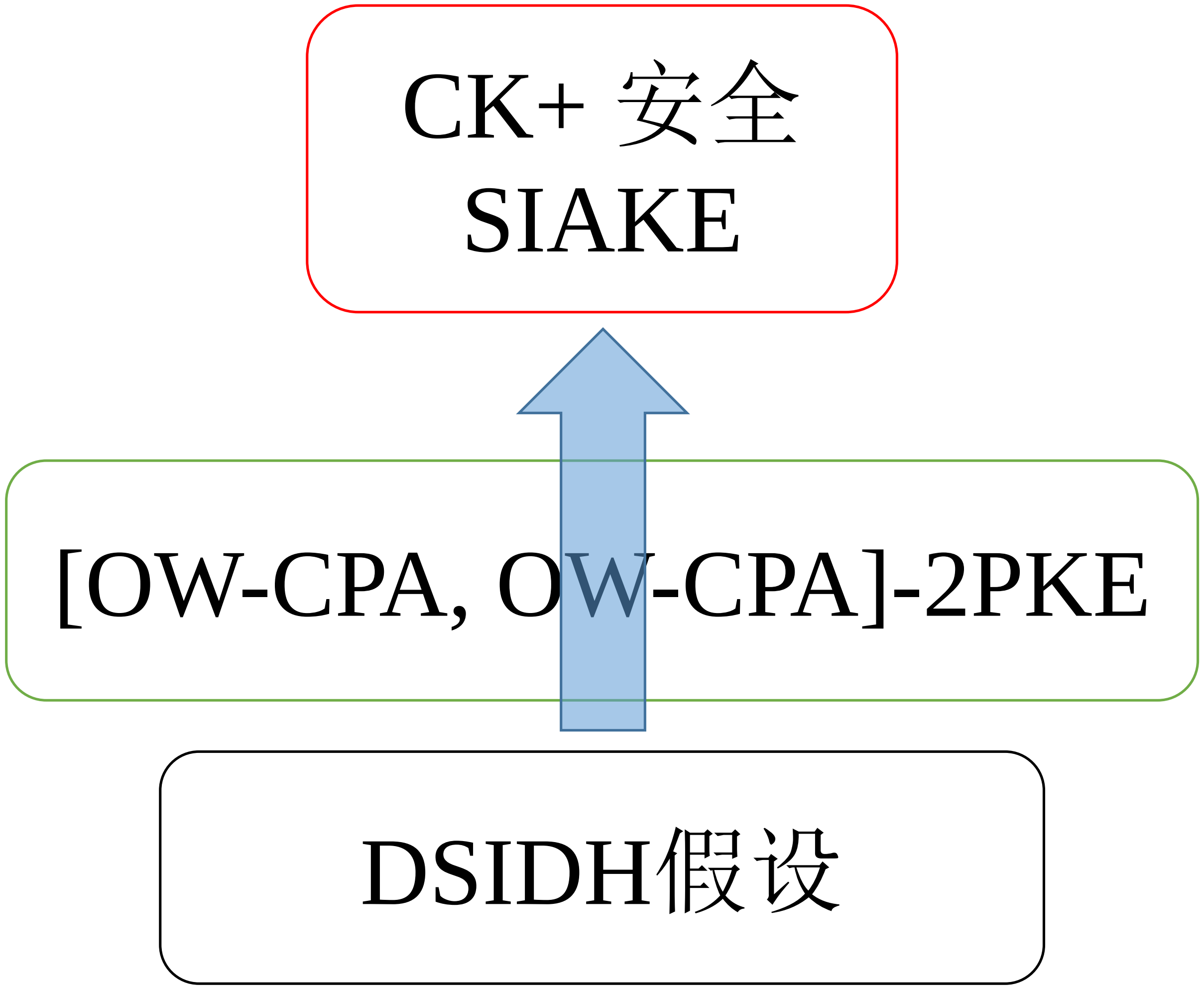
SIAKE
-基于超奇异同源的认证密钥交换协议

薛海洋、路献辉、王鲲鹏、田松、徐秀、贺婧楠、李宝

信息安全重点实验室
DCS中心

SIAKE概述

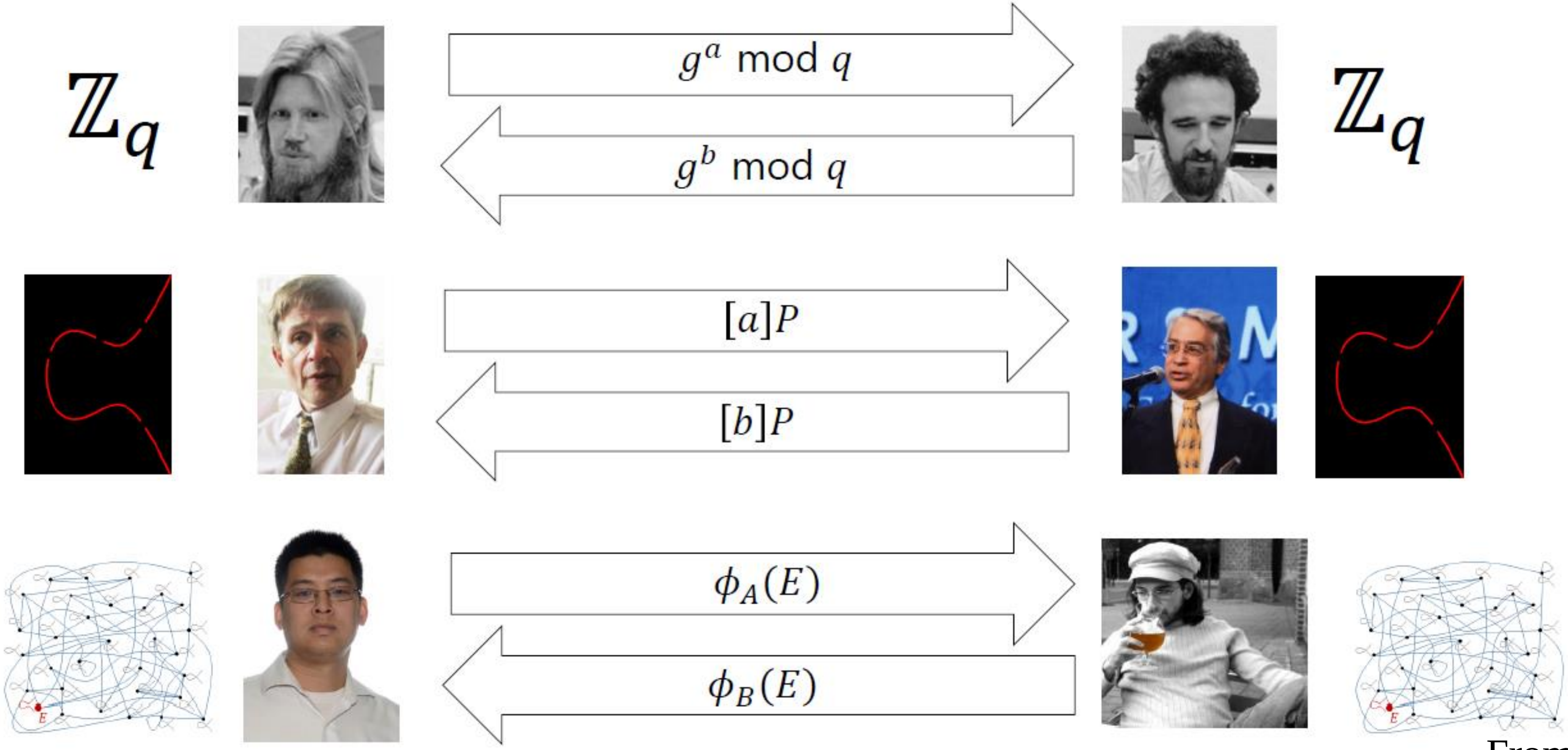
- 隐式认证密钥交换协议
- 基于超奇异椭圆曲线上的同源困难假设
- 经典和量子随机预言模型下CK+安全性



目录

- 基础SIDH（aka. SIKE）算法
- CK+AKE以及构造框架
- SIAKE的具体构造

Diffie-Hellman Key Exchange



From Croatia's slides

[JAC+18] Jao, D., Azarderakhsh, R., Campagna, M., et al: Supersingular Isogeny Key Encapsulation. NIST Round 2.

椭圆曲线→超奇异同源

- $a: P \to [a]P$

where P is a point over $E(F_q)$

- Given two points P and $[a]P$, compute a?

- $\phi: E \to \phi(E)$

- Given two curves E and $\phi(E)$, (and $\phi(P), \phi(Q)$) compute ϕ?

SIDH: in a nutshell

params public private

E's are isogenous curves
P's, Q's, R's, S's are points

$$
\begin{tikzcd}
 & E_0 \arrow[r, Rightarrow, "\phi_A"] \arrow[d, Rightarrow, "\phi_B"'] & E_A = E_0/\langle A \rangle \arrow[d, Rightarrow, "\phi_B'"'] \\
E_0/\langle B \rangle = & E_B \arrow[r, Rightarrow, "{\phi_A}'"] & E_{AB} = E_0/\langle A, B \rangle
\end{tikzcd}
$$

SIDH: in a nutshell

params   public   private

E's are isogenous curves
P's, Q's, R's, S's are points

$$
\begin{tikzcd}
E_0 \arrow[r, Rightarrow, "\phi_A"] \arrow[d, Rightarrow, "\phi_B"'] & E_A = E_0/\langle P_A + [s_A]Q_A \rangle \arrow[d, Rightarrow, "\phi_B'"] \\
E_0/\langle P_B + [s_B]Q_B \rangle = E_B \arrow[r, Rightarrow, "\phi_A{}'"] & E_{AB} = E_0/\langle A, B \rangle
\end{tikzcd}
$$

$(R_A, S_A) = (\phi_A(P_B), \phi_A(Q_B))$

$(\phi_B(P_A), \phi_B(Q_A)) = (R_B, S_B)$

Key: Alice sends her isogeny evaluated at Bob's generators, and vice versa

$$E_A/\langle R_A + [s_B]S_A \rangle \cong E_0/\langle P_A + [s_A]Q_A\,, P_B + [s_B]Q_B \rangle \cong E_B/\langle R_B + [s_A]S_B \rangle$$

SIDH

Alice

$k_A \in_R SK_A$:

Alice's secret key,

$R_A = P_A + k_A Q_A$,

$\phi_A : E \to E_A = E/\langle R_A \rangle$,

$R_{BA} = \phi_B(P_A) + k_A\, \phi_B(Q_A)$,

$K_{Alice} = j(E_B/\langle R_{BA} \rangle)$.

$$\xrightarrow{E_A,\ \phi_A(P_B),\ \phi_A(Q_B)}$$

$$\xleftarrow[E_B,\ \phi_B(P_A),\ \phi_B(Q_A)]{}$$

Bob

$k_B \in_R SK_B$:

Bob's secret key,

$R_B = P_B + k_B Q_B$,

$\phi_B : E \to E_B = E/\langle R_B \rangle$,

$R_{AB} = \phi_A(P_B) + k_B\, \phi_A(Q_B)$,

$K_{Bob} = j(E_A/\langle R_{AB} \rangle)$.

Fig. 1. Outline of SIDH Protocol (Original Description).

Crypto-friendly Notions[FTTY18]

$\mathfrak{g} = (E_0; P_1, Q_1, P_2, Q_2)$ and $\mathfrak{e} = (\ell_1, \ell_2, e_1, e_2)$. Let the sets of supersingular curves with an auxiliary basis be

$$\mathrm{SSEC}_p = \{\text{supersingular elliptic curves } E \text{ over } \mathbb{F}_{p^2} \text{ with } E(\mathbb{F}_{p^2}) \simeq (\mathbb{Z}_{\ell_1^{e_1}\ell_2^{e_2}f})^2\};$$

$$\mathrm{SSEC}_A = \{(E; P'_t, Q'_t) | E \in \mathrm{SSEC}_p, (P'_t, Q'_t) \text{ is basis of } E[\ell_t^{e_t}]\};$$

$$\mathrm{SSEC}_B = \{(E; P'_s, Q'_s) | E \in \mathrm{SSEC}_p, (P'_s, Q'_s) \text{ is basis of } E[\ell_s^{e_s}]\}.$$

Let $\mathfrak{a} = k_a$ and $\mathfrak{b} = k_b$, then we define,

$$\mathfrak{g}^{\mathfrak{a}} = (E_A; \phi_A(P_t), \phi_A(Q_t)) \in \mathrm{SSEC}_A, \text{ where } R_A = P_s + [k_a]Q_s, \phi_A : E_0 \to E_A = E_0/\langle R_A \rangle;$$

$$\mathfrak{g}^{\mathfrak{b}} = (E_B; \phi_B(P_s), \phi_B(Q_s)) \in \mathrm{SSEC}_B, \text{ where } R_B = P_t + [k_b]Q_t, \phi_B : E_0 \to E_B = E_0/\langle R_B \rangle;$$

$$(\mathfrak{g}^{\mathfrak{b}})^{\mathfrak{a}} = j(E_{BA}), \text{ where } R_{BA} = \phi_B(P_s) + [k_a]\phi_B(Q_s), \phi_{BA} : E_B \to E_{BA} = E_B/\langle R_{BA} \rangle;$$

$$(\mathfrak{g}^{\mathfrak{a}})^{\mathfrak{b}} = j(E_{AB}), \text{ where } R_{AB} = \phi_A(P_t) + [k_b]\phi_A(Q_t), \phi_{AB} : E_A \to E_{AB} = E_A/\langle R_{AB} \rangle.$$

[FTTY18] Fujioka, A., Takashima, K., Terada, S., Yoneyama, K.:
Supersingular Isogeny Diffie-Hellman Authenticated Key Exchange. IACR Cryptology ePrint Archive 2018/730.

SIDH with Crypto-friendly Notions[FTTY18]

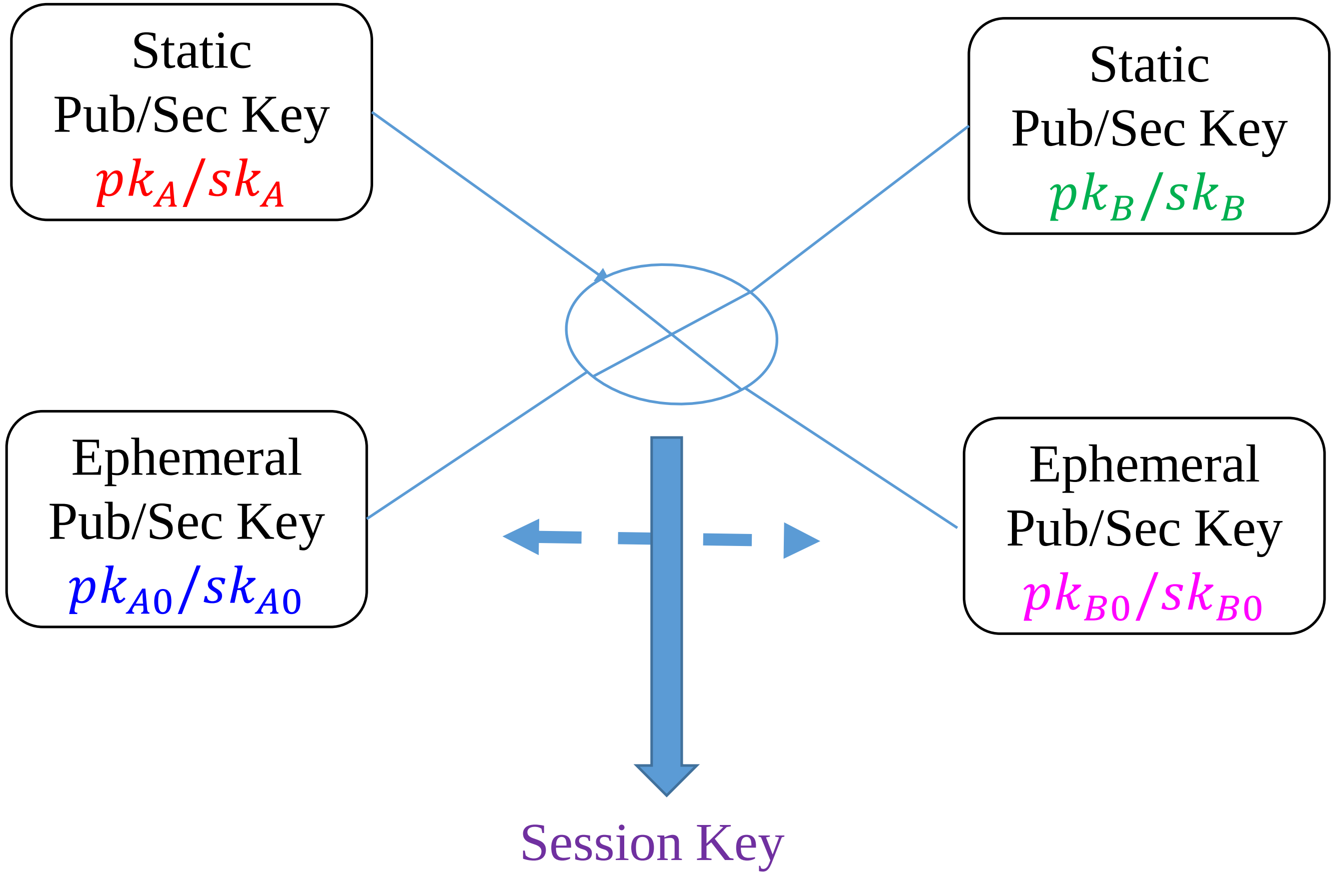
Alice		**Bob**
$\mathfrak{a} \in_R SK_{\mathtt{A}}$: Alice′s secret key,	$\xrightarrow{\mathfrak{g}^{\mathfrak{a}}}$	$\mathfrak{b} \in_R SK_{\mathtt{B}}$: Bob′s secret key,
compute $\mathfrak{g}^{\mathfrak{a}}$,	$\xleftarrow[\mathfrak{g}^{\mathfrak{b}}]{}$	compute $\mathfrak{g}^{\mathfrak{b}}$,
$K_{\mathtt{Alice}} = (\mathfrak{g}^{\mathfrak{b}})^{\mathfrak{a}}$.		$K_{\mathtt{Bob}} = (\mathfrak{g}^{\mathfrak{a}})^{\mathfrak{b}}$.

Fig. 2. Outline of SIDH Protocol (Crypto-friendly Description).

目录

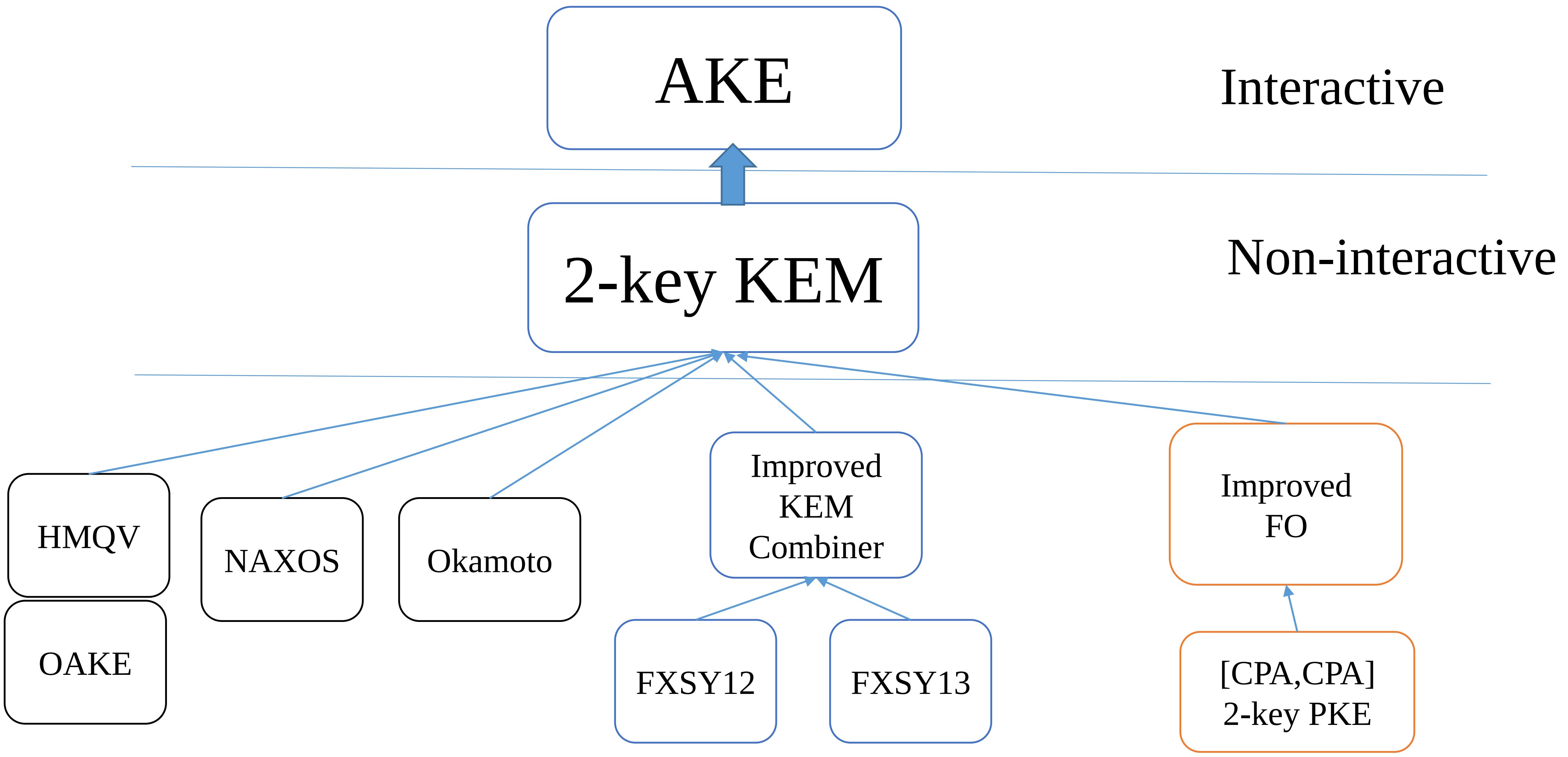
- 基础SIDH（aka. SIKE）算法
- CK+AKE以及构造框架
- SIAKE的具体构造

AKE 以及CK+安全性



- CK 安全性
- 弱前向安全性
- KCI
- MEX
- 任意注册公钥

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设计原理

CK+ AKE

[XLL+18] ↑ 经典（量子）RO模型

[OW-CPA, OW-CPA]
2PKE

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

$[OW-CPA,\cdot]$ Security of 2-key PKE

$\boldsymbol{A}$ Challenger

$\xleftarrow{pk_1, L}$ $pk_1 \leftarrow KGen1, L = \{pk_0^i / sk_0^i\} \leftarrow KGen0$

$\xrightarrow{pk_0^*}$

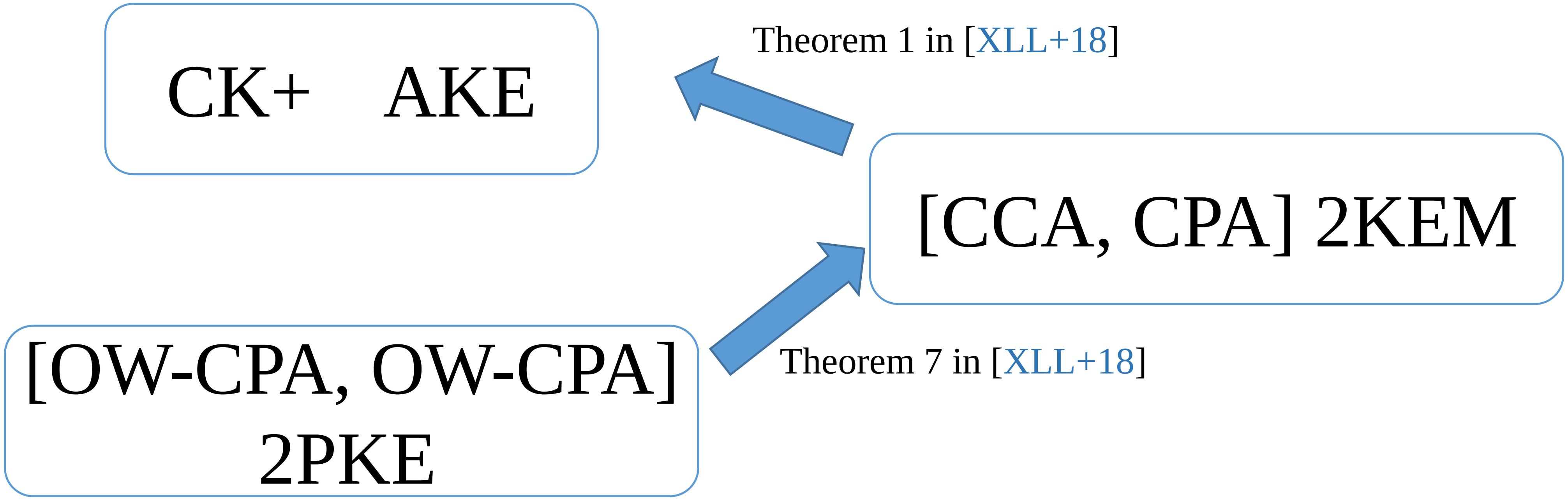
$\xleftarrow{C^*}$ $C^*, = Enc(pk_1, pk_0^*, r; m^*)$

$\xrightarrow{m'}$ $m^* ?= m'$

$[\cdot, OW-CPA]$ Security of 2-key PKE

$\boldsymbol{A}$		Challenger
	$\xleftarrow{pk_0, L}$	$pk_0 \leftarrow KGen0, L = \{pk_1^i/sk_1^i\} \leftarrow KGen1$
	$\xrightarrow{pk_1^*}$	
	$\xleftarrow{C^*}$	$C^* = Enc(pk_1^*, pk_0, r; m^*)$
	$\xrightarrow{m'}$	$m^* ?= m'$

AKE设计原理



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

AKE设计原理

Theorm 1 and Theorem 7 in [XLL+18]

CK+ AKE

[XLL+18] 经典RO模型

[OW-CPA, OW-CPA]
2PKE

$m, r \rightarrow pk_1 \rightarrow pk_0 \xrightarrow{Enc} C$

$m' = m \leftarrow sk_1 \leftarrow sk_0 \xleftarrow{Dec} C$

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

目录

- 基础SIDH（aka. SIKE）算法
- CK+AKE以及构造框架
- SIAKE的具体构造

SIAKE设计原理

CK+ SIAKE

[XLL+18]
[XAL+19]

经典（量子）RO模型

[OW-CPA, OW-CPA]
2PKE

[XXW+18]

类2-key Elgamal

DSIDH

- 因此重点在于基于SIDH
- 构造[OW-CPA, OW-CPA] 2PKE

[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, Bei Liang, Song Tian, Strongly secure AKE from Supersingular Isogeny, **eprint 2018\760**

[OW-CPA, OW-CPA] 2PKE from SIDH

– KeyG1(n,pp): on input security parameter and public parameter, randomly choose a secret $\mathfrak{a}_1 \leftarrow \mathbb{Z}_{\ell_s^{e_s}}$ and compute $\mathfrak{g}^{\mathfrak{a}_1}$. Then output

$$sk_1 := \mathfrak{a}_1, pk_1 := \mathfrak{g}^{\mathfrak{a}_1}.$$

– KeyG0(n,pp): on input security parameter and public parameter, randomly choose a secret $\mathfrak{a}_0 \leftarrow \mathbb{Z}_{\ell_s^{e_s}}$ and compute $\mathfrak{g}^{\mathfrak{a}_0}$. Then output

$$sk_0 := \mathfrak{a}_0, pk_0 := \mathfrak{g}^{\mathfrak{a}_0}.$$

[XXW+18] Xiu Xu, Haiyang Xue, Kunpeng Wang, Bei Liang, Song Tian, Strongly secure AKE from Supersingular Isogeny, **eprint 2018\760**

[OW-CPA, OW-CPA] 2PKE from SIDH

- $\mathsf{Enc}(pk_1, pk_0, m)$: on input public keys and a message $m = m_1 || m_0 \in \{0,1\}^{2n}$, randomly choose $\mathfrak{b} \leftarrow \mathbb{Z}_{\ell_t^{e_t}}$ and compute $\mathfrak{g}^{\mathfrak{b}}$, $h((\mathfrak{g}^{\mathfrak{a}_1})^{\mathfrak{b}}) \oplus m_1$ and $h((\mathfrak{g}^{\mathfrak{a}_\circ})^{\mathfrak{b}}) \oplus m_0$. The ciphertext is

$$c := \left(\mathfrak{g}^{\mathfrak{b}}, h\left((\mathfrak{g}^{\mathfrak{a}_1})^{\mathfrak{b}}\right) \oplus m_1, h\left((\mathfrak{g}^{\mathfrak{a}_\circ})^{\mathfrak{b}}\right) \oplus m_0\right).$$

- $\mathsf{Dec}(sk_1, sk_0, c)$: on input secret keys $sk_1 = \mathfrak{a}_1$, $sk_0 = \mathfrak{a}_\circ$ and ciphertext $c = (\mathfrak{c}_1, c_2, c_3)$, compute $m_1 := c_2 \oplus h\left(\mathfrak{c}_1^{\mathfrak{a}_1}\right)$ and $m_0 := c_3 \oplus h\left(\mathfrak{c}_1^{\mathfrak{a}_\circ}\right)$. The plaintext is $m = m_1 || m_0$.

[XXW+18] Xiu Xu, Haiyang Xue, Kunpeng Wang, Bei Liang, Song Tian, Strongly secure AKE from Supersingular Isogeny, **eprint 2018\760**

SIAKE

U_A		U_B
$sk_{A_1} := (\mathfrak{a}_1 \in \mathbb{Z}_{\ell_1^{e_1}}, s_{A1} \leftarrow \{0,1\}^{2n})$		$sk_{B_2} := (\mathfrak{b}_2 \in \mathbb{Z}_{\ell_2^{e_2}}, s_{B2} \leftarrow \{0,1\}^{2n})$
$pk_{A_1} := \mathfrak{g}^{\mathfrak{a}_1}$		$pk_{B_2} := \mathfrak{g}^{\mathfrak{b}_2}$
$sk_{A_2} := (\mathfrak{a}_2 \in \mathbb{Z}_{\ell_2^{e_2}}, s_{A2} \leftarrow \{0,1\}^{2n})$		$sk_{B_1} := (\mathfrak{b}_1 \in \mathbb{Z}_{\ell_1^{e_1}}, s_{B1} \leftarrow \{0,1\}^{2n})$
$pk_{A_2} := \mathfrak{g}^{\mathfrak{a}_2}$		$pk_{B_2} := \mathfrak{g}^{\mathfrak{b}_2}$
$r_A \leftarrow \mathbb{Z}_{\ell_1^{e_1}}, n_1 \leftarrow g(r_A, \mathfrak{a}_1)$		
$\mathfrak{x} \leftarrow G(n_1), \mathfrak{x}_\circ \leftarrow \mathbb{Z}_{\ell_1^{e_1}}.$		$r_B \leftarrow \mathbb{Z}_{\ell_2^{e_2}}, m_1 \Vert m_0 \leftarrow g(r_B, \mathfrak{b}_2)$
$X_0 := \mathfrak{g}^{\mathfrak{x}_\circ}$		$\mathfrak{y} \leftarrow G(m_1, m_0)$
$X := \mathfrak{g}^{\mathfrak{x}}, x_1 := h((\mathfrak{g}^{\mathfrak{b}_2})^{\mathfrak{x}}) \oplus n_1$	$\xrightarrow{X, x_1, X_0}$	$Y := \mathfrak{g}^{\mathfrak{y}}, y_1 := h((\mathfrak{g}^{\mathfrak{a}_1})^{\mathfrak{y}}) \oplus m_1$
$K_A := H(n_1, X, x_1)$		$y_0 := h((\mathfrak{g}^{\mathfrak{x}_\circ})^{\mathfrak{y}}) \oplus m_0$
	$\xleftarrow{Y, y_1, y_0}$	$K_B := H(X_0, m_1, m_0, Y, y_1, y_0)$
$m_1' := y_1 \oplus h((\mathfrak{g}^{\mathfrak{y}})^{\mathfrak{a}_1})$		
$m_0' := y_0 \oplus h((\mathfrak{g}^{\mathfrak{y}})^{\mathfrak{x}}), \mathfrak{y}' \leftarrow g(m_1', m_0')$		$n_1' := x_1 \oplus h((\mathfrak{g}^{\mathfrak{x}})^{\mathfrak{b}_2}, \mathfrak{x}' \leftarrow G(n_1')$
If $Y \neq \mathfrak{g}^{\mathfrak{y}'}, m_1' \Vert m_0' := s_{A1}$		If $X \neq \mathfrak{g}^{\mathfrak{x}'}, n_1' := s_{B2}$
$K_B' := H(X_0, m_1', m_2', Y, y_1, y_0)$		$K_A' := H(n_1', X, x_1)$
$SK := \hat{H}(sid, K_A, K_B')$		$SK := \hat{H}(sid, K_A', K_B)$

[XXW+18] Xiu Xu, Haiyang Xue, Kunpeng Wang, Bei Liang, Song Tian, Strongly secure AKE from Supersingular Isogeny, **eprint 2018\760**

SIAKE参数及安全级别

参数			经典RO下	量子RO下
		经典复杂度	量子计算复杂度	量子计算复杂度
SIAKEp503	128	2^{125}	2^{83}	2^{41}
SIAKEp751	192	2^{186}	2^{124}	2^{62}
SIAKEp964	256	2^{238}	2^{159}	2^{79}

针对SIDH中间相遇：经典$O(\sqrt[4]{p})$；量子$O(\sqrt[6]{p})$

[JAC+18] Jao, D., Azarderakhsh, R., Campagna, M., et al: Supersingular Isogeny Key Encapsulation. NIST Round 2.

[DG16] Delfs, Galbraith. Computing isogenies between supersingular elliptic curves over Fp. **Designs, Codes and Cryptography** 2016

[Tan09] Tani, S.: Claw finding algorithms using quantum walk. **Theoretical Computer Science** 2009

SIAKE通信性能

参数	A to B (Bytes)	B to A (Bytes)
SIAKEp503	780	434
SIAKEp751	1160	628
SIAKEp964	1492	798

SIAKE计算性能

参数	SIAKE.A.int (10^3cycles)	SIAKE.B.shared (10^3cycles)	SIAKE.A.shared (10^3cycles)
SIAKEp503	47308	84760	45898
SIAKEp751	151364	272975	147098
SIAKEp964	7754959	13261891	7456329

Intel酷睿i7-6500U 2.50GHz处理器，8GB内存，VS2015，优化x64实现

SIAKE优缺点

优点

- 通信量低
- 无解密错误
- 强安全性（ CK+ ）
- 经典和量子RO安全性
- 模块化构造

缺点

- 计算效率低