УДК 004.056.55
МРНТИ 81.93.29

MDS-МАТРИЦЫ, ПРИМЕНЯЕМЫЕ В КРИПТОГРАФИИ

Т.К. ЖУКАБАЕВА, Е. МАРДЕНОВ

Институт информационных и вычислительных технологий

Аннотация: *Безопасность информации является одним из важнейших аспектов коммуникаций, который из-за повышения опасности взлома в приложениях реального времени требует улучшения существующих и разработки новых криптосистем с высокой степенью безопасности и производительности. Криптосистемы, основанные на MDS-матрицах, являются формальными моделями вычислительных устройств, могут быть эффективно реализованы на программном и аппаратном уровнях. На сегодняшний день MDS-матрицы занимают особое место и являются важными компонентами при проектировании линейных диффузионных слоев многих блочных шифров и хеш-функций. В последнее время была проделана большая работа по построению облегченных MDS-матриц, большинство из которых основано на матрицах специальных типов над конечными полями. В данной статье рассматривается аналитический обзор применения MDS-матриц для криптографических алгоритмов. Рассматривается применение матрицы MDS для диффузии, а также сравнение их с другими алгоритмами.*

Ключевые слова: *криптография, MDS-матрицы, алгоритмы шифрования, блочные шифры, AES, SHARK, Square, Twofish, Anubis, KHAZAD, Manta, Hierocrypt, Kalyna*

MDS MATRIX APPLIED IN CRYPTOGRAPHY

Abstract: *The security of information is one of the most important aspects in communications, which always demands to improve the existing cryptosystems, and design new ones with high security and performance in real-time applications due to enhancing the danger of hacking efforts. Since MDS matrix a are formal models of computing devices, cryptosystems based on them can be efficiently implemented at software and hardware levels. Today, MDS matrices occupy a special place and are important components in designing the linear diffusion layers of many block ciphers and hash functions. Recently, a lot of work has been done on the construction of lightweight MDS matrices, most of which are based on special types of matrices over finite fields. This article provides an analytical overview of the use of MDS matrices for cryptographic algorithms. The use of the MDS matrix for diffusion is considered, as well as their comparison with other algorithms.*

Keywords: *cryptography, MDS matrix, encryption algorithms, block ciphers, AES, SHARK, Square, Twofish, Anubis, KHAZAD, Manta, Hierocrypt, Kalyna*

MDS МАТРИЦАЛАРЫН КРИПТОГРАФИЯДА ҚОЛДАНУЫ

Аңдатпа: *Ақпарат қауіпсіздігі сөзсіз коммуникациядағы ең маңызды мәселелердің бірі болып табылады. Ақпаратты қорғау үшін әртүрлі криптографиялық жүйелер қолданылады. MDS матрицалары негізіндегі криптожүйелер бағдарламалы және аппаратты деңгейлерде тиімді жүзеге асырылуы мүмкін, себебі есептеуіштердің формалды моделі болып есептеледі. Бүгінгі таңда көптеген блоктық шифрлерде және хэш функцияларында сызықты диффузиялық қабаттарын жобалауда MDS матрицалары ерекше орын алады және маңызды компоненттері болып саналады. Соңғы уақытта жеңілдетілген МДС матрицаларын құру бойынша көптеген жұмыстар жасалды, олардың көпшілігі ақырлы өрістерге негізделген. Бұл мақалада криптографиялық алгоритмдер үшін MDS матрицаларын пайдалану туралы аналитикалық шолу берілген. Диффузияға арналған MDS матрицасын қолдану, сондай-ақ оларды басқа алгоритмдермен салыстыру қарастырылады.*

Түйінді сөздер: *криптография, MDS матрицалары, шифрлау алгоритмдері, блоктық шифрлар, AES, SHARK, Square, Twofish, Anubis, KHAZAD, Manta, Hierocrypt, Kalyna*

Введение

Для обеспечения защиты информации необходимы простые в реализации, быстродействующие алгоритмы шифрования. В рамках парадигмы повсеместных вычислений основной тенденцией в криптографии является эффективность аппаратной реализации. В последнее время было предложено много криптографических алгоритмов, в частности, блочные шифры и хеш-функции.

MDS-матрицы имеют применение не только в теории кодирования, но также имеют большое значение при разработке блочных шифров и хеш-функций. MDS-матрицы очень широко используются при разработке современных криптографических алгоритмов [1], [2], [3], [4].

MDS-матрица (Maximal Distance Separable matrix) – проверочная матрица линейного блокового кода с максимальной дистанцией (расстоянием). Структура MDS-матрицы обеспечивает максимальное рассеивание и используется при создании SPN-шифров в качестве линейных рассеивающих преобразований. MDS-матрицы широко используется при разработке линейных диффузионных слоев блочного шифра. Диффузионные слои являются важной частью большинства симметричных шифров. Цель диффузии – максимально расширить внутренние зависимости. В некоторых разработках используется слабый, но быстрый диффузионный слой, основанный на простой операции XOR, сложении и сдвиге, но другой тенденцией является использование матриц сильной линейной диффузии, таких как MDS-матрицы. Причиной использования MDS-матрицы при разработке блочных шифров является то, что они обеспечивают оптимальный диффузионный эффект для обеспечения безопасности функции округления блочного шифра. С другой стороны, конструкции диффузионных слоев могут быть различными. С точки зрения безопасности и эффективности при выборе диффузионного слоя для блочного шифра необходимо определить надлежащий диффузионный слой. Важную роль занимает номер ветви диффузионного слоя, который представляет скорость диффузии и измеряет степень защиты [5,6].

Многие блочные шифры в качестве диффузионных слоев используют коды с разделением по максимальному расстоянию (MDS) и с максимально бинарно-линейным расстоянием (MDBL) [1],[7]. В своей конструкции в качестве диффузионных слоев AES и Khazad используют MDS-матрицы, а Camellia и ARIA используют MDBL (таблица 1).

Таблица 1 – Блочные шифры и соответствующий диффузионный слой

Блочный шифр	Диффузионный слой
AES	4×4 MDS $GF(2^8)$
Khazad	8×8 MDS $GF(2^8)$
Camellia	8×8 $GF(2^8)$
ARIA	16×16 $GF(2^8)$

Как показано в таблице 1, ARIA и Khazad используют инволюционные диффузионные слои. Инволюционные отображения снижают стоимость реализации операций шифрования и дешифрования и подразумевают, что оба преобразования имеют одинаковую криптографическую стойкость [8].

Развитие тенденции MDS-матрицы описано в работах [2,4], которые применяются для проектирования легковесных криптографических алгоритмов. MDS-матрицы часто используются для построения оптимальных линейных диффузионных слоев во многих легковесных шифрах. Современные легковесные криптографические алгоритмы применяют линейные слои для диффузии. Например, в хэш-функции PHOTON [9] был предложен новый тип матрицы MDS, который может быть вычислен последовательным или рекурсивным способом. Данная конструкция значительно уменьшает временную память (и, следовательно, аппаратную часть), необходи-

мую для вычисления матрицы. Такие матрицы позже были использованы в блочном шифре LED [7], в схеме шифрования с аутентификацией PRIMATE [10] и были дополнительно изучены и обобщены в работах [11, 12]. Последовательные матрицы за счет увеличения числа циклов применения матрицы обеспечивают оптимальное использование площади. Данный вариант отлично подходит для реализации с округлением или с низкой задержкой.

Важно отметить еще одно интересное свойство матрицы MDS – использование одной и той же диффузионной матрицы для шифрования и дешифрования. Такие шифры как PRINCE, ANUBIS, ICEBERG, KHAZAD использовали идею инволюции, определив функцию округления, которая состоит из операций инволюции, и где свойство неинволюции шифра, в основном, обеспечивается расписанием ключей.

Существует несколько способов построения MDS-матрицы [13-16], распространенным методом является использование циркулянтной конструкции как для блочного шифра AES, так и для хеш-функции WHIRLPOOL. Преимущество циркулянтной матрицы для аппаратных реализаций состоит в том, что все ее строки похожи (с точностью до правого смещения), и можно тривиально использовать схему умножения для экономии затрат на реализацию. В работе [17] было доказано, что циркулянтные матрицы 4-го порядка не могут быть одновременно MDS и инволютивными. Авторы [18] доказали, что циркулянтные инволютивные MDS-матрицы не существуют. Поиск облегченных матриц, которые являются одновременно и MDS, и инволюционными, является непростой задачей, и эта тема привлекла внимание научного сообщества.

В работе [19] авторы рассматривают матрицы Вандермонда или Адамара, а в работе [20] – матрицы Коши. Эти конструкции позволяют строить инволютивные матрицы MDS для больших размеров. Типы MDS-матриц: Матрица Вандермонда, Матрица Адамара, Инволютивная матрица (одна и та же

Таблица 2 – Сравнение MDS-матрицы над GF (2^8)

инволютивные MDS-матрицы			неинволютивные MDS-матрицы		
Типы матриц	Конечное поле	Коэффициенты	Типы матриц	Конечное поле	Коэффициенты
матрица 4x4					
Матрица Адамара	GF(2^8)/0x11d	(0x01; 0x02; 0x04; 0x06)	Циркулярная матрица	GF(2^8)/0x11b	(0x02; 0x03; 0x01; 0x01)
Матрица Коши	GF(2^8)/0x11b	(0x01; 0x12; 0x04; 0x16)			
Матрица Адамара-Коши	GF(2^8)/0x11b	(0x01; 0x02; 0xfc; 0xfe)			
матрица 8x8					
Матрица Адамара	GF(2^8)/0x11d	(0x01; 0x03; 0x04; 0x05; 0x06; 0x08; 0x0b; 0x07)	Циркулярная матрица	GF(2^8)/0x11d	(0x01; 0x01; 0x04; 0x01; 0x08; 0x05; 0x02; 0x09)
Матрица Адамара-Коши	GF(2^8)/0x11b	(0x01; 0x02; 0x06; 0x8c; 0x30; 0xfb; 0x87; 0xc4)	Циркулярная матрица	GF(2^8)/0x11d	Похоже на WHIRLPOOL
матрица 16x16					
Матрица Адамара-Коши	GF(2^8)/0x11b	(0x01,0x03,0x08,0xb2,0x0d, 0x60,0xe8,0x1c, 0x0f,0x2c,0xa2,0x8b, 0xc9,0x7a,0xac,0x3)	Матрица Адамара- Коши	GF(2^8)/0x1c3	0xb1; 0x1c; 0x30; 0x09; 0x08; 0x91; 0x18; 0xe4; 0x98; 0x12; 0x70; 0xb5; 0x97; 0x90; 0xa9; 0x5b
матрица 32x32					
Матрица Адамара-Коши	GF(2^8)/0x11b	0x01,0x02,0x04,0x69,0x07,0xec,0xcc,0x72, 0x0b,0x54,0x29,0xbe,0x74,0xf9,0xc4,0x87, 0x0e,0x47,0xc2,0xc3,0x39,0x8e,0x1c,0x85, 0x58,0x26,0x1e,0xaf,0x68, 0xb6,0x59,0x1f)	Матрица Адамара- Коши	GF(2^8)/0x1c3	0xb9; 0x7c; 0x93; 0xbc; 0xbd; 0x26; 0xfa; 0xa9;, 0x32; 0x31; 0x24; 0xb5; 0xbb; 0x06; 0xa0; 0x44;, 0x95; 0xb3; 0x0c; 0x1c; 0x07; 0xe5; 0xa4; 0x2e; 0x56; 0x4c; 0x55; 0x02; 0x66; 0x39; 0x48; 0x08

MDS-матрица для шифрования и расшифрования), Матрица Коши, Циркулярная матрица (как в AES) приведены в таблице 2.

В работе [21] приведено сравнение типов MDS-матриц, они были разделены на инволютивные MDS-матрицы и неинволютивные MDS-матрицы как показано в таблице 2. Распространенным способом построения MDS-матрицы является запуск с циркулянтной матрицы, причина в том, что вероятность нахождения матрицы MDS будет выше, чем у нормальной квадратной матрицы. Интересным свойством циркулянтных матриц является то, что каждая строка отличается от предыдущей строки смещением вправо, пользователь может просто реализовать одну строку умножения матриц аппаратно и повторно использовать схему умножения для последующих строк, просто сдвигая вход.

В последнее время несколько исследований [22,23] было посвящено построению рекурсивных MDS-матриц из матриц обобщенной структуры Фейстеля (GFN). Такой метод позволяет применять MDS-матрицу, используя итеративный процесс, который выглядит как сеть Фейстеля с линейными функциями вместо нелинейных. Также важно отметить преимущество построения MDS-матриц на основе матриц GFN, которое проявляется в двух аспектах. Во-первых, рекурсивная GFN MDS-матрица может быть реализована путем параллельных вычислений, что сократит время выполнения. Во-вторых, обратная матрица рекурсивной GFN MDS-матрицы, также является рекурсивной GFN MDS-матрицей, и они имеют одинаковое число XOR.

Выводы

В последнее время большое внимание уделяется поиску эффективно реализуемых MDS-матриц для криптографических алгоритмов. В работе было рассмотрено использование матрицы MDS для диффузии в таких блочных шифрах, как AES, SHARK, Square, Twofish, Anubis, KHAZAD, Manta, Hierocrypt, Kalyna, а также в потоковом шифре MUGI и криптографической хэш-функции Whirlpool. Были описаны MDS-матрицы, применяющиеся в легковесных криптографических алгоритмах PHOTON, LED, PRIMATE.

ЛИТЕРАТУРА

1. B. W. Koo, H. S. Jang, J. H. Song. Constructing and Cryptanalysis of a 16x16 Binary Matrix as a Diffusion Layer, Proceedings of Information Security Applications: 4th International Workshop (WISA2003), Lecture Notes in Computer Science, Vol. 2908, pp. 489-503, Springer-Verlag, 2003.
2. Duval S., Leurent G. MDS matrices with lightweight circuits //IACR Transactions on Symmetric Cryptology. – 2018.
3. Andreeva, E., Bilgin, B., Bogdanov, A., Luykx, A., Mendel, F., Mennink, B., Mouha, N., Wang, Q., Yasuda, K.: PRIMATEs v1. Submission to the CAESAR Competition (2014)
4. Christof Beierle, Thorsten Kranz, and Gregor Leander. Lightweight multiplication in GF(2n) with applications to MDS matrices. In Matthew Robshaw and Jonathan Katz, editors, CRYPTO 2016, Part I, volume 9814 of LNCS, pages 625–653. Springer, Heidelberg, August 201
5. E. Biham and A. Shamir, Differential cryptanalysis of DES-like cryptosystems, Proceedings of CRYPTO'90, Lecture Notes in Computer Science, Vol. 537, pp. 2-21, Springer-Verlag, 1991
6. M. Matsui, Linear cryptanalysis method for DES cipher, Proceedings of EUROCRYPT 93, Lecture Notes in Computer Science, Vol. 765, pp. 386-397, Springer-Verlag, 1994.
7. Jian Guo, Thomas Peyrin, Axel Poschmann, and Matthew J. B. Robshaw. The LED Block Cipher. In CHES, pages 326–341, 2011.
8. J. Nakahara Jr., E. Abrahão, A new Involutory MDS Matrix for the AES, International Journal of Network Security, Vol. 9, n. 2, pp. 109-116, 2009.
9. Guo, J., Peyrin, T., Poschmann, A.: The PHOTON family of lightweight hash functions. In: Rogaway, P. (ed.) CRYPTO 2011. LNCS, vol. 6841, pp. 222–239. Springer, Heidelberg (2011

10. Andreeva, E., Bilgin, B., Bogdanov, A., Luykx, A., Mendel, F., Mennink, B., Mouha, N., Wang, Q., Yasuda, K.: PRIMATEs v1. Submission to the CAESAR Competition (2014)
11. Augot, D., Finiasz, M.: Direct construction of recursive MDS diffusion layers using shortened BCH codes. In: Cid, C., Rechberger, C. (eds.) FSE 2014. LNCS, vol. 8540, pp. 3–17. Springer, Heidelberg (2015)
12. Augot, D., Finiasz, M.: Exhaustive search for small dimension recursive MDS diffusion layers for block ciphers and hash functions. In: ISIT, pp. 1551–1555 (2013)
13. Kishan Chand Gupta and Indranil Ghosh Ray. On Constructions of Involutory MDS Matrices. In AFRICACRYPT, pages 43–60, 2013.
14. K. Khoo, T. Peyrin, A. Poschmann, and H. Yap. FOAM: Searching for Hardware- Optimal SPN Structures and Components with a Fair Comparison. In Crypto- graphic Hardware and Embedded Systems CHES 2014, volume 8731 of Lecture Notes in Computer Science, pages 433–450. Springer Berlin Heidelberg, 2014
15. M.i Sajadieh, M. Dakhilalian, H. Mala, and B. Omoomi. On construction of in- volutory MDS matrices from Vandermonde Matrices in GF(2 q). Des. Codes Cryptography, 64(3):287–308, 2012.
16. Joan Daemen and Vincent Rijmen. The Design of Rijndael: AES - The Advanced Encryption Standard. Springer, 2002.
17. Pascal Junod and Serge Vaudenay. Perfect Diffusion Primitives for Block Ciphers. In Helena Handschuh and M. Anwar Hasan, editors, Selected Areas in Cryptogra- phy, volume 3357 of LNCS, pages 84–99. Springer, 2004.
18. Kishan Chand Gupta and Indranil Ghosh Ray. On Constructions of Circulant MDS Matrices for Lightweight Cryptography. In ISPEC, pages 564–576, 2014
19. M.i Sajadieh, M. Dakhilalian, H. Mala, and B. Omoomi. On construction of in- volutory MDS matrices from Vandermonde Matrices in GF(2 q). Des. Codes Cryptography, 64(3):287–308, 2012.
20. Kishan Chand Gupta and Indranil Ghosh Ray. On Constructions of Involutory MDS Matrices. In AFRICACRYPT, pages 43–60, 2013.
21. Sim S. M. et al. Lightweight MDS involution matrices //International Workshop on Fast Software Encryption. – Springer, Berlin, Heidelberg, 2015. – С. 471-493
22. Augot, D., Finiasz, M.: Direct construction of recursive MDS diffusion layers using shortened BCH codes. In: Cid, C., Rechberger, C. (eds.) FSE 2014. LNCS, vol. 8540, pp. 3–17. Springer, Heidelberg (2015).
23. Qiuping Li, Baofeng Wu, Liu Zhuojun Liu. Lightweight Recursive MDS Matrices with Generalized Feistel Network: 13th International Workshop on Security, IWSEC 2018, Sendai, Japan, September 3-5, 2018, Proceedings Advances in Information and Computer Security