

О стойкости алгоритмов belt-hash и belt-compress

Сергей Агиевич

НИИ прикладных проблем математики и информатики

Белорусский государственный университет

2026-06-04 [Минск]



Содержание

1. Целевые алгоритмы
2. Задачи криптоанализа
3. Обоснование стойкости
4. Атаки

Целевые алгоритмы

Алгоритм belt-hash

- хэширование $\{0, 1\}^* \rightarrow \{0, 1\}^{256}$;
- разработан в 2003 году;
- стандартизирован в 2007 году (СТБ П 34.101.31-2007);
- перенесен сначала в СТБ 34.101.31-2011, затем в СТБ 34.101.31-2020;
- основан на алгоритме belt-compress.

Алгоритм belt-compress

- хэширование $\{0, 1\}^{4 \cdot 128} \rightarrow \{0, 1\}^{2 \cdot 128}$
(с дополнительным выходом $\in \{0, 1\}^{128}$);
- используется функция сжатия $f: \{0, 1\}^{3 \cdot 128} \rightarrow \{0, 1\}^{128}$;
- функция f строится по блочному шифру
 $\text{Belt} = \{\text{Belt}_K: K \in \{0, 1\}^{2 \cdot 128}\} \subset \text{Perm}(\{0, 1\}^{128})$.

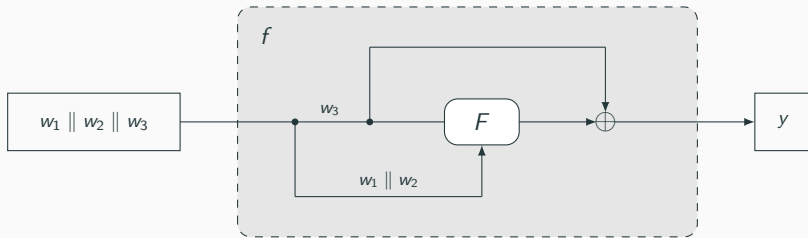
Обобщение: функция сжатия

Схема belt-hash[belt-compress[Belt]] обобщается через замену Belt на блочный шифр

$$F = \{F_K : K \in \{0, 1\}^{2n}\} \subset \text{Perm}(\{0, 1\}^n).$$

Функция сжатия $f: \{0, 1\}^{3n} \rightarrow \{0, 1\}^n$

$$w_1 \parallel w_2 \parallel w_3 \mapsto F_{w_1 \parallel w_2}(w_3) \oplus w_3, \quad w_i \in \{0, 1\}^n :$$

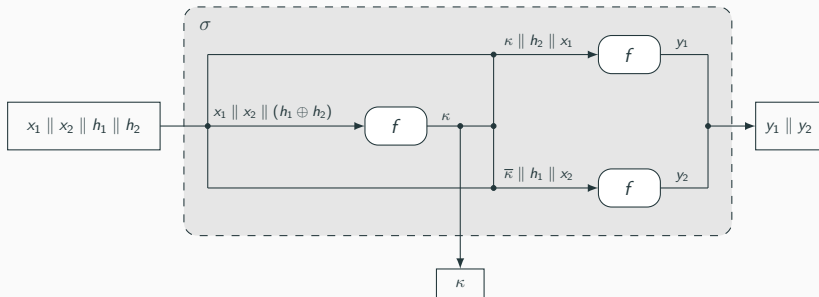


Обобщение: шаговая функция хэширования

Шаговая функция хэширования $\sigma: \{0, 1\}^{4n} \rightarrow \{0, 1\}^{2n}$

$$x_1 \parallel x_2 \parallel h_1 \parallel h_2 \mapsto f(\kappa \parallel h_2 \parallel x_1) \parallel f(\bar{\kappa} \parallel h_1 \parallel x_2), \quad x_i, h_i \in \{0, 1\}^n,$$

где $\kappa = f(x_1 \parallel x_2 \parallel (h_1 \oplus h_2)) = \sigma_1(\cdot)$ — дополнительный выход;
черта над κ — поразрядное битовое отрицание:



Обобщение: функция хэширования

Функция хэширования $\Phi: \{0, 1\}^* \rightarrow \{0, 1\}^{2n}$

1. $X' \leftarrow X \parallel 0^t$, $t = (2n - (|X| \bmod 2n)) \bmod 2n$.
2. $(X_1, X_2, \dots, X_m) \leftarrow \text{Split}(X', 2n)$.
3. $S \leftarrow 0^{2n}$ (*контрольная сумма*).
4. $Y \leftarrow \text{const} \in \{0, 1\}^{2n}$.
5. Для $i = 1, 2, \dots, m$:
 - 5.1 $(\kappa, Y) \leftarrow (\sigma_1, \sigma)(X_i \parallel Y)$ (*3 зашифрования на 2 блока X_i*);
 - 5.2 $S \leftarrow S \oplus \kappa$.
6. $Y \leftarrow \sigma(\langle |X| \rangle_n \parallel S \parallel Y)$ (*нестандартное MD-усиление: учитывается контрольная сумма*).
7. Возвратить Y .

Кратко: хэширование с удвоенным блоком, «усиленным» MD-усилением и коэффициентом эффективности $2/3$.

Задачи криптоанализа

Задачи криптоанализа

Задачи криптоанализа относительно $\varphi: \mathcal{X} \rightarrow \mathcal{Y}$

- 1) $\text{Pre}[\varphi]: \mathcal{Y} \ni Y \mapsto X \in \mathcal{X}: \varphi(X) = Y$
(*обращение*);
- 2) $\text{Pre2}[\varphi]: \mathcal{X} \ni X' \mapsto X \in \mathcal{X}: \varphi(X) = \varphi(X'), X \neq X'$
(*построение второго прообраза*);
- 3) $\text{Coll}[\varphi]: \perp \mapsto (X, X') \in \mathcal{X} \times \mathcal{X}: \varphi(X) = \varphi(X'), X \neq X'$
(*построение коллизии*).

задача	требования*	
	стандартные	облегченные (sponge-криптография)
$\text{Pre}[\varphi]$	$T = \Omega(\mathcal{Y})$	$T = \Omega(\mathcal{Y} ^{1/2})$
$\text{Pre2}[\varphi]$	$T = \Omega(\mathcal{Y})$	$T = \Omega(\mathcal{Y} ^{1/2})$
$\text{Coll}[\varphi]$	$T = \Omega(\mathcal{Y} ^{1/2})$	$T = \Omega(\mathcal{Y} ^{1/2})$

T — среднее число обращений к φ

Вопрос. Выполняются ли стандартные требования для $\sigma[f]$, $\Phi[f]$?

Идеализация

Будем считать, что f — случайная функция $\{0, 1\}^{3n} \rightarrow \{0, 1\}^n$.

Мотивация

В работах [Win84,PGV94,BRSS10] обосновывается надежность f (в контексте хеширования с ординарным блоком) при условии надежности F . Надежность f в том числе означает трудноотличимость от случайной функции.

Игра: начало

Противник $\mathcal{A}$ утверждает, что он может решить задачу $\varphi[f]$ для $\varphi \in \{\sigma, \Phi\}$.

Верификатор $\mathcal{V}$ проверяет, что это действительно так. Проверка выполняется в рамках протокола, который называется *игрой*.

Верификатор

1. Выбирает условие задачи. Это:
 - образ (хэш-значение) $Y \in \mathcal{Y}$ в задаче Pre;
 - прообраз $X' \in \mathcal{X}$ в задаче Pre2;
 - пустое условие в задаче Coll.
2. Передает условие задачи $\mathcal{A}$.
3. Выбирает случайную функцию сжатия f .
4. Открывает $\mathcal{A}$ доступ к f : противник может подать на вход f любое слово $R \in \{0, 1\}^{3n}$ и получить соответствующее значение $f(R)$.

Игра: поиск решения

Противник

1. Выполняет T обращений к f . Пусть $R_1, R_2, \dots, R_T$ — *стенограмма* обращений. Будем считать, что в стенограмме исключены неинформативные повторы и, таким образом, все слова различны.
2. По входам и выходам f с незначительными накладными расходами (которые мы будем игнорировать) вычисляет значения $\varphi[f]$ (при необходимости).
3. Решает целевую задачу относительно $\varphi[f]$ и предъявляет полученное решение $\mathcal{V}$. Решением является:
 - прообраз $X \in \mathcal{X}$ в задаче Pre;
 - второй прообраз $X \in \mathcal{X}$ в задаче Pre2;
 - пара (X, X') в задаче Coll.

Игра: проверка решения

Верификатор

1. Обработывает решение с помощью $\varphi[f]$, проверяя выполнение следующих условий:
 - $\varphi[f](X) = Y$ в задаче Pre;
 - $\varphi[f](X) = \varphi[f](X')$ и $X \neq X'$ в задачах Pre2 и Coll.

Все входы f в процессе вычисления $\varphi[f](X)$ должны входить в стенограмму. Если это правило нарушено, то проверка завершается с ошибкой.

2. Возвращает признак успеха b .

Преобладание

Преобладание (характеризует качество работы $\mathcal{A}$):

$$\text{Adv}_{\varphi[f]}^{\text{Atk}}(\mathcal{A}) = \mathbf{P} \{b = 1\}, \quad \text{Atk} \in \{\text{Pre}, \text{Pre2}, \text{Coll}\}.$$

Вероятность определяется случайным выбором f , а также случайной лентой, которую $\mathcal{A}$ использует в своей работе.

Вопрос (новая редакция). Верно ли, что для $\varphi \in \{\sigma, \Phi\}$ и $N = 2^n$ выполняется:

$$\text{Adv}_{\varphi[f]}^{\text{Atk}}(\mathcal{A}) = \begin{cases} O(T/N^2), & \text{Atk} = \text{Pre}, \text{Pre2}, \\ O(T/N), & \text{Atk} = \text{Coll?} \end{cases}$$

Спойлер: не обязательно.

Обоснование стойкости

Треугольники

При вычислении $(\kappa, y_1 \parallel y_2) \leftarrow (\sigma_1, \sigma)(x_1 \parallel x_2 \parallel h_1 \parallel h_2)$ выполняются 3 обращения к f : $f(R_a)$, $f(R_b)$ и $f(R_c)$. Слова тройки $\Delta = (R_a, R_b, R_c)$ связаны друг с другом, удовлетворяя определенным ограничениям (несложным, но громоздким).

Треугольник: всякая тройка Δ , слова которой удовлетворяют данным ограничениям.

Характеристики треугольника

- **вход** $\text{in}(\Delta)$ — слово $h_1 \parallel h_2$ (обновляемое хэш-значение);
- **выход** $\text{out}(\Delta)$ — слово $y_1 \parallel y_2$ (обновленное хэш-значение);
- **тело** $\text{body}(\Delta)$ — слово $x_1 \parallel x_2$ (фрагмент сообщения);
- **ключ** $\text{key}(\Delta)$ — слово k (добавляется к контрольной сумме).

Переформулировка задач (пример)

$\text{Pre}[\sigma[f]]$ — найти Δ с заданным выходом: $\text{out}(\Delta) = Y$.

Максимальное заполнение

Общая проблема (неформально). Одно и то же слово стенограммы может входить сразу в несколько треугольников. Чем больше треугольников, тем больше у противника шансов на успех. Нужно взять под контроль число треугольников.

Определения

Максимальное заполнение стенограммы $R_1, R_2, \dots, R_T$ — это величина

$$t = \max_{\kappa \in \{0,1\}^n} \sum_{i=1}^T [f(R_i) \stackrel{?}{=} \kappa],$$

Стенограмма выдерживает *отбраковку* с порогом τ , если $t < \tau$.

Ключевая лемма

В стенограмме объема T , выдержавшей отбраковку с порогом τ , не более τT треугольников.

Оценки максимального заполнения

1. Пусть $T \geq N \ln N$. Тогда

$$\mathbf{P} \{t \geq 6T/N\} \leq \frac{1}{N^2}.$$

2. Пусть $T \leq N \ln N$. Тогда

$$\mathbf{P} \{t \geq 6 \ln N\} \leq \frac{1}{N^2}.$$

3. Пусть $N \geq 3$, $1 \leq T \leq N$ и $\delta \geq e$. Тогда

$$\mathbf{P} \{t \geq \delta \ln N / (\ln N + \ln \ln N - \ln T)\} < \frac{1}{N^{\delta - \delta/e - 1}}.$$

В частности,

$$\mathbf{P} \{\eta_{(N)} \geq 3.17 \ln N / (\ln N + \ln \ln N - \ln T)\} < 1/N,$$

$$\mathbf{P} \{\eta_{(N)} \geq 4.75 \ln N / (\ln N + \ln \ln N - \ln T)\} < 1/N^2.$$

Обоснование стойкости: обращение

Теорема 1

При случайном выборе f для любого $\mathcal{A}$ справедлива оценка

$$\mathbf{Adv}_{\sigma[f]}^{\text{Pre}}(\mathcal{A}) \leq 6 \max\left(\frac{T^2}{N^3}, \frac{T \ln N}{N^2}\right) + \frac{1}{N^2}.$$

Следствие 1

При случайном выборе f для любого $\mathcal{A}$ справедлива оценка

$$\mathbf{Adv}_{\phi[f]}^{\text{Pre}}(\mathcal{A}) \leq 6 \max\left(\frac{T^2}{N^3}, \frac{T \ln N}{N^2}\right) + \frac{1}{N^2}.$$

Интерпретация: для обращения σ и ϕ нужна стенограмма объема $T = \Omega(N^{3/2})$.

Напомним: в belt-compress и belt-hash $N = 2^{128}$ и $N^{3/2} = 2^{192}$.

Обоснование стойкости: второй прообраз

Теорема 2

При случайном выборе f для любого $\mathcal{A}$ справедлива оценка

$$\mathbf{Adv}_{\sigma[f]}^{\text{Pre2}}(\mathcal{A}) < \beta(T, N, 6 \max(T/N, \ln N)) + \frac{1}{N^2},$$

где

$$\beta(T, N, \tau) = \frac{\tau T + 3T}{N^2} + \frac{6\tau + 15}{N}.$$

Следствие 2

Пусть Φ - L — функция хэширования, которая обрабатывает сообщения из L блоков длины $2n$ (последний блок может быть неполным) и делает это так же, как Φ . При случайном выборе f для любого $\mathcal{A}$ справедлива оценка

$$\mathbf{Adv}_{\Phi-L[f]}^{\text{Pre2}}(\mathcal{A}) < (L + 1)\beta(T, N, 6 \max(T/N, \ln N)) + \frac{1}{N^2}.$$

Обоснование стойкости: коллизия

Теорема 3

При случайном выборе f и $1 \leq T \leq N$ для любого $\mathcal{A}$ справедлива оценка

$$\text{Adv}_{\sigma[f]}^{\text{Coll}}(\mathcal{A}) < \frac{3.17 T \ln N}{\ln N + \ln \ln N - \ln T} \cdot \beta \left(T, N, \frac{3.17 \ln N}{\ln N + \ln \ln N - \ln T} \right) + \frac{1}{N}.$$

Следствие 3

При случайном выборе f и $1 \leq T \leq N$ для любого $\mathcal{A}$ справедлива оценка

$$\text{Adv}_{\phi[f]}^{\text{Coll}}(\mathcal{A}) < \frac{3.17 T \ln N}{\ln N + \ln \ln N - \ln T} \cdot \beta \left(T, N, \frac{3.17 \ln N}{\ln N + \ln \ln N - \ln T} \right) + \frac{1}{N}.$$

Интерпретация: для отыскания коллизии нужна стенограмма объема $T = \Omega(N/(\ln N / \ln \ln N)^2)$.

Атаки

Построение коллизии

1. Найдена атака по решению $\text{Coll}[\sigma]$ на стенограмме объема $T = \Theta(N/(\ln N/\ln \ln N)^2)$ (оценка теоремы 3 достижима!).
2. Нет оснований считать, что атаку можно распространить на $\text{Coll}[\Phi]$.
3. Время атаки, вообще говоря, больше, чем объем стенограммы: поиск в стенограмме, вычисления с элементами.
4. Прямая организация атаки — память большого объема.
5. В целом, нет оснований говорить о снижении коллизионной стойкости Φ и, следовательно, `belt-hash`.

Обращение

1. Найдена три атаки по решению $\text{Pre}[\sigma]$ на стенограмме объема $T = \Theta(N^{3/2})$ (оценка теоремы 1 достижима!). Атаки отличаются очередностью выбора вершин в искомом треугольнике $\Delta = (R_a, R_b, R_c)$.
2. Найдена атака по решению $\text{Pre}[\Phi](Y)$ на стенограмме объема $T = \Theta(N^{3/2+\alpha})$, $\alpha = 1/10$. В атаке определяется цепочка

$$\Delta_1, \Delta_2, \dots, \Delta_\ell,$$

в которой

- $\text{in}(\Delta_1) = H$;
- $\text{in}(\Delta_i) = \text{out}(\Delta_{i-1})$, $i = 1, 2, \dots, \ell$;
- $\text{out}(\Delta_\ell) = Y$;
- $\text{body}(\Delta_\ell)$ содержит представление ℓ и итоговой контрольной суммы

$$\text{key}(\Delta_1) \oplus \text{key}(\Delta_2) \oplus \dots \oplus \text{key}(\Delta_{\ell-1}).$$

Обращение: длина решения

Длина цепочки-решения $\ell > n + 4$ (благодаря «усилению» MD-усиления!).

- В частности, решение для belt-hash состоит из более чем $128 + 4 = 132$ блоков длины 256 (более 4 кБ).
- В частности, атаку нельзя применить при использовании belt-hash в алгоритмах электронной цифровой подписи Bign (СТБ 34.101.45).

Здесь под угрозой только 3-й уровень стойкости. Для подделки подписи требуется находить решения из не более чем 5 блоков. Ситуация для атакующего осложняется тем, что вместо задачи Pre нужно решать задачу RPP (Random Prefix Problem [NSW09]).