Lightweight Cryptography

Computer & Network Security

Solomon Himelbloom

UAF CS 665

2023-03-09

Overview

Overview

Key Terms

- Permutation vs. combination
- A map $f : \mathrm{D} \to \mathrm{D}$ is called a *permutation* of D, if f is bijective.
- Cryptographic nonce
- Round count

NIST Selection Announcement (2023-02-07)

An official website of the United States government Here's how you know

NIST

Search NIST Menu

NEWS

NIST Selects 'Lightweight Cryptography' Algorithms to Protect Small Devices

The algorithms are designed to protect data created and transmitted by the Internet of Things and other small electronics.

February 07, 2023

Share

Lightweight cryptography is designed to protect information created and transmitted by the Internet of Things, as well as for other miniature technologies.
Credit: N. Hanacek/NIST

Lightweight electronics, meet the heavyweight champion for protecting your information: Security experts at the National Institute of Standards and Technology (NIST) have announced a victor in their program to find a worthy defender of data generated by small devices. The winner, a group of cryptographic algorithms called Ascon, will be published as NIST's lightweight cryptography standard later in 2023.

MEDIA CONTACT
Chad Boutin
charles.boutin@nist.gov
(301) 975-4261

ORGANIZATIONS
Information Technology Laboratory
Computer Security Division
Cryptographic Technology Group

SIGN UP FOR UPDATES FROM NIST

Enter Email Address

Design Requirements

- Countermeasures against side-channel attacks
- Authenticated encryption w/ associated data (AEAD)

/‘askän/ — noun: ascon — plural noun: ascons

noun **Zoology** late 19th century: modern Latin (genus name), from Greek *askos* ‘bag’.

/‘askän/ — noun: ascon — plural noun: ascons

noun **Zoology** late 19th century: modern Latin (genus name), from Greek *askos* ‘bag’.

- a *sponge* of a grade of structure of the simplest type, in the form of a tube or bag lined with choanocytes.

Sponge Function / Construction

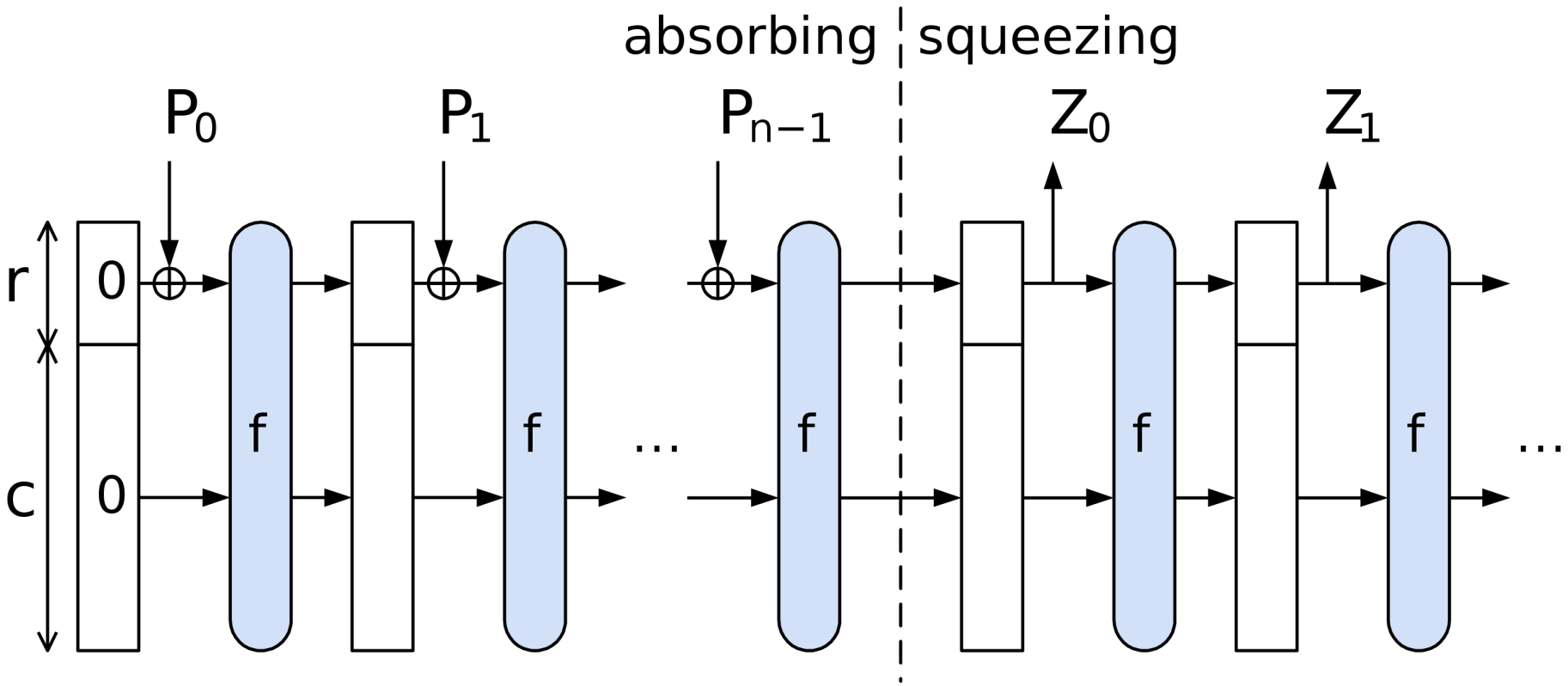


Image Source

By http://sponge.noekeon.org/, CC BY 3.0,
https://commons.wikimedia.org/w/index.php?curid=13463547

Potential Drawbacks

- Only for **ephemeral** secrets

Potential Drawbacks

- Only for **ephemeral** secrets
- Post-quantum encryption resistance?

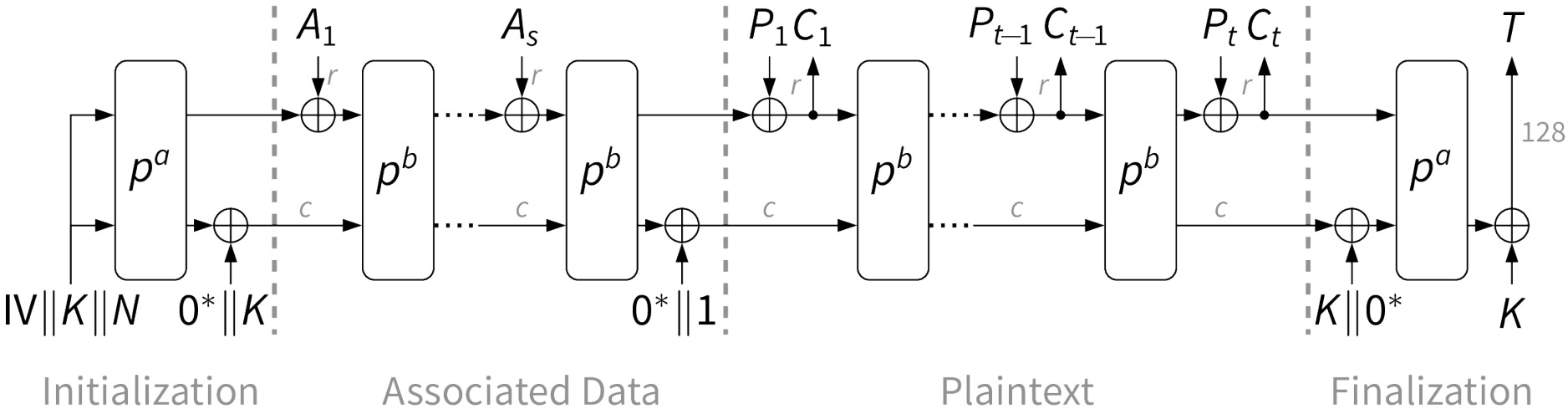
Potential Drawbacks

- Only for **ephemeral** secrets
- Post-quantum encryption resistance?

NIST Disclaimer

Not a replacement for AES or existing hash standards!

Ascon (Christoph Dobraunig, Maria Eichlseder, Florian Mendel, and Martin Schläffer)



Overview

Applications

- RFID tags

Applications

- RFID tags
- Sensor nodes

Applications

- RFID tags
- Sensor nodes
- Industrial control systems

Applications

- RFID tags
- Sensor nodes
- Industrial control systems
- Internet of Things (IoT) devices

Applications

- RFID tags
- Sensor nodes
- Industrial control systems
- Internet of Things (IoT) devices
- Vehicle-to-vehicle (V2V) communications

Specific Considerations (e.g. $\leq$ Raspberry Pi)

1. Message size
2. Device storage
3. Memory allocation

Specific Considerations (e.g. $\leq$ Raspberry Pi)

1. Message size
2. Device storage
3. Memory allocation

- Guard against counterfeiting
- Changes while in transit
- Data is authentic

Cryptography in Practice

Need to both be **secure** and **privacy preserving**.

HMAC

Hash-based message authentication code

Overview

Demo

Ascon v1.2, an authenticated cipher and hash function:
https://raw.githubusercontent.com/meichlseder/pyascon/master/ascon.py

Other Details

- Software Reference Implementations (C & Python)
- See also: https://ascon.iaik.tugraz.at/implementations.html
- Community-Maintained (C, Java, Rust, Jasmin, Go, & Typescript)

Overview

Alaska-Specific Use Cases

- Field deployed devices in the energy data sector
- Confirmation that message(s) have been received

Project Retrospective

Semester Goals + Minimum Viable Product (MVP)

Further Reading

- *Introduction to Cryptography: Principles and Applications* (Dr. Hans Delfs & Dr. Helmut Knebl)
- *Practical Cryptography* (Niels Ferguson & Bruce Schneier)

Overview

Questions?

Examples

Contact Information: sbhimelbloom@alaska.edu

Project Code: https://github.com/TechSolomon/lightweight-cryptography

Works Cited

- https://www.nist.gov/news-events/news/2023/02/nist-selects-lightweight-cryptography-algorithms-protect-small-devices
- https://www.nhtsa.gov/technology-innovation/vehicle-vehicle-communication
- https://uwaterloo.ca/communications-security-lab/lwc
- https://www.okta.com/identity-101/hmac/
- http://sponge.noekeon.org/