基于同源的
后量子认证密钥交换协议
-以及新进展

薛海洋

2020/9/28

目录

- 认证密钥交换协议（AKE）以及同源问题

- SIAKE-基于同源的AKE

- 后续研究进展
  - 量子随机预言模型（QROM）下的安全性
  - 框架以及具体方案的紧归约？

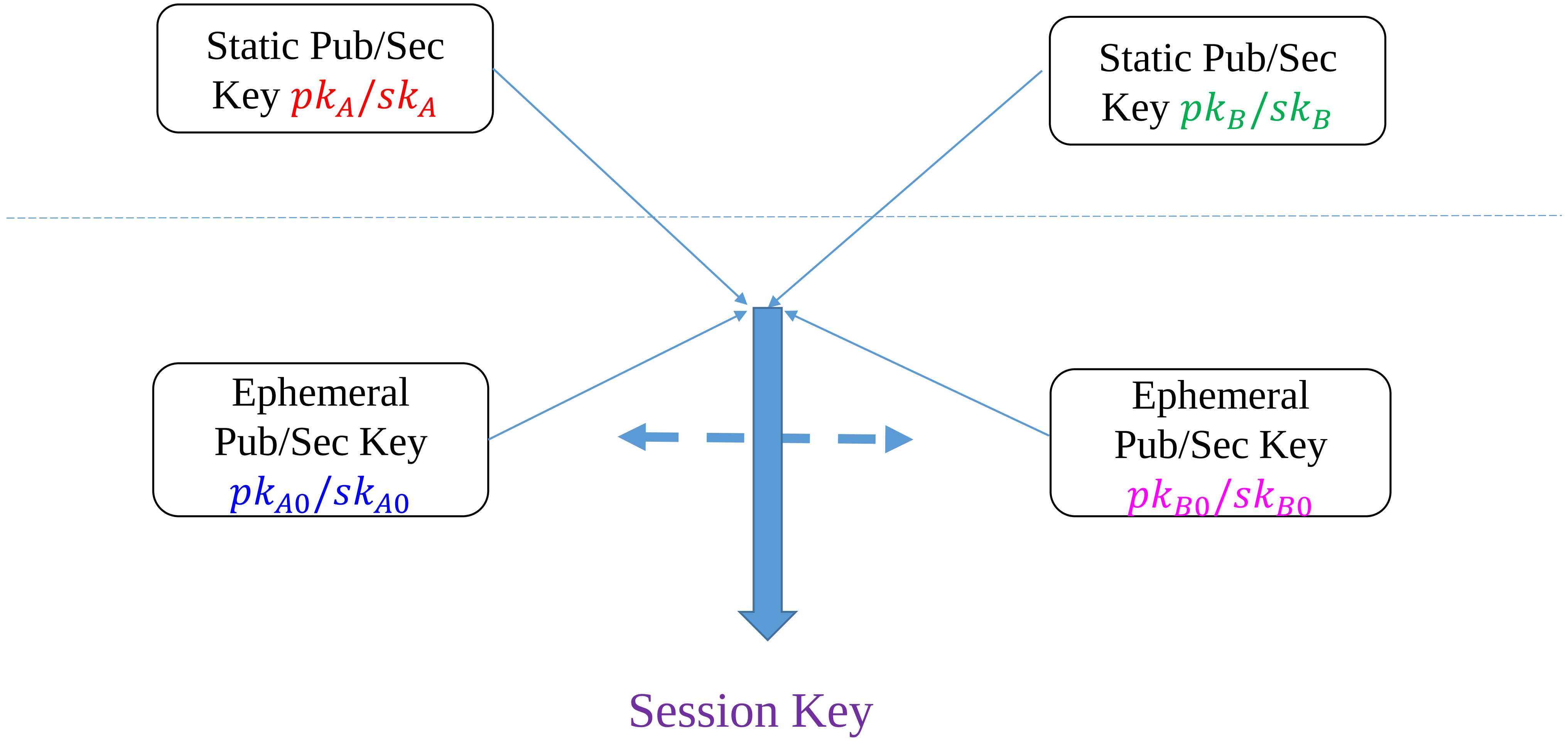
Authenticated Key Exchange (AKE)

U_A		U_B
$x \to g^x = X$	$\xrightarrow{\quad X \quad}$	$y \to g^y = Y$
$K = Y^x$	$\xleftarrow{\quad Y \quad}$	$K = X^y$

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

Authenticated Key Exchange (AKE)

- Binding id with static public key using PKI etc.



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

Constructions of AKE

- 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**: provable secure implicit-AKE via gap-DH and KEA
4. **YZ13:** OAKE
5. **Oka 07**: in standard model from DDH (Hashing Proof Sys.)
6. **LLM 07**: NAXOS scheme from gap-DBDH
7. **Boyd 08**: Diffie-Hellman+KEM
8. **FSXY 12**: 2CCA+CPA-KEM, std.
9. **FSXY 13**: 2CCAKEM,RO
10. **ZZD+15**: HMQV-type based on RLWE with weaker aim

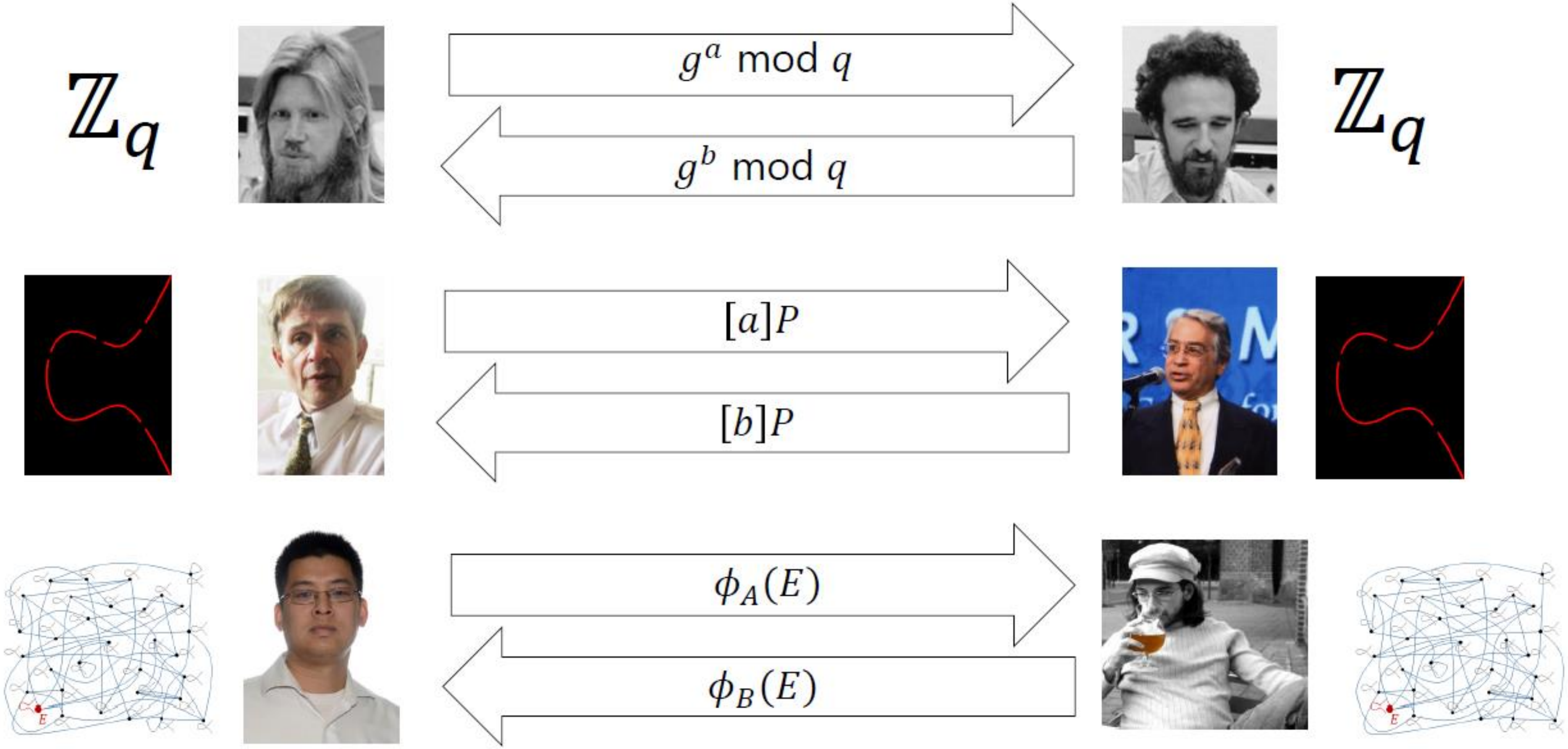
后量子安全AKE

- 后量子安全加密和签名正接近标准化（NIST）

- 然而后量子安全AKE的研究处于不完全的阶段;
  - AKE的安全性定义复杂(数10种敌手)
  - 半经典半后量子的过渡方案

数学结构	特点
Lattice	研究充分，综合性能最优
Isogeny 同源	尺寸上表现最优
编码	和Lattice 相互借鉴
Hash	适合设计签名
多变量	Rainbow签名

超奇异曲线同源的（超）简单介绍



From Croatia's slides

[JAC+18] Jao, D., Azarderakhsh, R., Campagna, M., et al: Supersingular Isogeny Key Encapsulation. NIST Round 3.

超奇异曲线同源的（超）简单介绍

	DH	ECDH	SIDH
Elements	integers g modulo prime	points P in curve group	curves E in isogeny class
Secrets	exponents x	scalars k	isogenies ϕ
computations	$g, x \mapsto g^x$	$k, P \mapsto [k]P$	$\phi, E \mapsto \phi(E)$
hard problem	given g, g^x find x	given $P, [k]P$ find k	given $E, \phi(E)$ find ϕ

[JAC+18] Jao, D., Azarderakhsh, R., Campagna, M., et al: Supersingular Isogeny Key Encapsulation. NIST Round 3.

超奇异曲线同源的（超）简单介绍

- 设 E_1 和 E_2 为定义在 F_q 上两条椭圆曲线，如果非常值有理映射

$$\phi: E_1 \to E_2,$$

是 E_1 到 E_2 的群同态，则称它为同源映射.

设 H是曲线 E 的有限子群，则存在唯一的椭圆曲线E' （在同构意义下）和可分同源

$$\phi: E \to E' \text{ 使得 } Ker(\phi) = H.$$

一般记为 $E' = \phi(E) = E/\langle H\rangle$

基于同源的Diffie-Hellman（SIDH）

$$\begin{tikzcd} g \arrow[r, "x"] \arrow[d, "y"'] & g^x \arrow[d, dashed] \\ g^y \arrow[r, dashed] & g^{xy} \end{tikzcd}$$

$$\boxed{\phi_A(P_B), \phi_B(P_A)}$$

$$\begin{tikzcd} E \arrow[r, "\phi_A"] \arrow[d, "\phi_B"'] & \frac{E}{H_A} \arrow[d, dashed] \\ \frac{E}{H_B} \arrow[r, dashed] & \frac{E}{\langle H_A, H_B \rangle} \end{tikzcd}$$

若能计算 $\frac{\langle H_A, H_B\rangle}{H_A}$, 则能得到 $\frac{E}{\langle H_A, H_B\rangle}$

$$\boxed{\frac{\frac{E}{H_A}}{\frac{\langle H_A, H_B\rangle}{H_A}} \cong \frac{E}{\langle H_A, H_B\rangle}}$$

$$H_B = \langle m_B P_B + n_B Q_B \rangle$$

私钥　公开参数

$$\frac{\langle H_A, H_B\rangle}{H_A} = \phi_A(\langle H_A, H_B\rangle)$$
$$= \langle \phi_A(H_A), \phi_A(H_B)\rangle$$
$$= \langle \phi_A(H_B)\rangle \quad = \langle m_B \phi_A(P_B) + n_B \phi_A(Q_B)\rangle$$

From Tian Song

SIDH→AKE Challenges

1. Sign-MAC? Signature via SIDH $O(\lambda^2)$
2. g^{ad+x}
3. Adaptive attack. Public Key Validation
4. Gap assumption

Open Problem[Gal18]: Strongly Secure AKE from SIDH?

[Gal18] Galbraith, S. D.: *Authenticated key exchange for SIDH*. **ePrint Archive 2018/266**.

SIAKE概述

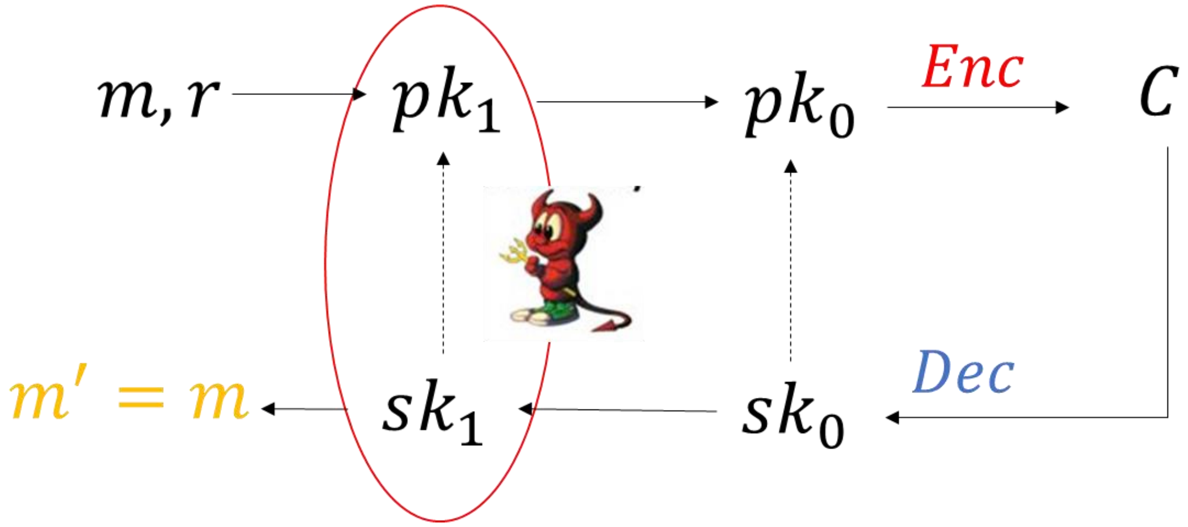
CK+ AKE

[XLL+18] ↑ 经典RO模型

[OW-CPA, OW-CPA]
2-key PKE

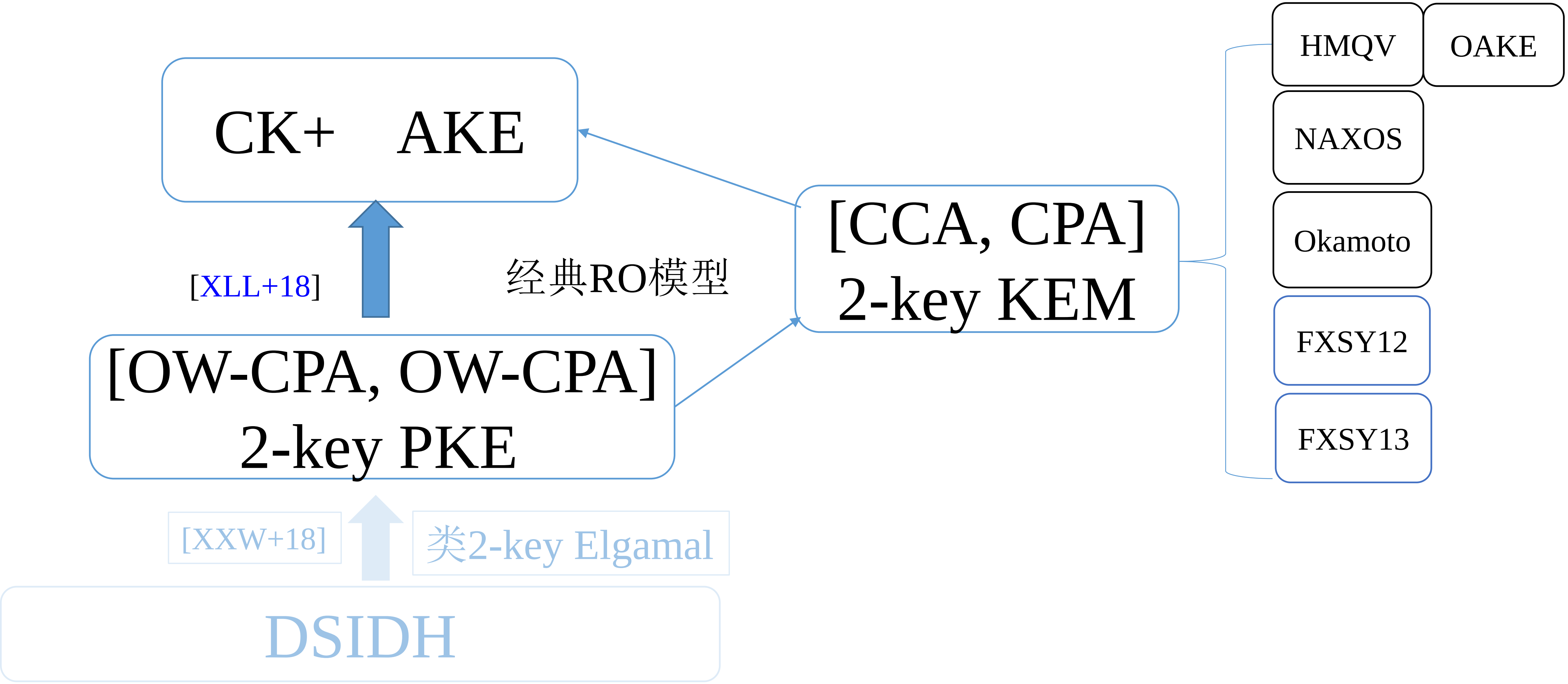
[XXW+18] ↑ 类2-key Elgamal

DSIDH



[XLL+18] Haiyang Xue, Xianhui Lu, Bao Li, Bei Liang, Jingnan He, Understanding and Constructing of AKE via 2-key KEM, **ASIACRYPT 2018**
[XXW+18] Xiu Xu, Haiyang Xue, Kunpeng Wang, Man Ho Au, Song Tian, Strongly secure AKE from Supersingular Isogenies, **ASIACRYPT2019**

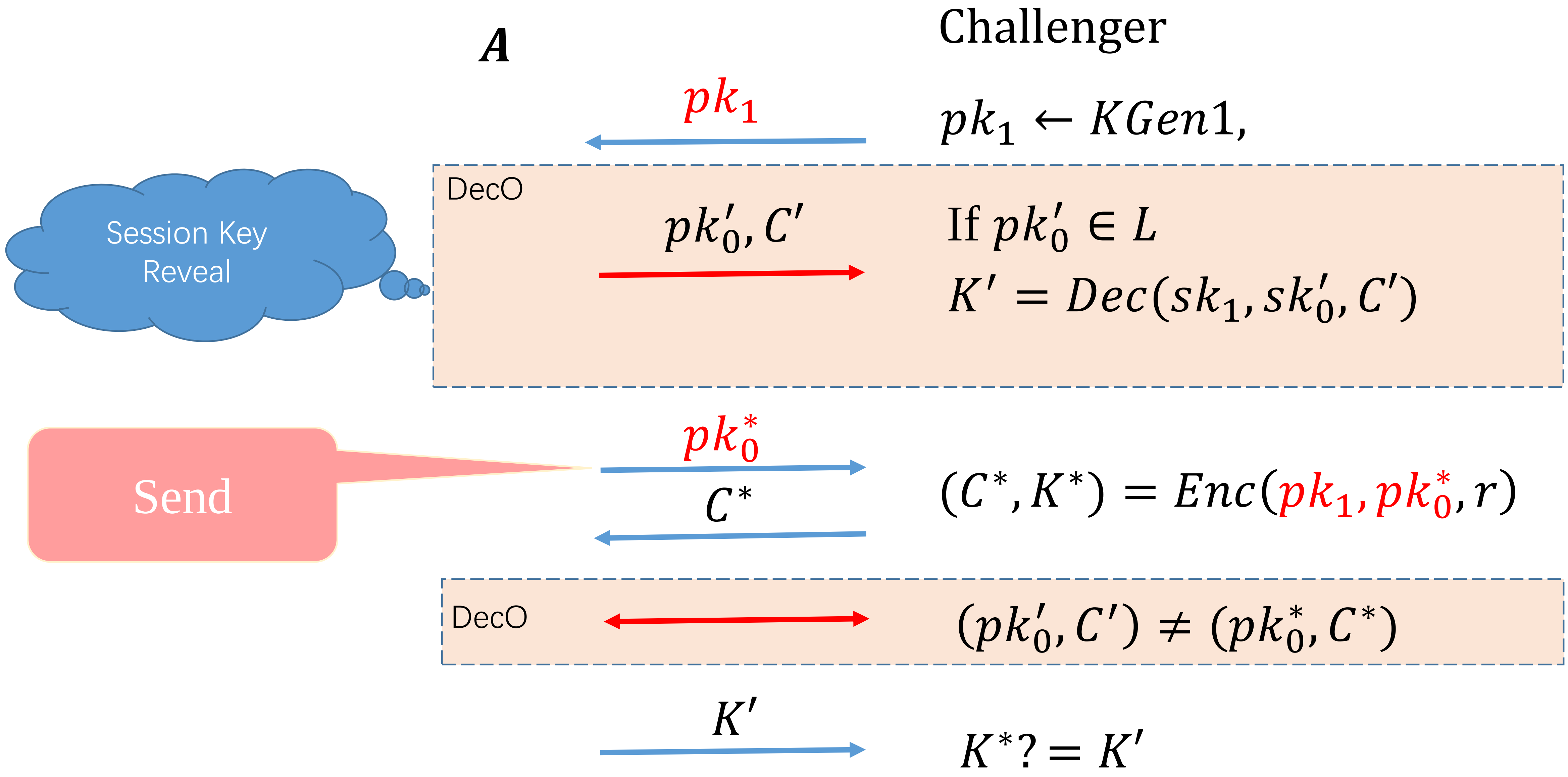
SIAKE概述



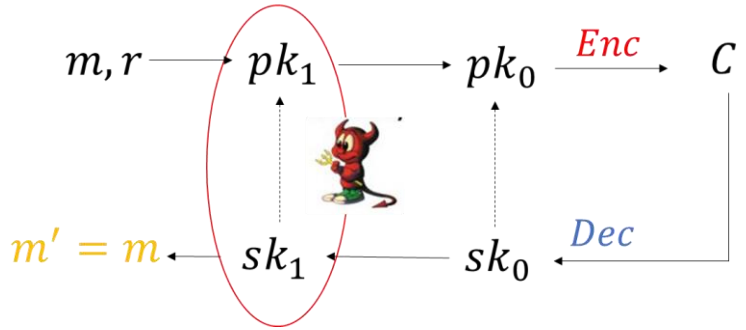
[XLL+18] Haiyang Xue, Xianhui Lu, Bao Li, Bei Liang, Jingnan He, Understanding and Constructing of AKE via 2-key KEM, **ASIACRYPT 2018**

[XXW+18] Xiu Xu, Haiyang Xue, Kunpeng Wang, Man Ho Au, Song Tian, Strongly secure AKE from Supersingular Isogenies, **ASIACRYPT2019**

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



2-key PKE



$$g^{r_1}, h_1^{r_1} \oplus m_1 \;||\; g^{r_2}, h_2^{r_2} \oplus m_2$$

$$g^{r}, H(h_1^{r}) \oplus m_1, H(h_1^{r}) \oplus m_2$$

SIAKE19

$$g^{r_1}, g^{r_2}, h_1^{r_1} \oplus h_2^{r_2} \oplus m$$

2Kyber18

SIAKE

参数(256)	A to B (Bytes)	B to A (Bytes)	Total(Bytes)
SIAKEp751	1160	628	1788
Lattice-Kyber	2912	3008	5912

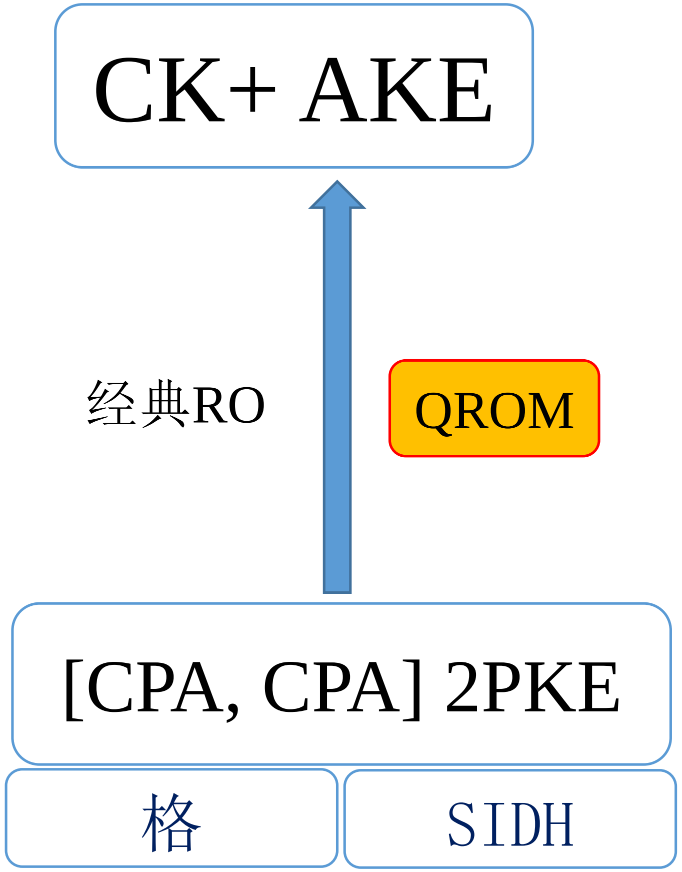
- SIAKE 通信还可以进一步压缩40%
- 缺点：计算效率慢

一些进展

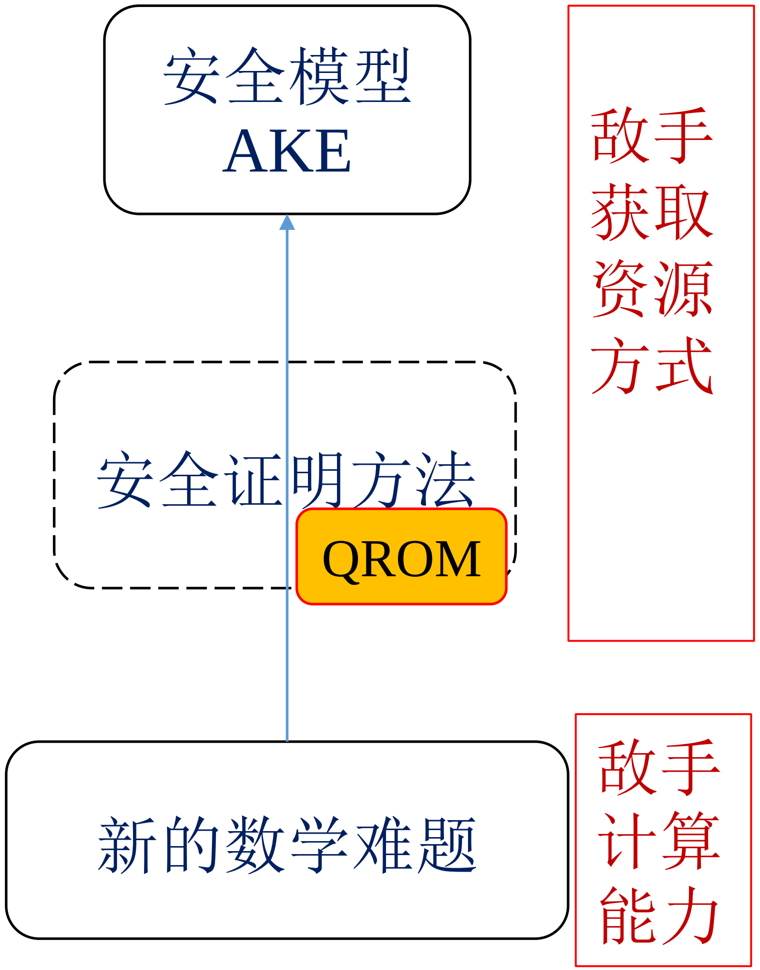
- 量子随机预言模型下的安全性
  - 必要性及我们的结果

- 紧归约问题
  - 理论 与 实际意义，初步工作

量子随机预言模型（QROM）



- QROM安全的必要性
- QROM-AKE公开问题 2013---
- 我们证明了所述框架（*略微修改*）的QROM安全性



Several techniques for FO in QROM

$Dec(\cancel{sk}, C)$	$C^* = Enc(pk, m^*, r^*)$ | $r^* = G(m^*)$ | $K^* = h(m^*)$
ROM G-list h-list	If $m^* \notin$ h-list G-list r^* K^*
$C \mid H(m)$	$\boxed{\text{OW2H Lemma}}$ 增加密文 [TU16] [HHK17]
QROM	
$h(m) := h_q \circ Enc(pk, m, G(m))$	$\boxed{\text{OW2H Lemma}}$ Puncture [SXY18]-1 [HKSU18] Additional Hash [SXY18]-2 One Way [JZC+18]

Several techniques for FO in QROM

$$Dec(\cancel{sk}, C) \qquad\qquad C^* = Enc(pk, m^*, r^*) \mid r^* = G(m^*) \mid K^* = h(m^*)$$

QROM [BDF+11]

If $h(m) \coloneqq h_q \circ Enc(pk, m, G(m))$

$$\begin{tikzcd}
m \arrow[r, dashed, "Enc(pk, m; G(m))", "\text{Injective mapping}"'] \arrow[d, "h"'] & C \arrow[dl, dashed, "h_q"] \\
h(m) &
\end{tikzcd}$$

$$\boxed{h(Dec(sk, C)) = h_q \circ Enc\big(pk, Dec(sk, C)\big) = h_q(C)}$$

Challenges for our AKE in QROM

$Dec(\cancel{sk_1}, sk_0, C)$ $\quad\quad$ $C^* = Enc(pk_1, pk_0, m^*, r^*) \mid \mathrm{K}^* = h(pk_1, pk_0^*, m^*)$

---

1. Putting pk_1, pk_0 in to h

2. $h(pk_1, pk_0, m) = H_q(pk_1, pk_0, Enc(pk_1, pk_0, m, G(m)))$ injective????

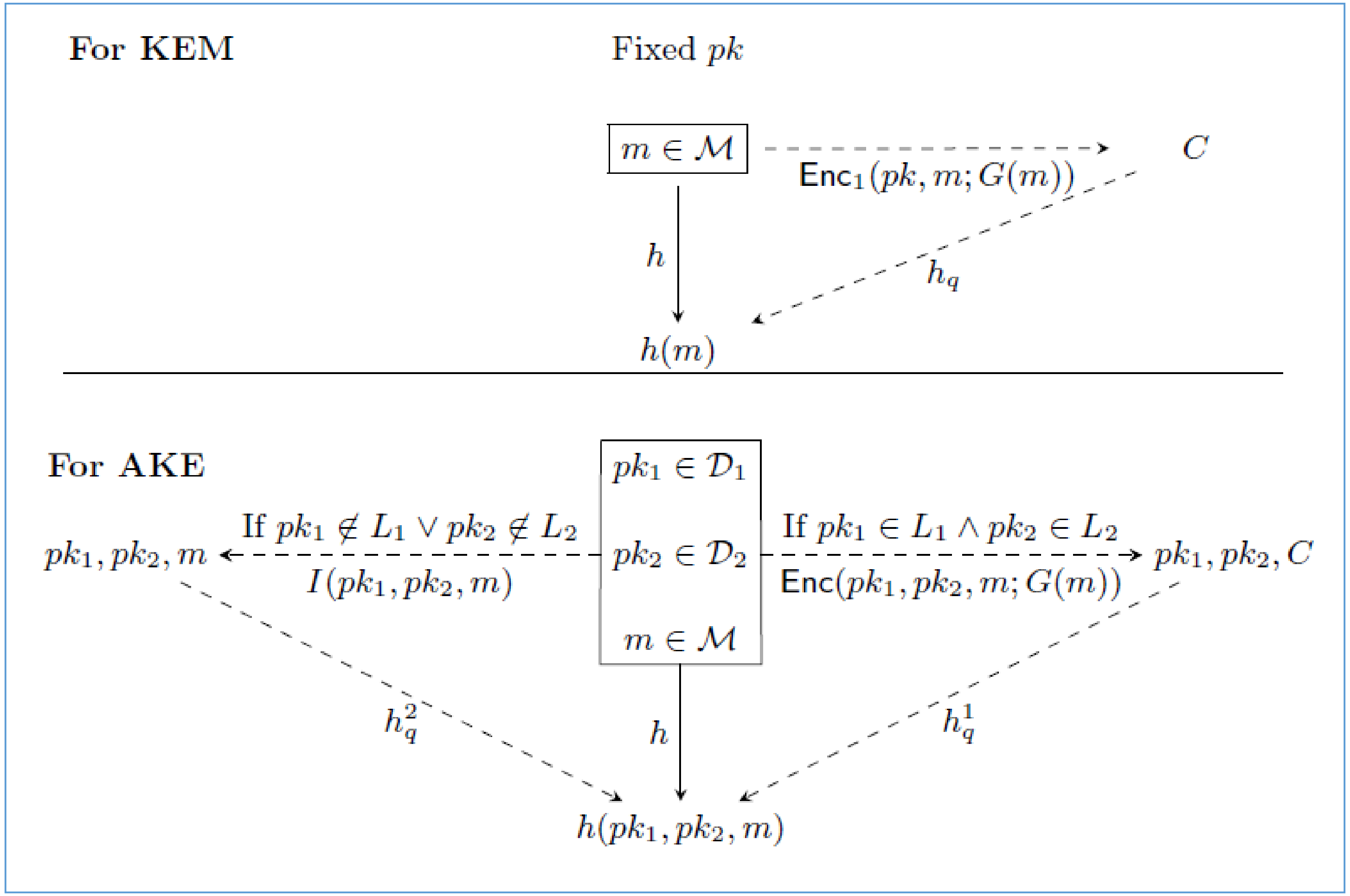
3.敌手可以选择 pk_0^*????

Challenges for our AKE in QROM

$Dec(\cancel{sk_1}, sk_0, C)$ $C^* = Enc(pk_1, pk_0, m^*, r^*)$ | $K^* = h(pk_1, pk_0^*, m^*)$

1. Putting pk_1, pk_0 in to h
2. Injective????

Domain Separation and
Injective mapping under many pks



3.敌手可以选择 pk_0^*

QROM结果（投稿中）

- AKE框架在QROM下的安全性

✓SIAKE [XLW+19]

✓FSXY13 （2013的公开问题）

✓2Kyber-AKE

- Multi-uer QROM
  - Putting public key into h; 争论中。。。。
  - 攻击 vs 证明

[XLW+19]薛海洋，路献辉，王鲲鹏，田松，徐秀，贺婧楠，李宝，SIAKE:基于超奇异同源的认证密钥交换协议，**算法竞赛**

紧归约问题？

$$\epsilon_{AKE} \leq l_{loss} \cdot \epsilon_{SIDH}$$

$l_{loss} = N^2 l$	2^{128}	2^{40}	2^{168}
$l_{loss} = o(1)$	2^{128}	$o(1)$	2^{128}

紧归约问题

- 显式认证+签名

  [BHJKL-TCC15] [GJ-CRYPTO18] [XZM-RSA20] [LLGW-eprint20]

- 隐式认证

  [CCGJJ-CRYPTO19] $l_{loss} = N$

紧归约问题

AKE	Multi-auth	KeyReveal	长期临时公钥	Corruption
KEM	Multi-user	[CCA,.]	2-key	Corruption
困难问题	随机自归约 Commutative SIDH		AND	OR proof

PK为2倍，通信量增加30%

可能的后续工作。。。

- QROM下的紧归约问题

- 基于同源的多用户签名，QROM？紧归约？
  - Lossy identification, sign with corruption?

总结

- 同源问题
- SIAKE
- QROM
- 紧归约

参考文献

Haiyang Xue, Xianhui Lu, Bao Li, Bei Liang, Jingnan He, Understanding and Constructing AKE via Double-key Key Encapsulation Mechanism, ASIACRYPT 2018

Xiu Xu, Haiyang Xue, Kunpeng Wang, Man Ho Au, Song Tian, Strongly Secure Authenticated Key Exchange from Supersingular Isogenies, ASIACRYPT 2019

薛海洋，路献辉，王鲲鹏，田松，徐秀，贺婧楠，李宝，SIAKE:基于超奇异同源的认证密钥交换协议, 算法竞赛

Haiyang Xue, Man Ho Au, Rupeng Yang, Bei Liang, Haodong Jiang, Compact Authenticated Key Exchange in the Quantum Random Oracle Model（投稿中）