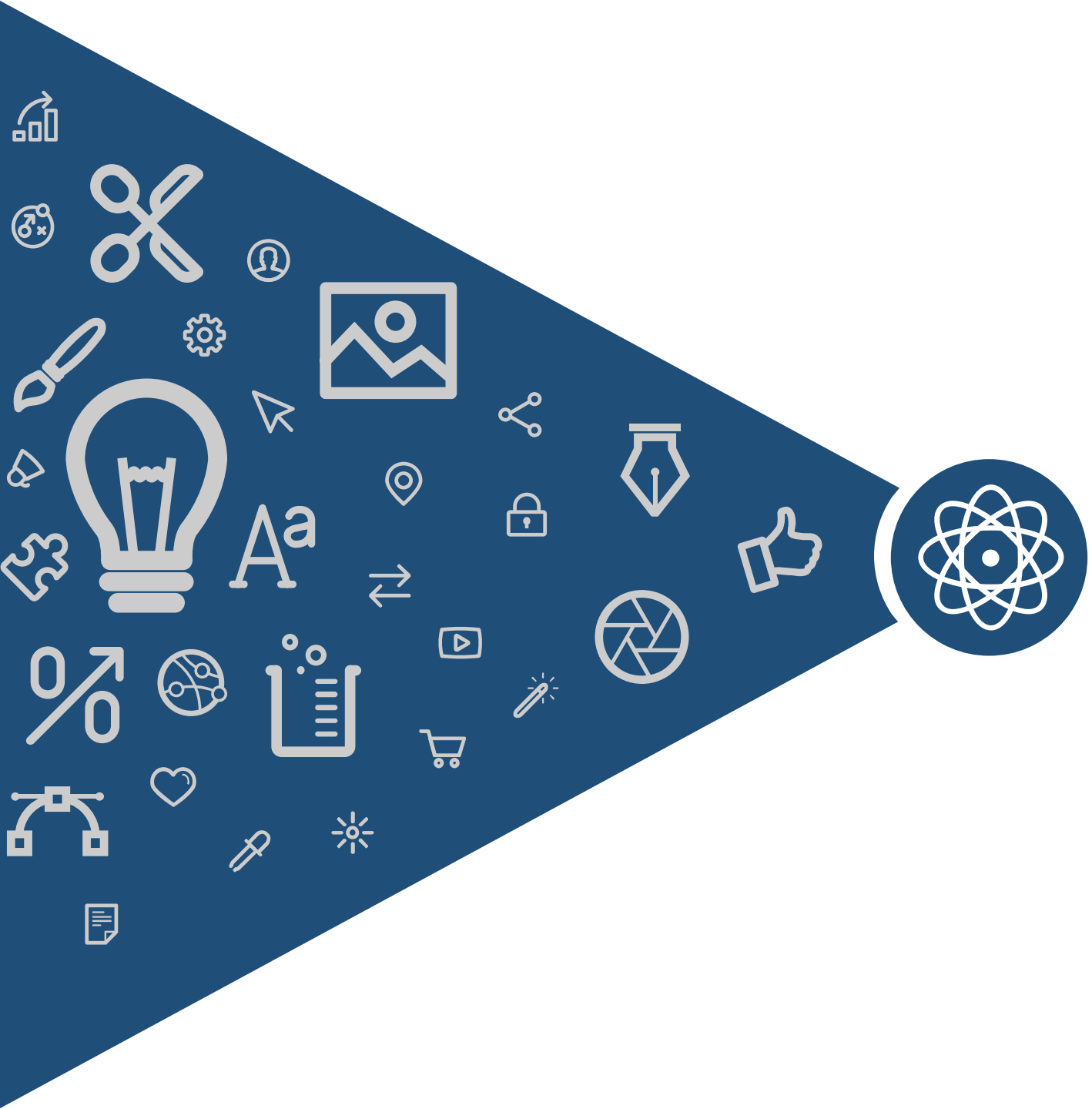
Revisiting Anonymity in Post-Quantum Public Key Encryption

Yao Cheng, Xianhui Lu, Ziyi Li, Bao Li
Institute of Information Engineering, CAS
chengyao@iie.ac.cn

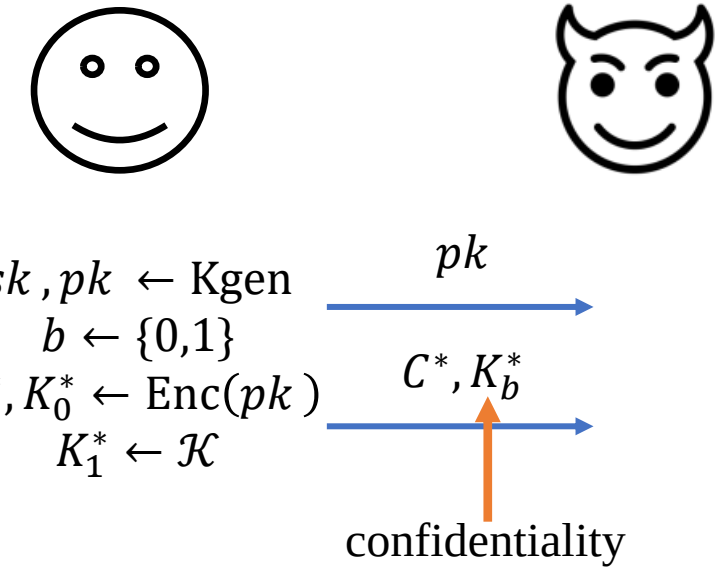
06/12/2024 PQCrypto 2024



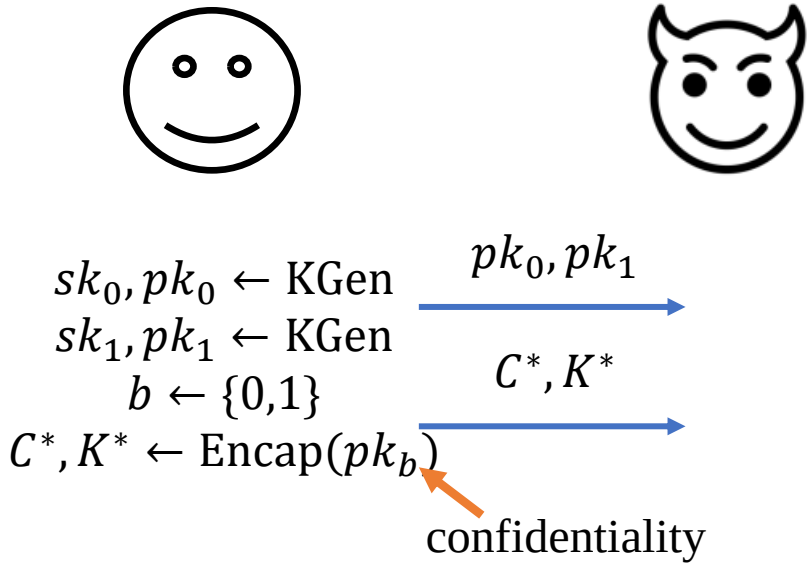
Backgrounds

Anonymity of KEM

Indistinguishability (IND):



Anonymity (ANO):



Applications:

Zcash、anonymous credential systems

auction protocols、anonymous AKE

UPDATES

PQC Standardization Process: Announcing Four Candidates to be Standardized, Plus Fourth Round Candidates

NIST is announcing four Post-Quantum Cryptography candidates for standardization, plus candidates for a fourth round of analysis.

July 5, 2022

Public-Key Encryption/ key encapsulation mechanism	Digital Signatures
CRYSTALS-KYBER(Standardization) BIKE、Classic McEliece、HQC、SIKE （candidates）	CRYSTALS-Dilithium FALCON SPHINCS^{+}

FO Transformations ANO-CPA⇝ ANO−CCA

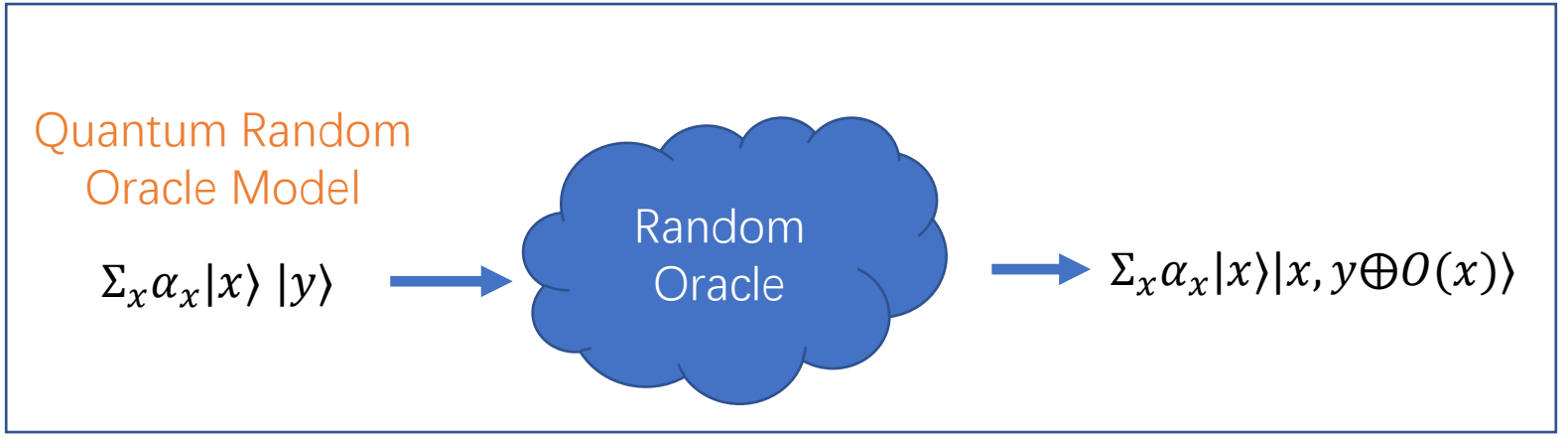
Previous Works(ANO-CCA KEM)

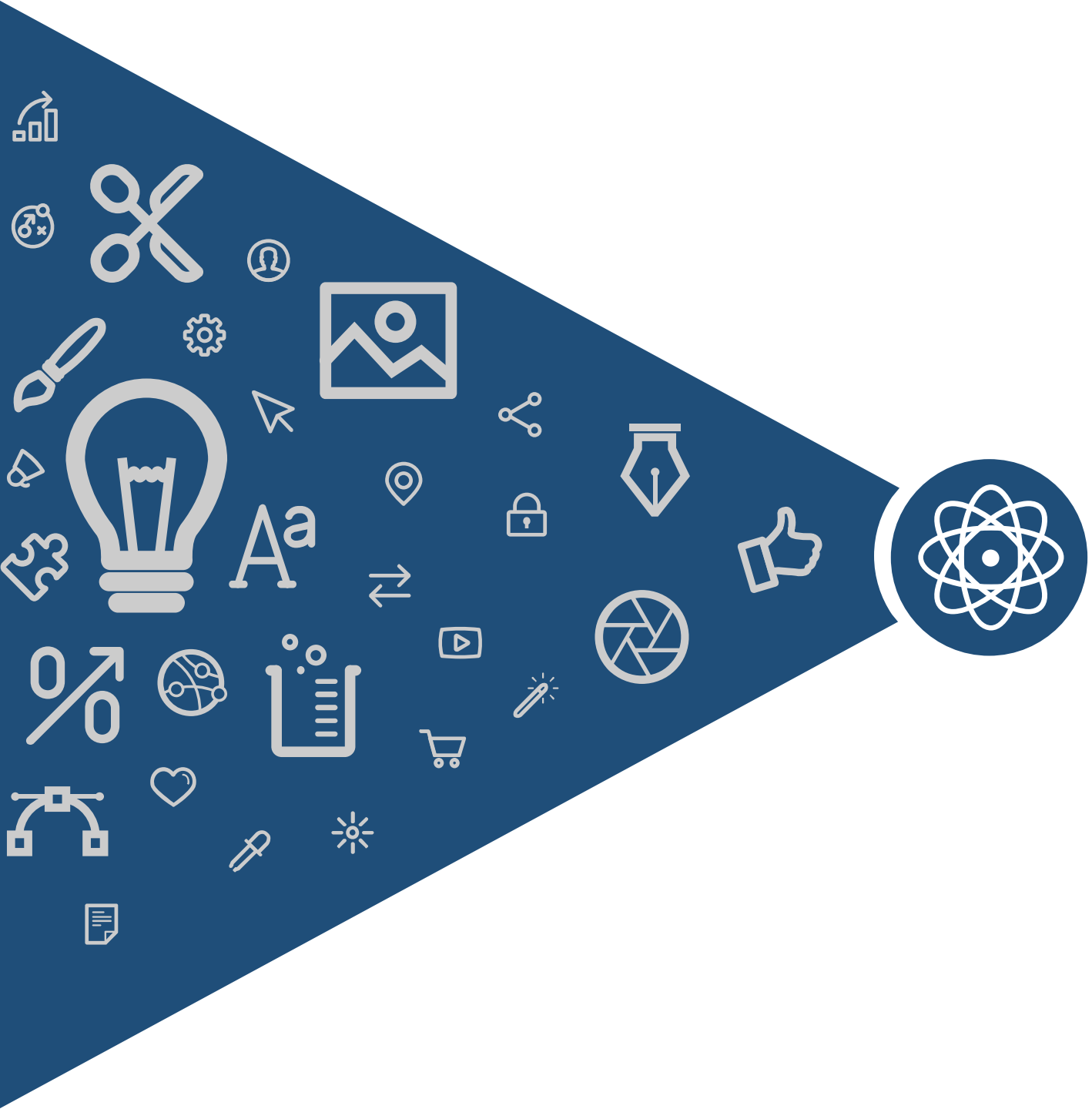
FO	Works	Underlying Security			Additional Hash
		wANO-CPA	OW-CPA	Additional Property	
Implicit	[GMP22]	✓	✓	SCFR-CPA	×
	[Xagawa22]	✓	✓	SDS-IND	×
Explicit	[Xagawa22]	✓	✓	SDS-IND	✓

Problems:

Hard to simulate: two dec oracles

Additional hash in the explicit case



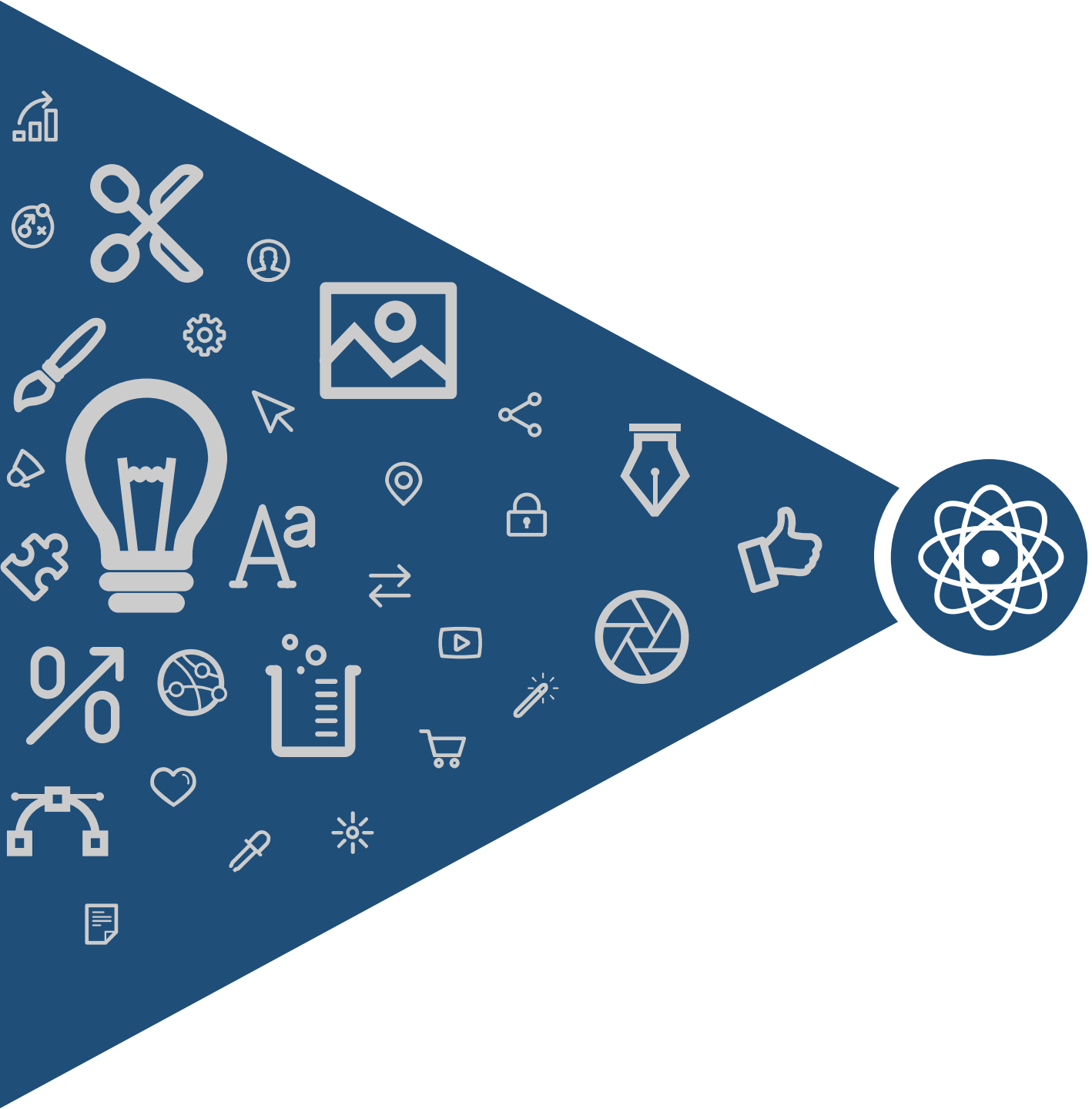


Our Results

Results

FO	Underlying Security			Additional Hash
	wANO-CPA	OW-CPA	Additional Property	
Implicit	✓	✓	$\gamma - spreadness$	×
Explicit	✓	✓	$\gamma - spreadness$	×

KEM-DEM	Underlying Security			
	KEM			DEM
Implicit	wANO-CCA	IND-CCA	η-randomness	INT−CTXT
Explicit	wANO-CCA	IND-CCA		INT−CTXT
[Mohassel10]	ANON-CCA		WROB-CCA	INT−CTXT



Technical Overview

Modular Analysis: T-trans & U-trans

$FO^{\not\perp} = U^{\not\perp} \circ T, FO^{\perp} = U^{\perp} \circ T$

[HHK17]

- $U^{\not\perp}: OW\text{-}qPCA \rightarrow IND\text{-}CCA$
- $U^{\perp}: OW\text{-}qPCVA \rightarrow IND\text{-}CCA$
- $T: OW\text{-}CPA \rightarrow OW\text{-}qPCA$

Our Works

- $U^{\not\perp}: wANO\text{-}CCOA \rightarrow ANO\text{-}CCA$
- $U^{\perp}: wANO\text{-}CCOVA \rightarrow ANO\text{-}CCA$
- $T: wANO\text{-}CPA \rightarrow wANO\text{-}CCA$

$\mathsf{Gen}^{\not\perp}$:	$\mathsf{Encaps}^{\not\perp}(pk)$:	$\mathsf{Decaps}^{\not\perp}(sk, c)$:
1 : $(pk, sk') \xleftarrow{\$} \mathsf{Gen}_1$	1 : $m \xleftarrow{\$} \mathcal{M}, c \leftarrow \mathsf{Enc}_1(pk, m)$	1 : Parse $sk = (sk', s)$
2 : $s \xleftarrow{\$} \mathcal{M}, sk := (sk', s)$	2 : $K := H(m, c)$	2 : $m' := \mathsf{Dec}_1(sk', c)$
3 : **return** (pk, sk)	3 : **return** (c, K)	3 : **if** $m' \neq \perp$
		4 : **return** $K := H(m, c)$
		5 : **else return** $K := H(s, c)$

The transformation $U^{\not\perp}$

$\mathsf{Gen}^{\perp}$:	$\mathsf{Encaps}^{\perp}(pk)$:	$\mathsf{Decaps}^{\perp}(sk, c)$:
1 : $(pk, sk) \xleftarrow{\$} \mathsf{Gen}_1$	1 : $m \xleftarrow{\$} \mathcal{M}, c \leftarrow \mathsf{Enc}_1(pk, m)$	1 : $m' := \mathsf{Dec}_1(sk, c)$
2 : **return** (pk, sk)	2 : $K := H(m, c)$	2 : **if** $m' \neq \perp$
	3 : **return** (c, K)	3 : **return** $K := H(m, c)$
		4 : **else return** $\perp$

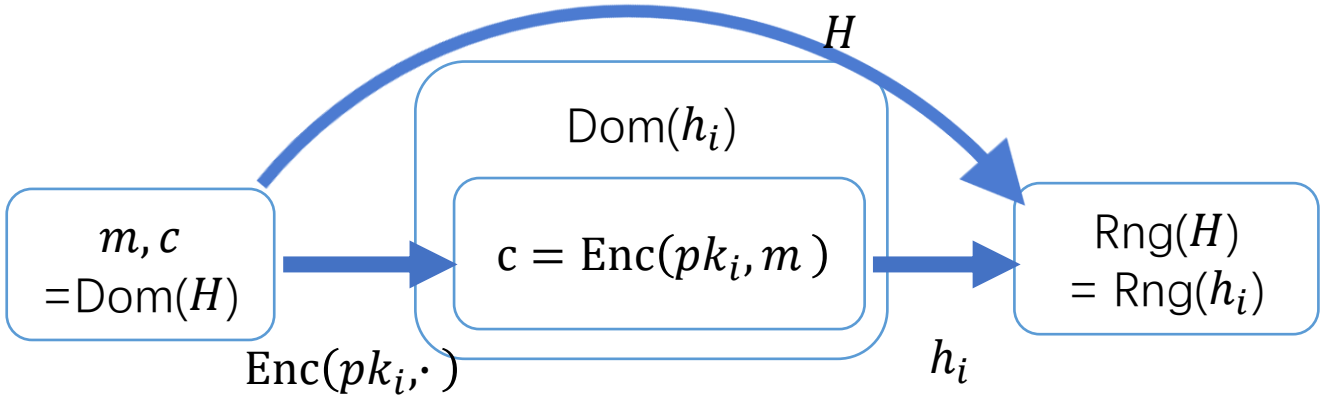
The transformation $U^{\perp}$

Gen_1:	$\mathsf{Enc}_1(pk, m)$:	$\mathsf{Dec}_1(sk, c)$:
1 : $(pk, sk) \xleftarrow{\$} \mathsf{Gen}_0$	1 : $r := G(m)$	1 : $m' := \mathsf{Dec}_0(sk, c)$
2 : **return** (pk, sk)	2 : $c \leftarrow \mathsf{Enc}_0(pk, m, r)$	2 : **if** $\mathsf{Enc}_0(pk, m', G(m')) = c$
	3 : **return** c	3 : **return** m'
		4 : **else return** $\perp$

The transformation T

$U : wANO\text{-}CCOA/wANO\text{-}CCOVA \rightarrow ANO\text{-}CCA$

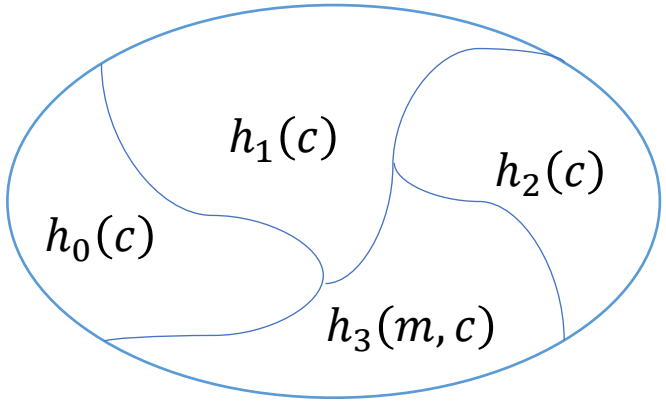
$\mathrm{Dec}(c \neq c^*)$	$\mathrm{CVO}(c \neq c^*)$	$\mathrm{CCO}(c \neq c^*)$
1 : **return** $\mathrm{Dec}(sk, c)$	1 : $m := \mathrm{Dec}(sk, c)$ 2 : **return** $[\![m \in \mathcal{M}]\!]$	1 : **return** $[\![\mathrm{Dec}(sk_0, c) = \mathrm{Dec}(sk_1, c) \neq \perp]\!]$



$U : wANO\text{-}CCOA/wANO\text{-}CCOVA \rightarrow ANO\text{-}CCA$

- The problem of responding $Decaps(sk_i, c)$ with $h_i(c)$

$$\mathrm{CCO}(pk_0, pk_1, c) = 1? \quad [\mathrm{Dec}(sk_0, c) = \mathrm{Dec}(sk_1, c) \neq \perp]$$

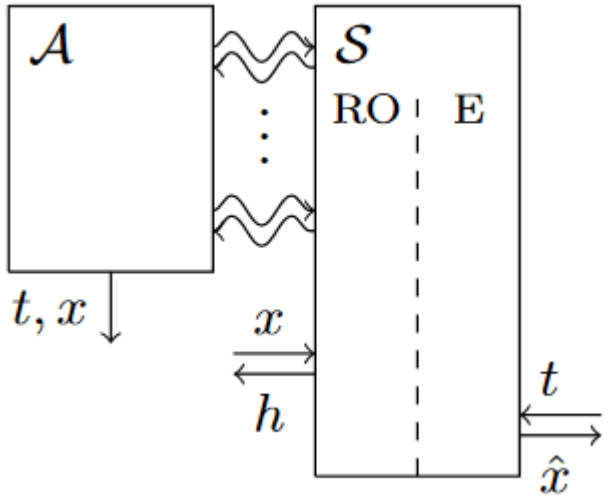


$H\ (m, c)$

$$\begin{cases} \mathrm{Enc}(pk_0, m) = c, \mathrm{Enc}(pk_1, m) \neq c: \ h_0(c) \\ \mathrm{Enc}(pk_0, m) \neq c, \mathrm{Enc}(pk_1, m) = c: \ h_1(c) \\ \mathrm{Enc}(pk_0, m) = c, \mathrm{Enc}(pk_1, m) = c: \ h_2(c) \\ \mathrm{Enc}(pk_0, m) \neq c, \mathrm{Enc}(pk_1, m) \neq c: h_3(m, c) \end{cases}$$

$T : wANO\text{-}CPA \rightarrow wANO\text{-}CCA$

$\mathrm{Dec}(c \neq c^*)$	$\mathrm{CVO}(c \neq c^*)$	$\mathrm{CCO}(c \neq c^*)$
1 : **return** $\mathrm{Dec}(sk, c)$	1 : $m := \mathrm{Dec}(sk, c)$	1 : **return** $[\![\mathrm{Dec}(sk_0, c) = \mathrm{Dec}(sk_1, c) \neq \perp]\!]$
	2 : **return** $[\![m \in \mathcal{M}]\!]$	



$$\mathrm{Enc}(pk_0, m; G(m)) = c \qquad \mathrm{Enc}(pk_1, m; G(m)) = c$$

Definition 2 (γ**-spread** [17]). *We say* $\mathsf{PKE} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *is* γ*-spread if*

$$\max_{m \in \mathcal{M}, c \in \mathcal{C}, pk} \Pr[c = \mathsf{Enc}(pk, m)] \leq 2^{-\gamma},$$

where the probability is over the randomness of the encryption. For a (pk, sk) *pair sampled by* Gen*, we also define parameter*

$$\gamma(pk, sk) := \max_{m \in \mathcal{M}, c \in \mathcal{C}} \Pr[c = \mathsf{Enc}(pk, m)].$$

[Zhandry20]: compressed oracle technique
[DFM+22]: online extraction technique

Q&A

chengyao@iie.ac.cn

06/12/2024 PQCrypto 2024