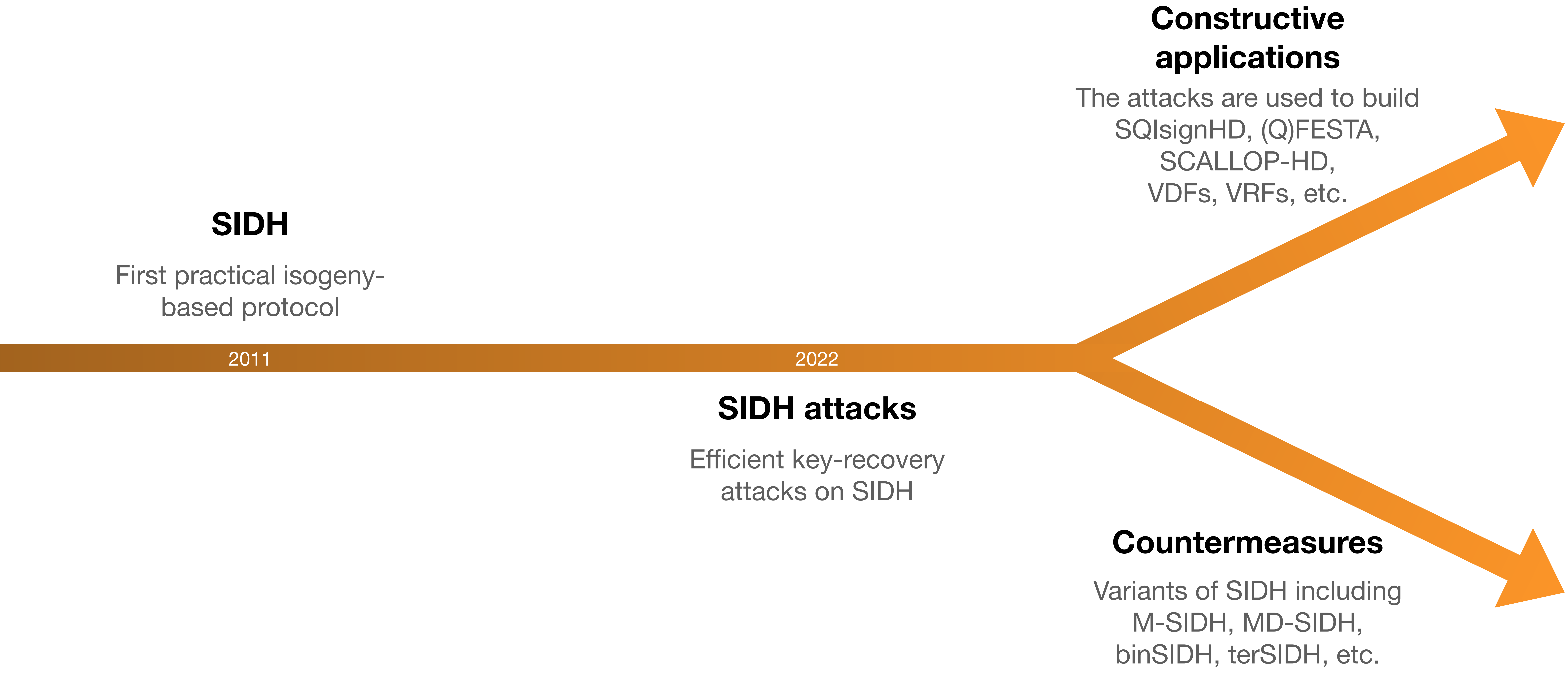
POKE: A Framework for Efficient PKEs, Split KEMs, and OPRFs from Higher-dimensional Isogenies

Andrea Basso

May 26th 2024 — Isogeny Club Brainstorm Days

A brief history of isogeny-based crypto



SIDH

First practical isogeny-based protocol

2011

2022

SIDH attacks

Efficient key-recovery attacks on SIDH

Constructive applications

The attacks are used to build SQIsignHD, (Q)FESTA, SCALLOP-HD, VDFs, VRFs, etc.

Countermeasures

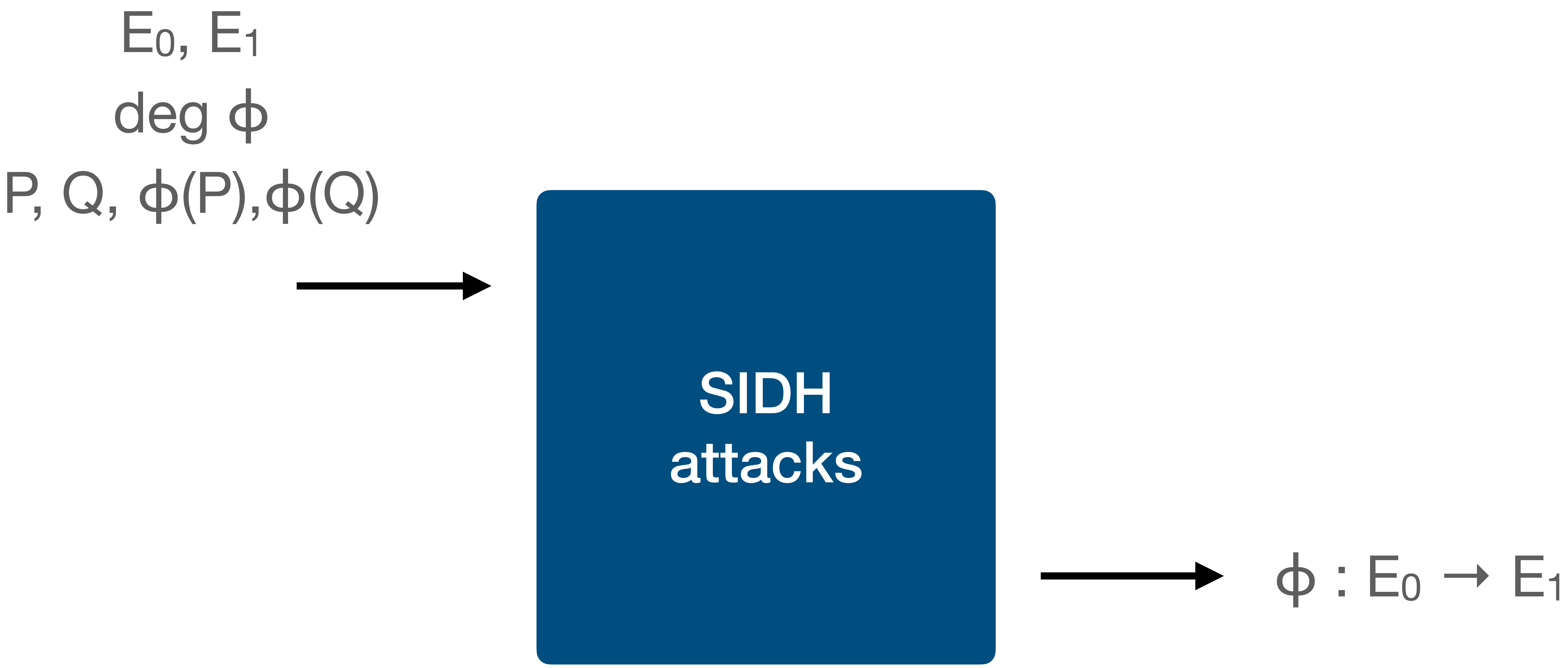
Variants of SIDH including M-SIDH, MD-SIDH, binSIDH, terSIDH, etc.

The SIDH protocol

$$\begin{tikzcd}[column sep=huge, row sep=huge]
\overset{\substack{P,\, Q \\ P,\, Q}}{\bullet} \arrow[r, "\phi", "\ker \phi = < [\alpha]P + [\beta]Q>"'] \arrow[d, "\psi"', "\substack{\ker \psi = \\ < [\gamma]P + [\delta]Q>}"] & \overset{\phi(P),\, \phi(Q)}{\bullet} \arrow[d, "\psi'", "\substack{\ker \psi = \\ < [\gamma]\phi(P) + [\delta]\phi(Q) >}"'] \\
\underset{\psi(P),\, \psi(Q)}{\bullet} \arrow[r, "\ker \phi' = < [\alpha]\psi(P) + [\beta]\psi(Q) >", "\phi'"'] & \bullet
\end{tikzcd}$$

$$\ker \psi' = \phi(\ker \psi) \qquad \ker \phi' = \psi(\ker \phi)$$

The attacks on SIDH



E_0, E_1

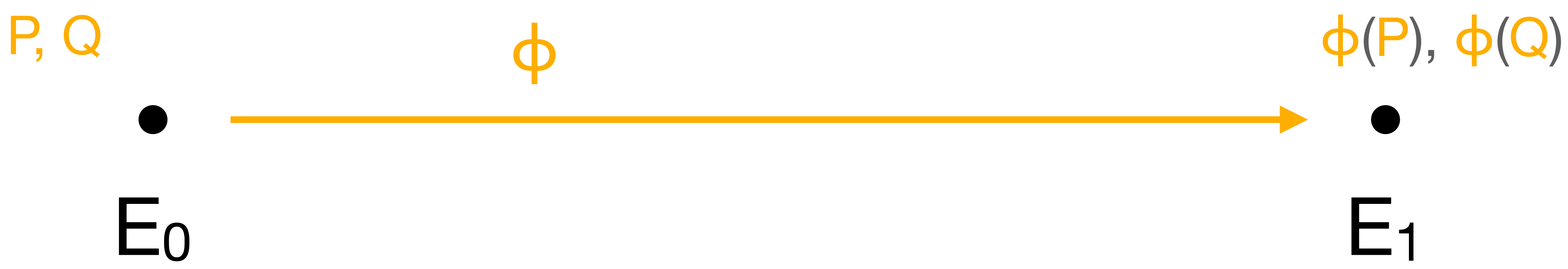
$\deg \phi$

$P, Q, \phi(P), \phi(Q)$

SIDH attacks

$\phi : E_0 \to E_1$

Higher-dimensional representations



Higher-dimensional representation

- E_0, E_1
- P, Q and $[\alpha]\phi(P)$, $[\beta]\phi(Q)$
- deg ϕ
- α, β

of the form $q(2^a - q)$

How to push HD representations

$$\begin{tikzcd}
\substack{P_0\\ Q_0} \arrow[r, "\phi"] \arrow[d, "\psi"'] & \substack{P_A\\ Q_A} = \substack{[\alpha]\ \phi(P_0)\\ {[\delta]\ \phi(Q_0)}} \arrow[d, "\psi'"] \\
\substack{P_B\\ Q_B} = \substack{[\beta]\ \psi(P_0)\\ {[\beta^{-1}]\psi(Q_0)}} \arrow[r, "\phi'"] & \substack{P_{AB}\\ Q_{AB}} = \substack{[\beta]\ \psi'(P_A)\\ {[\beta^{-1}]\psi'(Q_A)}}
\end{tikzcd}$$

$$\phi'\begin{pmatrix}P_B\\ Q_B\end{pmatrix} = \begin{matrix}[\beta]\\ {[\beta^{-1}]}\end{matrix}\phi'\psi\begin{pmatrix}P_0\\ Q_0\end{pmatrix} = \begin{matrix}[\beta]\\ {[\beta^{-1}]}\end{matrix}\psi'\phi\begin{pmatrix}P_0\\ Q_0\end{pmatrix} = \begin{matrix}[\delta^{-1}\beta]\\ {[\alpha^{-1}\beta^{-1}]}\end{matrix}\psi'\begin{pmatrix}P_A\\ Q_A\end{pmatrix} = \begin{matrix}[\delta^{-1}]P_{AB}\\ {[\alpha^{-1}]Q_{AB}}\end{matrix}$$

How to get a shared secret

$$\begin{tikzcd} \begin{matrix} P_0 \\ Q_0 \end{matrix} \; X_0 \arrow[r, "\phi"] \arrow[d, "\psi"'] & \bullet \arrow[d, "\psi'"] \\ \bullet \arrow[r, "\phi'"] & \bullet \end{tikzcd}$$

$$\begin{matrix} P_A \\ Q_A \end{matrix} = \begin{matrix} [\alpha]\ \phi(P_0) \\ [\alpha^{-1}]\phi(Q_0) \end{matrix} \qquad X_A = [\gamma]\phi(X_0)$$

$$\begin{matrix} P_B \\ Q_B \end{matrix} = \begin{matrix} [\beta]\ \psi(P_0) \\ [\beta^{-1}]\psi(Q_0) \end{matrix}$$

$$X_B = [\delta]\psi(X_0)$$

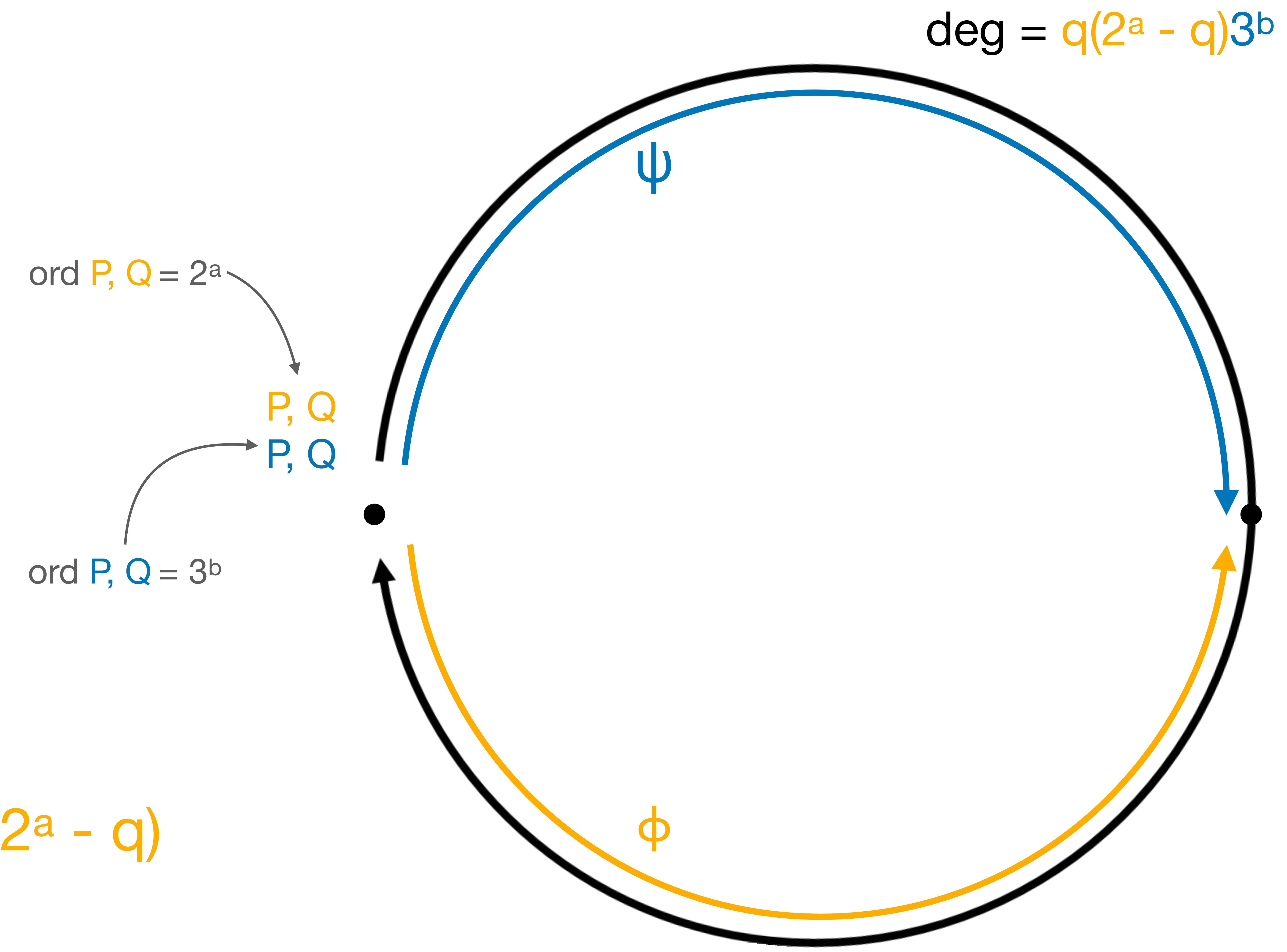
$$\begin{matrix} P_{AB} \\ Q_{AB} \end{matrix} = \begin{matrix} [\beta]\ \psi'(P_A) \\ [\beta^{-1}]\psi'(Q_A) \end{matrix}$$

$$\boxed{X_{AB} = [\delta]\psi'(X_A) = [\gamma]\phi'(X_B)}$$

The **POKE** PKE

Key generation

1. Sample q
2. Generate endomorphism
3. Compute ψ
4. Compute $[3^{-b}]\psi(P)$, $[3^{-b}]\psi(Q)$
5. Obtain a repr. of ϕ of deg $q(2^a - q)$



The POKE PKE

$\operatorname{ord} P, Q = 2^a$

$\operatorname{ord} P, Q = 3^b$

$\operatorname{ord} X = x$

P, Q
P, Q
X

$P_A = [\alpha]\phi(P), Q_A = [\alpha']\phi(Q)$
$P_A = [\beta]\phi(P), Q_A = [\beta]\phi(Q)$
$X_A = [\gamma]\phi(X)$

$$\begin{tikzcd}
\bullet \arrow[r, "\phi", "\deg\phi = q(2^a - q)"'] \arrow[d, "\psi"', "\ker \psi = \langle P + [r]Q \rangle"] & \bullet \arrow[d, "\psi'"', "\ker \psi' = \langle P_A + [r]Q_A \rangle"] \\
\bullet \arrow[r, "\phi'"'] & \bullet
\end{tikzcd}$$

$[\delta]\psi(P), [\delta']\psi(Q)$
$X_B = [\eta]\psi(X)$

$[\delta]\psi'(P_A), [\delta']\psi'(Q_A)$

$$\boxed{X_{AB} = [\delta]\psi'(X_A) = [\gamma]\phi(X_B)}$$

Security

can we recover an isogeny of secret degree given its action on large torsion?

ord $P, Q = 2^a$

ord $P, Q = 3^b$

ord $X = x$

P, Q

P, Q

X

$P_A = [\alpha]\phi(P)$, $Q_A = [\alpha']\phi(Q)$

$P_A = [\beta]\phi(P)$, $Q_A = [\beta]\phi(Q)$

$X_A = [\gamma]\phi(X)$

$$\begin{tikzcd}
\bullet \arrow[r, "\phi", "\deg\phi = q(2^a - q)"'] \arrow[d, "\psi"'] & \bullet \arrow[d, "\psi'"'] \\
\bullet \arrow[r, "\phi'"'] & \bullet
\end{tikzcd}$$

ker ψ = $< P + [r]Q>$

ker ψ' = $< P_A + [r]Q_A >$

$[\delta]\psi(P)$, $[\delta']\psi(Q)$

$X_B = [\eta]\psi(X)$

$[\delta]\psi'(P_A)$, $[\delta']\psi'(Q_A)$

$X_{AB} = [\delta]\psi'(X_A) = [\gamma]\phi(X_B)$

Results

Parameters

- 2^{λ} : order of torsion points for HD repr
- $3^b \approx 2^{2\lambda}$: degree of smooth isogenies
- $x \approx 2^{\lambda/2}$: order of X

$$\Bigg\} \quad p = 2^a 3^b f - 1 \quad \approx 2^{3\lambda} \rightarrow 2^{2\lambda}$$

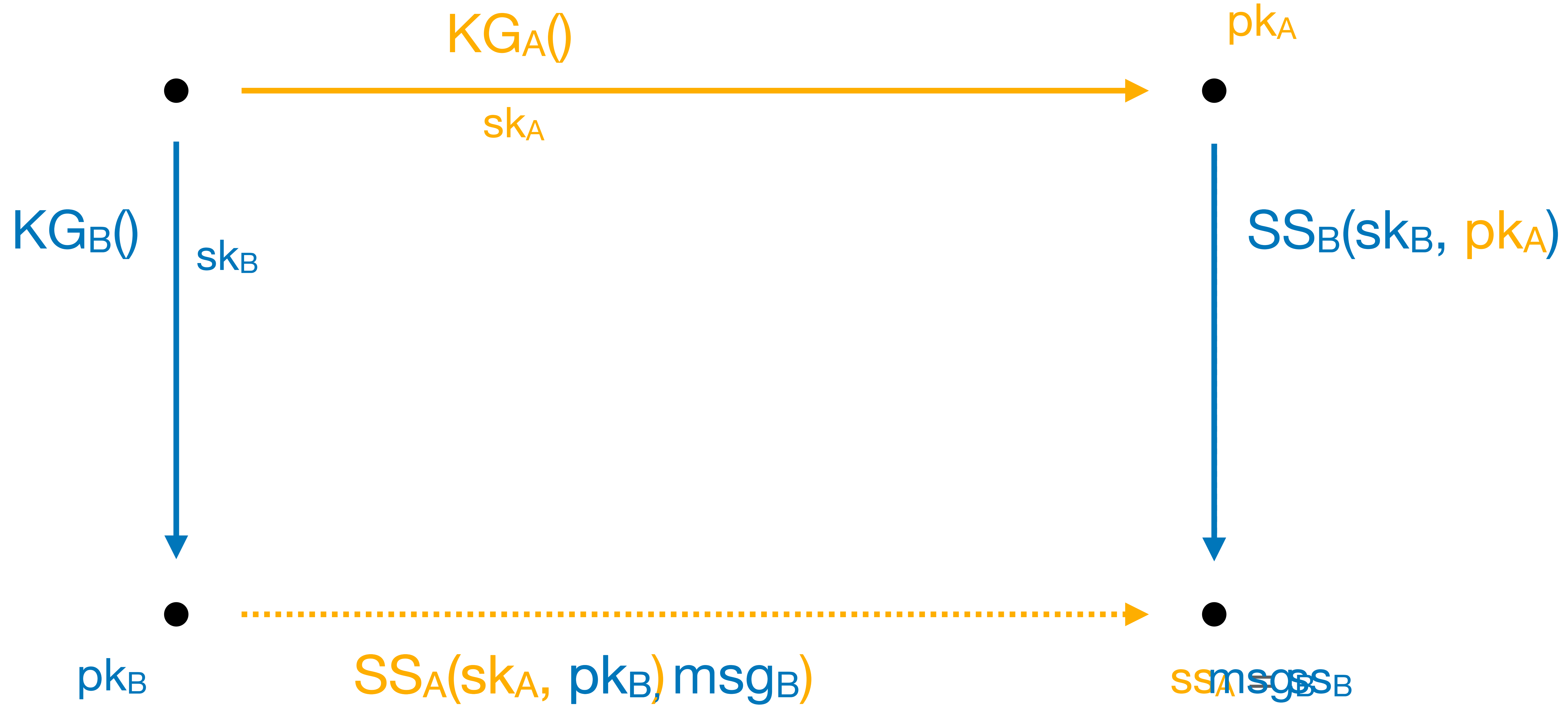
with x | p-1

	Size (bytes)		Time (ms)		
λ	$\lvert \mathsf{pk_{cmp}} \rvert$	$\lvert \mathsf{ct_{cmp}} \rvert$	KeyGen	Encrypt	Decrypt
128	272	384	496	110	190
192	408	576	840	201	382
256	544	768	1552	342	657

A non-interactive$^{\text{ish}}$ key exchange

~~Non-interactive key exchanges~~ Split KEMs

Proposed by Brendel, Fischlin, Günther, Janson, and Stebila



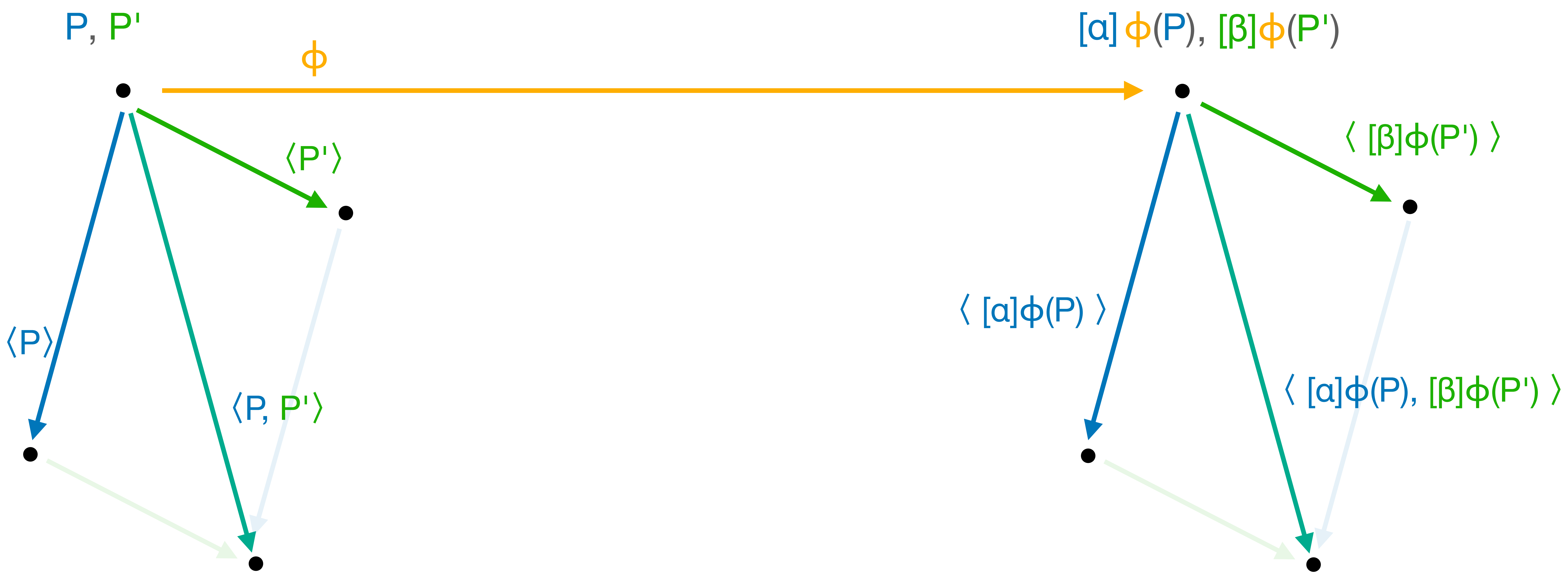
A split KEM?

$$\begin{tikzcd}
\begin{array}{c} P, Q \\ P, Q \\ X \end{array} \bullet \arrow[r, "\phi", "\deg\phi = q(2^a - q)"'] \arrow[d, "\psi"', "\begin{array}{l}\ker \psi = \\ < P + [r]Q> \end{array}"] & \bullet \begin{array}{c} P_A = [\alpha]\phi(P),\ Q_A = [\alpha^{-1}]\phi(Q) \\ P_A = [\beta]\phi(P),\ Q_A = [\beta]\phi(Q) \\ X_A = [\gamma]\phi(X) \end{array} \arrow[d, "\psi'"', "\begin{array}{l}\ker \psi' = \\ < P_A + [r]Q_A > \end{array}"] \\
\begin{array}{c} [\delta]\psi(P),\ [\delta^{-1}]\psi(Q) \\ X_B = [\eta]\psi(X) \end{array} \bullet \arrow[r, "\phi'"'] & \bullet \begin{array}{c} [\delta]\psi'(P_A),\ [\delta^{-1}]\psi'(Q_A) \\ \\ X_{AB} = [\delta]\psi'(X_A) = [\gamma]\phi(X_B) \end{array}
\end{tikzcd}$$

A simple attack

$\ker \phi' = \psi(\ker \phi)$ ⇒ $P \in \ker \phi \Rightarrow \psi(P) \in \ker \phi'$ ⇒ recover $[\alpha]\psi(P)$

uniSIDH isogenies



parameters

R

$\operatorname{ord} R = B = p_1 \cdot p_2 \cdot \ldots \cdot p_\lambda$

secret key

B' | B

$B' = p_2 \cdot p_3 \cdot \ldots \cdot p_{122}$

isogeny

ker = < [B/B'] R>

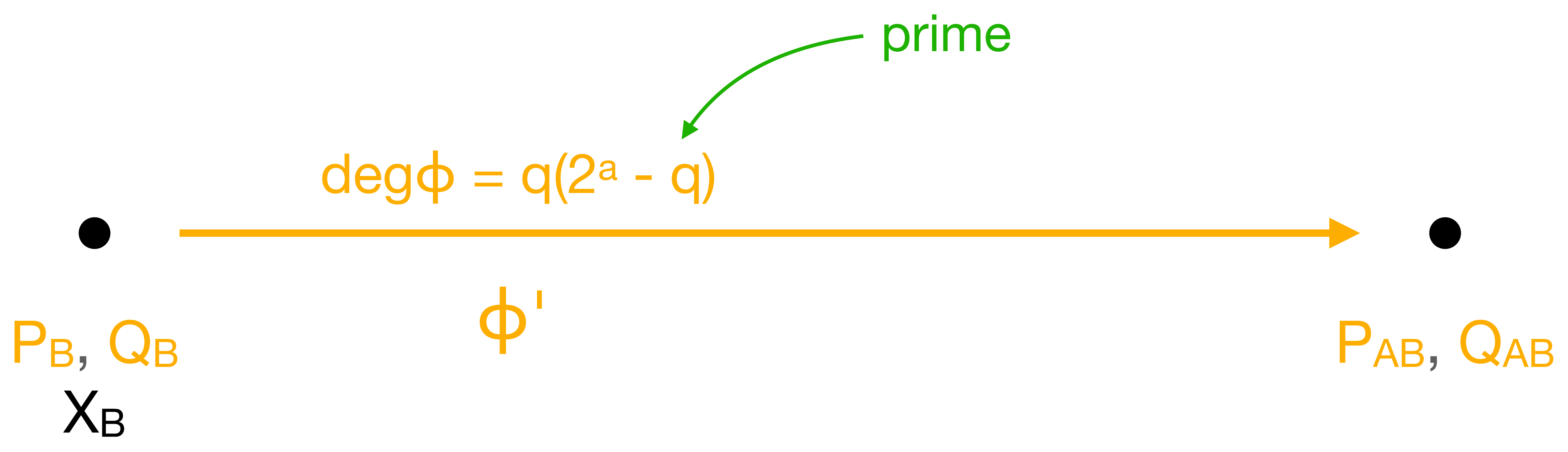
A split KEM?

$$\begin{tikzcd}[column sep=huge, row sep=huge]
\begin{array}{c} P, Q \\ R, X \end{array} \bullet \arrow[r, "\phi", "\deg\phi = q(2^a - q)"'] \arrow[d, "\psi"', "\begin{array}{l} \ker \psi = \\ < [B/B']R > \end{array}"] & \bullet \begin{array}{c} P_A = [\alpha]\phi(P),\ P_A = [\alpha']\phi(Q) \\ R_A = [\beta]\phi(R),\ X_A = [\gamma]\phi(X) \end{array} \arrow[d, "\psi'"', "\begin{array}{l} \ker \psi' = \\ < [B/B']R_A > \end{array}"] \\
\bullet \begin{array}{c} [\delta]\psi(P),\ [\delta']\psi(Q) \\ X_B = [\eta]\psi(X) \end{array} \arrow[r, "\phi'"'] & \bullet \ [\delta]\psi'(P_A),\ [\delta^{-1}]\psi'(Q_A)
\end{tikzcd}$$

$$X_{AB} = [\eta]\psi'(X_A) = [\gamma]\phi(X_B)$$

secure against active attacks?

Active attacks countermeasures – Alice



prime

$\deg\phi = q(2^a - q)$

ϕ'

P_B, Q_B

X_B

P_{AB}, Q_{AB}

1. Scale P_{AB}, Q_{AB} by $[\alpha^{-1}]$ and $[\alpha'^{-1}]$
2. Compute HD repr. of ϕ'
3. Obtain $X_{AB} = \phi'(X_B)$
4. Check $P_{AB} = [\cdot]\phi'(P_A)$ and $Q_{AB} = [\cdot]\phi'(Q_A)$

Active attacks countermeasures – Bob

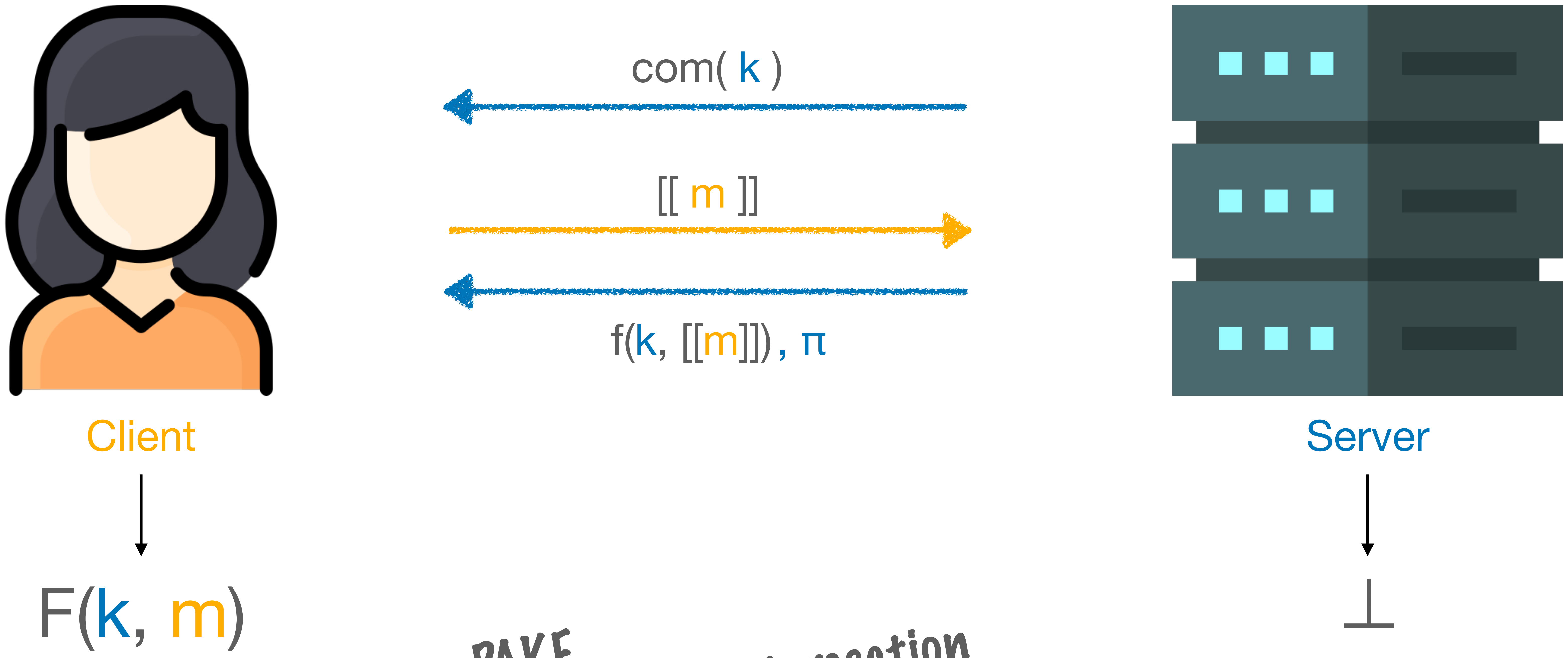
repeat multiple times

$$\begin{tikzcd}
\bullet \arrow[rr, "\phi'_{eph}"] & & X_{AB} = [\delta]\psi'_{eph}(X_A) \\
P, Q \quad R, X \arrow[u, "\psi_{eph}"] \arrow[rr, "\phi", "\deg\phi = q(2^a - q)"'] \arrow[d, "\psi"', "\ker\psi = < [B/B']R >"] & & P_A = [\alpha]\phi(P),\ P_A = [\alpha^{-1}]\phi(Q) \quad R_A = [\beta]\phi(R),\ X_A = [\gamma]\phi(X) \arrow[u, "\psi'_{eph}"'] \arrow[d, "\psi'"', "\ker\psi' = < [B/B']R_A >"] \\
[\delta]\psi(P), [\delta^{-1}]\psi(Q) \quad X_B = [\eta]\psi(X) \arrow[rr, "\phi'"'] & & \boxed{X_{AB} = [\eta]\psi'(X_A) = [\gamma]\phi(X_B)}
\end{tikzcd}$$

(Symm.) Encrypted under $sk = X_{AB1} \,||\, X_{AB2} \,||\, \ldots \,||\, X_{ABt}$

An oblivious PRF

Oblivious PRFs



- PAKE
- Private-set intersection
- Password checking
- Privacy pass
- ....

A POKE OPRF

$X_{AB} = [\delta]\psi'_{eph}(X_A)$

repeat multiple times

ψ_{eph}

ψ'_{eph}

$P_A = [\alpha]\phi(P)$, $P_A = [\alpha']\phi(Q)$

$R_A = [\beta]\phi(R)$, $X_A = [\gamma]\phi(X)$

P, Q

R, X

ϕ_m

$\deg\phi_m = q$

ϕ_b

$\deg\phi_b = 2^a - q$

ψ

$\ker \psi = \langle [B/B']R \rangle$

ψ'

$\ker \psi' = \langle [B/B']R_A \rangle$

(Symm.) encrypted under

sk = $X_{AB1} \,||\, X_{AB2} \,||\, \dots \,||\, X_{ABt}$

$[\delta]\psi(P)$, $[\delta']\psi(Q)$

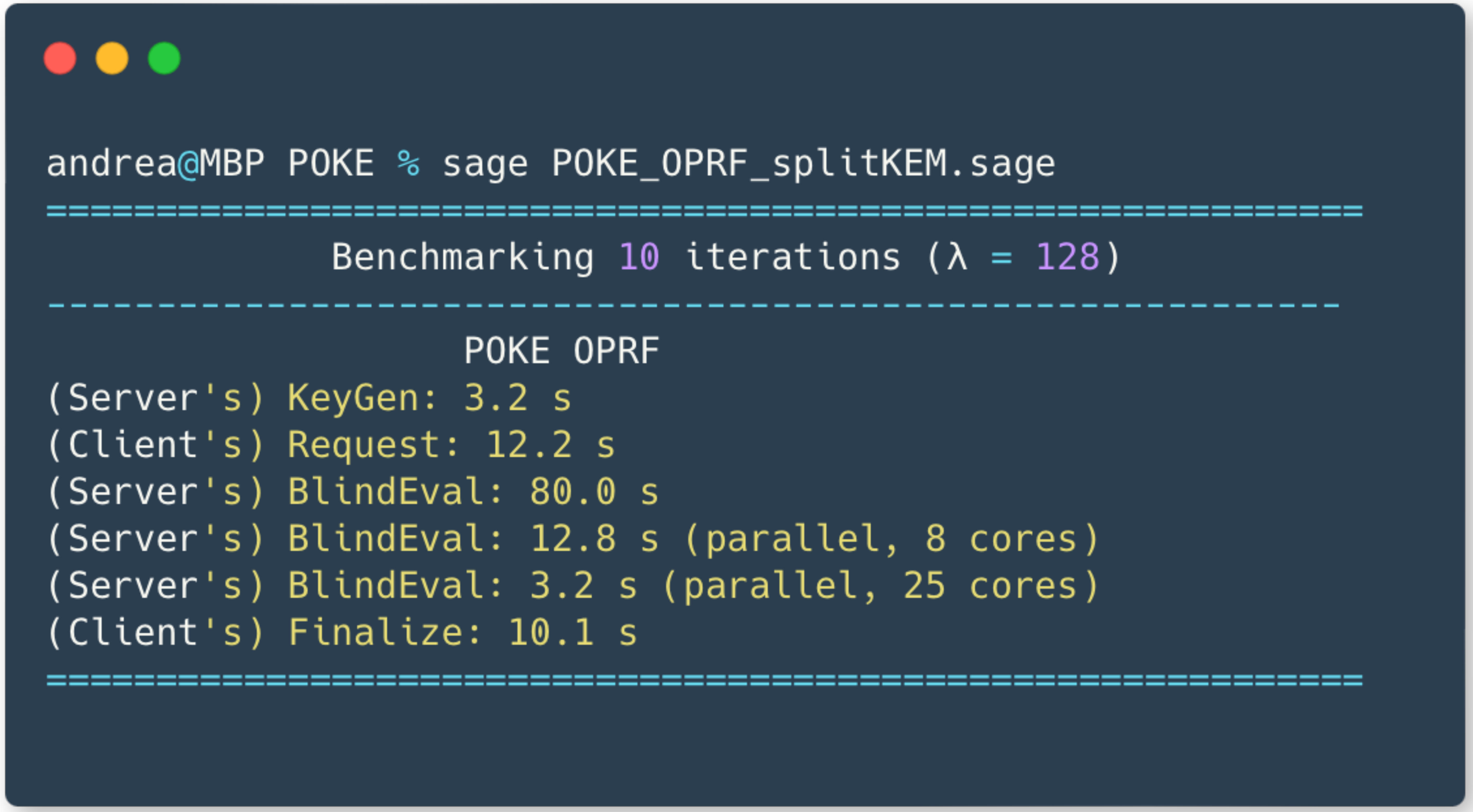
$[\delta]\psi'(P_A)$, $[\delta']\psi'(Q_A)$

ϕ'_m

ϕ'_b

Results

$p = 2^a B f - 1$ ≈ 1500 bit (for $\lambda = 128$) ⇒ total bandwidth: < 29 kB



```
andrea@MBP POKE % sage POKE_OPRF_splitKEM.sage
============================================================
             Benchmarking 10 iterations (λ = 128)
-----------------------------------------------------------
                        POKE OPRF
(Server's) KeyGen: 3.2 s
(Client's) Request: 12.2 s
(Server's) BlindEval: 80.0 s
(Server's) BlindEval: 12.8 s (parallel, 8 cores)
(Server's) BlindEval: 3.2 s (parallel, 25 cores)
(Client's) Finalize: 10.1 s
============================================================
```

Conclusion

1 New framework for SIDH-like diagrams with high-dimensional representations

2 A new PKE, both efficient and compact

3 Many more applications, including split KEMs and OPRFs