h_da
HOCHSCHULE DARMSTADT
UNIVERSITY OF APPLIED SCIENCES

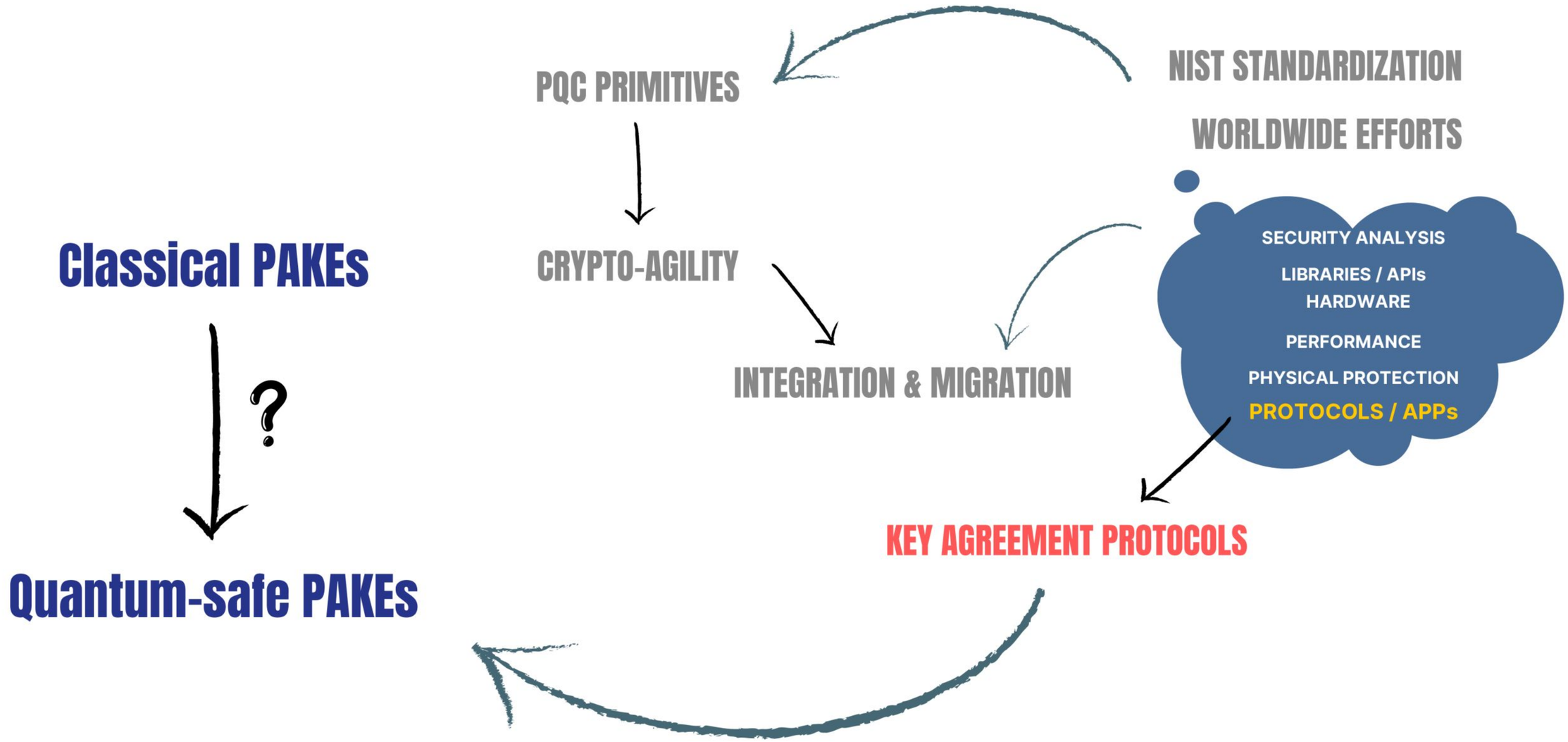
acsd applied cyber security darmstadt

PQC PAKES
AN OVERVIEW

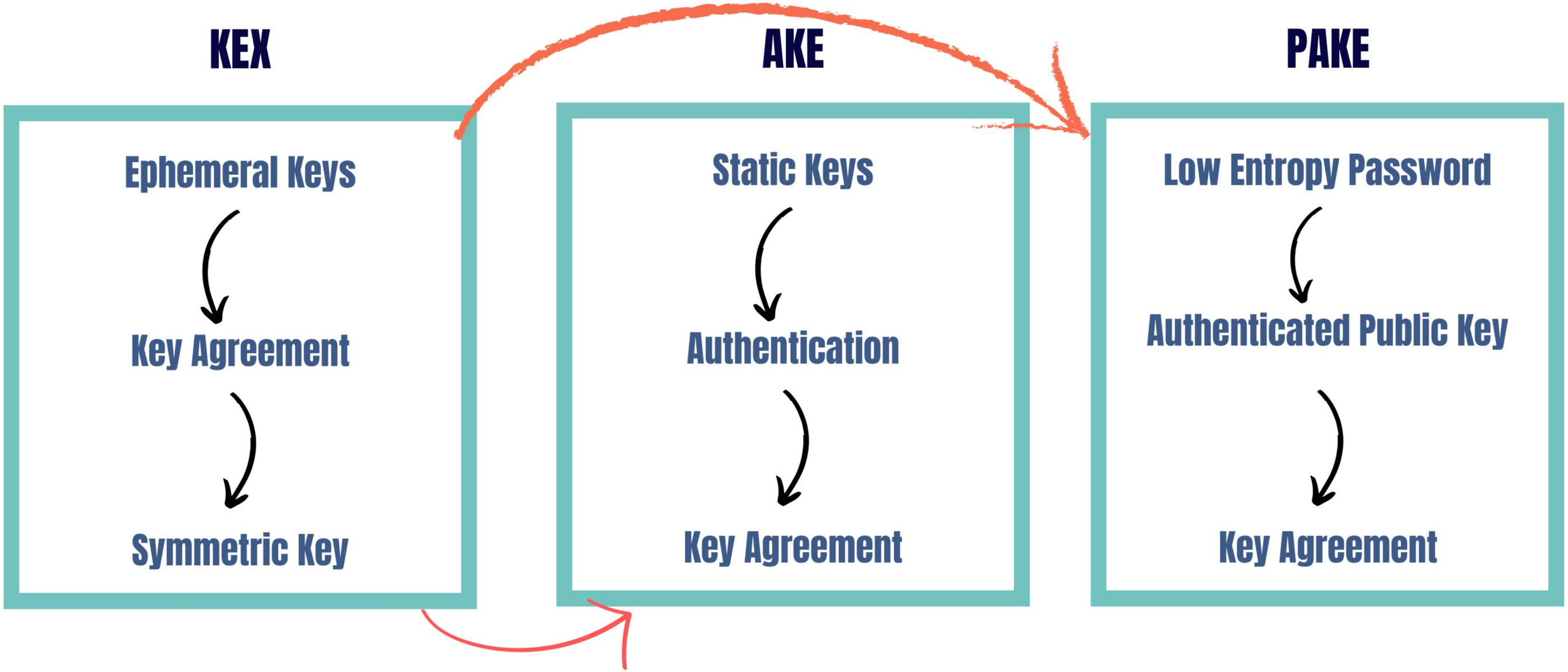
Nouri Alnahawi - David Haas - Erik Mauß - Alex Wiesmaier

PQC Workshop - Darmstadt - 2025

MOTIVATION


Classical PAKEs
?
Quantum-safe PAKEs
PQC PRIMITIVES
CRYPTO-AGILITY
INTEGRATION & MIGRATION
NIST STANDARDIZATION
WORLDWIDE EFFORTS
SECURITY ANALYSIS
LIBRARIES / APIs
HARDWARE
PERFORMANCE
PHYSICAL PROTECTION
PROTOCOLS / APPs
KEY AGREEMENT PROTOCOLS

KEY EXCHANGE AND PAKE



FROM KEX TO PAKE

- Many designs use a password to authenticate a DH or RSA key agreement

KEX	PAKE
Only Agreement	Password Based Authenticated
DH	PAK
ECDH	EKE
RSA	SPEKE
...	PACE
	...

FROM CLASSICAL TO PQC

- Replace DH in PACE by a PQC KEX?

PQC KEX → PQC PAKE

Only Agreement

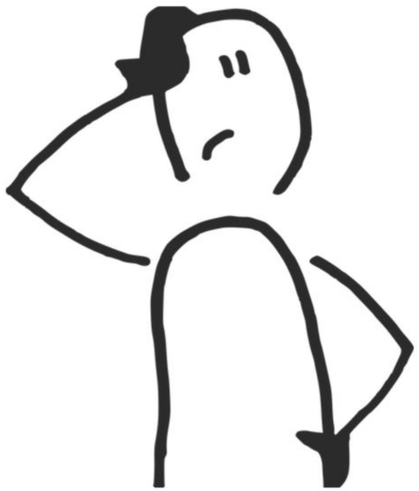
Peikert-KEX
DING-KEX
...

Password Based Authenticated

?

PQC KEY AGREEMENT

- DH and SIDH are commutative, contributive and non-interactive
- LWE is semi-commutative (error reconciliation)
- Early LWE schemes rely on signaling and are thus interactive



	(EC)DH	SIDH	LWE
G	$g \in \mathbb{G}$	$(P_i, Q_i)_i$	$\mathbf{A} \in R_q^{k \times k}$
a	$a \in \lvert\mathbb{G}\rvert$	ϕ_A	$(\mathbf{s}_a, \mathbf{e}_a)$ short
A	g^a	$E_A, \phi_A(E_2)$	$\mathbf{s}_a^t \cdot \mathbf{A} + \mathbf{e}_a^t$
B	g^b	$E_B, \phi_B(E_3)$	$\mathbf{A} \cdot \mathbf{s}_b + \mathbf{e}_b$
h	-	-	Yes
Static?	Yes	No	No

DING-RLWE PAK

- Based on Mackenzie's PAK
- Uses Ding's RLWE crypto-system
- Requires signaling for reconciliation

$$(\mathbf{s}_a^t \cdot \mathbf{A} + \mathbf{e}_a^t)\mathbf{s}_b \approx \mathbf{s}_a^t(\mathbf{A} \cdot \mathbf{s}_b + \mathbf{e}_b)$$

Alice		**Bob**
Password π		*Password* π
	Mapping Protocol	
generate $\mathbf{s}_A, \mathbf{e}_A \in \mathbb{R}_q[\chi]$		generate $\mathbf{s}_B, \mathbf{e}_B \in \mathbb{R}_q[\chi]$
$\mathbf{p}_A = \mathbf{M}\mathbf{s}_A + 2\mathbf{e}_A$	$\leftarrow \mathbf{p}_B$	$\mathbf{p}_B = \mathbf{M}\mathbf{s}_B + 2\mathbf{e}_B$
$\mathbf{v}_A = \mathbf{p}_A + H(\pi)$	$\rightarrow \mathbf{v}_A$	
		$\mathbf{p}_A = \mathbf{v}_A - H(\pi)$
	authentication token	
	$sid = (A, B, \mathbf{v}_A, \mathbf{p}_B, \sigma, -H(\pi))$	
$K_A = \mathbf{p}_B^T \mathbf{s}_A$		$K_B = \mathbf{p}_A^T \mathbf{s}_B$
$= \mathbf{M}^T \mathbf{s}_B^T \mathbf{s}_A + 2\mathbf{e}_B^T \mathbf{s}_A$		$= \mathbf{s}_A^T \mathbf{M}^T \mathbf{s}_B + 2\mathbf{e}_A^T \mathbf{s}_B$
	$\leftarrow w_B$	$w_B = CHA(K_B)$
$\sigma = MOD_2(K_A, w_B)$		$\sigma = MOD_2(K_B, w_B)$
$T_A = H_A(sid)$	$\rightarrow T_A$	
	$\leftarrow T_B$	$T_B = H_B(sid)$
abort if $T_B \neq H_B(sid)$		abort if $T_A \neq H_A(sid)$
	Establish key	
$K_{AB} = KDF(sid)$		$K_{AB} = KDF(sid)$

OVERVIEW SO FAR...

Classical PAKEs

???

Direct PQC PAKEs

Non-NIST

Lattices & Isogenies

RLWE KEX

ROM

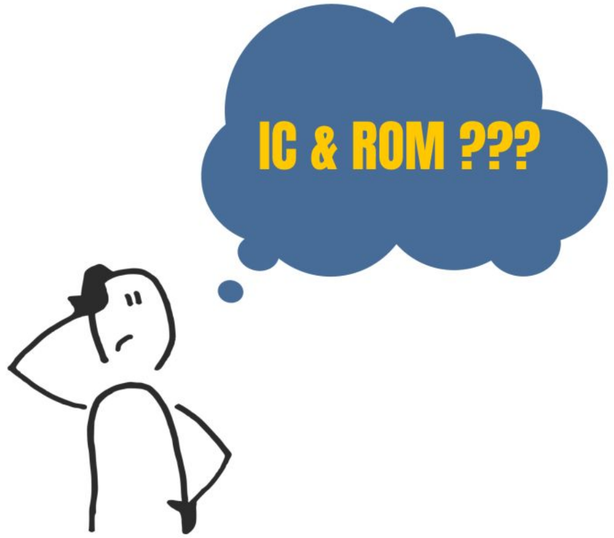
Direct Assumptions

BPR

PAK-Style

(O)EKE & (O)CAKE

- Generic design based on (O)EKE [8]
- Do not establish a new generator
- Authenticate the public key
- Encrypt public key instead of modifying it
- **Relies on the ROM and IC model**

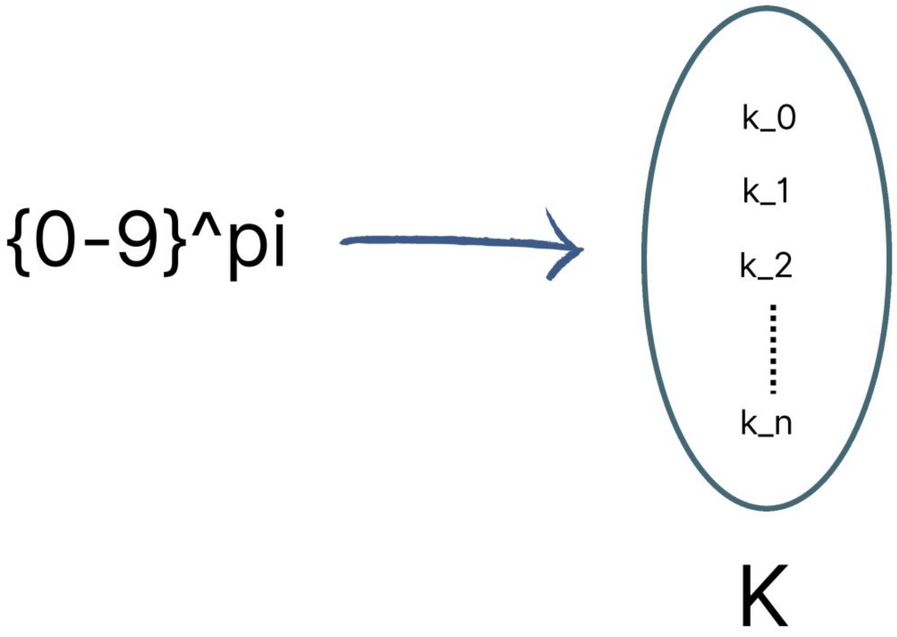


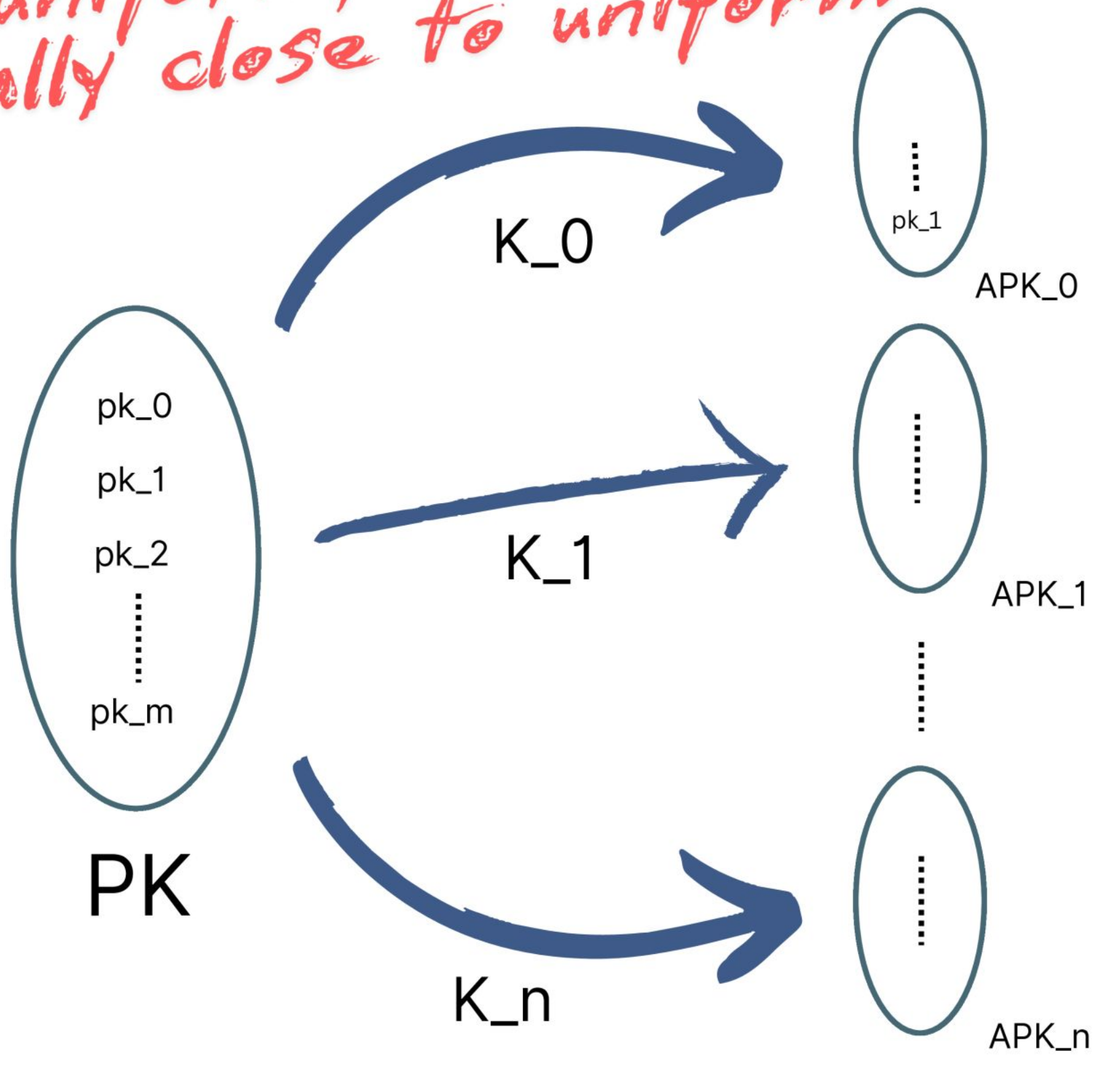
Alice	**Bob**
$Password\ \pi$	$Password\ \pi'$
$K_\pi = \mathcal{KDF}(\pi)$	$K_{\pi'} = \mathcal{KDF}(\pi')$
$sk_a, pk_a \xleftarrow{\$} KeyGen$	
$apk_a \xleftarrow{\$} C_{K_\pi}(pk)$	
$\xrightarrow{apk_a}$	
	$pk'_a = \mathcal{C}^{-1}_{K_{\pi'}}(apk_a)$
	$(c_b, \overline{K}) = Encap(pk'_a)$
$\xleftarrow{c_b}$	
$\overline{K}^* = Decap(sk_a, c_b)$	
$K = \mathcal{KDF}(\overline{K}^*)$	$K = \mathcal{KDF}(\overline{K})$

ROM & IC

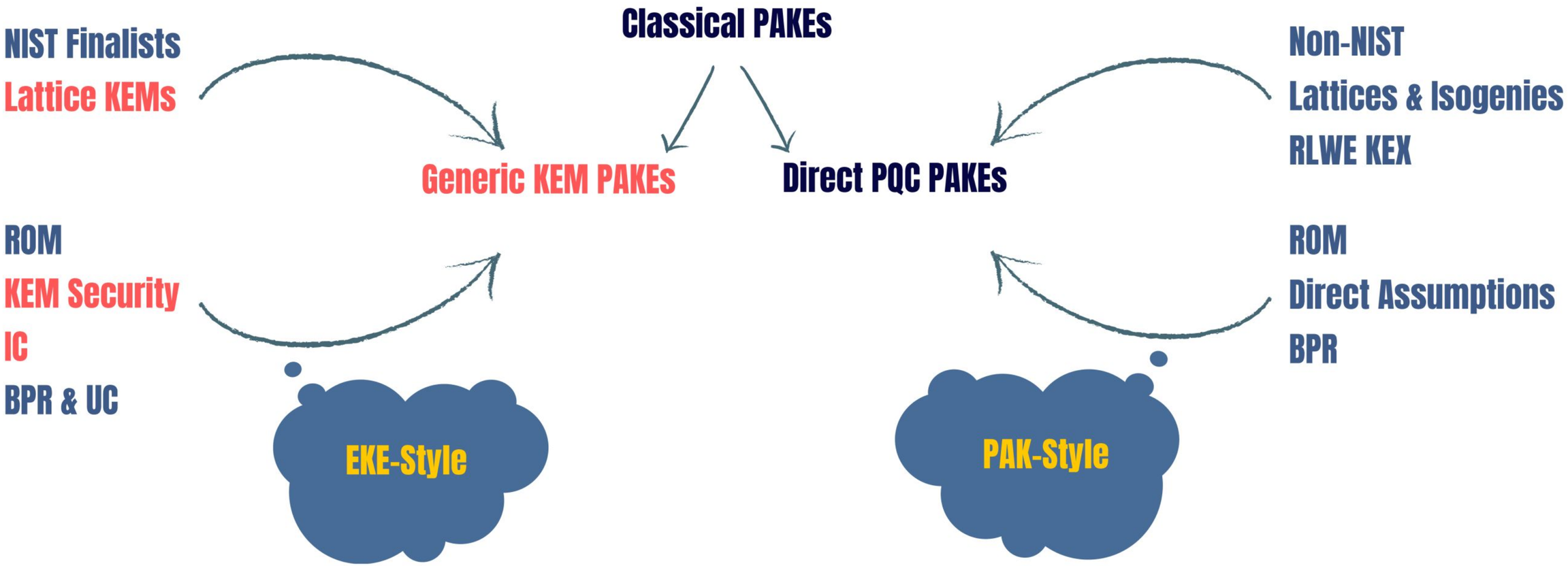
Kyber keys are only computationally indistinguishable from uniform, but not statistically close to uniform

- Deterministic mapping of inputs to outputs
- Deterministic mapping of permutations in both directions





OVERVIEW SO FAR...



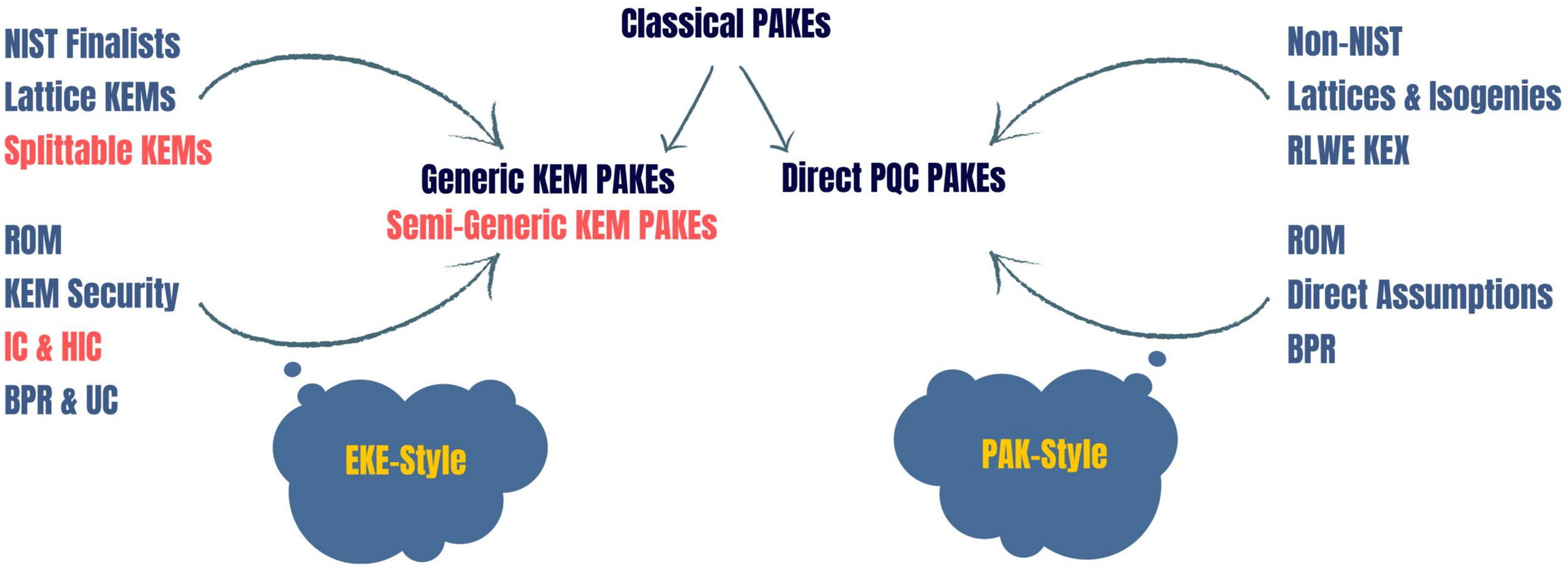
HALF IC & SPLITTABLE LWE KEYS

- Randomized Half IC on Groups by Dos Santos, Gu and Jarecki (EC'23)
- **C'est très CHIC by Arriaga, Barbosa, Jarecki and Skrobot (AC'24)**

Split a key and use the uniform bit string part to achieve a domain extension!

- LWE, RLWE and MLWE public keys of the form (A,<b = As+e>)
- A is sampled from a uniform random bit string of fixed length (call it rho!)
- Use lattice base seed for an IC encryption instead of a structured public key

OVERVIEW SO FAR...



ADDING OTHER COMPONENTS

NIZKs

Zero Knowledge Proofs

Public key as CRS

KOY-GL or PAK PAKEs

SPHFs

Hashing

Complicated stuff...

KOY-GL or PAK PAKEs

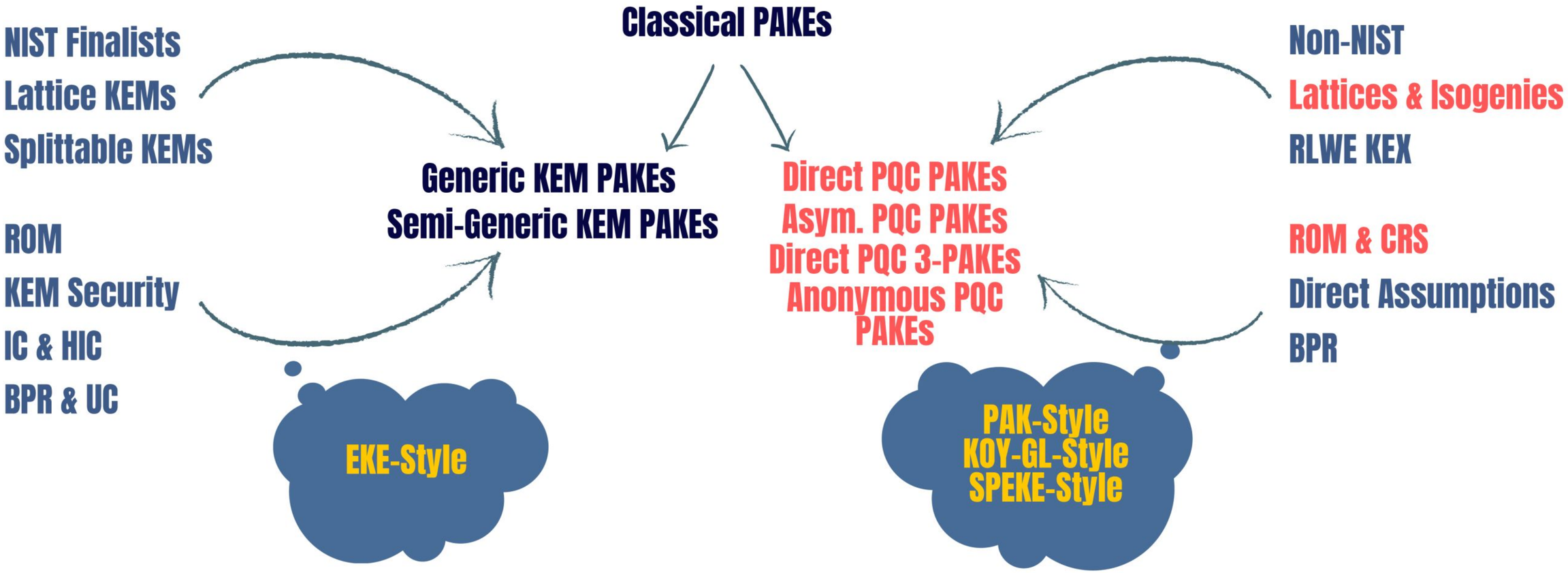
CRS

Pre-Registeration

Static Public Key

KOY-GL or PAK PAKEs

OVERVIEW SO FAR...



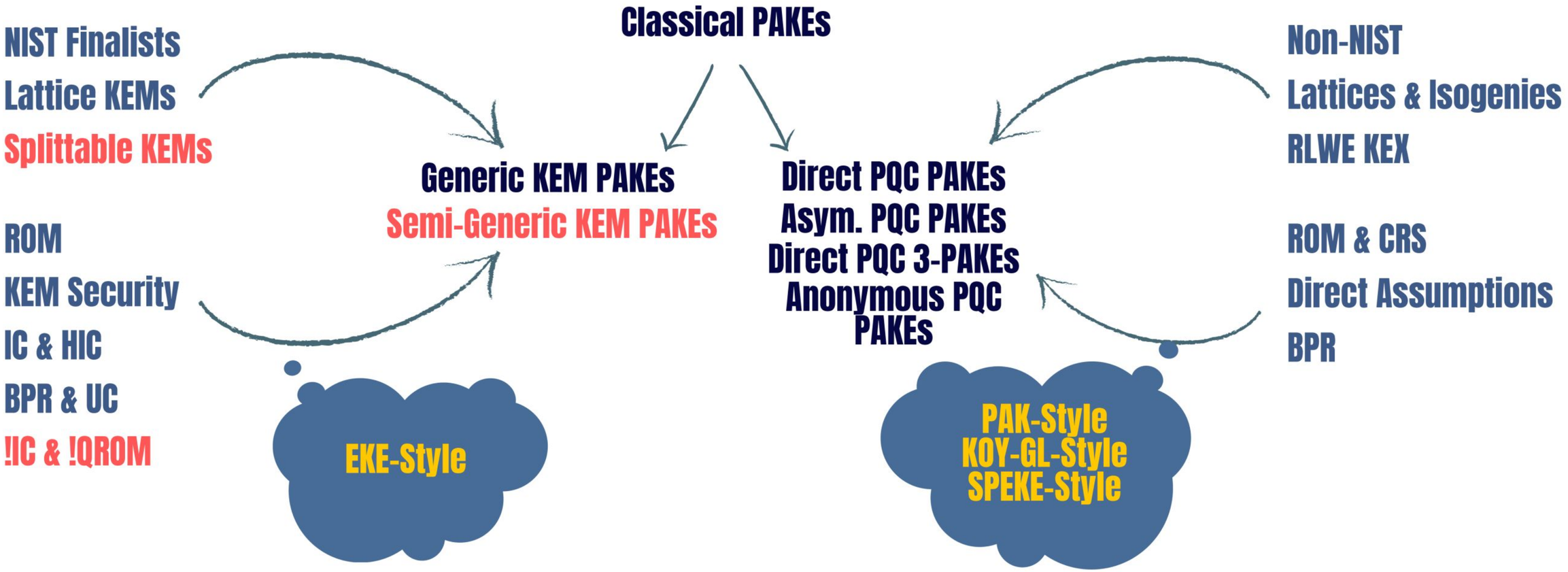
NICE-PAKE

- Splittable KEMs from LWE, RLWE and MLWE
- Inspired by CHIC
- Authenticate sampling seed of lattice base
- Simple XOR of hash output from password
- **No IC or QROM involved in proof!**

Alice		**Bob**
Password π		*Password* π'
$sk_a, pk_a \xleftarrow{\$} \mathbf{KEM.KeyGen}$		
$(\rho, \mathbf{b}) \leftarrow pk_a$		
$z \leftarrow \rho \oplus \mathcal{H}(\pi)$		
	$\xrightarrow{z, \mathbf{b}}$	
		$\rho' \leftarrow z \oplus \mathcal{H}(\pi')$
		$pk'_a \leftarrow (\rho', \mathbf{b})$
		$(C_b, \overline{K'}) = \mathbf{KEM.Encap}(pk'_a)$
	$\xleftarrow{C_b}$	
$\overline{K} = \mathbf{KEM.Decap}(sk_a, C_b)$		

Relies on specific lattice assumptions and requires additional KEM security preoperties!

OVERVIEW SO FAR...



HONORABLE MENTIONS

Fuzzy

Biometrics

↓

Garbled Circuits & ECC

↓

Symmetric PAKEs

Annoying

Hiding Elements

↓

d-log based schemes

↓

Quantum-Annoying PAKEs

OVERVIEW SO FAR...

- Only one PQC PAKE in the QROM
- Only four in UC
- Almost all from lattices
- Almost all based on DING-RLWE PAK

						Generic?	Quantum-Safe?	Peer-Reviewed	2-Party	3-Party	Benchmarks	Provide Impl.	Recomm. Param.
Balanced													
C1	Terada, Yoneyama [TY19] ((C)SIDH-EKE)	2019	IC, ROM	SIDH, CSIDH	BPR			✓	o		✓		
	Dos Santos et al. [DGJ23] (HIC-EKE)	2023	IC, ROM	MLWE, MLWR	UC	✓		✓	o				
	Beguinet et al. [BCP+23] ((O)CAKE)	2023	IC, ROM	MLWE	UC	✓		✓	o				
	Alnahawi [AHHR24] (OCAKE)	2023	IC, ROM	MLWE, LWE	BPR	✓			o		✓		
	Pan, Zeng [PZ23] (CAKE)	2023	IC, ROM	LWE	BPR	✓		✓	o				
	Arriaga et al. [ABJS24] (CHIC)	2024	IC, ROM	MLWE	UC	✓			o		✓	✓	✓
	Alnahawi et al. [AASAW24] (NICE-PAKE)	2024	ROM	NLWE / whLWE	BPR	✓	✓?		o				✓
C2	Zhu, Geng [ZG15]	2015	-	SIDH/CSIDH	CK				o				
	Alsayigh [Als16]	2016	ROM	RLWE	BPR				o				✓
	Ding et al. [DAL+17, Din17] (RLWE-PAK-PPK)	2017	ROM	RLWE	BPR			✓	o		✓		
	Gao et al. [GDL+17] (RLWE-PAK-PPK)	2017	ROM	RLWE	BPR				o		✓		
	Taraskin et al. [TSJL20] (SIDH-PAK)	2019	ROM	SIDH	BPR				o		✓		✓
	Yang et al. [YGWX19] (RLWE-PAK)	2019	ROM	RLWE	BPR			✓	o		✓		✓
	Jiang et al. [JGH+20] (PAKEs)	2020	ROM	LWE, RLWE	BPR			✓	o		✓		✓
	Ren et al. [RGW23]([RG22]) (MLWE-PAK)	2022	-	MLWE	Hybrid			✓	o		✓	✓	✓
	Seyhan, Akleylek [SA23]	2023	ROM	MLWR	Hybrid				o		✓	✓	✓
	Basu et al. [BSIA23] (MLWR-2PAKA)	2023	ROM	MLWR	DY			✓	o				✓
C3	Katz, Vaikuntanathan [KV09]	2009	CRS	LWE	BPR		✓	✓	o				
	Xu et al. [XHCC17] (RLWE-3PAKE)	2017	ROM	RLWE	BPR					o	✓		✓
	Zhang, Yu [ZY17]	2017	CRS, ROM	LWE	BPR				o				
	Choi et al. [CAK+18] (AtLast)	2018	ROM	RLWE	BPR			✓		o			
	Li, Wang [LW18]	2018	CRS	LWE	BPR		✓	✓	o				
	Li, Wang [LW19]	2019	CRS	LWE	BPR		✓	✓	o				
	Karbasi et al. [KAA19] (Ring-PAKE)	2019	CRS	RLWE	BPR		✓	✓	o				
	Yin et al. [YGS+20]	2020	ROM	LWE	BPR			✓	o	o			
	Lyu et al. [LLH24]	2024	(Q)ROM	LWE, GA-DDH	UC	✓	✓	✓	o				
Augmented													
C2	Gao et al. [GDLL17]	2018	-	RLWE	UC			✓	o		✓		✓
C3	Zhu et al. [ZHS14]	2014	-	SIDH	CK			✓		o			
	Feng et al. [FHZ+18]	2018	ROM	RLWE	BPR			✓	o		✓		✓
	Liu et al. [LZJY19]	2019	ROM	RLWE	Hybrid					o	✓	✓	✓
	Dabra et al. [DBK20] (LBA-PAKE)	2020	ROM	RLWE	FTG			✓	o		✓		✓
	Li et al. [LWM22]	2020	CRS	LWE, LWR	BPR		✓	✓	o		✓		✓
	Tang et al. [TLZ+21]	2021	ROM	RLWE	BPR			✓		o	✓		✓
	Islam, Basu [IB21] (BP-3PAKA)	2021	ROM	RLWE	BPR			✓		o	✓		
	Ding et al. [DCQ22]	2022	RoR	RLWE	FTG			✓	o		✓	✓	✓
	Abdalla et al. [AEK+22a] (X-GA-PAKE)	2022	CRS	CSIDH	BPR		✓		o				
	Wang et al. [WCL+23] (LB-ID-2PAKA)	2023	ROM	MLWE	BPR			✓	o				
	Dharminder et al. [DRD+23]	2023	Standard	RLWE	Hybrid			✓	o		✓		✓
	Dadsena et al. [DJRD23]	2023	ROM	RLWE	BPR			✓	o		✓		✓
	Kumar et al. [KGKD23]	2023	ROM	RLWE	BPR			✓	o		✓		✓
	Guo et al. [GSG+23]	2023	ROM	MLWE	BPR			✓		o	✓		✓
	Chaudhary et al. [CKS23]	2023	ROM	RLWE	BPR			✓		o	✓		✓

h_da
HOCHSCHULE DARMSTADT
UNIVERSITY OF APPLIED SCIENCES

acsd applied cyber security darmstadt

THANK YOU

Nouri Alnahawi - David Haas - Erik Mauß - Alex Wiesmaier
PQC Workshop - Darmstadt - 2025