Перспективный алгоритм хэширования

Д. В. Матюхин, В. И. Рудской, В. А. Шишкин

2 апреля 2010 года

Основные криптографические требования к функции хэширования $H : \{0,1\}^* \to \{0,1\}^n$

Задача (построение ...)	Трудоемкость (вычислений H)
прообраза: по $h \in \{0,1\}^n$ найти $M \in \{0,1\}^*$: $H(M) = h$	$\gtrsim 2^n$
коллизии: найти $M, M' \in \{0,1\}^*$: $M \neq M', H(M) = H(M')$	$\gtrsim 2^{n/2}$
второго прообраза: по $M \in \{0,1\}^*$ найти $M' \in \{0,1\}^*$: $M' \neq M, H(M') = H(M)$	$\gtrsim 2^n/\lvert M\rvert$
по $\lvert M\rvert, H(M)$ найти $M' \in \{0,1\}^*, H(M\|M')$ (length-extension attack)	$\gtrsim 2^n$

Последние результаты криптографического анализа хэш-функции ГОСТ Р 34.11-94 ($n = 256$)

F. Mendel, N. Pramstaller, C. Rechberger, M. Kontak, J. Szmidt, CRYPTO 2008: алгоритмы построения прообраза за 2^{192} вычислений функций сжатия, коллизии за 2^{105} вычислений функций сжатия. Меньше «универсальных» оценок 2^{256} и 2^{128} соответственно!

Принципы синтеза перспективной хэш-функции

- отсутствие свойств, позволяющих эффективно применить известные методы криптографического анализа
- использование только хорошо изученных конструкций и преобразований
- максимальное быстродействие при указанных выше условиях
- ничего лишнего: каждое преобразование обеспечивает определенные криптографические свойства

Общая схема перспективной хэш-функции

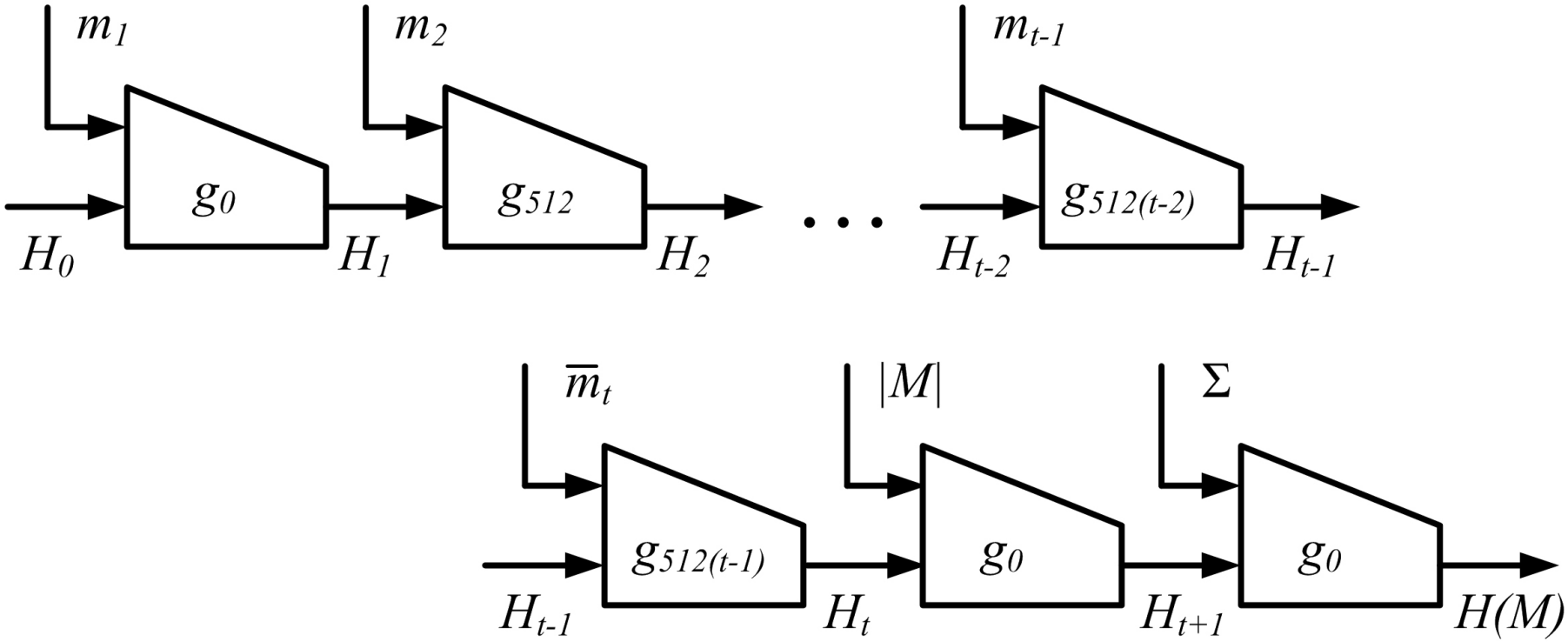
- $n = 512$, итерационная конструкция Меркля-Дамгорда: $M = m_t||\ldots||m_1$, $H_i = g_{512(i-1)}(H_{i-1}, m_i), i = 1, \ldots, t-1$

- функция сжатия $g_{512(i-1)} : \{0,1\}^{512} \times \{0,1\}^{512} \to \{0,1\}^{512}$ зависит от номера итерации

- MD-усиление: $\overline{m}_t = 0^{511-|m_t|}||1||m_t$, $H_t = g_{512(t-1)}(H_{t-1}, \overline{m}_t)$

- применение функции сжатия для длины сообщения $|M|$ и контрольной суммы $\Sigma = m_1 \boxplus \ldots \boxplus m_{t-1} \boxplus \overline{m}_t$ в качестве завершающих итераций: $H_{t+1} = g_0(H_t, |M|), H(M) = g_0(H_{t+1}, \Sigma)$

Общая схема перспективной хэш-функции

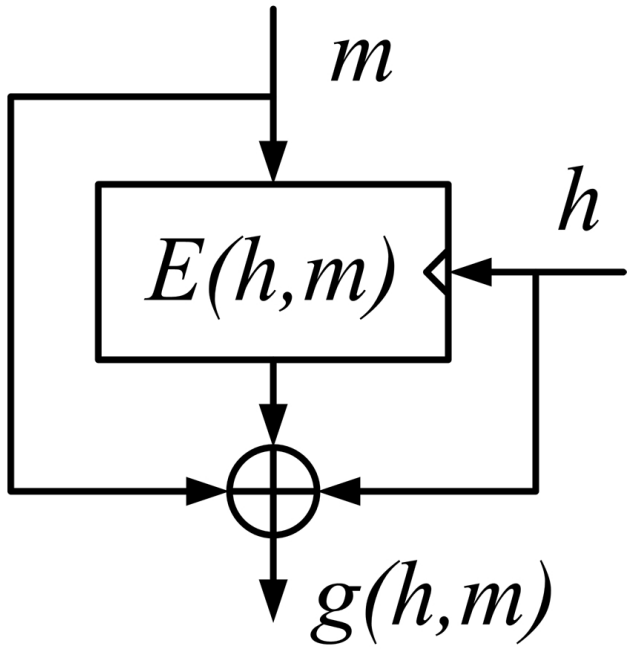


Функции сжатия

Конструкция Миягучи-Принеля:

$$g_N(h, m) = E(K_N(h), m) \oplus h \oplus m,$$

где $E : \{0,1\}^{512} \times \{0,1\}^{512} \to \{0,1\}^{512}$ – блочный шифр



Функции сжатия

$$K_N(h) = LPS(h \oplus N)$$

$$E(K, m) = X[K_{13}]LPSX[K_{12}] \dots LPSX[K_2]LPSX[K_1](m)$$

$$K_1 = K, \quad K_i = LPS(K_{i-1} \oplus C_{i-1}), i = 2, \dots, 13$$

Фиксированные $C_i \in \{0,1\}^{512}$ и $X[k], S, P, L : \{0,1\}^{512} \to \{0,1\}^{512}$

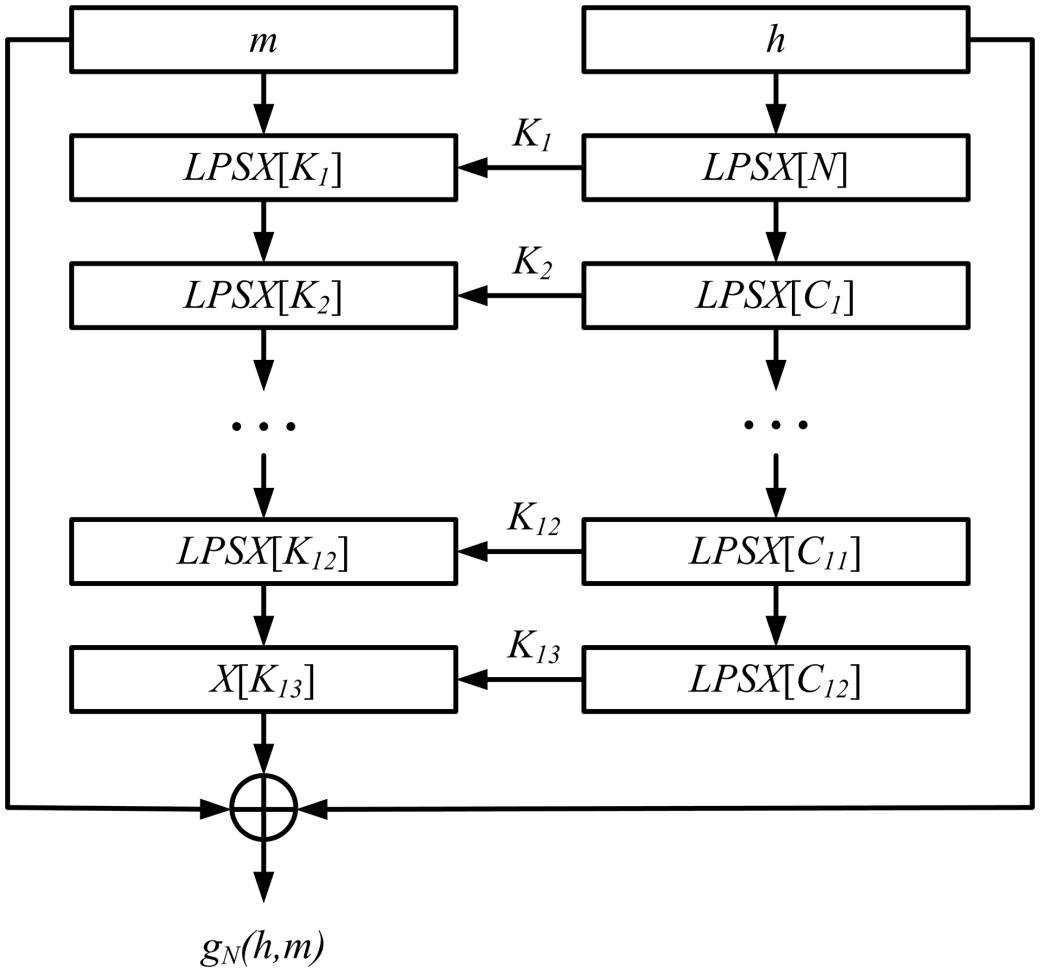
$$X[k](a) = k \oplus a, k \in \{0,1\}^{512}$$

$$S(a) = S(a_{63}|| \dots ||a_0) = \pi(a_{63})|| \dots ||\pi(a_0), \pi \in S_{256}, a_i \in \{0,1\}^8$$

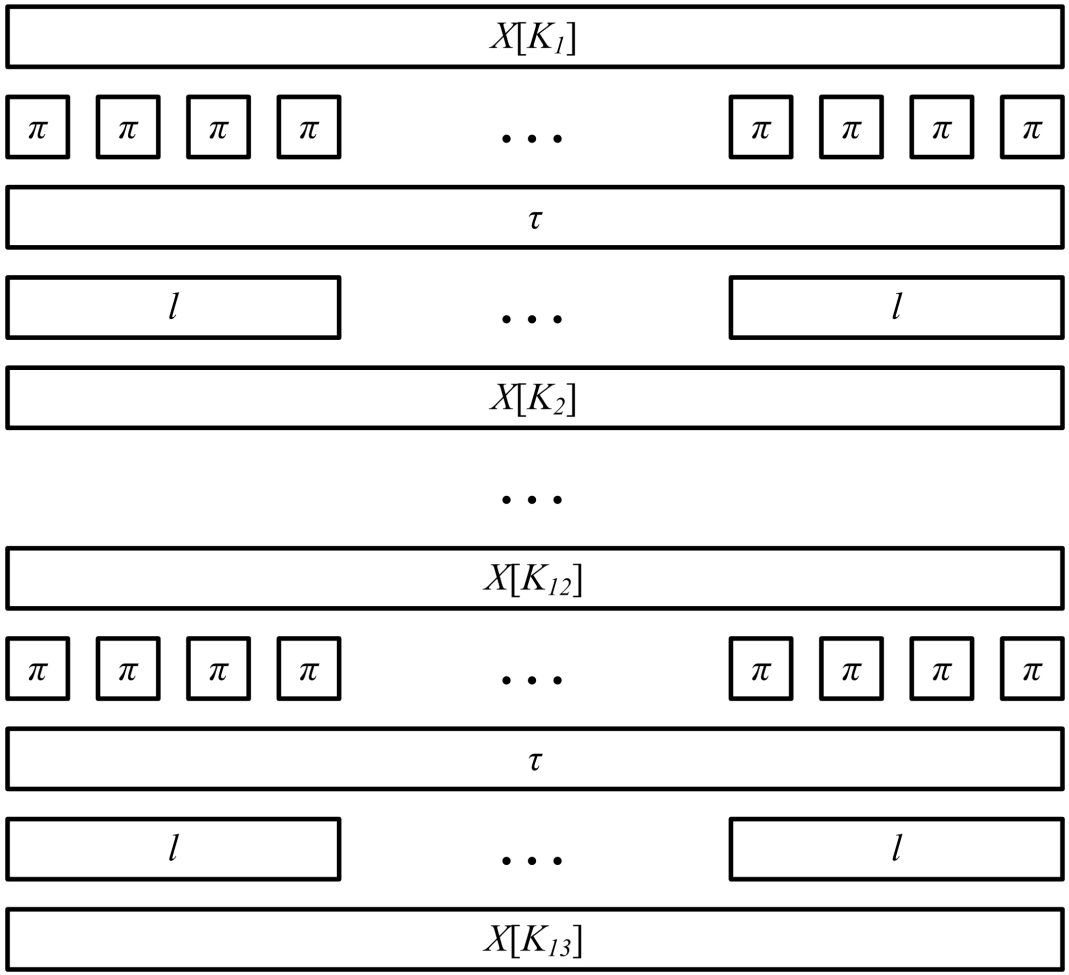
$$P(a) = P(a_{63}|| \dots ||a_0) = a_{\tau(63)}|| \dots ||a_{\tau(0)}, \tau \in S_{64}, a_i \in \{0,1\}^8$$

$L(a) = L(a_7|| \dots ||a_0) = l(a_7)|| \dots ||l(a_0)$, l линейное на 64 битах

Функции сжатия



Блочный шифр



Криптографические и эксплуатационные качества перспективной хэш-функции

- удовлетворяет основным криптографическим требованиям к функциям хэширования (см. выше)

- скорость хэширования 40 Мбайт/с (50 тактов/байт) на 1 ядре Intel Xeon quadcore (64 bit) 2.0 ГГц, компилятор Microsoft Visual Studio 2005 (C++) (на 20% быстрее ГОСТ Р34.11-94)