Parallel Sponge-Based Authenticated Encryption With Side-Channel Protection and Adversary-Invisible Nonces

By: Jimale, MA (Jimale, Mohamud Ahmed) [1] ; Z'aba, MR (Z'aba, Muhammad Reza) [1] ; Kiah, MLBM (Kiah, Miss Laiha Binti Mat) [1] ; Idris, MYI (Idris, Mohd Yamani Idna) [1] ; Jamil, N (Jamil, Norziana) [2] ; Mohamad, MS (Mohamad, Moesfa Soeheila) [3] ; Rohmad, MS (Rohmad, Mohd Saufy) [4]

IEEE ACCESS

Volume: 10 **Page:** 50819-50838

DOI: 10.1109/ACCESS.2022.3171853

Published: 2022

Indexed: 2022-05-28

Document Type: Article

Abstract

Since its birth in 2000, authenticated encryption (AE) has been a hot research topic, and many new features have been proposed to boost its security or performance. The Block cipher was the dominant primitive in constructing AE schemes, followed by stream ciphers and compression functions until the sponge construction emerged in 2011. Sponge-based AE schemes provide functional characteristics such as parallelizability, incrementality, and being online. They also offer security features for protection against active or passive adversaries. Currently, there exist parallel sponge-based AE schemes, but they are not protected against simple power analysis (SPA) and differential power analysis (DPA). On the other hand, sponge-based AE schemes that protect against such attacks are serial and cannot be parallelized. Furthermore, sponge-based AE schemes handle the nonces in a way that could allow misuse. So, sponge-based AE schemes that hide the nonce from adversaries are also an open problem. This work aims to bridge these gaps by proposing a parallel sponge-based AE with side-channel protection and adversary-invisible nonces (PSASPIN), using parallel fresh rekeying and the duplex mode of the sponge construction. A leveled implementation is used to implement the key generation part using a pseudorandom function (PRF) based on the Galois field multiplication. The data processing (the rekeyed) part is implemented using the sponge-based duplex mode. Finally, the security proof of the proposed scheme is provided using game-based theory according to the PRP/PRF switching lemma, and its performance is analyzed.

Keywords

Author Keywords: Cryptography; Security; Encryption; Ciphers; NIST; Codes ; Authentication; Integrity; authenticated encryption; authentication; confidentiality; CAESAR competition; message authentication code; NIST-LW competition; cryptographic sponge function

Keywords Plus: SECURITY; NOTIONS; ATTACKS

Citation Network

In Web of Science Core Collection

0
Citations

Create citation alert

102
Cited References
View Related Records

Use in Web of Science

Web of Science Usage Count

0	0
Last 180 Days	Since 2013

Learn more

This record is from:

Web of Science Core Collection

- Science Citation Index Expanded (SCI-EXPANDED)

Suggest a correction

If you would like to improve the quality of the data in this record, please Suggest a correction

Author Information

Corresponding Address: Jimale, Mohamud Ahmed (corresponding author)
▾ Univ Malaya, Fac Comp Sci & Informat Technol, Dept Comp Syst & Technol, Kuala Lumpur 50603, Malaysia

Addresses:
▾ [1] Univ Malaya, Fac Comp Sci & Informat Technol, Dept Comp Syst & Technol, Kuala Lumpur 50603, Malaysia
▾ [2] Univ Tenaga Nas, Coll Comp & Informat, Kajang 43000, Selangor, Malaysia
▾ [3] MIMOS Berhad, Informat Secur Lab, Kuala Lumpur 57000, Malaysia
▾ [4] Univ Teknol MARA, Fac Elect Engn, Shah Alam 40450, Selangor, Malaysia

E-mail Addresses: mahamudjimale@gmail.com

Categories/Classification

Research Areas: Computer Science; Engineering; Telecommunications

Funding

Funding agency	Grant number
Fundamental Research Grant Scheme (FRGS) of the Ministry of Higher Education, Malaysia	FP072-2019A
	FRGS/1/2019/ICT05/UM/02/1

View funding text

+ See more data fields

Journal information

IEEE ACCESS

ISSN: 2169-3536
Current Publisher: IEEE-INST ELECTRICAL ELECTRONICS ENGINEERS INC, 445 HOES LANE, PISCATAWAY, NJ 08855-4141
Journal Impact Factor: Journal Citation Reports TM
Research Areas: Computer Science; Engineering; Telecommunications
Web of Science Categories: Computer Science, Information Systems; Engineering, Electrical & Electronic; Telecommunications

3.367
Journal Impact Factor ™ (2020)

IEEE ACCESS **Journal Citation Indicator ™ (2020)**

102 Cited References

Showing 30 of 102 View as set of results

(from Web of Science Core Collection)