ЛИНЕЙНЫЕ СВОЙСТВА МОДУЛЯРНОГО ПОДХОДА К РАЗДЕЛЕНИЮ СЕКРЕТА

Т. В. Галибус

Белорусский государственный университет
Минск, Беларусь
E-mail:tan2tan@gmail.com

Продолжено исследование эффективности модулярного подхода на некоторые общие свойства модулярного и широко изученного линейного подхода. Дано точное определение общей модулярной схемы и доказано, что всякая линейная схема может быть представлена в виде модулярной. Указаны условия, в которых использование модулярного алгоритма для построения общей схемы более эффективно с точки зрения информационного уровня, чем использование общей линейной схемы Беналоу–Ляйхтера. Представлена структура доступа, для которой модулярный подход дает существенное преимущество с точки зрения информационного уровня.

Ключевые слова: модулярная схема, структуры доступа, совершенность, разделение секрета.

Разделение секрета – широко используемый криптографический примитив. Основной сферой применения схем разделения секрета являются распределенные вычисления, электронные системы обмена данными, защищенная групповая подпись.

Основные задачи в разделении секрета: генерация совершенных, т. е. защищенных схем, для определенных структур доступа, во-вторых, эффективная с точки зрения хранения информации реализация схем с оптимальным информационным уровнем.

Наиболее на данный момент изучен линейный подход к разделению секрета, в основе которого лежат классические конструкции линейной алгебры [5]. Общая совершенная линейная схема разделения секрета основывается на методе Беналоу–Ляйхтера [4]. Таким образом, любая линейная схема обладает совершенной реализацией. Вопрос об идеальности линейных схем в полной общности не разрешен, однако известна нижняя граница информационного уровня для таких схем, связанная со специальными преобразованиями матриц MSP (Monotone Span Program), которые эквивалентны линейным схемам [9]. В последнее время, однако, возрастает интерес к нелинейным подходам в разделении секрета [3].

Нашей задачей было исследование свойств модулярного подхода [1], который длительное время не развивался в силу того, что был недостаточно изучен и считался узкоприменимым и незащищенным. Основным препятствием для развития подхода стало отсутствие прикладных совершенных модулярных схем [10]. Нам удалось это препятствие обойти и построить общую совершенную [7],[11] и идеальную пороговую схему [8], применимую на практике. Кроме того, в некоторых случаях модулярный подход дает выигрыш по сравнению с линейным с точки зрения сложности вычислений [1].

В данной работе мы продолжаем изучение свойств и преимуществ модулярного подхода. Во-первых, мы покажем, что всякая модулярная схема может быть представлена в виде линейной. Во-вторых, мы сравниваем наш алгоритм построения общей модулярной схемы с точки зрения эффективности с общим линейным подходом

Беналоу–Ляйхтера. Наконец, мы докажем, что существуют структуры доступа, модулярный подход к реализации который эффективнее, нежели линейный.

Введем общее определение схемы распределения секрета [3].

Обозначим через S конечное множество секретов, $|S| \geq 2$. **Схемой распределения с n участниками** называется рандомизированное отображение Π: $S \rightarrow S_0 \times \ldots \times S_{n-1}$, где S_i – множество частичных секретов участника i.

Схема распределения называется **схемой разделения секрета s, реализующей структуру доступа Г**, если дополнительно дилер распределяет секрет s из S согласно Π путем выбора вектора $(s_0, ..., s_{n-1})$ из $\Pi(s)$ и передачи значений частичных секретов участникам по секретным каналам, и полученная схема удовлетворяет свойствам корректности (любое разрешенное подмножество из Г в точности восстанавливает секрет) и совершенности (любое запрещенное подмножество не получает никакой информации о секрете).

Общепринятое определение линейной схемы распределения основывается на данном общем определении [3], [9].

Для **линейной схемы разделения секрета** множество S должно быть подмножеством конечного поля F, S_i – подмножествами конечномерных векторных пространств над данным конечным полем, а отображение Π должно быть линейным, т. е. любой частичный секрет вычисляется как линейная комбинация l равномерно распределенных элементов поля и секрета s.

Аналогичным образом можно ввести определение модулярной схемы. Насколько нам известно, такое определение вводится впервые.

Пусть S – RT(I) (множество приведенных мономов идеала в кольце полиномов над конечным полем), S_i – RP(I_i) (множество приведенных полиномов идеала в кольце полиномов над конечным полем), а отображение Π является преобразованием приведения, т. е. любой частичный секрет вычисляется как результат приведения по модулю I_i значения С, полученного путем применения китайской теоремы об остатках к l равномерно распределенным элементам RP(I) и секрету s [2]. Тогда построенная таким образом схема разделения секрета s реализует структуру доступа Г, при условии выполнения свойств корректности и совершенности.

Обычное определение модулярной схемы эквивалентно данному [11].

Из определения следует, что любое модулярное преобразование является линейным для максимальных равноостаточных идеалов [11], т. е. верно следующее

Утверждение. Любая модулярная схема с использованием максимальных равноостаточных идеалов может быть представлена в виде линейной.

Утверждение позволяет указать на взаимосвязь модулярного и линейного подхода. При этом одному набору модулей может соответствовать несколько различных линейных схем, в зависимости от случайного выбора частичных секретов. Мы считаем, что для любой структуры доступа возможно дать ответ о том, какой подход предпочтительнее – модулярный или линейный.

Пока мы рассмотрели наш модулярный алгоритм для реализации общей схемы [7],[11] по сравнению с общим подходом Беналоу–Ляйхтера [4].

Утверждение. Общая схема разделения секрета, основанная на модулярном подходе, эффективнее с точки зрения информационного уровня, нежели общая схема Беналоу–Ляйхтера, в том случае, когда:

$$\left|\Gamma^*\right| < \max C_i,$$

где C_i – количество минимальных разрешенных и максимальных запрещенных подмножеств, в которых участвует участник i.

Доказательство. Следует из того факта, что в первом случае размер частичного секрета определяется количеством максимальных запрещенных подмножеств, в которых не участвует i, а во втором – размер определяется количеством минимальных разрешенных, в которых i участвует.

Можем уточнить данную оценку, применив следующую лемму.

Лемма. Любому минимальному разрешенному подмножеству мощности k структуры доступа соответствует k попарно различных максимальных запрещенных подмножеств, мощность которых больше либо равна k–1.

Доказательство. Очевидно, что все (k–1) – подмножества минимального разрешенного подмножества A являются либо попарно различными максимальными запрещенными либо подмножествами максимальных запрещенных. Докажем, что два (k–1)-подмножества B_1 и B_2, $B_1, B_2 \subset A$ не могут принадлежать одному и тому же максимальному запрещенному B. В самом деле, это означало бы, что и $A \subset B$, поскольку $A = B_1 \cup B_2$.

Из утверждения и леммы следует теорема.

Теорема. Общая схема разделения секрета, основанная на модулярном подходе, эффективнее с точки зрения информационного уровня, нежели общая схема Беналоу–Ляйхтера в том случае, когда:

$$\left|\Gamma^*\right| < 1 + k_{\max}\left(k_{\max} - 1\right)/2,$$

где $k_{\max}$ – максимальная мощность минимального разрешенного подмножества.

Доказательство. Из леммы следует, что $C_i \geq 1 + C_k^{k-2} = 1 + k(k-1)/2$, т. е. $\max C_i \geq 1 + k_{\max}(k_{\max} - 1)/2$.

Для случая, когда все максимальные запрещенные и минимальные разрешенные являются подмножествами мощности k, имеется более точная оценка.

Утверждение. Общая схема разделения секрета, основанная на модулярном подходе, эффективнее с точки зрения размера частичных ключей, нежели общая схема Беналоу–Ляйхтера, в том случае, когда:

$$\left|\Gamma^*\right| < k/(t-k+1)C_t^k.$$

Приведем пример структуры доступа, для которой мы доказали, что информационный уровень ее линейной реализации не превышает 1/2, в то время как существует ее модулярная реализация с уровнем 2/3.

Утверждение. Существует структура доступа, модулярная реализация которой эффективнее любой линейной.

Доказательство. Для оценки нижней границы эффективности (размера матрицы MSP) линейных схем мы использовали метод [6], опирающийся на оценку ранга специальной матрицы коллекции уникальных пересечений данной структуры доступа.

Пусть Γ – структура доступа для трех участников, где {1, 2}, {2, 3} – запрещенные подмножества, а {1, 3} – разрешенные. Коллекцией множеств с уникальным пересечением [6] для такой структур является набор {{1},{2}}, {{3},{2}}. Ранг соответствующей матрицы D = 2. Это означает, что нижняя граница эффективности любой линейной схемы для данной структуры доступа есть 1/2. Приведем модулярную реализацию в кольце полиномов от одной переменной с уровнем 2/3:

$$m_1 = p_1^2(x)p_2(x), m_2 = p_2(x)p_3(x), m_3 = p_4^2(x)p_3(x),$$

где $p_i(x)$ – приведенные полиномы одной степени. Таким образом, мы показали, что модулярное разделение секрета обладает преимуществами по сравнению с хорошо изученным линейным подходом.

Библиографические ссылки

1. *Asmuth C. A., Bloom J.* A modular approach to key safeguarding // IEEE Trans. on inf. theory. 1983. V. 29. P. 156–169.
2. *Becker T., Weispfenning V.* Grebner bases. A Computational Approach to Commutative Algebra. Springer-Verlag, 1993.
3. *Beimel A., Ishai Y.* On the power of nonlinear secret-sharing // SIAM J. on Discrete Mathematics. 2005. V. 19(1). P. 258–280.
4. *Benaloh J., Leichter J.* Generalized secret sharing and monotone functions // LNCS. 1990. V. 403. P. 27–35.
5. *Blakley G. R.* Safeguarding cryptographic keys // Proc. of the 1979 AFIPS National Computer Conference. 1979. V. 48. P. 313–317.
6. *Gal A., Pudlak P.* Monotone complexity and the rank of matrices // Inform. Process. Lett 2003. V. 87. P. 321–326.
7. *Galibus T., Matveev G.* Generalized Mignotte Sequences in Polynomial Rings // Electronic Notes on Theoretical Computer Science. 2007. V. 186. P. 39–45.
8. *Galibus T., Matveev G., Shenets N.* Some structural and security properties of the modular secret sharing // SYNASC'08, V. Negru [et al.] eds., IEEE Comp. Soc. CPC, California, 2009. P. 197–200.
9. *Karchmer M., Wigderson A.* On span programs // Proc. of the 8th IEEE Structure in Complexity Theory. 1993. P. 102–111.
10. *Quisquater M., Prenel B., Wandervalle J.* On the security of the threshold scheme based on the Chinese remainder theorem // LNCS. 2002. V. 2274. P. 199–210.
11. *Галибус Т. В.* Идеалы симметрических отношений и разделение секрета // Вестник Белорус. гос. ун-та. Сер. 1. Физика. Математика. Информатика. 2011. № 2. С. 141–143.