How (not) to Build Identity-Based Encryption from Isogenies

Elif Özbay Gürler[1] and Patrick Struck[2]

[1]Technische Universität Darmstadt, Germany
[2]Universität Konstanz, Germany

SAC 2025

identity-based encryption [Sha84]

$\mathsf{KGen}(1^n) \rightarrow (mpk, msk)$

$\mathsf{Enc}(mpk, id, m) \rightarrow c$

$\mathsf{Ext}(msk, id) \rightarrow sk$

$\mathsf{Dec}(sk, c) \rightarrow m$

(mpk, msk)

id_A

$||$

alice@ibe.test

id_B

$||$

bob@ibe.test

[Sha84] Shamir — CRYPTO 1984
Icons created by juicy_fish — Flaticon

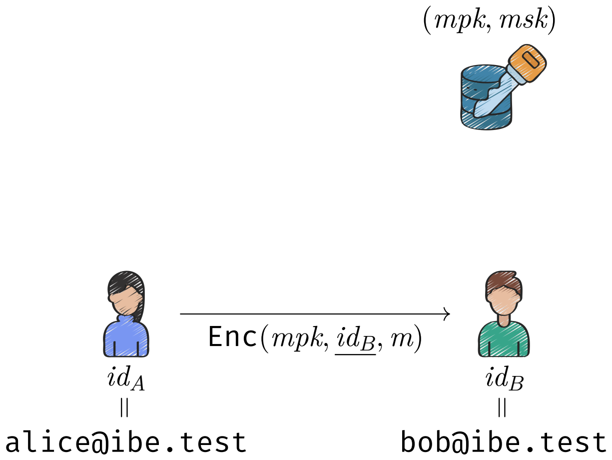
identity-based encryption [Sha84]

$\mathsf{KGen}(1^n) \to (mpk, msk)$

$\mathsf{Enc}(mpk, id, m) \to c$

$\mathsf{Ext}(msk, id) \to sk$

$\mathsf{Dec}(sk, c) \to m$



[Sha84] Shamir — CRYPTO 1984
Icons created by juicy_fish — Flaticon

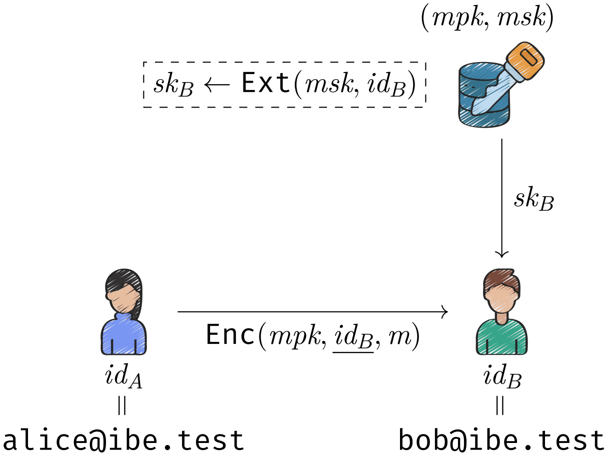
identity-based encryption [Sha84]

$\mathsf{KGen}(1^n) \to (mpk, msk)$

$\mathsf{Enc}(mpk, id, m) \to c$

$\mathsf{Ext}(msk, id) \to sk$

$\mathsf{Dec}(sk, c) \to m$



[Sha84] Shamir — CRYPTO 1984
Icons created by juicy_fish — Flaticon

motivation

Post-quantum IBE

- Lattices [GPV08, ...]
- Codes [GHPT17] (broken)
- Isogenies? [this work]

Post-quantum IBE

- Lattices [GPV08, ...]
- Codes [GHPT17] (broken)
- Isogenies? [this work]

Why isogenies?

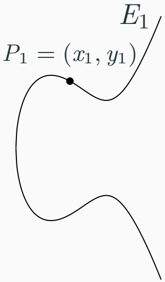
- Small keys and ciphertexts
- Lower-bound for FS signature sizes [BGZ23]
- IBE $\implies$ short signatures [BF01]

[BGZ23] Boneh, Guan, Zhandry — EUROCRYPT 2023
[BF01] Boneh, Franklin — CRYPTO 2001

isogeny background

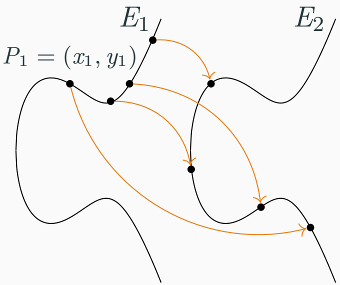
Supersingular Elliptic Curve

An algebraic curve $E \colon y^2 = x^3 + Ax + B$ over $\mathbb{F}_q$ s.t. $E(\mathbb{F}_q) = q + 1$



Supersingular Elliptic Curve

An algebraic curve $E\colon y^2 = x^3 + Ax + B$ over $\mathbb{F}_q$ s.t. $E(\mathbb{F}_q) = q + 1$

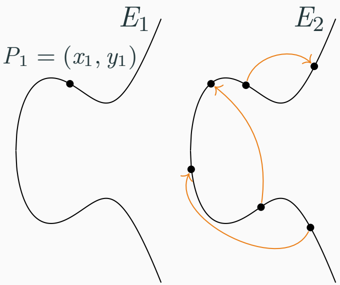


Isogeny

A rational map $\varphi\colon E_1 \to E_2$ with the dual $\hat{\varphi}\colon E_2 \to E_1$

Supersingular Elliptic Curve

An algebraic curve $E\colon y^2 = x^3 + Ax + B$ over $\mathbb{F}_q$ s.t. $E(\mathbb{F}_q) = q + 1$



Isogeny

A rational map $\varphi\colon E_1 \to E_2$ with the dual $\hat{\varphi}\colon E_2 \to E_1$

Endomorphism

An isogeny $\theta\colon E \to E$

Endomorphism Ring

$\mathrm{End}(E) = \{\theta\colon E \to E\}$

hard problems

l-Isogeny Path Problem

Given two supersingular elliptic curves E_1 and E_2,

hard problems

l-Isogeny Path Problem

Given two supersingular elliptic curves E_1 and E_2, compute an l-isogeny path $\varphi\colon E_1 \to E_2$.

hard problems

l-Isogeny Path Problem

Given two supersingular elliptic curves E_1 and E_2, compute an l-isogeny path $\varphi \colon E_1 \to E_2$.

Endomorphism Ring Problem

Given a supersingular elliptic curve E,

l-Isogeny Path Problem

Given two supersingular elliptic curves E_1 and E_2, compute an l-isogeny path $\varphi\colon E_1 \to E_2$.

Endomorphism Ring Problem

Given a supersingular elliptic curve E, compute $\mathrm{End}(E)$.

l-Isogeny Path Problem

Given two supersingular elliptic curves E_1 and E_2, compute an l-isogeny path $\varphi\colon E_1 \to E_2$.

$\downarrow$

Endomorphism Ring Problem

Given a supersingular elliptic curve E, compute $\mathrm{End}(E)$.

$E_1^{\checkmark}$

E_2^{X}

hard problems

l-Isogeny Path Problem

Given two supersingular elliptic curves E_1 and E_2, compute an l-isogeny path $\varphi \colon E_1 \to E_2$.

$$\downarrow$$

Endomorphism Ring Problem

Given a supersingular elliptic curve E, compute $\mathrm{End}(E)$.

$$\begin{tikzcd} E_1^{\checkmark} \arrow[d, bend left, "\varphi"] \\ E_2^{X} \end{tikzcd}$$

hard problems

l-Isogeny Path Problem

Given two supersingular elliptic curves E_1 and E_2, compute an l-isogeny path $\varphi\colon E_1 \to E_2$.

$\downarrow$

Endomorphism Ring Problem

Given a supersingular elliptic curve E, compute $\mathrm{End}(E)$.

$$\begin{tikzcd} E_1^{\checkmark} \arrow[d, "\varphi"] \\ E_2^{\checkmark} \end{tikzcd}$$

l-Isogeny Path Problem

Given two supersingular elliptic curves E_1 and E_2, compute an l-isogeny path $\varphi\colon E_1 \to E_2$.

$\downarrow \quad \uparrow$

Endomorphism Ring Problem

Given a supersingular elliptic curve E, compute $\mathrm{End}(E)$.

$E_1^{\checkmark}$

$E_2^{\checkmark}$

hard problems

l-Isogeny Path Problem

Given two supersingular elliptic curves E_1 and E_2, compute an l-isogeny path $\varphi\colon E_1 \to E_2$.

$$\downarrow \qquad \uparrow$$

Endomorphism Ring Problem

Given a supersingular elliptic curve E, compute $\mathrm{End}(E)$.

$$\begin{tikzcd} E_1^{\checkmark} \arrow[d, bend left, "\varphi"] \\ E_2^{\checkmark} \end{tikzcd}$$

Prevalent settings for isogeny-based PKE

- $pk = E_A$ and $sk = \varphi\colon E_0 \to E_A$
- $pk = E_A$ and $sk = \mathsf{End}(E_A)$

curve generation

SECUER = Supersingular Elliptic Curves of Unknown Endomorphism Ring [BCC+23]

$$E_A^{\circ} = \mathsf{H}^{\mathsf{UE}}_{\mathcal{E}ll}(x)$$

[BCC+23] Basso, Codogni, Connolly, De Feo, Fouotsa, Lido, Morrison, Panny, Patranabis, Wesolowski — EUROCRYPT 2023
[CGL09] Charles, Lauter, Goren — Journal of Cryptology 2009

curve generation

SECUER = Supersingular Elliptic Curves of Unknown Endomorphism Ring [BCC+23]

$$E_A^{\circ} = \mathsf{H}_{\mathcal{E}ll}^{\mathsf{UE}}(x)$$

SECKER = Supersingular Elliptic Curves of Known Endomorphism Ring [this work]

$$E_A^{\bullet} = \mathsf{H}_{\mathcal{E}ll}^{\mathsf{KE}}(x)$$

[BCC+23] Basso, Codogni, Connolly, De Feo, Fouotsa, Lido, Morrison, Panny, Patranabis, Wesolowski — EUROCRYPT 2023
[CGL09] Charles, Lauter, Goren — Journal of Cryptology 2009

curve generation

SECUER = Supersingular Elliptic Curves of Unknown Endomorphism Ring [BCC+23]

$$E_A^{\circ} = \mathsf{H}_{\mathcal{E}ll}^{\mathsf{UE}}(x)$$

SECKER = Supersingular Elliptic Curves of Known Endomorphism Ring [this work]

$$E_A^{\bullet} = \mathsf{H}_{\mathcal{E}ll}^{\mathsf{KE}}(x)$$

CGL = Random isogeny walks [CGL09]

$$E_0^{\circ} \xrightarrow{\varphi_x} E_A^{\circ} = \mathsf{H}_{\mathcal{E}ll}^{\mathsf{CGL}}(E_0, x)$$

[BCC+23] Basso, Codogni, Connolly, De Feo, Fouotsa, Lido, Morrison, Panny, Patranabis, Wesolowski — EUROCRYPT 2023
[CGL09] Charles, Lauter, Goren — Journal of Cryptology 2009

how not to build?

a new definition

Canonical IBE

IKD (Identity Key Derivation)
$\mathsf{KGen}(1^n) \to (mpk, msk)$
$\mathsf{Ext\text{-}pk}(mpk, id) \to pk$
$\mathsf{Ext\text{-}sk}(msk, id) \to sk$

PKE
$\mathsf{KGen}(1^n) \to (pk, sk)$
$\mathsf{Enc}(pk, m) \to c$
$\mathsf{Dec}(sk, c) \to m$

a new definition

Canonical IBE

IKD (Identity Key Derivation)
$\mathsf{KGen}(1^n) \to (mpk, msk)$
$\mathsf{Ext\text{-}pk}(mpk, id) \to pk$
$\mathsf{Ext\text{-}sk}(msk, id) \to sk$

compatible

PKE
$\mathsf{KGen}(1^n) \to (pk, sk)$
$\mathsf{Enc}(pk, m) \to c$
$\mathsf{Dec}(sk, c) \to m$

a new definition

Canonical IBE

IKD (Identity Key Derivation)
$\mathsf{KGen}(1^n) \to (mpk, msk)$
$\mathsf{Ext\text{-}pk}(mpk, id) \to pk$
$\mathsf{Ext\text{-}sk}(msk, id) \to sk$

compatible

PKE
$\mathsf{KGen}(1^n) \to (pk, sk)$
$\mathsf{Enc}(pk, m) \to c$
$\mathsf{Dec}(sk, c) \to m$

$\parallel$

IBE

Canonical IBE

IKD (Identity Key Derivation)
$\mathsf{KGen}(1^n) \to (mpk, msk)$
$\mathsf{Ext\text{-}pk}(mpk, id) \to pk$
$\mathsf{Ext\text{-}sk}(msk, id) \to sk$

compatible

PKE
$\mathsf{KGen}(1^n) \to (pk, sk)$
$\mathsf{Enc}(pk, m) \to c$
$\mathsf{Dec}(sk, c) \to m$

$\|$

IBE

sk = isogeny

$$\begin{tikzcd} E_0 \arrow[r, dashed, "\varphi_{sk_A}"] \arrow[dr, dashed, "\varphi_{sk_B}"'] & E_{1,A} \\ & E_{1,B} \end{tikzcd}$$

domain curve fixed

$$\begin{tikzcd} E_{0,A} \arrow[r, dashed, "\varphi_{sk_A}"] & E_{1,A} \\ E_{0,B} \arrow[r, dashed, "\varphi_{sk_B}"] & E_{1,B} \end{tikzcd}$$

no curve fixed

sk = isogeny

$$\begin{tikzcd} E_0 \arrow[r, dashed, "\varphi_{sk_A}"] \arrow[dr, dashed, "\varphi_{sk_B}"'] & E_{1,A} \\ & E_{1,B} \end{tikzcd}$$

domain curve fixed

$$\begin{tikzcd} E_{0,A} \arrow[r, dashed, "\varphi_{sk_A}"] & E_{1,A} \\ E_{0,B} \arrow[r, dashed, "\varphi_{sk_B}"] & E_{1,B} \end{tikzcd}$$

no curve fixed

SECUER public key

$\mathtt{IKD}_{1.1}$

$\mathtt{KGen}(1^n) \to (mpk, msk)$
$\mathtt{Ext\text{-}sk}(msk, id) \to \varphi_{sk}$
$\mathtt{Ext\text{-}pk}(mpk, id) \to E^{\circ}_{1,id}$

Let the public key be a SECUER s.t.

$$E^{\circ}_{1,id} \leftarrow \mathsf{H}^{\mathsf{UE}}_{\mathcal{E}ll}(mpk, id).$$

$E_0^{\bullet}$ $E^{\circ}_{1,A}$

SECUER public key

$\mathsf{IKD}_{1.1}$

$\mathsf{KGen}(1^n) \to (mpk, msk)$
$\mathsf{Ext\text{-}sk}(msk, id) \to \varphi_{sk}$
$\mathsf{Ext\text{-}pk}(mpk, id) \to E^{\circ}_{1,id}$

Infeasible
Ext-sk must solve the isogeny problem.

Let the public key be a SECUER s.t.

$$E^{\circ}_{1,id} \leftarrow \mathsf{H}^{\mathsf{UE}}_{\mathcal{E}ll}(mpk, id).$$

$$E_0^{\bullet} \xrightarrow{\varphi_{sk_A}} E^{\circ}_{1,A}$$

SECKER public key

$\mathsf{IKD}_{1.2}$

$\mathsf{KGen}(1^n) \to (mpk, msk)$

$\mathsf{Ext\text{-}sk}(msk, id) \to \varphi_{sk}$

$\mathsf{Ext\text{-}pk}(mpk, id) \to E^{\bullet}_{1,id}$

Let the public key be a SECKER s.t.

$$E^{\bullet}_{1,id} \leftarrow \mathsf{H}^{\mathsf{KE}}_{\mathcal{E}ll}(mpk, id).$$

$E^{\bullet}_{1,A}$

$E^{\bullet}_0$ $E^{\bullet}_{1,B}$

SECKER public key

$\mathsf{IKD}_{1.2}$

$\mathsf{KGen}(1^n) \to (mpk, msk)$

$\mathsf{Ext\text{-}sk}(msk, id) \to \varphi_{sk}$

$\mathsf{Ext\text{-}pk}(mpk, id) \to E^{\bullet}_{1,id}$

Let the public key be a SECKER s.t.

$$E^{\bullet}_{1,id} \leftarrow \mathsf{H}^{\mathsf{KE}}_{\mathcal{E}ll}(mpk, id).$$

$$\begin{tikzcd}
 & E^{\bullet}_{1,A} \\
E^{\LEFTcircle}_{0} \arrow[ur, dashed, "\varphi_{sk_A}"] \arrow[r, dashed, "\varphi_{sk_B}"] & E^{\bullet}_{1,B}
\end{tikzcd}$$

SECKER public key

$\mathsf{IKD}_{1.2}$

$\mathsf{KGen}(1^n) \rightarrow (mpk, msk)$

$\mathsf{Ext\text{-}sk}(msk, id) \rightarrow \varphi_{sk}$

$\mathsf{Ext\text{-}pk}(mpk, id) \rightarrow E^{\bullet}_{1,id}$

Let the public key be a SECKER s.t.

$$E^{\bullet}_{1,id} \leftarrow \mathsf{H}^{\mathsf{KE}}_{\mathcal{E}ll}(mpk, id).$$

$$\begin{tikzcd}
 & E^{\bullet}_{1,A} \arrow[d, "\lambda"'] \\
E^{\LEFTcircle}_0 \arrow[ur, dashed, "\varphi_{sk_A}"] \arrow[r, dashed, "\varphi_{sk_B}"] & E^{\bullet}_{1,B}
\end{tikzcd}$$

SECKER public key

$\mathsf{IKD}_{1.2}$

$\mathsf{KGen}(1^n) \to (mpk, msk)$
$\mathsf{Ext\text{-}sk}(msk, id) \to \varphi_{sk}$
$\mathsf{Ext\text{-}pk}(mpk, id) \to E^{\bullet}_{1,id}$

Insecure

Alice learns Bob's secret key!

Let the public key be a SECKER s.t.

$$E^{\bullet}_{1,id} \leftarrow \mathsf{H}^{\mathsf{KE}}_{\mathcal{E}ll}(mpk, id).$$

$$\begin{tikzcd}
 & E^{\bullet}_{1,A} \arrow[d, "\lambda"] \\
E^{\LEFTcircle}_{0} \arrow[ur, "\varphi_{sk_A}"] \arrow[r, dashed, "\varphi_{sk_B}"] & E^{\bullet}_{1,B}
\end{tikzcd}$$

CGL public key

$\mathsf{IKD}_{1.3}$

$\mathsf{KGen}(1^n) \rightarrow (mpk, msk)$
$\mathsf{Ext\text{-}sk}(msk, id) \rightarrow \varphi_{sk}$
$\mathsf{Ext\text{-}pk}(mpk, id) \rightarrow E^{\LEFTcircle}_{1,id}$

Let the public key be a CGL codomain s.t.

$$E^{\LEFTcircle}_{1,id} \leftarrow \mathsf{H}^{\mathsf{CGL}}_{\mathcal{E}ll}(mpk, id).$$

$$\begin{tikzcd}
 & E^{\LEFTcircle}_1 \arrow[d, "\varphi_A"'] \arrow[dd, bend left, "\varphi_B"] \\
E^{\LEFTcircle}_0 & E^{\LEFTcircle}_{1,A} \\
 & E^{\LEFTcircle}_{1,B}
\end{tikzcd}$$

CGL public key

$\mathtt{IKD}_{1.3}$

$\mathsf{KGen}(1^n) \to (mpk, msk)$
$\mathsf{Ext\text{-}sk}(msk, id) \to \varphi_{sk}$
$\mathsf{Ext\text{-}pk}(mpk, id) \to E^{\LEFTcircle}_{1,id}$

Let the public key be a CGL codomain s.t.

$$E^{\LEFTcircle}_{1,id} \leftarrow \mathsf{H}^{\mathsf{CGL}}_{\mathcal{E}ll}(mpk, id).$$

$$\begin{tikzcd}
 & E_1^{\LEFTcircle} \arrow[d, "\varphi_A"] \arrow[dd, bend left, "\varphi_B"] \\
E_0^{\LEFTcircle} \arrow[ur, dashed, "msk = \lambda"] \arrow[r, dashed, "\varphi_{sk_A}"] \arrow[dr, dashed, "\varphi_{sk_B}"'] & E_{1,A}^{\LEFTcircle} \\
 & E_{1,B}^{\LEFTcircle}
\end{tikzcd}$$

CGL public key

$\mathsf{IKD}_{1.3}$

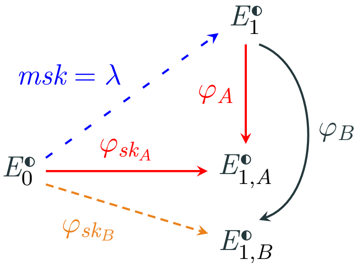
$\mathsf{KGen}(1^n) \to (mpk, msk)$
$\mathsf{Ext\text{-}sk}(msk, id) \to \varphi_{sk}$
$\mathsf{Ext\text{-}pk}(mpk, id) \to E^{\bullet}_{1,id}$

Insecure

Alice learns the master secret key!

Let the public key be a CGL codomain s.t.

$$E^{\bullet}_{1,id} \leftarrow \mathsf{H}^{\mathsf{CGL}}_{\mathcal{E}ll}(mpk, id).$$



sk = isogeny

$$\begin{tikzcd} E_0 \arrow[r, dashed, "\varphi_{sk_A}"] \arrow[dr, dashed, "\varphi_{sk_B}"'] & E_{1,A} \\ & E_{1,B} \end{tikzcd}$$

domain curve fixed

$$\begin{tikzcd} E_{0,A} \arrow[r, dashed, "\varphi_{sk_A}"] & E_{1,A} \\ E_{0,B} \arrow[r, dashed, "\varphi_{sk_B}"] & E_{1,B} \end{tikzcd}$$

no curve fixed

sk = isogeny

$$\begin{tikzcd} E_0 \arrow[r, "\varphi_{sk_A}"] \arrow[dr, "\varphi_{sk_B}"'] & E_{1,A} \\ & E_{1,B} \end{tikzcd}$$

~~domain curve fixed~~

$$\begin{tikzcd} E_{0,A} \arrow[r, dashed, "\varphi_{sk_A}"] & E_{1,A} \\ E_{0,B} \arrow[r, dashed, "\varphi_{sk_B}"] & E_{1,B} \end{tikzcd}$$

no curve fixed

SECUER public key

$\mathsf{IKD}_{2.1}$

$\mathsf{KGen}(1^n) \to (mpk, msk)$
$\mathsf{Ext\text{-}sk}(msk, id) \to \varphi_{sk}$
$\mathsf{Ext\text{-}pk}(mpk, id) \to (E^{\circ}_{0,id}, E^{\bullet}_{1,id})$

Let one public key be a SECUER s.t.

$$E^{\circ}_{0,id} \leftarrow \mathsf{H}^{\mathsf{UE}}_{\mathcal{E}ll}(mpk, id),$$

SECUER public key

$\mathtt{IKD}_{2.1}$

$\mathsf{KGen}(1^n) \to (mpk, msk)$
$\mathsf{Ext\text{-}sk}(msk, id) \to \varphi_{sk}$
$\mathsf{Ext\text{-}pk}(mpk, id) \to (E^{\circ}_{0,id}, E^{\LEFTcircle}_{1,id})$

Infeasible

Ext-sk must solve the isogeny problem.

Let one public key be a SECUER s.t.

$$E^{\circ}_{0,id} \leftarrow \mathsf{H}^{\mathsf{UE}}_{\mathcal{E}ll}(mpk, id),$$
$$E^{\circ}_{1,id} \leftarrow \mathsf{H}^{\mathsf{UE}}_{\mathcal{E}ll}(mpk, id).$$

$$E^{\circ}_{0,A} \overset{\varphi_{sk}}{\dashrightarrow} E^{\circ}_{1,A}$$

SECUER public key

$\mathtt{IKD}_{2.1}$

$\mathsf{KGen}(1^n) \to (mpk, msk)$
$\mathsf{Ext\text{-}sk}(msk, id) \to \varphi_{sk}$
$\mathsf{Ext\text{-}pk}(mpk, id) \to (E^{\circ}_{0,id}, E^{\LEFTcircle}_{1,id})$

Infeasible

Ext-sk must solve the isogeny problem.

Let one public key be a SECUER s.t.

$$E^{\circ}_{0,id} \leftarrow \mathsf{H}^{\mathsf{UE}}_{\mathcal{E}ll}(mpk, id),$$
$$E^{\bullet}_{1,id} \leftarrow \mathsf{H}^{\mathsf{KE}}_{\mathcal{E}ll}(mpk, id).$$

$$E^{\circ}_{0,A} \xrightarrow{\varphi_{sk}} E^{\bullet}_{1,A}$$

SECUER public key

$\mathsf{IKD}_{2.1}$

$\mathsf{KGen}(1^n) \to (mpk, msk)$
$\mathsf{Ext\text{-}sk}(msk, id) \to \varphi_{sk}$
$\mathsf{Ext\text{-}pk}(mpk, id) \to (E^{\circ}_{0,id}, E^{\LEFTcircle}_{1,id})$

Infeasible

Ext-sk must solve the isogeny problem.

Let one public key be a SECUER s.t.

$$E^{\circ}_{0,id} \leftarrow \mathsf{H}^{\mathsf{UE}}_{\mathcal{E}ll}(mpk, id),$$
$$E^{\LEFTcircle}_{1,id} \leftarrow \mathsf{H}^{\mathsf{CGL}}_{\mathcal{E}ll}(mpk, id).$$

$$\begin{tikzcd} & E^{\LEFTcircle}_1 \arrow[d, "\varphi_A"'] \\ E^{\circ}_{0,A} \arrow[r, dashed, "\varphi_{sk}"] & E^{\LEFTcircle}_{1,A} \end{tikzcd}$$

SECKER-CGL public keys

$\mathsf{IKD}_{2.2}$

$\mathsf{KGen}(1^n) \to (mpk, msk)$

$\mathsf{Ext\text{-}sk}(msk, id) \to \varphi_{sk}$

$\mathsf{Ext\text{-}pk}(mpk, id) \to (E^\bullet_{0,id}, E^\bullet_{1,id})$

Let both public keys be SECKERs s.t.

$$E^\bullet_{0,id} \leftarrow \mathsf{H}^{\mathsf{KE}}_{\mathcal{E}ll}(mpk, id),$$
$$E^\bullet_{1,id} \leftarrow \mathsf{H}^{\mathsf{KE}}_{\mathcal{E}ll}(mpk, id).$$

$$\begin{tikzcd} E^\bullet_{0,A} \arrow[r, dashed, "\varphi_{sk}"] & E^\bullet_{1,A} \end{tikzcd}$$

SECKER-CGL public keys

$\mathsf{IKD}_{2.2}$

$\mathsf{KGen}(1^n) \to (mpk, msk)$
$\mathsf{Ext\text{-}sk}(msk, id) \to \varphi_{sk}$
$\mathsf{Ext\text{-}pk}(mpk, id) \to (E^{\bullet}_{0,id}, E^{\bullet}_{1,id})$

Insecure

Anyone can compute the secret keys!

Let both public keys be SECKERs s.t.

$$E^{\bullet}_{0,id} \leftarrow \mathsf{H}^{\mathsf{KE}}_{\mathcal{E}ll}(mpk, id),$$
$$E^{\bullet}_{1,id} \leftarrow \mathsf{H}^{\mathsf{KE}}_{\mathcal{E}ll}(mpk, id).$$

$$E^{\bullet}_{0,A} \xrightarrow{\varphi_{sk}} E^{\bullet}_{1,A}$$

SECKER-CGL public keys

$\mathtt{IKD}_{2.2}$

$\mathsf{KGen}(1^n) \to (mpk, msk)$

$\mathsf{Ext\text{-}sk}(msk, id) \to \varphi_{sk}$

$\mathsf{Ext\text{-}pk}(mpk, id) \to (E^{\bullet}_{0,id}, E^{\LEFTcircle}_{1,id})$

Let the public keys be a SECKER/ CGL s.t.

$$E^{\bullet}_{0,id} \leftarrow \mathsf{H}^{\mathsf{KE}}_{\mathcal{E}ll}(mpk, id),$$
$$E^{\LEFTcircle}_{1,id} \leftarrow \mathsf{H}^{\mathsf{CGL}}_{\mathcal{E}ll}(mpk, id).$$

$$\begin{tikzcd}
 & E^{\LEFTcircle}_{1} \arrow[d, "\varphi_A"'] \arrow[dd, bend left, "\varphi_B"] \\
E^{\bullet}_{0,A} \arrow[r, dashed, "\varphi_{sk_A}"] & E^{\LEFTcircle}_{1,A} \\
E^{\bullet}_{0,B} \arrow[r, dashed, "\varphi_{sk_B}"] & E^{\LEFTcircle}_{1,B}
\end{tikzcd}$$

SECKER-CGL public keys

$\mathtt{IKD}_{2.2}$

$\mathsf{KGen}(1^n) \to (mpk, msk)$
$\mathsf{Ext\text{-}sk}(msk, id) \to \varphi_{sk}$
$\mathsf{Ext\text{-}pk}(mpk, id) \to (E^{\bullet}_{0,id}, E^{\LEFTcircle}_{1,id})$

Let the public keys be a SECKER/ CGL s.t.

$$E^{\bullet}_{0,id} \leftarrow \mathsf{H}^{\mathsf{KE}}_{\mathcal{E}ll}(mpk, id),$$
$$E^{\LEFTcircle}_{1,id} \leftarrow \mathsf{H}^{\mathsf{CGL}}_{\mathcal{E}ll}(mpk, id).$$

$$\begin{tikzcd}
 & E^{\LEFTcircle}_{1} \arrow[d, "\varphi_A"'] \arrow[dd, bend left, "\varphi_B"] \\
E^{\bullet}_{0,A} \arrow[r, dashed, "\varphi_{sk_A}"] \arrow[d, "\lambda_0"] & E^{\LEFTcircle}_{1,A} \arrow[d, "\lambda_1"'] \\
E^{\bullet}_{0,B} \arrow[r, dashed, "\varphi_{sk_B}"] & E^{\LEFTcircle}_{1,B}
\end{tikzcd}$$

SECKER-CGL public keys

$\mathsf{IKD}_{2.2}$

$\mathsf{KGen}(1^n) \to (mpk, msk)$
$\mathsf{Ext\text{-}sk}(msk, id) \to \varphi_{sk}$
$\mathsf{Ext\text{-}pk}(mpk, id) \to (E^{\bullet}_{0,id}, E^{\LEFTcircle}_{1,id})$

Insecure

Alice learns Bob's secret key!

Let the public keys be a SECKER/ CGL s.t.

$$E^{\bullet}_{0,id} \leftarrow \mathsf{H}^{\mathsf{KE}}_{\mathcal{E}ll}(mpk, id),$$
$$E^{\LEFTcircle}_{1,id} \leftarrow \mathsf{H}^{\mathsf{CGL}}_{\mathcal{E}ll}(mpk, id).$$

$$\begin{tikzcd}
 & E^{\LEFTcircle}_1 \arrow[d, "\varphi_A"'] \arrow[dd, bend left, "\varphi_B"] \\
E^{\bullet}_{0,A} \arrow[r, "\varphi_{sk_A}"] \arrow[d, "\lambda_0"] & E^{\LEFTcircle}_{1,A} \arrow[d, "\lambda_1"'] \\
E^{\bullet}_{0,B} \arrow[r, dashed, "\varphi_{sk_B}"] & E^{\LEFTcircle}_{1,B}
\end{tikzcd}$$

SECKER-CGL public keys

$\texttt{IKD}_{2.2}$

$\mathsf{KGen}(1^n) \to (mpk, msk)$

$\mathsf{Ext\text{-}sk}(msk, id) \to \varphi_{sk}$

$\mathsf{Ext\text{-}pk}(mpk, id) \to (E^{\LEFTcircle}_{0,id}, E^{\LEFTcircle}_{1,id})$

Let the public keys be a CGLs s.t.

$$E^{\LEFTcircle}_{0,id} \leftarrow \mathsf{H}^{\mathsf{CGL}}_{\mathcal{E}ll}(mpk, id),$$
$$E^{\LEFTcircle}_{1,id} \leftarrow \mathsf{H}^{\mathsf{CGL}}_{\mathcal{E}ll}(mpk, id).$$

$$\begin{tikzcd}
E^{\LEFTcircle}_0 \arrow[d, "\varphi_A"] \arrow[dd, bend right, "\varphi_B"'] & E^{\LEFTcircle}_1 \arrow[d, "\varphi'_A"'] \arrow[dd, bend left, "\varphi'_B"] \\
E^{\LEFTcircle}_{0,A} \arrow[r, dashed, "\varphi_{sk_A}"] & E^{\LEFTcircle}_{1,A} \\
E^{\LEFTcircle}_{0,B} \arrow[r, dashed, "\varphi_{sk_B}"] & E^{\LEFTcircle}_{1,B}
\end{tikzcd}$$

SECKER-CGL public keys

$\mathsf{IKD}_{2.2}$

$\mathsf{KGen}(1^n) \to (mpk, msk)$
$\mathsf{Ext\text{-}sk}(msk, id) \to \varphi_{sk}$
$\mathsf{Ext\text{-}pk}(mpk, id) \to (E^{\LEFTcircle}_{0,id}, E^{\LEFTcircle}_{1,id})$

Insecure

Alice learns Bob's secret key!

Let the public keys be a CGLs s.t.

$$E^{\LEFTcircle}_{0,id} \leftarrow \mathsf{H}^{\mathsf{CGL}}_{\mathcal{E}ll}(mpk, id),$$
$$E^{\LEFTcircle}_{1,id} \leftarrow \mathsf{H}^{\mathsf{CGL}}_{\mathcal{E}ll}(mpk, id).$$

$$\begin{tikzcd}
E^{\LEFTcircle}_0 \arrow[d, "\varphi_A"] \arrow[dd, bend right, "\varphi_B"'] & E^{\LEFTcircle}_1 \arrow[d, "\varphi'_A"'] \arrow[dd, bend left, "\varphi'_B"] \\
E^{\LEFTcircle}_{0,A} \arrow[r, "\varphi_{sk_A}"] \arrow[d, "\lambda_0"] & E^{\LEFTcircle}_{1,A} \arrow[d, "\lambda_1"'] \\
E^{\LEFTcircle}_{0,B} \arrow[r, dashed, "\varphi_{sk_B}"] & E^{\LEFTcircle}_{1,B}
\end{tikzcd}$$

sk = isogeny

$$\begin{tikzcd} E_0 \arrow[r, "\varphi_{sk_A}"] \arrow[dr, "\varphi_{sk_B}"'] & E_{1,A} \\ & E_{1,B} \end{tikzcd}$$

~~domain curve fixed~~

$$\begin{tikzcd} E_{0,A} \arrow[r, dashed, "\varphi_{sk_A}"] & E_{1,A} \\ E_{0,B} \arrow[r, dashed, "\varphi_{sk_B}"] & E_{1,B} \end{tikzcd}$$

no curve fixed

sk = isogeny

$$\begin{tikzcd} E_0 \arrow[r, "\varphi_{sk_A}"] \arrow[dr, "\varphi_{sk_B}"'] & E_{1,A} \\ & E_{1,B} \end{tikzcd}$$

~~domain curve fixed~~

$$\begin{tikzcd} E_{0,A} \arrow[r, "\varphi_{sk_A}"] & E_{1,A} \\ E_{0,B} \arrow[r, "\varphi_{sk_B}"] & E_{1,B} \end{tikzcd}$$

~~no curve fixed~~

larger keys

Enriching the user keys

$$E_{0,A}, E_{1,A}, E_{2,A}, \dots \in pk \text{ and } \varphi_{sk_0}, \varphi_{sk_1}, \varphi_{sk_2}, \dots \in sk$$

larger keys

Enriching the user keys

$$E_{0,A}, E_{1,A}, E_{2,A}, \dots \in pk \text{ and } \varphi_{sk_0}, \varphi_{sk_1}, \varphi_{sk_2}, \ldots \in sk$$

$\implies$ same problems

Enriching the user keys

$$E_{0,A}, E_{1,A}, E_{2,A}, \dots \in pk \text{ and } \varphi_{sk_0}, \varphi_{sk_1}, \varphi_{sk_2}, \dots \in sk$$

$\implies$ same problems

Enriching the master key

$$E_0, E_1, E_2, \dots \in mpk$$

larger keys

Enriching the user keys

$$E_{0,A}, E_{1,A}, E_{2,A}, \dots \in pk \text{ and } \varphi_{sk_0}, \varphi_{sk_1}, \varphi_{sk_2}, \dots \in sk$$

$\implies$ same problems

Enriching the master key

$$E_0, E_1, E_2, \dots \in mpk$$

$\implies$ size(mpk) = #users

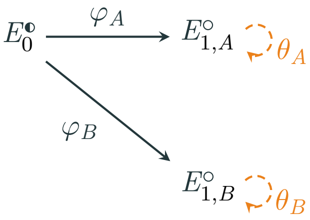
sk = endomorphism ring

IKD_3

$\mathsf{KGen}(1^n) \to (mpk, msk)$
$\mathsf{Ext\text{-}sk}(msk, id) \to \mathsf{End}(E^\bullet_{1,id})$
$\mathsf{Ext\text{-}pk}(mpk, id) \to E^\bullet_{1,id}$

Let the public key be a CGL s.t.

$$E^\circ_{0,id} \leftarrow \mathsf{H}^{\mathsf{CGL}}_{\mathcal{E}ll}(mpk, id),$$



sk = endomorphism ring

IKD$_3$

$\mathsf{KGen}(1^n) \to (mpk, msk)$
$\mathsf{Ext\text{-}sk}(msk, id) \to \mathsf{End}(E^{\bullet}_{1,id})$
$\mathsf{Ext\text{-}pk}(mpk, id) \to E^{\bullet}_{1,id}$

Let the public key be a CGL s.t.

$$E^{\circ}_{0,id} \leftarrow \mathsf{H}^{\mathsf{CGL}}_{\mathcal{E}ll}(mpk, id),$$

$$\begin{tikzcd}
E_0^{\LEFTcircle} \arrow[r, "\varphi_A"] \arrow[dr, "\varphi_B"'] & E^{\circ}_{1,A} \arrow[d, shift left, "\lambda"] \arrow[loop right, dashed, "\theta_A"] \\
& E^{\circ}_{1,B} \arrow[u, shift left, "\hat{\lambda}"] \arrow[loop right, dashed, "\theta_B"]
\end{tikzcd}$$

sk = endomorphism ring

IKD$_3$

$\mathsf{KGen}(1^n) \to (mpk, msk)$
$\mathsf{Ext\text{-}sk}(msk, id) \to \mathsf{End}(E^\bullet_{1,id})$
$\mathsf{Ext\text{-}pk}(mpk, id) \to E^\bullet_{1,id}$

Insecure

Computing many $\lambda \circ \theta_A \circ \hat{\lambda} = \theta_B \in \mathsf{End}(E^\circ_{1,B})$, Alice learns Bob's key!

Let the public key be a CGL s.t.

$$E^\circ_{0,id} \leftarrow \mathsf{H}^{\mathsf{CGL}}_{\mathcal{E}ll}(mpk, id),$$

$$\begin{tikzcd}
E_0^{\bullet} \arrow[r, "\varphi_A"] \arrow[dr, "\varphi_B"'] & E^\circ_{1,A} \arrow[d, shift left, "\lambda"] \arrow[loop right, "\theta_A"] \\
 & E^\circ_{1,B} \arrow[u, shift left, "\hat{\lambda}"] \arrow[loop right, dashed, "\theta_B"]
\end{tikzcd}$$

trapdoors

Let $(\mathsf{KGen}, f, f^{-1})$ be a trapdoor function family. Then,

$$(mpk, msk) \leftarrow\!\!\$\ \mathsf{KGen}(1^n)$$
$$E_{pk} \leftarrow f(mpk, id)$$
$$\varphi_{sk} \leftarrow f^{-1}(msk, id)$$

[BMP23] Basso, Maino, Pope — ASIACRYPT 2023
[DFV24] Duparc, Fouotsa, Vaudenay — SAC 2024

Let $(\mathsf{KGen}, f, f^{-1})$ be a trapdoor function family. Then,

$$(mpk, msk) \leftarrow_{\$} \mathsf{KGen}(1^n)$$
$$E_{pk} \leftarrow f(mpk, id)$$
$$\varphi_{sk} \leftarrow f^{-1}(msk, id)$$

However,

- FESTA [BMP23], SILBE [DFV24] use CGL paths
- f must generate SECUERs
- recipe: SECUER trapdoors

[BMP23] Basso, Maino, Pope — ASIACRYPT 2023
[DFV24] Duparc, Fouotsa, Vaudenay — SAC 2024

wrap up

→ a modular IBE definition

wrap up

- → a modular IBE definition
- → structured feasibility analysis

wrap up

- $\rightarrow$ a modular IBE definition
- $\rightarrow$ structured feasibility analysis
- $\rightarrow$ non-trivial obstacles

wrap up

- → a modular IBE definition
- → structured feasibility analysis
- → non-trivial obstacles
- → formalized missing ingredient

pre-proceeding version

wrap up

- → a modular IBE definition
- → structured feasibility analysis
- → non-trivial obstacles
- → formalized missing ingredient

contact: elif.oezbay@tu-darmstadt.de

thanks!