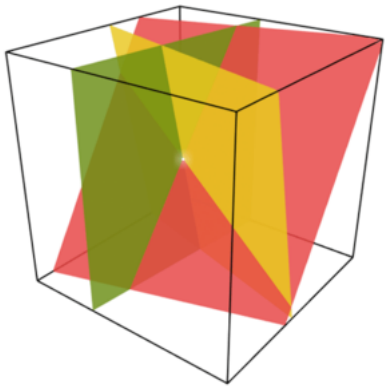
ВикипедиЯ

Разделение секрета

Материал из Википедии — свободной энциклопедии

Разделение секрета (англ. *Secret sharing*) — термин в криптографии, под которым понимают любой из способов распределения секрета среди группы участников, каждому из которых достаётся своя некая доля. Секрет может воссоздать только коалиция участников из первоначальной группы, причём входить в коалицию должно не менее некоторого изначально известного их числа.



Каждая доля секрета — это плоскость, а секрет представляет собой точку пересечения трёх плоскостей. Две доли секрета позволяют получить линию, на которой лежит секретная точка.

Схемы разделения секрета применяются в случаях, когда существует значимая вероятность компрометации одного или нескольких хранителей секрета, но вероятность недобросовестного сговора значительной части участников считается пренебрежимо малой.

Существующие схемы имеют две составляющие: разделение и восстановление секрета. К разделению относится формирование частей секрета и распределение их между членами группы, что позволяет разделить ответственность за секрет между её участниками. Обратная схема должна обеспечить его восстановление при условии доступности его хранителей в некотором необходимом количестве[1].

Пример использования: протокол тайного голосования на основе разделения секрета[2].

Содержание

Простейший пример схемы разделения секрета

Пусть имеется группа из t человек и сообщение s длины n, состоящее из двоичных символов. Если подобрать случайным образом такие двоичные сообщения $s_1, \ldots, s_t$, что в сумме они будут равняться s, и распределить эти сообщения между всеми членами группы, получится, что прочесть сообщение будет возможно только в случае, если все члены группы соберутся вместе[1].

В такой схеме есть существенная проблема: в случае утраты хотя бы одного из членов группы, секрет будет утерян для всей группы безвозвратно.

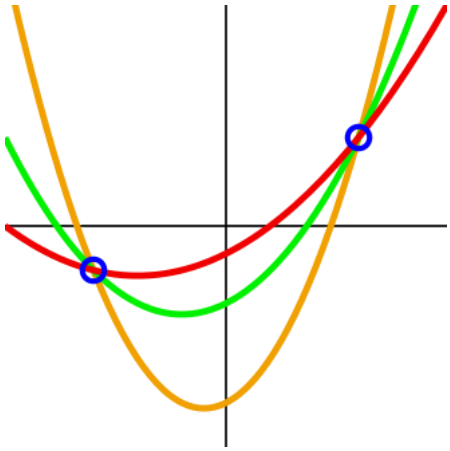
Пороговая схема

В отличие от процедуры разбиения секрета, где $t = n$, в процедуре разделения секрета количество долей, которые нужны для восстановления секрета, может отличаться от того, на сколько долей секрет разделён. Такая схема носит названия **пороговой схемы** (t, n), где n — количество долей, на которые был разделён секрет, а t — количество долей, которые нужны для восстановления секрета. Идеи схем $t \neq n$ были независимо предложены в 1979 году Ади Шамиром и Джорджем Блэкли. Кроме этого, подобные процедуры исследовались Гусом Симмонсом[3][4][5].

Если коалиция участников такова, что они имеют достаточное количество долей для восстановления секрета, то коалиция называется разрешённой. Схемы разделения секрета, в которых разрешённые коалиции участников могут однозначно восстановить секрет, а неразрешённые не получают никакой апостериорной информации о возможном значении секрета, называются совершенными[6].

Схема Шамира

Идея схемы заключается в том, что двух точек достаточно для задания прямой, трех точек — для задания параболы, четырёх точек — для кубической параболы, и так далее. Чтобы задать многочлен степени k требуется $k + 1$ точек.



Через две точки можно провести неограниченное число полиномов степени 2. Чтобы выбрать из них единственный — нужна третья точка

Для того, чтобы после разделения секрет могли восстановить только k участников, его «прячут» в формулу многочлена степени $(k - 1)$ над конечным полем G. Для однозначного восстановления этого многочлена необходимо знать его значения в k точках, причем, используя меньшее число точек, однозначно восстановить исходный многочлен не получится. Количество же различных точек многочлена не ограничено (на практике оно ограничивается размером числового поля G, в котором ведутся расчёты).

Кратко данный алгоритм можно описать следующим образом. Пусть дано конечное поле G. Зафиксируем n различных ненулевых несекретных элементов данного поля. Каждый из этих элементов приписывается определённому члену группы. Далее выбирается произвольный набор из t элементов поля G, из которых составляется многочлен $f(x)$ над полем G степени $t - 1, 1 < t \leq n$. После получения многочлена высчитываем его значение в несекретных точках и сообщаем полученные результаты соответствующим членам группы[1].

Чтобы восстановить секрет можно воспользоваться интерполяционной формулой, например формулой Лагранжа.

Важным достоинством схемы Шамира является то, что она легко масштабируема[5]. Чтобы увеличить число пользователей в группе, необходимо лишь добавить соответствующее число несекретных элементов к уже существующим, при этом должно выполняться условие $r_i \neq r_j$ при $i \neq j$. В то же время, компроментация одной части секрета переводит схему из (n, t)-пороговой в $(n - 1, t - 1)$-пороговую.

Схема Блэкли

Две непараллельные прямые на плоскости пересекаются в одной точке. Любые две некомпланарные плоскости пересекаются по одной прямой, а три некомпланарные плоскости в пространстве пересекаются тоже в одной точке. Вообще n n-мерных гиперплоскостей всегда пересекаются в одной точке. Одна из

координат этой точки будет секретом. Если закодировать секрет как несколько координат точки, то уже по одной доле секрета (одной гиперплоскости) можно будет получить какую-то информацию о секрете, то есть о взаимозависимости координат точки пересечения.

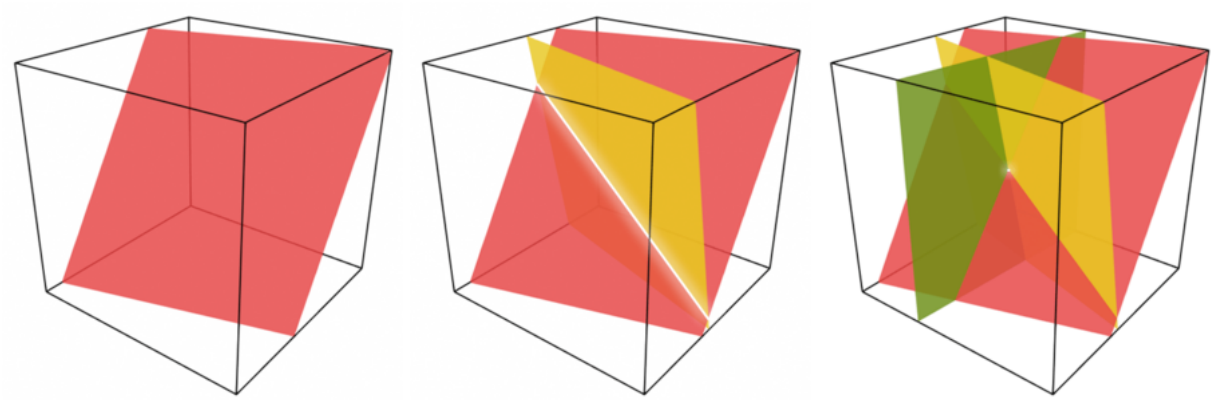


Схема Блэкли в трёх измерениях: каждая доля секрета — это плоскость, а секрет — это одна из координат точки пересечения плоскостей. Двух плоскостей недостаточно для определения точки пересечения.

С помощью схемы Блэкли[4] можно создать *(t, n)*-схему разделения секрета для любых *t* и *n*: для этого надо положить размерность пространства равную *t*, и каждому из *n* игроков дать одну гиперплоскость, проходящую через секретную точку. Тогда любые *t* из *n* гиперплоскостей будут однозначно пересекаться в секретной точке.

Схема Блэкли менее эффективна, чем схема Шамира: в схеме Шамира каждая доля такого же размера, как и секрет, а в схеме Блэкли каждая доля в *t* раз больше. Существуют улучшения схемы Блэкли, позволяющие повысить её эффективность.

Схемы, основанные на китайской теореме об остатках

В 1983 году Морис Миньотт, Асмут и Блум предложили две схемы разделения секрета, основанные на китайской теореме об остатках. Для некоторого числа (в схеме Миньотта это сам секрет, в схеме Асмута — Блума — некоторое производное число) вычисляются остатки от деления на последовательность чисел, которые раздаются сторонам. Благодаря ограничениям на последовательность чисел, восстановить секрет может только определённое число сторон[7][8].

Пусть количество пользователей в группе равно n. В схеме Миньотта выбирается некоторое множество попарно взаимно простых чисел $\{m_1, m_2, \ldots, m_n\}$ таких, что произведение $k-1$ наибольших чисел меньше, чем произведение k наименьших из этих чисел. Пусть эти произведения равны M и N, соответственно. Число k называется порогом для конструируемой схемы по множеству $\{m_1, m_2, \ldots, m_n\}$. В качестве секрета выбирается число S такое, для которого выполняется соотношение $M < S < N$. Части секрета распределяются между участниками группы следующим образом: каждому участнику выдается пара чисел (r_i, m_i), где $r_i \equiv S \pmod{m_i}$.

Чтобы восстановить секрет, необходимо объединить $t \geq k$ фрагментов. В этом случае получим систему сравнений вида $x \equiv r_i \pmod{m_i}$, множество решений которой можно найти, используя китайскую теорему об остатках. Секретное число S принадлежит этому множеству и удовлетворяет условию $S < m_1 \cdot m_2 \cdot \ldots \cdot m_t$. Также несложно показать, что если число фрагментов меньше k, то, чтобы найти секрет S, необходимо перебрать порядка $\frac{N}{M}$ целых чисел. При правильном выборе чисел m_i такой перебор практически невозможно реализовать. К примеру, если разрядность m_i будет от 129 до 130 бит, а $k < 15$, то соотношение $\frac{N}{M}$ будет иметь порядок 2^{100}[9].

Схема Асмута — Блума является доработанной схемой Миньотта. В отличие от схемы Миньотта, её можно построить в таком виде, чтобы она была совершенной[10].

Схемы, основанные на решении систем уравнений

В 1983 году Карнин, Грин и Хеллман предложили свою схему разделения секрета, которая основывалась на невозможности решить систему с m неизвестными, имея менее m уравнений[11].

В рамках данной схемы выбираются $n+1$ m-мерных векторов $V_0, V_1, \ldots, V_n$ так, чтобы любая матрица размером $m \times m$, составленная из этих векторов, имела ранг m. Пусть вектор U имеет размерность m.

Секретом в схеме является матричное произведение $U^T \cdot V_0$. Долями секрета являются произведения $U^T \cdot V_i, 1 \leq i \leq n$.

Имея любые m долей, можно составить систему линейных уравнений размерности $m \times m$, неизвестными в которой являются коэффициенты U. Решив данную систему, можно найти U, а имея U, можно найти секрет. При этом система уравнений не имеет решения в случае, если долей меньше, чем m[12].

Способы обмана пороговой схемы

Существуют несколько способов нарушить протокол работы пороговой схемы:

- владелец одной из долей может помешать восстановлению общего секрета, отдав в нужный момент неверную (случайную) долю[13];
- злоумышленник, не имея доли, может присутствовать при восстановлении секрета. Дождавшись оглашения нужного числа долей, он быстро восстанавливает секрет самостоятельно и генерирует ещё одну долю, после чего предъявляет её остальным участникам. В результате он получает доступ к секрету и остаётся непойманным[14].

Также существуют другие возможности нарушения работы, не связанные с особенностями реализации схемы:

- злоумышленник может сымитировать ситуацию, при которой необходимо раскрытие секрета, тем самым выведав доли участников[14].

Примечания

1. Алферов, Зубов, Кузьмин и др., 2002, с. 401.
2. Schoenmakers, 1999.
3. *C. J. Simmons* An introduction to shared secret and/or shared control schemes and their application (англ.) // Contemporary Cryptology. — IEEE Press, 1991. — P. 441—497.
4. Blakley, 1979.
5. Shamir, 1979.
6. Блэкли, Кабатянский, 1997.
7. Mignotte, 1982.
8. Asmuth, Bloom, 1983.
9. Молдовян, Молдовян, 2005, с. 225.
10. Шенец, 2011.
11. Karnin, Greene, Hellman, 1983.
12. *Шнайер Б.* Прикладная криптография. — 2-е изд. — Триумф, 2002. — С. 590. — 816 с. — ISBN 5-89392-055-4.
13. Pasailă, Alexa, Iftene, 2010.
14. Шнайер, 2002, с. 69.

Литература

- *Шнайер Б.* 3.7. Разделение секрета // Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си = Applied Cryptography. Protocols, Algorithms and Source Code in C. — М.: Триумф, 2002. — С. 93—96. — 816 с. — 3000 экз. — ISBN 5-89392-055-4.
- *Шнайер Б.* 23.2 Алгоритмы разделения секрета // Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си = Applied Cryptography. Protocols, Algorithms and Source Code in C. — М.: Триумф, 2002. — С. 588—591. — 816 с. — 3000 экз. — ISBN 5-89392-055-4.

- *Blakley G. R.* Safeguarding cryptographic keys (https://www.computer.org/csdl/proceedings/afips/1979/5087/00/50870313.pdf) // *Proceedings of the 1979 AFIPS National Computer Conference* — Montvale: AFIPS Press, 1979. — P. 313–317. — doi:10.1109/AFIPS.1979.98 (http://dx.doi.org/10.1109/AFIPS.1979.98)
- *Shamir A.* How to share a secret (http://cs.jhu.edu/~sdoshi/crypto/papers/shamirturing.pdf) // *Commun. ACM* — New York City: ACM, 1979. — Vol. 22, Iss. 11. — P. 612–613. — ISSN 0001-0782 (https://www.worldcat.org/issn/0001-0782) — doi:10.1145/359168.359176 (http://dx.doi.org/10.1145/359168.359176)
- *Mignotte M.* How to Share a Secret // *Cryptography*: *Proceedings of the Workshop on Cryptography Burg Feuerstein, Germany, March 29–April 2, 1982* / T. Beth — Springer Berlin Heidelberg, 1983. — P. 371–375. — (Lecture Notes in Computer Science; Vol. 149) — ISBN 978-3-540-11993-7 — ISSN 0302-9743 (https://www.worldcat.org/issn/0302-9743) — doi:10.1007/3-540-39466-4_27 (http://dx.doi.org/10.1007/3-540-39466-4_27)
- *Asmuth C., Bloom J.* A modular approach to key safeguarding // *IEEE Trans. Inf. Theory* / F. Kschischang — IEEE, 1983. — Vol. 29, Iss. 2. — P. 208–210. — ISSN 0018-9448 (https://www.worldcat.org/issn/0018-9448) — doi:10.1109/TIT.1983.1056651 (http://dx.doi.org/10.1109/TIT.1983.1056651)
- *Karnin E. D., Greene J. W., Hellman M. E.* On Secret Sharing Systems (http://www-ee.stanford.edu/~hellman/publications/45.pdf) // *IEEE Trans. Inf. Theory* / F. Kschischang — IEEE, 1983. — Vol. 29, Iss. 1. — P. 35–41. — ISSN 0018-9448 (https://www.worldcat.org/issn/0018-9448) — doi:10.1109/TIT.1983.1056621 (http://dx.doi.org/10.1109/TIT.1983.1056621)
- *Блэкли Д., Кабатянский Г. А.* Обобщенные идеальные схемы, разделяющие секрет, и матроиды (http://www.mathnet.ru/php/archive.phtml?wshow=paper&jrnid=ppi&paperid=381) // *Пробл. передачи информ.* — 1997. — Т. 33, вып. 3. — С. 102–110.
- *Schoenmakers B.* A Simple Publicly Verifiable Secret Sharing Scheme and Its Application to Electronic Voting (http://link.springer.com/content/pdf/10.1007%2F3-540-48405-1_10.pdf) // *Advances in Cryptology — CRYPTO' 99*: *19th Annual International Cryptology Conference Santa Barbara, California, USA, August 15–19, 1999 Proceedings* / M. Wiener — Springer Berlin Heidelberg, 1999. — P. 148–164. — ISBN 978-3-540-66347-8 — doi:10.1007/3-540-48405-1_10 (http://dx.doi.org/10.1007/3-540-48405-1_10)
- *Алферов А. П., Зубов А. Ю., Кузьмин А. С. и др.* Основы криптографии: Учебное пособие — 2-е изд., испр. и доп. — М.: Гелиос АРВ, 2002. — ISBN 978-5-85438-137-6
- *Молдовян Н. А., Молдовян А. А.* Введение в криптосистемы с открытым ключом — СПб.: БХВ-Петербург, 2005. — 288 с. — (Учебное пособие) — ISBN 978-5-94157-563-3
- *Pasailă D., Alexa V., Iftene S.* Cheating Detection and Cheater Identification in CRT-based Secret Sharing Schemes (http://computingonline.net/index.php/computing/article/view/702) // *International Journal of Computing* — 2010. — Vol. 9, Iss. 2. — P. 107–117. — ISSN 2312-5381 (https://www.worldcat.org/issn/2312-5381)
- *Шенец Н. Н.* Об идеальных модулярных схемах разделения секрета в кольцах многочленов от нескольких переменных (http://www.elib.bsu.by/bitstream/123456789/9565/1/pages%20from%20%D0%9A%D0%BE%D0%BD%D1%84%D0%B5%D1%80%D0%B5%D0%BD%D1%86%D0%B8%D1%8F_1.%20169-173pdf.pdf) // *Международный конгресс по информатике: информационные системы и технологии*: *материалы международного научного конгресса 31 окт.* — Минск: БГУ, 2011. — Т. 1. Статьи факультета прикладной математики и информатики. — С. 169–173. — ISBN 978-985-518-563-6
