TU Graz
SCIENCE
PASSION
TECHNOLOGY

Ascon

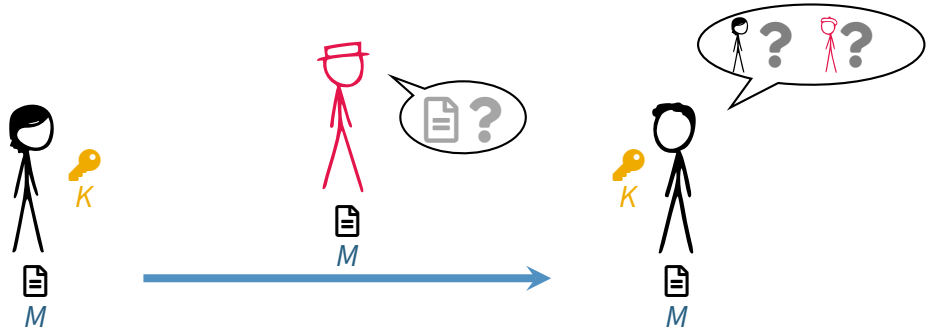
Doing More With Less –
Der neue NIST-Standard für Lightweight Cryptography

Maria Eichlseder

TU Graz | Institute of Information Security

NCC-AT Community Event 2025

Kryptographie – Der Schlüssel für sichere Kommunikation



Schlüsselaustausch

Signaturen

Verschlüsselung

Worauf basiert kryptographische Sicherheit?

Kryptographische Konstruktionen

- Sicherheit baut auf Primitive auf
- Geprüft via **Reduktionsbeweis**

Kryptographische Primitive

- Grundlage jeglicher Sicherheit
- Geprüft via **Kryptoanalyse**

Gutes Ergebnis = gutes Rezept + gute Zutaten!

Challenge: Neue Randbedingungen

Lightweight Cryptography

Lightweight Cryptography: **Vertraulichkeit** ⊕ **Authentizität**

effiziente, sichere, robuste Implementationen bei limitierten Ressourcen

Low **area** · Low **energy** · Low **power** · Low **latency**

NIST LWC Competition (2019–2023)

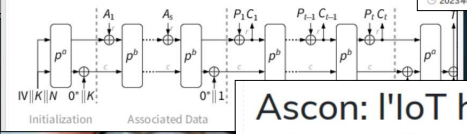
NIST เลือกกระบวนการเข้ารหัส Ascon เป็นมาตรฐานสำหรับ

By: lew on 10 February 2023 - 00:28 Tags: NIST Cryptography Internet of Things

Ascon มีการทำงาน 7 รูปแบบ ทาง NIST ยังไม่ตัดสินใจว่าจะรวม
(authenticated encryption with associated data) และการแฮช
แต่มีการยืนยันว่าข้อมูลไม่เปลี่ยนแปลง ซึ่งสำคัญต่อการใช้งานในอุปกรณ์ IoT เช่น
โดยการทดสอบกระบวนการเข้ารหัสครั้งนี้มักทดสอบกับไมโครคอนโทรลเลอร์ขนาด
ความทนทานต่อการสังเกตพฤติกรรมพลังงานและเวลา (side channel attack) ตัว A
จะไม่ได้นำประเด็นนี้มาพิจารณาเป็นหลัก

ทาง NIST ระบุว่าแม้มาตรฐานสำหรับอุปกรณ์ขนาดเล็กจะออกมาแล้ว แต่หากอุปกร
AES ต่อไปได้ ที่สำคัญคือโปรโตคอลส่วนมากรองรับกระบวนการเข้ารหัสเดิมอยู่แล้ว

ที่มา - NIST



NIST宣布採用Ascon系列演算法作為IoT裝置輕量

的認證加密（AEAD），與雜湊加密任務的Ascon系列演算法，作為保護物聯網與微型

@IT > セキュリティ > Security & Trust > NISTが選定、IoT向け軽量暗号アルゴリズム「Ascon」...

NISTの軽量暗号規格として2023年内に公開

NISTが選定、IoT向け軽量暗号アルゴリズム「Ascon」とは

NISTは、IoTなどの小型デバイスで作成、送信されるデータを保護するための軽量暗号アルゴリズムとして、「Ascon」を選定。標準暗号に採用すると発表した。

2023年02月13日 08時00分 公開 [@IT]

UPDATE

Ascon: l'IoT ha la sua nuova crittografia standard

Redazi

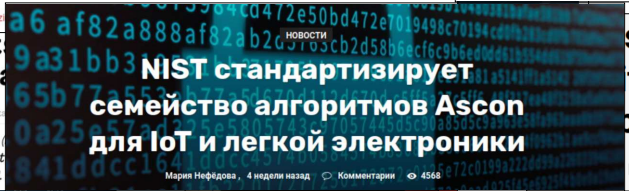
Los algoritmos Ascon serán un estándar de criptografía ligera del NIST para la tecnología diminuta

Publicado: 09/02/2023

L'Internet des Objet
chiffrement : tout sa

Elina S. 15 février 2023 Sécurité Ecrire un commenta

L'Institut national des normes et de la technologie (
cryptographiques, Ascon, pour sécuriser l'Internet
de cryptographie légère du NIST courant de 2023.



standardizuje šifro
tmy Ascon pro IoT
oná zařízení

9. 2. 2023

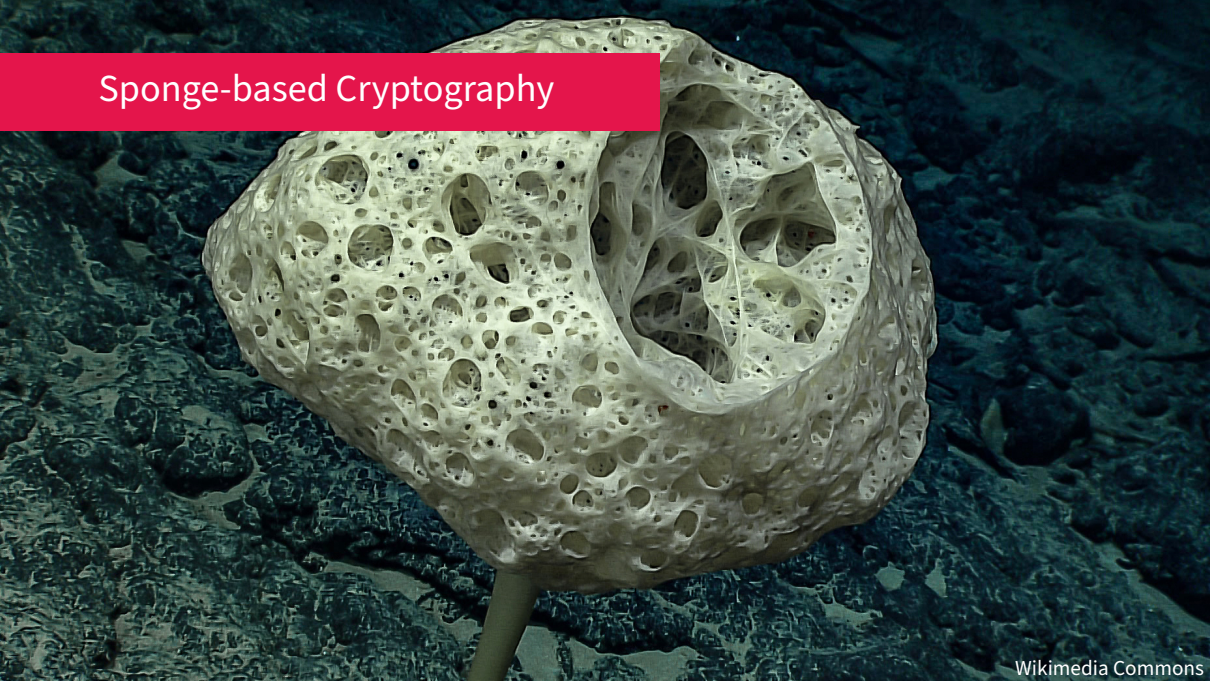
PŘIDEJTE NÁZ

The ASCON Team:

- Martin Schläffer
- Florian Mendel
- Christoph Dobraunig
- Maria Eichlseder

(c) Lunghammer, TU Graz

Sponge-based Cryptography



Wikimedia Commons

Ascon: “Doing More With Less”

- Sicherheitslevel vergleichbar mit AES-128
- **Effizienter** als AES-GCM auf relevanten Plattformen
  - **3x bis 5x Speed auf Mikrocontrollern** (https://lwc.las3.de)
  - **2x Throughput** bei **0.5x Energie** in Hardware (https://ia.cr/2021/049)
- **Robuster** als AES-GCM
  - Besserer Schutz gegen **physikalische Angriffe**
  - Resilienz bei **Misuse-Angriffen**

Ausblick

- Neue zukunftssichere Kryptographie-Standards
  - **NIST PQC**: Post-quantum-sichere asymmetrische Algorithmen
  - **NIST LWC**: Effiziente, robuste symmetrische Algorithmen
- NIST SP 800-232 ipd:
  Ascon-Based Lightweight Cryptography Standards for Constrained Devices: Authenticated Encryption, Hash, and Extendable Output Functions
- Implementationen etc.: `https://ascon.isec.tugraz.at/`