Оптимизация перспективных постквантовых алгоритмов на малоресурсных микроконтроллерах

ОЛЕГ ТАРАСКИН

ЗАО “АКТИВ-СОФТ”

Постквантовые алгоритмы

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

Краткая история

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

2016:

“Efficient algorithms for supersingular isogeny Diffie-Hellman”

Craig Costello and Patrick Longa and Michael Naehrig

Области применения изогений

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

Защита от атак по побочным каналам.

Исследования стойкости кривых, методом приведения

Аналог Диффи-Хеллмана

ЭЦП

Эллиптические кривые

GF(p^n), p - характеристика

для p > 3 сокр. форма Вейерштрасса :

Элл. кривая E : $y^2 = x^3 + Ax + B$

где $4A^3 + 27B^2$ не равно 0

j–инвариант кривой E :

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

У изоморфных кривых над одним полем j–инварианты равны.

Эллиптические кривые

порядок группы точек кривой E :

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

где 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 $GF(GF(p^{n*k}))$, где *к* - небольшое натуральное число.

Суперсингулярные и даже “гладкого” порядка кривые можно использовать в криптосистемах с изогениями:

Безопасность изогений не зависит от сложности решения ECDLP использующихся в них кривых. Скорее – наоборот !

Эллиптические кривые

Подгруппа кручения (torsion subgroup) порядка n :

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

$E[n]$ изоморфна $(\mathrm{Z}/\mathrm{nZ})^2$ при $\mathrm{n} \perp q$

Изогении

Пусть E1 и E2 элл. кривые над полем F

Изогенией E1 → E2 над F называется неконстантное рациональное отображение над F,

которое также является групповым гомоморфизмом

$(x,\ y)$ -----> $(\frac{f1(x,y)}{f2(x,y)}, \frac{g1(x,y)}{g1(x,y)})$, где $f1, f2, g1, g2$ – полиномы

Степенью изогении называется степень рационального отображения

(в случае сепарабельной изогении она равна порядку ядра гомоморфизма)

Теорема Tate :

Две кривые изогенны тогда и только тогда, когда порядки их групп равны.

Пример

F = GF(29) , E1: $y^2 = x^3 + 9x + 19$

E2: $y^2 = x^3 + 5$

#E1 = #E2 = 30

$(x, y) \longrightarrow \left(\frac{x^3 + 13x^2 + 2x + 8}{x^2 + 13x + 6}, \frac{x^3y + 5x^2y - 7xy - 3y}{x^3 + 5*x^2 - 11x + 10}\right)$

Степень изогении = 3

Ядро изогении – подгруппа порядка 3

Изогении

Эндоморфизм – это изогения кривой на саму себя.

Примеры:

Скалярное умножение точки

Эндоморфизм Фробениуса для кривой E над полем GF(p^n) :

$$(x, y) \longrightarrow (x^p, y^p)$$
$$\infty \longrightarrow \infty$$

Алгоритм Velu (1971)

Вход: кривая $y^2 = x^3 + Ax + B$, подгруппа C

Выход: изогенная кривая и рациональное отображение

Сложность : O(#H)

1. Отбрасываем точку на бесконечности
2. C_2 - мн-во точек кручения порядка 2 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

Даны две изогенные кривые E1 и E2.

Требуется найти изогению между ними.

Обычные элл. кривые:

Классическая атака: O($q^{1/4}$) Galbraith, Hess, Smart (GHS – атака 2002 г)

Атака на квантовом компьютере: (субэкспоненциальная) Childs, Jao, Soukharev 2010 г

Суперсингулярные элл. кривые над полем GF(p^2):

Классическая атака: O($p^{1/4}$)

Атака на квантовом компьютере: O($p^{1/6}$)

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.

Для простого числа l существует $l + 1$ изогений эллиптических кривых степени l в расширении поля K

Граф изогений суперсингуляных кривых

Пример :

P = 241 #J-inv = 20 (~241/12)

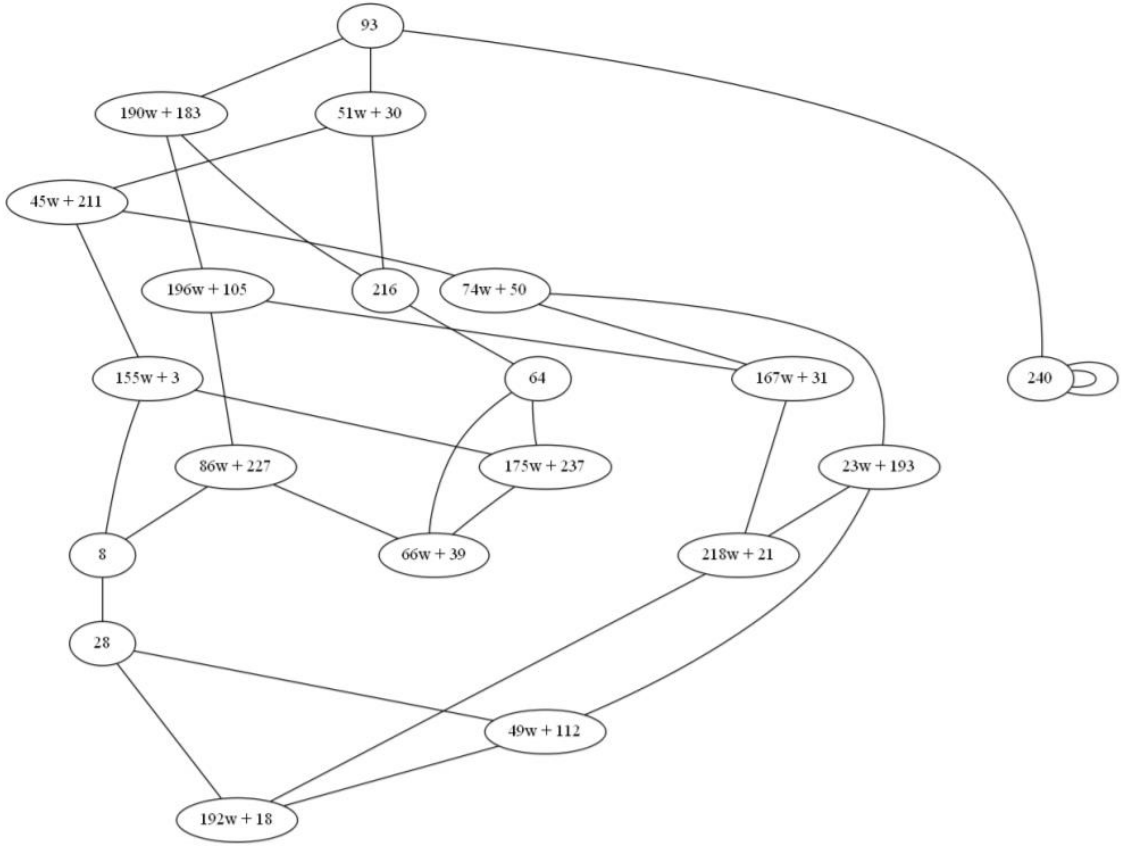
GF(241^2), неприводимый многочлен : x^2+ 238 x + 7

Множество j-инвариантов :

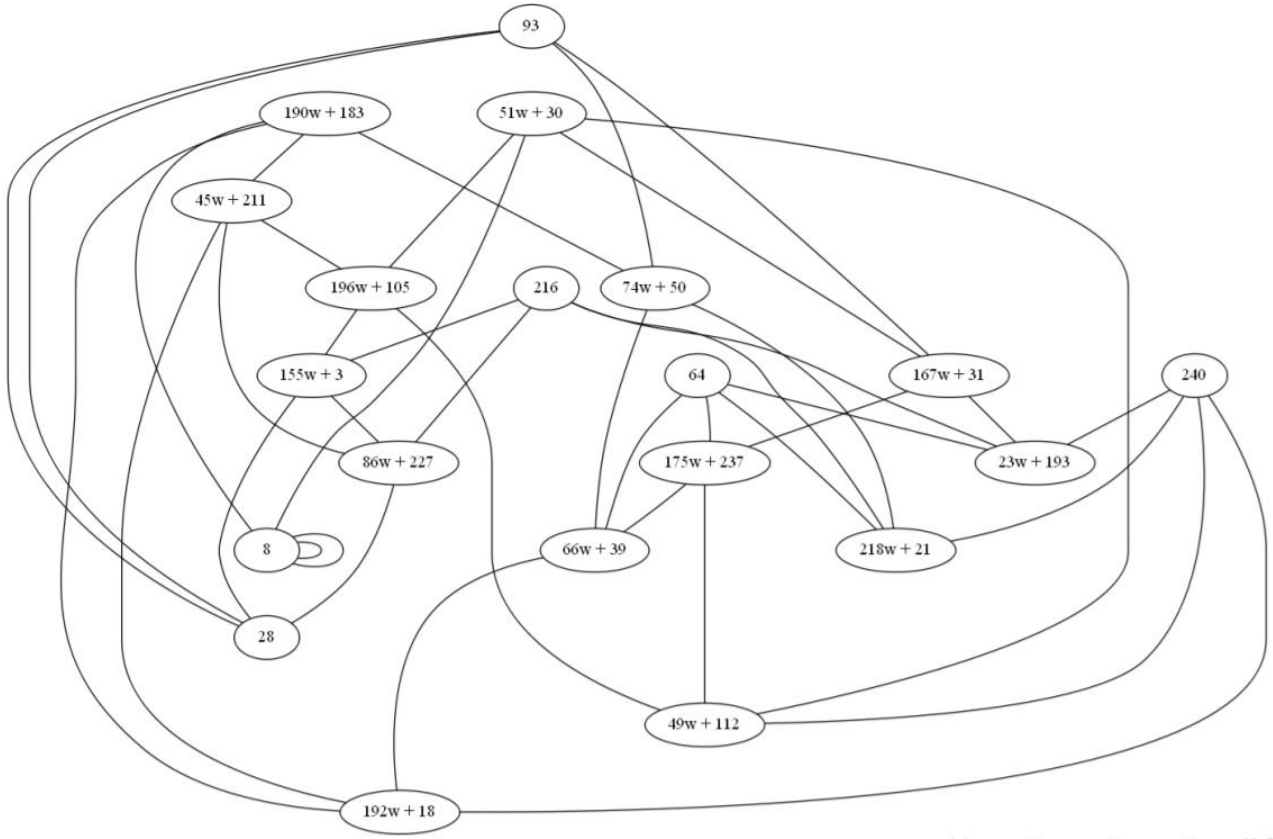
93, 51w + 30, 190w + 183, 240, 216, 45w + 211, 196w + 105, 64, 155w + 3, 74w + 50, 86w + 227,

167w + 31, 175w + 237, 66w +39, 8, 23w +193, 218w +21, 28, 49w +112, 192w +18

Степень = 2


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

Степень = 3


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

Выбор поля для суперсингулярных кривых

Выбираем поле $\mathrm{GF}(p^2)$

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

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

$E[\ l_a^{\,e_a}\ ]$ 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

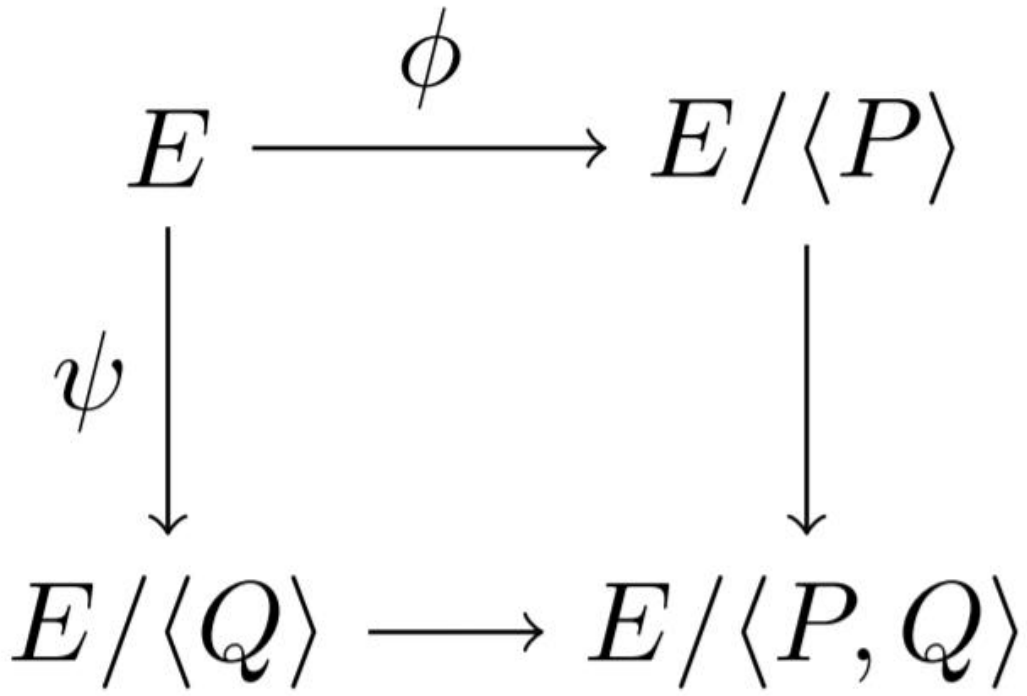
$\#E = (2^m 3^n f)^2$

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

Коммутативная диаграмма



SIDH (supersingular isogeny Diffie-Hellman) Jao, De Feo (2011)

$P_a, Q_a \in E[2^m]$

Алиса

Ген. случ. $0 < a1, a2 < 2^m$,

$G_a = a1 * P_a + a2 * Q_a$

и изогению $\varphi A : E \rightarrow E_a$

$E_a = E/\langle G_a \rangle$

$P_b, Q_b \in E[3^n]$

Боб

Ген. случ $0 < b1, b2 < 3^n$

$G_b = b1 * P_b + b2 * Q_b$

и изогению $\varphi B : E \rightarrow E_b$

$E_b = E/\langle G_b \rangle$

$E_a, \quad \varphi A(P_b), \quad \varphi A(Q_b)$ --------->

<---------$E_b, \quad \varphi B(P_a), \quad \varphi B(Q_a)$

$E_{ab} = E_b/\langle a1 * \varphi B(P_a) + a1 * \varphi B(Q_a) \rangle$

$E_{ba} = E_b/\langle b1 * \varphi A(P_b) + b2 * \varphi A(Q_b) \rangle$

$E_{ab} = E_{ba}$

Безопасность алгоритма

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

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

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

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

Вычисление изогений степени l^e

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

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

φ_0 = E, P_0 = P

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

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 :

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

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

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

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

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

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

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 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 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~ 2^{768})

Половину времени занимает вычисление эфемеральных ключей.

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) :

3,2 сек. для p~ 2^{1024} (170-битного квантового уровня безопасности)

Если задействовать SIMD-инструкции NEON:

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

1,6 сек. для p~ 2^{1024} (170-битного квантового уровня безопасности)

Используется кривые Монтгомери и афинные координаты (на ARM I/M ~ 6)

Спасибо !