IETF Hackathon
Ultra Low-Latency Crypto, Areion

IETF 120
20-21 July 2024
Vancouver, Canada

Yumi Sakemi - GMO Cybersecurity by Ierae

What is Areion

- Low-latency crypto, Areion
  - Areion is a secure and low-latency cryptographic permutation
    - cryptographic permutation based AES instructions
    - Areion can be applied to **encryption** and **hashing**
  - For more details, please refer the IETF117 hackathon slides and I-D

- Use case of Areion
  - Use case that requires real-time secure communication
    - ex) e-Sports, remote surgery, satellite communication…

Hackathon Plan

- Performance comparison with the major used cryptographic primitives
  - Encryption
    - Areion256-OPP VS AES256-GCM
  - Hashing
    - Areion-md VS SHA-256

Measurement Conditions

- Experimental Environment
  1. AES-NI environment
     - Intel(R) Xeon(R) Platinum 8380 CPU @ 2.30GHz
  2. ARM environment
     - m7g instances on AWS (NEON is used)
- Implementation of comparison algorithm
  - AES256-GCM: OpenSSL
  - SHA256: OpenSSL
- Measurement Precautions
  - The measurement range includes initialization processes.
  - 12.5M times executions

Areion256-OPP VS AES256-GCM

- Areion is approximately **two times** as fast than AES-GCM

Unit: cycles per byte

AES-NI

primitive		mlen 32	64	128	256
areion-opp-256-encrypt	keylen=32	22.00	10.26	5.15	2.66
aes-gcm-encrypt	keylen=16	44.63	22.34	11.49	5.81
aes-gcm-encrypt	keylen=24	45.18	22.68	11.56	5.86
aes-gcm-encrypt	keylen=32	47.88	23.20	11.94	6.04

NEON

areion-opp-256-encrypt	keylen=32	24.93	12.46	6.23	3.11
aes-gcm-encrypt	keylen=16	47.00	23.93	12.29	6.49
aes-gcm-encrypt	keylen=24	48.10	24.52	12.58	6.68
aes-gcm-encrypt	keylen=32	48.20	24.66	12.62	6.72

Areion-md VS SHA256

- Areion is approximately **three times** as fast than SHA256

Unit: cycles per byte

AES-NI

hash	32	64	128	256
areion-md	5.28	3.80	3.02	2.67
sha256	19.18	11.52	6.71	4.34

NEON

hash	32	64	128	256
areion-md	6.89	4.82	3.76	3.20
sha256	21.09	11.92	6.73	4.15

Considerations

- From the experimental results, it was found that Areion is effective under the following conditions.
  - A situation where keys are frequently updated.
  - The message length is short (around 32 ~ 256 bytes)

Looking for effective applications of the above features ☺

Your comments welcome!!

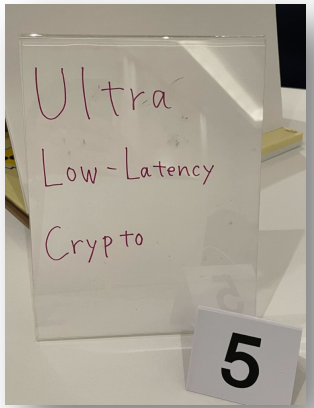
Next Step

- Implementation
  - WebRTC with Areion
    - Already implemented after IETF118
  - Hash functions
    - add into OpenSSL
  - Encryption modes
    - OTR mode
  - Independent implementations
    - Call for volunteers!
  - If you are interested in our activities, please contact us!
- Performance
  - Compare and evaluate the performance of AES256-GCM and AREION256-OPP
    - **Mobile devices**
- Application
  - Discussion with experts

Wrap Up

Champions:

- Yumi Sakemi
  yumi.sakemi@gmo-cybersecurity.com
- Satoru Kanno
  satoru.kanno@gmo-cybersecurity.com



For more details

・Open Source

- Reference code
  https://github.com/gmo-ierae/low-latency-crypto-areion
- For OpenSSL
  https://github.com/gmo-ierae/areion-openssl

・Internet Draft

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