SIAKE

–基于超奇异同源的认证密钥交换协议

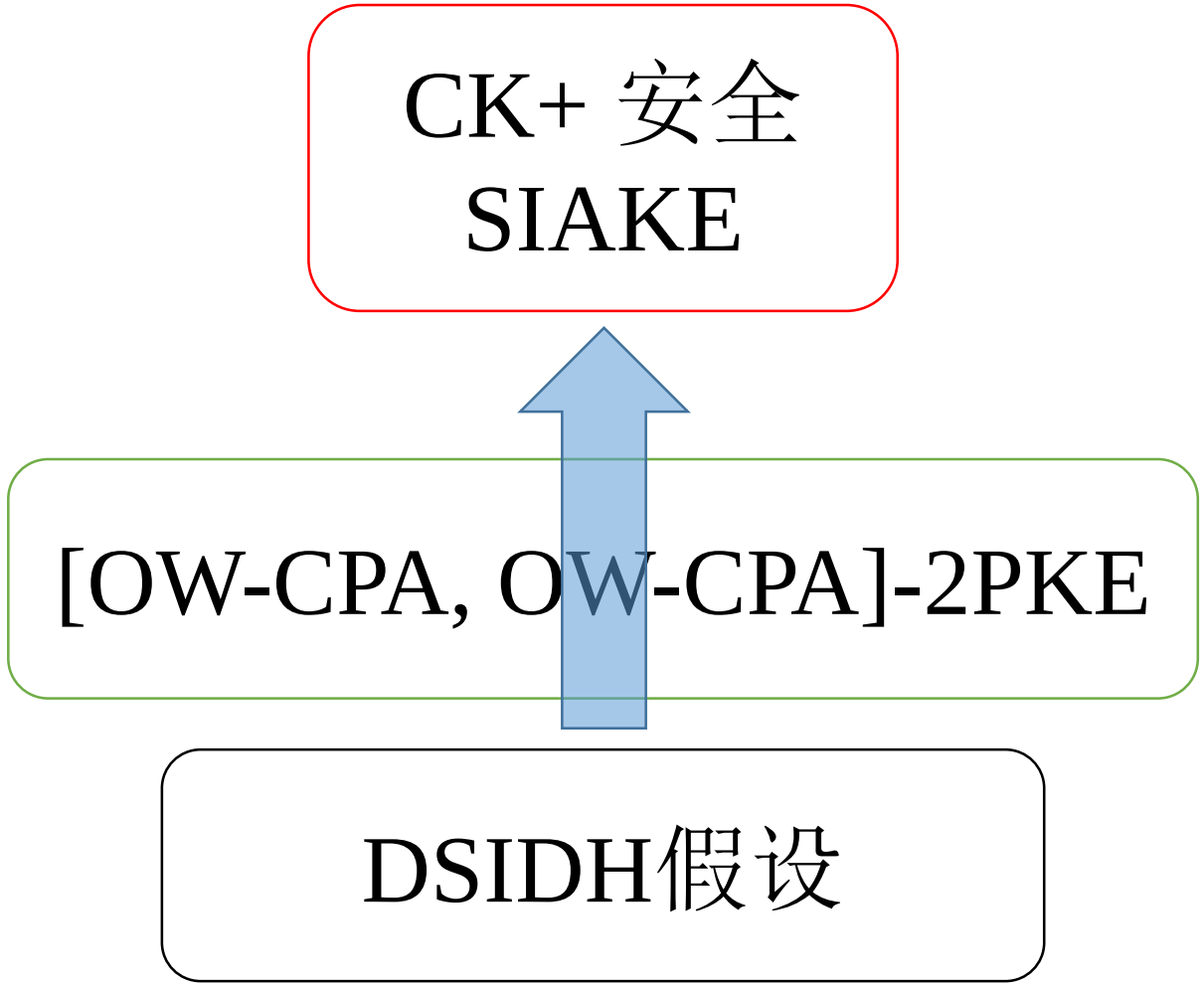
薛海洋、路献辉、王鲲鹏、田松、徐秀、贺婧楠、李宝

信息安全重点实验室

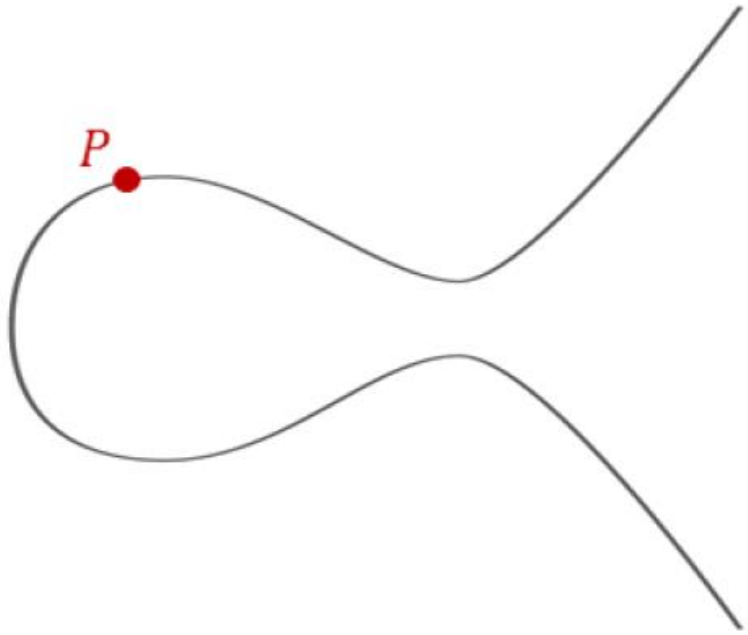
DCS中心

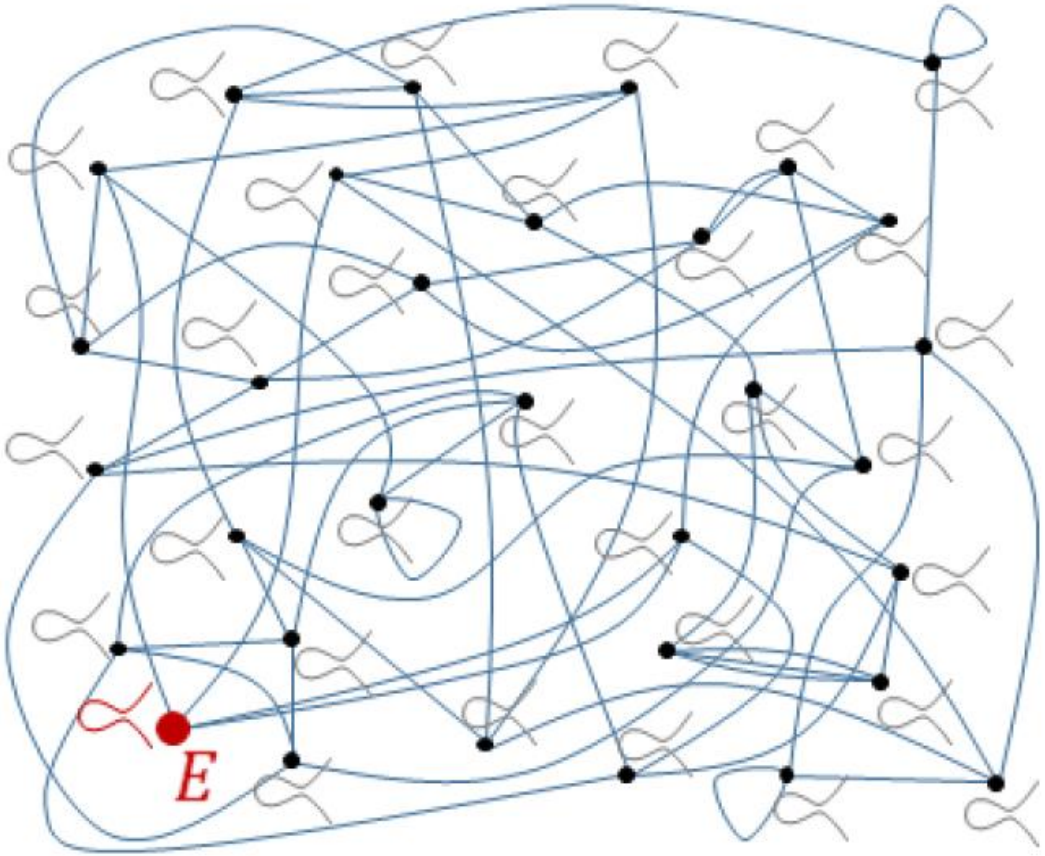
SIAKE概述

- 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



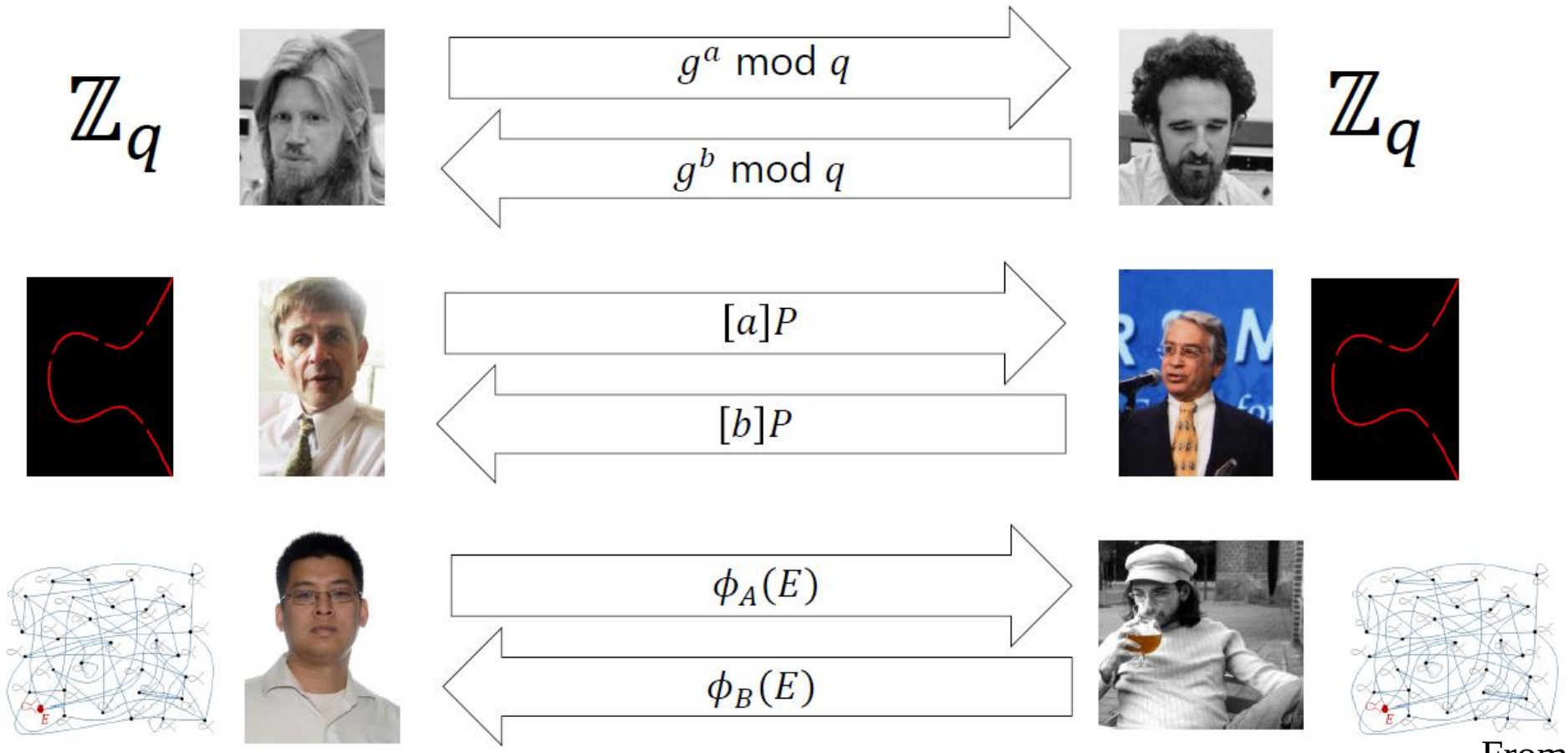
椭圆曲线→超奇异同源





From Croatia’s slides

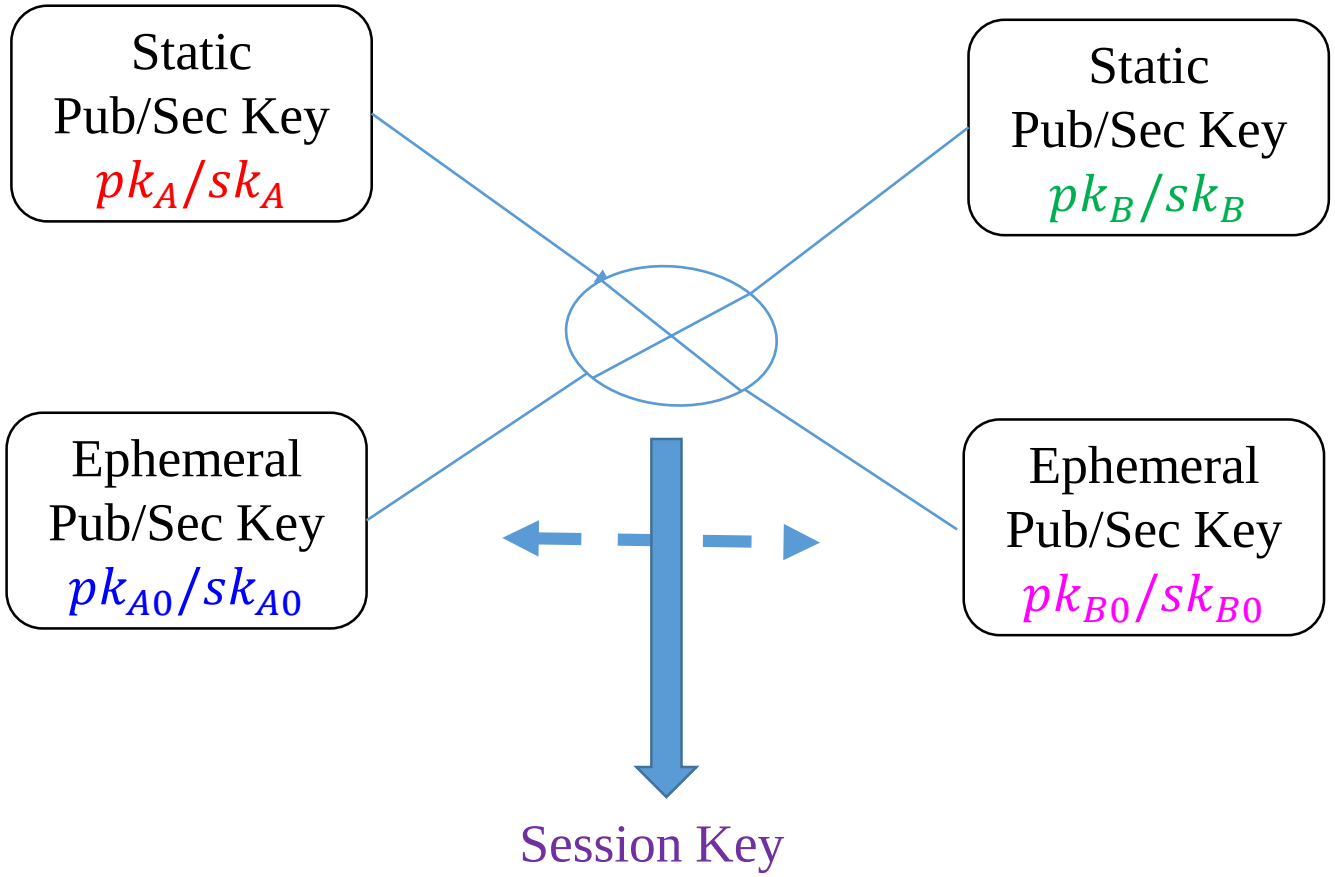
Diffie-Hellman Key Exchange



From Croatia's slides

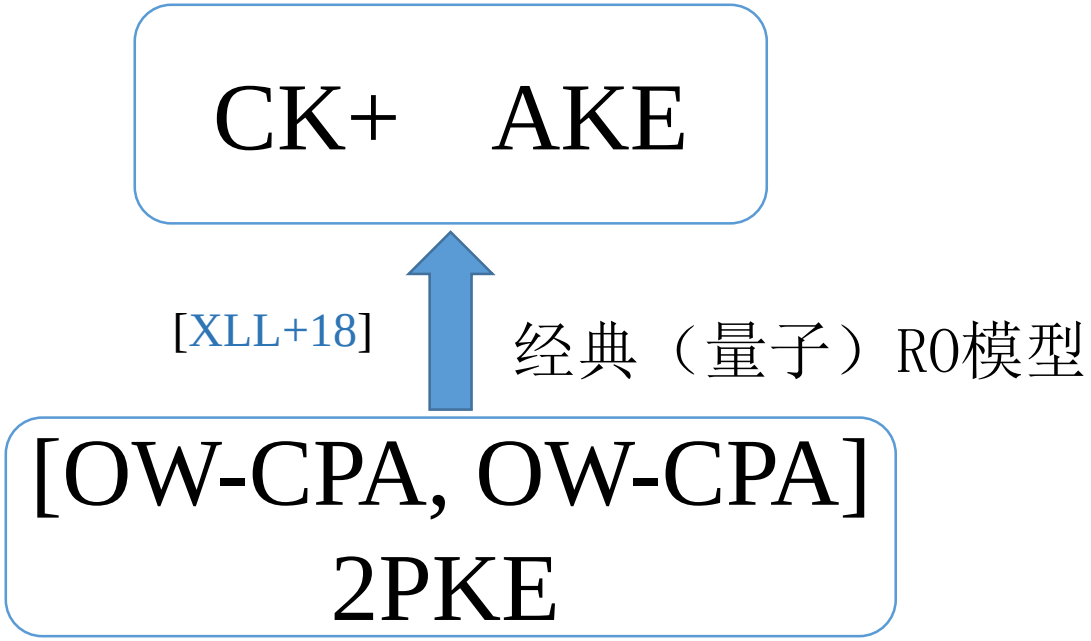
[JAC+18] Jao, D., Azarderakhsh, R., Campagna, M., et al: Supersingular Isogeny Key Encapsulation. NIST Round 2.

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

SIAKE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**

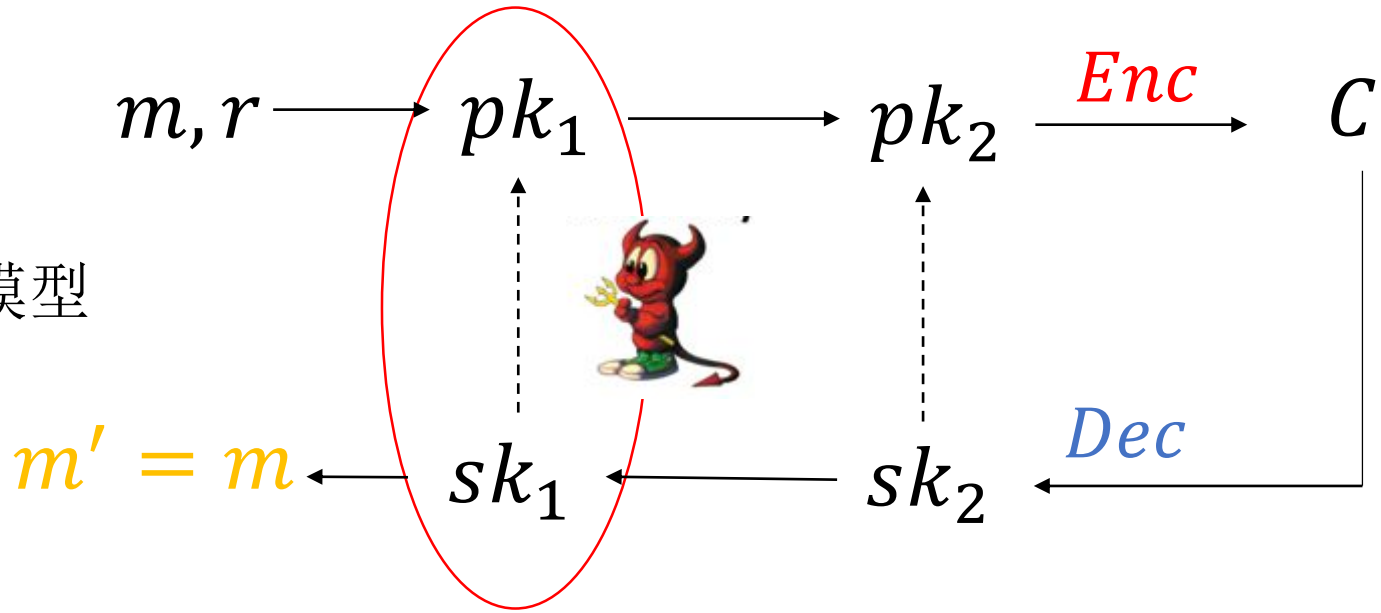
SIAKE设计原理

CK+ AKE

[XLL+18]

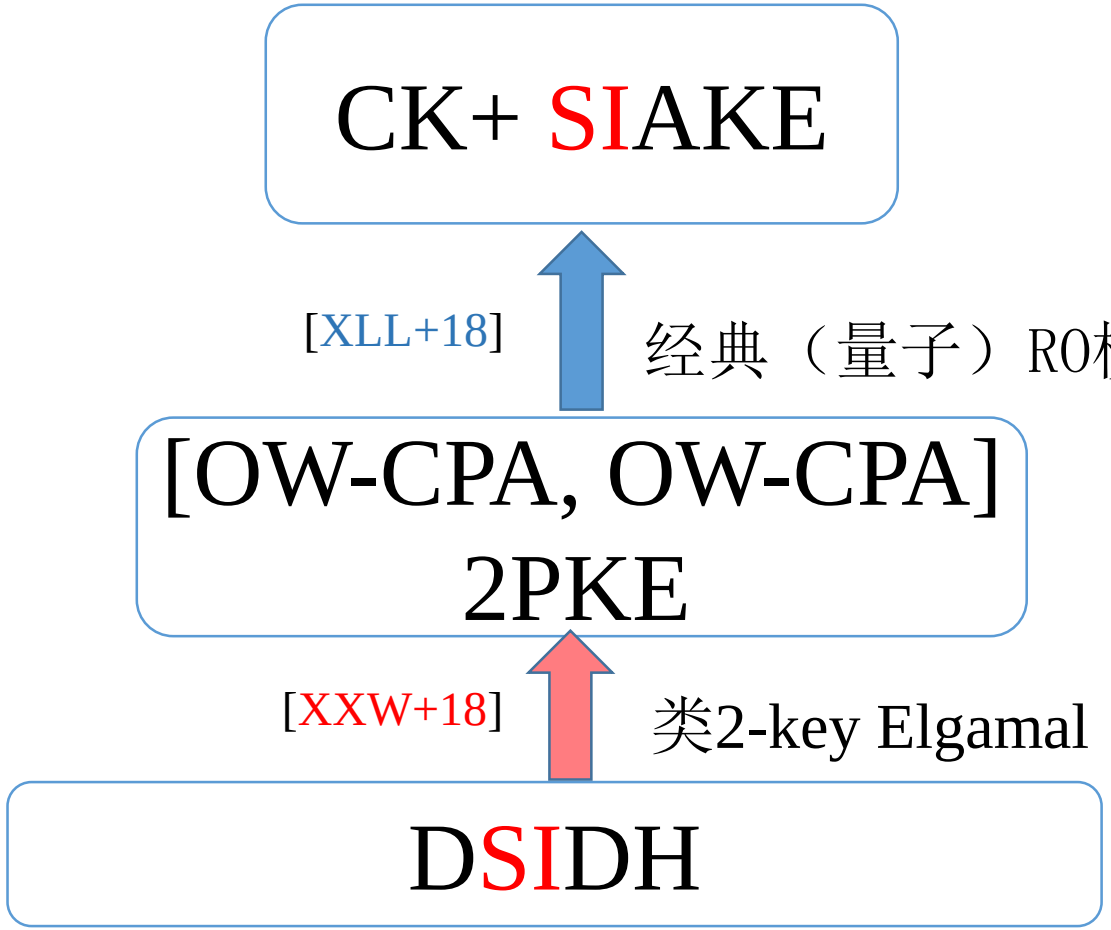
经典（量子）RO模型

[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**

SIAKE设计原理



$$g^r, H(h_1^r) \oplus m_1, H(h_0^r) \oplus m_0$$

[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**

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}

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

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