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]

$\boldsymbol{U_A}$		$\boldsymbol{U}_{\mathrm{B}}$
$x \rightarrow g^x = X$		$y \rightarrow g^y = Y$
	X →	
$K = Y^x$	← Y	$K = X^y$

- 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

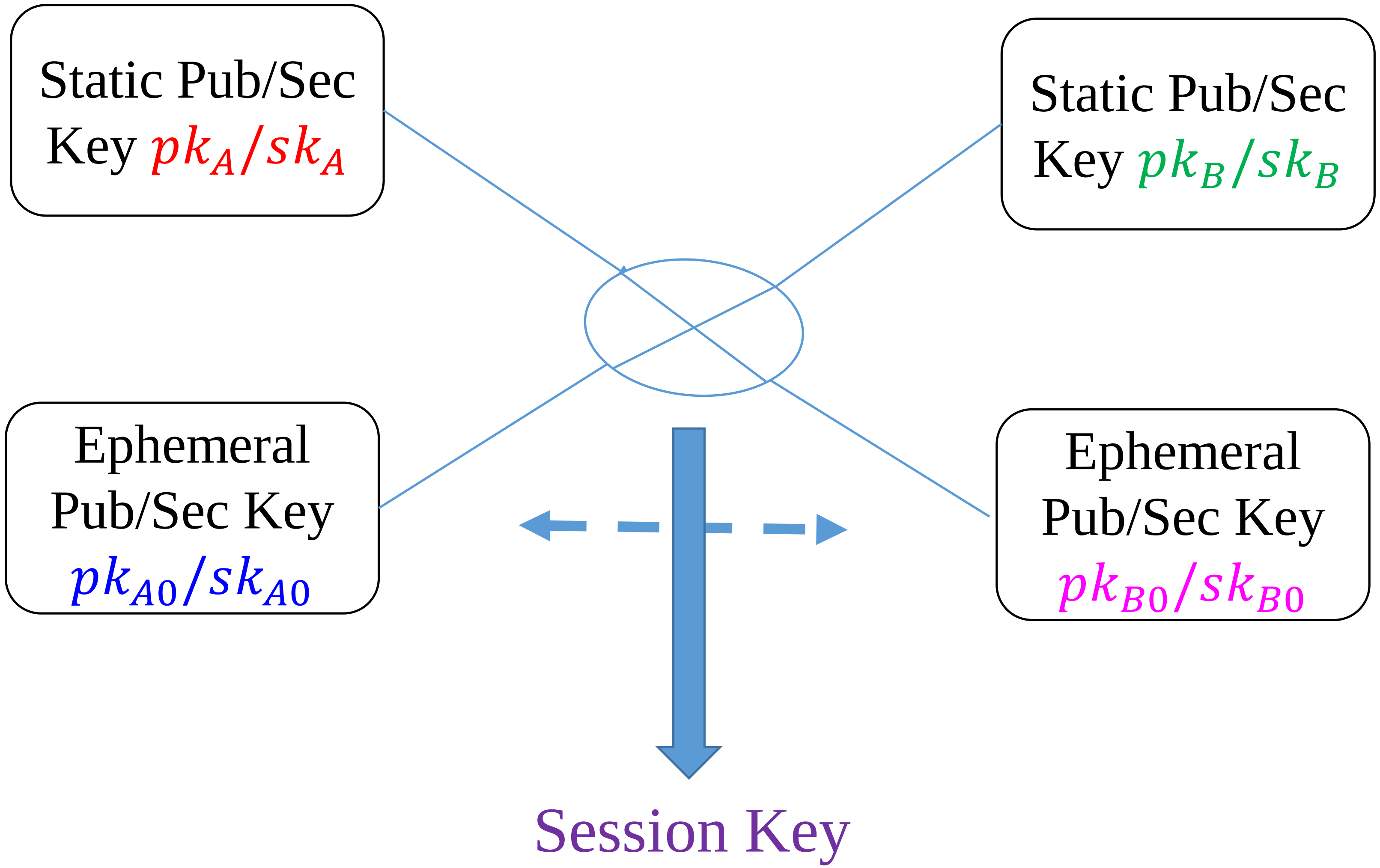
   BR model, CK model, HMQV-CK, eCK model, CK+ model

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



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

$$K^* \approx_c K_U$$

$\boldsymbol{sk_A/a}$	$\boldsymbol{sk_{A0}/x}$	$\boldsymbol{sk_{B0}/y}$	$\boldsymbol{sk_B/b}$
1	0	0	1

- (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*
- *AKE ← 2-key KEM ←*
- *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

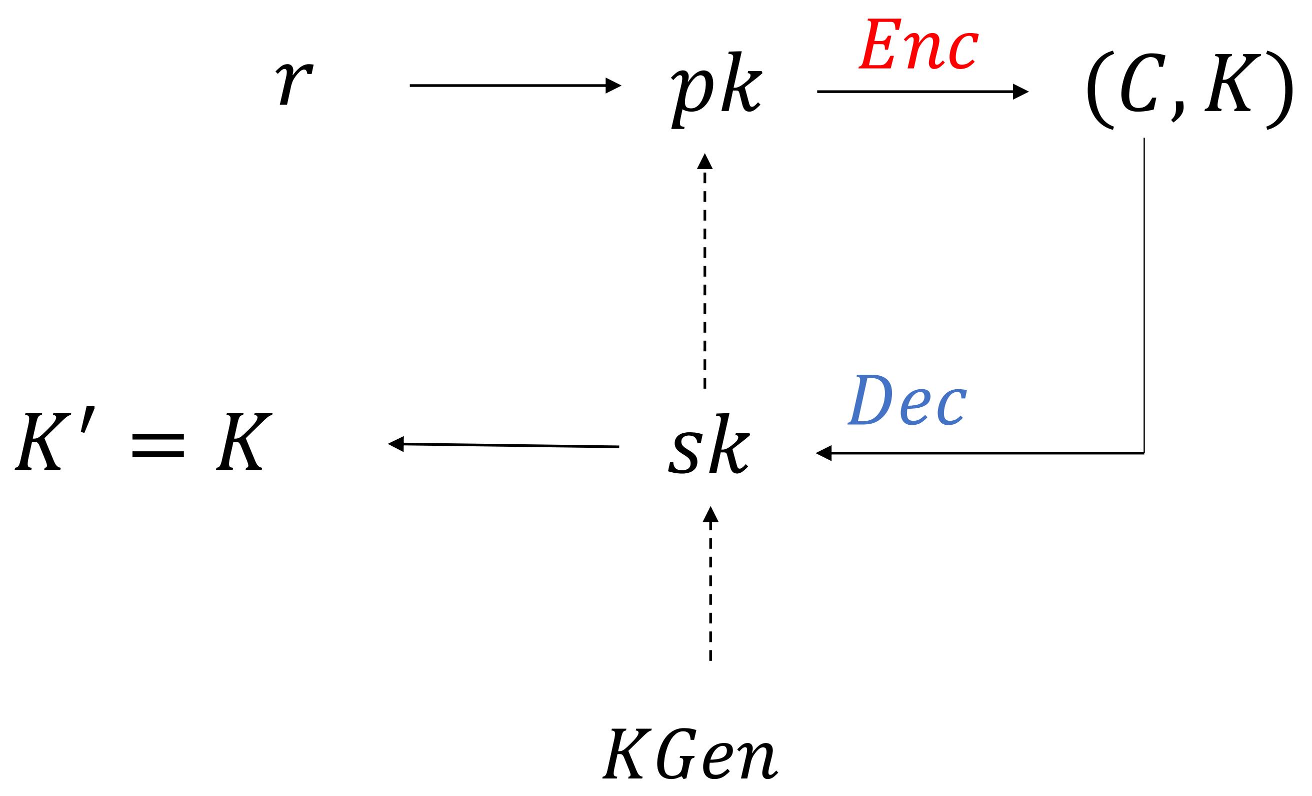
- What is the (non-interactive) core building block of implicit AKE?
- propose a new primitive 2-key KEM

- 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)



Key Exchange (transport) and KEM

$\boldsymbol{U}_{\mathrm{A}}$ $\boldsymbol{U}_{\mathrm{B}}$

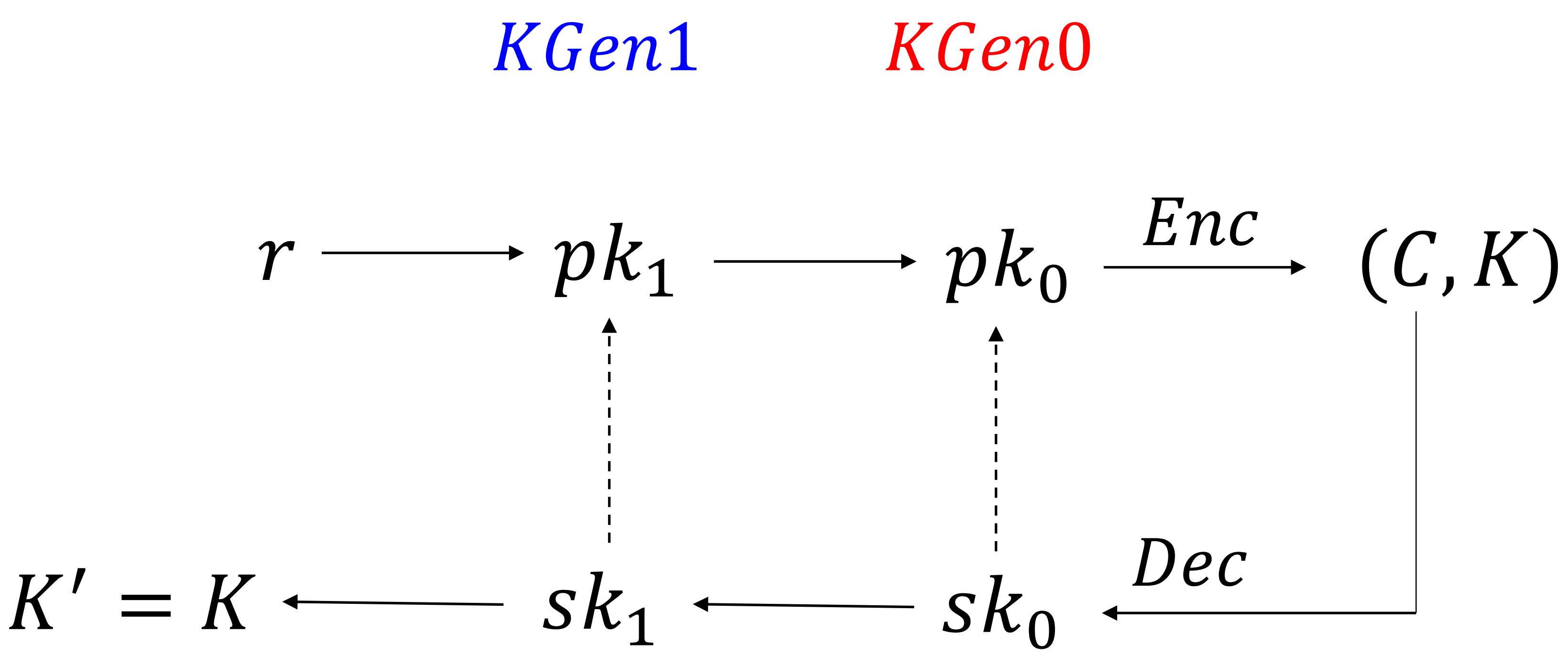
pk →

C ←

$$(C, K) = Enc(pk, r)$$

$$Dec(sk, C) = K = Enc(pk, r)$$

Our 2-key KEM



It is simple, not a big deal

One-side AKE from 2-key KEM?

$\boldsymbol{U}_{\mathrm{A}}$ $\quad$ $\boldsymbol{U}_{\mathrm{B}}$

pk_1

pk_0 →

C ←

$(C, K) = Enc(pk_1, pk_0, R_B)$

$Dec(sk_1, sk_0, C) = K$

The key point is how to define its security to fit the requirement of AKE

$[CCA,\cdot]$ Security of 2-key KEM

A — Challenger

Session State Reveal
Session Key Reveal

pk_1, L (Challenger → A): $pk_1 \leftarrow KGen1, L = \{pk_0^i / sk_0^i\} \leftarrow KGen0$

DecO

pk_0', C' (A → Challenger): If $pk_0' \in L$

$K' = Dec(sk_1, sk_0', C')$

Send

pk_0^* (A → Challenger)

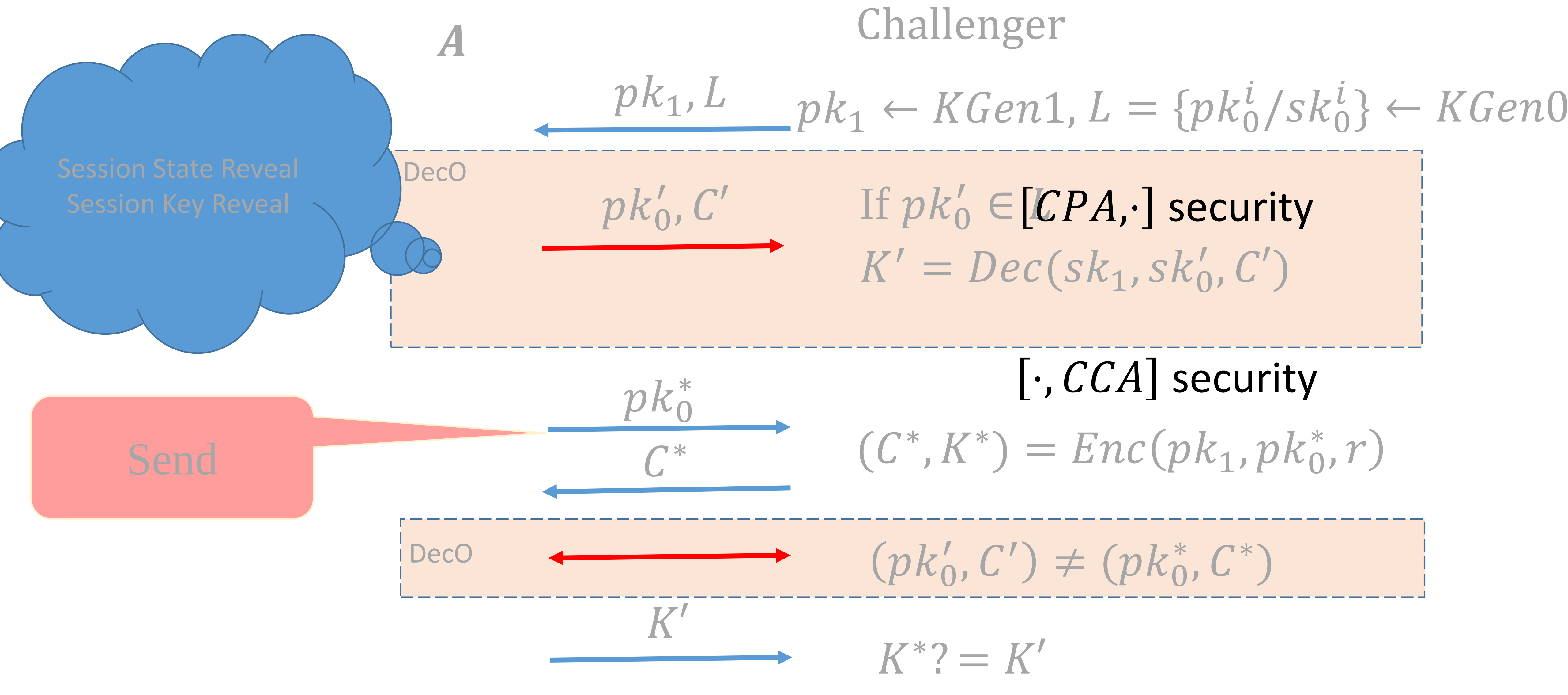
C^* (Challenger → A): $(C^*, K^*) = Enc(pk_1, pk_0^*, r)$

DecO

$(pk_0', C') \neq (pk_0^*, C^*)$

K' (A → Challenger): $K^* ?= K'$

$[CCA, \cdot]$ Security of 2-key KEM



One-side AKE from [CCA, CPA] 2-key KEM

$\boldsymbol{U}_{\mathrm{A}}$ pk_{A1}

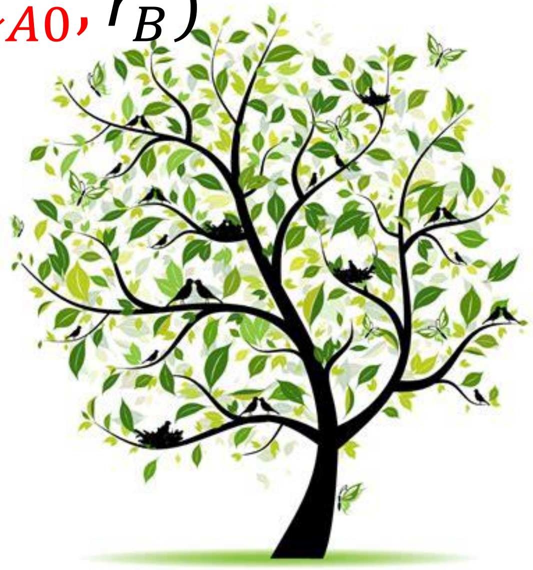
$\boldsymbol{U}_{\mathrm{B}}$

pk_{A0}

C

$(C, K) = Enc(pk_{A1}, pk_{A0}, r_B)$

$K = Dec(sk_{A1}, sk_{A0}, C)$



The other side AKE from [CCA, CPA] 2-key KEM

$\boldsymbol{U}_{\text{A}}$

$\boldsymbol{U}_{\text{B}}$ pk_{B1}

pk_{B0}

$(C_B, K_B) = Enc(pk_{B1}, pk_{B0})$

C_B

$K_B = Dec(sk_{B1}, sk_{B0}, C_A)$

Main AKE frame?← $[CCA, CPA]$ 2-key KEM

$\boldsymbol{U}_{\mathrm{A}}$ pk_{A1}

$\boldsymbol{U}_{\mathrm{B}}$ pk_{B1}

$(C_B, K_B) = Enc(pk_{B1}, pk_{B0})$ — pk_{A0} C_B → $K_B = Dec(sk_{B1}, sk_{B0}, C_A)$

$K_A = Dec(sk_{A1}, sk_{A0}, C_A)$ ← C_A pk_{B0} — $(C_A, K_A) = Enc(pk_{A1}, pk_{A0})$

$$K = Hash(sid, K_A, K_B) or\ PRF(K_B) \oplus PRF(K_A)$$

Several AKE frames with Tricks

$\boldsymbol{U}_{\mathrm{A}}$ pk_{A1}

$\boldsymbol{U}_{\mathrm{B}}$ pk_{B1}

$(C_B, K_B) = Enc(pk_{B1}, pk_{B0})$

pk_{A0} C_B

$K_B = Dec(sk_{B1}, sk_{B0}, C_A)$

$K_A = Dec(sk_{A1}, sk$

$) = Enc(pk_{A1}, pk_{A0})$

Trick 1

All the randomness for Enc and $KGen0$ is generated from both *ephemeral secret* r_{A0} and *static secret key* sk_A

$K = Hash(sid, K_A, K_B) or\ PRF(K_B) \oplus PRF(K_A)$

Several AKE frames with Tricks

2-key KEM is public key pk_{B0} independent

U_A pk_{A1}

$(C_B, -) = Enc1(pk_{B1}, -)$ Trick 2 pk_{A0} C_B $K_B = Dec(sk_{B1}, sk_{B0}, C_A)$

$K_A = Dec(sk_{A1}, sk_{A0}, C_A)$ C_A pk_{B0} $(C_A, K_A) = Enc(pk_{A1}, pk_{A0})$

$K = Hash(sid, K_A, K_B) or\ PRF(K_B) \oplus PRF(K_A)$

Several AKE frames with Tricks

U_A pk_{A1}

U_B pk_{B1}

$(C_B, K_B) = Enc(pk_{B1}, pk_{B0})$ → pk_{A0} ~~C_B~~ → $K_B = Dec(sk_{B1}, sk_{B0}, C_A)$

$K_A = Dec(sk_{A1}, sk_{A0}, C_A)$ ← ~~C_A~~ pk_{B0} ← $(C_A, K_A) = Enc(pk_{A1}, pk_{A0})$

Trick 3

C_B can be publicly computed from pk_{A0}
C_A can be publicly computed from pk_{B0}

$K = Hash(sid, K_A, K_B)$ or $PRF'(K_B) \oplus PRF'(K_A)$

Understanding HMQV-A based on 2-key KEM

$\boldsymbol{U}_{\mathrm{A}}$ $A = g^a$

$\boldsymbol{U}_{\mathrm{B}}$

$X = g^x$

X →

$Y = g^y, C_A = YB^e$

$d = h(X, B)$

YB^e ←

$e = h(Y, A)$

$K_A = (YB^e)^{x+ad}$

$K_B = \left(XA^d\right)^{y+be}$

Understanding HMQV-B based on 2-key KEM

$\boldsymbol{U}_{\mathrm{A}}$

$\boldsymbol{U}_{\mathrm{B}}$ $B = g^b$

$X = g^x, C_B = XA^d$ → XA^d → $Y = g^y$

$d = h(X, B)$

$e = h(Y, A)$

← Y ←

$K_A = (YB^e)^{x+ad}$

$K_B = \left(XA^d\right)^{y+be}$

Understanding HMQV based on 2-key KEM

$\boldsymbol{U}_{\mathrm{A}}$ $A = g^a$

$\boldsymbol{U}_{\mathrm{B}}$ $B = g^b$

$X = g^x, C_B = XA^d$

$d = h(X, B)$

$K_A = (YB^e)^{x+ad}$

X ~~XA^d~~ →

← ~~YB^e~~ Y

$Y = g^y, C_A = YB^e$

$e = h(Y, A)$

$K_B = \left(XA^d\right)^{y+be}$

$$K = Hash(\mathrm{A}, \mathrm{B}, X, Y, K_A, K_B)$$

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 $(C_1, K_1) = Enc(pk_1), and\ (C_0, K_0) = Enc(pk_0)$

$$C = C_1 | C_0, K = f(K_1, K_0, C)$$

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

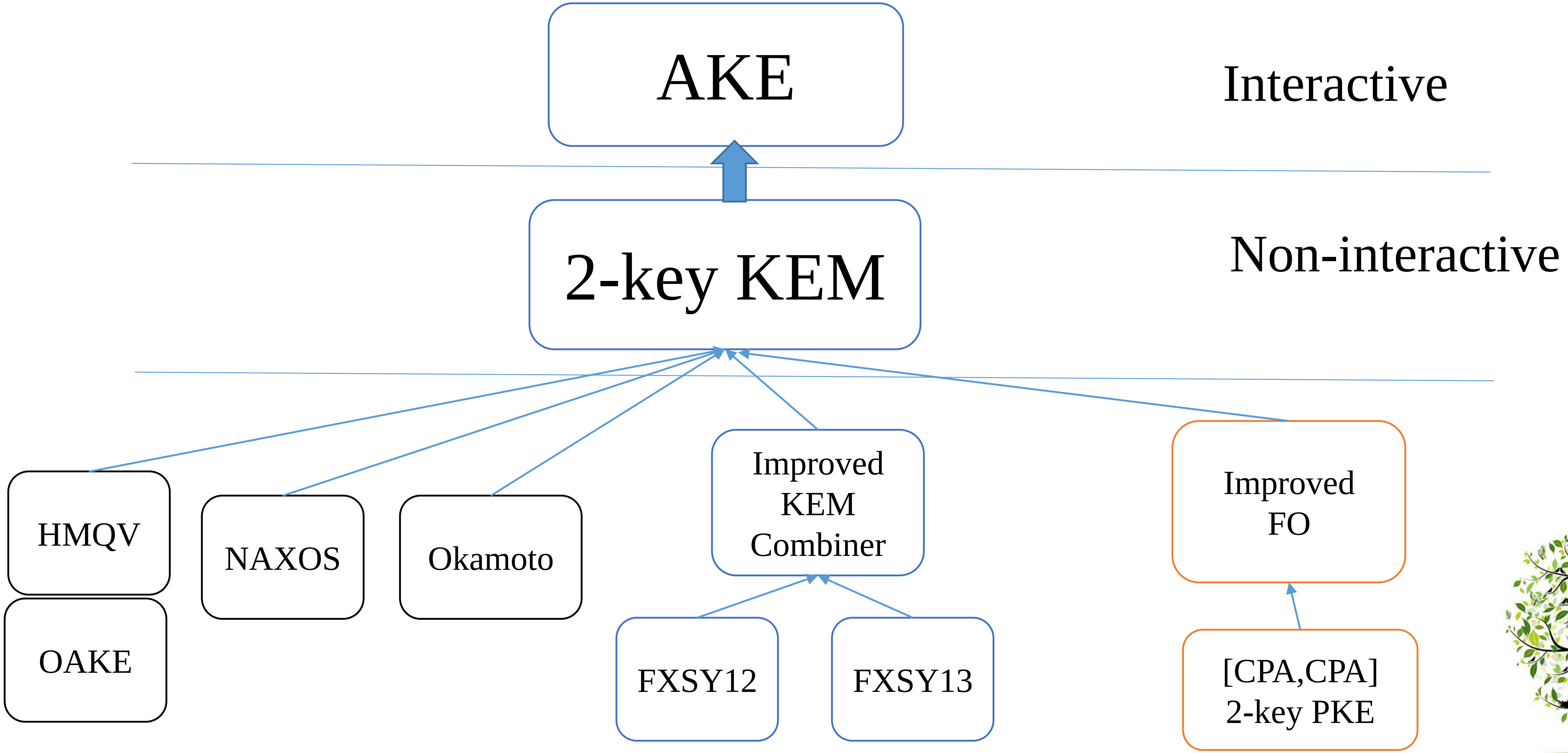
- It is not $[CCA,\cdot]$ secure
- However when adding pk_0 in hashing or PRF step, it is $[CCA,\cdot]$ secure

More Generic Constructions of 2-key KEM

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

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

Roadmap



AKE
Interactive
2-key KEM
Non-interactive
HMQV
OAKE
NAXOS
Okamoto
Improved KEM Combiner
FXSY12
FXSY13
Improved FO
[CPA,CPA] 2-key PKE

AKE from Lattice

- ZDD+15 proposed HMQV-type RLWE with BR and wPRF security

  e_1 e_2 e_3 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

ZZD+15, Zhang J., Zhang Z., Ding J., Snook M., Dagdelen O EUROCRYPT 2015.

BDK+18, Bos, J.W., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schanck, J.M., Schwabe, P., Stehle, D Euro S&P 2018

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