IETF 123 HotRFC

# Ultra Low-Latency Crypto, Areion

Yumi SAKEMI

GMO CONNECT

# Background

Future Internet architectures such as 6G has increased demand for high-speed, high-throughput, and low-latency communication.
More advanced cryptographic mechanisms will be needed, as conventional algorithms may not meet these new performance and security requirements.

**Concrete Examples :**

- Concerns of security limitation of 128-bit block size like AES-GCM are mentioned in NIST SP800-38A public comments
  - URL: https://csrc.nist.gov/csrc/media/Projects/crypto-publication-review-

- Due to performance problems of hash function in SFrame, authentication per sender is not provided
  - "No per sender authentication" is mentioned in security consideration

- Trends in NIST regarding wide block ciphers

# What is Areion?

Areion is developed as an ultra-low-latency, high-security cryptographic permutation.

## Technical specification:

- cryptographic permutation based on AES instruction
- 256-bit block size (exceeds 128-bit AES-GCM limitation)
- Combines high security with low latency
- Accepted by TCHES 2023

## Features:

- Areion can be applied to encryption and hashing
  - Encryption: Areion256-OPP (key size: 256, 512 bits)
  - Hashing: Areion-md (faster than SHA-256)
  - Implemented on both Intel AES-NI and ARM NEON

## Use case:

- Use case that requires real-time secure communication
  - Ex) e-Sports, remote surgery, satellite communication, etc.

# Areion Performance Comparison

**Performance advantages :**

- Approximately **2x faster** than AES256-GCM
- Approximately **3x faster** than SHA256

**Performance confirmed on both:**

- Intel processors (AES-NI instructions)
- ARM processors (NEON instructions)

**Particularly effective conditions:**

- Frequent key updates
- Short messages (32-256 bytes)

Measurement details: please refer to IETF XXX slides

# Open Source Implementations

Multiple open source implementations of Areion are available for your use!

## Available Implementations

- Reference implementation (Encryption, Hash)
- OpenSSL module integration ARM NEON optimized version
- Rust language implementation
- WebRTC implementation

# How to Use & Contact

**Internet-Draft:**

datatracker.ietf.org/doc/draft-sakemi-areion/

**Open Source:**

github.com/gmo-ierae

**Contact:**

Yumi Sakemi: sakemi-yumi@gmo-connect.jp

Satoru Kanno: kanno@gmo-connect.jp

**Example Applications:**

TLS, IPsec, WebRTC, QUIC, etc.

**Questions and collaboration welcome!**

We're interested in partnerships for implementation testing and real-world applications.