

# PQarrots

Post Quantum Actions for Round Robin Threshold Schemes  
An overview of isogeny-based threshold schemes package

Presented at : MPTS 2026: NIST Workshop on Multi-Party Threshold Schemes 2026 - Preview Talk  
Date : 2026-01-29

Presented by : **Giacomo Borin**, IBM Research Zurich, University of Zurich  
joint work with ...



Universität  
Zürich<sup>UZH</sup>



Marius A. Aardal,  
Shahla Atapoor,  
Karim Baghery,  
Andrea Basso,  
Xavier Bonnetain,  
Giacomo Borin,  
Daniele Cozzo,  
Pierrick Dartois,  
Luca De Feo,  
Max Duparc,  
Jonathan K.  
Eriksen,

Tako Boris  
Fouotsa,  
Chloe Martindale,  
Arthur H. Le  
Merdy,  
Riccardo  
Invernizzi,  
Samuel Jaques,  
Yi-Fu Lai,  
Dania Lazzarini,  
Jason T. LeGrow,  
Luciano Maino,  
Jonas Meers,

Michael Meyer,  
Sikhar  
Patranabis,  
Robi Pedersen,  
Giacomo Pope,  
Doreen Riepel,  
Damien Robert,  
Ryan Rueger,  
Sina Schaeffler,  
André  
Schrottenloher,  
Frederik  
Vercauteren

# PQarrots: Post Quantum Actions for Round Robin Threshold Schemes

## Macaw (signature S1)

- Costly offline preprocessing
- 2 round online signing
- Interactive IA protocol

## Kea (pke S2)

- Compact Encaps
- Sequential Decaps procedure
- Interactive IA protocol

## Kakapo (dkg S4)

- Combines VSS and NIZK proofs a la CSI-RaShi++
- Honest majority

## Advantages

1. Quantum-safety, with a non-lattice assumption
2. Compactness wrt keys, sigs and cts
3. Generic isogeny-agnostic framework

## Disadvantages

1. Quantum sub-exponential attack
2. Less efficient schemes wrt to some other isogeny-based ones.
3. Inherently sequential structure

# Cryptographic group actions

Pro and cons of the framework

Group:  
set with an  
associative  
invertible  
**commutative**  
operation

Set

$$G \times X \rightarrow X$$

$$(a, x) \mapsto a \star x$$

Properties  
it needs to  
satisfy

$$a \star (b \star x) = (ab) \star x$$

$$a \star (a^{-1} \star x) = x$$

gaDLOG  
hardness  
assumption

Given:  $x, a \star x \in X$

Find:  $a \in G$

# Differences with DLOG & Distributing the group action

$$G \times X \rightarrow X$$

$$(a, x) \mapsto a \star x$$

Shared secret

$$s = \lambda_1 s_1 + \dots + \lambda_T s_T$$

For ECC:  $a \star g = g^a$   
 $G =$  modular integers  
 $X =$  points of a curve

X is also a Group!

$$g^{s_1}, \dots, g^{s_T} \xrightarrow{\text{combine}} (g^{s_1})^{\lambda_1} \dots (g^{s_T})^{\lambda_T} = g^s$$

(public)

For Isogenies :  
 $G =$  ideals  
 $X =$  curves

No "curve addition"

$$g^{s_1} \star x, \dots, g^{s_T} \star x \xrightarrow{\text{combine}} g^{s_1 \lambda_1} \dots g^{s_T \lambda_T} \star x = g^s \star x$$

(public)

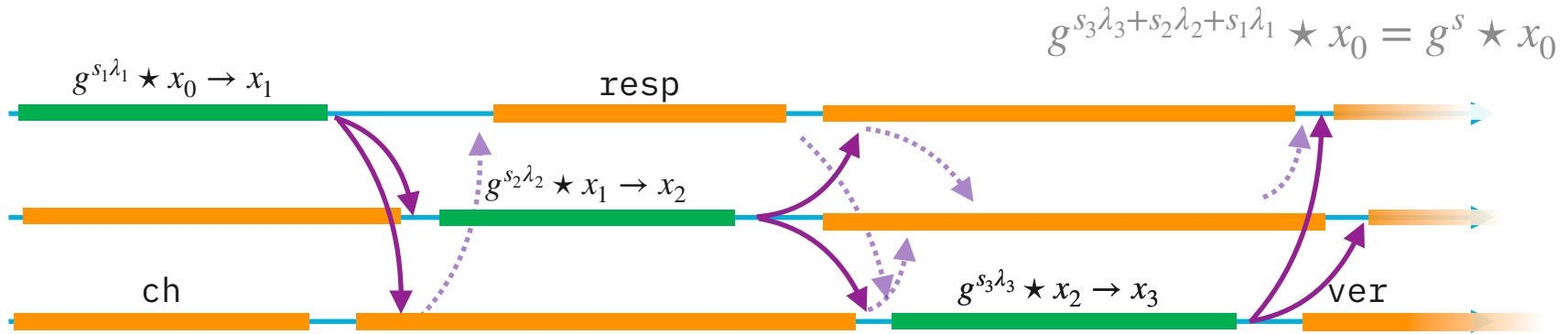
More general sharing (BBSS, LISS or Recursive)

Round Robin computation

Cozzo, Daniele, and Emanuele Giunta. "Round-robin is optimal: lower bounds for group action based protocols."  
 Yvo Desmedt, Giovanni Di Crescenzo, and Mike Burmester. "Multiplicative Non-abelian Sharing Schemes and their Application to Threshold Cryptography"  
 Ronald Cramer and Serge Fehr. "Optimal Black-Box Secret Sharing over Arbitrary Abelian Groups".

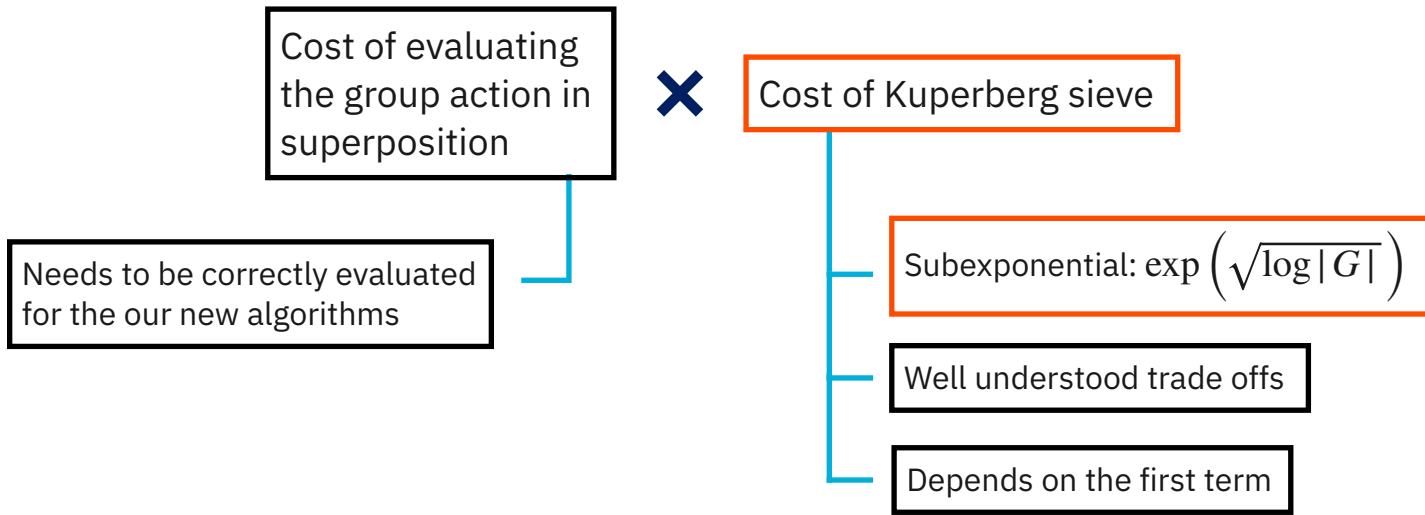
# Sequential computation of the action

	[Sig Prepr]	[PKE Decaps]	[DKG]	[IA]
ga Sequential computation	✓	✓	✓	
NIZK			✓	✓
Private Coin Proofs	✓	✓		



# Quantum security and impact on parameters

- The Group Action is commutative, so quantum sub-exponential algorithms applies
- The cost needs to be concretely evaluated:



We are producing tools to compute the actual practical security of gaDLOG

# Group action evaluation estimates

Same classical security as SQIsign NIST I, III, V

Parameter set	<i>optimist</i>	<i>prudent</i>	<i>pessimist</i>
Size of $p$ (in bits)	512	1024	2048
Estimated C timings (in MCycles)	103	510	3633
Estimated C timings (in ms)	41	204	1450

Size of $p$	512 bits			1024 bits			2048 bits		
profile	(2,3)	(3,5)	(8,16)	(2,3)	(3,5)	(8,16)	(2,3)	(3,5)	(8,16)

Threshold Signing Preprocessing estimates for three different choices of pk size (in sec)

Small	6.03	10.04	30.14	29.99	49.98	149.94	213.74	356.23	1068.69
Medium	2.34	3.90	11.69	11.63	19.38	58.14	82.88	138.13	414.39
Large	1.35	2.25	6.76	6.73	11.22	33.66	47.98	79.97	239.91

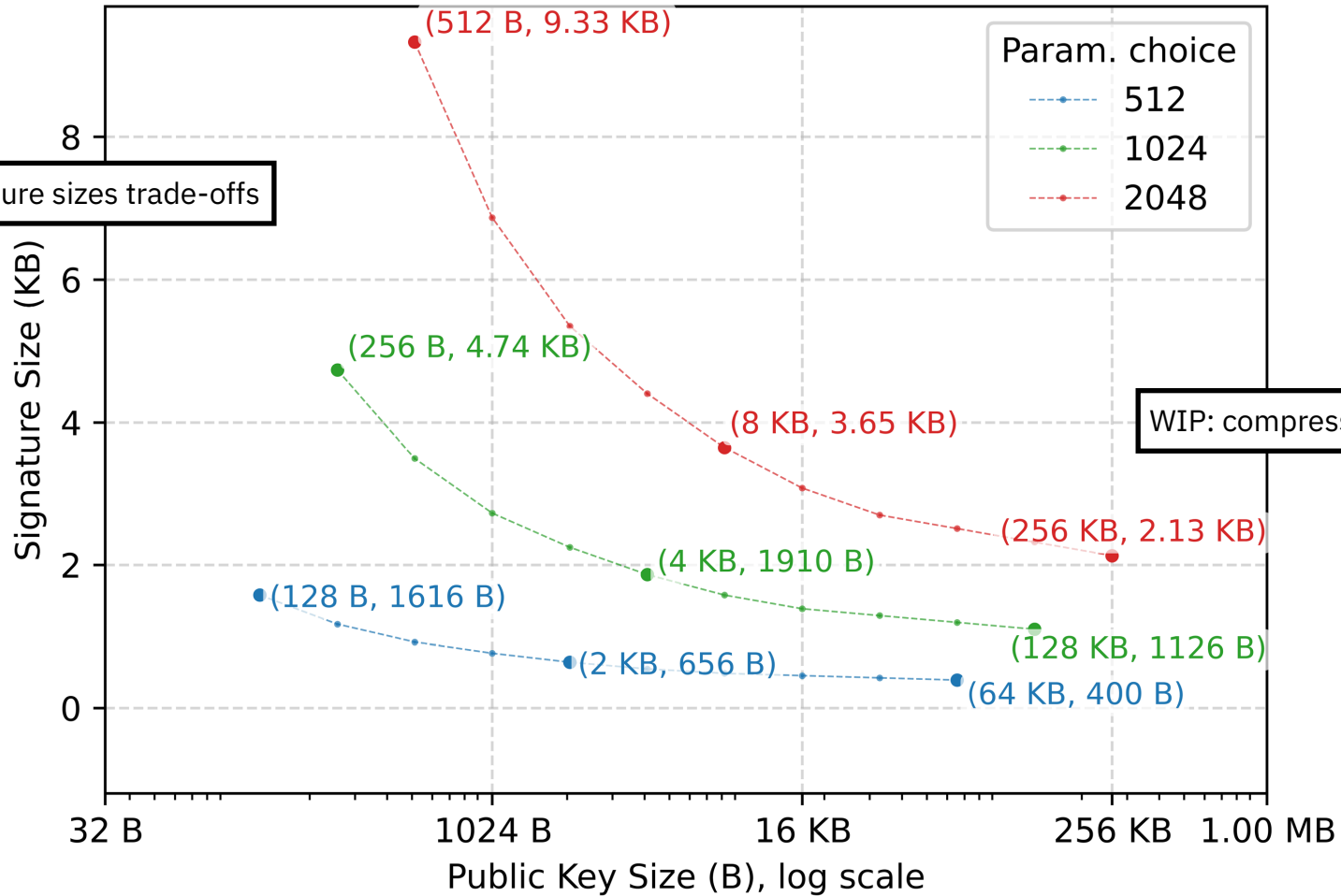
Threshold PKE estimates (in ms)

Dec.	123	246	1476	612	1224	7344	4362	8724	52344
Enc.		82			408			2908	

Distributed Key Generation estimates (in min)

DKG	0.4	0.5	1.4	1.7	2.6	7.0	12.5	18.7	49.8
DKG IA	1.4	3.2	23.9	17.5	55.0	678.1	124.6	392.4	4832.9

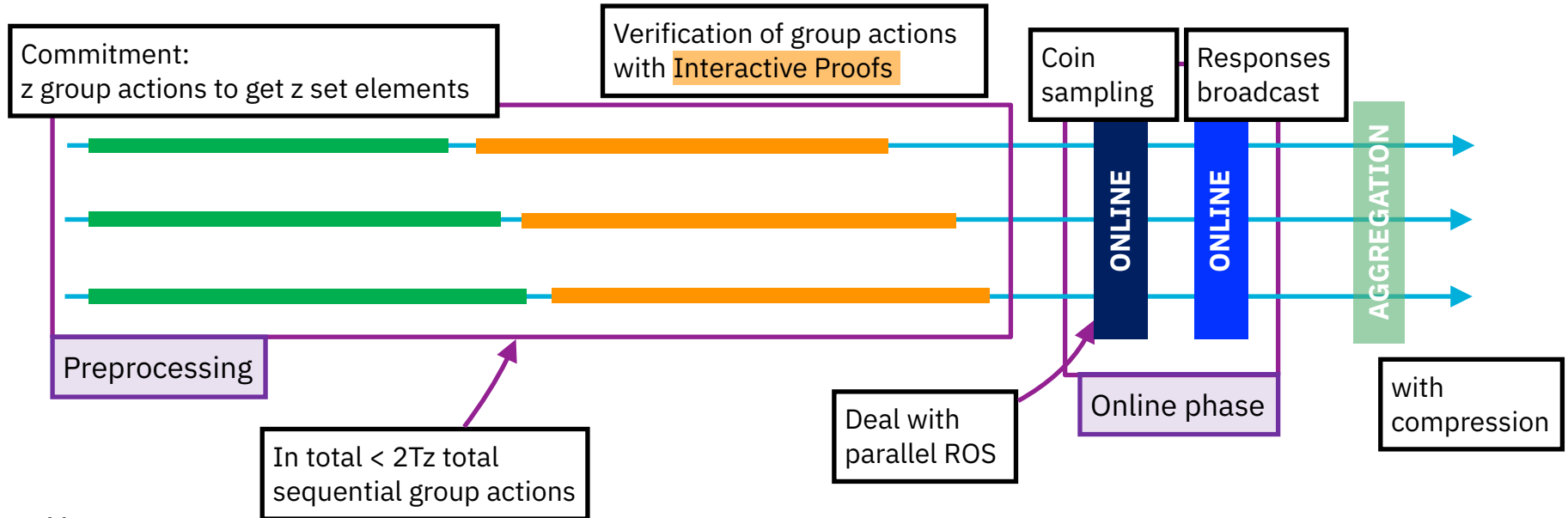
Signature sizes trade-offs



**Details on the schemes**

# Macaw: Threshold Signing

- Inspired by SeaSign and CSI-FiSh.
- Unforgeable against active adversaries (static)
- Interactive Identifiable Aborts with **NIZKs**



# Kea: Threshold PKE

## ▪ Encaps:

- 2 group actions
- 1 NIZK

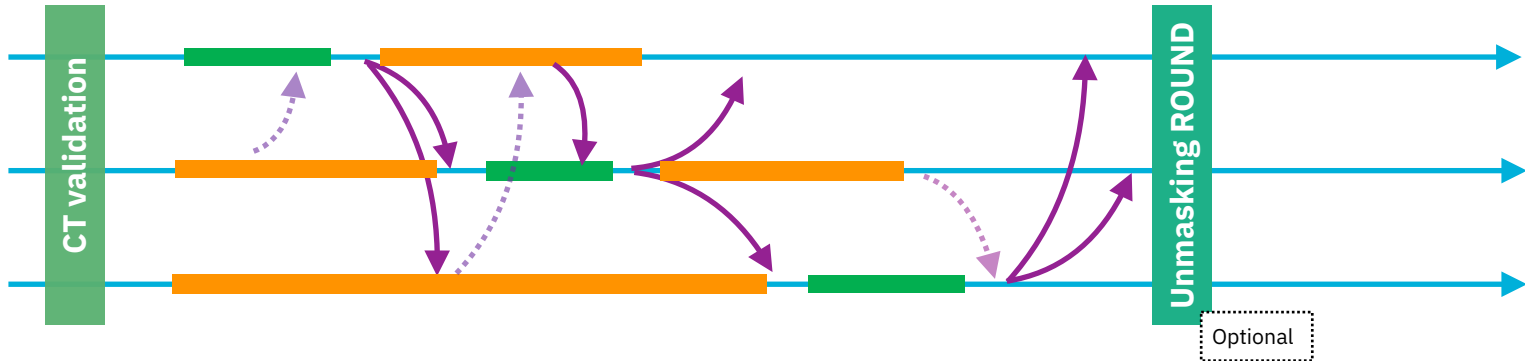
Ensure CCA\*

Compact gadget  
(isogeny-specific)

## ▪ Decaps:

- CT validation
- T sequential group actions
- Interactive proofs for CCA

- We define a restricted notion of threshold CCA
- Interactive Identifiable Aborts with NIZKs



# Bonus: Alternative *Naïve* Threshold PKE

Classical Secret Sharing +  $N$ -wise PKE + Randomness Reuse

## Cons

- Public keys scale in  $N$ , the number of parties
- Ciphertexts scale in  $N-T^*$  ( $\sim 5$  KB per  $(T,N)=(16,32)$ )
- Encryption is linearly slow

## Pros

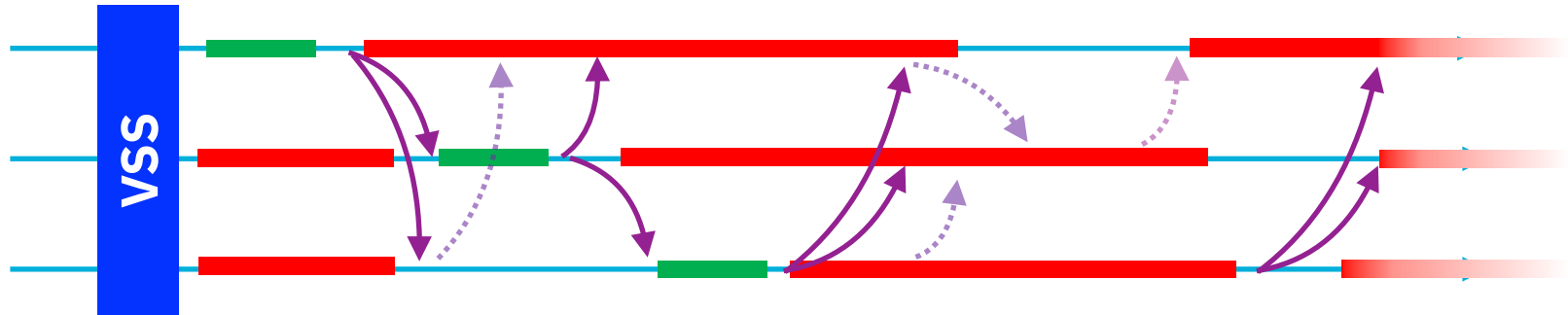
- Silent setup
- Updatable public keys
- Full CCA security
- Constant round complexity in Decaps
- Adaptive corruptions
- Security under standard assumptions

**CALL FOR  
FEEDBACKS**

# Kakapo: Distributed key generation

- A. Verifiable Secret Sharing (honest majority)
- B. Sequential group actions computations
- C. NIZK to verify the correct sharing and public shares

for Macaw it needs to be  
repeated multiple times (1x to 1024x)

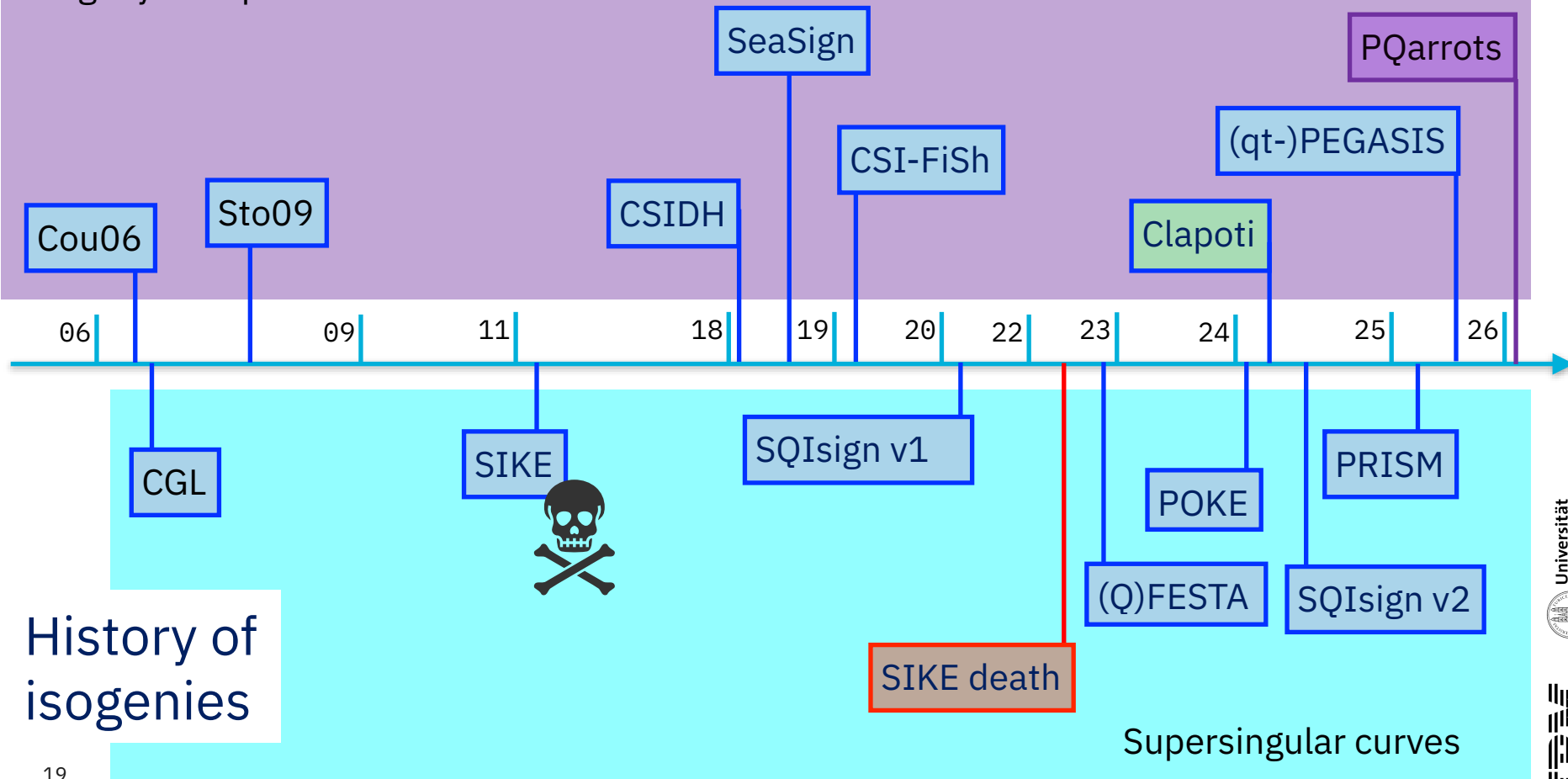


Same as piVer,  
adapted to our sharings

# Isogeny-based group action

A contextualisation of PQarrots in Isogeny-based cryptography

# Isogeny Group Action



## History of isogenies

# Project Organisation with two layers of abstraction

1. Analysis, specification and high-level **Python** implementation of the threshold schemes, in a group-action-agnostic way.
2. Specification and low-level **pure-C** implementations of the isogeny group action and isogeny-specific gadgets.
3. A report on the (quantum) security of our assumptions.



Thanks

[tga-nist@groupe.renater.fr](mailto:tga-nist@groupe.renater.fr)