A Post-Quantum Oblivious PRF from Isogenies

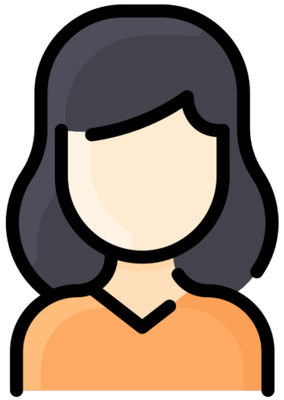
Andrea Basso

UNIVERSITY OF BIRMINGHAM

University of BRISTOL

14th February, 2023
Isogeny Club

Oblivious PRF



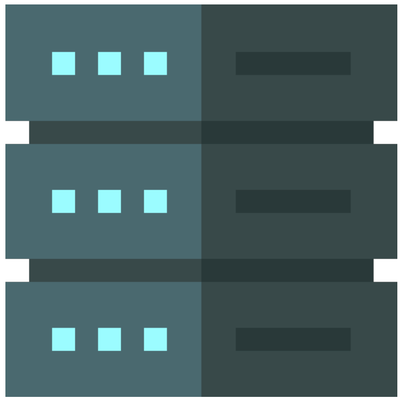
Client

F(k, m)

com(k)

[[m]]

f(k, [[m]]), π

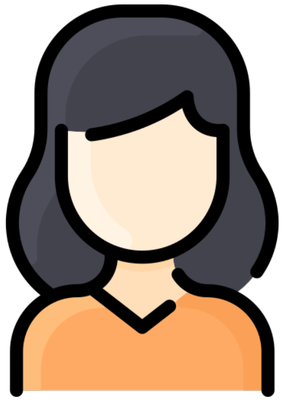


Server

⊥

- Password-checking in Microsoft Edge
- OPAQUE
- Privacy pass
- Private-set intersection
- Adaptive OT
- ....

HashDH OPRF



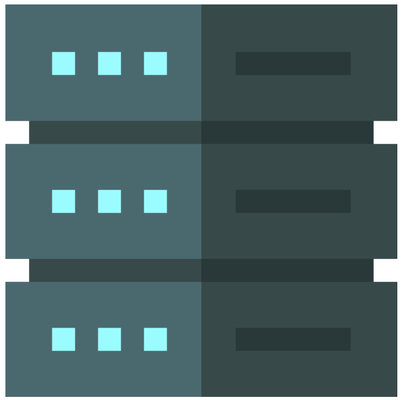
Client

$H(m)^k$

$H(m)^b$

$H(m)^{bk}$

- Server doesn't learn anything ✓
- Output is deterministic ✓
- Client only learns one output ✓



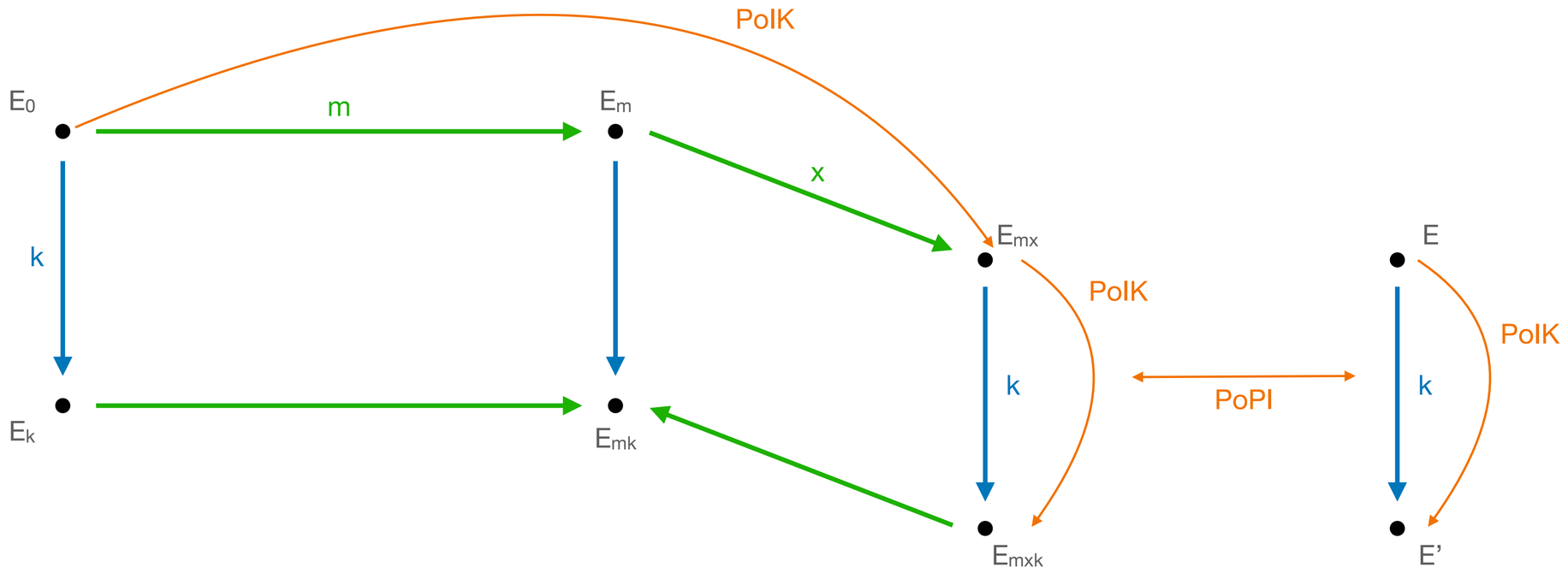
Server

$\perp$

Post-quantum OPRFs

- Generic MPC techniques → many rounds (≥ 5)
- VOPRF based on lattices [ADDS19] →
  - round optimal
  - feasibility result (> 2^{40} bits of comms)
- VOPRF based on SIDH [BKW20] →
  - six rounds
  - broken by attack on PR and on SIDH
- OPRF based on CSIDH [BKW20] →
  - three rounds (OT required)
  - CSIDH parameters?

The original OPRF [BKW20]

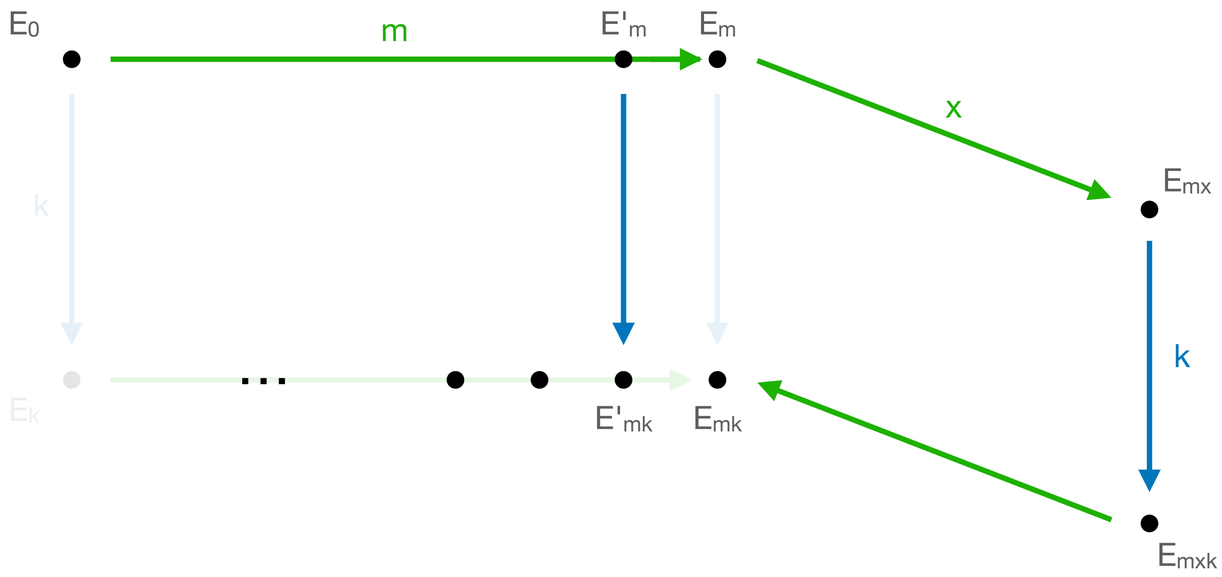


$$F(k, m) = H(m, j_{mk}, E')$$

Breaking pseudorandomness [BKMPS21]

Pseudorandomness: after n interactions, an attacker cannot generate n+1 PRF outputs

Part 1



Part 2

- Repeat the attack 3 times
- Find a basis on E_k
- Evaluate the PRF on *any* message

The server can check the degree with the PoK!

Actual complexity: sub-exponential

Countermeasures?

It seems hard to prevent an attacker from recovering a basis on E_k

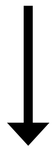
Validate more

Ensure that the client submits valid message isogenies

The protocol is oblivious

Update values

Use dynamic values for server's computations



The PRF needs to be deterministic

Scale parameters

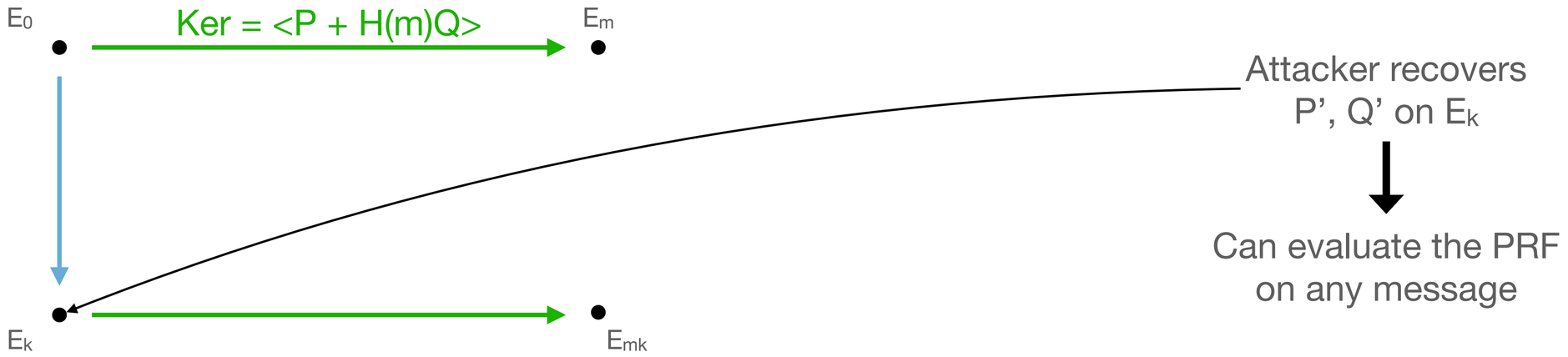
Attack is sub exponential

$p \approx 2^{16,000}$

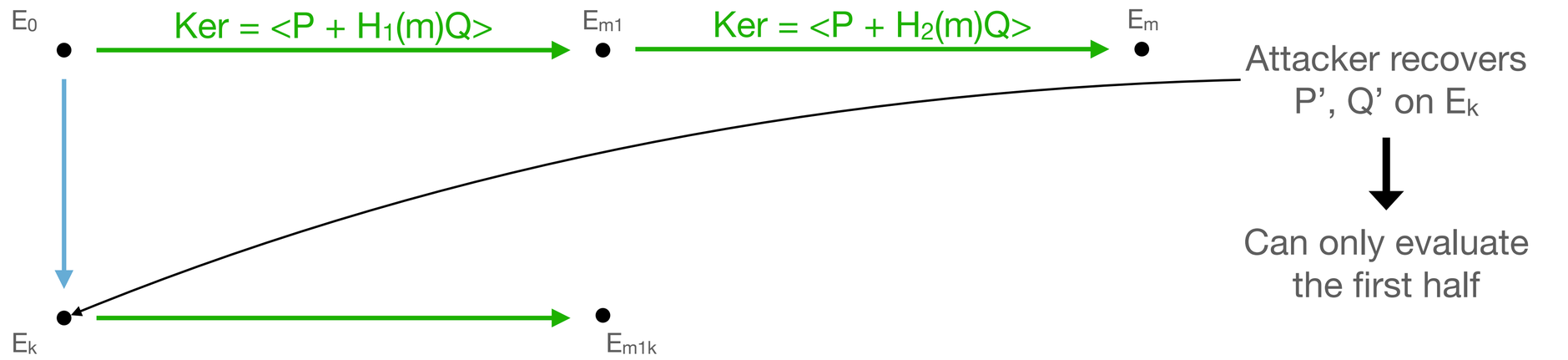
Idea: make the basis on E_k not enough for an attack

An efficient countermeasure

[BKM20]



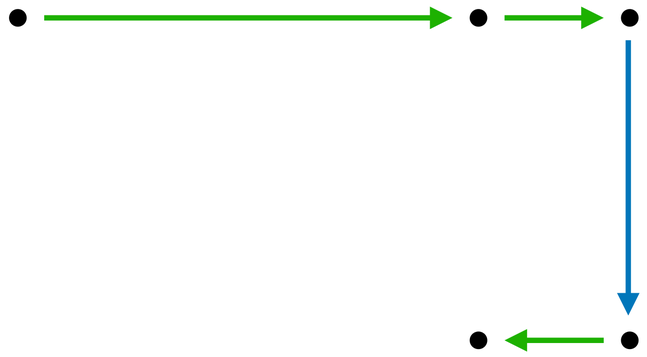
Our countermeasure



Preventing the SIDH attacks

First attempt

SIDH attacks requires N torsion
to recover a N^2 - degree isogeny



not really an OPRF

SIDH countermeasures

- Longer isogenies

only works for one party

- Masked-degree isogenies [Mor22]

hard to build proofs

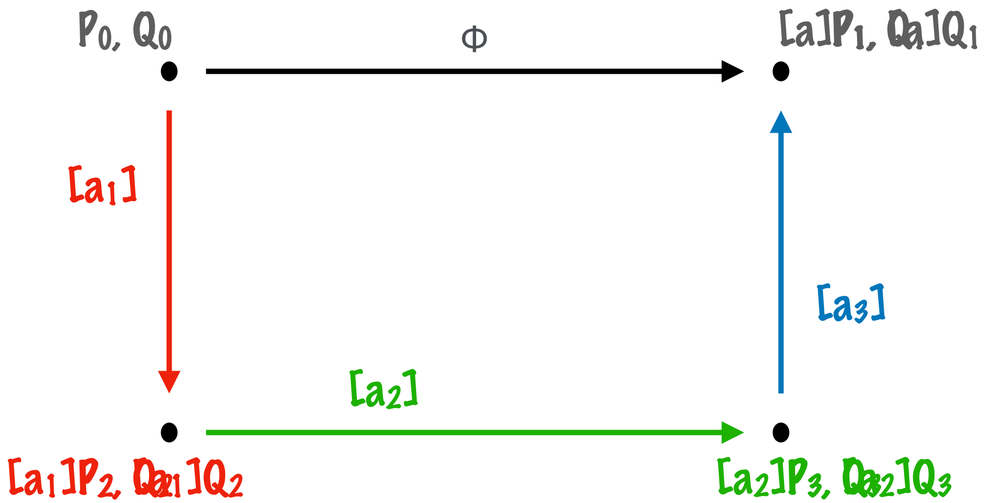
- Masked torsion points [Fou22]

it works

large prime

needs new PolK

PoIK with masked torsion



$a = a_1 \times a_2 \times a_3$

challenges from {-1, 0, 1}

soundness error = 2/3
—> need 1.7λ repetitions

Verifiability

[BKW20] uses 3 proofs:

Server's isogeny

Server's commitment

Run together

Isogeny is parallel
to commitment

Prove "parallelness" when
revealing horizontal isogeny

Non-interactive

Saves computations

Interactive (5 rounds)

Putting it all together

- Pseudorandomness countermeasure — no need for special prime; more efficient than original
- SIDH counteremeasures — would require $p \approx 2^{6000}$
- New SIDH proof requires a larger prime — requires $p \approx 2^{9000}$
- New PoPI — more efficient than original; round optimal

Protocol	Rounds	Bandwidth (avg.)	Verifiable	Secure
[ADDS21] (LWE)	2	>128 GB	✓	✓
[BKW20] (SIDH)	6	1.4 MB	✓	✗
[BKW20] (CSIDH)	3	424 kB	✗	✓
[This work]	2	1.9 MB	✓	✓