

МЕТОДЫ ПОСТРОЕНИЯ ПРООБРАЗОВ ДЛЯ ХЭШ-ФУНКЦИЙ BELT-COMPRESS И BELT-HASH

ВИТАЛИЙ КИРЮХИН

ООО «СФБ Лаб»

CTCrypt 2026

4 июня 2026

vitaly.kiryukhin@sfblaboratory.ru



КЛАССИЧЕСКИЕ ЗАДАЧИ КРИПТОАНАЛИЗА ХЭШ-ФУНКЦИЙ

Хэш-функция **Hash**: $\{0, 1\}^* \rightarrow \{0, 1\}^n$

ПРООБРАЗ

Условие: поиск M к заданному хэш-значению H , для которого **Hash**(M) = H

Сложность: 2^n

ВТОРОЙ ПРООБРАЗ

Условие: поиск к заданному M иного $\tilde{M}$, для которых **Hash**(M) = **Hash**($\tilde{M}$)

Сложность: 2^n

БАЗОВЫЕ АЛГОРИТМЫ

- Шифрование блока – **belt-block**
- Шифрование широкого блока
- Сжатие – **belt-compress**

АЛГОРИТМЫ ШИФРОВАНИЯ И КОНТРОЛЯ ЦЕЛОСТНОСТИ

- Шифрование в режиме ...
- Выработка имитовставки
- Аутентифицированное шифрование ...
- **Хэширование – belt-hash**
- Дисковое шифрование
- Шифрование с сохранением формата

ГОСУДАРСТВЕННЫЙ СТАНДАРТ
РЕСПУБЛИКИ БЕЛАРУСЬ

СТБ 34.101.31-2020

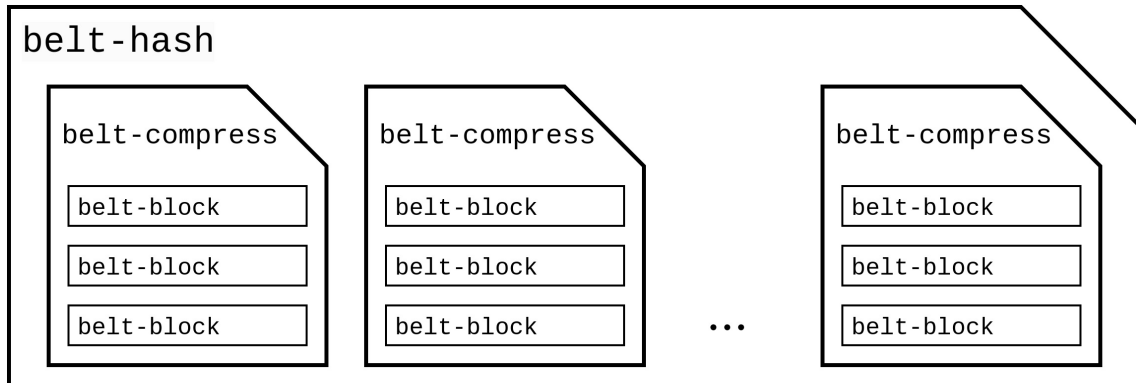
Информационные технологии и безопасность
АЛГОРИТМЫ ШИФРОВАНИЯ И КОНТРОЛЯ
ЦЕЛОСТНОСТИ

Інфармацыйныя тэхналогіі і бяспека
АЛГАРЫТМЫ ШЫФРАВАННЯ І КАНТРОЛЮ
ЦЭЛАСНАСЦІ



Госстандарт
Мінск

BELT-BLOCK – BELT-COMPRESS – BELT-HASH

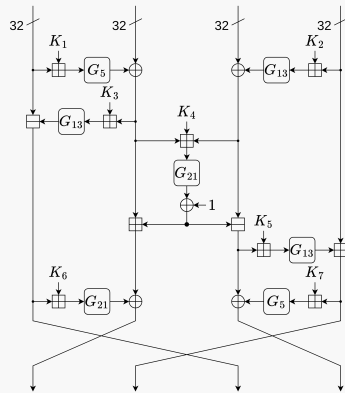


Блочный шифр BELT-BLOCK

ХАРАКТЕРИСТИКИ

- Ключ 256 бит
- Блок 128 бит
- 8 раундов
- Схема Ляя-Мэсси

РАУНДОВАЯ ФУНКЦИЯ



ФУНКЦИЯ СЖАТИЯ BELT-COMPRESS

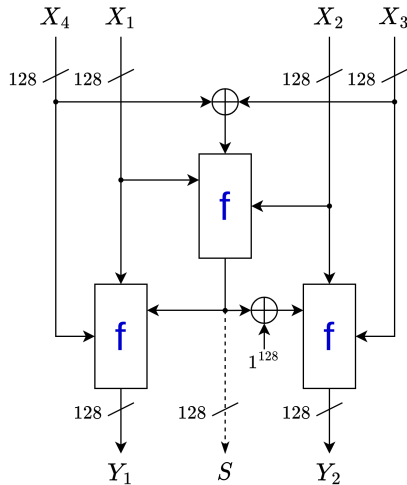
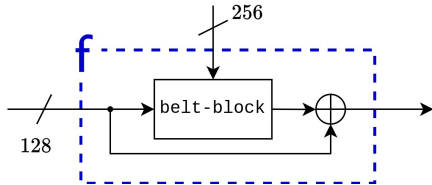
ХАРАКТЕРИСТИКИ

Вход: 512 бит

Выход: 256 [+ 128] бит

3 обращения к **f**

f – belt-block в схеме ДМ

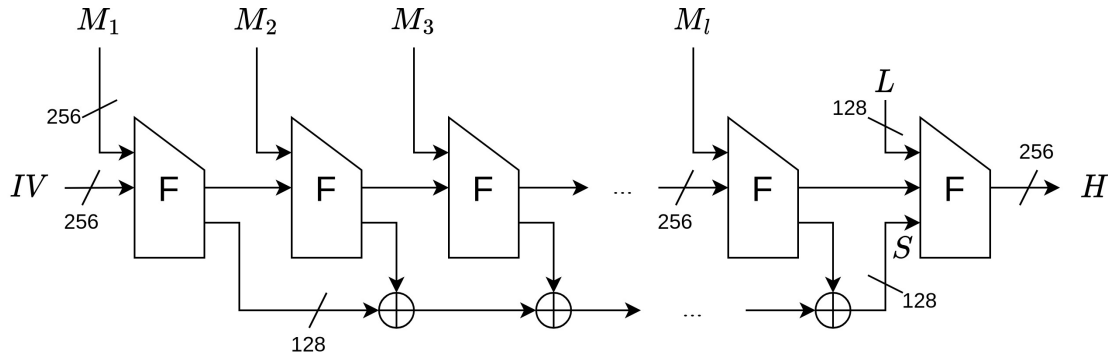


ФУНКЦИЯ ХЭШИРОВАНИЯ BELT-HASH

Схема МД + механизм контрольной суммы (КС).

Блок/состояние/хэш-значение по 256 бит, КС – 128 бит.

F = belt-compress.



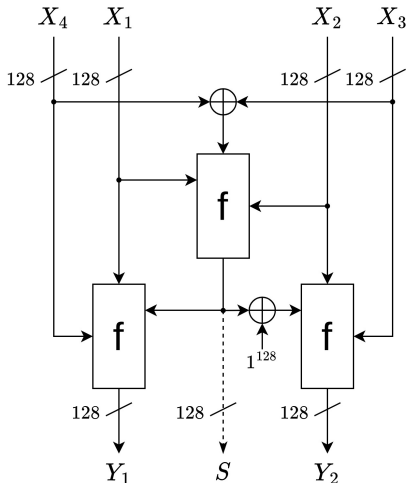
ПРООБРАЗ ДЛЯ BELT-COMPRESS

BELT-COMPRESS: ПРООБРАЗ

ЗАДАЧА

Дан выход (Y_1, Y_2, S) – 384 бита

Найти вход (X_1, X_2, X_3, X_4) – 512 бит



BELT-COMPRESS: ПРООБРАЗ

ЗАДАЧА

Дан выход (Y_1, Y_2, S) – 384 бита

Найти вход (X_1, X_2, X_3, X_4) – 512 бит

НАБЛЮДЕНИЕ

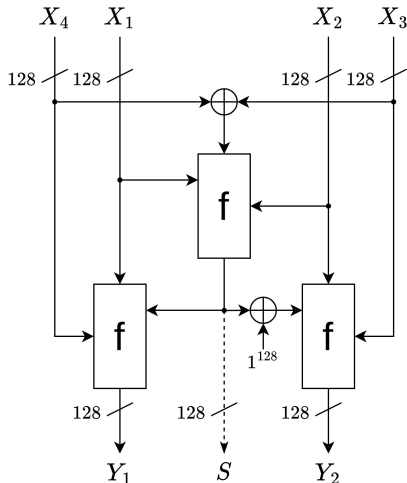
При зафиксированном S :

- вычисление Y_1 зависит только от (X_1, X_4)
- вычисление Y_2 зависит только от (X_2, X_3)

$$S = \mathbf{f}(X_3 \oplus X_4, X_1 \parallel X_2)$$

$$Y_1 = \mathbf{f}(X_1, S \parallel X_4)$$

$$Y_2 = \mathbf{f}(X_2, (S \oplus 1^{128}) \parallel X_3)$$



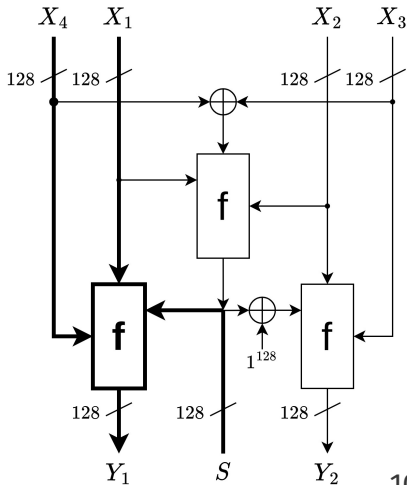
BELT-COMPRESS: ПРООБРАЗ

ШАГ 1

Переберём $N_1 = 2^{192}$ пар $(\tilde{X}_1, \tilde{X}_4)$.

Для каждой вычисляем $\tilde{Y}_1$.

Получим и сохраним $2^{64} = N_1 / 2^{128}$ значений равных Y_1 .



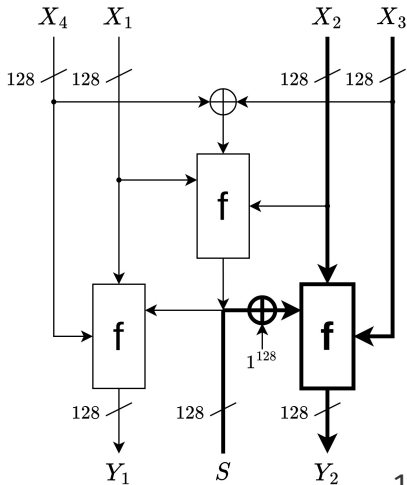
BELT-COMPRESS: ПРООБРАЗ

ШАГ 2

Переберём $N_2 = 2^{192}$ пар $(\tilde{X}_2, \tilde{X}_3)$.

Для каждой вычисляем $\tilde{Y}_2$.

Получим $2^{64} = N_2 / 2^{128}$ значений равных Y_2 .



BELT-COMPRESS: ПРООБРАЗ

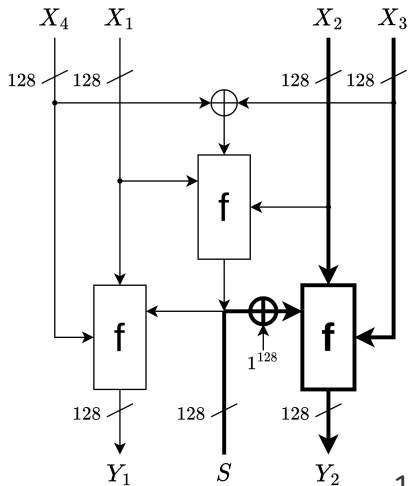
ШАГ 2

Переберём $N_2 = 2^{192}$ пар $(\tilde{X}_2, \tilde{X}_3)$.

Для каждой вычисляем $\tilde{Y}_2$.

Получим $2^{64} = N_2 / 2^{128}$ значений равных Y_2 .

Получили 2^{128} четвёрок $(\tilde{X}_1, \tilde{X}_2, \tilde{X}_3, \tilde{X}_4)$,
каждая из которых даёт (Y_1, Y_2) .



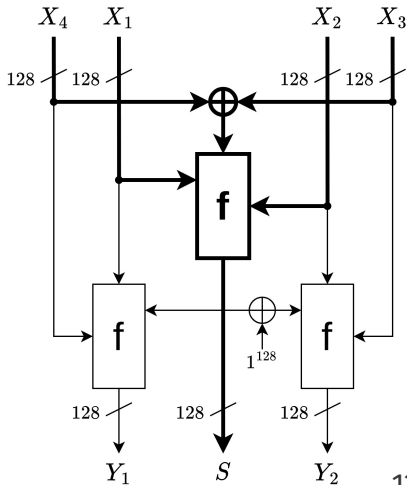
BELT-COMPRESS: ПРООБРАЗ

ШАГ 3

Для каждой четвёрки $(\tilde{X}_1, \tilde{X}_2, \tilde{X}_3, \tilde{X}_4)$ вычислим $\tilde{S}$.

Проверим $S \stackrel{?}{=} \tilde{S}$.

В среднем будет одно решение – прообраз.



BELT-COMPRESS: ПРООБРАЗ

СЛОЖНОСТЬ МЕТОДА**Время:**

$$t = \frac{1}{3}2^{193} = \frac{1}{3} \left(N_1 + N_2 + \frac{N_1 N_2}{2^{256}} \right) \text{ операций belt-compress.}$$

Память:

$$\sigma = 2^{64} = \frac{N_1}{2^{128}} \text{ блоков } (2^{72} \text{ бит}).$$

Снижение стойкости: на 64 и более бит.

BELT-COMPRESS: МУЛЬТИПРООБРАЗ

К заданному хэшу можно построить μ прообразов – мультипрообраз.
Увеличиваем N_1 и N_2 так, чтобы

$$\frac{N_1 \cdot N_2}{2^{384}} = \mu.$$

ПРИМЕР

Построим $\mu = 2^{32}$ прообразов.

Выберем $N_1 = N_2 = 2^{192+16}$.

Сложность: $t = \frac{1}{3}2^{209}$, $\sigma = 2^{80}$.

BELT-COMPRESS: ПРООБРАЗ С ОГРАНИЧЕНИЯМИ

До 128 бит совокупно в $(\tilde{X}_1, \tilde{X}_4)$ и в $(\tilde{X}_2, \tilde{X}_3)$

можно зафиксировать произвольным образом.

Можем строить «удобные» прообразы, с ведущими нулевыми битами и т.д.

BELT-COMPRESS: ПРООБРАЗ С КОМПРОМИССОМ ВРЕМЯ/ПАМЯТЬ

Уменьшаем N_1 и увеличиваем N_2 так, чтобы

$$N_1 \cdot N_2 = 2^{384},$$

память $\sigma = \frac{N_1}{2^{128}}$, время $t = \frac{1}{3} \cdot \frac{N_2}{2^{128}}$.

ПРИМЕР

Выберем $N_1 = 2^{160}$, $N_2 = 2^{224}$.

Сложность: $t = \frac{1}{3} 2^{225}$, $\sigma = 2^{32}$.

BELT-COMPRESS: ПРООБРАЗ И ПРЕДВЫЧИСЛЕНИЯ

- Пусть значение S задано.
- Сохраняем в памяти вычисления шагов 1 и 2, $\sigma = 2 \cdot N \cdot 2^{64}$, для $N \leq 2^{128}$ «удобных» Y_1 и Y_2 .
- Прообраз к (Y_1, Y_2) из «удобных» значений, можно построить за $t = \frac{1}{3} \cdot 2^{128}$ операций.

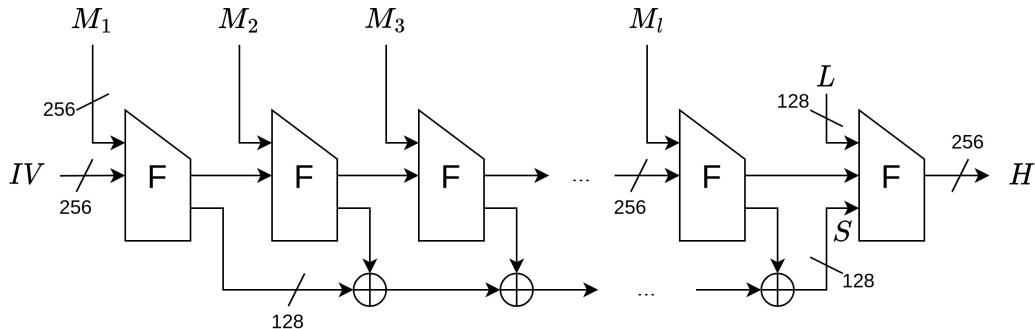
ПРООБРАЗ ДЛЯ BELT-HASH

BELT-HASH: ПРООБРАЗ

ЗАДАЧА

Дан выход H – 256 бит.

Найти подходящий вход $M = (M_1, M_2, \dots)$ произвольной длины.



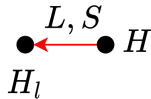
BELT-HASH: ПРООБРАЗ

Шаг 1

Строим прообраз к H для belt-compress. Блок L выбираем «достаточно малым». Получаем состояние H_ℓ , блок L (длину сообщения) и блок S (КС сообщения).

Сложность: $t_1 = \frac{1}{3} \cdot 2^{193}$.

$IV \bullet$



BELT-HASH: ПРООБРАЗ

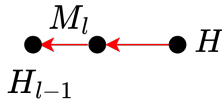
Шаг 2

Строим прообраз к H_ℓ для belt-compress.

Получаем «удобный» $H_{\ell-1}$ и M_ℓ .

Сложность: $t_2 = \frac{1}{3} \cdot 2^{193}$.

$IV \bullet$



BELT-HASH: ПРООБРАЗ

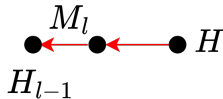
ШАГ 3 – ПРЕДВЫЧИСЛЕНИЯ

Выполним предвычисления для построения прообразов к «удобным» хэсам.

Сложность: $t_3 = \frac{1}{3} \cdot 2^{195}$, $\sigma = 2^{133}$, $N_1 = N_2 = 2^{194}$.

Для любого «удобного» хэша сможем построить хотя бы два прообраза.

$IV \bullet$



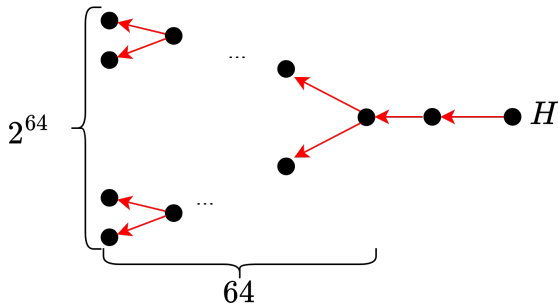
BELT-HASH: ПРООБРАЗ

ШАГ 4 – ДРЕВОВИДНЫЙ МУЛЬТИПРООБРАЗ

Для каждого состояния строим два прообраза до тех пор, пока их не станет 2^{64} .

Сложность: $t_4 = \frac{1}{3}2^{129} \cdot 2^{64} = \frac{1}{3}2^{193}$.

IV ●



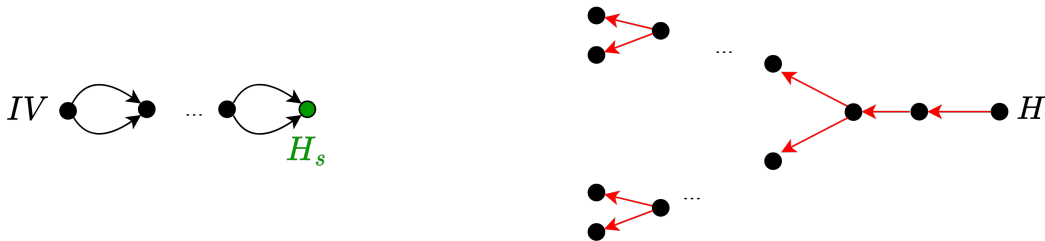
BELT-HASH: ПРООБРАЗ

ШАГ 5 – МУЛЬТИКОЛЛИЗИЯ В ПРЕФИКСЕ

Начиная с IV строим последовательно 128 коллизий.

Сможем потом подобрать префикс с нужной КС.

Сложность: $t_5 = 128 \cdot 2^{129}$.

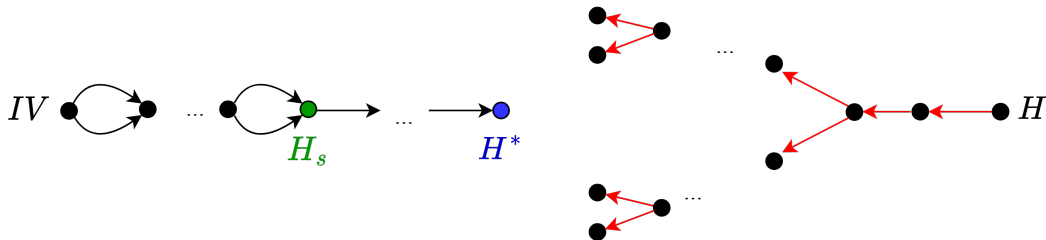


BELT-HASH: ПРООБРАЗ

Шаг 6

Продлеваем префикс до целевой длины.

Сложность: $t_6 \leq \ell$.

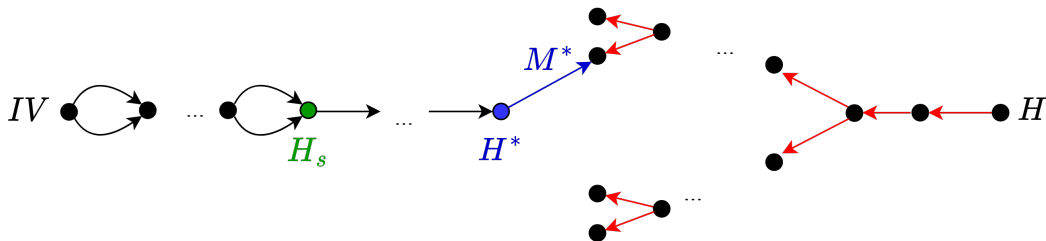


BELT-HASH: ПРООБРАЗ

ШАГ 7 – СОГЛАСОВАНИЕ

Перебираем M^* до получения одного из листьев дерева.

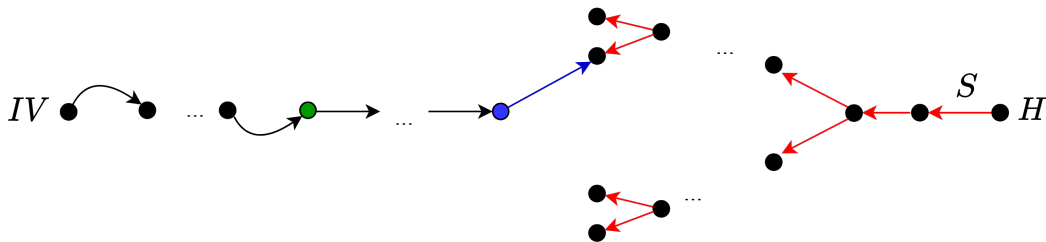
Сложность: $t_7 = 2^{256}/2^{64} = 2^{192}$.



BELT-HASH: ПРООБРАЗ

Шаг 8

Подбираем префикс так, чтобы КС у получившегося прообраза была равна S .
Сложность: $t_8 = 2^{65}$.



BELT-HASH: ПРООБРАЗ

СЛОЖНОСТЬ МЕТОДА**Время:**

$$t \approx t_1 + t_2 + t_3 + t_4 + t_7 \approx \frac{1}{3}2^{196} \text{ операций belt-compress.}$$

Память:

$$\sigma = 2^{133} \text{ блоков } (2^{141} \text{ бит}).$$

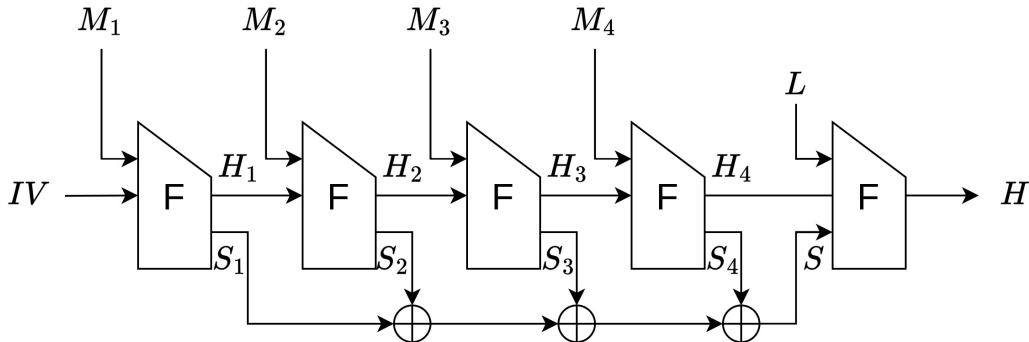
Снижение стойкости: на ≈ 62 бита.

BELT-HASH: КОРОТКИЙ ПРООБРАЗ

ЗАДАЧА

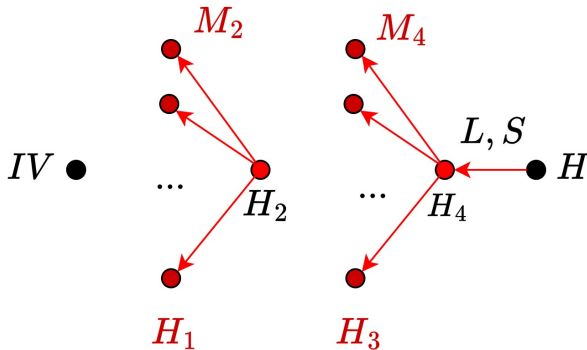
Дан выход H – 256 бит.

Найти подходящий вход $M = (M_1, M_2, M_3, M_4)$ из 4 блоков.



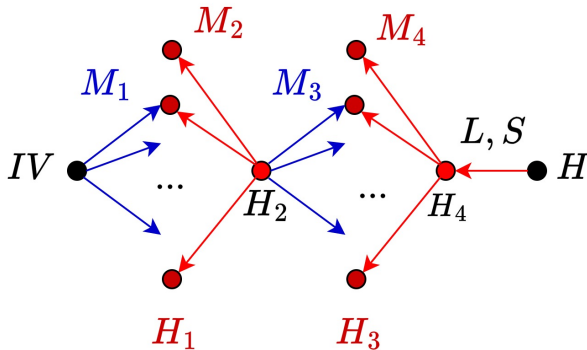
BELT-HASH: КОРОТКИЙ ПРООБРАЗ

1. Прообраз для H при $L = \text{const}$. Получаем (H_4, S) . $t_1 = \frac{1}{3} \cdot 2^{193}$.
2. μ -прообраз для H_4 при $S_4 = \text{const}$. Получаем $\mu = 2^{86}$ пар (H_3, M_4) . $t_2 = \frac{1}{3} \cdot 2^{236}$.
3. μ -прообраз для $(H_2, S_2) = \text{const}$. Получаем $\mu = 2^{86}$ пар (H_1, M_2) . $t_3 = \frac{1}{3} \cdot 2^{236}$.



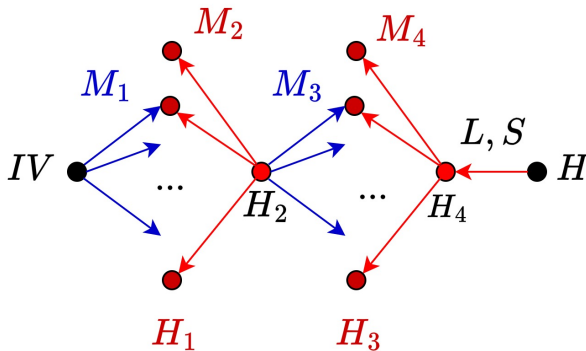
BELT-HASH: КОРОТКИЙ ПРООБРАЗ

4. Перебор M_1 . Получаем $\alpha = 2^{64} = t_4 \cdot \mu / 2^{256}$ пар (M_1, M_2) . $t_4 = 2^{234}$.
5. Перебор M_3 до согласования с H_3 и КС, $t_5 = 2^{234}$. Условие $\alpha \cdot t_5 \cdot \mu / 2^{384} = 1$.



BELT-HASH: КОРОТКИЙ ПРООБРАЗ

4. Перебор M_1 . Получаем $\alpha = 2^{64} = t_4 \cdot \mu / 2^{256}$ пар (M_1, M_2) . $t_4 = 2^{234}$.
5. Перебор M_3 до согласования с H_3 и КС, $t_5 = 2^{234}$. Условие $\alpha \cdot t_5 \cdot \mu / 2^{384} = 1$.



Время $t = 2^{236}$, память $\sigma = 2^{107}$, снижение стойкости на 20 бит.

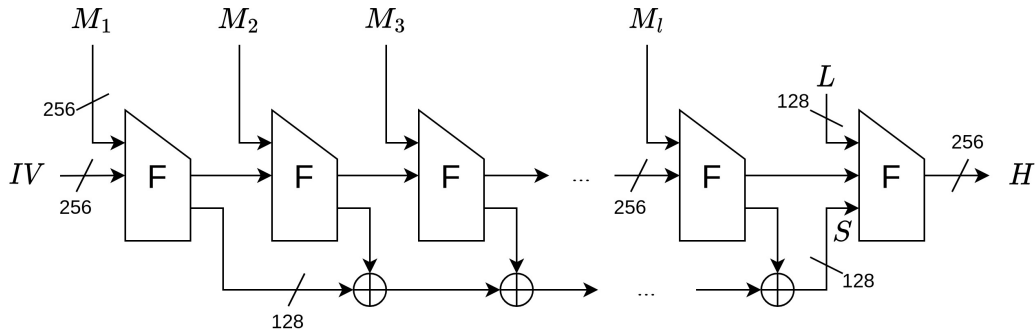
ВТОРОЙ ПРООБРАЗ ДЛЯ BELT-HASH

BELT-HASH: ВТОРОЙ ПРООБРАЗ

ЗАДАЧА

Дан вход $M = (M_1, M_2, \dots, M_\ell)$ произвольной длины.

Найти иной вход $\tilde{M}$ с таким же хэшем.



BELT-HASH: ВТОРОЙ ПРООБРАЗ

ЗАДАЧА

Дан вход $M = (M_1, M_2, \dots, M_\ell)$ произвольной длины.
Найти вход $\tilde{M}$ с таким же хэшем.

При $\ell \leq 2^{62}$ пользуемся методом построения *прообраза*.
При $\ell > 2^{62}$ можем действовать эффективнее,
не используя специфику belt-compress

BELT-HASH: ВТОРОЙ ПРООБРАЗ

Покажем, что механизм КС не повышает защиту от универсальных методов.



Joux A.

MULTICOLLISIONS IN ITERATED HASH FUNCTIONS. APPLICATION TO CASCADED CONSTRUCTIONS

CRYPTO 2004



Kelsey J., Schneier B.

SECOND PREIMAGES ON N-BIT HASH FUNCTIONS FOR MUCH LESS THAN 2^n WORK

Москва: EUROCRYPT 2005



Kelsey J., Kohno T.

HERDING HASH FUNCTIONS AND THE NOSTRADAMUS ATTACK

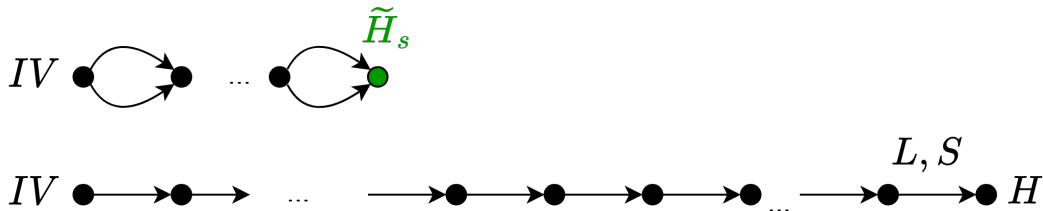
EUROCRYPT 2006

BELT-HASH: ВТОРОЙ ПРООБРАЗ

ШАГ 1 – МУЛЬТИКОЛЛИЗИЯ В ПРЕФИКСЕ

Начиная с IV строим последовательно 128 коллизий.
Сможем потом подобрать префикс с нужной КС.

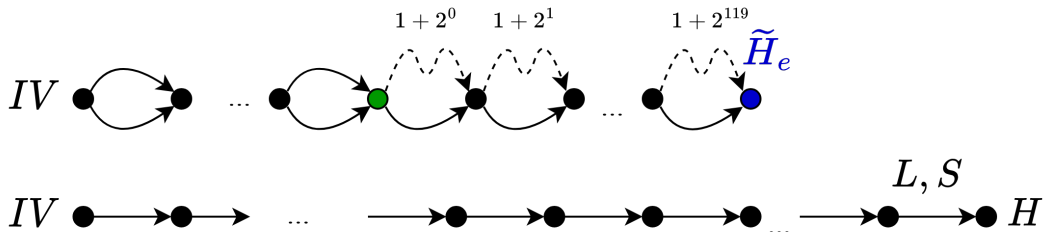
$$t_1 = 128 \cdot 2^{129}.$$



Начиная с *IV* строим последовательно 120 коллизий.

Сможем потом подобрать префикс с нужной длиной от 256 до $256 + 2^{120}$.

$$t_2 = 120 \cdot 2^{128}.$$

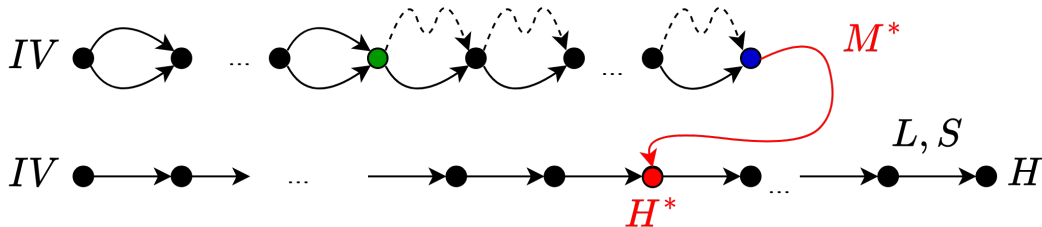


BELT-HASH: ВТОРОЙ ПРООБРАЗ

ШАГ 3 – СОГЛАСОВАНИЕ СОСТОЯНИЯ

Перебираем M^* до получения одного из состояний.

$$t_3 = 2^{256}/\ell.$$

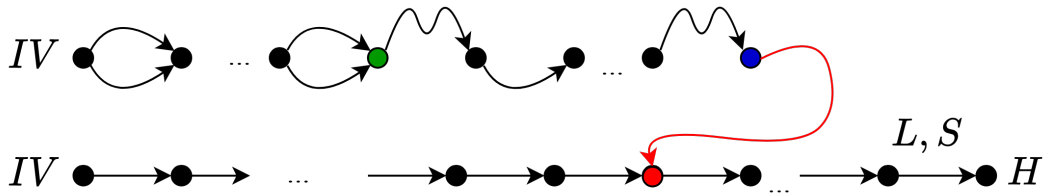


BELT-HASH: ВТОРОЙ ПРООБРАЗ

ШАГ 4 – СОГЛАСОВАНИЕ ДЛИНЫ

Подбираем префикс нужной длины ℓ .

$$t_4 \leq \ell.$$

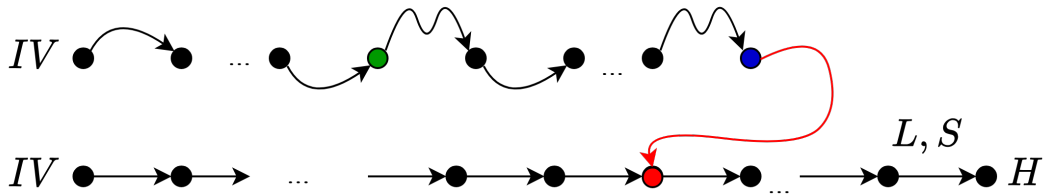


BELT-HASH: ВТОРОЙ ПРООБРАЗ

ШАГ 5 – СОГЛАСОВАНИЕ КС

Подбираем префикс с нужной КС.

$$t_5 \leq 2^{65}.$$



BELT-HASH: ВТОРОЙ ПРООБРАЗ

СЛОЖНОСТЬ МЕТОДА

Время:

$$t \approx \min(2^{196} / 3, 2 \cdot 2^{136} + 2^{256} / \ell),$$

$$t \approx 3 \cdot 2^{136} \text{ при } \ell = 2^{120}.$$

Память:

$$\sigma = 2 \cdot \ell \text{ блоков.}$$

Снижение стойкости: на 120 бит.

ЗАКЛЮЧЕНИЕ

1. Прообраз для belt-compress, $t = 2^{193} / 3$ вместо 2^{256} .
2. Прообраз для belt-hash, $t = 2^{196} / 3$ вместо 2^{256} .
3. Второй прообраз для belt-hash, $t = 3 \cdot 2^{136}$ – как для схемы МД без КС.

Благодарю за внимание!

ВИТАЛИЙ КИРЮХИН

ООО «СФБ Лаб»

СТCrypt 2026

4 июня 2026

vitaly.kiryukhin@sfblaboratory.ru

