Understanding and Constructing AKE via 2-key KEM

Haiyang Xue, Xianhui Lu, Bao Li, Bei Liang Jingnan He
Outline

- Authenticated key exchange
- Motivations & our contributions
- AKE ← 2-key KEM ←
- AKE in a post quantum world
Diffie-Hellman Key Exchange [DH76]

• Passive secure under DDH assumption
• Adaptive attacks: Man-in-the-middle attack etc.
• Basic and general idea: Authenticated Key Exchange (AKE)
Authenticated Key Exchange

- Authenticated Key Exchange (AKE). Binding id with static public key using PKI etc.

1. Security models
   - BR model, CK model, HMQV-CK, eCK model, CK+ model

2. Constructions
   - **Explicit**: BR, CK01, IKE, Krawczyk03(SIGMA), …, Peikert14 etc.
   - **Implicit**: MTI, MQV, HMQV, OAKE, Okamoto07, NAXOS, BCNP+09, FSXY12-13 etc
General Structure of AKE

Static Pub/Sec Key $pk_A/sk_A$

Ephemeral Pub/Sec Key $pk_{A0}/sk_{A0}$

Session Key

Static Pub/Sec Key $pk_B/sk_B$

Ephemeral Pub/Sec Key $pk_{B0}/sk_{B0}$
Challenges of AKE

• The models are tedious to describe and difficult to get right;

• just describing a concrete protocol itself can be hard enough;

• the security proofs and checking even more so.
Security of AKE

Adversary Capability

• Send
• Session state Reveal
• Session Key Reveal
• Corrupt

• Test (Target) Session

\[ K^* \approx_c K_U \]

<table>
<thead>
<tr>
<th>( sk_A/a )</th>
<th>( sk_{A0}/x )</th>
<th>( sk_{B0}/y )</th>
<th>( sk_B/b )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

• (1, 1) wPFS
• (1, -) KCI
• ...
• 8 cases
Security of AKE

- Bellare-Rogaway 93 (BR93)
  indistinguishable type definition
- Canetti-Krawczyk 01 (CK01)
  stronger security (session key, session state)
- LaMacchia-Lauter-Mityagin 07 (eCK)
  stronger (session key, ephemeral randomness, wPFS+KCI+MEX)
- Fujioka-Suzuki-Xagawa-Yoneyama 12 (CK+)
  reform the security of HMQV: CK01+wPFS+KCI+MEX
Outline

- Authenticated key exchange
- *Motivations & our contributions*
- $\text{AKE} \leftarrow 2\text{-key KEM} \leftarrow$
- $\text{AKE in a post quantum world}$
Constructions of AKE

- Explicit AKE: using additional primitives i.e., signature or MAC
  1. IKE, Canetti-Krawczyk 02
  2. SIGMA, Krawczyk 03, Peikert 14
  3. TLS, Krawczyk 02

- Implicit AKE: unique ability so as to compute the resulted session key
  1. MTI 86: the first one
  2. MQV 95: various attacks
  3. HMQV 05: the first provable secure implicit-AKE via gap-DH and KEA
  4. Okamoto 07: in standard model from DDH (Hashing Proof Sys.)
  5. LLM 07: NAXOS scheme from gap-DBDH
  6. Boyd et al. 08: Diffie-Hellman+KEM
  7. FSXY 12 (std.), FSXY 13 (RO)
  8. ZZD+15 HMQV-type based on RLWE with weaker aim
Motivation

• Explicit AKE
  SIGMA
  Krawczyk 03

• Implicit AKE
  ???
Motivations

• What is the (non-interactive) core building block of implicit AKE?

• How to grasp and simplify the construction and analysis of implicit AKE?
Our Works

- What is the (non-interactive) core building block of implicit AKE?
- propose a new primitive 2-key KEM

- How to grasp and simplify the construction and analysis of AKE?
- give frames of AKE to understand several well-know AKEs
- construct new AKEs from 2-key KEM
Outline

- Authenticated key exchange
- Motivations & our contributions
- AKE ← 2-key KEM ←
- AKE in a post quantum world
Key Encapsulation Mechanism (KEM)

\[ K' = K \]

\[ k \xrightarrow{Enc} (C, K) \]

\[ KGen \]

\[ r \xrightarrow{Enc} pk \]

\[ sk \xleftarrow{Dec} \]
Key Exchange (transport) and KEM

\[ (C, K) = \text{Enc}(pk, r) \]

\[ \text{Dec}(sk, C) = K = \text{Enc}(pk, r) \]
Our 2-key KEM

$K_{Gen1} \quad K_{Gen0}$

$r \rightarrow pk_1 \rightarrow pk_0 \xrightarrow{Enc} (C, K)$

$K' = K \leftarrow sk_1 \leftarrow sk_0 \xrightarrow{Dec}$

It is simple, not a big deal
One-side AKE from 2-key KEM?

\[ U_A \]
\[ p_{k_1} \]

\[ U_B \]

\[ p_{k_0} \]

\[ C \]

\[ (C, K) = Enc(p_{k_1}, p_{k_0}, R_B) \]

\[ Dec(s_{k_1}, s_{k_0}, C) = K \]

The key point is how to define its security to fit the requirement of AKE.
Security of 2-key KEM

\[ \text{CCA}_\cdot \text{ Security of 2-key KEM} \]

\[ \begin{align*}
\text{A} & \quad \text{Challenger} \\
\text{pk}_1, L & \quad \text{pk}_1 \leftarrow \text{KGen}1, L = \{\text{pk}_0^i/\text{sk}_0^i\} \leftarrow \text{KGen}0 \\
\text{pk}_0', C' & \quad \text{If } \text{pk}_0' \in L \\
\text{If } \text{pk}_0' \in L & \quad K' = \text{Dec}(\text{sk}_1, \text{sk}_0', C') \\
\text{pk}_0^* & \quad (C^*, K^*) = \text{Enc}(\text{pk}_1, \text{pk}_0^*, r) \\
C^* & \quad (\text{pk}_0', C') \neq (\text{pk}_0^*, C^*) \\
K' & \quad K^*? = K' \\
\end{align*} \]
[CCA,·] Security of 2-key KEM

Session State Reveal
Session Key Reveal

Challenger

\[ p_{k_1} \leftarrow KGen1, \quad L = \{pk_0^i / sk_0^i\} \leftarrow KGen0 \]

\[ p_{k_1}, L \]

\[ pk_1' \]

\[ C' \]

\[ \text{If } pk_0' \in [\text{CPA,·}] \text{ security} \]

\[ K' = Dec(sk_1, sk_0', C') \]

\[ (C^*, K^*) = Enc(p_{k_1}, pk_0^*, r) \]

\[ (pk_0', C') \neq (pk_0^*, C^*) \]

\[ K^*? = K' \]
One-side AKE from [CCA, CPA] 2-key KEM

\[ U_A \quad p_{k_{A1}} \quad U_B \]

\[ C \]

\[ (C, K) = Enc(p_{k_{A1}}, p_{k_{A0}}, r_B) \]

\[ K = Dec(s_{k_{A1}}, s_{k_{A0}}, C) \]
The other side AKE from [CCA, CPA] 2-key KEM

\[ (C_B, K_B) = Enc(pk_{B1}, pk_{B0}) \]

\[ K_B = Dec(sk_{B1}, sk_{B0}, C_A) \]
Main AKE frame? ← [CCA, CPA] 2-key KEM

\[ (C_B, K_B) = Enc(pk_{B1}, pk_{B0}) \]

\[ K_A = Dec(sk_{A1}, sk_{A0}, C_A) \]

\[ K = Hash(sid, K_A, K_B) \text{ or PRF}(K_B) \oplus PRF(K_A) \]
Several AKE frames with Tricks

\[ (C_B, K_B) = Enc(pk_{B1}, pk_{B0}) \]

\[ K_A = Dec(sk_{A1}, sk_{A0}) \]

Trick 1: All the randomness for \( Enc \) and \( KGen0 \) is generated from both ephemeral secret \( r_{A0} \) and static secret key \( sk_A \)

\[ K = Hash(sid, K_A, K_B) \text{ or } PRF(K_B) \oplus PRF(K_A) \]
Several AKE frames with Tricks

\[ (C_B, -) = Enc(pk_{B1}, -) \]

\[ K_A = Dec(sk_{A1}, sk_{A0}, C_A) \]

\[ K_B = Dec(sk_{B1}, sk_{B0}, C_A) \]

\[ (C_A, K_A) = Enc(pk_{A1}, pk_{A0}) \]

\[ K = Hash(sid, K_A, K_B) \text{ or } PRF(K_B) \oplus PRF(K_A) \]
Several AKE frames with Tricks

\[
\begin{align*}
U_A \quad pk_{A1} & \quad U_B \quad pk_{B1} \\
(C_B, K_B) = Enc(pk_{B1}, pk_{B0}) & \quad pk_{A0} \quad C_B \\
K_B = Dec(sk_{B1}, sk_{B0}, C_A) & \quad (C_A, K_A) = Enc(pk_{A1}, pk_{A0}) \\
K_A = Dec(sk_{A1}, sk_{A0}, C_A) & \quad pk_{B0} \quad C_A \\
K = Hash(sk_{A0}, pk_{A1}, K_B) \oplus PRF(K_B) \oplus PRF(K_A)
\end{align*}
\]

Trick 3

\[C_B \text{ can be publicly computed from } pk_{A0}\]
\[C_A \text{ can be publicly computed from } pk_{B0}\]
Understanding HMQV-A based on 2-key KEM

\[ U_A \quad A = g^a \]

\[ X = g^x \]
\[ d = h(X, B) \]
\[ K_A = (YB^e)^x + ad \]

\[ U_B \]
\[ Y = g^y, C_A = YB^e \]
\[ e = h(Y, A) \]
\[ K_B = (XA^d)^y + be \]
Understanding HMQV-B based on 2-key KEM

\[ U_A \]

\[ X = g^x, C_B = XA^d \]
\[ d = h(X, B) \]
\[ K_A = (YB^e)^{x+ad} \]

\[ U_B \]

\[ B = g^b \]
\[ Y = g^y \]
\[ e = h(Y, A) \]
\[ K_B = (XA^d)^{y+be} \]
Understanding HMQV based on 2-key KEM

\[ U_A \quad A = g^a \]

\[ X = g^x, C_B = XA^d \]
\[ d = h(X, B) \]
\[ K_A = (YB^e)^x + ad \]

\[ Y = g^y, C_A = YB^e \]
\[ e = h(Y, A) \]
\[ K_B = (XA^d)^{y+be} \]

\[ K = \text{Hash}(A, B, X, Y, K_A, K_B) \]
Understanding AKE

• Every well-known implicit AKE implies a 2-key KEM
  • HMQV(&OAKE): 2-key KEM from gap-DH and KEA
  • LLM07: (aka. NAXOS) 2-key KEM from gap-DH
  • Okamoto 07: 2-key KEM from DDH (modified Cramer-Shoup)
  • FSXY12, improved KEM combiner in std. model
  • FSXY13, improved KEM combiner in RO model
Generic constructions of 2-key KEM

• CCA secure \((C_1, K_1) = Enc(pk_1), \text{ and } (C_0, K_0) = Enc(pk_0)\)

\[ C = C_1|C_0, \quad K = f(K_1, K_0, C) \]

• GHP18, CCA secure when \(f\) is a hash (in RO) or PRF function (in std.).

• It is not \([CCA,\cdot]\) secure

• However when adding \(pk_0\) in hashing or PRF step, it is \([CCA,\cdot]\) secure
More Generic Constructions of 2-key KEM

- Classical Fujioka-Okamoto transformation does not work for $[CCA,\cdot]$ security

- Improved FO transformation by putting public key in hashing step to generate $K$
Roadmap

A KE

2-key KEM

Interactive

- Improved KEM Combiner
  - FXSY12
  - FXSY13

Non-interactive

- Improved FO
  - [CPA, CPA] 2-key PKE

HMQV

NAXOS

Okamoto

OAKE
AKE from Lattice

- ZDD+15 proposed HMQV-type RLWE with BR and wPRF security
  \[ e_1 \ e_2 \ e_3 \text{ more communications} \]
- BDK+18 Kyber utilized FSXY to give a CK+ secure AKE from Module-LWE

- By applying the Improved FO transformation and AKE frame, we get AKE with less communications from Module-LWE

Conclusion

• [CCA, CPA] secure 2-key KEM and its (generic) constructions

• Understand HMQV, NAXOS, Okamoto, FSXY12-3 etc. via 2-key KEM

• New Constructions based on lattice and SIDH

Thanks
Following work: Supersingular Isogeny DH-AKE

- Galbraith pointed out several challenges (eprint 2018\226)
  1. Sign-MAC? Signature via SIDH $O(\lambda^2)$
  2. $g^{ad+x}$
  3. Adaptive attack. Public Key Validation
  4. formal Gap assumption

AKE-SIDH that is CK+ secure and supports arbitrary registration