SUPERSINGULAR ISOGENY DIFFIE-HELLMAN KEY EXCHANGE

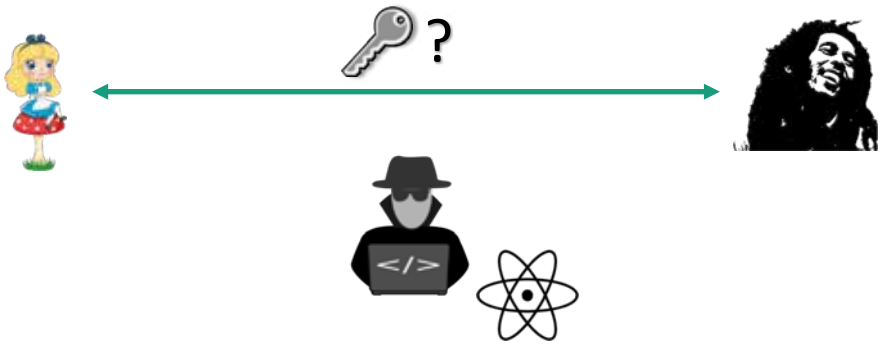
Benjamin Zengin @ OMNISECURE 2020, Berlin

21.01.2020

Fraunhofer AISEC

OMNISECURE

Motivation



Auffrischung: Diffie-Hellman Schlüsselaustausch

Öffentliche Parameter:
Primzahl p, Generator g

wählt x zufällig — $A = g^x \bmod p$ →

← $B = g^y \bmod p$ — wählt y zufällig

berechnet $B^x \bmod p$

berechnet $A^y \bmod p$

$$A^y = (g^x)^y = g^{xy} = \boldsymbol{K} = g^{yx} = (g^y)^x = B^x$$

Fraunhofer AISEC 3

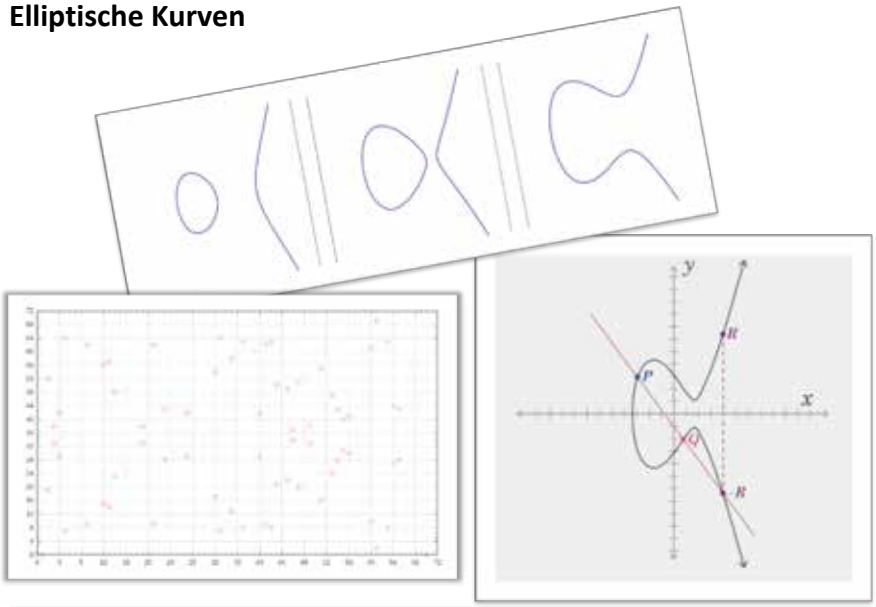
Das Problem

$$A = g^x \bmod p$$
$$\log_g A = x$$

Der diskrete Logarithmus ist auf einem hinreichend großen Quantencomputer effizient berechenbar.

Fraunhofer AISEC 4

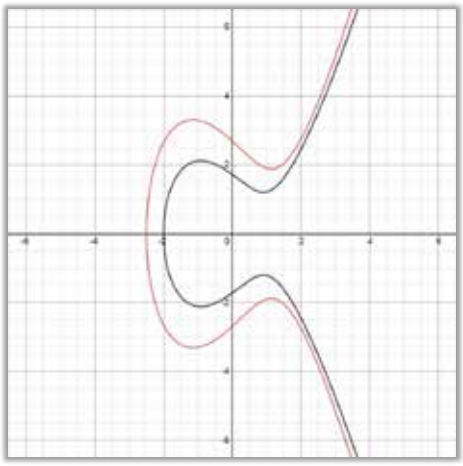
Elliptische Kurven



Fraunhofer AISEC

Isogenieklassen

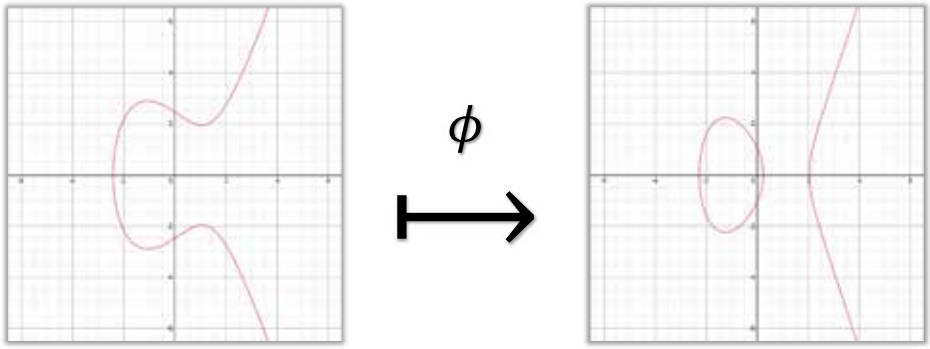
- Isomorphe Kurven mit Kennziffer eindeutig identifizierbar (*j*-Invariante)
- Eine Isogenieklasse enthält alle isomorphen Kurven mit derselben Kennziffer *j*



isomorph ≡ von gleicher Gestalt

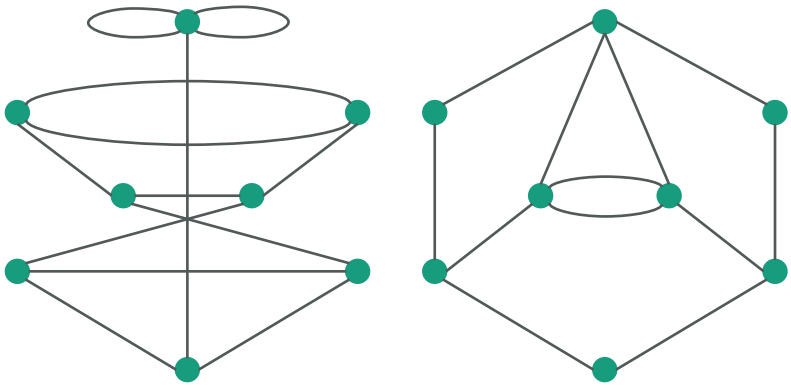
Fraunhofer AISEC

Isogenien auf supersingulären elliptischen Kurven



Fraunhofer AISEC 7

Isogeniegraphen



Grad 2 Isogeniegraph über $\mathbb{F}_{97^2}$

Grad 3 Isogeniegraph über $\mathbb{F}_{97^2}$

Fraunhofer AISEC 8

Supersingular Isogeny Diffie-Hellman (SIDH)

Öffentliche Parameter:
Basispunkte P_A, P_B
Elliptische Kurve E

wählt ϕ_A zufällig
unter Benutzung von P_A

$E_A = \phi_A(E); \phi_A(P_B)$ →

← $E_B = \phi_B(E); \phi_B(P_A)$

wählt ϕ_B zufällig
unter Benutzung von P_B

berechnet ϕ'_A
unter Benutzung von ϕ_A und $\phi_B(P_A)$

berechnet ϕ'_B
unter Benutzung von ϕ_B und $\phi_A(P_B)$

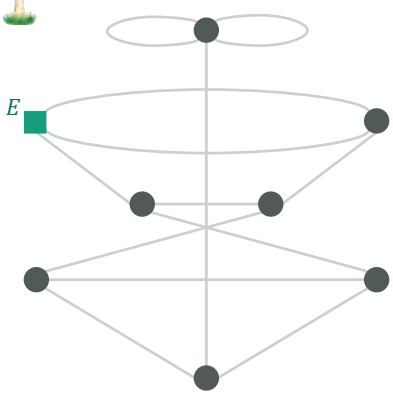
berechnet $\phi'_A(E_B)$

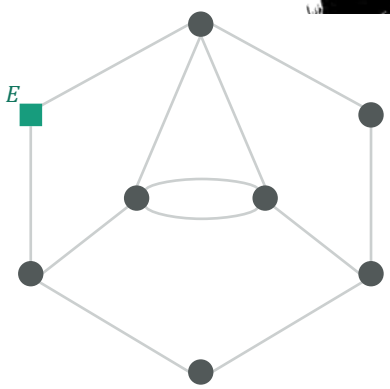
Berechnet $\phi'_B(E_A)$

$$\phi'_A(E_B) = \phi'_A(\phi_B(E)) = \boldsymbol{E_{AB}} = \phi'_B(\phi_A(E)) = \phi'_B(E_A)$$

Fraunhofer AISEC

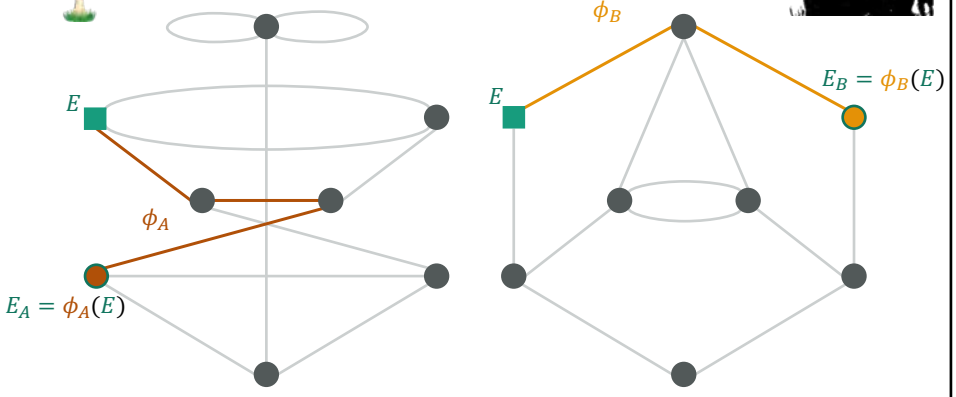
Supersingular Isogeny Diffie-Hellman (SIDH)





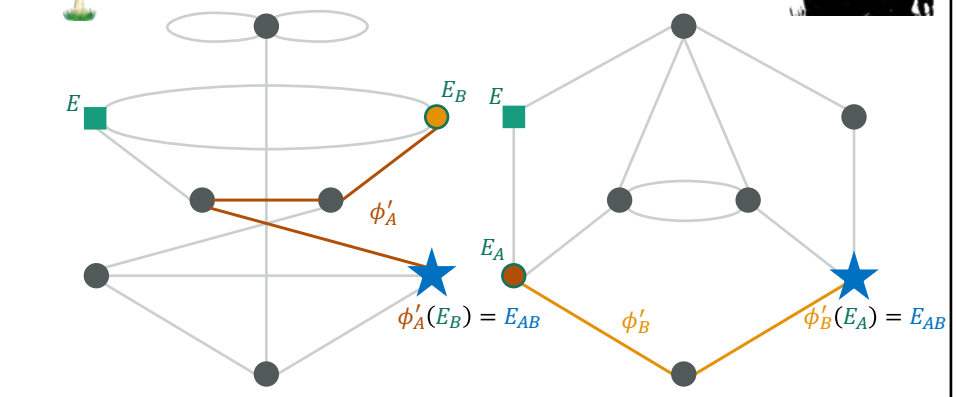
Fraunhofer AISEC

Supersingular Isogeny Diffie-Hellman (SIDH)



Fraunhofer AISEC

Supersingular Isogeny Diffie-Hellman (SIDH)



Fraunhofer AISEC

Diffie-Hellman mit verschiedenen Gruppen

	DH	ECDH	SIDH
Elemente	Ganzzahlen g modulo Primzahl	Punkte P in Kurvengruppe	Kurven E in Isogenieklasse

Fraunhofer AISEC

Diffie-Hellman mit verschiedenen Gruppen

	DH	ECDH	SIDH
Elemente	Ganzzahlen g modulo Primzahl	Punkte P in Kurvengruppe	Kurven E in Isogenieklasse
Geheimnisse	Exponenten x	Skalare k	Isogenien ϕ

Fraunhofer AISEC

Diffie-Hellman mit verschiedenen Gruppen

	DH	ECDH	SIDH
Elemente	Ganzzahlen g modulo Primzahl	Punkte P in Kurvengruppe	Kurven E in Isogenieklasse
Geheimnisse	Exponenten x	Skalare k	Isogenien ϕ
Berechnungen	$g, x \mapsto g^x$	$k, P \mapsto [k]P$	$\phi, E \mapsto \phi(E)$

Diffie-Hellman mit verschiedenen Gruppen

	DH	ECDH	SIDH
Elemente	Ganzzahlen g modulo Primzahl	Punkte P in Kurvengruppe	Kurven E in Isogenieklasse
Geheimnisse	Exponenten x	Skalare k	Isogenien ϕ
Berechnungen	$g, x \mapsto g^x$	$k, P \mapsto [k]P$	$\phi, E \mapsto \phi(E)$
Schwere Probleme	Gegeben g, g^x finde x	Gegeben $P, [k]P$ finde k	Gegeben $E, \phi(E)$ finde ϕ

Diffie-Hellman mit verschiedenen Gruppen

	DH	ECDH	SIDH
Elemente	Ganzzahlen g modulo Primzahl	Punkte P in Kurvengruppe	Kurven E in Isogenieklasse
Geheimnisse	Exponenten x	Skalare k	Isogenien ϕ
Berechnungen	$g, x \mapsto g^x$	$k, P \mapsto [k]P$	$\phi, E \mapsto \phi(E)$
Schwere Probleme	Gegeben g, g^x finde x	Gegeben $P, [k]P$ finde k	Gegeben $E, \phi(E)$ finde ϕ
Post-Quanten sicher	Nein	Nein	Ja

Danke!