

ДВУХУРОВНЕВАЯ МУЛЬТИЛИНЕЙНАЯ ХЭШ-ФУНКЦИЯ – ЭФФЕКТИВНЫЕ ПРЕДВЫЧИСЛЕНИЯ ЦЕНОЙ ОДНОГО БИТА СТОЙКОСТИ

ВИТАЛИЙ КИРЮХИН

ООО «СФБ Лаб»

CTCrypt 2026

2 июня 2026

vitaly.kiryukhin@sfblaboratory.ru



ε-УНИВЕРСАЛЬНЫЕ ХЭШ-ФУНКЦИИ (AU, AXU, и др.)

ОБЩИЕ СВЕДЕНИЯ

hash : {ключи} × {сообщения} → {выход}

Построение:

обычно с помощью операций в конечных полях.

Применение:

- имитозащита (MAC);
- псевдослучайные функции (PRF);
- AEAD-схемы;
- экстракторы энтропии.

ε-УНИВЕРСАЛЬНЫЕ ХЭШ-ФУНКЦИИ (AU, AXU, и др.)

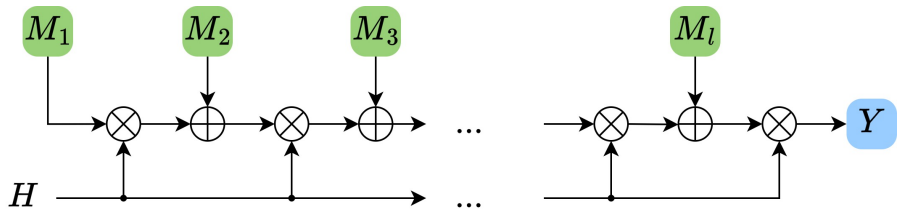
ГЛАВНАЯ ХАРАКТЕРИСТИКА (AU)

Макс. вероятность коллизии пары сообщений по случайному выбору ключа H

$$\max_{M \neq \tilde{M}} \Pr(\mathbf{hash}(H, M) = \mathbf{hash}(H, \tilde{M})) \leq \epsilon_{\text{hash}}.$$

Для имитозащиты и AEAD: $\epsilon_{\text{hash}} \approx$ вероятность навязывания, подделки,
 $\log_2(\epsilon_{\text{hash}}^{-1}) \approx$ стойкость к атакам навязывания (в битах).

Полиномиальная хэш-функция



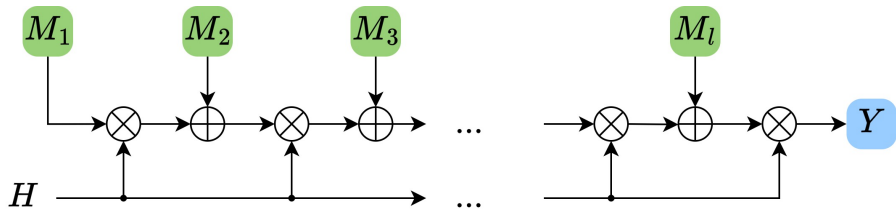
$$\text{PH}(H, M) = H \otimes M_\ell \oplus H^2 \otimes M_{\ell-1} \oplus \dots \oplus H^\ell \otimes M_1$$

Ключ: один n -битный блок H

Вероятность коллизии: $\epsilon_{\text{PH}} = \ell \cdot 2^{-n}$

Используется в: GCM, Poly1305, belt-dwp и belt-che (СТБ 34.101.31-2020)

Полиномиальная хэш-функция



$$\mathbf{PH}(H, M) = H \otimes M_\ell \oplus H^2 \otimes M_{\ell-1} \oplus \dots \oplus H^\ell \otimes M_1$$

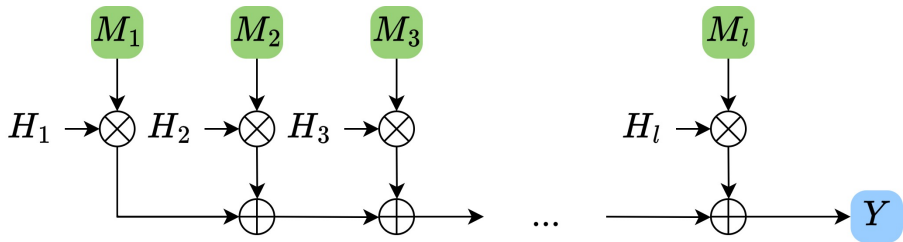
Ключ: один n -битный блок H

Вероятность коллизии: $\epsilon_{\mathbf{PH}} = \ell \cdot 2^{-n}$

Используется в: GCM, Poly1305, belt-dwp и belt-che (СТБ 34.101.31-2020)

Главный недостаток: при $n = 64$ бита $\epsilon_{\mathbf{PH}}$ слишком велика для практики

Мультилинейная хэш-функция



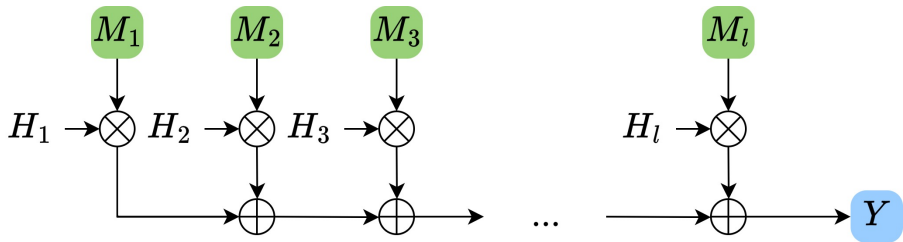
$$\mathbf{MH}(H, M) = H_1 \otimes M_1 \oplus H_2 \otimes M_2 \oplus \dots \oplus H_\ell \otimes M_\ell$$

Ключ: ℓ блоков $H = (H_1, \dots, H_\ell)$

Вероятность коллизии: «идеальная» $\epsilon_{\mathbf{MH}} = 2^{-n}$

Используется в: MGM (ГОСТ 34.13-2018), MGM2, sMGM, SUM-MGM, MXP

Мультилинейная хэш-функция



$$\mathbf{MH}(H, M) = H_1 \otimes M_1 \oplus H_2 \otimes M_2 \oplus \dots \oplus H_\ell \otimes M_\ell$$

Ключ: ℓ блоков $H = (H_1, \dots, H_\ell)$

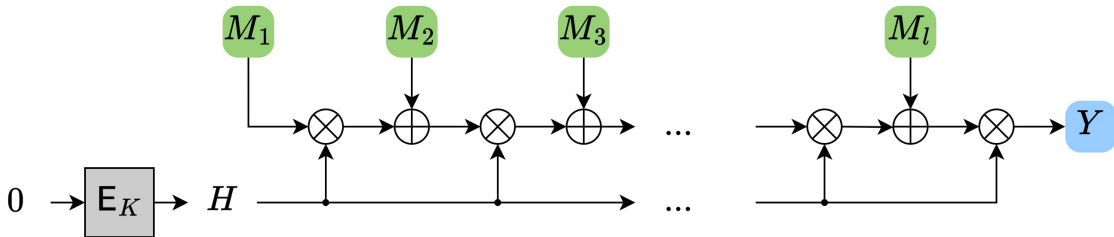
Вероятность коллизии: «идеальная» $\epsilon_{\mathbf{MH}} = 2^{-n}$

Используется в: MGM (ГОСТ 34.13-2018), MGM2, sMGM, SUM-MGM, MXP

Какова на практике «цена» за идеальную стойкость?

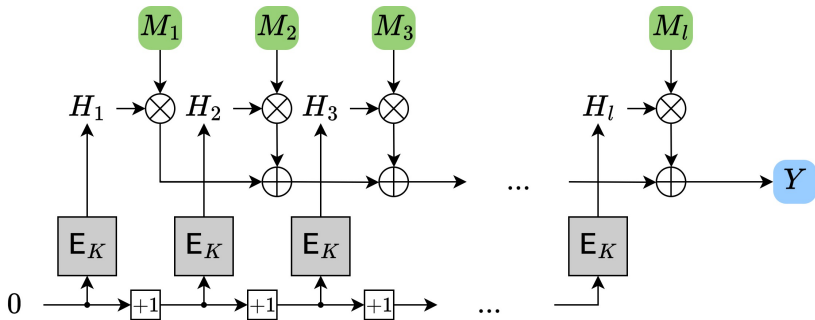
ПРАКТИКА: БЛОК КЛЮЧА – РЕЗУЛЬТАТ ШИФРОВАНИЯ

РН: одно шифрование и ℓ умножений



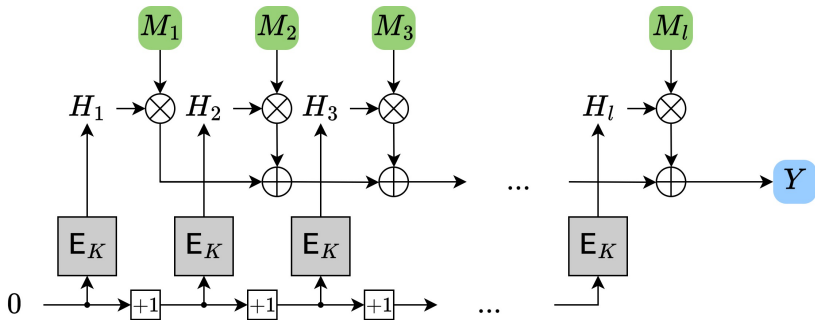
ПРАКТИКА: БЛОК КЛЮЧА – РЕЗУЛЬТАТ ШИФРОВАНИЯ

МН: ℓ шифрований и ℓ умножений



ПРАКТИКА: БЛОК КЛЮЧА – РЕЗУЛЬТАТ ШИФРОВАНИЯ

МН: ℓ шифрований и ℓ умножений



Недостаток: скорость работы. Шифрование кратно медленнее умножения, а хранение ключа в памяти (МХР, SUM-MGM) возможно только для малых ℓ .

Цель – новая хэш-функция

КРИПТОГРАФИЧЕСКИЕ СВОЙСТВА

«Почти идеальная» вероятность коллизии $\approx 2^{-n}$
– полноблоковые n -битные имитовставки.

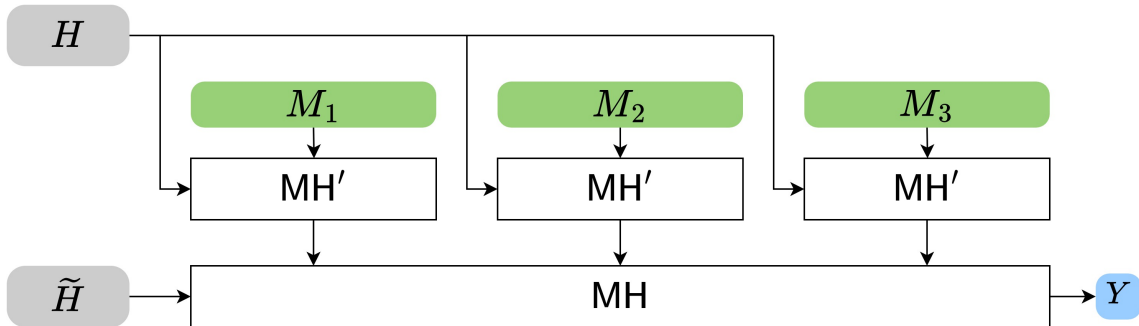
ЭКСПЛУАТАЦИОННЫЕ СВОЙСТВА

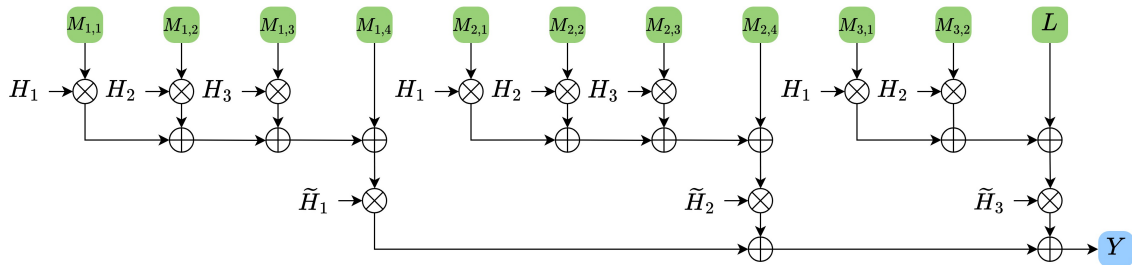
1. Скорость: в среднем одно умножение на один блок сообщения.
2. Память: несколько блоков.
3. НЕ переходим к полям размерности более 2^n .

МН2 – ДВУХУРОВНЕВАЯ МУЛЬТИЛИНЕЙНАЯ ХЭШ-ФУНКЦИЯ

ИДЕЯ

- Делим ℓ -блоковое сообщение на t **секций** по s блоков в каждой
- Первый уровень: каждую секцию хэшируем на *одном и том же* ключе H
- Второй уровень: хэшируем результаты первого уровня на другом ключе $\tilde{H}$





$$\mathbf{MH2}(H, M) = \bigoplus_{i=1}^m \left(\tilde{H}_i \otimes \left(\bigoplus_{j=1}^{s-1} (M_{i,j} \otimes H_j) \oplus M_{i,s} \right) \right)$$

- последний блок в секции не умножается на блок ключа
- сообщение дополняется блоком L – «битовая длина входа»

ХАРАКТЕРИСТИКИ

- Ключ первого уровня: $(s - 1)$ блоков – храним в памяти
- Ключ второго уровня: $m \approx \ell/s$ блоков – вычисляем «на лету» (или храним)
- Итого для хэширования: ℓ умножений и $m \ll \ell$ шифрований
- Общая длина ключа снижается вплоть до $2\sqrt{\ell}$ блоков

РЕЗУЛЬТАТ

ЛЕММА

M – ненулевое сообщение из $\ell \leq s \cdot m$ блоков.

$(m + s - 1)$ блоков ключа выбираются **без возвращения** из $\{0, 1\}^n \setminus \{X_1, \dots, X_u\}$.

Вероятность получить хэш из множества W

$$\Pr(\mathbf{MH2}(H, M) \in W) \leq \frac{|W| + 1}{2^n - u - m - s + 2} \approx \frac{|W|}{2^n} + \frac{1}{2^n}, \quad u + m + s \leq 2^n.$$

РЕЗУЛЬТАТ

ЛЕММА

M – ненулевое сообщение из $\ell \leq s \cdot m$ блоков.

$(m + s - 1)$ блоков ключа выбираются **без возвращения** из $\{0, 1\}^n \setminus \{X_1, \dots, X_u\}$.

Вероятность получить хэш из множества W

$$\Pr(\mathbf{MH2}(H, M) \in W) \leq \frac{|W| + 1}{2^n - u - m - s + 2} \approx \frac{|W|}{2^n} + \frac{1}{2^n}, \quad u + m + s \leq 2^n.$$

Легко обобщается на:

- другие схемы выбора блоков ключа;
- недвоичные поля.

При $s = 1$ получаем **MH** из **MH2**.

СЛЕДСТВИЕ

ВЕРОЯТНОСТЬ КОЛЛИЗИИ (AU и AXU) ПРИ ВЫХОДЕ $\tau \leq n$ БИТ

$$\epsilon_{\text{MH2}} \approx 2^{-n} + 2^{-\tau}$$

- Рост вероятности не более чем вдвое, $\epsilon_{\text{MH2}} \approx 2 \cdot 2^{-n}$ при $\tau = n$
– теряем не более одного бита стойкости.
- При $\tau < n$ вероятность почти совпадает с «идеальной», $\epsilon_{\text{MH2}} \approx 2^{-\tau}$.

ТОЧНОСТЬ ОЦЕНКИ

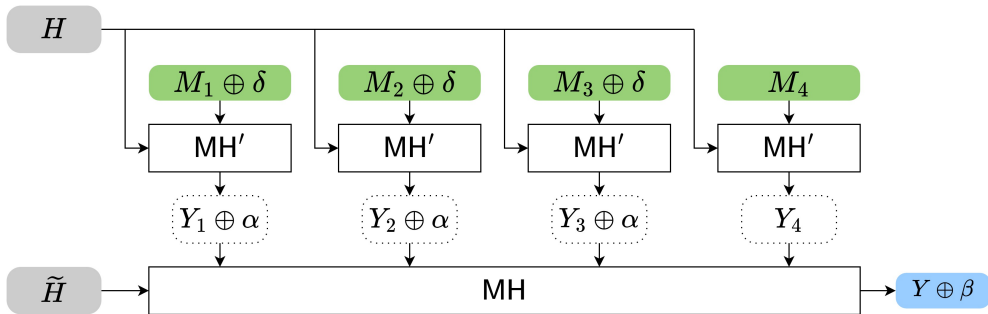
Дано: сообщение M , ключ секретен

Задача: построить сообщение M' с таким же хэшем (нулевой разностью)

Атака: внесём разность δ с двумя ненулевыми блоками в три секции, в каждой секции получаем разность α , в результате хэширования – разность β .

Вероятность успеха: $2^{-n} + 2^{-r} \approx \Pr(\alpha = 0) + \Pr(\alpha \neq 0 \cap \beta = 0)$.

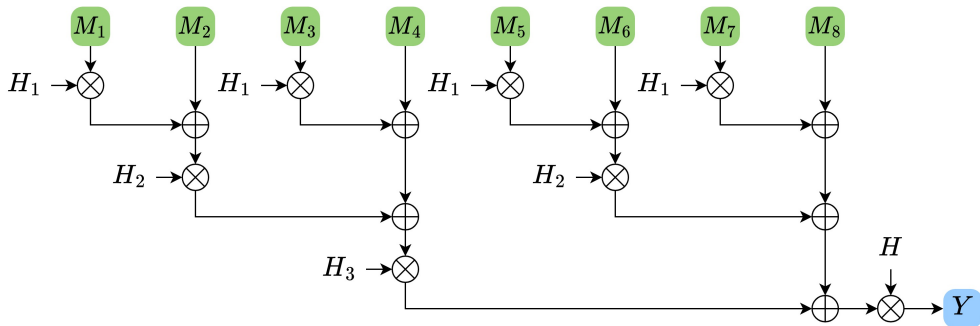
В каждой попытке меняем номера/значения блоков и номера секций.



ОБОБЩЕНИЕ

Легко обобщить с двух уровней до N , но:

- вероятность коллизии растёт в N раз, а не в 2
– теряем не один бит стойкости, а $\log_2(N)$
- техническая сложность реализации увеличивается
- выигрыш в скорости сомнителен



ПРАКТИЧЕСКОЕ ПРИМЕНЕНИЕ

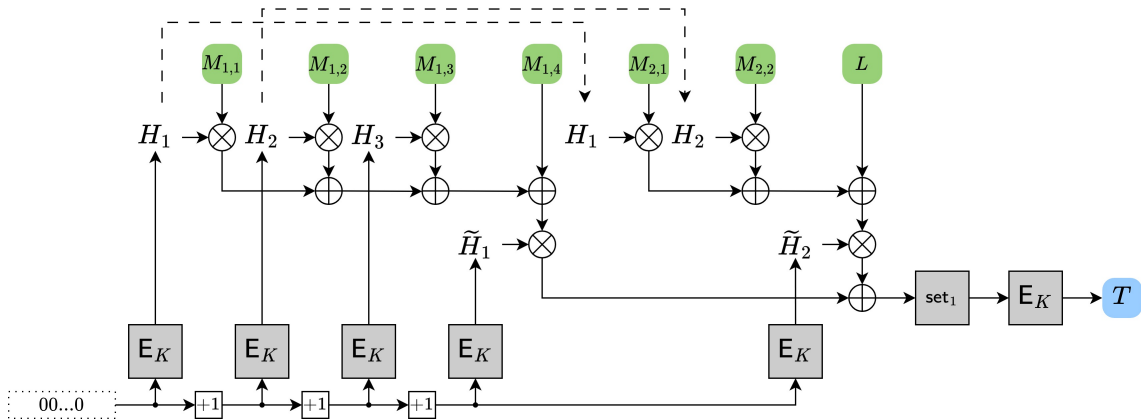
ПРАКТИЧЕСКОЕ ПРИМЕНЕНИЕ

Замена **МН** на **МН2** даёт режимам работы шифра:

- **ускорение** вплоть до паритета с **РН**
- **улучшение оценок стойкости** за счёт снижения длины ключа

ПСЕВДОСЛУЧАЙНАЯ ФУНКЦИЯ MH2-PRF

Аналог **MGM2-PRF** [CTCrypt 2024]



ПСЕВДОСЛУЧАЙНАЯ ФУНКЦИЯ **MH2-PRF**

ТЕОРЕМА

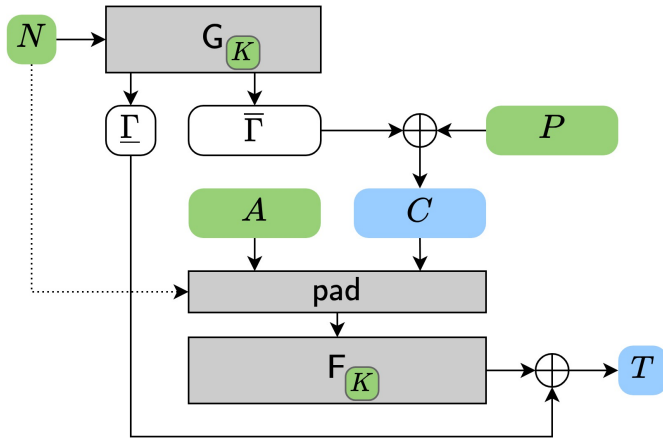
Преобладание противника, решающего задачу различения «алгоритм **MH2-PRF** или случайная функция», не превосходит

$$\text{Adv}_{\text{MH2-PRF}}^{\text{PRF}}(t, q, l) \leq \text{Adv}_{\text{E}}^{\text{PRP}}(t', q') + \frac{7(q^2 - q)}{2^{n+1}}, (q + s + m) \leq 2^{n-1}.$$

ПРИМЕР

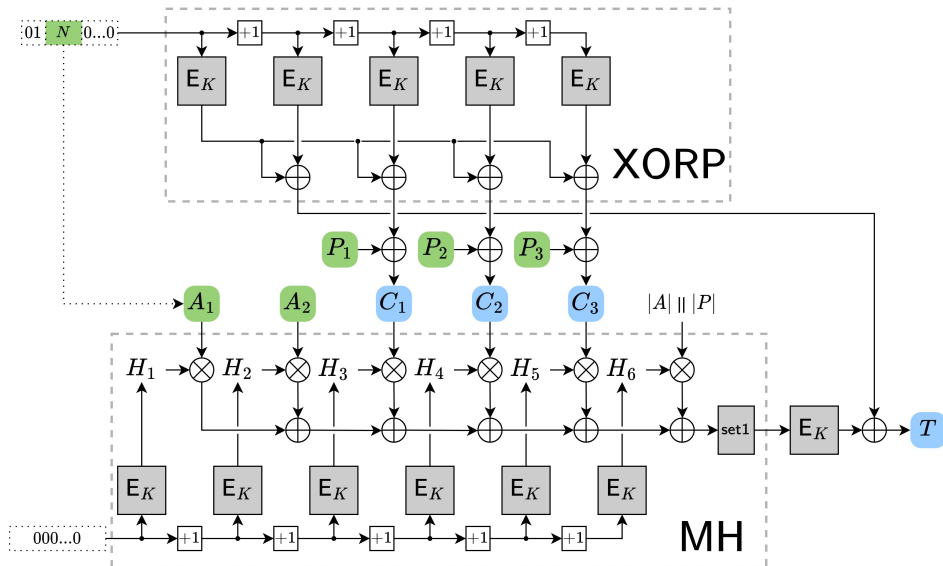
Шифр «Магма», $n = 64$, $\pi_{\text{mac}} = 2^{-10}$.

На одном ключе можно имитозащитить до $q = 2^{26}$ сообщений длины до $\ell = 2^{124}$ блоков каждое.

AEAD-РЕЖИМ **МХР** [СТCРУПТ 2025]

- Один ключ у блочного шифра
- Допустимая нагрузка на ключ много больше $2^{\frac{n}{2}}$ (BBV)

AEAD-РЕЖИМ МХР [СТСРyПТ 2025]



AEAD-РЕЖИМ **МХР** – ОБОБЩЕНИЕ ДЛЯ ПРОИЗВОЛЬНЫХ **G** И **F**

ТЕОРЕМА

Преобладание противника, атакующего **МХР** в модели NAE , не превосходит

$$\text{Adv}_{\mathbf{MXP}[E]}^{NAE}(t, q, v, a, p) \leq \text{Adv}_E^{PRP}(\tilde{t}, g + f) + \text{Adv}_{\mathbf{G}[\Pi]}^{PRF-EKU}(\infty, q + v, f) + v \cdot \text{Adv}_{\mathbf{F}[\Pi]}^{AXU}(\ell),$$

- q – число защищаемых пакетов (заголовков a блоков и ОТ p блоков);
- v – число попыток навязывания;
- ℓ – максимальная длина имитозащищаемых данных;
- $\tilde{t} = t + t' + g + f \approx t$ – вычислительные ресурсы противника.

G и **F** допускают эффективное вычисление за счёт g и f запросов к шифру $E(K, \cdot)$ и выполнено «разделение доменов».

AEAD-РЕЖИМ **МХР** – ОБОБЩЕНИЕ ДЛЯ ПРОИЗВОЛЬНЫХ **G** И **F**

ТЕОРЕМА [СТCRYPT 2025]

Преобладание в задаче различения «(**XORP**[Π], Π) или (R , Π)» не превосходит

$$\text{Adv}_{\mathbf{XORP}[\Pi]}^{\text{PRF-EKU}}(\infty, \chi, f) \leq \frac{2\chi^3\tilde{w}^4}{3 \cdot 2^{2n}} + \frac{2\chi\tilde{w}^2f^2}{2^{2n}} + \frac{2\chi^2f\tilde{w}^3}{2^{2n}} + \frac{\chi w}{2^n} + \frac{\chi w^2}{2^{n+1}},$$

- w – длина выхода **XORP** в n -битных блоках, $\tilde{w} = w + 1$,
- χ – число запросов к **XORP** или к случайной функции R ,
- f – число запросов к случайной подстановке Π .

ЛЕММА

$$\text{Adv}_{\mathbf{XORP}[\Pi]}^{\text{PRF-EKU}}(\infty, \chi, f) \leq \frac{\chi \cdot f \cdot (w + 1)}{2^n - f + 1} + \frac{\chi w}{2^n} + \frac{\chi w^2}{2^{n+1}}$$

- более точный результат для **МН2** из-за короткого ключа – малого f .

AEAD-РЕЖИМ МХР – ХАРАКТЕРИСТИКИ

ПРИМЕР

Шифр «Магма», $n = 64$, $\pi_{\text{mac}} = \pi_{\text{enc}} = 2^{-10}$.

G = XORP с длиной выхода $w = 15$ (16 шифрований).

F = MH2 с длиной секции $s = 15$.

Оперативная память: около 20 блоков – ключ MH2, счётчики и др.

Скорость: на блок ОТ одно умножение и $1.13 \approx (1 + 1/s + 1/w)$ шифрований.

Нагрузка на ключ:

$q \leq 2^{34}$ сообщений по $\ell \leq 2^{12}$ блоков, всего $q \cdot \ell \leq 2^{46}$ блоков.

ЗАКЛЮЧЕНИЕ

ЗАКЛЮЧЕНИЕ

1. **МН2** – двухуровневая мультилинейная хэш-функция – практическое повышение производительности вплоть до уровня **РН** при стойкости почти как у **МН**.

ЗАКЛЮЧЕНИЕ

1. **МН2** – двухуровневая мультилинейная хэш-функция – практическое повышение производительности вплоть до уровня **РН** при стойкости почти как у **МН**.
2. Замена **МН** на **МН2** позволяет не только ускорить вычисления, но и увеличить нагрузку на ключ – **МН2-PRF**, **МХР** с **МН2** и т.д.

В следующих сериях...

МХР с «длинными» синхропосылками и SIV-режим работы.

Благодарю за внимание!

Референсные реализации:

<https://gitflic.ru/project/vkir/mxp>

ВИТАЛИЙ КИРЮХИН

ООО «СФБ Лаб»

СТCrypt 2026

2 июня 2026

vitaly.kiryukhin@sfblaboratory.ru

