AEAD режимы на основе полиномиальных хэш–функций: существующие решиния, их криптографические свойства и возможные модификации

Кислякова Анастасия Сергеевна

Студент

Факультет ВМК МГУ имени М. В. Ломоносова, Москва, Россия

E-mail: a.kislyakova.95@gmail.com

В последние годы перед современным криптографическим сообществом остро встал вопрос создания AEAD режима блочного шифрования (AEAD — Authenticated Encryption with Additional Data), то есть алгоритма, позволяющего одновременно производить шифрование и аутентификацию данных. По определению, данному в стандарте ISO/IEC 19772:2009 «Информационные технологии. Методы защиты. Установленные криптографические методы», аутентифицированное шифрование — это преобразование данных с помощью криптографического алгоритма для создания шифртекста, который не может быть незаметно изменен третьим лицом. Один из распространенных способов реализации аутентификации в AEAD–режимах — использование полиномиальных хэш–функций, заданных над конечными полями. Представителями такого подхода являются режимы Galois/Counter Mode (GCM) ([1]), белорусский стандарт СТБ 34.101.31–2011 ([2]) и режим MGM, так же известный как PD ([3]). Общий вид функции хэширования сообщения x на ключе H GCM (операция умножения — умножение в поле $\mathcal{GF}(2^{128})$):

$$\mathrm{GHASH}_H(x) = x_1 \cdot H^m \oplus x_2 \cdot H^{m-1} \oplus \cdots \oplus x_{m-1} \cdot H^2 \oplus x_m \cdot H. \quad (1)$$

К сожалению, существует несколько атак на GCM, основанных на свойствах полиномиальных хэш–функций. Так, например, Нил Фергюсон в статье [4] приводит способ успешной подмены исходного сообщения и вычисления ключа H, используя линейность операций умножения на константу и возведения в квадрат в конечном поле. Маркку-Юхани Олави Сааринен в статье [5] описывает процесс подмены блоков сообщения, возможный благодаря цикличности значений степеней ключа H.

Функция хэширования белорусского стандарта отличается от $GHASH$ наличием дополнительной константы. Таким образом, подобные атаки применимы к белорусскому стандарту. Для алгорит-

ма MGM различия с GCM более существенные: вместо различных степеней ключа H используются шифрованные значения счетчика. Следовательно, для каждого блока сообщения используется новое значение ключа, что делает атаки, основанные на свойствах полиномиальных хэш–функций, не применимыми для MGM.

В докладе предлагается еще одна интересная для изучения модификация алгоритма GCM — замена операции умножения в конечном поле на операцию умножения в целых числах по модулю 2^{128}. Предварительные исследования показали, что при таком подходе множество элементов, попадание в которые позволяет применить атаку Фергюсона, сужается до множества делителей нуля для кольца вычетов по модулю 2^{128}. Для атаки Сааринена слабыми ключами будут обратимые элементы, образующие циклические подгруппы малого порядка, и необратимые элементы с малым индексом нильпотентности.

Литература

1. David A. McGrew, John Viega. The Galois/Counter Mode of Operation (GCM). `http://csrc.nist.gov/groups/ST/toolkit/BCM/documents/proposedmodes/gcm/gcm-spec.pdf`
2. Государственный стандарт Республики Беларусь. СТБ 34.101.31–2011. Минск, Госстандарт, 2011.
3. Vladislav Nozdrunov. Parallel and double block cipher mode of operation (PD–mode) for authenticated encryption. Принят к опубликованию.
4. Niels Ferguson. Authentication weaknesses in GCM. 2005 `http://csrc.nist.gov/groups/ST/toolkit/BCM/documents/comments/CWC-GCM/Ferguson2.pdf`
5. Markku-Juhani O. Saarinen. Cycling Attacks on GCM, GHASH and Other Polynomial MACs and Hashes. IACR Cryptology ePrint Archive, 2011, 202. `https://eprint.iacr.org/2011/202.pdf`