

# Создание надежного протокола на основе криптосистемы Э.М. Габидулина

Выполнила: студентка группы 09-875  
Князева Яна Дмитриевна  
Научный руководитель: профессор, доктор т.н.  
Латыпов Рустам Хафизович

# Цели и задачи:

**Цель:** выбор темы магистерской диссертации, ее исследование и обзор научной литературы по данной области.

## **Задачи:**

- проверить и обосновать актуальность и новизну темы диссертации;
- изучить литературу по криптографии;
- сформулировать цели и задачи магистерской работы.

# Описание Криптосистемы ГПТ:



## Открытый текст

В качестве открытого текста может использоваться любой  $k$ -вектор  $m = (m_1, m_2, \dots, m_k)$ ,  $m_s \in \mathbb{F}_{qN}$ ,  $s = 1, 2, \dots, k$ .

# Описание Криптосистемы ГПТ:

- Открытый ключ

Открытым ключом является порождающая матрица размера  $k \times (n + t_1)$ :

$$G_{pub} = S[XG_k]P,$$

где:

- $G_k$  – порождающая матрица  $(n,k,d)$  кода с максимальным ранговым расстоянием  $d$  для длины кода  $n \leq N$  с количеством символов  $k$ , задающаяся матрицей следующей формы:

$$G_k = \begin{bmatrix} g_1 & g_2 & \cdots & g_n \\ g_1^{[1]} & g_2^{[1]} & \cdots & g_n^{[1]} \\ \vdots & \vdots & \ddots & \vdots \\ g_1^{[k-1]} & g_2^{[k-1]} & \cdots & g_n^{[k-1]} \end{bmatrix}$$

# Описание Криптосистемы ГПТ:

## ■ Открытый ключ

- Строковый скремблер  $S$  — невырожденная квадратная матрица порядка  $k$  над полем  $\mathbb{F}_{qN}$
- $X$  — матрица искажений размера  $(k \times t_1)$  над полем  $\mathbb{F}_{qN}$  со столбцовым рангом  $Rk_{col}(X|\mathbb{F}_q) = t_1$  и рангом  $Rk_{col}(X|\mathbb{F}_{qN}) = t_X, t_X \leq t_1$ .
- Матрица  $[XG_k]$  имеет столбцовый ранг  $Rk_{col}([XG_k]|\mathbb{F}_{qN}) = n + t_1$ .
- Столбцовый скремблер  $P$  — квадратная матрица порядка  $(t_1 + n)$  над полем  $\mathbb{F}_q$ .
- $t_1 + n$  может быть больше  $N$ , но  $n \leq N$ .

# Описание Криптосистемы ГПТ:



## Закрытый ключ

В качестве закрытого ключа выступает набор  $(S, G_k, X, P)$ , а также алгоритм быстрого декодирования MPP-кода, в котором используется матрица проверки четности  $H^{(n-k) \times k}$ , такая, что  $G_k H^T = 0$

$$H = \begin{bmatrix} h_1 & h_2 & \dots & h_n \\ h_1^{[1]} & h_2^{[1]} & \dots & h_n^{[1]} \\ \vdots & \vdots & \ddots & \vdots \\ h_1^{[d-2]} & h_2^{[d-2]} & \dots & h_n^{[d-2]} \end{bmatrix}$$

# Описание Криптосистемы ГПТ:

- Оптимальные параметры кода
- Длина кода  $n \leq N$ ,
- Размерность  $k = n - d + 1$ ,
- Ранговое расстояние кода  $d = n - k + 1$ .

# Описание Криптосистемы ГПТ:



## Шифрование

Соответствующий открытому тексту криптотекст вычисляется следующим образом:

$$c = mG_{pub} + e = mS[XG_k]P + e$$

где  $e$  — искусственный вектор ошибок ранга не выше  $t_2$ , причем  $t_1 + t_2 \leq t = \left\lfloor \frac{n-k}{2} \right\rfloor$ .



# Описание Криптосистемы ГПТ:

## ■ Дешифрование

- Законный получатель, получая  $c$ , выполняет следующие действия:
- Вычисляет  $c' = (c'_1, c'_2, \dots, c'_{t_1+n}) = cP^{-1} = mS[XG_k] + eP^{-1}$
- Из  $c'$  выделяет подвектор  $c'' = (c''_1, c''_2, \dots, c''_{t_1+n}) = cP^{-1} = mSG_k + e''$ , где  $e''$  - подвектор  $eP^{-1}$
- Применяет алгоритм быстрого декодирования для исправления ошибки  $e''$
- Получает  $mS$
- Восстанавливает  $m = (mS) S^{-1}$

# Описание Криптосистемы ГПТ:

- Размер открытого ключа составляет:

$$V = k(t_1 + n)N \text{ бит}$$

- Скорость передачи информации:

$$R = \frac{k}{t_1 + n}$$

# Заключение

В процессе прохождения учебной (ознакомительной) практики были поставлены цель и задачи по научно-исследовательской деятельности для написания магистратской диссертации.

Были приобретены первичные профессиональные навыки для ведения самостоятельной научно-исследовательской работы. Цель на следующий семестр – выполнить подробное изучение методов шифрования, их реализацию с перспективой последующего внедрения в современные телекоммуникационные системы, предъявляющих повышенные требования к надежности передачи информации.

Спасибо за внимание