Edwards Curves for Isogeny-based Cryptosystems?

18.12.04

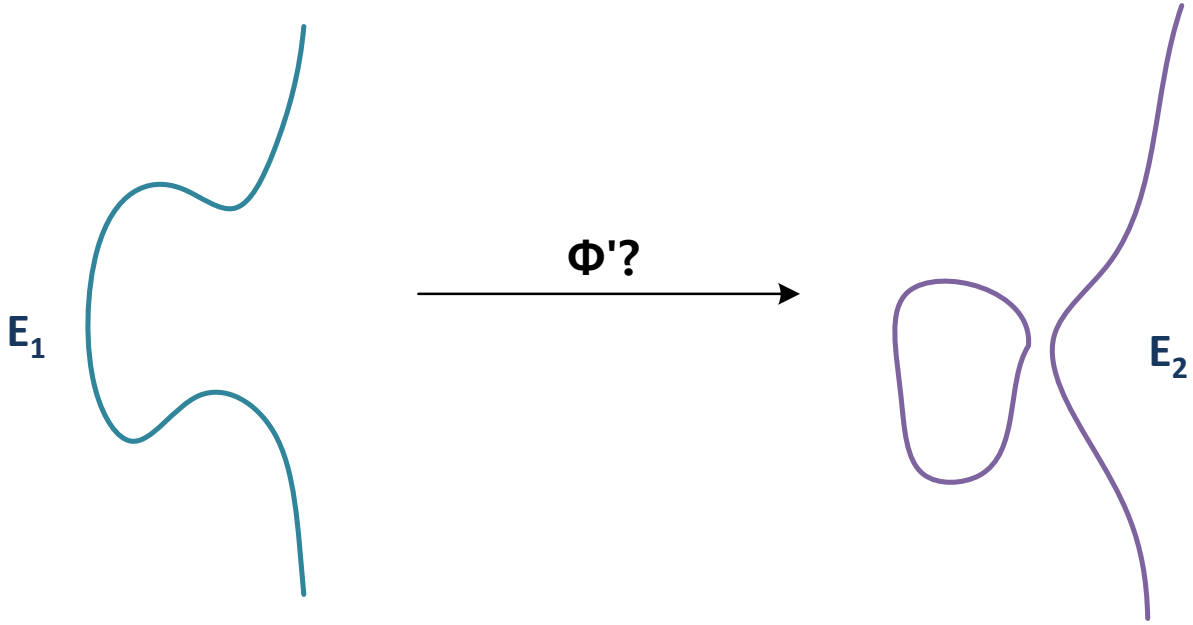
Rump Session, Asiacrypt 2018

Suhri Kim, Kisoon Yoon, Jihoon Kwon, Young Ho Park, Seokhie Hong

Korea University, NSHC, Samgsung SDS, Sejong Cyber University

Introduction

- Isogeny-based cryptosystem

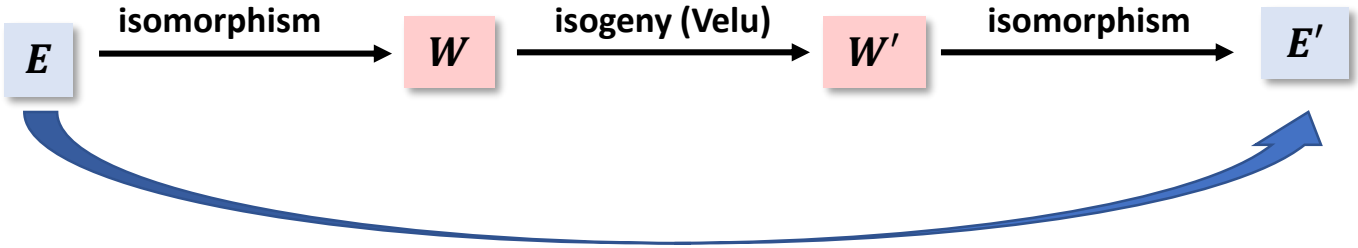


Motivation

- **"Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curves Isogenies"** – David Jao and Luca De Feo
  - *Twisted Edwards curves or Montgomery curves*
- **"A Simple and Compact Algorithms for SIDH with Arbitrary Degree Isogenies"** - Craig Costello and Huseyin Hisil
  - *There might be savings to be gained in a twisted Edwards version of SIDH, or perhaps in some sort of hybrid that passes back and forth between the two model*
- **"On Hybrid SIDH Schemes using Edwards and Montgomery Curve Arithmetic"** - Michael Meyer, Steffen Reith, and Fabio Campos
  - *Proposed hybrid SIDH that uses Edwards curves for point operation and Montgomery curves for isogenies*
- **"Twisted Edwards Curves"** - Daniel J. Bernstein, Peter Birkner, Marc Joye, Tanja Lange, and Christiane Peters
  - *If k is a finite field with $\#k \equiv 3 \bmod 4$ then every Montgomery curve over k is birationally equivalent over k to an **Edwards curve**.*

Isogenies on Edwards Curves

- **3- isogeny formula**
  - Use Velu's formula

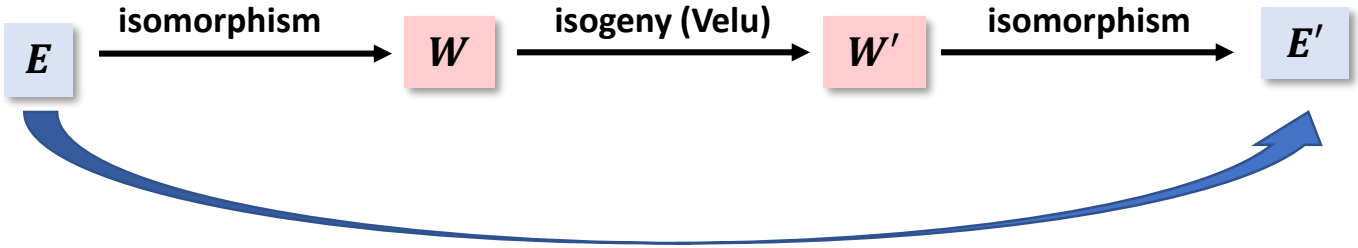


  - **Optimize Edwards isogenies proposed by Moody and Daniel Shumow**

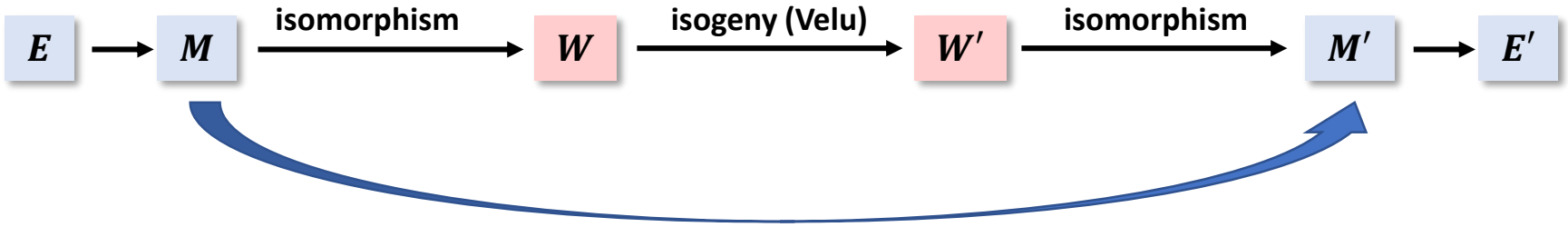
$$\Psi(x,y) = \left((-1)^s \frac{x}{A^2} \prod_{i=1}^{s} \frac{\beta_i^2 x^2 - \alpha_i^2 y^2}{1 - d^2 \alpha_i^2 \beta_i^2 x^2 y^2}, \frac{y}{B^2} \prod_{i=1}^{s} \frac{\beta_i^2 y^2 - \alpha_i^2 x^2}{1 - d^2 \alpha_i^2 \beta_i^2 x^2 y^2} \right)$$

Isogenies on Edwards Curves

- **4-isogeny formula**
  - Use Velu's formula



  - **Use isogeny formula on Montgomery curves proposed by Costello et al.**



Results

- **3-isogeny formula ($\phi: E_d \rightarrow E_{d'}$)**
  - $P = (Y_3 : Z_3)$: 3-torsion point on $E_d: x^2 + y^2 = 1 + dx^2y^2$
  - $Q = (Y : Z)$: Additional point on E_d
  - $\phi\,(Q) = (Y' : Z')$: Image point of Q
  - $(C' : D')$: Curve coefficients of the image curve $E_{d'}, (d = D/C\,, d' = D'/C')$

$$(Y' : Z') = (Y(Z^2Y_3^2 + 2Z^2Y_3Z_3 + Y^2Z_3^2) : Z(Z^2Y_3^2 + 2Y^2Y_3Z_3 + Y^3Z_3^2))$$

- **4-isogeny formula ($\phi: E_d \rightarrow E_{d'}$)**
  - $P = (Y_4 : Z_4)$: 4-torsion point on $E_d: x^2 + y^2 = 1 + dx^2y^2$
  - $Q = (Y : Z)$: Additional point on E_d
  - $\phi\,(Q) = (Y' : Z')$: Image point of Q
  - $(C' : D')$: Curve coefficients of the image curve $E_{d'}, (d = D/C\,, d' = D'/C')$

$$(Y' : Z') = ((Z^2Y_4^2 + Y^2Z_4^2)YZ(Y_4 + Z_4)^2 : (Z^2Y_4^2 + Y^2Z_4^2)^2 + 2Y^2Z^2Y_4Z_4(Y_4^2 + Z_4^2))$$

"Efficient Isogeny Computations on Twisted Edwards Curve" - Suhri Kim, Kisoon Yoon, Jihoon Kwon, Young-Ho Park, Seokhie Hong

Results

	Montgomery	Edwards
get_4_isog	4**S**+4**a**+1**s**	4**S**+2**a**+2**s**
eval_4_isog	6**M**+2**S**+3**a**+3**s**	6**M**+2**S**+4**a**+3**s**
get_3_isog	2**M**+3**S**+12**a**+3**s**	2**M**+3**S**+7**a**+4**s**
eval_3_isog	4**M**+2**S**+2**a**+2**s**	4**M**+2**S**+3**a**+3**s**

- **M : field multiplication**
- **S : field squaring**
- **a : field addition**
- **S : field subtraction**

"Efficient Isogeny Computations on Twisted Edwards Curve" - Suhri Kim, Kisoon Yoon, Jihoon Kwon, Young-Ho Park, Seokhie Hong