РУТОКЕН

Конференция РусКрипто-2018

Протокол SIKE и его устойчивость к классическим и квантовым атакам

Олег Тараскин,
компания «Актив»

Постквантовые алгоритмы

Теория кодов испр. ошибки	McEliece
Теория решеток:	NTRU, LWE, R-LWE
Хэши :	Merkle hash thee signature
Multivariate	HFE
Изогении элл. кривых:	SIDH

Квантовая сложность

- Факторизация n-битного модуля RSA:

~2n кубит, $4n^3$ операций

- ECDLP для кривых над GF(p):

~6n кубит, $360n^3$ операций

(Пример: для ГОСТ Р 34.10-2012 — 1536 и 3072 кубит)

Shor’s discrete logarithm quantum algorithm for elliptic curves, John Proos and Christof Zalka, 2008

Последние достижения в квантовых вычислениях:

Июль 2017: 51 кубит в связном состоянии

(проф. Михаил Лукин, Гарвард)

Ноябрь 2017: создан прототип 50 кубитного процессора

(Dario Jil, IBM)

Области применения изогений :

Алгоритм SEA (Shoof – Elkies – Atkin) подсчета точек кривой

Защита эллиптических кривых от атак по побочным каналам

Исследования стойкости кривых, методом приведения

Аналог Диффи-Хеллмана

ЭЦП

Наиболее значимые результаты

- 2006:

“**Public-Key Cryptosystem Based on Isogenies**”

Alexander Rostovtsev, Anton Stolbunov

- 2010:

Constructing elliptic curve isogenies in quantum subexponential time

Andrew M. Childs, David Jao , Vladimir Soukharev

- 2011:

“**Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies**”

David Jao, Luca De Feo

Эллиптические кривые

GF(p^n), p - характеристика
для p > 3 сокращенная форма Вейерштрасса :

$$y^2 = x^3 + Ax + B$$

(где $4A^3 + 27B^2 \neq 0$)

j–инвариант кривой E :

$$j(E) = 1728 \frac{4A^3}{4A^3+27B^2}$$

У изоморфных кривых над одним полем j–инварианты равны.

Изогении

Пусть E1 и E2 эллиптические кривые над полем F

Изогенией E1⟶ E2 над F называется неконстантное рациональное отображение над F, которое также является групповым гомоморфизмом

$$(x,\ y) \longrightarrow \left(\frac{f1(x,y)}{f2(x,y)}, \frac{g1(x,y)}{g2(x,y)}\right) \quad , \quad \text{где } f1, f2, g1, g2 \text{ – полиномы}$$

Степенью изогении называется степень рационального отображения

Теорема Tate :

Две кривые над одним полем изогенны тогда и только тогда, когда порядки их групп равны

Пример

F = GF(19), E1: $y^2 = x^3 + x + 1$

E2: $y^2 = x^3 + 4x + 13$

#E1 = #E2 = 21

$$(x, y) \longrightarrow \left(\frac{x^3 - 4x^2 - 8x - 8}{x^2 - 4x + 4}, \frac{x^3y - 6x^2y + 5xy - 6y}{x^3 - 6x^2 - 7x - 8}\right)$$

Степень изогении = 3

Пример

Выберем точки A1 (9, 6) и B1 (14, 2) E1

C1 = A1 + B1

Изогения на E2 :

A1 (9, 6) → A2 (14, 1)
B1 (14, 2) → B2 (17, 4)
C1 (5, 6) → C2 (8, 5)

Легко проверить на кривой E2 что A2 + B2 = C2

Изогении

Эндоморфизм – это изогения кривой на саму себя.

Пример: Скалярное умножение точки на число n

Для n = 2:

$$2 * P = \left(\frac{x^4 - 2Ax^2 - 8Bx - A^2}{4(x^3 + Ax + B)}, \frac{(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B - A)y}{8(x^3 + Ax + B)^2}\right)$$

Для произвольного n аналогичная (но более длинная) формула может быть получена рекуррентно при помощи так называемых полиномов деления (division polynomials)

Алгоритм Velu (1971)

Вход:

кривая $y^2 = x^3 + Ax + B$, подгруппа C (ядро изогении)

Выход:

изогенная кривая $y^2 = x^3 + A'x + B'$

и рациональное отображение $(x, y) \longrightarrow \left(\frac{f1(x,y)}{f2(x,y)}, \frac{g1(x,y)}{g1(x,y)}\right)$

Сложность : O(порядок C)

Алгоритм Velu

1. Отбрасываем точку на бесконечности

2. C_2 - мн-во точек четного порядка из C, R все остальные

3. Разбиваем R на две части R_+ и R_- : если точка P – в R_+ то обратная ей – в R_-

4. Мн-во S = $C_2 \cup R_+$

Алгоритм Velu

Для каждой точки $Q = (x_Q, y_Q) \in S$:

$g_Q^x = 3x_Q^2 + A$

$g_Q^y = -2y_Q$

$$v_Q = \begin{cases} g_Q^x \text{ если } Q = -Q \\ 2g_Q^x, \text{ если } Q \neq -Q \end{cases}$$

$u_Q = (g_Q^y)^2$

$v = \sum_{Q \in S} (v_Q)$, $w = \sum_{Q \in S} (u_Q + x_Q v_Q)$

Коэфф. Уравнения изогенной кривой E' : $A' = A - 5v$, $B' = B - 7w$

Алгоритм Velu

Отображение :

$$(x, y) \longrightarrow (\alpha,\ \beta)$$

$$\alpha = x + \sum_{Q \in S}\left(\frac{v_Q}{x - x_Q} - \frac{u_Q}{(x - x_Q)^2}\right)$$

$$\beta = y + \sum_{Q \in S}\left(u_Q \frac{2y}{(x - x_Q)^3} - v_Q \frac{y - y_Q}{(x - x_Q)^2} - \frac{g_Q^x g_Q^y}{(x - x_Q)^2}\right)$$

Сложная задача вычисления изогений

Даны две кривые E1 и E2 одинакового порядка над одним полем.

Требуется найти изогению $(x,\ y) \longrightarrow \left(\frac{f1(x,y)}{f2(x,y)}, \frac{g1(x,y)}{g1(x,y)}\right)$ между ними

Вычисление изогений степени l^e

Пусть P – точка порядка l^e. Необходимо подсчитать изогению φ:
E -> E /< P >

Разложим φ на $\varphi_{e-1} * \varphi_{e-2} * \dots * \varphi_0$,

$\varphi_0 = E, \quad P_0 = P$

$\varphi_i : \quad E_i \text{ -> } E_{i+1}, \quad E_{i+1} = E_i / <l^{e-i-1} * P_i > \ , P_{i+1} = \varphi(P_i)$

Т.е. вычисление изогении степени l^e требует $e - 1$ шагов
с использованием Velu

и скалярным умножением точки на число l

Пример для l^5

Пусть имеется точка P порядка l^5

Требуется вычислить изогению $E \rightarrow E / < P >$

Метод 1 : Подать на вход алгоритма Velu точку P, выполнить ~ $\frac{l^5}{2}$ шагов и получить E / <P>

Метод 2 :

$\varphi = \varphi_4 * \varphi_3 * \varphi_2 * \varphi_1 * \varphi_0$

$\varphi_0 = E_0 \rightarrow E_0 / <l^4 * P> \quad P_1 = \varphi_0(P)$

$\varphi_1 = E_1 \rightarrow E_1 / <l^3 * P_1> \quad P_2 = \varphi_0(P_1)$

$\varphi_2 = E_2 \rightarrow E_2 / <l^2 * P_2> \quad P_3 = \varphi_0(P_2)$

$\varphi_3 = E_3 \rightarrow E_3 / <l * P_3> \quad P_4 = \varphi_0(P_3)$

$\varphi_4 = E_4 \rightarrow E_4 / <P_4>$

Суперсингулярные эллиптические кривые

Порядок группы точек кривой E :

$\#E(GF(p^n)) = p^n + 1 - t$ t – след Фробениуса

Если $t = 0 \bmod p$ -> E – суперсингулярная кривая, иначе – обычная.

MOV – атака: у суперсингулярных кривых задача ECDLP для кривой $E(GF(p^n))$ сводится к решению DLP над полем $GF(p^{n*k})$, где *к* — небольшое натуральное число.

Суперсингулярные кривые «гладкого» порядка можно использовать в криптосистемах с изогениями.

Выбор типа поля суперсингулярных кривых

Поле	число j - инвариантов
GF(p)	$\sim p^{1/2}$
GF(p^n)	$\sim \frac{p}{12}$

Граф изогений суперсингуляных кривых

Граф изогений представляет собой правильный граф.

Существует $l + 1$ изогений эллиптических кривых степени l в расширении поля K

Граф изогений суперсингуляных кривых

Пример (пример и изображения графов — Dr. Fre Vercauteren):

P = 241

число J-инвариантов : #J-inv = 20 (~P/12)

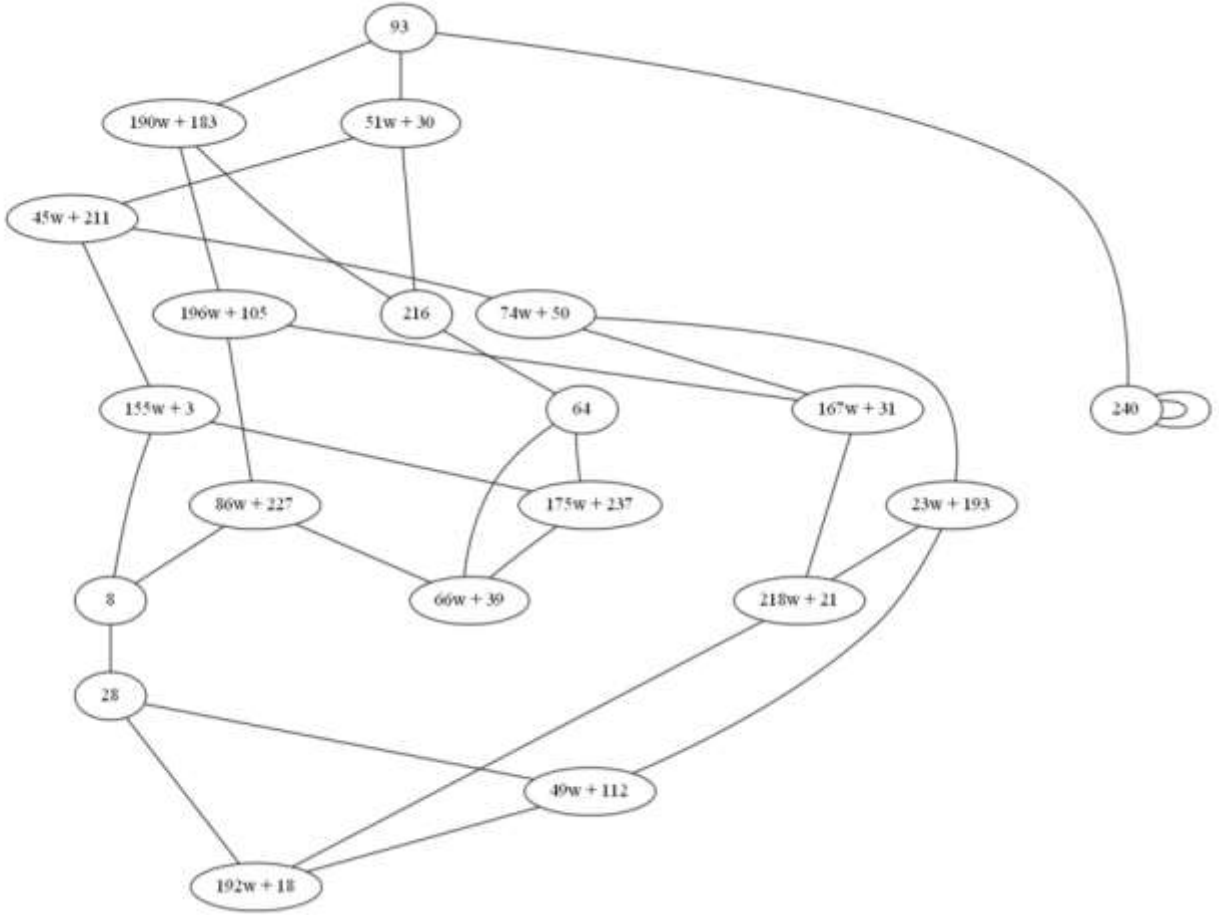
Поле GF(241^2), неприводимый многочлен : x^2+ 238 x + 7

Для кривых порядка #E = 57600 = $2^8 3^2 5^2$

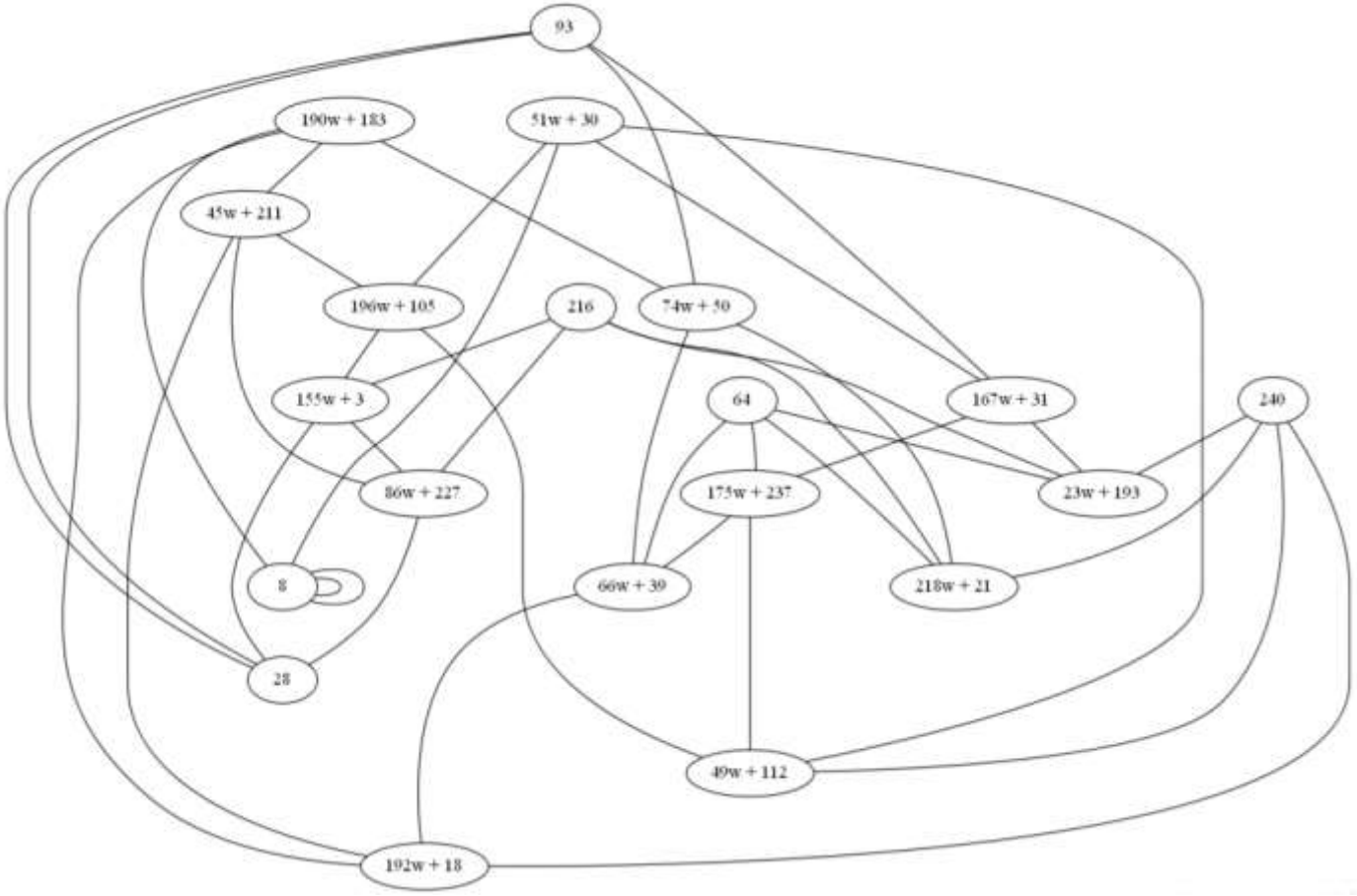
j-инварианты :

93, 51w + 30, 190w + 183, 240, 216, 45w + 211, 196w + 105, 64, 155w + 3, 74w + 50, 86w + 227, 167w + 31, 175w + 237, 66w +39, 8, 23w +193, 218w +21, 28, 49w +112, 192w +18

Степень изогении = 2



Степень изогении = 3



Подгруппа n-кручения (n-torsion subgroup):

Если при умножении точки P кривой E на n получается точка на бесконечности, то такая точка называется точкой n-кручения (n-torsion point)

Подгруппа n-кручения (n-torsion subgroup) :

$E[n] = \{ P \in E(\overline{F_q}) : n*P = \infty \}$

Эта подгруппа состоит из всех точек n-кручения

E[n] изоморфна $(Z/nZ)^2$ (т.е. имеет порядок n^2)

при $n \perp q$

Выбор поля для суперсингулярных кривых

Выбираем поле $\mathrm{GF}(p^2)$:

Для p = $l_a^{\,e_a}\ l_b^{\,e_b}\ f \pm 1$

Выбираем след Фробениуса = $2p$ или $-2p$, чтобы

$\#E = p^2+1 \pm 2\,p = (p \pm 1)^2$

и ----> $\#E = (\,l_a^{\,e_a}\ l_b^{\,e_b}\ f)^2$

$E[\,l_a^{\,e_a}\,]$ содержит $l_a^{\,e_a-1}\,(\,l_a + 1)$ цикл. подгрупп порядка $l_a^{\,e_a}$

Выбор поля для суперсингулярных кривых

Пусть l_a = 2, l_b = 3

Характеристика поля : p = $2^m 3^n f \pm 1$

Где f – небольшое число, 2^m приблизительно равно 3^n

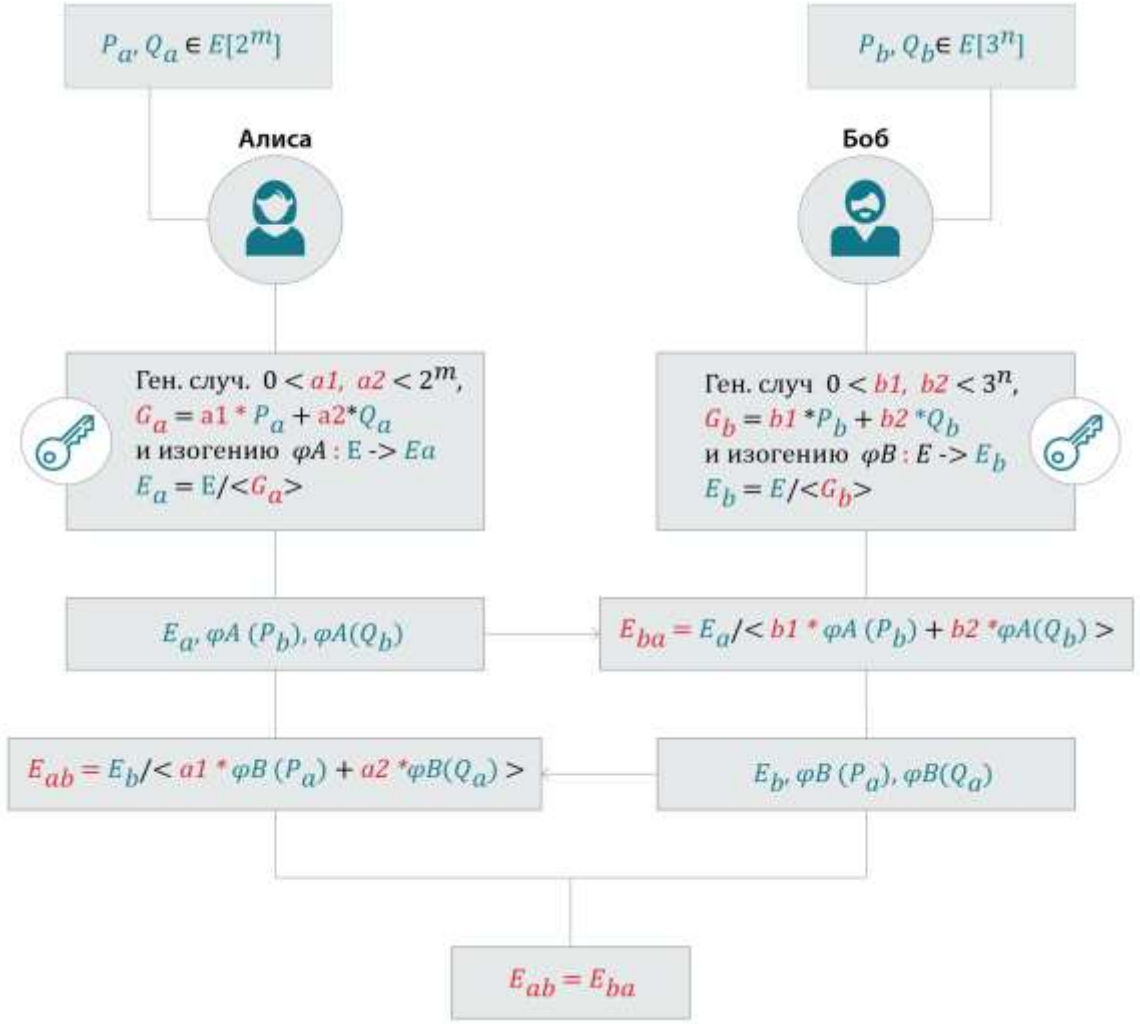
$\#E = (2^m 3^n f)^2$

Подгруппы кручения $E[2^m]$ и $E[3^n] \subseteq E(p^2)$

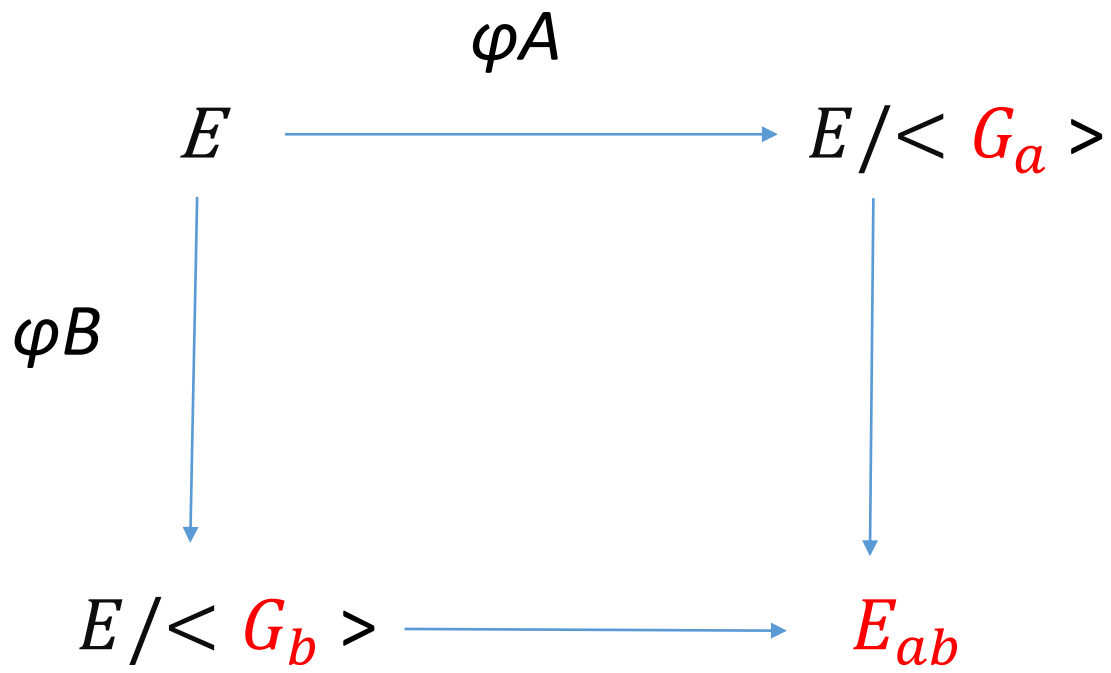
$E[2^m]$ содержит 2^{m-1} (2+1) = 3* 2^{m-1} цикл. подгрупп порядка 2^m

$E[3^n]$ содержит 3^{n-1} (3+1) = 4* 3^{n-1} цикл. подгрупп порядка 3^n

SIDH (Supersingular Isogeny Diffie-Hellman)



Почему работает SIDH ?



$$E_{ab} = E/< G_b > / < \varphi B(G_a) > = E/< G_a > / < \varphi A(G_b) >$$

Почему работает SIDH ?

Alice:

$a1*\varphi B(P_a) + a2*\varphi B(Q_a) = \varphi B(a1*P_a) + \varphi B(a2*Q_a) = \varphi B(a1*P_a + a2*Q_a) = \varphi B(G_a)$

$E_{ab} = E/< G_b > / < \varphi B(G_a) >$

Bob :

$b1*\varphi A(P_b) + b2*\varphi A(Q_b) = \varphi A(b1*P_b) + \varphi A(b2*Q_b) = \varphi A(b1*P_b + b2*Q_b) = \varphi A(G_b)$

$E_{ba} = E/< G_a > / < \varphi A(G_b) >$

$$E/< G_b > / < \varphi B(G_a) > \quad = \quad E/< G_a > / < \varphi A(G_b) >$$

Доказательство с нулевым разглашением

Алиса :

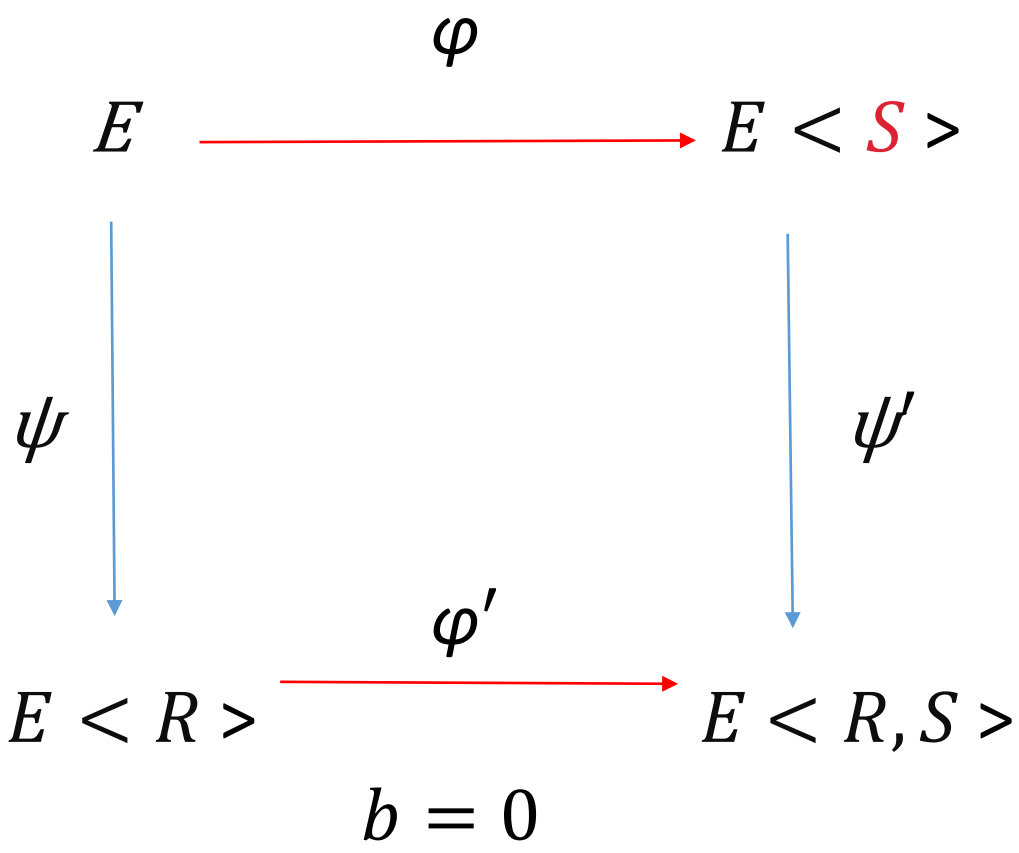
закрытый ключ: точка S

открытый ключ: кривая $E/<S>$

Алиса хочет доказать Бобу, что знает точку S , но так, чтобы не Боб не узнал S.

Для уровня безопасности λ бит необходимо выполнить λ раундов

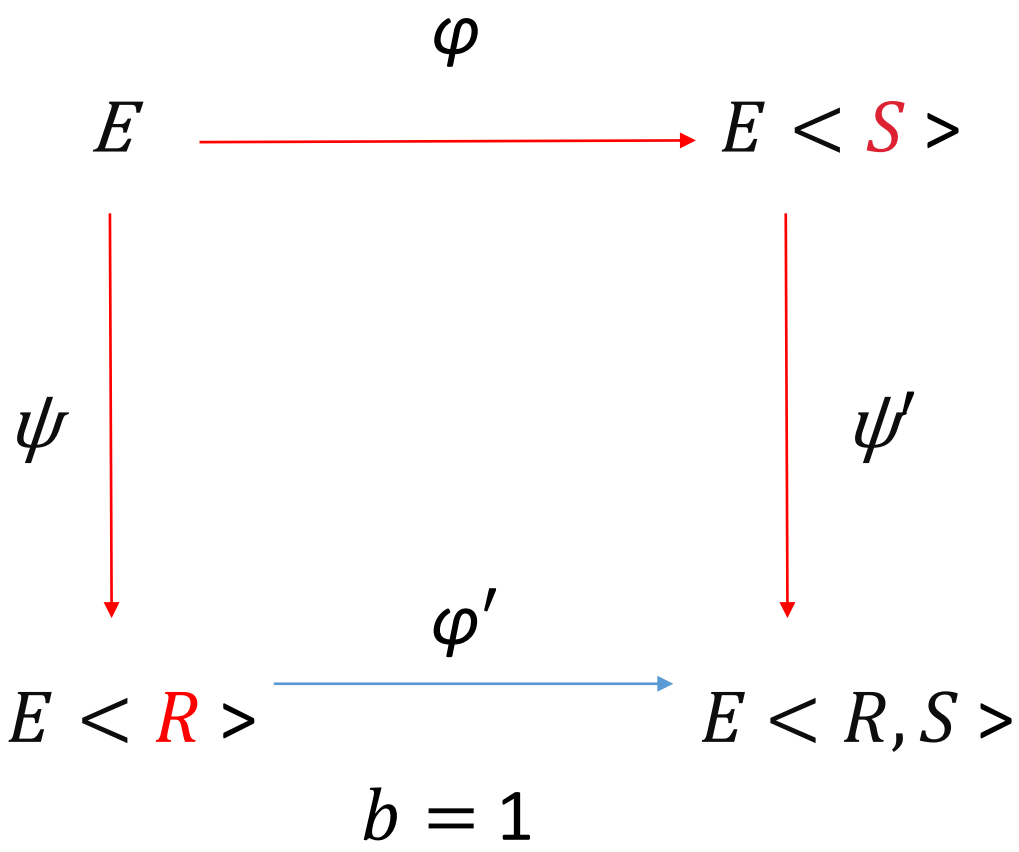
Доказательство с нулевым разглашением



для challenge $b = 0$

response : R, $\varphi(R)$

Доказательство с нулевым разглашением



для challenge $b = 1$

response : $\psi(S)$

Безопасность алгоритма

	Алиса	Боб
Классическая	$\sqrt{2^m}$	$\sqrt{3^n}$
Квантовая	$\sqrt[3]{2^m}$	$\sqrt[3]{3^n}$

Для успешной атаки надо найти путь хотя бы на одном из графов :

Квантовый уровень безопасности = min ($\sqrt[3]{2^m}$, $\sqrt[3]{3^n}$) ≈ $p^{\frac{1}{6}}$

Классический уровень безопасности = min ($\sqrt{2^m}$, $\sqrt{3^n}$) ≈ $p^{\frac{1}{4}}$

Размеры ключей

Открытый ключ :

генераторы P и Q группы кручения

коэффициенты A, B кривой

~ 8 log_2p бит

~ 6 log_2p бит (Costello , Crypto 2016)

~ 4 log_2p бит (Azarderakhsh, AsiaPKC 2016 – за счет уменьшения скорости)

Пример 1: длина характеристики поля = 768 бит:

768/6 = 128 - битный квантовый уровень безопасности

768/4 = 192 - битный классический уровень безопасности

Длина ключа 6 log_2p бит = 4608 бит = 576 байт

Длина ключа в сжатой форме 4 log_2p бит = 3072 бит = 384 байт

Размеры ключей

Пример 2: длина характеристики поля = 1536 бит:

1536 /6 = 256 - битный квантовый уровень безопасности

1536/4 = 384 - битный классический уровень безопасности

Длина ключа 6 log_2p бит = 9216 бит = 1152 байт

Длина ключа в сжатой форме 4 log_2p бит = 6144 бит = 768 байт

Реализация для PC

C. Costello и др. (Microsoft Research) “Efficient algorithms for supersingular isogeny Diffie-Hellman” 2016

Результат:

~100 млн. тактов на 3,4 Ггц Intel Haswell для одной из сторон

(для 128-битного квантового уровня безопасности: характеристика $p = 2^{372} 3^{239} - 1$,

т.е. $p \sim 2^{768}$)

Используется кривые Монтгомери и проективные координаты

Реализация для ARMv7

R. Azarderaksh, D. Jao и др “NEON-SIDH: Efficient implementation of supersingular isogeny Diffie-Hellman Key Exchange protocol on ARM” 2016

Результаты для чипа Beagle Board Black Cortex-A8 на частоте 1 Ггц

1,5 сек. для p~ 2^{768} (128-битного квантового уровня безопасности) :

Если задействовать SIMD-инструкции NEON:

0,2 сек. для p~ 2^{768} (128-битного квантового уровня безопасности) :

Вопросы

Спасибо за внимание!