Strongly Secure Authenticated Key Exchange from Supersingular Isogenies

Xiu Xu, Haiyang Xue, Kunpeng Wang, Man Ho Au, Song Tian

Institute of Information Engineering, Chinese Academy of Sciences
The Hong Kong Polytechnic University

2019/12/9

xuxiu@iie.ac.cn

Outline

1. SIDH Key Exchange
2. The State-of-the-art of SIDH AKE
3. Our SIAKE

Outline

1. SIDH Key Exchange
2. The State-of-the-art of SIDH AKE
3. Our SIAKE

● SIDH: Background

- **OIDH**: Rostovtsev-Stolbunov 2006.
  - ➢ Subexponential time: Childs-Jao-Soukharev 2011.
- **SIDH**: De Feo-Jao 11.
- **SIKE**: submit to NIST (Jao et.al. 2017).
- **CSIDH**: commutative SIDH (Castryck-Lange 2018).

- **Isogeny**: A surjective group morphism.
  - ➢ **Existence and Uniqueness**:
$$\begin{tikzcd} \phi : E_1 \arrow[rr] \arrow[dr] & & E_2 \arrow[dl, dash, "\cong"] \\ & E_1/K & \end{tikzcd}$$
  - ➢ **Degree(separable)**: $\deg\phi = \#\ker\phi$
- **Isogeny Computation**: Vélu formulas.

SIDH: Supersingular Elliptic Curves

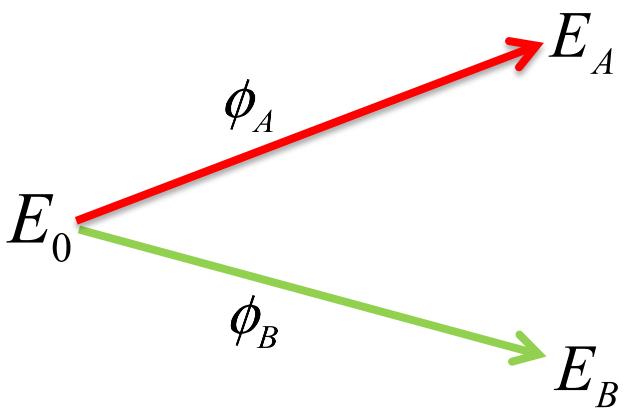
- **Supersingular curve**:

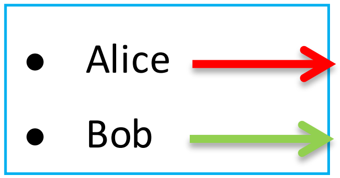
  E/F_q, $char(F_q)=p$, $\#E(F_q)=q+1-t_q$

- The trace t_q is divisible by prime p.
- Its endomorphism ring is isomorphic to the maximal order of the quaternion algebra (non-commutative).
- All supersingular elliptic curves can be defined over F_{p^2}.

SIDH: Introduction

- **Parameters :** $E_0 / F_{p^2},\ p = l_1^{e_1} l_2^{e_2} \cdot f \pm 1,\ E_0[l_1^{e_1}] = \langle P_1, Q_1 \rangle,\ E_0[l_2^{e_2}] = \langle P_2, Q_2 \rangle$





$\ker \phi_A = \langle P_1 + k_a Q_1 \rangle = \langle R_A \rangle$

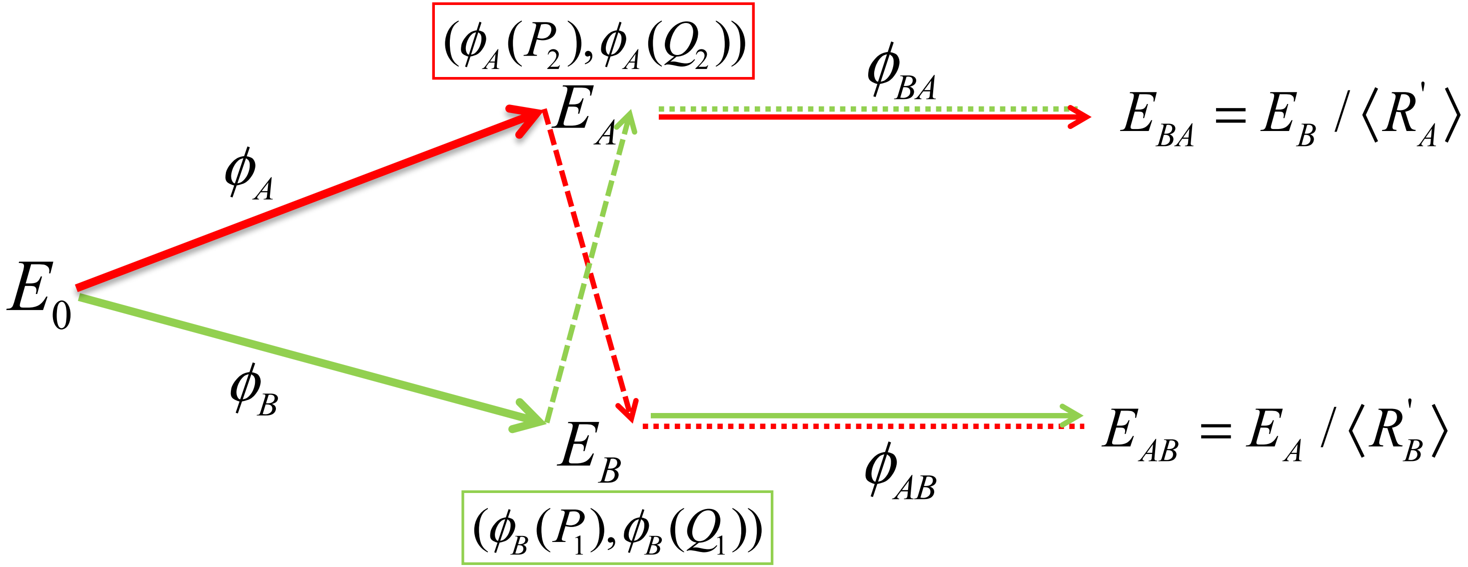
$\ker \phi_B = \langle P_2 + k_b Q_2 \rangle = \langle R_B \rangle$

$E_A = E_0 / \langle R_A \rangle$

$E_B = E_0 / \langle R_B \rangle$

SIDH: Introduction

- **Parameters :** $\boxed{E_0 / F_{p^2},\ p = l_1^{e_1} l_2^{e_2} \cdot f \pm 1,\ E_0[l_1^{e_1}] = \langle P_1, Q_1 \rangle,\ E_0[l_2^{e_2}] = \langle P_2, Q_2 \rangle}$

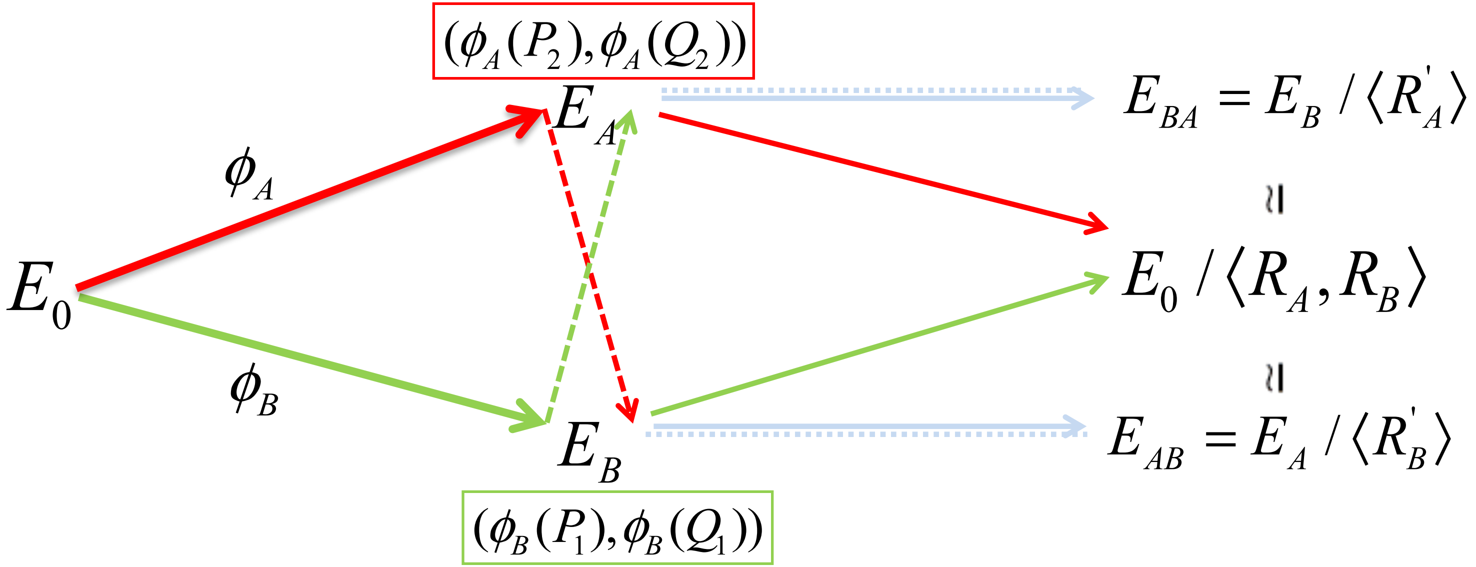


$$\boxed{\ker \phi_{AB} = \langle \phi_A(P_2) + k_b \phi_A(Q_2) \rangle = \langle R_B' \rangle}$$

$$\boxed{\ker \phi_{BA} = \langle \phi_B(P_1) + k_a \phi_B(Q_1) \rangle = \langle R_A' \rangle}$$

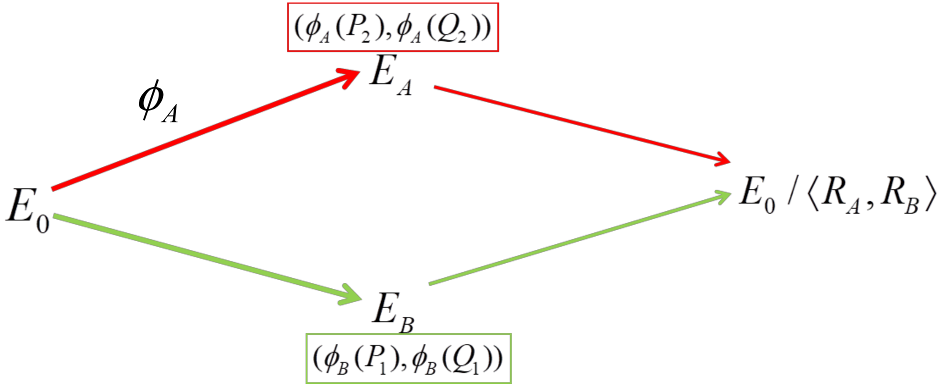
SIDH: Introduction

- **Parameters :** $E_0 / F_{p^2},\ p = l_1^{e_1} l_2^{e_2} \cdot f \pm 1,\ E_0[l_1^{e_1}] = \langle P_1, Q_1 \rangle,\ E_0[l_2^{e_2}] = \langle P_2, Q_2 \rangle$



$$\boxed{E_{AB} = \phi_{AB}(\phi_B(E_0)) \cong E_0 / \langle P_1 + k_a Q_1, P_2 + k_b Q_2 \rangle \cong \phi_{BA}(\phi_A(E_0)) = E_{BA}}$$

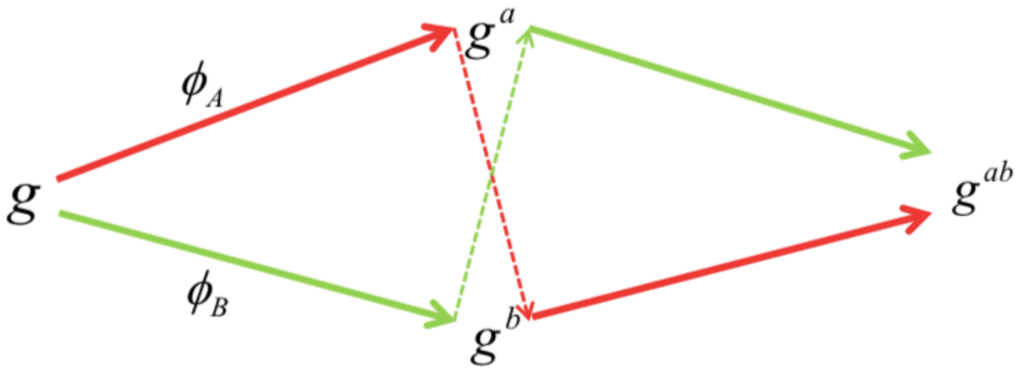
SIDH: Assumptions



- **Prob.1 (CSSI):** Given $\{E_A,\phi_A(P_2),\phi_A(Q_2)\}$, get ϕ_A.
- **Prob.2 (SI-CDH):** Given $\{E_A,\phi_A(P_2),\phi_A(Q_2)\}$ and $\{E_B,\phi_B(P_1),\phi_B(Q_1)\}$, compute E_{AB}.
- **Prob.3 (SI-DDH):** Given two distributions D_0 and D_1, determine b (0 or 1).

*De Feo L, Jao D, Plût J. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies[J]. Journal of Mathematical Cryptology, 2014, 8(3):209-247.

SIDH: Crypto-friendly Description



$$g^a = \{E_A, \phi_A(P_2), \phi_A(Q_2)\}$$
$$g^b = \{E_B, \phi_B(P_1), \phi_B(Q_1)\}$$
$$g^{ab} = j(E_{AB})$$

- **Prob.1 (CSSI):** Given g^a, get a.
- **Prob.2 (SI-CDH):** Given g^a and g^b, compute g^{ab}.
- **Prob.3 (SI-DDH):** Given two distributions D_0 and D_1, determine b (0 or 1).

*Fujioka, A., Takashima, K., Terada, S., Yoneyama, K.: Supersingular isogeny Diffie–Hellman authenticated key exchange. In: Lee, K. (ed.) ICISC 2018. LNCS, vol. 11396, pp. 177–195. Springer, Cham (2019).

Outline

1. SIDH Key Exchange
2. The State-of-the-art of SIDH AKE
3. Our SIAKE

AKE: Security Models

- **BR model**

  indistinguishable type definition

- **CK model**

  stronger security (session key, session state)

- **eCK model**

  session key, ephemeral randomness, wPFS+KCI+MEX

- **CK^{+} model** (Fujioka-Suzuki-Xagawa-Yoneyama 12)

  Send, SessionKeyReveal,SessionStateReveal, Corrupt

  reform the security of HMQV: CK+wPFS+KCI+MEX

AKE: CK⁺ Model

Event	sid^*	$\overline{sid^*}$	sk_A	ek_A	ek_B	sk_B	Security
E_1	A	No	√	×	-	×	KCI
E_2	A	No	×	√	-	×	MEX
E_3	B	No	×	-	√	×	MEX
E_4	B	No	×	-	×	√	KCI
E_5	A or B	Yes	√	×	×	√	wPFS
E_6	A or B	Yes	×	√	√	×	MEX
E_{7-1}	A	Yes	√	×	√	×	KCI
E_{7-2}	B	Yes	×	√	×	√	KCI
E_{8-1}	A	Yes	×	√	×	√	KCI
E_{8-2}	B	Yes	√	×	√	×	KCI

- √ means the secret key may be leaked to adversary.
- × means not.
- \- means the key does not exist.
- $\overline{sid^*}$ is the matching session of sid^*.

Existing Constructions

- **Explicit:** using additional primitives (Sign or MAC)

  SIGMA-SIDH, SIGMA-I-SIDH (Longa 18).

- **Implicit:**

  General construction: BCNP, AKE-SIDH-SIKE (FSXY), GSW, etc.

  Non-general: TS2, NAXOS (defined as Gal 1 and Gal 2 in our paper);

  MQV-style (defined as FTTY 1 and FTTY 2).

*Longa, P.: A note on Post-Quantum Authenticated Key Exchange from Supersingular Isogenies. IACR Cryptology ePrint Archive 2018/267.

**Galbraith, S. D.: Authenticated key exchange for SIDH. IACR Cryptology ePrint Archive 2018/266.

Existing Constructions

- **AKE-SIDH-SIKE (FSXY):**

  OW-CCA KEM + OW-CPA KEM

- **FTTY 2 (or 1):**

  4 (or 2) Diffie-Hellman values, MQV-style.

AKE-SIDH-SIKE*

A	B
Isogen_2(1)	
Encap (2)	isogen_3(1)
	isoex_3(1)
	Encap(2)
	Decap(2)
Decap(2)	
Isoex_2(1)	

6+6 isogenies

Existing Constructions

Scheme	Key Reg.	Model	wPFS	KCI	MEX	Iso	Mess Size
Gal 1	Honest	CK	√	–	–	6	108 λ
Gal 2	Honest	BR	√	√	–	8	108 λ
FTTY 1	Honest	CK	√	–	–	6	72 λ
FTTY 2	Honest	CK^+	√	√	√	10	72 λ
GSW	Arbi.	CK	√	–	–	12	186 λ
BCNP	Arbi.	CK	√	√	–	12	148 λ
FSXY	Arbi.	CK^+	√	√	√	12	148 λ

*"Honest" indicates it can not resist adaptive attack.

- Limited securities
- Low efficiency
- Adaptive attack

Motivation

AKE

the widest adversarial goals — security

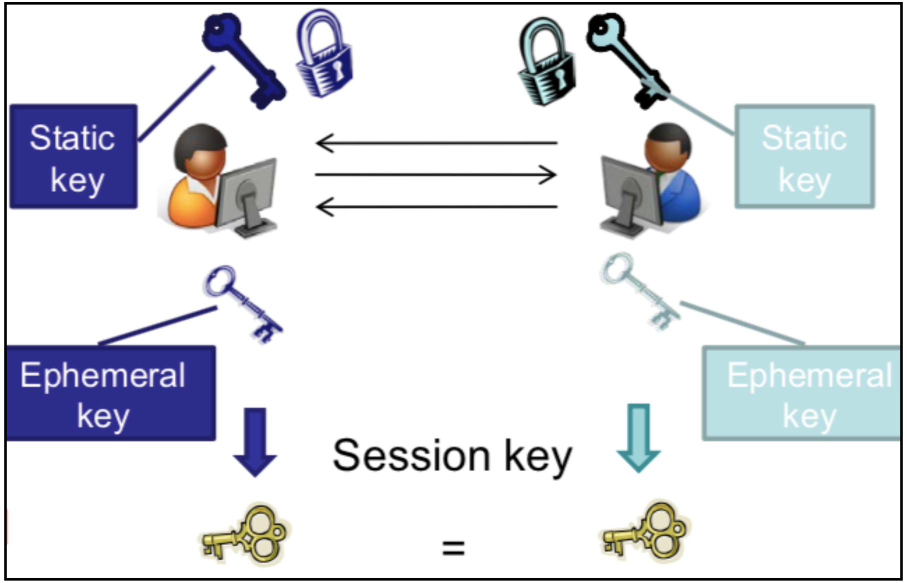
more efficient — efficiency

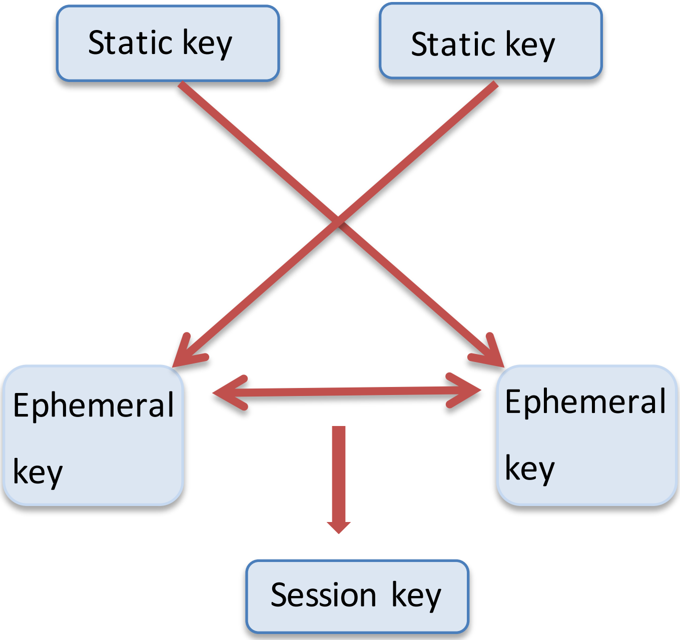
short message size — Bandwidth

Outline

1. **SIDH Key Exchange**
2. **The State-of-the-art of SIDH AKE**
3. **Our SIAKE**

SIAKE: Structure





SIAKE: Building Block 2-key KEM

2-key KEM was proposed by Xue et.al. in Asiacrypt2018.

- Two pairs of public and secret keys: (pk_1, pk_0), (sk_1, sk_0).

- **[CCA,·] security of 2-key KEM**:

(1) The adversary has the capability of choosing one of the challenge public key pk_0^*;

(2) could query a strong decryption oracle, which decapsulates the ciphertext under several public keys (pk_1^*, pk_0') where pk_0' is generated by the challenger.

- **Modified FO transformation** to achieve [CCA,·] security: Hashing with public keys as input.

SIAKE: Basic Tool 2-key PKE

- KeyGen_1, KeyGen_0;
- C=Encrypt (pk_1,pk_0,m,r);

$$m_1 \| m_0 \leftarrow m,$$
$$C = (g^b, h(g^{a_1 b}) \oplus m_1, h(g^{a_0 b}) \oplus m_0)$$
$$=(X, x_1, x_0)$$

- m=Decrypt (sk_1,sk_0,C).

[CPA, CPA] 2-key PKE $\xrightarrow[\text{FO trans}]{\text{Modified}}$ [CCA, ·] 2-key KEM

*Xue, H., Lu, X., Li, B., Liang, B., He, J.: Understanding and Constructing AKE via Double-Key Key Encapsulation Mechanism. In ASIACRYPT 2018. LNCS, vol 11273, pp. 158-189.

SIAKE

Alice

Bob

pkA_1

pkB_1

$pkA_0=(X,x_1,x_0)$

$(pkA_0,KA)=Encap(pkB_1,--)$ $\longrightarrow$

$(pkB_0,KB)=Encap(pkA_1,X)$

$pkB_0=(Y,y_1,y_0)$

$Decap(skA_1,skA_0,\ pkB_0)=KB$ $\longleftarrow$ $Decap(skB_1,--,\ pkA_0)=KA$

$\boxed{K=H(sid,KA,KB)}$

- X (or Y) has two functionalities.

(1) X is part of the public key (pkA_1,X) under which the ciphertext (Y,y_1,y_0) is computed.

(2) X is part of the ciphertext pkA_0 in which KA is encapsulated.

SIAKE

- X (or Y) has two functionalities.

(1) X is part of the public key (pkA_1, X), under which the ciphertext (Y, y_1, y_0) is computed.
(2) X is part of the ciphertext pkA_0 in which KA is encapsulated.

- Problems:

(1) If the security depends on pkA_0, the randomness of X should be secret.

(2) In the test session, the simulator could perform decapsulation with public key X.

SIAKE: Solution 1

Alice		Bob
pkA_1		pkB_1
X_0		
$(pkA_0,KA)=Encap(pkB_1,--)$	$\boxed{pkA_0=(X,x_1),X_0}$ $\longrightarrow$	$(pkB_0,KB)=Encap(pkA_1,X_0)$
$Decap(skA_1,skA_0,\ pkB_0)=KB$	$pkB_0=(Y,y_1,y_0)$ $\longleftarrow$	$Decap(skB_1,--,\ pkA_0)=KA$

$$\boxed{K=H(sid,KA,KB)}$$

SIAKE: Solution 1

- **SIAKE_2** is CK$^+$ secure under SI-DDH.

Assumption	2-Key PKE	2-Key KEM	Events
SI-DDH	[.,OW-CPA], $pk_0 = g^{x_0}$	[.,OW-CPA], $pk_0 = g^{x_0}$	E_5
SI-DDH	[OW-CPA,.], $pk_1 = g^{a_1}$	[OW-CCA,.], $pk_1 = g^{a_1}$	$E_3, E_4, E_6, E_{7-2}, E_{8-1}$
SI-DDH	OW-CPA	OW-CCA, $pk_1 = g^{b_2}$	$E_1, E_2, E_{7-1}, E_{8-2}$

The outline of security reduction.

SIAKE: Solution 2

Alice

Bob

pkA_1

pkB_1

$(pkA_0,--)=Encap(pkB_1,--)$

$pkA_0=(X,x_1)$

$pkB_0=(Y,y_1,y_0)$

$(pkB_0,KA)=Encap(pkA_1,X)$

$Decap(skA_1,skA_0,pkB_0)=KA$

$(x_0,KB)=Encap(--,pkB_0)$

x_0

$Decap(skB_1,skB_0, pkA_0,x_0)=KB$

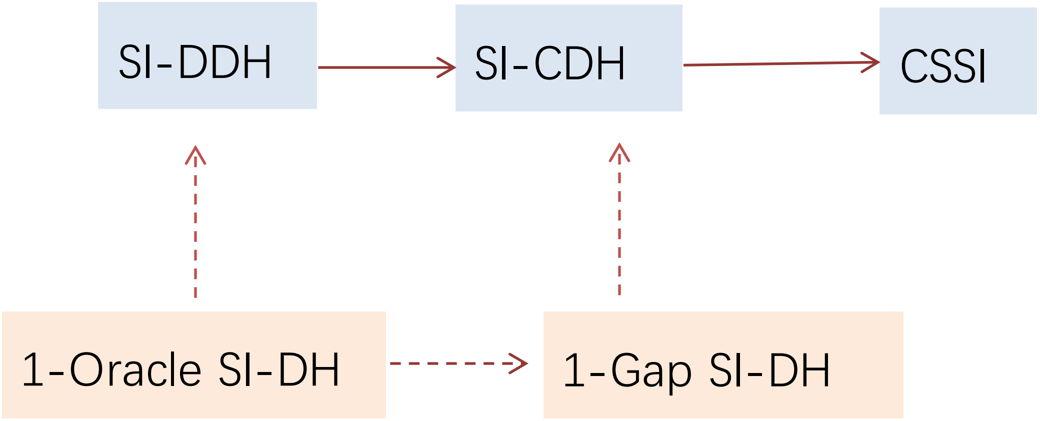
$K=H(sid,KA,KB)$

- **SIAKE$_3$** is CK^+ secure under 1-Oracle SI-DH.

Proposed Assumptions

- **Prob.4 (1- Oracle SI-DH):** On the basis of SI-DDH with a one-time oracle H_B .
  (input $y \neq g^a$, output $H(y, y^b)$).

- **Prob.5 (1- Gap SI-DH):** Given g^a and g^b, and a oracle $O_{siddh}(y,\cdot)$, compute g^{ab}.
  ($O_{siddh}(y,\cdot)$ will return 1 if $j = y^b$).



• Comparison

Scheme	Key Reg.	Assum	Model	wPFS	KCI	MEX	Iso	Mess Size
FSXY	Arbi.	SI-DDH	CK^+	√	√	√	12	148λ
$SIAKE_2$	Arbi.	SI-DDH	CK^+	√	√	√	11	114λ
$SIAKE_3$	Arbi.	1-OSIDH	CK^+	√	√	√	10	80λ

* λ is the security parameter.

Conclusion

1. Propose two AKEs $SIAKE_2$ and $SIAKE_3$.
2. Both CK^+ secure in RO model.
3. 12%-20% speedup and 23%-49.3% lower bandwidth.

Thank you !