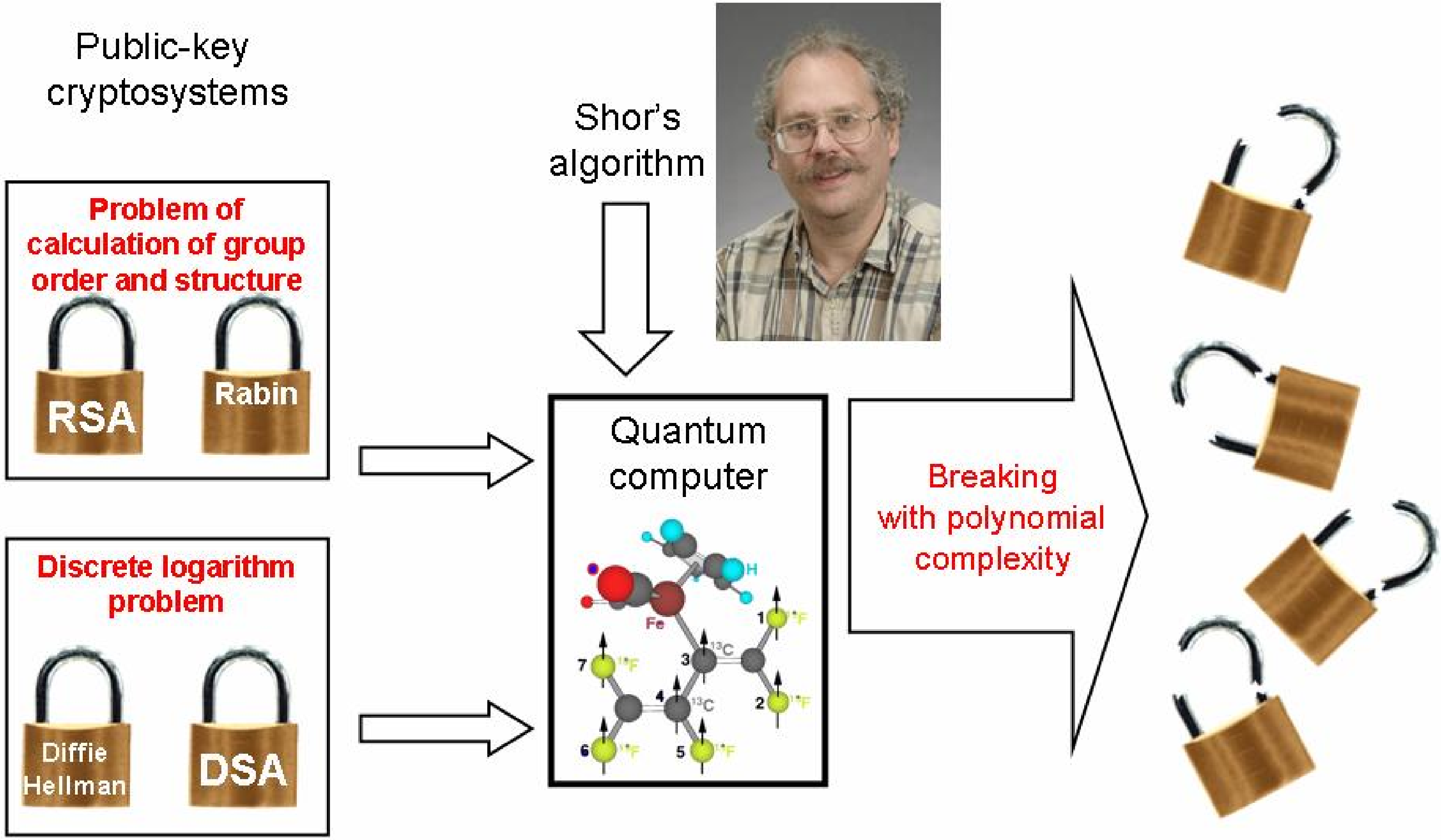
Public-Key Cryptosystem Based on Isogenies

Alexander Rostovtsev
Anton Stolbunov

Saint-Petersburg State
Polytechnical University

Quantum Computer



Basic conceptions

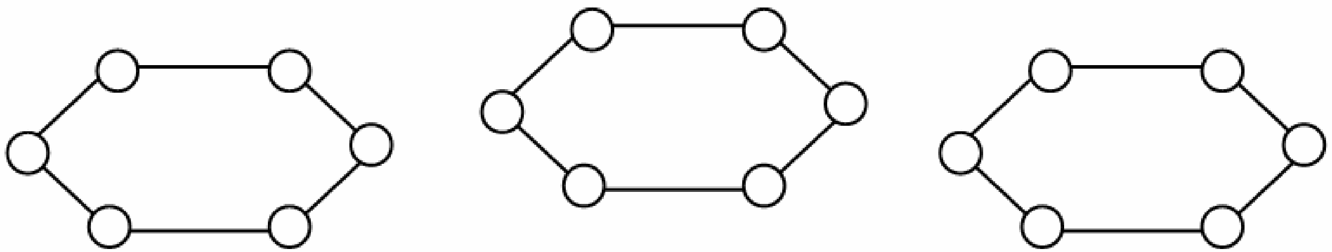
- Non-supersingular elliptic curves over a finite field F_p: $Y^2 = X^3 + aX + b$; $j \neq 0, 1728$
- $\pi^2 - t\pi + p = 0$ - a Frobenius equation
- $D_\pi = t^2 - 4p$ - a Frobenius discriminant
- Isogenous elliptic curves
- Isogeny degree
- Isogeny kernel
- Modular equation: $\Phi_l(S, T) = 0$

Branchless Cycles

- Elkies criterion: for an elliptic curve given, if

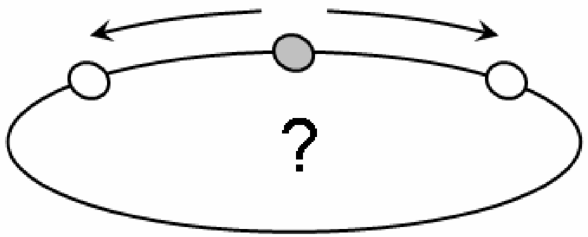
  $$\left(\frac{D_\pi}{l}\right) = 1,$$

  then there are two l -isogenous elliptic curves over F_p
- Isogenies of an Elkies degree form branchless cycles:



Direction Determination

- Frobenius equation for points of order l: $\pi^2 - t\pi + p = 0 \pmod{l}$



- $\left(\frac{t^2-4p}{l}\right)=1$ => there are 2 roots: π_1, π_2 over F_l – the Frobenius eigenvalues
- Action of the Frobenius endomorphism on an isogeny kernel is equivalent to multiplication of points by an eigenvalue [Elkies 1998]: $(X^p, Y^p) = \pi\cdot(X, Y)$ in $F_p[X, Y] / (Y^2 - X^3 - aX - b, H(X))$

Directed Step

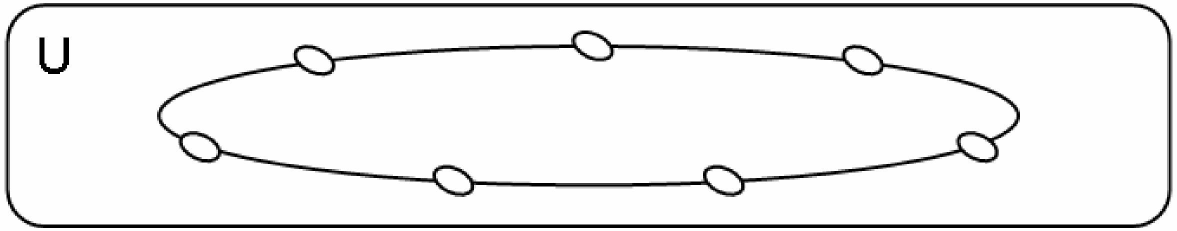
Input: field F_p, curve E, degree l, direction π

Algorithm:

- Find a root j_1 of $\Phi_l (j, T) = 0$ over F_p
- Compute an isogenous elliptic curve E_1
- Compute the polynomial $H_1(X)$ which determines the isogeny kernel [Müller 1995]
- Check whether $(X^p, Y^p) = \pi \cdot (X, Y)$ in $F_p [X, Y] / (Y^2 - X^3 – aX - b, H_1(X))$
  If not, then compute E_2 using the root j_2

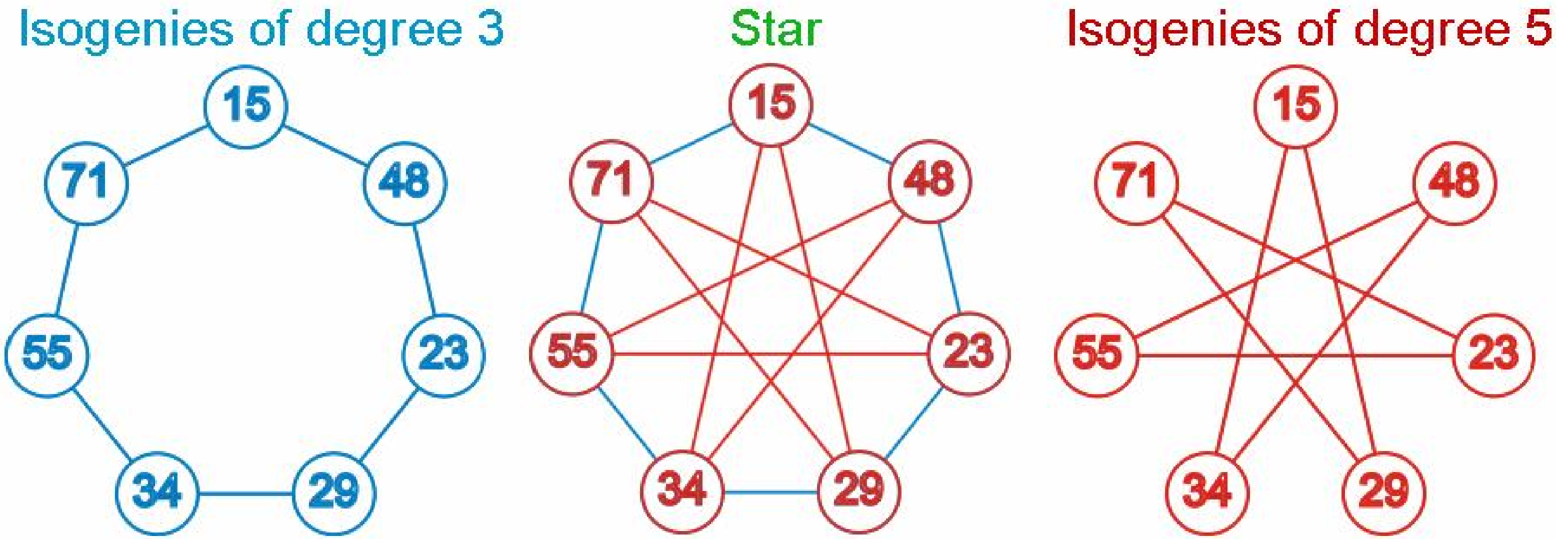
Cycle of Prime Length

- U - a set of isogenous elliptic curves over F_p
- #U = H (D_π) - a class number [Schoof 1987]
- Practical observation:
  #U is prime => single isogeny cycle



Isogeny Star

Example over F_{83} :

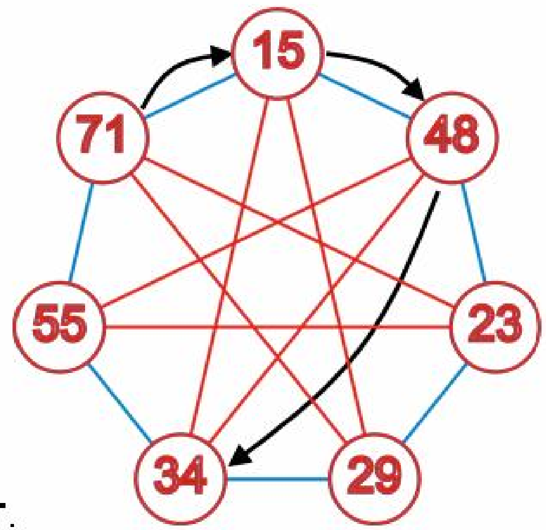


A graph of prime number of elliptic curves, connected by isogenies of Elkies degrees

Route on Star

- For given
  - F_p – a finite field
  - E – an elliptic curve in a star
  - $\{ l_i \}$ – a set of isogeny degrees
  - $\{ \pi_i \}$ - a set of positive directions
- A route is a set $R = \{ r_i \}$, where r_i is a number of steps by l_i -isogeny in the direction π_i
- Routes are commutative: $R_A R_B = R_B R_A$

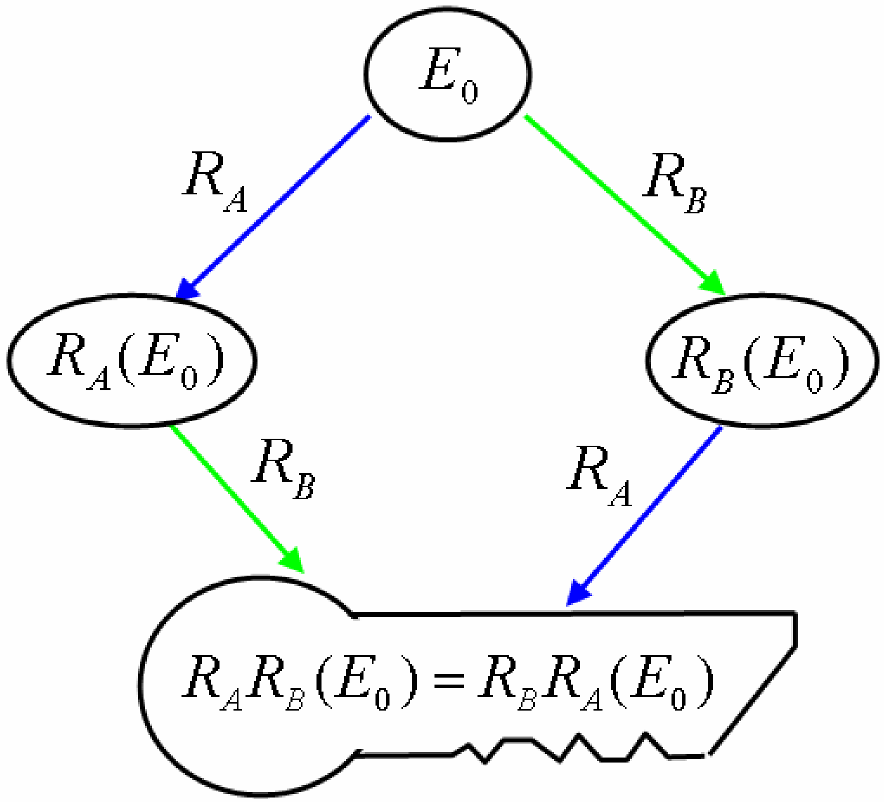
a route {2,1}:



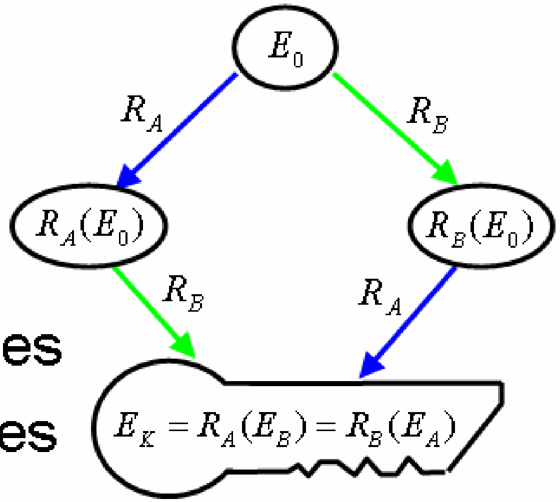
Key Agreement

$$A \xrightarrow{R_A(E_0)} B$$

$$A \xleftarrow{R_B(E_0)} B$$



Key Agreement – Algorithm



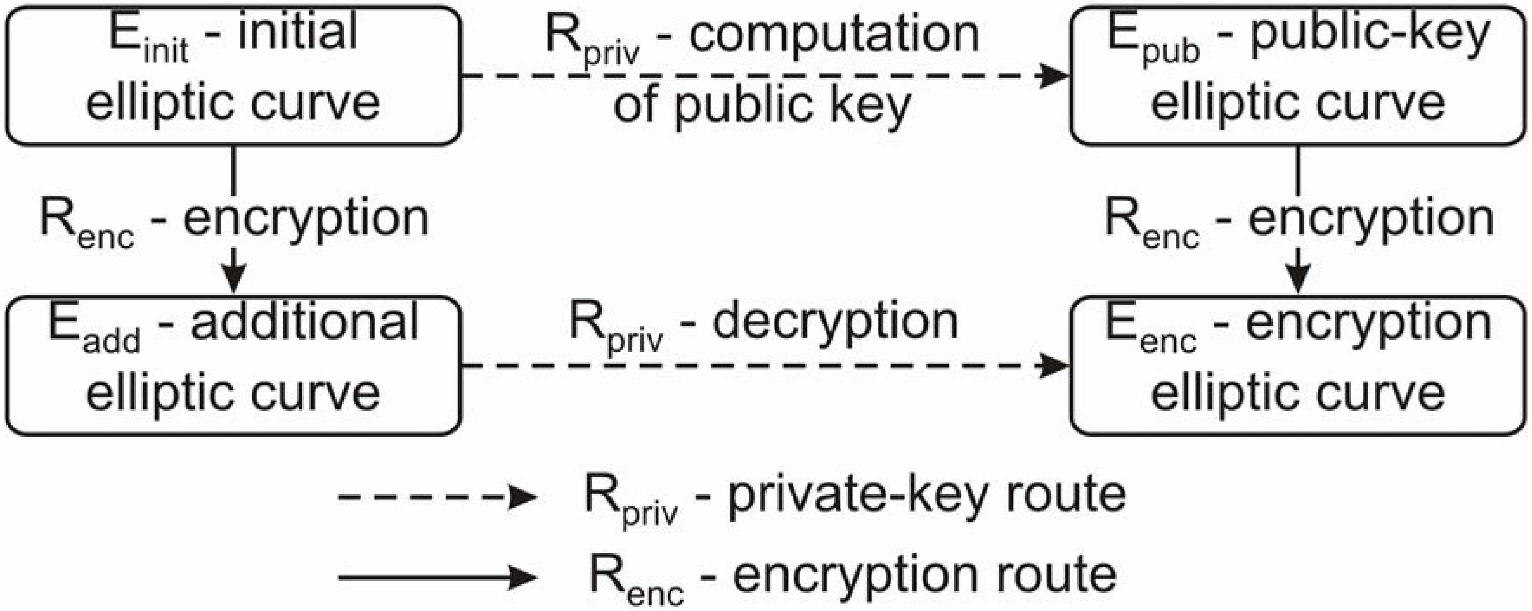
Common parameters:

- F_p – a finite field
- E_0 – an initial elliptic curve
- $\{ l_i \}$ – a set of Elkies isogeny degrees
- $\{ \pi_i \}$ - a set of Frobenius eigenvalues

Algorithm:

- A randomly chooses a route R_A and sends $E_A=R_A(E_0)$
- B randomly chooses a route R_B and sends $E_B=R_B(E_0)$
- A computes $E_K=R_A(E_B)$, B computes $E_K=R_B(E_A)$
- Resulting key is the j-invariant of E_K

Public-Key Encryption



Security

- Problem of searching for a route between elliptic curves
- Solving methods on an #U-curves star:
  - Brute-force: O (#U) isogenous steps
  - Meet-in-the-middle: O (√#U) isogenous steps
  - Others - ?

Quantum Computer Resistance

- An algorithm of a route search requires a subroutine, which calculates a chain of isogeny steps
- Calculation of an isogeny chain requires consecutive solving of modular equation
  $\Phi_l (j, T) = 0$,
  where j is being changed with every step
- Leads to exponential time of the algorithm

Complexity and Sizes

- Key agreement complexity:
  - O (log #U) isogeny steps, or
  - O ($\log^4$ p) field operations
- Consuming operations:
  - X^p mod H(X)
  - solving of Φ_l (j, T) = 0
- For 2^{80} secrecy:
  - field characteristic: p ~ 2^{320}
  - star size ~ 2^{160}
  - number of isogeny degrees ~ 40
  - steps per degree: 0 … ±8

Parameters Selection

- Obtaining a large prime #U is very complicated
- Hypothesis: #U must have a large prime divisor
- Choose $D_\pi = D f^2$, where f is a large prime conductor and h(D) is small. Then [Cohen, 1996]

$$h_{D_\pi} = h_D \cdot \left(f - \left(\frac{D}{f} \right) \right) = h_D \cdot (f \pm 1)$$

Choose f such that $\frac{f \pm 1}{2}$ is prime

Test Implementation

- Mathematica 5.0
- $F_{2038074743}$
- Star of 55103 elliptic curves (prime), chosen by direct computation of a class number
- 6 isogeny degrees: {3, 5, 7, 11, 13, 17}
- 0…9 steps per each isogeny degree

The End

A. Rostovtsev and A. Stolbunov
Public-Key Cryptosystem Based on Isogenies
http://eprint.iacr.org/2006/145