Усиление безопасности криптосистемы, сохраняющей порядок, на основе матричного шифрования

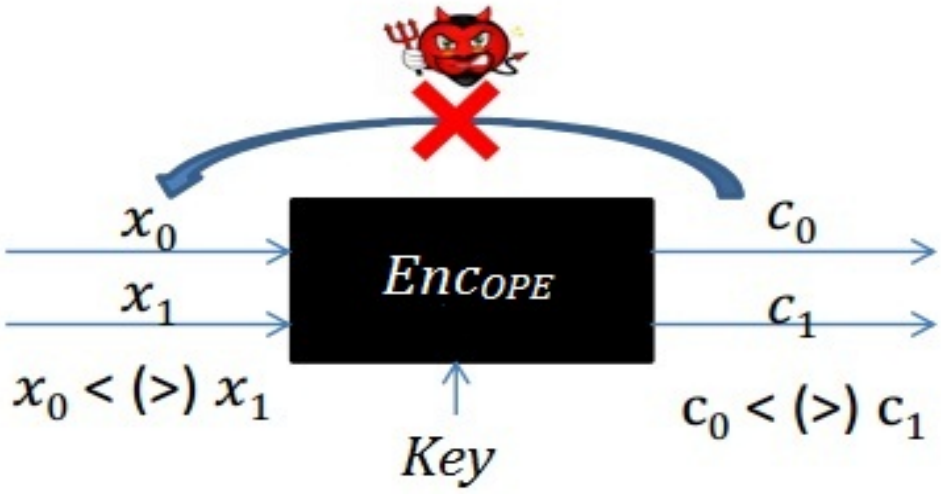
Усольцева Мария
Научный руководитель: к.ф.-м.н. Кренделев С.Ф.

Лаборатория НГУ-Parallels

Работа выполняется при финансовой поддержке Минобрнауки РФ (договор № 02.G25.31.0054).

Цель исследования

Разработка схемы шифрования чисел из $Z_{\geq 0}$, сохраняющей порядок OPE (Order-preserving encryption), для последующего внедрения в проект CryptoDB.



Генерация ключей

Ключ шифрования:

$$K = (A_1, ..., A_l, \sigma),$$

где $A_i \in M_{n_i}[Z_{m_i}]$, $det\ A_i\ mod\ m_i \neq 0$, $i = 1, ..., l$,

σ - случайная перестановка элементов матрицы размера $n_l \times n_l$.

Процедура шифрования

Обозначения:

$A^i \stackrel{def}{=} A^i \ mod \ m$

$sum(A) \stackrel{def}{=} \sum_{i=1}^{n} \sum_{j=1}^{n} a_{ij}$, a_{ij} - элементы матрицы $A \in M_n[Z_p]$

a'_i - элементы матрицы σA_l^r

Требуется зашифровать число $x \in Z_{\geq 0}$, $K = (A_1, ..., A_l, \sigma)$:

$$x = \sum_{i=1}^{r_1 - 1} sum(A_1^i) + ... + \sum_{i=1}^{r_l - 1} sum(A_l^i) + \sum_{i=1}^{k} a'_i + t$$

Шифротекст:

$$Enc_K(x) = (r_1, ..., r_l, k, t)$$

Преобразования вектора $(r_1, ..., r_l, k, t)$ в число

Представление числа в смешаннной системе счисления

$x = \sum_{k=0}^{n-1} a_k b_k$, где a_k - k-я цифра в записи числа,

b_k - весовой коэффициент k-го разряда, $0 \leq a_k \leq b_k - 1$.

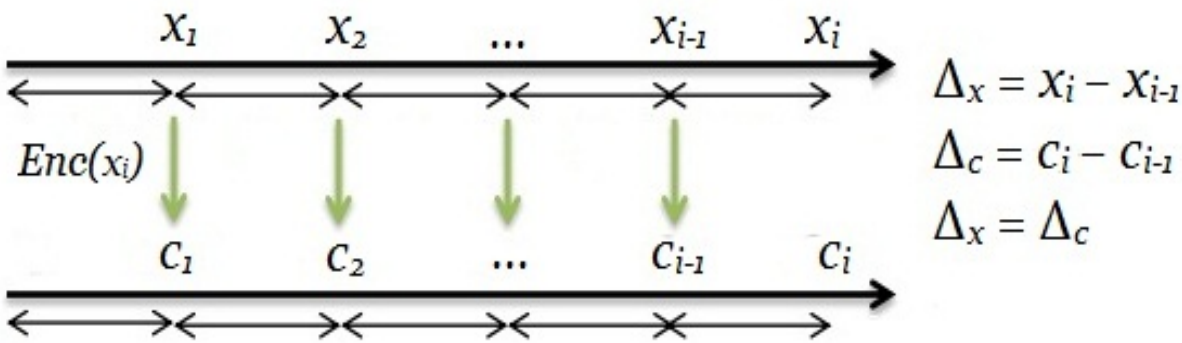
$$(r, k, t) \longrightarrow t + k(m-1) + r(m-1)n^2$$

$$(r_1, ..., r_l, k, t) \longrightarrow \sum_{i=1}^{l+2} \alpha_i \prod_{j=1}^{i} \beta_j$$

$\bar{\alpha} = (t, k, r_l, ..., r_1)$,

$\bar{\beta} = (1, m_l - 1, n^2, \frac{sum(A^r_{l-1})}{(n_l+1)(m_l-1)} + 1, ..., \frac{sum(A^r_1)}{(n_2+1)(m_2-1)} + 1)$

Проблема сохранения расстояний между шифротекстами



Решение проблемы

Возможно скрыть в среднем $l = \lceil \log_2 A \rceil$ младших бит числа

$$Enc(x) = 2^l u + y \mid y \in [0..2^l - 1],\ x, u \in Z_{\geq 0}$$

применив строго возрастающую монотонную функцию

$$Rep(x) = Ax + B,$$

где $A, B \in Z_{\geq 0},\ A > 1,\ B = random(0, A)$

Обратная функция

$$Rep^{-1}(Rep(x)) = Rep(x)\ mod\ A$$

Другие возможные функции

Полиномиальные:

$$Rep_1(x) = Ax^2 + B,$$

$$Rep_2(x) = Ax^2 + Akx + B,\ k > 0,\ k \in Z$$

Обратные функции

$$Rep_1^{-1}(Rep(x)) = \sqrt{Rep(x)\ mod\ A},$$

$$Rep_2^{-1}(Rep(x)) = \tfrac{1}{2}(-k + \sqrt{k^2 + Rep(x)\ mod\ A})$$

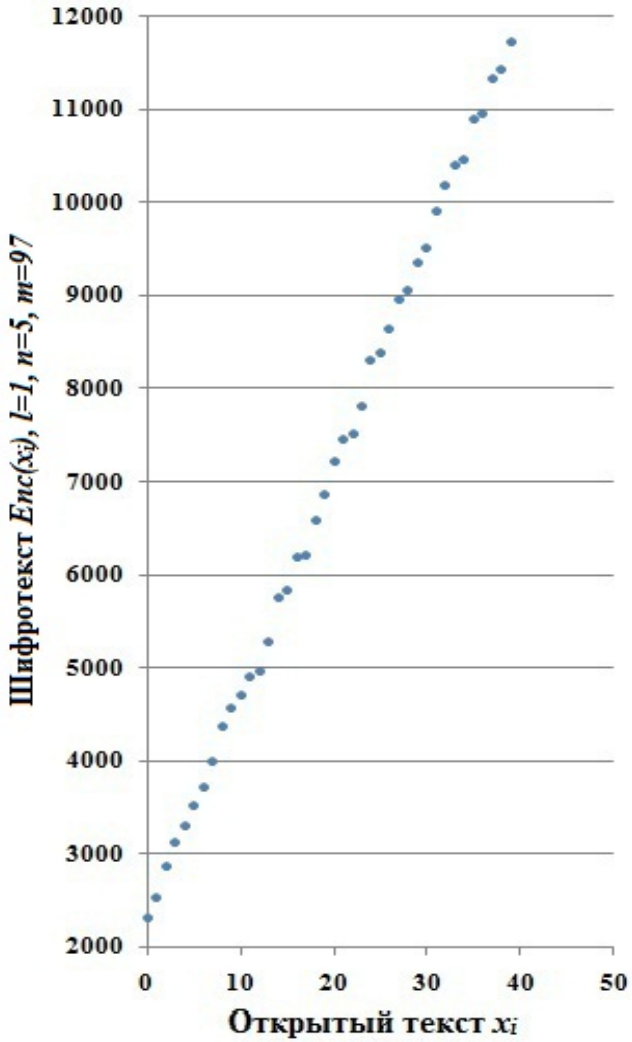
Преобразования схемы

$$K' = K \cup \{A\}$$

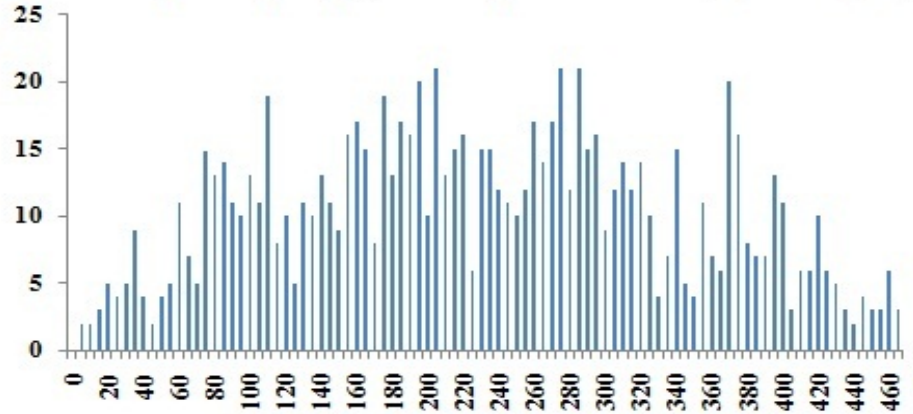
$$Enc'_K(x) = Enc_K(Rep(x))$$

$$Dec'_K(c) = Rep^{-1}(Dec_K(c))$$

Статистические данные: $Rep(x) = Ax + B$, $A = 2^7$



Гистограмма распределения разностей $Enc(x_i) - Enc(x_{i-1})$



Результаты работы

- Продолжено исследование публикаций по данной теме
- Разработан алгоритм для преобразования результирующего вектора в число
- Реализован прототип схемы шифрования с произвольным числом матриц и одним числом на выходе в виде библиотеки на языке C++
- Выявлены и решены некоторые проблемы криптостойкости схемы
- Проведен ряд оптимизаций и тестов на производительность

Дальнейшие планы

- Изучение подходов к криптоанализу схем OPE и предложенных в публикациях атак (POPF-CCA, WOW, WDOW)
- Оптимизация существующих библиотек
- Внедрение в приложениние CryptoDB

Спасибо за внимание!

Ваши вопросы?