RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: **CRYP-R09**

Mathematical Advances in Cryptography

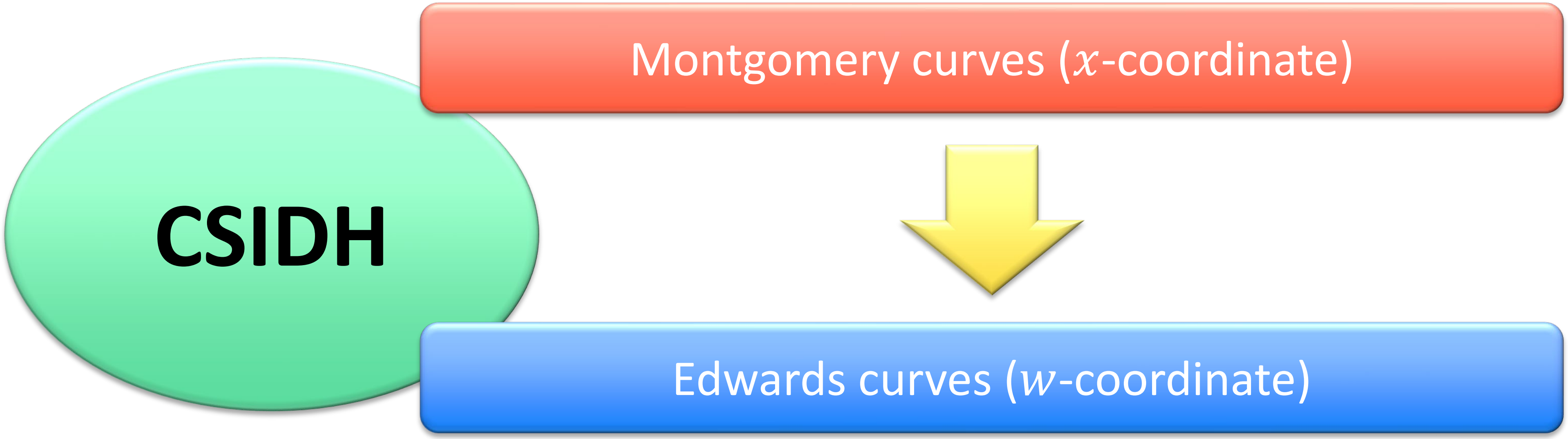
Tomoki Moriya

How to Construct CSIDH on Edwards Curves
The University of Tokyo

#RSAC

Main result

We extend a CSIDH algorithm to that on Edwards curves.



CSIDH

Montgomery curves (x-coordinate)

Edwards curves (w-coordinate)

Contents

1. Isogeny-based cryptography
2. CSIDH
3. Construct CSIDH on Edwards curves
4. Computational complexity
5. Conclusion

1. Isogeny-based cryptography

Currently public key cryptography

- RSA crypto. [Rivest, Shamir, Adleman (Communications of the ACM 1978)]
- Elliptic curve crypto. [Miller (CRYPTO 1985)], [Koblitz (Mathematics of Computation 1987)]

They are broken in polynomial time by using quantum computers.
[Shor (FOCS 1994)]

We need new cryptosystems: post-quantum cryptography.

Candidates for post-quantum cryptography

- Isogeny-based cryptography
- Lattice-based cryptography
- Multivariate cryptography
- Code-based cryptography
- Hash-based signature
- etc…

Main property of isogeny-based cryptography

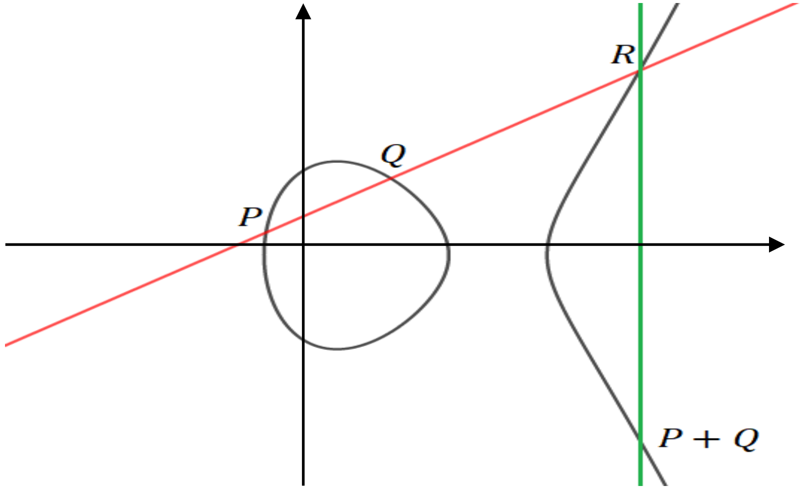
- Based on Isogeny Problem
- Using elliptic curves
- Main merit: key lengths are short.
- Main demerit: it takes more time to execute protocols.

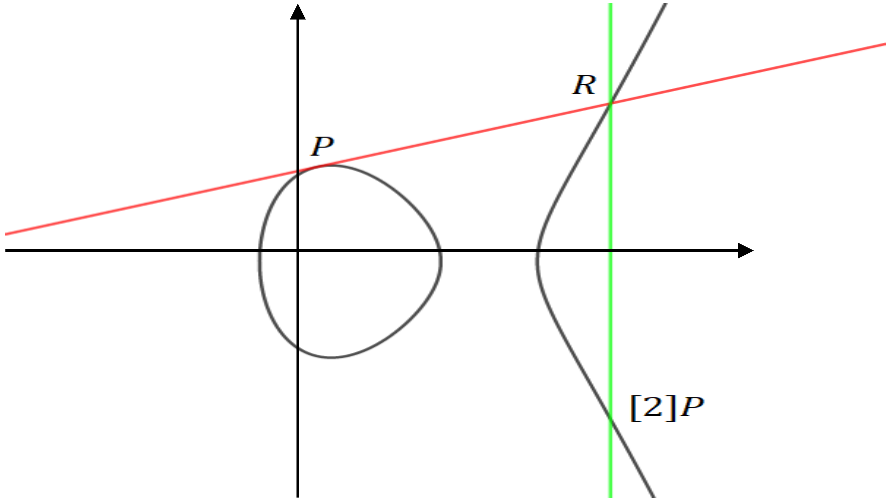
Elliptic curves and isogenies (1/3)

Elliptic curves

Elliptic curves are smooth algebraic curves with genus 1.

Elliptic curves have abelian group structures.





Elliptic curves and isogenies (2/3)

- Montgomery curves

$$y^2 = x^3 + ax^2 + x \ (a^2 \neq 4)$$

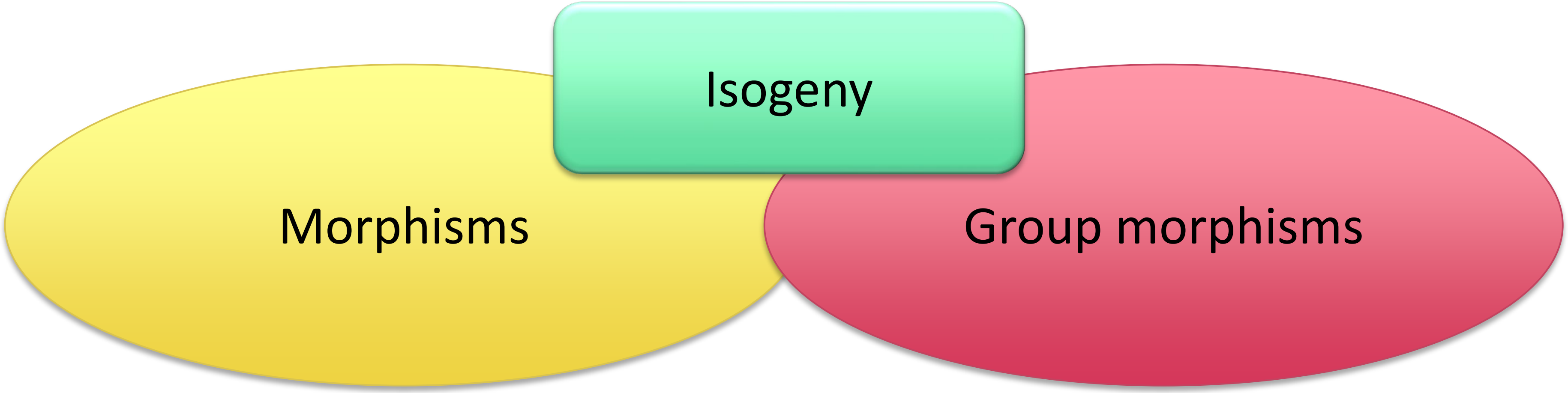
- Edwards curves

$$x^2 + y^2 = 1 + dx^2y^2 \ (d \neq 0, 1)$$

Elliptic curves and isogenies (3/3)

Isogenies

An isogeny is a morphism between elliptic curves which is also a group morphism on elliptic curves.



Velu formulas and Isogeny Problem (1/3)

Velu formulas [Velu (CR Acad. Sci. 1971)]

Input : an elliptic curve E and a finite subgroup G of E

Output : an elliptic curve E/G
and an isogeny $\phi: E \to E/G$ satisfying $\ker \phi = G$

$$(E, G) \Longrightarrow (E/G, \phi)$$

Velu formulas and Isogeny Problem (2/3)

Isogeny Problem

From two given isogenious elliptic curves E and F, compute an isogeny $\phi: E \to \mathrm{F}$

$$\phi \text{ or } G \qquad \not\Longleftarrow \qquad (E, E/G)$$

Velu formulas and Isogeny Problem (3/3)

Velu formulas (easy)

$$(E,G) \Longrightarrow (E/G,\phi)$$

Isogeny Problem (difficult)

$$\phi \text{ or } G \;\not\Longleftarrow\; (E,E/G)$$

2. CSIDH

CSIDH key exchange (1/2)

CSIDH key exchange [Castryck et al. (ASIACRYPT 2018)]

CSIDH is an isogeny-based key exchange protocol based on a group action of a finite abelian group to a set of $\mathbb{F}_p$-isomorphism classes of supersingular elliptic curves.

$$\begin{tikzcd}
E_0 \arrow[r] \arrow[d] & {[\mathfrak{a}]E_0} \arrow[d] \\
{[\mathfrak{b}]E_0} \arrow[r] & {[\mathfrak{a}][\mathfrak{b}]E_0 : y^2 = x^3 + Sx^2 + x}
\end{tikzcd}$$

CSIDH key exchange (2/2)

CSIDH key exchange [Castryck et al. (ASIACRYPT 2018)]

- A group action of an ideal class group of $\mathbb{Z}[\sqrt{-p}]$ [Waterhouse (1969)]
- This group is a finite abelian group, and a set of equivalent classes of ideals of $\mathbb{Z}[\sqrt{-p}]$.

$$\begin{tikzcd}
E_0 \arrow[r] \arrow[d] & {[\mathfrak{a}]E_0} \arrow[d] \\
{[\mathfrak{b}]E_0} \arrow[r] & {[\mathfrak{a}][\mathfrak{b}]E_0 : y^2 = x^3 + Sx^2 + x}
\end{tikzcd}$$

An algorithm of CSIDH (1/2)

How do we compute an elliptic curve $[\mathfrak{a}]E_0$?

- Let a prime p satisfy $p = 4l_1 \cdots l_n - 1$, where the $l_1, \cdots, l_n$ are distinct small odd primes.
- A group element $[\mathfrak{a}]$ satisfies $[\mathfrak{a}] = [\mathfrak{l}_1]^{e_1} \cdots [\mathfrak{l}_n]^{e_n}$, where $[\mathfrak{l}_i] = [(l_i, \sqrt{-p} - 1)]$, $[\mathfrak{l}_i]^{-1} = [(l_i, \sqrt{-p} + 1)]$, and $e_1, \ldots, e_n$ are small integers. (let max absolute value of them be m.)

- Let secret keys $(e_1, \ldots, e_n)$.
- We only consider actions of $[\mathfrak{l}_i]$ and $[\mathfrak{l}_i]^{-1}$.

An algorithm of CSIDH (2/2)

How do we compute actions of $[\mathfrak{l}_i]$ and $[\mathfrak{l}_i]^{-1}$?

- $[\mathfrak{l}_i]E = E/E[\mathfrak{l}_i]$, and $[\mathfrak{l}_i]^{-1}E = E/E[\overline{\mathfrak{l}_i}]$. (Waterhouse)
- $E[\mathfrak{l}_i] :=$ a subgroup of E generated by a point of order l_i contained in $\ker(\pi_p - 1)$, where π_p is p-Frobenius map $(x, y) \mapsto (x^p, x^p)$.
- $E[\overline{\mathfrak{l}_i}] :=$ a subgroup of E generated by a point of order l_i contained in $\ker(\pi_p + 1)$.

→ Velu formulas

CSIDH on Montgomery curves (1/2)

Montgomery curves : $y^2 = x^3 + ax^2 + x$

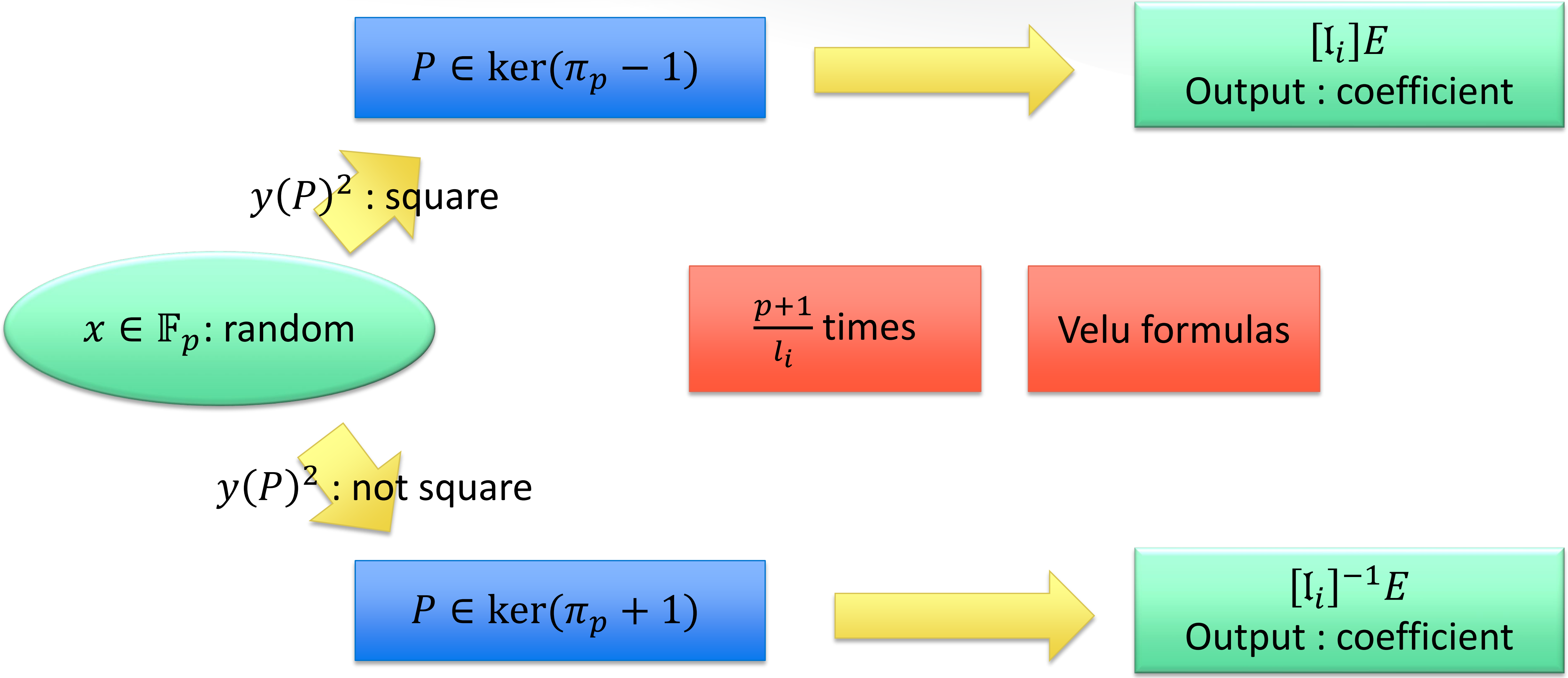
- x-coordinate [Montgomery (Mathematics of Computation 1987)] [Costello et al. (ASIACRYPT 2017)]
- $x \in \mathbb{F}_p$: random $\Rightarrow P \in \ker(\pi_p - 1)$ or $\ker(\pi_p + 1)$, where $x(P) = x$.

  $y(P)^2 = x^3 + ax^2 + x$: square $\Rightarrow P \in \ker(\pi_p - 1)$.

  $y(P)^2 = x^3 + ax^2 + x$: not square $\Rightarrow P \in \ker(\pi_p + 1)$.

  $\frac{\mathrm{p+1}}{l_i} P$ is a point of order l_i with high probability $(1 - 1/l_i\ )$.
- a is unique up to $\mathbb{F}_p$-isomorphism.

CSIDH on Montgomery curves (2/2)



$x \in \mathbb{F}_p$: random

$y(P)^2$: square

$P \in \ker(\pi_p - 1)$

$[\mathrm{I}_i]E$
Output : coefficient

$\frac{p+1}{l_i}$ times

Velu formulas

$y(P)^2$: not square

$P \in \ker(\pi_p + 1)$

$[\mathrm{I}_i]^{-1}E$
Output : coefficient

3. Construct CSIDH on Edwards curves

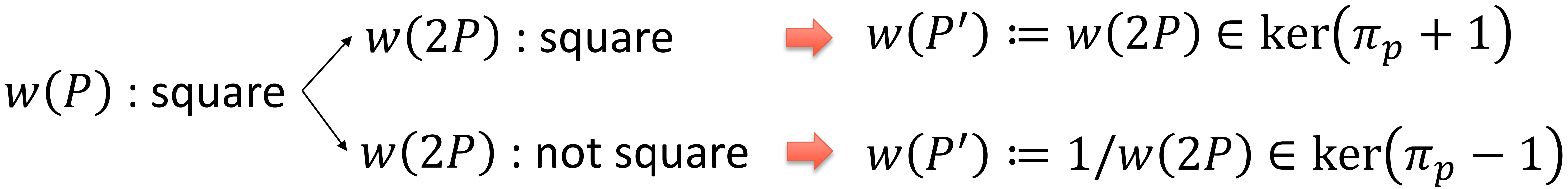
CSIDH on Edwards curves

Edwards curves : $x^2 + y^2 = 1 + dx^2y^2$

- w-coordinate : $w(x, y) = dx^2y^2$ [Farashahi et al. (ACISP 2017)][Kim et al. (ASIACRYPT 2019)]
- $w \in \mathbb{F}_p$: random ⇒ sometimes $P \notin \ker(\pi_p - 1)$ and $P \notin \ker(\pi_p + 1)$, where $w(P) = w$.
- There is no proof that d is unique up to $\mathbb{F}_p$-isomorphism.

Main theorems (1/3)

Theorem 1,3



$w(P)$: square

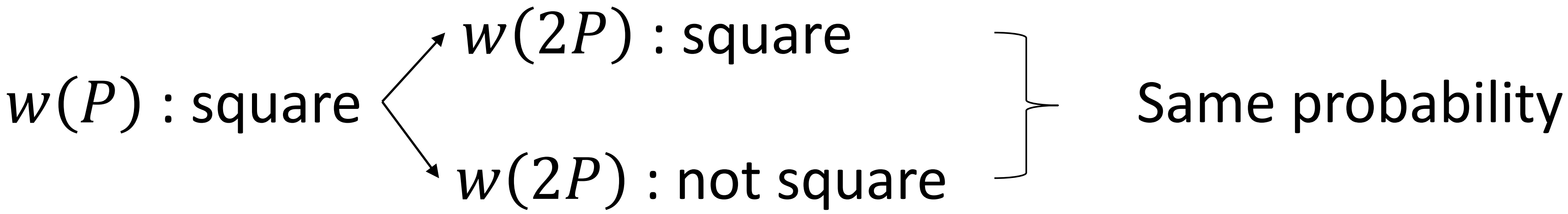
$w(2P)$: square → $w(P') := w(2P) \in \ker(\pi_p + 1)$

$w(2P)$: not square → $w(P') := 1/w(2P) \in \ker(\pi_p - 1)$

In each case, $\frac{\mathrm{p}+1}{4l_i} P'$ is a point of order l_i with high probability ($1 - 1/l_i$).

Main theorems (2/3)

Theorem 2



$w(P)$: square

$w(2P)$: square

$w(2P)$: not square

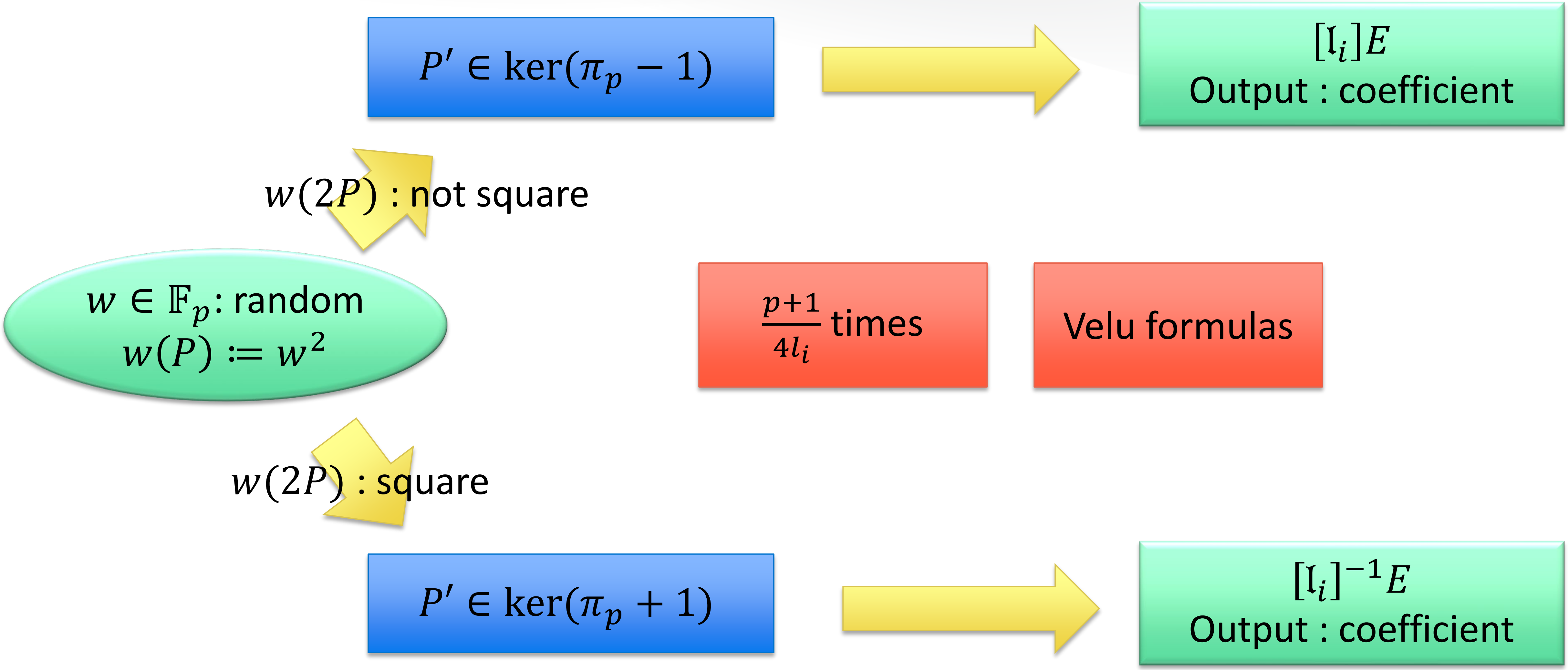
Same probability

Main theorems (3/3)

Theorem 4

Coefficients of Edwards curves d $\xleftrightarrow{\mathbf{1:1}}$ $\mathbb{F}_p$-isomorphism classes

CSIDH on Edwards curves



$P' \in \ker(\pi_p - 1)$

$[\mathrm{I}_i]E$

Output : coefficient

$w(2P)$: not square

$w \in \mathbb{F}_p$: random

$w(P) \coloneqq w^2$

$\frac{p+1}{4l_i}$ times

Velu formulas

$w(2P)$: square

$P' \in \ker(\pi_p + 1)$

$[\mathrm{I}_i]^{-1}E$

Output : coefficient

4. Computational complexity

Theoretical comparing computational complexity (1/2)

Montgomery

Sampling points

- Compute $Cx^3 + Ax^2 + Cx$

  $3\mathbf{M} + 1\mathbf{S} + 2\mathbf{a}$

Edwards

Sampling points

- Compute w^2

  $1\mathbf{S}$

- Compute $w(2P)$

  $4\mathbf{M} + 1\mathbf{S} + 5\mathbf{a}$

$1\mathbf{M} + 1\mathbf{S} + 3\mathbf{a}$

Montgomery

Scalar multiplication

- Compute $Q = \left[\frac{p+1}{\Pi_{k\in S}\ell_k}\right] P$

Edwards

Scalar multiplication

- Compute $Q = \left[\frac{p+1}{4\Pi_{k\in S}\ell_k}\right] P'$

$-8\mathbf{M} - 3\mathbf{S} - 9\mathbf{a}$

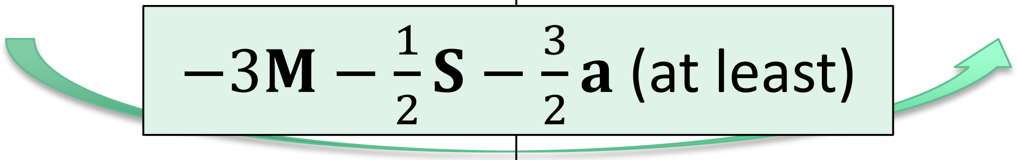
Theoretical comparing computational complexity (2/2)

Montgomery

Sampling points and scalar multiplication

Edwards

Sampling points and scalar multiplication



$-3\mathbf{M} - \frac{1}{2}\mathbf{S} - \frac{3}{2}\mathbf{a}$ (at least)

Compute isogenies **[Meyer et al. (INDOCRYPT 2018)]**

- Compute $E \to E/\langle R \rangle$

  $(6s + 2)\mathbf{M} + 8\mathbf{S} + (4s + 8)\mathbf{a}$

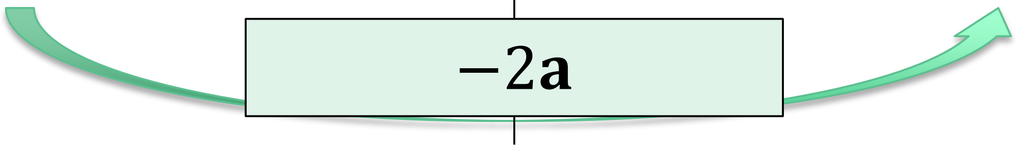
  two s th-power

Compute isogenies **[Kim et al. (ASIACRYPT 2019)]**

- Compute $E \to E/\langle R \rangle$

  $(6s + 2)\mathbf{M} + 8\mathbf{S} + (4s + 6)\mathbf{a}$

  two s th-power



$-2\mathbf{a}$

Implementation

Based on the original paper of CSIDH, p was chosen as $p = 4 \cdot l_1 \cdots l_{74} - 1$, where $l_1, \cdots, l_{73}$ were the smallest distinct odd primes, and $l_{74} = 587$.
Let $m = 5$.

We measured the average computational complexity by executing it 50000 times.

	Montgomery	Edwards
M	328,195	328,055
S	116,915	116,857
a	332,822	331,844
Total	438,368	438,133

$1\mathbf{S} = 0.8\mathbf{M},\ 1\mathbf{a} = 0.05\mathbf{M}$

5. Conclusion

Conclusion

- We proposed a new CSIDH algorithm on Edwards curves.
- This algorithm is as fast as (a little bit faster than) that on Montgomery curves.

Thank you for listening!