V. V. Korobov

Effective Implementations of Data Encryption and Generation of Message Authentication Code in Block-Oriented Devices

Keywords: block-oriented devices, encryption modes, message authentication code, parallel computing
The article gives a brief overview of the encryption modes, which are described in standards IEEE P1619 for use in block-oriented devices. The possibility of using these modes together with the Russian cryptographic algorithms, the technology of parallel computing for simultaneous encryption and generation of message authentication is considered in this paper.

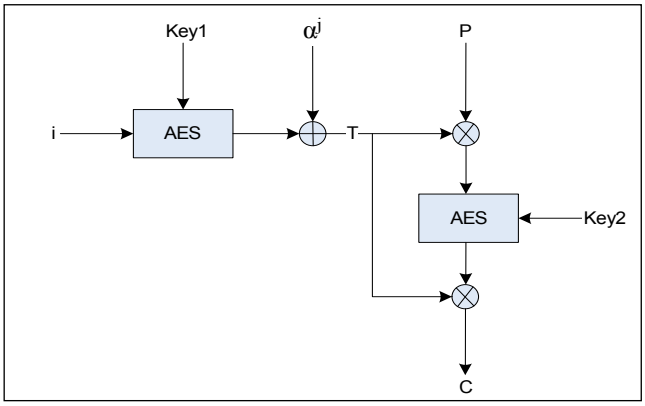
В. В. Коробов

ЭФФЕКТИВНАЯ РЕАЛИЗАЦИЯ ШИФРОВАНИЯ И ИМИТОЗАЩИТЫ ДАННЫХ В УСТРОЙСТВАХ С БЛОЧНОЙ ВНУТРЕННЕЙ СТРУКТУРОЙ

Во многих реализациях шифрованных дисковых накопителей для шифрования данных используется режим шифрования XTS. Стандартизацией режима XTS занимается рабочая группа SIS-WG IEEE, которая разработала ряд стандартов — IEEE P1619 [1]. В этих стандартах, помимо описания режима XTS, дополнительно предлагаются другие режимы шифрования, использование которых целесообразно в зависимости от внутренней организации устройства хранения данных и требований безопасности. Ниже приведено более детальное рассмотрение этих стандартов.

IEEE P1619-2007 - IEEE Standard for Cryptographic Protection of Data on Block-Oriented Storage Devices

В стандарте приводится описание режима шифрования XTS-AES, который относится к группе шифров, именуемых **Tweakable Block Cyphers** (подход к шифрованию, предполагающий использование при вычислении дополнительного параметра, так называемого «tweak value»). На рисунке ниже изображена структурная схема XTS.



Режим предполагает использование пары ключей, в качестве i используется номер сектора, j — номер 128-битного блока внутри сектора (не больше 2^{20}), α — примитивный элемент поля $GF(2^{128})$. Также в стандарте описывается техника Ciphertext Stealing (CTS), которая заключается в особой обработке двух последних блоков открытого текста, размер которого не кратен 128 битам.

Документ NIST Special Publication 800-38E [2] также содержит описание режима XTS.

IEEE P1619.1-2007 - IEEE Standard for Authenticated Encryption with Length Expansion for Storage Devices

IEEE P1619.1 содержит описание режимов, рекомендуемых к использованию в случаях необходимости дополнительного обеспечения имитозащищенности данных. Нужно отметить, что это неизбежно влечет за собой дополнительное увеличение размера шифротекста (за счет добавления значения кода аутентификации сообщения). Режимы шифрования, рекомендуемые к применению стандартом:

- CBC-MAC (CCM);
- Galois/counter mode (GCM);
- Cipher Block Chaining with HMAC-SHA (CBC-HMAC-SHA);
- Tweakable block-cipher with HMAC (XTS-AES-256-HMAC-SHA-512).

Помимо режимов аутентифицированного шифрования CCM и GCM, в которых имитозащищенность достигается за счет собственных вычислений, стандарт также рекомендует применять HMAC к шифротексту, полученному в результате применения режимов шифрования CBC и XTS к исходному тексту.

IEEE P1619.2-2010 - IEEE Standard for Wide-Block Encryption for Shared Storage Media

Стандарт содержит описание режимов шифрования блоков данных, размер которых превышает 512 байт. Предполагается, что совместно с данными, для которых требуется обеспечение конфиденциальности и целостности, предлагаемые режимы могут обрабатывать ассоциированные данные (например, логический номер блока), для которых требуется только обеспечение аутентификации. Режимы шифрования, рекомендуемые к применению:

- EME2-AES;
- XCB-AES.

Стандартом регламентируется, что применение таких режимов целесообразно в ситуациях, когда нарушитель имеет непосредственный доступ к зашифрованным данным или может осуществлять перехват в канале. В таблице ниже приведены алгоритмические затраты по шифрованию n 16-байтных блоков данных. Выбор конкретного режима зависит от требований к производительности и размеру аппаратной реализации.

	EME2-AES	XCB-AES
Шифрование AES	$2n + 1$	$n + 1$
Сдвиг и сложение по модулю 2	$3n$	–
Умножение в поле $GF(2^{128})$	–	$2n$

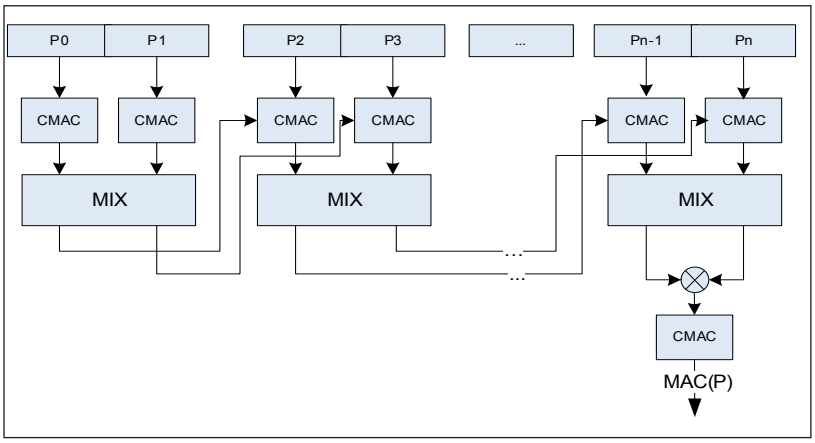
Особенности применения режимов, рекомендуемых IEEE P1619, совместно с российскими криптографическими алгоритмами

Использование режима шифрования XTS совместно с российским алгоритмом шифрования возможно. Для этого требуется скорректировать разрядность поля Галуа в соответствии с размером входного блока данных ГОСТ 28147. Такое требование вытекает из необходимости генерации «tweak value»-разрядности, соответствующей ГОСТ 28147.

Для построения высокопроизводительных решений очень хорошо подходит режим XTS, который достаточно просто распараллеливается (например, за счет использования множества независимых функциональных блоков в FPGA), чего нельзя сказать о режимах EME2 и XCB.

При построении решений с дополнительным требованием обеспечения целостности данных идеальным является подход, при котором имитовставка вычисляется параллельно с шифрованием. Стандарт IEEE P1619.1 рекомендует режимы CCM и GCM, в которых выполняются подобные

вычисления, но, к сожалению, распараллелить вычисления таких режимов достаточно сложно. Существует возможность модифицировать режим XTS-HMAC использованием вместо HMAC алгоритма вычисления имитовставки, рекомендуемого ТК 26 (CMAC), что позволит не использовать хэш-функцию, тем самым упростив реализацию.



Кроме всего прочего, можно распараллелить вычисление имитовставки, применяя CMAC к двум независимым блокам шифротекста с последующим перемешиванием полученных промежуточных результатов (MIX). На рисунке выше представлена схема предлагаемого решения.

Предполагается, что результат двух соседних операций шифрования обрабатывается по алгоритму выработки имитовставки, рекомендуемому ТК 26 [3]. Полученные результаты перемешиваются определенным способом (перестановка, регистр сдвига с линейной обратной связью) и используются для вычисления на следующем шаге алгоритма вычисления имитовставки. Последние блоки при указанном подходе необходимо сократить до требуемой длины. Для этого предлагается сложить полученные промежуточные значения и применить к результату CMAC.

Применением такого подхода достигается повышение производительности шифрования и вычисления имитовставки для больших блоков данных.

СПИСОК ЛИТРАТУРЫ:

1. IEEE Standards Association. Security in Storage Working Group. URL: http://standards.ieee.org/develop/wg/SIS-WG.html (дата обращения: 12.10.2014).
2. NIST. Modes development. URL: http://csrc.nist.gov/groups/ST/toolkit/BCM/modes_development.html (дата обращения: 12.10.2014).
3. Технический комитет по стандартизации «Криптографическая защита информации». «Режимы работы блочных шифров». URL: https://www.tc26.ru/standard/draft/GOSTR-rbsh.pdf (дата обращения: 12.10.2014).

REFERENCES:

1. IEEE Standards Association. Security in Storage Working Group. URL: http://standards.ieee.org/develop/wg/SIS-WG.html.
2. NIST. Modes development. URL: http://csrc.nist.gov/groups/ST/toolkit/BCM/modes_development.html.
3. Technical committee for standardization “Cryptography and security mechanisms”. “Encryption Modes”. URL: https://www.tc26.ru/standard/draft/GOSTR-rbsh.pdf.