RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: **CRYP-R07**

Post-Quantum Provably-Secure Authentication and MAC from Mersenne Primes

Keita Xagawa

Researcher
NTT Secure Platform Laboratories, Japan
@xagawa
This is a joint work with **Houda Ferradi** (Hong Kong Polytechnic, Hong Kong)

#RSAC

Summary

- We revisit the MERS assumption [AJPS18]
- Authentication from the MERS assumption
- MAC from the MERS assumption

RSAConference2020

Lightweight Authentication and Post-Quantum Security

Authentications in Resource restricted devices

Context

- ePassport
- Credit card
- NFC mobile payment
- IoT sensors
- and so on

RFID tags in $0.05--$0.10 [AHM14]

Area	< 4000 GE
Non-Volatile Memory	< 4096 bits
Power	< 10 µW
Clock	< 100 kHz

[AHM14] F. Armknecth, M. Hamann, V. Mikhalev (RFIDSec 2014)

HB Family

Auth. from Learning Parity with Noise (LPN) [HB01]

😁 **Pros**: Secure if the underlying LPN problem is hard

😁 **Pros**: Efficient implementation

😟 **Cons**: Not so compact implementation (> that of AES) [AHM14]

[HB01] N.J. Hopper, M. Blum (Asiacrypt 2001)
[AHM14] F. Armknecth, M. Hamann, V. Mikhalev (RFIDSec 2014)

Our Proposal – Alternative to HB family

- Auth. from **MERS** instead of LPN
- The MERS assumption [AJPS18]:
- $(a, as + e \mod p) \approx (a, u)$
  - $a \leftarrow \mathbb{Z}_p,\ e \leftarrow \mathfrak{H}_{n,h} := \{HW(e) = h\},\ u \leftarrow \mathbb{Z}_p$
- In the sym-key setting, n = 521, h = 128.

[AJPS18] D. Aggarwal, A. Joux, A. Prakash, M. Santha (CRYPTO 2018)

Discussion

- Auth from MERS > Auth from LPN
- But, there are Auth. From BC and MAC
- Auth. From Blockcipher (e.g., AES, Camellia, PRESENT, and so on)
  - Secure if the underlying BC is post-quantumly secure
  - Not so compact implementation (but, atomic-AES: 2.5k GE)
- We think those are competitive

RSAConference2020

The MERS Assumption

The Mersenne Primes

- The Mersenne prime: $p = 2^n - 1$
- keep the Hamming weight!
- -> Use the properties to construct public-key encryption.
- Let $x, y \in \mathbb{Z}_p$:

1. $\|x + y\| \leq \|x\| + \|y\|$
2. $\|x \cdot y\| \leq \|x\| \cdot \|y\|$
3. $\|-x\| \leq n - \|x\|$

The MERS Assmption

- MERS assumption:
- $(a, as + e \mod p) \approx (a, u)$
  - $a \leftarrow \mathbb{Z}_p,\ e \leftarrow \mathfrak{H}_{n,h} \coloneqq \{HW(e) = h\},\ u \leftarrow \mathbb{Z}_p$
- Introduced by [AJPS18]
- Their parameter setting: $n = 756839, h = 256$
- Our candidate: $n = 521, h = 128$

[AJPS18] D. Aggarwal, A. Joux, A. Prakash, M. Santha (CRYPTO 2018)

Warm Up: Passively-secure Auth.

Passively-secure Authentication Auth$_{pa}$

SK: $S \leftarrow \mathfrak{H}_{n,h}$: e.g., $n = 521$, $h = 128$

$A \leftarrow \mathbb{Z}_p$

A

$E \leftarrow \mathfrak{H}_{n,h}$

$B \leftarrow AS + E$

B

If $\|B - AS\| = h$

then Accept

Security against passive attack

- **Real game**: the adversary gets real transcripts and tries to impersonate P
- **Random game**: the adversary gets random transcripts and tries to impersonate P
- **Intuition 1**: Real ≈ Random, because the MERS assumption
- **Intuition 2**: In Random, the adversary's chance is negligible
- (See the full version or [KSS10])

[KSS10] J. Katz, J.S. Shin, A.D. Smith (J. Cryptology 23(3), 2010)

Auth_{pa} is not AC-secure

SK: $S \leftarrow \mathfrak{H}_{n,h}$: e.g., $n = 511$, $h = 128$

Fix A and repeat
→ Learn LSB(AS) and so on

$A \leftarrow \mathbb{Z}_p$

A

$E \leftarrow \mathfrak{H}_{n,h}$
$B \leftarrow AS + E$

B

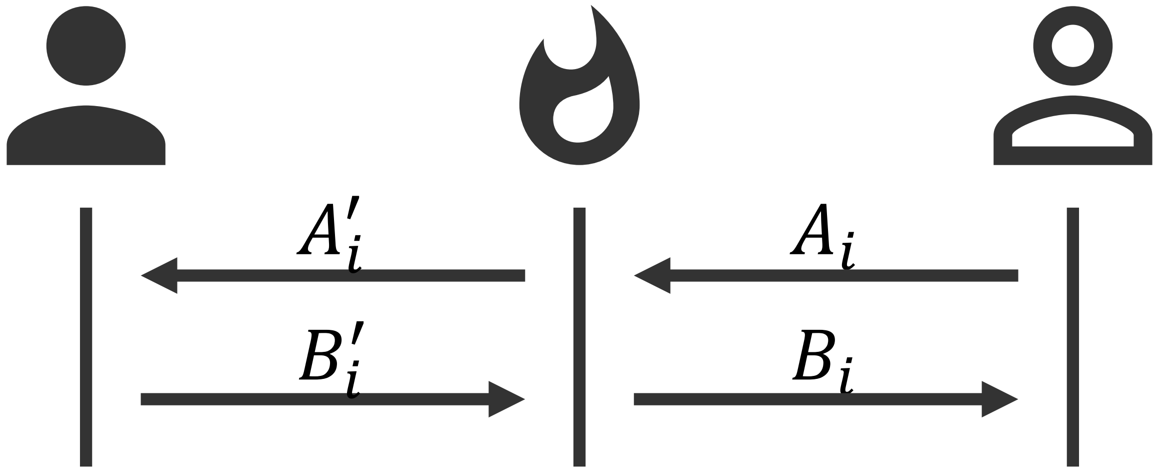
If $\|B - AS\| = h$
then Accept

RSAConference2020

S-MIM-secure Auth.

S-MIM-secure Authentication

- Auth. secure against sequential Man-in-the-Middle attacks
- The adversary can intercept sessions **sequentially**
- The adversary wins if $(A_i, B_i) \neq (A'_i, B'_i)$ and V accepts



ROR-> S-MIM conversion in [CKT16]

ROR is sufficient!

Auth_{ROR}

- V: $c \leftarrow \mathcal{C}$
- P: $\tau = (\tau_1, \tau_2) \leftarrow \mathcal{P}(sk, c)$
- V: $d \leftarrow \mathcal{V}(s, c, \tau)$

$\text{Auth}_{\text{smim}}$

- $K \leftarrow \mathbb{F}$, H: universal hash.
- V: $c \leftarrow \mathcal{C}$
- P: $\tau = (\tau_1, \tau_2) \leftarrow \mathcal{P}(sk, c)$
- $\sigma = (\sigma_1, \sigma_2) \leftarrow (\tau_1, \tau_2 * K + H(\tau_1))$
- V: $\tau = (\tau_1, \tau_2) \leftarrow (\sigma_1, (\sigma_2 - H(\tau_1)) * K^{-1})$
- $d \leftarrow \mathcal{V}(s, c, \tau)$

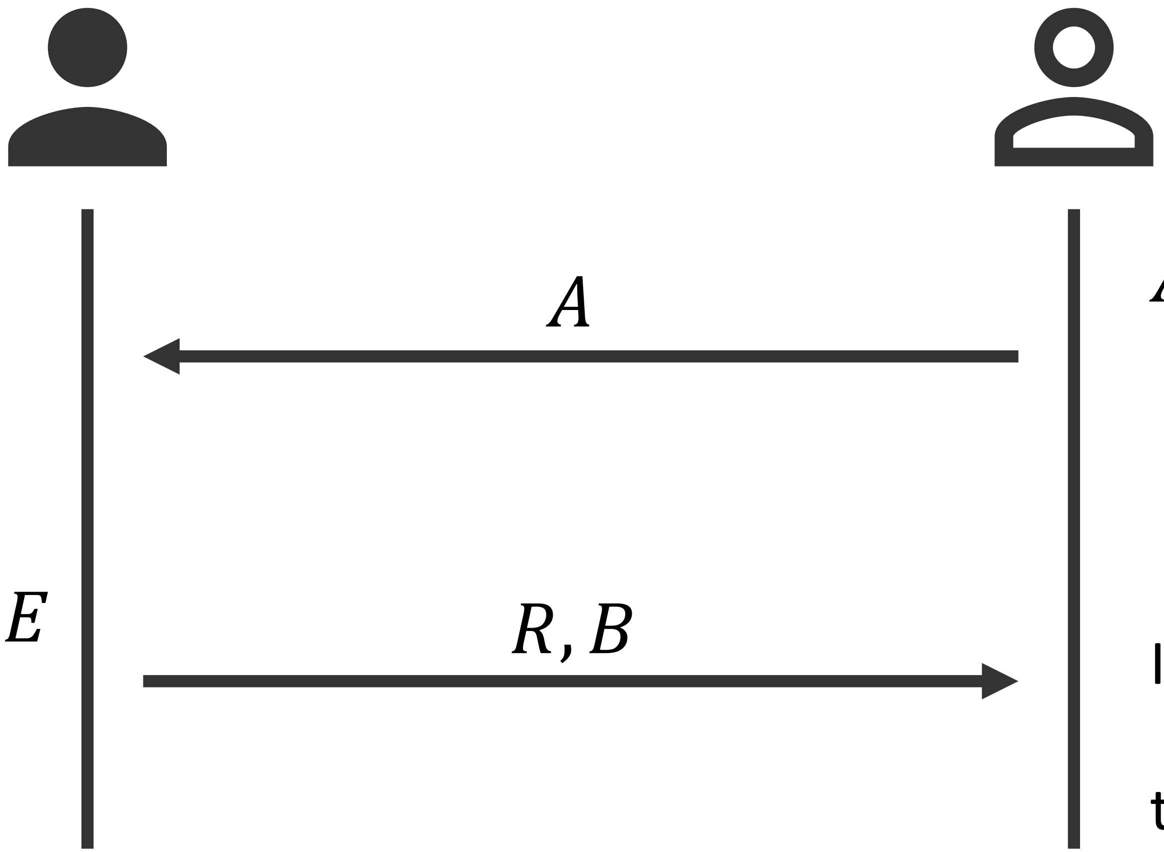
[CKT16] D. Cash, E. Kiltz, S. Tessaro (TCC 2016-A1)

ROR-secure Authentication $\mathsf{Auth}_{\mathsf{ror}}$

MERS holds
→ B is pseudorandom

SK: $S = (S_1, S_2) \leftarrow \mathbb{Z}_p \times \mathbb{Z}_p$

$A \leftarrow \mathbb{Z}_p$



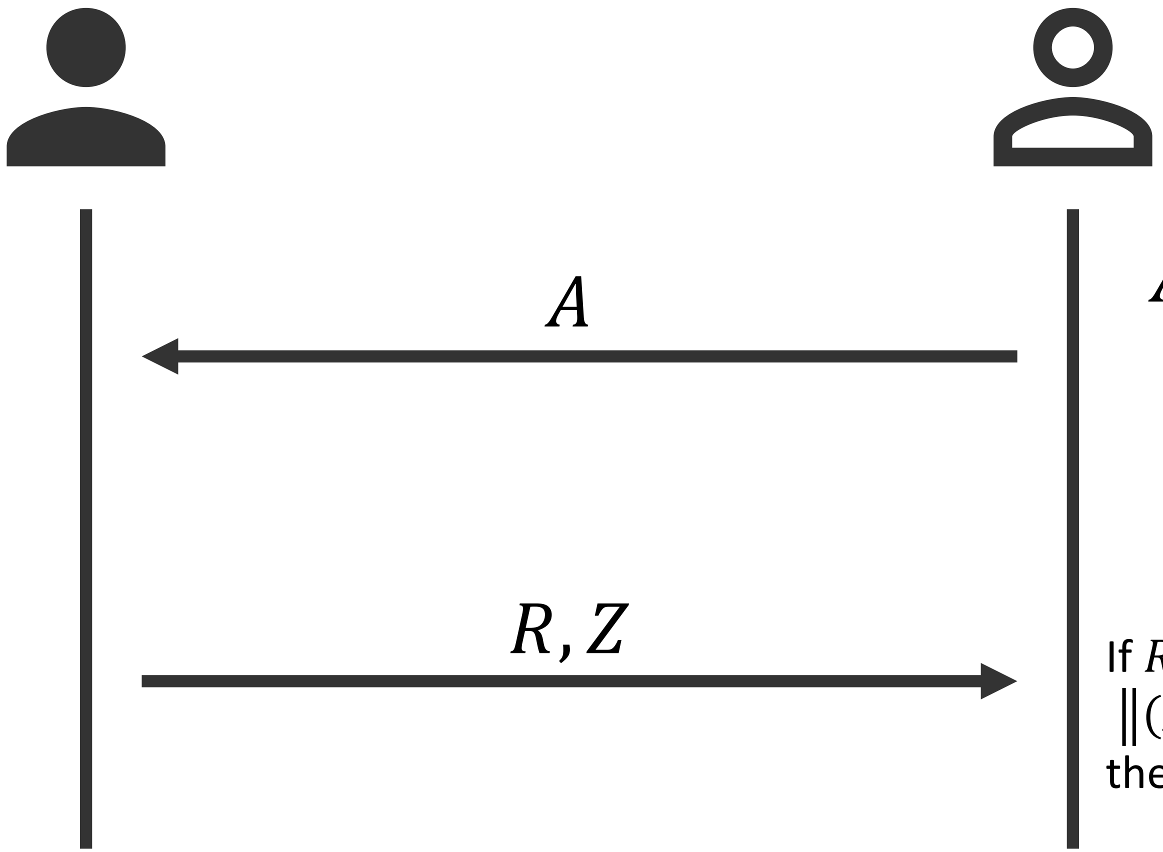
$E \leftarrow \mathfrak{H}_{n,h}$
$R \leftarrow \mathbb{Z}_p^*$
$B \leftarrow R(S_1 A + S_2) + E$

If $R \neq 0$ and
$\|B - R(S_1 A + S_2)\| = h$
then Accept

Compiled S-MIM-secure Authentication $\mathrm{Auth}_{\mathrm{smim}}$

$$\mathrm{SK}{:}S = (X_1, X_2, X_3, X_4) \leftarrow \mathbb{Z}_p^* \times \mathbb{Z}_p \times \mathbb{Z}_p^* \times \mathbb{Z}_p$$

$A \leftarrow \mathbb{Z}_p$



$E \leftarrow \mathfrak{H}_{n,h}$

$R \leftarrow \mathbb{Z}_p^*$

$Z \leftarrow R(X_1 A + X_2) + X_3 E + X_4$

If $R \neq 0$ and
$\|(Z - R(X_1 A + X_2) - X_4)X_3^{-1}\| = h$
then Accept

MAC

MAC

SK: $(s'_0, s_0, s_1, \dots, s_\mu, h, \pi)$

- Following MAC2 [KPCJV11,KPVCJ17]

MAC

1. $R \leftarrow \mathbb{Z}_p^*, E \leftarrow \mathfrak{H}_{n,h}, \beta \leftarrow \{0,1\}^\nu$
2. Compute $A = h(m, \beta) \in \{0,1\}^\mu$
3. Compute $S_A = s_0 + \sum_{i=1}^{\mu} A[i] \cdot s_i$
4. Compute $B = R\,S_A + E + s'_0$
5. Output $\sigma = \pi(R, B, \beta)$

Vrfy

1. Parse $(R, B, \beta) = \pi^{-1}(\sigma)$
2. Compute $A = h(m, \beta)$
3. Compute $S_A = s_0 + \sum_{i=1}^{\mu} A[i] \cdot s_i$
4. If $R \neq 0$ and $\|B - (RS_A + s'_0)\| = h$, then Accept

[KPCJV11] E. Kiltz, K. Pietrzak, D. Cash, A. Jain, D. Venturi (EUROCRYPT 2011)
[KPVCJ17] E. Kiltz, K. Pietrzak, D. Venturi, D. Cash, A. Jain (J. Cryptology 30(4), 2017)

RSAConference2020

Summary

Summary

- We revisit the MERS assumption [AJPS18]
- Authentication from the MERS assumption
- MAC from the MERS assumption
- Selling points
  - Auth is easy to implement!
  - All except Authpa don't need the Mersenne prime!