

Атака на MGM в модели PRF на основе парадокса дней рождения

Илья Махонин

Известные результаты анализа

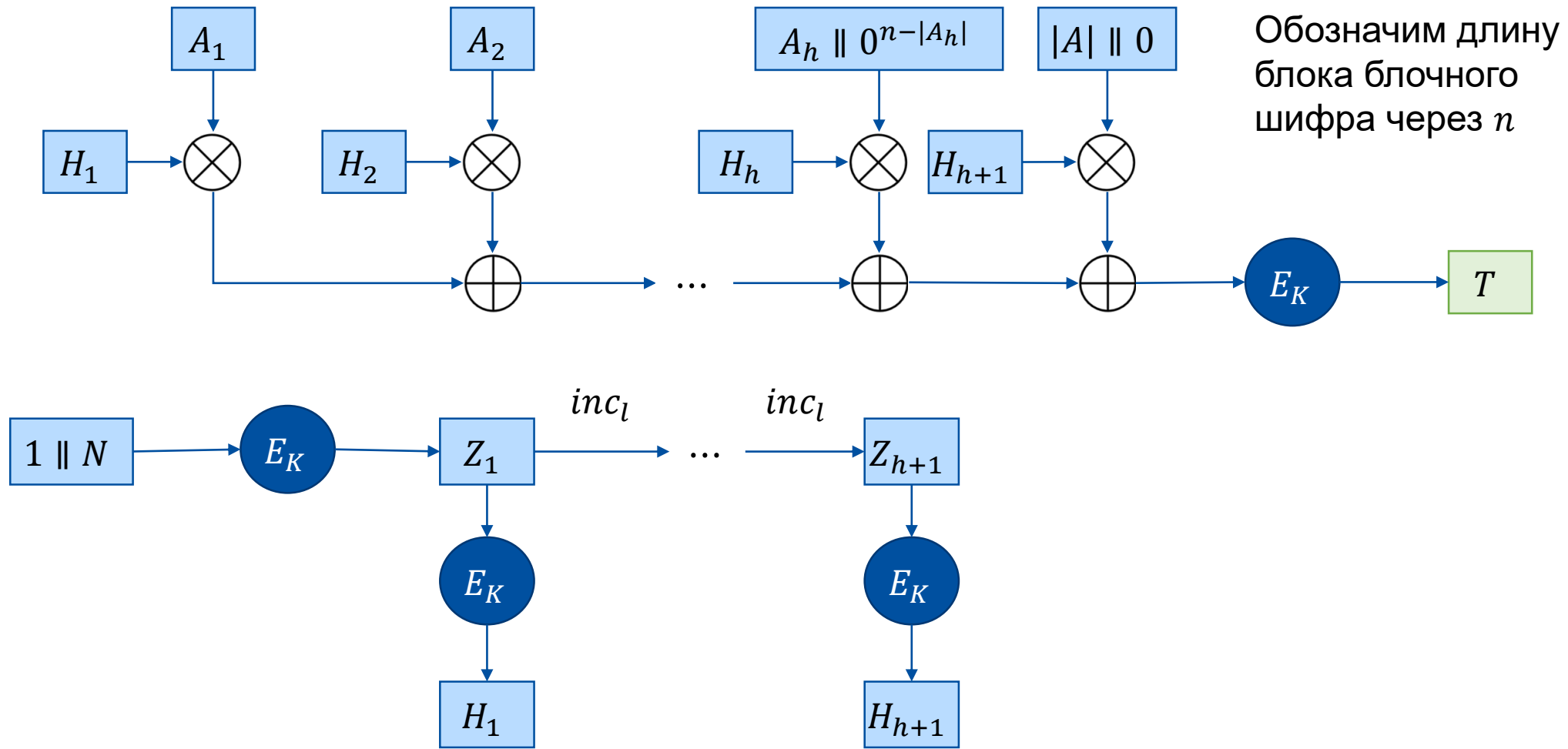
Оценка стойкости в двух моделях, полученная в результате теоретико-сложностного сведения

- Akhmetzyanova L. et al. Security of multilinear galois mode (MGM) //Cryptology ePrint Archive. – 2019.

Две атаки на нарушение целостности

- Kurochkin A., Fomin D. MGM beyond the birthday bound //Journal of Computer Virology and Hacking Techniques. – 2024. – Т. 20. – №. 2. – С. 231-235.

Объект анализа: MGM без шифрования



Модель PRF

Нарушитель имеет возможность подавать запросы вида N, A с уникальными N и получать в ответ

- значения имитовставки T для синхропосылки N и данных A
- или
- значения случайной функции для синхропосылки N и данных A .

Задача нарушителя: отличить MGM без шифрования от случайной функции



Описание атаки

Нарушитель выполняет следующие действия

- фиксирует некоторый параметр $L' > 0$
- подает запросы с различными N и $A = 0^{L'}$

$$T = E_K \left((L' \parallel 0) \otimes \underbrace{E_K \left(E_K(1 \parallel N) \boxplus_l \left\lfloor \frac{L'}{n} \right\rfloor \right)}_{H_{h+1}} \right) = G_{K,L'}(N)$$

$G_{K,L'}$ – **инъективное** отображение

Если нашлись $T_i, T_j: T_i = T_j$, значит нарушитель делал запросы к **случайной** функции

Вероятность успеха $\approx \frac{q^2}{2^n}$ (парадокс дней рождения), где q – число запросов.



Практическая применимость результатов

Пусть MGM без шифрования используется в качестве KDF в некоторой криптосистеме.

Длина вырабатываемого ключа равна $k = l \cdot n$ для некоторого l

Трудоемкость (в худшем случае) метода опробования для вырабатываемого ключа равна

$$2^n \cdot (2^n - 1) \cdot \dots \cdot (2^n - l + 1)$$

вместо $2^{l \cdot n}$



Спасибо
за внимание!

