Encryption algorithm Rocca-S
IETF Hackathon

IETF 118

4-5 November 2023

Prague, Czech Republic

Rocca-S

- Design
  - Sponge-based construction
  - 256-bit key and 256-bit tag
  - three modes: AEAD, encryption only and keystream generation
- Security (in the nonce respecting setting)
  - Classical setting: 256-bit security against key-recovery and 192-bit security against forgery
  - Quantum setting: 128bit-bit security against key-recovery and forgery
- Internet draft: https://datatracker.ietf.org/doc/draft-nakano-rocca-s/
- Reference implementation: https://github.com/yt-nakano/rocca-s
- The paper is presented at ESORICS 2023

Hackathon Plan

- Include Rocca-S to quictls to realise OpenSSL with Rocca-S
  - Evaluate the performance
  - Establish TLS connection between server and client

- (As Future plan) make the implementation public

What got done

Added Rocca-S to quictls as TLS_ROCCA-S_SHA384

```
$ ./openssl ciphers –v | grep –i rocca-s
TLS_ROCCA-S_SHA384        TLSv1.3 Kx=any      Au=any   Enc=ROCCAS      Mac=AEAD
```

Evaluated the performance

```
$ ./openssl speed -evp rocca-s
Doing ROCCA-S for 3s on 16 size blocks: 242775500 ROCCA-S's in 3.00s
Doing ROCCA-S for 3s on 64 size blocks: 273957568 ROCCA-S's in 3.00s
Doing ROCCA-S for 3s on 256 size blocks: 162557432 ROCCA-S's in 3.00s
Doing ROCCA-S for 3s on 1024 size blocks: 56992051 ROCCA-S's in 3.00s
Doing ROCCA-S for 3s on 8192 size blocks: 9290839 ROCCA-S's in 3.00s
Doing ROCCA-S for 3s on 16384 size blocks: 4733520 ROCCA-S's in 3.00s
```

What got done

Confirmed TLS connection with Rocca-S between s_client and s_server

```
$ ./apps/openssl s_server -cert server.crt -key
localhost.key -accept 10000 -ciphersuites
"TLS_ROCCA-S_SHA384“

Using default temp DH parameters
ACCEPT
…
Shared ciphers:TLS_ROCCA-S_SHA384:ECDHE-
ECDSA-AES256-GCM-SHA384:…
CIPHER is TLS_ROCCA-S_SHA384
…
```

```
$ ./apps/openssl s_client -connect
localhost:10000 -ciphersuites "TLS_ROCCA-
S_SHA384“

…
New, TLSv1.3, Cipher is TLS_ROCCA-S_SHA384
Server public key is 521 bit
…
```

The result of this Hackathon will be published later

acknowledgement

- This activity is partially supported by a contract of "Research and development on new generation cryptography for secure wireless communication services" among "Research and Development for Expansion of Radio Wave Resources (JPJ000254)", which was supported by the Ministry of Internal Affairs and Communications, Japan.