MAGISKE ISOGENIER

Forskningsgruppe: NTNU Applied Cryptology Lab (NaCl)

Jonathan Komada Eriksen

- Agenda

Kvantesikker Kryptografi

Elliptiske Kurver og Isogenier

Kryptografi fra Isogenier: Fortid, Nåtid og Fremtid

Kvantesikker Kryptografi - Introduksjon

- Nesten all offentlig-krypto idag er basert på RSA eller Diffie-Hellman
- Shor's algoritme knekker begge disse i polynomisk tid!
  - Men, kjører kun på kvantemaskiner
- Vi bør ha ny offentlig-nøkkel krypto klar til kvantemaskiner kommer
  - Nøkkelutveksling: Kan ta opp hele samtalen nå, og dekryptere i fremtiden.
- NIST har hatt en standardiseringskonkurranse gående i noen år nå
  - Første kandidater klare for standardisering!
  - Ny runde med signaturer fra neste år

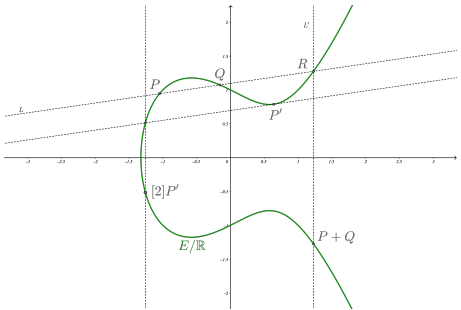
Kvantesikker Kryptografi

Elliptiske Kurver og Isogenier

Kryptografi fra Isogenier: Fortid, Nåtid og Fremtid

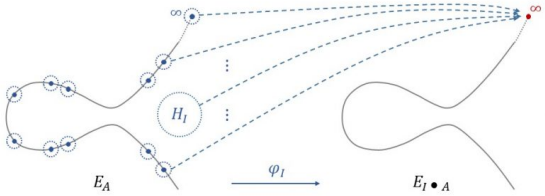
Elliptiske Kurver og Isogenier - Elliptiske Kurver

- Elliptiske Kurver er utrolig spennende objekter, som dukker opp mange steder i matematikken
- Punktene på en kurve kan gis en gruppestruktur
- Mye av moderne offentlig-nøkkel kryptografi skjer i en slik gruppe
  - Også knekt av Shor's algoritme.



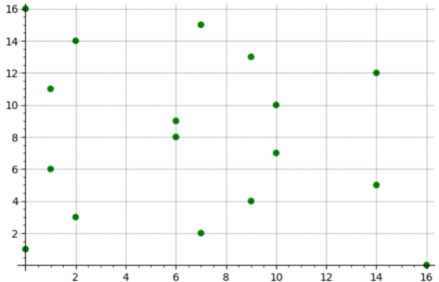
Elliptiske Kurver og Isogenier - Isogenier

- En isogeni $\phi : E_1 \to E_2$ er en tuppel av rasjonale funksjoner, som tar punktene på E_1 til punktene på E_2, og som sender identiteten til identiteten
- En isogeni induserer en gruppe-homomorfi mellom gruppene av punkter

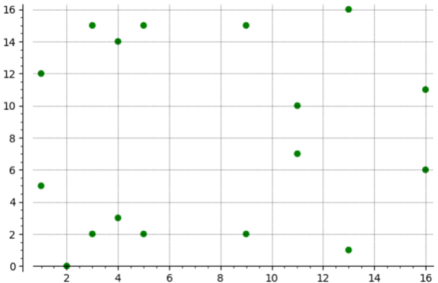


- Lett: Gitt en undergruppe av E_1, finn en isogeni med denne gruppen som kjerne.
- Vanskelig: Gitt E_1, E_2 finn en isogeni mellom disse kurvene.

Elliptiske Kurver og Isogenier - Isogeni: Eksempel

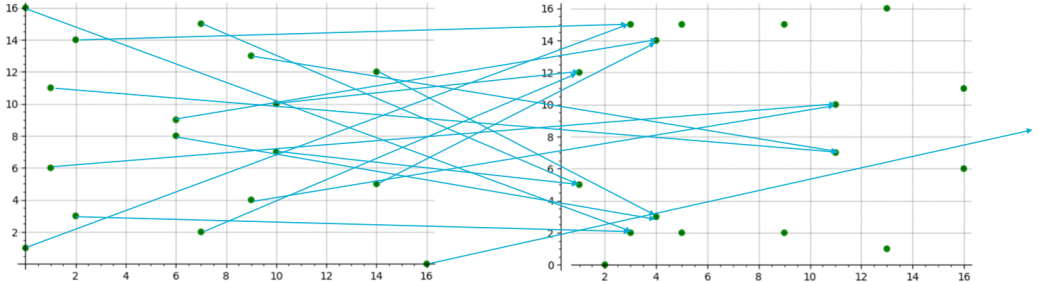


$E_0/\mathbb{F}_{17} : y^2 = x^3 + 1$



$E_1/\mathbb{F}_{17} : y^2 = x^3 + 2x + 5$

Elliptiske Kurver og Isogenier - Isogeni: Eksempel



$$\phi : E_0/\mathbb{F}_{17} : y^2 = x^3 + 1 \longrightarrow E_1/\mathbb{F}_{17} : y^2 = x^3 + 2x + 5$$

$$\phi((x,y)) = \left(\frac{x^2 + x + 3}{x + 1}, \frac{x^2 y + 2xy - 2y}{x^2 + 2x + 1} \right)$$

Kvantesikker Kryptografi

Elliptiske Kurver og Isogenier

Kryptografi fra Isogenier: Fortid, Nåtid og Fremtid

Kryptografi fra Isogenier: Fortid, Nåtid og Fremtid -
Forhistorie

- CRS nøkkelutveksling (2006)
  - Første benyttelse av isogenier innen kryptografi
  - Benyttet ordinære elliptiske kurver
  - Sub-eksponensielt kvante angrep
- CGL Hash function (2009)
  - Hashing algoritme basert på isogenier mellom *supersingulære* elliptiske kurver
  - Polynomisk tid angrep ved KLPT algoritmen.

Kryptografi fra Isogenier: Fortid, Nåtid og Fremtid - Fortid

- SIDH nøkkelutveksling (2011)
  - Nøkkelutveksling ved isogenier mellom supersingulære kurver
  - Var lenge lovende som kandidat til standardisering
  - Polynomisk tid angrep funnet i sommer!

Kryptografi fra Isogenier: Fortid, Nåtid og Fremtid - Nåtid

- CSIDH nøkkelutveksling (2018)
  - Videreutvikling av CRS nøkkelutveksling
  - Ligner veldig Diffie-Hellman, så unike egenskaper som NIKE osv.
  - Sub-eksponensielt kvante angrep gjelder fortsatt
- SQISign (2020)
  - Signaturalgoritme basert på KLPT algoritmen
  - 10x mindre nøkler enn Dilithium, 100x-1000x tregere
  - Vil bli sendt inn til NIST standardiseringskonkurranse.

Kryptografi fra Isogenier: Fortid, Nåtid og Fremtid - Fremtid

- Praktisk nøkkelutveksling?
  - CSIDH bruker flere sekunder, selv med aggressive valg av parametere
- Hash til kurve algoritme?
  - Et enormt åpent spørsmål i feltet
  - Ville fjernet "trusted setup" fra flere konstruksjoner
- Nye konstruksjoner!
  - Offentlig nøkkel krypto er mer enn bare signatur og nøkkelutveksling
  - Isogenier har mye struktur, som kan gi mange muligheter

Tusen takk!