Об одном режиме шифрования с возможностью аутентификации

Лебедев П.А. Нестеренко А.Ю.

Московский институт электроники и математики
национального исследовательского университета
«Высшая школа экономики»

РусКрипто'2013

Мотивация

Задача: разработка системы защищённой системы прозрачного хранения данных в облачных службах с использованием российских криптографических стандартов.

Специфика: в отличие от традиционных систем защиты информации на блочных устройствах, нет доверия к самому «носителю» — облачной службе.

Подход: не использовать традиционные решения для шифрования данных на устройствах хранения, а применить режим аутентифицированного шифрования.

Проблемы

- Нет российского стандарта на режим аутентифицированного шифрования.
- Режим выработки имитовставки ГОСТ 28147-89 даёт очень короткий результат (32 бита).
- Существующие режимы аутентифицированного шифрования ограничивают длину кода аутентификации длиной одного блока шифра, что для ГОСТ 28147-89 составляет 64 бита и недостаточно.

Общая схема режима

Шифрование: XEX (xor-encrypt-xor) (*Liskov, Rivest, Wagner*)

$$C_i = E_K(P_i \oplus \Delta_i) \oplus \Delta_i$$

Код аутентификации: NH (*Krovetz*)

$$h = \left(\sum_{i=1}^{n/2} ((m_{2i-1} + k_{2i-1}) \mod 2^w) \cdot ((m_{2i} + k_{2i}) \mod 2^w) \right) \mod 2^{2w}$$

Объединение: использовать ключевую информацию с этапа шифрования в универсальной хэш-функции, вычисляющей код аутентификации.

Детали режима

Вычисление смещений:
$\Delta_i = \xi \oplus \alpha^i$, где $\xi = E_K(\gamma)$, γ — константа.
Вычисления с α в $\mathrm{GF}(2^w)$, α — примитивный элемент.

Ключевая информация для хэш-функции:
$m_i = P_i \oplus \Delta_i, \quad k_i = E_K(P_i \oplus \Delta_i)$.

Начальное преобразование: $h_0 = IV$.

Финальное преобразование: $H = E_K^{ECB}(h + l \cdot E_K(l))$.

Особенности режима

- Удвоение длины кода аутентификации по сравнению с длиной блока шифра;
- Стойкость кода аутентификации в случае нарушителя, обладающего ключом (сравни: OCB);
- Невосприимчивость к атакам на полиноминальные хэш-функции (сравни: GCM);
- Стойкость к атакам, связанным с изменением длины сообщения.
- Соответствие современным требованиям к режиму работы шифра:
  - Возможность параллельной реализации;
  - Доступность реализаций используемых математических операций;
  - Знание итоговой длины сообщения заранее не требуется;
  - Поддержка аутентифицируемых, но не шифруемых данных (в разработке);
  - Отсутствие отягощённости патентами.

Производительность

Производительность ГОСТ 28147-89 в различных режимах, тактов/байт

	Длина сообщения		
Режим	16 байт	1 КБ	1 МБ
ECB	39	37	37
CFB+HMAC-Gost34.11-2012	1059	83	67
Предлагаемый режим	117	42	39

(ассемблер x86_64, ЦП архитектуры Nehalem)