УДК 004.056.5

О СПОСОБАХ СОВМЕСТНОГО ШИФРОВАНИЯ И АУТЕНТИФИКАЦИИ

В.М. Фомичев[1, 2, 3], Д.А. Бобровский[2], И.Э. Недомолкин[2]
[1]Российский технологический университет (РТУ МИРЭА), Москва, Россия
[2]ООО «Код Безопасности», Москва, Россия
[3]Федеральный исследовательский центр «Информатика и управление» Российской Академии Наук, Москва, Россия

Аннотация. В докладе рассматривается разработка нового способа совместного шифрования и аутентификации данных – способа E-IB, который ориентирован на повышение вычислительной эффективности при сохранении высокого уровня безопасности. Этот способ объединяет функции шифрования и аутентификации, используя общий ключ и минимизируя вычислительные затраты по сравнению с традиционными подходами, что особенно важно для маломощных устройств, не поддерживающих AVX-инструкции. Для аутентификации используются промежуточные блоками процесса шифрования, что позволяет обеспечить безопасность с низкими затратами на вычисления и память. В докладе представлены экспериментальные результаты применения предложенного метода на примере шифра Магма, где показана его высокая производительность и преимущество по быстродействию по сравнению с известными режимами, такими как XTSMAC и MGM. Также обсуждаются возможности применения этого подхода в условиях ограниченных вычислительных ресурсов, например, в IoT-устройствах и других встраиваемых системах. Режим CBC-IB устойчив к атакам CPA при корректном использовании IV и защищен от атак на целостность шифртекста, однако для защиты от атак CCA требуются дополнительные меры.
Ключевые слова: AEAD; шифрование; аутентификация; промежуточные блоки; вычислительная эффективность; маломощные устройства; AVX; шифр Магма; производительность.

ON COMBINED ENCRYPTION AND AUTHENTICATION METHODS

V.M. Fomichev[1, 2, 3], D.A. Bobrovskiy[2], I.E. Nedomolkin[2]
[1]Moscow Technological University (MIREA), Moscow, Russia
[2]LLC "Code Security", Moscow, Russia
[3]Federal Research Center "Informatics and Management" of the Russian Academy of Sciences, Moscow, Russia

Abstract. This paper presents the development of a new combined encryption and authentication method, the E-IB method, which aims to improve computational efficiency while maintaining a high level of security. This method combines encryption and authentication functions, using a shared key and minimizing computational costs compared to traditional approaches, which is particularly important for low-power devices that do not support AVX instructions. The method integrates control of intermediate blocks during the encryption process, ensuring high security with low computational and memory overhead. Experimental results of applying the proposed method, based on the Magma cipher, are also presented, demonstrating its high performance and superior speed compared to well-known modes such as XTSMAC and MGM. The potential of applying this approach in environments with limited computational resources, such as IoT devices and other embedded systems, is also discussed. The CBC-IB mode is resistant to CPA attacks when the IV is used correctly and protected against ciphertext integrity attacks; however, additional measures are required to defend against CCA attacks.
Keywords: AEAD; encryption; authentication; intermediate blocks; computational efficiency; low-power devices; AVX; Magma cipher; performance.

Введение

При синтезе средств криптографической защиты информации актуальна разработка режимов шифрования класса AEAD – совместного шифрования и аутентификации данных. Целью AEAD-режимов является объединение шифрования и аутентификации при сохранении криптостойкости и эффективности использования

памяти, а также снижение вычислительной сложности по сравнению с их раздельным выполнением [1].

Известные режимы шифрования класса AEAD не всегда удовлетворяют требованиям по вычислительной сложности при совместном выполнении шифрования и аутентификации. В связи с этим актуальна разработка режима с достаточно высокими криптографическими свойствами и приемлемыми характеристиками сложности [2].

В связи с режимами класса AEAD в докладе представлен E-IB (E – encryption, IB - intermediate blocks) – способ совместного шифрования и аутентификации данных с использованием суммирования промежуточных блоков. Представлены данные для сравнения характеристик нового способа с характеристиками прототипов. Способ EIB особенно актуален для применения в маломощных устройствах, не поддерживающих инструкции AVX, где важно снизить вычислительные требования и эффективнее использовать ресурсы процессора. Этот подход позволяет реализовать эффективные механизмы защиты данных, минимизируя нагрузку на аппаратные ресурсы, что критично для таких устройств.

Способ E-IB шифрования и генерации кода аутентификации

Способ E-IB может быть реализован для различных режимов блочного шифрования с обратной связью по шифрованному тексту, например, для режимов CBC, CFB и других. Название конкретного режима получится, если заменить букву E на аббревиатуру конкретного режима блочного шифра, например, CBC-IB.

Обозначим V_n множество двоичных n-битовых векторов.

Опишем способ CBC-IB на примере $2r$-раундового блочного шифра Фейстеля с ключом $k \in V_n$ на основе режима шифрования CBC, $r > 1$. Для простоты изложения число раундов четное, однако это условие не нарушает общности рассуждений.

Запишем уравнения в режиме CBC с использованием функции шифрования E_k с ключом k и случайным и уникальным инициальным вектором $z \in V_{2m}$, присоединяемым к сообщению в открытом виде. Шифрование сообщения $x_1, \dots, x_t$, состоящего из $2m$-битовых блоков, задано уравнениями:

$$E_k(x_i \oplus y_{i-1}) = y_i, i = 1, \dots, t, \quad (1)$$

где $y_1, \dots, y_t$ – шифрованный текст, $y_i \in V_{2m}$, $y_0 = z \oplus E_k(z)$, $\oplus$ – XOR-суммирование.

Шифр Фейстеля построен на основе нелинейной рекурренты порядка 3 над множеством V_m. Обозначим U_k зависящую от ключа k нелинейную часть генерирующей функции рекурренты, и пусть для $b_i \in V_m$ выполнено

$$b_{j+1} = U_k(b_j) \oplus b_{j-1}, j \geq 1. \quad (2)$$

Тогда в соответствии с (2) шифрование есть вычисление для открытого текста $x = (b_0, b_1)$ шифрованного текста $y = (b_{2r+1}, b_{2r})$. Отметим, что шифртекст состоит из двух последних членов рекуррентной последовательности, взаимно переставленных по сравнению с естественным порядком. В шифрах Фейстеля такая перестановка необходима для инволютивности алгоритмов зашифрования и расшифрования.

При шифровании блока x_i на ключе k для начального блока $x_i \oplus y_{i-1} = (b_0^{(i)}, b_1^{(i)})$, $i = 1, \dots, t$, в соответствии с (2) вычисляем рекуррентную последовательность $\{b_2^{(i)}, b_3^{(i)}, \dots, b_{2r}^{(i)}, b_{2r+1}^{(i)}\}$ и получаем шифртекст

$y_1 = \left(b_{2r+1}^{(1)}, b_{2r}^{(1)}\right), \dots, y_t = \left(b_{2r+1}^{(t)}, b_{2r}^{(t)}\right)$. Попутно с шифрованием вычисляем промежуточные блоки $a_r^{(i)} = \left(b_r^{(i)}, b_{r+1}^{(i)}\right) \in V_{2m}$, $i = 1, \dots, t$, и код аутентификации $A_k(y_0, x_1, \dots, x_t)$:

$$A_k(y_0, x_1, \dots, x_t) = \left(\sum_{1 \le i \le t} a_r^{(i)}\right) \bmod 2^{2m}. \quad (3)$$

Шифрованное сообщение в режиме CBC-IB вкупе с кодом аутентификации есть последовательность $y_1, \dots, y_t, A_k(y_0, x_1, \dots, x_t)$.

Расшифрование и проверка аутентичности открытого текста

При расшифровании используем равенство, следующее из (2):

$$b_{j-1} = U_k(b_j) \oplus b_{j+1}, 1 \le j \le 2r. \quad (4)$$

В соответствии с (4) при расшифровании вычисляем блоки открытого текста $(b_0^{(i)}, b_1^{(i)})$ по блокам шифртекста $\left(b_{2r+1}^{(i)}, b_{2r}^{(i)}\right)$, попутно вычисляя промежуточные блоки $c_r^{(i)} = \left(b_r^{(i)}, b_{r+1}^{(i)}\right)$, $i = 1, \dots, t$, и суммируя их по $\bmod 2^{2m}$. Данные признаются аутентичными $\Leftrightarrow$

$$\left(\sum_{1 \le i \le t} c_r^{(i)}\right) \bmod 2^{2m} = A_k(y_0, x_1, \dots, x_t).$$

Анализ свойств способа CBC-IB

1. Ключ k общий (одинаковый) для функций шифрования и аутентификации.

2. Создание кода аутентификации и проверка аутентичности открытого текста не увеличивает значительно сложность вычислений по сравнению с алгоритмами зашифрования-расшифрования и не требует значительной дополнительной памяти.

3. Параметры r и m не должны быть малы. Блочный шифр после r раундов должен реализовать вполне перемешивающую нелинейную подстановку, т.е. каждая координатная функция подстановки после r раундов должна быть нелинейной и зависеть существенно от всех битов открытого текста и ключа. Во избежание случайного угадывания кода аутентификации достаточно взять $m \ge 32$.

4. «Подделка» нарушителем кода аутентификации и вектора y_0 требует знания ключа k вкупе с открытым текстом. Сложность определения ключа блочного шифра по открытому тексту, шифртексту и коду аутентификации должна быть столь же высокая, как и без знания кода.

Для анализа свойств безопасности AEAD-схем относительно угроз нарушения конфиденциальности и целостности в работе [3] были введены базовые определения безопасности. CBC-IB устойчив к простым атакам CPA, если IV генерируется случайным образом и используется корректно. Защита от CCA требует дополнительных механизмов для предотвращения манипуляций с шифртекстами и расшифрованиями. CBC-IB устойчив к атакам на целостность шифртекста.

Заключение

Результаты практической реализации способа аутентифицированного шифрования CBC-IB подтверждают целесообразность его применения в средствах

защиты информации.

Экспериментально получены показатели скорости работы различных режимов для шифра Магма, а также предложенного способа CBC-IB на основе шифра Магма. Эксперименты проводились на ЭВМ с процессором AMD Ryzen 5 5600G с постоянной тактовой частотой 4.0 ГГц. В таблице ниже для различных алгоритмов указаны число затраченных тактов процессора, скорость зашифрования и производительность относительно алгоритма Магма в режиме CBC, принятая за 100%.

Таблица 1. Сравнение производительности
Table 1. Performance comparison

Режим	Число тактов процессора	Скорость, MiB/s	Относительная производительность, %
Magma CBC	$59.5 * 10^6$	72.27	100
Magma CBC-IBS	$60 * 10^6$	71.67	99,2
XTSMAC	$64 * 10^6$	67.19	93,1
AK Magma MGM	$121 * 10^6$	35.54	49,2

Таблица показывает, что аутентифицированное шифрование CBC-IB фактически не уступает по быстродействию режиму CBC и превосходит известные режимы: на 6,1 % XTSMAC и более чем в 2 раза MGM. Достоинством CBC-IB является также техническая простота интеграции режима AEAD в среде, где применяется CBC: переход на CBC-IB упрощен по сравнению с XTSMAC или MGM.

Аналогичный эффект ожидается от аутентифицированного шифрования CFB-IB.

Список использованных источников / References

1. Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (2001). Handbook of Applied Cryptography. CRC Press

2. Kampanakis P., Campagna M., Crocket E. (2024) Practical Challenges with AES-GCM and the need for a new cipher. Practical Challenges with AES-GCM and the need for a new cipher. NIST PQC

3. Bellare, M., & Namprempre, C. (2000). Authenticated Encryption: Relations among notions and analysis of the generic composition paradigm. In Proceedings of the 3rd International Conference on Theory of Cryptography (TCC 2000).

Сведения об авторах

Фомичев В.М., д.ф.-м.н., проф., Российский технологический университет (РТУ МИРЭА), ООО «Код Безопасности», Федеральный исследовательский центр "Информатика и управление" Российской Академии Наук.
Бобровский Д.А., руководитель группы отдела криптографического анализа, ООО «Код Безопасности»
Недомолкин И.Э., младший системный аналитик отдела криптографического анализа, ООО «Код Безопасности.

Information about the authors

V.M. Fomichev, Dr. Sci., Prof., Russian Technological University (RTU MIREA), "Security Code" LLC, Federal Research Center "Informatics and Management" of the Russian Academy of Sciences.
D.A. Bobrovsky, Team Leader, Cryptographic Analysis Department, "Security Code" LLC.
I.E. Nedomolkin, Junior Systems Analyst, Cryptographic Analysis Department, "Security Code" LLC.