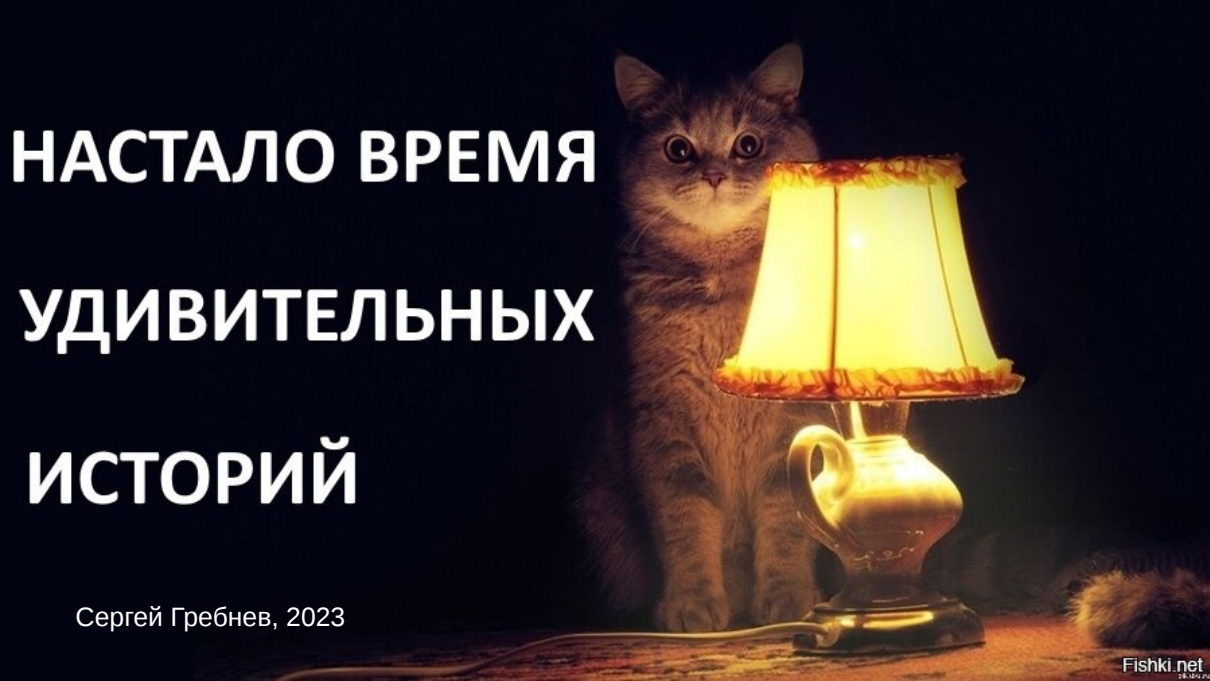
НАСТАЛО ВРЕМЯ УДИВИТЕЛЬНЫХ ИСТОРИЙ



Сергей Гребнев, 2023

QApp

Классическая криптография с открытым ключом

Диффи-Хеллман-Меркль, 1976

$x, A = g^x$ $\xrightarrow{A}$ $\xleftarrow{B}$ $B^x = g^{xy} = A^y$ $y, B = g^y$

RSA, 1978

$N = pq$; e, d :
$ed \equiv 1 \pmod{\phi(N)}$ $\overset{N,e}{\rightsquigarrow}$ $\xleftarrow{c}$ $c = m^e \pmod{N}$
$m = c^d \pmod{N}$.

QApp

История постквантовой криптографии

- 2003 год: Д. Бернштейн предлагает термин ``постквантовая криптография''
- 2006 год: первая конференция PQCrypto
- 2014 год: меморандум ЕС ``Horizon 2020''
- 2015 год: меморандум АНБ о переходе на постквантовые алгоритмы
- 2017 год: объявлен конкурс NIST
- 2019 год: старт проекта в России
- 2020 год: конкурс CACR
- 2023 год: определены результаты конкурса NIST

QApp

``Конкурс'' NIST-PQ

30 ноября 2017 г. -- закончен прием заявок.
Апрель 2018 г. -- рабочая встреча по презентации предложений и заявок.
30 января 2019 г. -- опубликованы результаты I этапа.
30 марта 2019 г. -- доработка схем, прошедших во II этап, с учетом поступивших замечаний.
июль 2020 г. -- старт III этапа
июль 2022 г. -- финиш III этапа
июль 2023 г. -- старт дополнительных этапов для KEM и подписи

QApp

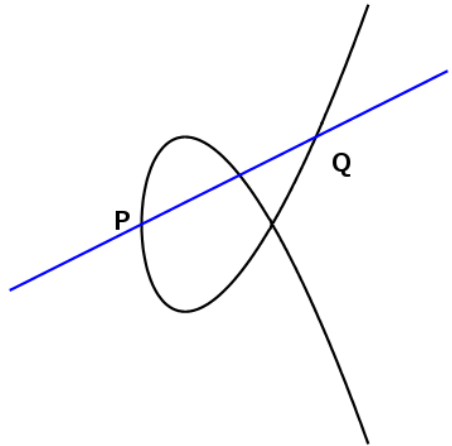
Основные подходы к синтезу

- Использование теории целочисленных решеток.
- Использование кодов, исправляющих ошибки.
- Использование многочленов от многих переменных.
- Использование криптографических хэш-функций.
- Использование изогений на суперсингулярных эллиптических кривых.
- ``Эзотерика'' (проблемы сопряженного поиска (search problem) или операции в группах кос (braid groups), алгебра октонионов, многочлены Чебышёва и т.д)

QApp

Эллиптические кривые

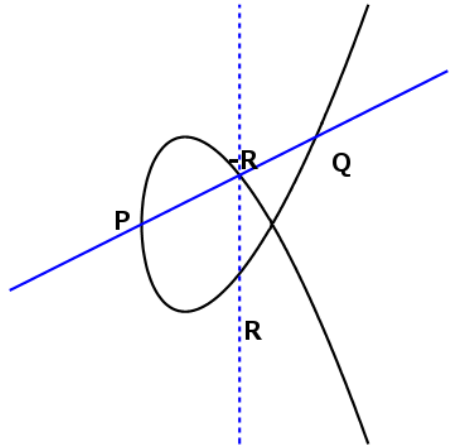
$$E(\mathbb{Z}/p\mathbb{Z}) = \{(x,y) : y^2 = x^3 + ax + b \pmod{p}\} \cup \{\mathcal{O}\}$$



QApp

Эллиптические кривые

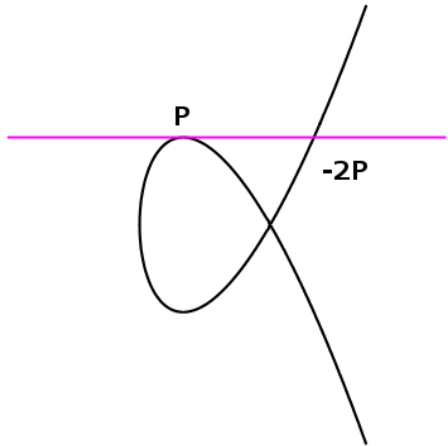
$$E(\mathbb{Z}/p\mathbb{Z}) = \{(x,y) : y^2 = x^3 + ax + b \pmod{p}\} \cup \{\mathcal{O}\}$$



QApp

Эллиптические кривые

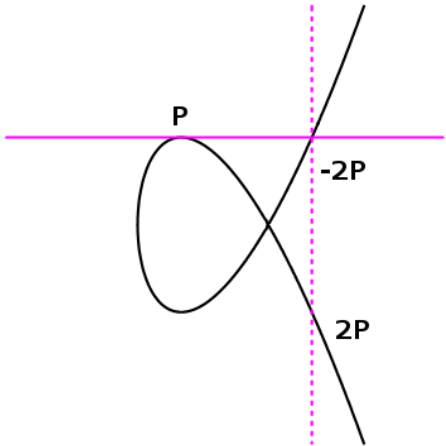
$$E(\mathbb{Z}/p\mathbb{Z}) = \{(x,y) : y^2 = x^3 + ax + b \pmod{p}\} \cup \{\mathcal{O}\}$$



QApp

Эллиптические кривые

$$E(\mathbb{Z}/p\mathbb{Z}) = \{(x,y) : y^2 = x^3 + ax + b \pmod{p}\} \cup \{\mathcal{O}\}$$



QApp

Эллиптические кривые

$$E(\mathbb{Z}/p\mathbb{Z}) = \{(x,y) : y^2 = x^3 + ax + b \pmod p\} \cup \{\mathcal{O}\}$$

Относительно этого закона эллиптическая кривая образует абелеву группу.
Кратная точка: $[k]P = \underbrace{P + \cdots + P}_{k \text{ раз}}$.

DLP: для $P, Q \in E(GF(p))$: найти $x \in [0, m] : [x]P = Q$, если он существует.

j-инвариант кривой $j(E) = \frac{1728(4a^3)}{4a^3+b^2}$

Н. Коблиц, В. Миллер, 1986: криптографические приложения.

П. Шор, 1994: полиномиальный квантовый алгоритм.

QApp

Изогении

Что такое изогения?
$\phi : E \to E'$,

- Групповой морфизм
- с конечным ядром ($H \subseteq E$)
- сюръективна в алгебраическом замыкании
- задается рациональным отображением степени $\#H$

E_1, E_2 -- кривые над K, тогда изогения -- отличный от константы гомоморфизм $\alpha : E_1 \to E_2$, заданный рациональными ф-циями:

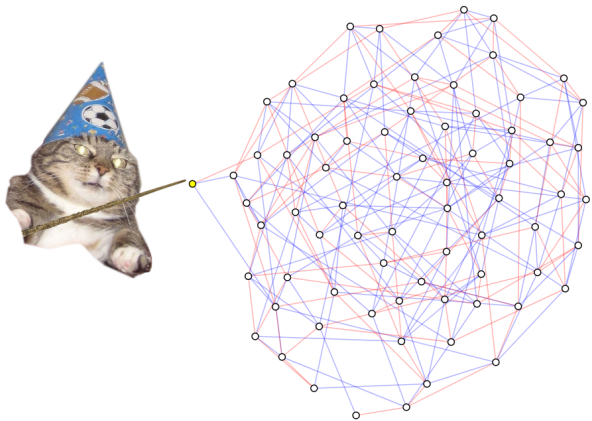
- $\alpha(P+Q) = \alpha(P) + \alpha(Q) \forall P, Q \in E(\overline{K})$;
- $x_2 = R_1(x_1, y_1); y_2 = R_2(x_1, y_1)$ для всех (кроме конечного мн-ва) $(x_1, y_1) \in E_1(\overline{K})$.

QApp

Пример

$p = 2^5 \cdot 3^3 - 1 = 863$; 73 суперсингулярных j-инварианта.

2-изогении, 3-изогении, $E_0 : y^2 = x^3 + x$.



(c) https://isogenies.enricflorit.com/visualizations/graph.html

QApp

Немного истории

1997: Couveignes --- Hard Homogenous Spaces
2006: Charles-Goren-Lauter, хэш
2006: Rostovtsev--Stolbunov, ординарные ЭК
2010: Jao, Soukharev -- субэкспоненциальный квантовый алгоритм
2011: Jao, de Feo --- SIDH
2017: первая подпись
2017: SIKE
2018: CSIDH, SeaSIGN, CSI-Fish
2020: O-SIDH, Seta, SQISign
2022: Castryk-Decru (Kani, 1997); Maino-Martindale; Robert
2023: SQISign
`https://ellipticnews.wordpress.com/2022/08/12/attacks-on-sidh-sike/`

QApp

Параметры

Возьмем простое число p вида $p = l_A^{e_A} l_B^{e_B} \cdot f \pm 1$, где l_A, l_B -- маленькие простые (например, 2 и 3), $(l_A, f) = (l_B, f) = 1$, поле $GF(p^2)$. Построим суперсингулярную кривую $E(GF(p^2))$, мощность группы точек кривой которой равна $(l_A^{e_A} l_B^{e_B})^2$. По построению $E[l_A^{e_A}]$ содержит $l_A^{e_A - 1}(l_A + 1)$ циклических подгрупп порядка $l_A^{e_A}$, каждая из которых определяет собственную изогению (т.е. ядром которой она является), аналогичное замечание верно и для $E[l_B^{e_B}]$.

QApp

SIDH

В основе протокола лежит следующая коммутативная диаграмма:

$$\begin{array}{ccc} E & \xrightarrow{\varphi} & E/\langle P \rangle \\ \psi \downarrow & & \downarrow \\ E/\langle Q \rangle & \longrightarrow & E/\langle P, Q \rangle \end{array} \tag{1}$$

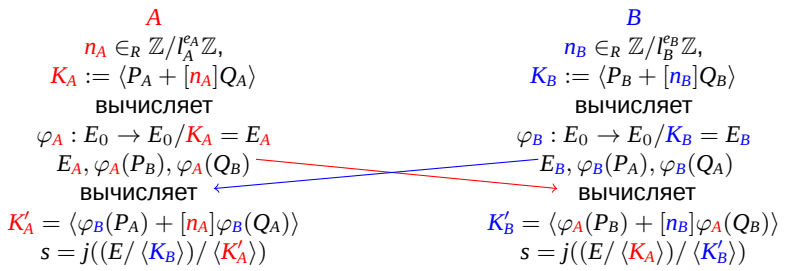
где φ, ψ -- случайные пути в графах изогений степеней l_A, l_B соответственно. Стойкость протокола основана на сложности нахождения пути, соединяющего две вершины в графе.

QApp

SIDH

Открытые параметры:

- большое простое $p = l_A^{e_A} l_B^{e_B} \cdot f - 1$ и суперсингулярная $E_0(GF(p^2))$
- базисы $\{P_A, Q_A\}$ и $\{P_B, Q_B\}$ групп $E_0[l_A^{e_A}]$ и $E_0[l_B^{e_B}]$



QApp

Тотальный перебор

Поскольку в $E(GF(p^2))$ имеется $(l+1)l^{e-1}$ циклических подгрупп порядка l^e (опускаем индексы), то тотальный перебор занимает $O(l^e)$ или $O(p^{1/2})$ опробований.

QApp

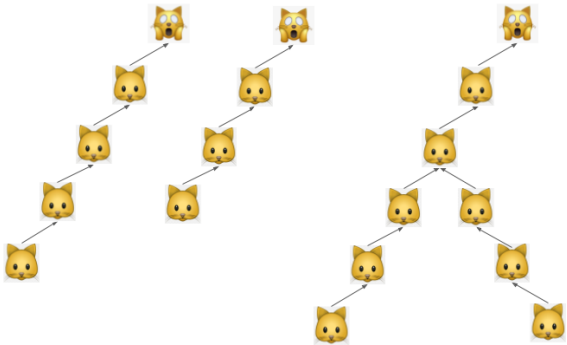
MITM

Пусть e четное. Строим два дерева таких, что листья первого определяют классы изоморфизмов кривых, $l^{e/2}$-изогенных E; листья второго -- классы изоморфизмов кривых, $l^{e/2}$-изогенных E/G (напоминание: мы ищем генератор G или изогению $\phi : E \to E/G$)
В каждом наборе по $(l+1)l^{e/2-1}$ классов; с большой вероятностью единственный класс содержится в их пересечении. Найдя его, строим ϕ как композицию изогении из E и двойственной к изогении из E/G.
Память -- $O(p^{1/4})$, время -- $O(p^{1/4})$.
(Adj et al., eprint 2018/313)

QApp

Метод ван Ооршота -- Винера

Общий метод поиска коллизий, адаптированный к CSSI.



QApp

Метод ван Ооршота -- Винера

Оценки трудоемкости:

$$T = \frac{2.5}{m}\sqrt{|S|^3/w}\cdot t;$$

m -- кол-во процессоров, $|S|$ -- мощность мн-ва определения итерационной ф-ции, w -- объем памяти, t -- трудоемкость итерационной ф-ции.

В нашем случае $|S| \approx p^{1/2}$, т.о. $O\left(\frac{p^{3/8}}{m\ w^{1/2}}t\right)$.

Вывод: метод ван Ооршота--Винера --- наилучший.
(Costello et al., eprint 2019/298)

QApp

Квантовый вычислитель

Алгоритм поиска зацеплений (claw) (Tani): пусть $g_1 : X_1 \to Y$, $g_2 : X_2 \to Y$, найти такие x_1, x_2: $g_1(x_1) = g_2(x_2)$.
Пусть $\#X_1 \approx \#X_2 \approx N$, $\#Y \gg N$, тогда время работы -- $O(N^{2/3})$.
У нас X_1 -- множество $l^{e/2}$-изогений из $E = E_1$; X_2 -- множество $l^{e/2}$-изогений из $E/G = E_2$, $g_i(\phi) = j(\phi(E_i))$. Имеем $\#X_1 = \#X_2 \approx p^{1/4}$, отсюда время -- $O(p^{1/6})$ (и память $O(p^{1/6})$).
Метод Гровера: время -- $O(p^{1/4})$, память -- $O(1)$.
(Jacques et Schanck, eprint 2019/103)

QApp

Несбалансированные простые

Рассмотрим l_A, l_B, e_A, e_B; положим $A = l_A^{e_A}$, $B = l_B^{e_B}$, тогда:

- $B > A^2 > p^2$ или $B > A^3 > p^{3/2}$: полиномиальная атака;
- небольшой дисбаланс -- улучшение в классических атаках;
- при $B > A^2$ -- существуют слабые стартовые кривые.

(Kutas et al., eprint 2020/633)

QApp

Случай долговременного ключа

Пусть B имеет долговременный ключ $E_B = E/\langle P_B + [\beta]Q_B\rangle$. Пусть φ_X -- изогения A, $R = \varphi_X(P_B)$, $S = \varphi_X(Q_B)$. Пусть A знает K_i, $0 < K_i < l_2^i$, т.ч. $\beta = K_i + l_2^i z$, и пусть z_0 -- предположение о $z \pmod{l_2}$. Атака состоит в выборе $R' = R + [-l_2^{m-1-i}K_i - l_2^{m-1}z_0]S$ и $S' = [1 + l_2^{m-i-1}]S$ и отправке $\{E_X, R', S'\}$ абоненту B.
B вычисляет

$$R' + [\beta]S = \cdots = (R + [\beta]S) + [(z - z_0)l_2^{m-1}]S,$$

полученное ядро корректно iff $z \equiv z_0 \pmod{l_2}$. После $(l_2 - 1)e_2$ сеансов секретный ключ восстановлен.
(Galbraith et al., eprint 2016/859)

QApp

Итак

Attacks

Name	Complexity	Quantum?	References	Additional Information
MITM	$\exp(n)^{1/2}$	No	JDF11	▷ Comment
Tani	$\exp(n)^{1/3}$	Yes	Tan07	▷ Comment
vOW	$\exp(n)^{3/4}$	No	vOW99 AC+18	▷ Comment
Castryck-Decru	$\tilde{O}(n^3)$	No	CD22	▷ Comment
CDMM	$L(1/2)$	No	CD22 MM22	▷ Comment
Robert	$\tilde{O}(n^8)$	No	Rob22	▷ Comment
BJS	$\exp(n)^{1/4}$	Yes	BJS14	▷ Comment
DG	$\exp(n)^{1/2}$	No	DG13	▷ Comment
Kuperberg	$L(1/2)$	Yes	Kup04 CJS13	▷ Comment
Galbraith	$\exp(n)^{1/2}$	No	Gal99 GHS01	▷ Comment
Dartois-De Feo	$\exp(n)^{0.292}$	No	DD21	▷ Comment

https://issikebrokenyet.github.io/

QApp

Введение

MPKC: Multivariate Public Key Cryptosystem
Открытый ключ: нелинейная система многочленов от нескольких переменных

$$
\begin{aligned}
p^{(1)}(x_1,\ldots,x_n) &= \sum_{i=1}^{n}\sum_{j=1}^{n} p_{ij}^{(1)} \cdot x_i x_j + \sum_{i=1}^{n} p_i^{(1)} x_i + p_0^{(1)} \\
p^{(2)}(x_1,\ldots,x_n) &= \sum_{i=1}^{n}\sum_{j=1}^{n} p_{ij}^{(2)} \cdot x_i x_j + \sum_{i=1}^{n} p_i^{(2)} x_i + p_0^{(2)} \\
&\vdots \\
p^{(m)}(x_1,\ldots,x_n) &= \sum_{i=1}^{n}\sum_{j=1}^{n} p_{ij}^{(m)} \cdot x_i x_j + \sum_{i=1}^{n} p_i^{(m)} x_i + p_0^{(m)}
\end{aligned}
$$

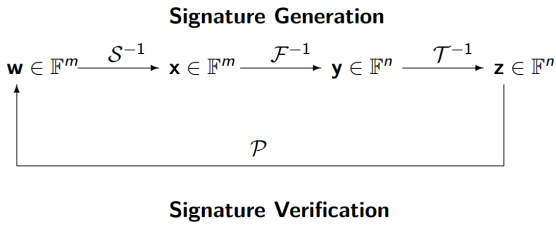
QApp

Построение

- Легко обратимое квадратичное отображение $\mathcal{F} : \mathbb{F}^n \to \mathbb{F}^m$
- два обратимых аффинных (линейных) отображения $\mathcal{S} : \mathbb{F}^m \to \mathbb{F}^m$ и $\mathcal{T} : \mathbb{F}^n \to \mathbb{F}^n$
- открытый ключ $\mathcal{P} = \mathcal{S} \circ \mathcal{F} \circ \mathcal{T}$ -- выглядит как случайная система
- секретный ключ $\mathcal{S}, \mathcal{F}, \mathcal{T}$

QApp

Схема подписи ($m \leq n$)



- **Выработка подписи** Для документа $d \in \{0,1\}^*$ вычислить хэш $w = H(d) \in \mathbb{F}^m$ и вычислить поочередно $x = \mathcal{S}^{-1}(w)$, $y = \mathcal{F}^{-1}(x)$, $z = \mathcal{T}^{-1}(y)$. Подписью становится $z \in \mathbb{F}^n$.
- **Проверка подписи** Вычислить хэш $h = H(d) \in \mathbb{F}^m$, вычислить $h' = \mathcal{P}(z)$. Подпись верна, если $h = h'$.

QApp

Схемы типа Unbalanced Oil-vinegar (UOV)

- $F = (f_1(x_1, \ldots, x_o, x'_1, \ldots, x'_v), \ldots, f_o(x_1, \ldots, x_o, x'_1, \ldots, x'_v))$
- $f_l(x_1, \ldots, x_o, x'_1, \ldots, x'_v) = \sum a_{lij} x_i x'_j + \sum b_{lij} x'_i x'_j + \sum c_{li} x_i + \sum d_{li} x'_i + e_l$

Переменные разбиты на две группы:
``Масло'': $x_1, \ldots, x_o$
``Уксус'': $x'_1, \ldots, x'_v$

QApp

Обращение UOV-отображения

$$f_l(x_1, \ldots, x_o, \underbrace{x'_1, \ldots, x'_v}_{\text{фиксируем переменные}}) =$$

$$= \sum a_{lij} x_i x'_j + \sum b_{lij} x'_i x'_j + \sum c_{li} x_i + \sum d_{li} x'_i + e_l$$

QApp

Обращение UOV-отображения

$$f_l(x_1, \ldots, x_o, x'_1, \ldots, x'_v) =$$

$$= \sum a_{lij} x_i x'_j + \sum b_{lij} x'_i x'_j + \sum c_{li} x_i + \sum d_{li} x'_i + e_l$$

Для подписи нужно решить простую линейную систему.

QApp

Обращение UOV-отображения

$$f_l(x_1, \ldots, x_o, x'_1, \ldots, x'_v) =$$

$$= \sum a_{lij} x_i x'_j + \sum b_{lij} x'_i x'_j + \sum c_{li} x_i + \sum d_{li} x'_i + e_l$$

Система линейная относительно ``масляных'' переменных $x_1, \ldots, x_o$

QApp

Схема ЦП Rainbow

- $\mathbb{F} = GF(q)$; целые числа $0 < v_1 < v_2 < \cdots < v_u < v_{u+1} = n$
- множества $V_i = \{1, \ldots, v_i\}$ и $O_i = \{v_i + 1, \ldots, v_{i+1}\} (i = 1, \ldots, u)$. при этом $|V_i| = v_i, |O_i| = v_{i+1} - v_i := o_i$
- Центральное отображение $\mathcal{F}$ состоит из $m := n - v_1$ многочленов $f^{(v_1+1)}, \ldots, f^{(n)}$ вида

$$f^{(k)}(x_1, \ldots, x_n) = \sum_{i,j \in V_l} \alpha_{ij}^{(k)} x_i x_j + \sum_{i \in V_l, j \in O_l} \beta_{ij}^{(k)} x_i x_j + \sum_{i \in V_l \cup O_l} \gamma_i^{(k)} x_i + \delta^{(k)},$$

  где l -- единственное целое такое, что $k \in O_l$
- два обратимых аффинных (линейных) отображения $\mathcal{S} : \mathbb{F}^m \to \mathbb{F}^m$ и $\mathcal{T} : \mathbb{F}^n \to \mathbb{F}^n$
- открытый ключ $\mathcal{P} = \mathcal{S} \circ \mathcal{F} \circ \mathcal{T}$
- секретный ключ $\mathcal{S}, \mathcal{F}, \mathcal{T}$

QApp

Выработка подписи

Для заданного сообщения $d \in \{0,1\}^*$:

1. Вычислить хэш $H : \{0,1\}^* \to \mathbb{F}^m$, $w = H(d)$
2. вычислить $x = \mathcal{S}^{-1}(w)$
3. подставить вместо ``уксусных'' переменных случайные значения в $f^{(v_1+1)}, \ldots, f^{(n)}$
4. для $i := 1$ до u решить линейную систему, заданную $f^{(v_i+1)}, \ldots, f^{(v_{i+1})}$, получить значения $y_{v_i+1}, \ldots, y_{v_{i+1}}$ и подставить их в многочлены $f^{(v_{i+1}+1)}, \ldots, f^{(n)}$
5. положить $y = (y_1, \ldots, y_n) \in \mathbb{F}^n$
6. вычислить подпись $z \in \mathbb{F}^n$, $z = \mathcal{T}^{-1}(y)$.

QApp

Проверка подписи

Для заданного сообщения $d \in \{0,1\}^*$, подписи $z \in \mathbb{F}^n$:

1. вычислить $w' = \mathcal{P}(z) \in \mathbb{F}^m$
2. вычислить $w = H(d) \in \mathbb{F}^m$
3. Если $w = w'$, то подпись принимается.

QApp

О стойкости Rainbow

Нарушитель, который хочет подделать электронную подпись, имеет следующую информацию:

- Исходное сообщение M и, как следствие, значение

$$(e_1, \ldots, e_o) = H(M).$$

- Набор многочленов $\mathcal{P} = \{p_1, \ldots, p_o\} \in \mathbb{F}_q[x_1, \ldots, x_n]$.

QApp

О стойкости Rainbow

В самом простом случае подделка подписи эквивалентна поиску решения $x_1, \ldots, x_n$, удовлетворяющего условию

$$p_k(x_1, \ldots, x_n) = e_k, \quad k = 1, \ldots, o, \tag{2}$$

или, в векторной записи, $\mathcal{P}(x) = e$.
Поскольку $n = o + v$ и $v > 1$, то число уравнений меньше, чем число неизвестных, а рассматриваемая система может иметь пространство решений размерности $n - o$.
Поскольку поле $\mathbb{F}_q$ конечно, то можно реализовать алгоритм тотального опробования, в котором перебираются все возможные значения переменных $x_1, \ldots, x_n$. Сложность такого алгоритма оценивается величиной

$$O(q^n on)$$

операций в поле $\mathbb{F}_q$.

QApp

Обзор атак на Rainbow

Общие атаки: задача сводится к задаче MQ: для заданного квадратичного отображения $\mathcal{P}(x) : \mathbb{F}_q^n \to \mathbb{F}_q^m$ и $t \in \mathbb{F}_q^m$ найти s т.ч. $\mathcal{P}(s) = t$
NP-сложная задача. Методы, основанные на базисах Гребнера: F_4, F_5, XL.

QApp

Rank Attacks: MinRank

Для заданных m матриц размера $n \times n$ $P_1, \ldots, P_m$ найти линейную комбинацию $H = \sum_{i=1}^{m} \lambda_i P_i$ с рангом $\leq r$.
В случае Rainbow, это матрицы $P_1, \ldots, P_m$ публичных полиномов как квадратичных форм. Найдя o_1 таких линейных комбинаций, мы можем отделить 1-й ``слой'', а затем и остальные.
Трудоемкость атаки:

$$o_1 q^{v_1+1} \left(\frac{m^3}{3} - \frac{m^2}{6} \right).$$

QApp

Rank Attacks: MinRank

Algorithm 5.5 MinRank attack

Input: matrices $P^{(v_1+1)}, \ldots, P^{(n)}$
Output: Linear combination $C = \sum_{i=v_1+1}^{n} c_i \cdot P^{(i)}$ of rank $\leq v_2$

1: **repeat**
2: Choose randomly a vector $\lambda \in \mathbb{F}^m$ and compute $P = \sum_{i=v_1+1}^{n} \lambda_i P^{(i)}$.
3: **if** Rank $(P) > 1$ and Rank$(P) < n$ **then**
4: Choose randomly a vector γ from ker(P).
5: $C \leftarrow \sum_{i=v_1+1}^{n} \gamma_i P^{(i)}$
6: **end if**
7: **until** Rank $(C) \leq v_2$
8: **return** C

Jintai Ding, Albrecht Petzoldt, Dieter S. Schmidt. ``Multivariate Public Key Cryptosystems''

QApp

Rank Attacks: HighRank

``Масляные'' подпространства:

$$\mathcal{O}_i = \{x \in \mathbb{F}^n : x_1 = \cdots = x_{v_i} = 0\};$$

$$\mathcal{O}_u \subset \mathcal{O}_{u-1} \subset \cdots \subset \mathcal{O}_1 \subset \mathbb{F}^n;$$

$$\forall F^{(k)}, k \in O_i, \forall x \in \mathcal{O}_i, x^T \cdot F^{(k)} \cdot x = 0.$$

$$\mathcal{O}_i \subset \ker F^{(k)} \forall k \in O_i.$$

Найдя линейные комбинации матриц $P^{(k)}$, найдем пространство $\mathcal{T}^{-1}(\mathcal{O}_u)$.
Трудоемкость атаки:

$$q^{o_u} \frac{n^3}{6}.$$

QApp

Rank Attacks: HighRank

Algorithm 5.6 HighRank attack

Input: public matrices $P^{(v_1+1)}, \ldots, P^{(n)}$
Output: $\mathcal{T}^{-1}(\mathcal{O}_u)$

1: Form an arbitrary linear combination $H = \sum_{k=v_1+1}^{n} \lambda_k P^{(k)}$. Find $V = \ker H$.
2: If $\dim V \geq 1$, set $\left(\sum_{k=v_1+1}^{n} \lambda_k P^{(k)}\right) V = 0$. Test, if the solution set has dimension $m - o_u$.
3: With probability q^{-o_u}, we have therefore found $V \subset \mathcal{T}^{-1}(\mathcal{O}_u)$. We continue this process, until we have found the whole space $\mathcal{T}^{-1}(\mathcal{O}_u)$.
4: **return** $\mathcal{T}^{-1}(\mathcal{O}_u)$

Jintai Ding, Albrecht Petzoldt, Dieter S. Schmidt. ``Multivariate Public Key Cryptosystems''

QApp

Rainbow Band Separation

С большой вероятностью существует эквивалентный секретный ключ вида $\tilde{\mathcal{S}}, \tilde{\mathcal{F}}, \tilde{\mathcal{T}}$:

$$\tilde{S} = \begin{pmatrix} 1_{o_1 \times o_1} & \tilde{S}^{(1,2)}_{o_1 \times o_2} & \cdots & \tilde{S}^{(1,u)}_{o_1 \times o_u} \\ 0_{o_2 \times o_1} & 1_{o_2 \times o_2} & \ddots & \vdots \\ \vdots & \ddots & \ddots & \tilde{S}^{(u-1,u)}_{o_{u-1}, o_u} \\ 0_{o_u, o_1} & \cdots & 0_{o_u, o_{u-1}} & 1_{o_u \times o_u} \end{pmatrix}$$

$$\tilde{T} = \begin{pmatrix} 1_{v_1 \times v_1} & \tilde{T}^{(1,2)}_{v_1 \times o_1} & \cdots & \tilde{T}^{(1,u+1)}_{v_1 \times o_u} \\ 0_{o_1 \times v_1} & 1_{o_1 \times o_1} & \ddots & \vdots \\ \vdots & \ddots & \ddots & \tilde{T}^{(u,u+1)}_{o_{u-1}, o_u} \\ 0_{o_u, v_1} & \cdots & 0_{o_u, o_{u-1}} & 1_{o_u \times o_u} \end{pmatrix}.$$

QApp

Rainbow Band Separation

Для этого представим матрицу $\tilde{T}^{-1} = T_n^{-1} \cdot \dots \cdot T_{v_1+1}^{-1}$:

$$T_i = \begin{pmatrix} 1 & & 0 & 0 & t_{1,i} & 0 \\ & \ddots & \vdots & \vdots & \vdots & \\ 0 & & 1 & 0 & t_{v_\ell,i} & 0 \\ 0 & \dots & 0 & 1 & 0 & 0 \\ \vdots & & \vdots & & \ddots & \\ 0 & \dots & 0 & 0 & & 1 \end{pmatrix} \quad (i = v_1 + 1, \dots, n)$$

$$F^{(k)} = \sum_{l=1}^{m} \tilde{s}_{kl} (\tilde{T}_{v_1+1}^T \cdot \dots \cdot \tilde{T}_n^T \cdot P^{(l)} \cdot \tilde{T}_n \cdot \dots \cdot \tilde{T}_{v_1+1})$$

QApp

Rainbow Band Separation

Ищем для $k = v_1 + 1, \ldots, n$ последовательность матриц $P_n^{(k)} = P^{(k)}, P_{n-1}^{(k)}, \ldots, P_{v_1}^{(k)}$ т.ч. $P_{v_1}^{(k)}$ имеет форму $F^{(k)}$. Тогда матрицы $P_{v_1}^{(k)}$, $k = v_1 + 1, \ldots, n$ вместе с $\tilde{T}_i$ и $\tilde{s}_{kl}$ образуют эквивалентный секретный ключ.
Трудоемкость: имеем систему из $(n - j + 1)(m + n - 1)$ уравнений от n неизвестных; $XL/F_4/F_5$. m таких систем ($j = n, \ldots, v_1 + 1$).
Общая трудоемкость определяется трудоемкостью решения n-й системы:

- 1 кубическое уравнение
- $m - 1$ квадратичных уравнений в переменных $\tilde{T}_n$
- $n - 1$ билинейных уравнений (линейных по $\tilde{T}_n$ и $\tilde{s}_{nk}$)

Jintai Ding, Albrecht Petzoldt, Dieter S. Schmidt. ``Multivariate Public Key Cryptosystems''

QApp

Beullens' Attack

Конкретный случай Rainbow с двумя слоями (как в проекте).
Рассмотрим полярную форму открытого ключа:

$$\mathcal{P}'(x,y) = \mathcal{P}(x+y) - \mathcal{P}(x) - \mathcal{P}(y).$$

Существуют подпространства $W \subset \mathbb{F}_q^m$, $\mathcal{O}_2 \subset \mathcal{O}_1 \subset \mathbb{F}_q^n$ т.ч.

$$\mathcal{P}'(x,\cdot)(\mathcal{O}_2) \subset W, \mathcal{P}(\mathcal{O}_1) \subset W, \mathcal{P}(\mathcal{O}_1) = \{0\}$$

$$L_x = \begin{bmatrix} \mathcal{P}'(e_1,x) \\ \vdots \\ \mathcal{P}'(e_n,x) \end{bmatrix}.$$

QApp

Beullens' Attack

Если $y \in \mathcal{O}_2$, то все столбцы L_y лежат в W, и ранг матрицы не больше $\dim W = o_2$. Соответствующие матрицы есть $L_y = \sum_{j=1}^{n} y_j L_{e_j}$, L_{e_j} известны. Итак, $\exists$ нетривиальная линейная комбинация из $k = n - o_2 + 1$ матриц $L_{e_1}, \ldots, L_{e_{n-o_2+1}}$ ранга o_2.
Берем базис W и диагонализируем его, получаем $o_2 \times m$ матрицу C. Возьмем любой столбец матрицы L_y (как линейную форму от y_i). Рассмотрим $(o_2 + 1) \times (o_2 + 1)$ - миноры матрицы

$$\begin{bmatrix} r_i \\ C \end{bmatrix}$$

и все $o_2 \times o_2$-миноры матрицы C и все y_i как переменные; получим систему из $n\binom{m}{o_2+1}$ уравнений, к-рую решаем XL-методом (если $n\binom{m}{o_2+1} \geq (n - o_2 + 1)\binom{m}{o_2} - 1$).

QApp

Взлом

2002: Ward Beullens, "Breaking Rainbow takes a weekend on a laptop"
“Best Early Career Researcher Paper”
ABCMint:

QApp

СПАСИБО ЗА ВНИМАНИЕ