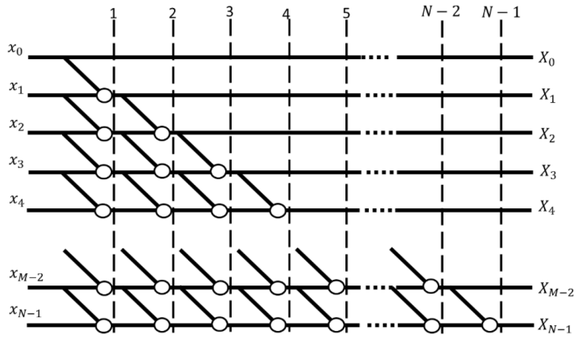
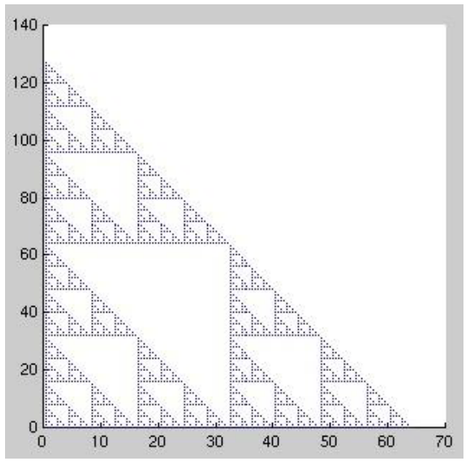
КОРРЕКТИРУЮЩИЕ КОДЫ НА ОСНОВЕ БИНОМИАЛЬНЫХ ФРАКТАЛЬНЫХ СТРУКТУР

С.Б. САЛОМАТИН, А.Э. АЛЕКСЕЕНКО

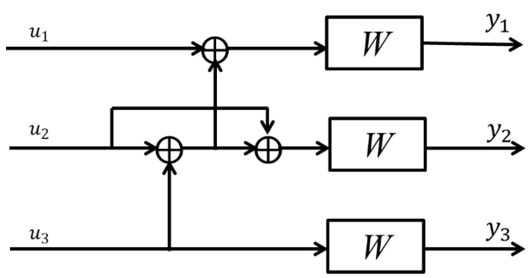
Рассмотрена связь полярных кодов и кодов Рида-Маллера с фрактальными биномиальными матрицами Паскаля, что позволяет увеличить многообразие кодов для достижения пропускной способности канала.



Граф дискретного преобразования Паскаля



Треугольник Серпинского



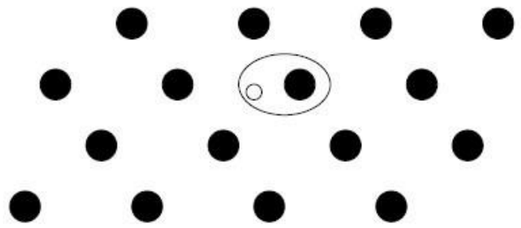
W_3

Структура симметрично канала полярного кода

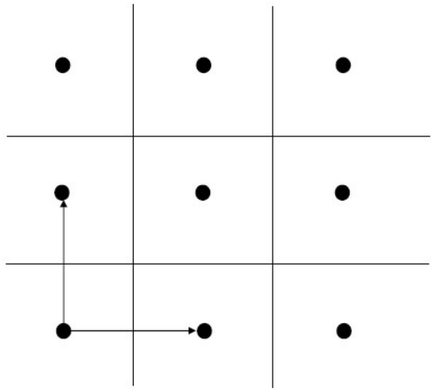
ОПРЕДЕЛЕНИЕ ПАРАМЕТРОВ АКТИВНЫХ ИСТОЧНИКОВ СЕНСОРНОЙ СЕТИ С ИСПОЛЬЗОВАНИЕМ ТЕОРИИ КОДОВЫХ РЕШЕТОК

С. Б. САЛОМАТИН

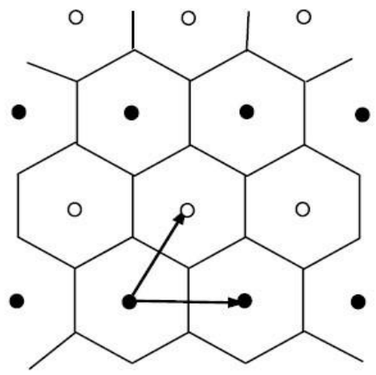
Рассмотрены алгоритмы определения параметров активных источников сенсорных сетей с использованием теории решеток и процедур сферического декодирования и векторного квантования.



Геометрия процесса декодирования



Ячейки Вороного и базисные векторы прямоугольной решетки



Гексагональная решетка

ЦИФРОВАЯ ПОДПИСЬ ВЕБ-СЕРВИСА ПРОТОКОЛА TLS НА ОСНОВЕ ЭЛЛИПТИЧЕСКИХ КРИВЫХ И ОБЛАЧНОЙ ПЛАТФОРМЫ HEROKU

Н.С. ФИЛИППОВ, С.Б. САЛОМАТИН

Рассмотрены криптографические алгоритмы цифровой подписи на эллиптических кривых в контексте «Интернет вещей», а также расширение возможностей стандартного протокола защиты транспортного уровня TLS на основе устройства *raspberry pi* и облачного протокола *Heroku.*

Raspberry pi zero w

График эллиптической кривой secp256k1

```
   def sign_message(private_key, message):
z = hash_message(message)
r = 0
s = 0
while not r or not s:
    k = random.randrange(1, curve.n)
    x, y = scalar_mult(k, curve.g)
    r = x % curve.n
    s = ((z + r * private_key) * inverse_mod(k, curve.n)) % curve.n
return (r, s)
```

Функция генерации цифровой подписи

Результаты измерений времени генерации цифровой подписи на *raspberry pi*

Эллиптическая кривая	Время генерации подписи, с
Secp192k1	0,78
Secp192r1	0,73
Secp224r1	0,92
Secp256k1	1,20
Secp256r1	1,32
Secp384r1	2,91

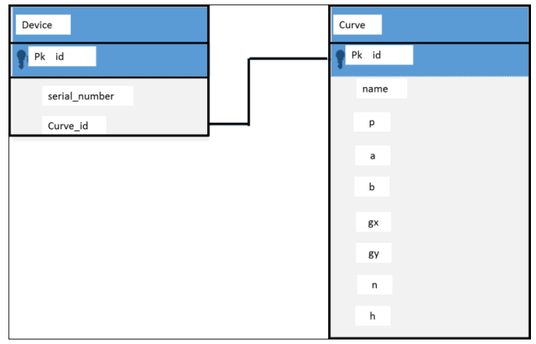
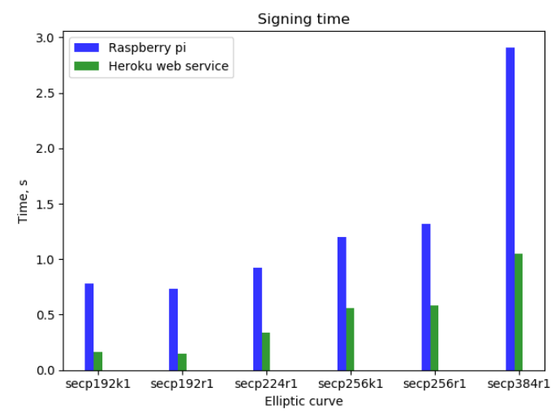


Схема сущностей в базе данных

Результаты измерений времени генерации цифровой подписи с использованием веб-сервиса

Эллиптическая кривая	Время генерации подписи, с
secp192k1	0,16
secp192r1	0,15
secp224r1	0,34
secp256k1	0,56
secp256r1	0,58
secp384r1	1,05



Сравнение времени генерации цифровой подписи на *raspberry pi* и веб-сервисе