- Legal Center
Privacy Statement
Copyright Notice
- Training Portal
Product Support
Newsletter
- Cookie Policy
Manage cookie preferences
Data Correction
- Accessibility Help
Terms of Use

