САНКТ-ПЕТЕРБУРГСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ПЕТРА ВЕЛИКОГО

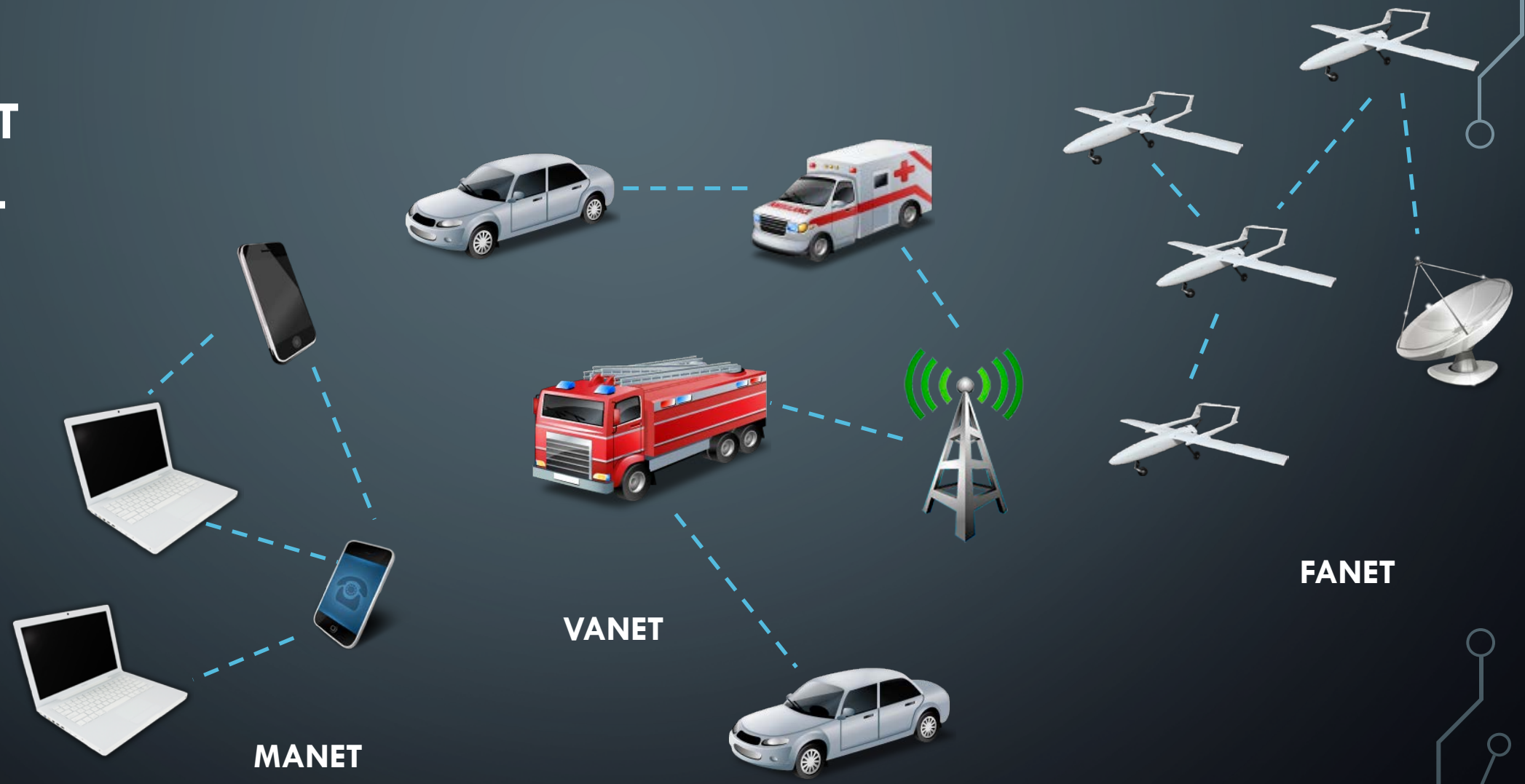
КАФЕДРА «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КОМПЬЮТЕРНЫХ СИСТЕМ»

СИСТЕМА РАСПРЕДЕЛЕННОЙ АУТЕНТИФИКАЦИИ В ИНТЕРНЕТЕ ВЕЩЕЙ НА ОСНОВЕ ИЗОГЕНИЙ ЭЛЛИПТИЧЕСКИХ КРИВЫХ

Александрова Елена Борисовна

ИНТЕРНЕТ ВЕЩЕЙ: БЕСПРОВОДНЫЕ СЕТИ

- MANET
- VANET
- FANET
- FUSN



ОСОБЕННОСТИ СЕТЕЙ

- Постоянное перемещение объектов
- Необходимость организации общения объектов друг с другом и с управляющим центром
- Необходимость обеспечения анонимности каждого объекта для недопущения возможности целевой атаки на отдельный объект

Объекты должны быть защищены:

- От перехвата информации
- От выведения из строя любого объекта

ПОДХОД НА ОСНОВЕ ГРУППОВОЙ АУТЕНТИФИКАЦИИ

- Разделение всего наблюдаемого пространства на зоны/группы
- Выделение в каждой группе аутентифицирующего узла (trusted node)
- Мониторинг выхода объекта за пределы зоны
- Аутентификация объекта в новой зоне
- Сохранение анонимности объекта

СХЕМА РАСПРЕДЕЛЕННОЙ АУТЕНТИФИКАЦИИ: ГРУППОВЫЕ ПОДПИСИ

БИЛИНЕЙНЫЕ ОТОБРАЖЕНИЯ

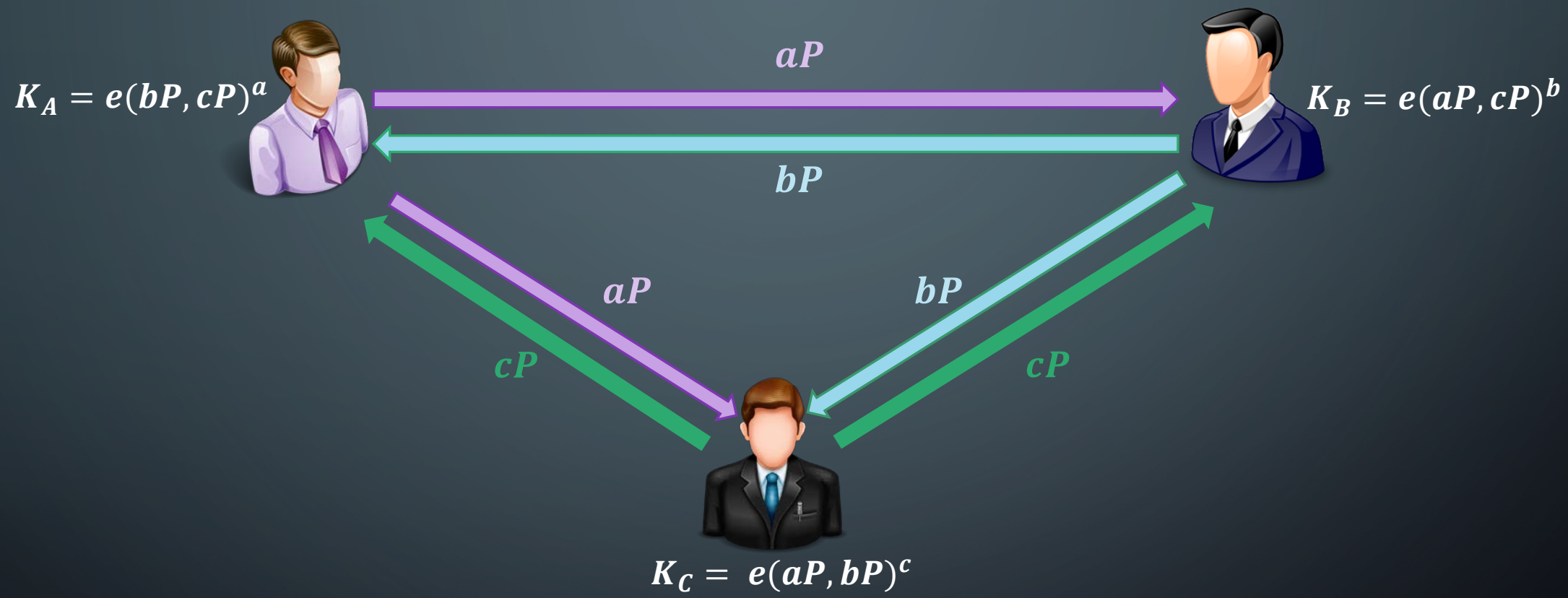
G_1, G_2 – аддитивные циклические группы простого порядка r

G_T – мультипликативная группа простого порядка r

Билинейное отображение (спаривание) e: $G_1 \times G_2 \to G_T$

- Аддитивность:
  - $\forall R, S \in G_1,\ T \in G_2 : e(R+S, T) = e(R, T)e(S, T)$
  - $\forall R \in G_1,\ S, T \in G_2 : e(R, S+T) = e(R, S)e(R, T)$
  - $e(aR, bS) = e(R, S)^{ab}$
- Невырожденность: $e(R, S) \neq 1_{G_2}$

БИЛИНЕЙНЫЕ ОТОБРАЖЕНИЯ: УСТАНОВЛЕНИЕ КЛЮЧА (JOUX)



$$K_{ABC} = K_A = K_B = K_C = e(P, P)^{abc}$$

БИЛИНЕЙНЫЕ ОТОБРАЖЕНИЯ: СХЕМА ПОДПИСИ BLS (BONEH, LYNN,SHACHAM)

$\langle P \rangle = G_1$

d – ключ подписи

$Q = dP$ – ключ проверки

$Hash: \{0,1\}^* \longrightarrow G_1$ – хэш-функция

Формирование подписи

$message$ – сообщение

$M = Hash(message)$

$S = dM$ – подпись

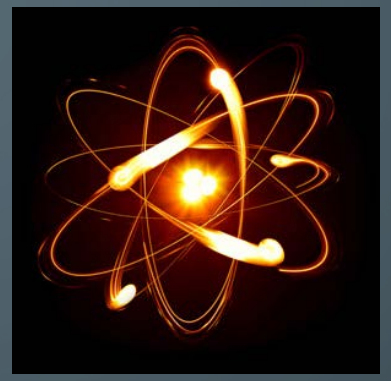
Проверка подписи

$M = Hash(message)$

Проверка: $e(P,S) \stackrel{?}{=} e(Q,M)$

АЛЬТЕРНАТИВНЫЕ МАТЕМАТИЧЕСКИЕ СТРУКТУРЫ

- ✓ Теория решеток
- ✓ Скрытые отображения полей (HFE)
- ✓ Изогении эллиптических кривых



Квантовый компьютер

Эффективные решения пока неизвестны

Разработка криптографических протоколов

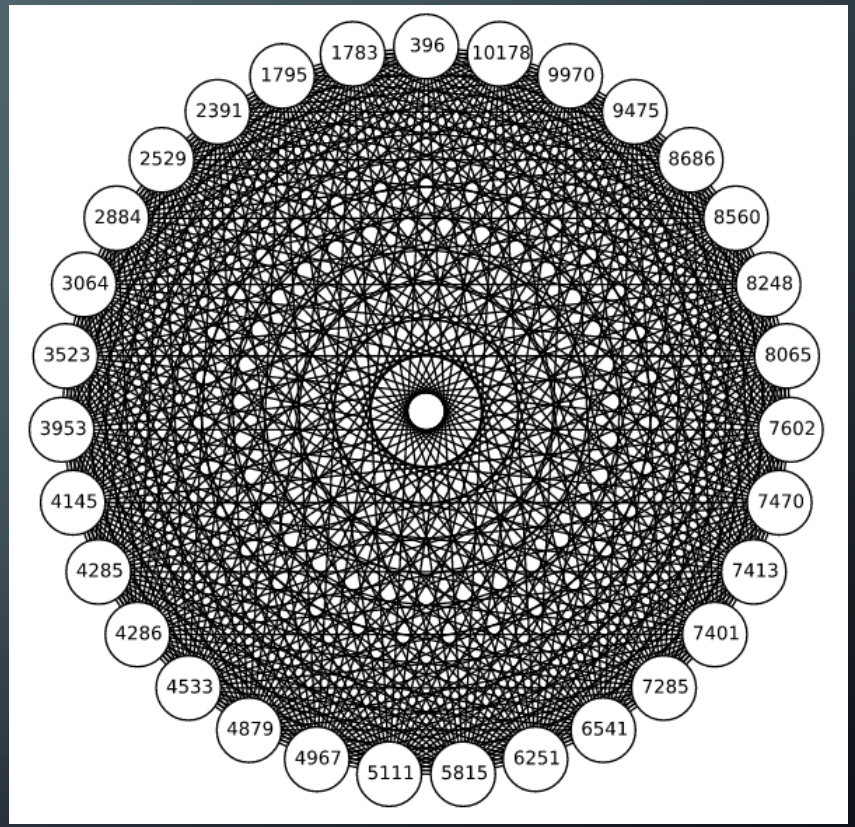
Разработка быстрых вычислительных алгоритмов

Разработка алгоритмов генерации параметров

Анализ безопасности

ВЫЧИСЛЕНИЕ ИЗОГЕНИЙ ЭЛЛИПТИЧЕСКИХ КРИВЫХ

- Эллиптическая кривая E: $Y^2 = X^3 + AX + B$ над полем F_{p^n}
- Инвариант $j(E) = 1728\frac{4a^3}{4a^3+27b^2}$
- Изогения φ: $E_1 \to E_2$, где $\varphi(P_\infty) = P_\infty$
- Дуальная изогения: $\hat{\varphi}$: $E_2 \to E_1$
- Степень l изогении: $\hat{\varphi}\varphi = [l]$, где
  - $[l]$ – умножение точки кривой E_1 на число l
  - l – степень изогении



Звезда изогений

Кривые, связанные изогенией степени l, образуют циклы

КРИПТОСИСТЕМЫ НА ИЗОГЕНИЯХ: ПРОТОКОЛ УСТАНОВЛЕНИЯ КЛЮЧА

Параметры: эллиптическая кривая $E(F_{p^n})$с инвариантом j, набор степеней (l_j) изогений

A

- ✓ Выбрать набор $n = \{n_i\}$ целых чисел
- ✓ Для инварианта j вычислить
  n_1 изогений степени l_1,
  n_2 изогений степени l_2 и т.д.
- ✓ Результат: инвариант j_A

Инвариант j_A

Инвариант j_B

- ✓ Для инварианта j_B вычислить
  n_1 изогений степени l_1,
  n_2 изогений степени l_2 и т.д.
- ✓ Результат: инвариант j_K

B

- ✓ Выбрать набор $m = \{m_i\}$ целых чисел
- ✓ Для инварианта j вычислить
  m_1 изогений степени l_1,
  m_2 изогений степени l_2 и т.д.
- ✓ Результат: инвариант j_B

- ✓ Для инварианта j_A вычислить
  m_1 изогений степени l_1,
  m_2 изогений степени l_2 и т.д.
- ✓ Результат: инвариант j_K

Произведение изогений коммутативно, поэтому *A* и *B* получают одинаковый инвариант j_K, который и является ключом

КРИПТОСИСТЕМЫ НА ИЗОГЕНИЯХ: ГРУППОВЫЕ ПОДПИСИ

Для протоколов на изогениях можно использовать свойство:

$$e_r\left(P, \hat{\varphi}(Q)\right) = e_r(\varphi(P), Q)$$

$$P \in E_1[r], \quad Q \in E_2[r]$$

$$\varphi\colon\ E_1 \to E_2, \quad \hat{\varphi}\colon\ E_2 \to E_1$$

СХЕМА ПОДПИСИ НА ИЗОГЕНИЯХ

Параметры криптосистемы: E_0 - известная эллиптическая кривая, для каждого участника группы генерируются образующие $\{P_i, Q_i\}$

Подписывающий

1. $m_a, n_a \in_R \mathbb{Z}/l_A^a\mathbb{Z}$

2. ψ_A: $E_0 \longrightarrow E_A$ – изогения, ядро изогении $K_A = \langle [m_a]P_A, [n_a]Q_A \rangle$

3. $\gamma_{A,AB}$: $E_A \longrightarrow E_{AB}$, $K_{AB} = \langle [m_a]\psi_B(P_A), [n_a]\psi_B(Q_A) \rangle$

$\{\psi_A(P_B), \psi_A(Q_B)\}$

$\{\psi_B(P_A), \psi_B(Q_A)\}$

$E_{AB} = E_{BA}$

Получатель

1. $m_b, n_b \in_R \mathbb{Z}/l_B^b\mathbb{Z}$

2. ψ_B: $E_0 \longrightarrow E_B$ – изогения, ядро изогении $K_B = \langle [m_b]P_B, [n_b]Q_B \rangle$

3. $\gamma_{B,AB}$: $E_A \longrightarrow E_{AB}$, $K_{BA} = \langle [m_b]\psi_A(P_B), [n_b]\psi_A(Q_B) \rangle$

Подпись сообщения

- $P \in E_0, Hash: \{0,1\}^* \longrightarrow E_{AB}$
- Ключ подписи: φ: $E_{AB} \longrightarrow E_0$
- Ключ проверки: $A = \varphi(P)$
- $message$: $M = Hash(mes) \in E_{AB}$, $S = \hat{\varphi}(M)$
- Подпись: $e(P, S)$

$e(P, S), mes, \varphi(P)$

Проверка

- $message$: $M = Hash(mes) \in E_{AB}$
- Проверка: $e(P, S) \stackrel{?}{=} e(\varphi(P), M)$

КРИПТОСИСТЕМЫ НА ИЗОГЕНИЯХ: ПУТИ РЕАЛИЗАЦИИ

Ресурсозависимые устройства: ограничения по памяти и вычислительной мощности

Уменьшение длины коэффициентов модулярных полиномов и повышение их разреженности за счет использования полинома Вебера вместо полинома Гильберта

(требуется для вычисления изогений)

Дискриминант $D = -71$

- полином Гильберта

$$H_{-71}(X) = X^7 + 313645809715X^6 - 3091990138604570X^5 + 98394038810047812049302X^4 - 82353426343973077996809138 9X^3 + 513880036645397678032372632944 6X^2 - 42531947394613960327460515118765 9X + 737707086760731113357714241006081263$$

- полином Вебера

$$W_{-71}(X) = X^7 - X^6 - X^5 + X^4 - X^3 - X^2 + 2X + 1$$

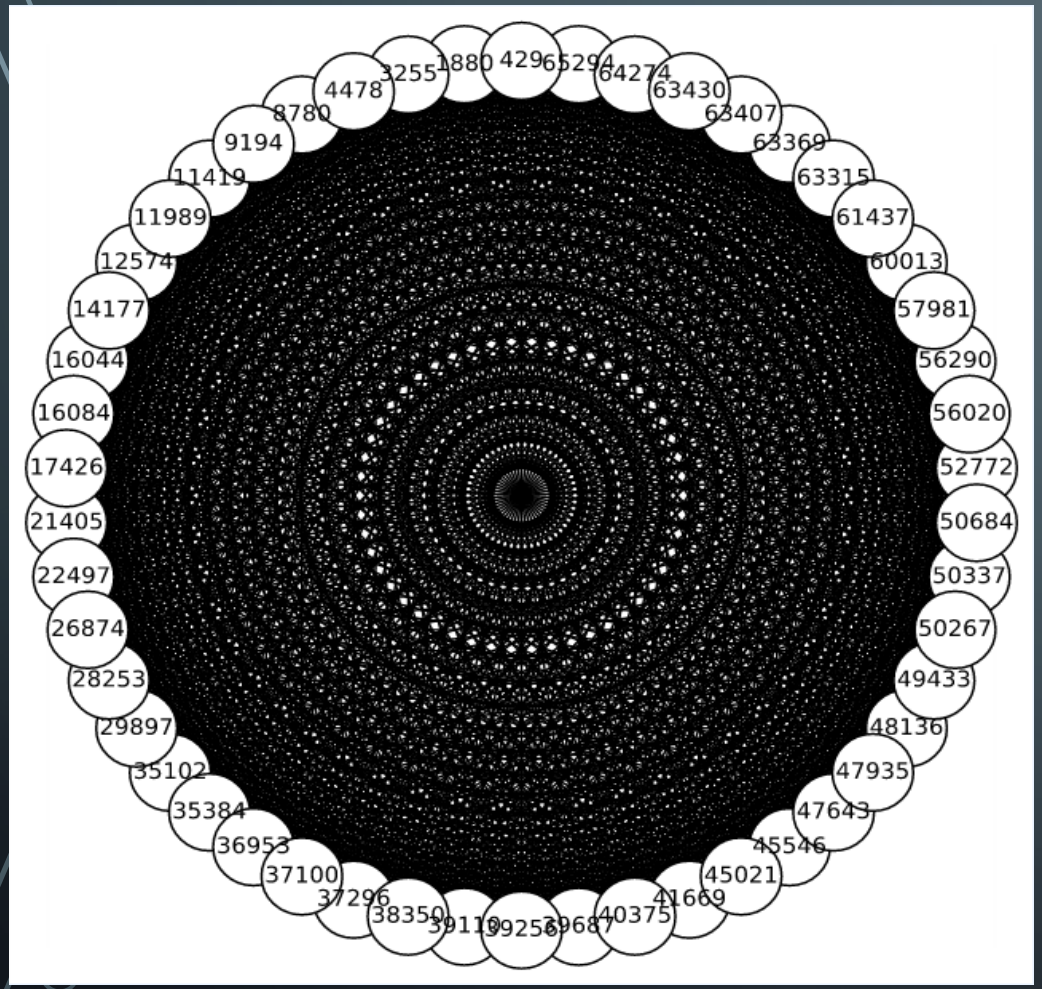
КРИПТОСИСТЕМЫ НА ИЗОГЕНИЯХ: ПУТИ РЕАЛИЗАЦИИ

- Использование полей псевдомерсенновых характеристик
- Задание расширенного поля разреженными полиномами
- Умножение на степень собственного значения эндоморфизма Фробениуса
- «Лестница Монтгомери» - защита от атак по внешнему каналу

ВЫБОР ХАРАКТЕРИСТИКИ ПОЛЯ

БПЛА	Используемый процессор, разрядность	Изготовитель модуля	Возможная характеристика поля
БПЛА eBee. SenseFly, Швейцария	Компьютер-модуль Gumstix Overo Tide с процессором OMAP3530 на базе ядра Cortex-A8, 32 бита	Texas Instruments, США	$2^{32}-5, 2^{31}+11$
Квадрокоптер Bebop Dron. Parrot, Франция.	Parrot P7 на базе двухъядерного Cortex-A9, 32 бита	Parrot, Франция	$2^{32}-5, 2^{31}+11$
БПЛА	Модуль CPC107 (CPU188R) с процессором innovASIC™ IA188ES, 8/16 бит	Fastwel, Россия	$2^7+3, 2^8-5;$ $2^{15}+3, 2^{16}-15, 2^{16}+1$
БПЛА	Модуль CPC109 с процессором Vortex86DX, 32 бита	Fastwel, Россия	$2^{32}-5, 2^{31}+11$
БПЛА	Модуль CPC150 процессором AMD Geode LX 800, 32 бита	Fastwel, Россия	$2^{32}-5, 2^{31}+11$

КРИПТОСИСТЕМЫ НА ИЗОГЕНИЯХ: ПУТИ РЕАЛИЗАЦИИ



Эллиптическая кривая E:

$$Y^2 = X^3 + 1228X + 1 \text{ над полем } F_{p^n}$$

$$p = 2^{16} + 1, n = 11$$

Степени изогении $l = [3, 5, 11, 13, 31, 43, 53, 61, 73, 83, 89, 97]$

j – инварианты изогенных кривых

$j = \{65294, 65153, 64571, 64439, 64274, 64253, 63967, 63430, 63407, 63369, 63349, 63315, 63208, 61904, 61437, 60013, 59933, 59438, 59224, 57981, 57121, 56290, 56020, 55003, 54005, 53083, 52772, 52262, 50684, 50420, 50371, 50337, 50267, 49433, 48136, 47935, 47643, 45546, 45021, 44336, 44109, 43741, 42151, 41669, 40375, 39687, 39356, 39256, 39165, 39123, 39110, 38350, 37296, 37100, 36953, 36763, 36627, 35744, 35384, 35151, 35102, 34956, 32253, 31882, 31608, 29897, 29232, 28253, 27519, 26874, 23314, 23121, 23032, 22497, 21897, 21405, 21072, 17426, 16739, 16084, 16044, 14454, 14442, 14336, 14177, 12574, 11989, 11419, 9194, 8780, 8010, 4793, 4478, 3879, 3255, 3068, 2081, 1880, 1166, 429\}$

СПАСИБО ЗА ВНИМАНИЕ!

helen@ibks.ftk.spbstu.ru