ВикипедиЯ

Схема разделения секрета Шамира

Материал из Википедии — свободной энциклопедии

Схема интерполяционных полиномов Лагранжа (**схема разделения секрета Шамира** или **схема Шамира**) — схема разделения секрета, широко используемая в криптографии. Схема Шамира позволяет реализовать (k, n) — пороговое разделение секретного сообщения (секрета) между n сторонами так, чтобы только любые k и более сторон ($k \le n$) могли восстановить секрет. При этом любые $k-1$ и менее сторон не смогут восстановить секрет.

Содержание

История
Идея
Описание
- Подготовительная фаза
- Генерация долей секрета
- Восстановление секрета

Свойства
Использование
Пример
См. также
Примечания
Литература
Ссылки

История

В 1979 году израильский криптоаналитик Ади Шамир предложил пороговую схему разделения секрета между n сторонами, которая позволяет проводить разделение таким образом, что[1]:

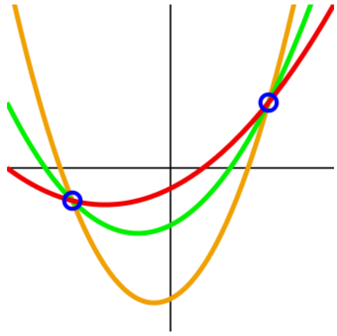
- Для восстановления секрета достаточно k и больше сторон.
- Никакие $(k-1)$ и меньше сторон не смогут получить никакой информации о секрете.

Идея

Для интерполяции многочлена степени $k-1$ требуется k точек. К примеру, для задания прямой достаточно двух точек, для задания параболы —трех точек, и так далее.

Основная идея данной схемы состоит в том, что интерполяция **невозможна**, если известно меньшее число точек[1].

Если мы хотим разделить секрет между n людьми таким образом, чтобы восстановить его могли только k человек ($k \le n$), мы «прячем» его в формулу многочлена степени $k-1$. Восстановить этот многочлен и исходный секрет можно только по k точкам. Количество же различных точек многочлена не ограничено (на практике оно ограничивается размером числового поля, в котором ведутся расчёты)[2].



Через две точки можно провести неограниченное число полиномов степени 2. Чтобы выбрать из них единственный — нужна третья точка. Данные графики приведены только для иллюстрации идеи — в схеме Шамира используется конечное поле, полиномы над которым сложно представить на графике

Описание

Подготовительная фаза

Пусть нужно разделить секрет M между n сторонами таким образом, чтобы любые k участников могли бы восстановить секрет (то есть нужно реализовать (k, n)-пороговую схему).

Выберем некоторое простое число $p > M$. Это число можно открыто сообщать всем участникам. Оно задаёт конечное поле размера p. Над этим полем построим многочлен степени $k-1$ (то есть случайно выберем все коэффициенты многочлена, кроме M)[3]:

$$F(x) = \left(a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + \cdots + a_1 x + M\right) \mod p$$

В этом многочлене M — это разделяемый секрет, а остальные коэффициенты $a_{k-1}, a_{k-2}, \ldots, a_1$ — некоторые случайные числа, которые нужно будет «забыть» после того, как процедура разделения секрета будет завершена[3].

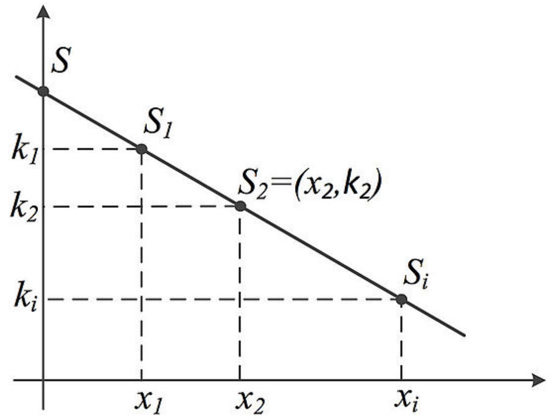
Генерация долей секрета

Теперь вычисляем «тени» — значения построенного выше многочлена, в n различных точках, причём $(x \neq 0)$[3]:

$$\begin{aligned} k_1 = &\quad F(1) = &\quad \left(a_{k-1} \cdot 1^{k-1} + a_{k-2} \cdot 1^{k-2} + \cdots + a_1 \cdot 1 + M\right) \mod p \\ k_2 = &\quad F(2) = &\quad \left(a_{k-1} \cdot 2^{k-1} + a_{k-2} \cdot 2^{k-2} + \cdots + a_1 \cdot 2 + M\right) \mod p \\ &\quad \ldots \\ k_i = &\quad F(i) = &\quad \left(a_{k-1} \cdot i^{k-1} + a_{k-2} \cdot i^{k-2} + \cdots + a_1 \cdot i + M\right) \mod p \\ &\quad \ldots \\ k_n = &\quad F(n) = &\quad \left(a_{k-1} \cdot n^{k-1} + a_{k-2} \cdot n^{k-2} + \cdots + a_1 \cdot n + M\right) \mod p \end{aligned}$$

Аргументы многочлена (номера секретов) не обязательно должны идти по порядку, главное — чтобы все они были различны по модулю p.

После этого каждой стороне, участвующей в разделении секрета, выдаётся доля секрета — тень k_i вместе с номером i. Помимо этого, всем сторонам сообщается степень многочлена $k-1$ и размер поля p. Случайные коэффициенты $a_{k-1}, a_{k-2}, \ldots, a_1$ и сам секрет M «забываются»[3].



Рассмотрим простой случай, когда для восстановления секрета необходимо две тени. Многочлен, в этом случае, будет задавать прямую, пересекающуюся с осью k в точке S (секрет). Каждая тень — точка на прямой. Секрет может быть восстановлен по двум произвольным теням. Однако, в случае задания лишь одной тени в качестве искомого секрета может быть выбрана любая точка на оси k, так как через одну точку можно провести множество различных прямых, пересекающихся с осью k в произвольных точках

Восстановление секрета

Теперь любые k участников, зная координаты k различных точек многочлена, смогут восстановить многочлен и все его коэффициенты, включая последний из них — разделяемый секрет[3].

Особенностью схемы является то, что вероятность раскрытия секрета в случае произвольных $k-1$ теней оценивается как p^{-1}. То есть в результате интерполяции по $k-1$ точке секретом может быть любой элемент поля с равной вероятностью[2]. При этом попытка полного перебора всех возможных теней не позволит злоумышленникам получить дополнительную информацию о секрете.

Прямолинейное восстановление коэффициентов многочлена через решение системы уравнений можно заменить на вычисление интерполяционного многочлена Лагранжа (отсюда одно из названий метода). Формула многочлена будет выглядеть следующим образом[3]:

$$\begin{aligned} F(x) = &\quad \sum_i l_i(x)\, y_i \mod p \\ l_i(x) = &\quad \prod_{i \neq j} \frac{x - x_j}{x_i - x_j} \mod p \end{aligned}$$

где (x_i, y_i) — координаты точек многочлена. Все операции выполняются также в конечном поле p[3].

Свойства

К достоинствам данной схемы разделения секрета относят[1]:

1. **Идеальность:** отсутствует избыточность — размер каждой из теней равен размеру секрета.
2. **Масштабируемость:** в условиях схемы (k, n) число владельцев части секрета n может дополнительно увеличиться вплоть до p, где p — размер поля, в котором ведутся вычисления. При этом количество теней k, необходимых для получения секрета, останется неизменным.
3. **Динамичность:** можно периодически менять используемый многочлен и пересчитывать тени, сохраняя секрет (свободный член) неизменным. При этом вероятность нарушения защиты путем утечки теней уменьшится, так как для получения секрета нужно k теней, полученных на одной версии многочлена.
4. **Гибкость:** в тех случаях, когда стороны не являются равными между собой схема позволяет это учесть путём выдачи сразу нескольких теней одной стороне. Например, пусковой код баллистической ракеты может быть разделён по схеме $(3, 6)$ так, чтобы ракету могли запустить лишь три генерала, которые соберутся вместе, либо один президент, которому при разделении секрета было выдано сразу три тени.

Недостатки[4]:

1. **Ненадёжность дилера:** по умолчанию в схеме предполагается, что тот, кто генерирует и раздаёт тени, надёжен, что не всегда верно.
2. **Нет проверки корректности теней сторон:** участвующая в разделении сторона не может с уверенностью сказать, что её тень подлинна — при подстановке в исходный многочлен получается верное равенство.

Использование

Данная схема нашла применение в аппаратных криптографических модулях. Где она используется для многопользовательской авторизации в инфраструктуре открытых ключей[5].

Также схема используется в цифровой стеганографии для скрытой передачи информации в цифровых изображениях[6][7][8][9], для противодействия атакам по сторонним каналам при реализации алгоритма AES[10].

Помимо этого, с помощью схемы Шамира может осуществляться нанесение цифрового водяного знака при передаче цифрового видео[11] и генерация персонального криптографического ключа, используемого в биометрических системах аутентификации[12].

Пример

Пусть нужно разделить секрет «11» между 5-ю сторонами. При этом любые 3 стороны должны иметь возможность восстановить этот секрет. То есть нужно реализовать $(3,5)$-пороговую схему[3].

Возьмём простое число $p = 13$. Построим многочлен степени $k - 1 = 3 - 1 = 2$:

$$F(x) = \left(7x^2 + 8x + 11\right) \mod 13$$

В этом многочлене 11 — это разделяемый секрет, а остальные коэффициенты 7 и 8 — некоторые случайные числа, которые нужно будет «забыть» после того, как процедура разделения секрета будет завершена.

Теперь вычисляем координаты 5 различных точек:

$$\begin{aligned}
k_1 = F(1) &= \left(7 \cdot 1^2 + 8 \cdot 1 + 11\right) \mod 13 = 0 \\
k_2 = F(2) &= \left(7 \cdot 2^2 + 8 \cdot 2 + 11\right) \mod 13 = 3 \\
k_3 = F(3) &= \left(7 \cdot 3^2 + 8 \cdot 3 + 11\right) \mod 13 = 7 \\
k_4 = F(4) &= \left(7 \cdot 4^2 + 8 \cdot 4 + 11\right) \mod 13 = 12 \\
k_5 = F(5) &= \left(7 \cdot 5^2 + 8 \cdot 5 + 11\right) \mod 13 = 5
\end{aligned}$$

После этого ключи (вместе с их номером, числом $p = 13$ и степенью многочлена $k - 1 = 2$) раздаются сторонам. Случайные коэффициенты $7, 8$ и сам секрет $M = 11$ «забываются».

Теперь любые 3 участника смогут восстановить многочлен и все его коэффициенты, включая последний из них — разделённый секрет. Например, чтобы восстановить многочлен по трём долям k_2, k_3, k_5 им нужно будет решить систему:

$$\begin{cases}
\left(a_2 \cdot 2^2 + a_1 \cdot 2 + M\right) \mod 13 = 3 \\
\left(a_2 \cdot 3^2 + a_1 \cdot 3 + M\right) \mod 13 = 7 \\
\left(a_2 \cdot 5^2 + a_1 \cdot 5 + M\right) \mod 13 = 5
\end{cases}$$

Очевидно, что с меньшим числом известных секретов получится меньше уравнений и систему решить будет нельзя (даже полным перебором решений).

Построим интерполяционный многочлен Лагранжа:

$$F(x) = \sum_i l_i(x)\, y_i \mod p$$

$$l_i(x) = \prod_{i \neq j} \frac{x - x_j}{x_i - x_j} \mod p$$

$$\begin{aligned}
l_1(x) &= \frac{x - x_2}{x_1 - x_2} \cdot \frac{x - x_3}{x_1 - x_3} = \frac{x-3}{2-3} \cdot \frac{x-5}{2-5} = \frac{1}{3}\left(x^2 - 8x + 15\right) = 9\left(x^2 + 5x + 2\right) = 9x^2 + 6x + 5 \mod 13 \\
l_2(x) &= \frac{x - x_1}{x_2 - x_1} \cdot \frac{x - x_3}{x_2 - x_3} = \frac{x-2}{3-2} \cdot \frac{x-5}{3-5} = \frac{1}{11}\left(x^2 - 7x + 10\right) = 6\left(x^2 + 6x + 10\right) = 6x^2 + 10x + 8 \mod 13 \\
l_3(x) &= \frac{x - x_1}{x_3 - x_1} \cdot \frac{x - x_2}{x_3 - x_2} = \frac{x-2}{5-2} \cdot \frac{x-3}{5-3} = \frac{1}{6}\left(x^2 - 5x + 6\right) = 11\left(x^2 + 8x + 6\right) = 11x^2 + 10x + 1 \mod 13
\end{aligned}$$

Получим исходный многочлен:

$$\begin{aligned}
&F(x) = 3 \cdot l_1(x) + 7 \cdot l_2(x) + 5 \cdot l_3(x) \mod p \\
&\quad a_2 = 9 \cdot 3 + 6 \cdot 7 + 11 \cdot 5 = 7 \mod 13 \\
&\quad a_1 = 6 \cdot 3 + 10 \cdot 7 + 10 \cdot 5 = 8 \mod 13 \\
&\quad M = 5 \cdot 3 + 8 \cdot 7 + 1 \cdot 5 = 11 \mod 13 \\
&F(x) = 7x^2 + 8x + 11 \mod 13
\end{aligned}$$

Последний коэффициент многочлена — $M = 11$ — и является секретом[3].

См. также

- Схема Блэкли
- Схема Карнина — Грина — Хеллмана

Примечания

1. *Shamir A.* How to share a secret (http://cs.jhu.edu/~sdoshi/crypto/papers/s

hamirturing.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)
2. *Чмора А.Л.* Современная прикладная криптография. — 2-е изд., стер.. — М.: Гелиос АРВ, 2002. — С. 123—124. — 256 с. — ISBN 5-85438-046-3.
3. *Шнайер Б.* 23.2 Алгоритмы разделения секрета. Схема интерполяционных полиномов Лагранжа // Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си = Applied Cryptography. Protocols, Algorithms and Source Code in C. — М.: Триумф, 2002. — С. 588—589. — 816 с. — 3000 экз. — ISBN 5-89392-055-4.
4. *Dawson E., Donovan D.* The breadth of Shamir's secret-sharing scheme // *Computers & Security* — Elsevier, 1994. — Vol. 13, Iss. 1, 69-78. — ISSN 0167-4048 (https://www.worldcat.org/issn/0167-4048); 1872-6208 (https://www.worldcat.org/issn/1872-6208) — doi:10.1016/0167-4048(94)90097-3 (http://dx.doi.org/10.1016/0167-4048(94)90097-3)
5. *P. Luo, A. Yu-Lun Lin, Z. Wang, M. Karpovsky.* Hardware Implementation of Secure Shamir's Secret Sharing Scheme (англ.) // HASE '14 Proceedings of the 2014 IEEE 15th International Symposium on High-Assurance Systems Engineering : Proceeding. — Washington, DC, USA: IEEE Computer Society, 2014. — P. 193—200. — ISSN 978-1-4799-3466-9 (https://www.worldcat.org/search?fq=x0:jrnl&q=n2:978-1-4799-3466-9). — DOI:10.1109/HASE.2014.34 (https://dx.doi.org/10.1109%2FHASE.2014.34).
6. *Chia-Chun Wu , Shang-Juh Kao, Wen-Chung Kuo, Min-Shiang Hwang.* Reversible Secret Image Sharing Based on Shamir's Scheme (англ.) // IIH-MSP '09 Proceedings of the 2009 Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing : Proceeding. — Washington, DC, USA: IEEE Computer Society, 2009. — P. 1014—1017. — ISBN 978-0-7695-3762-7. — DOI:10.1109/IIH-MSP.2009.158 (https://dx.doi.org/10.1109%2FIIH-MSP.2009.158).
7. *Ulutas M., Ulutas G., Nabiyev V. V.* Medical image security and EPR hiding using Shamir's secret sharing scheme // *J. Syst. Software* — Elsevier, 2011. — Vol. 84, Iss. 3. — P. 341–353. — ISSN 0164-1212 (https://www.worldcat.org/issn/0164-1212); 1873-1228 (https://www.worldcat.org/issn/1873-1228) — doi:10.1016/J.JSS.2010.11.928 (http://dx.doi.org/10.1016/J.JSS.2010.11.928)
8. *S. Salim, S. Suresh, R. Gokul, Reshma S.* Application of Shamir Secret Sharing Scheme for Secret Data Hiding and Authentication (англ.) // International Journal of Advanced Research in Computer Science & Technology : Journal. — 2014. — Vol. 2, no. 2. — P. 220—224. — ISSN 2347-8446 (https://www.worldcat.org/search?fq=x0:jrnl&q=n2:2347-8446).
9. *Che-Wei Lee, Wen-Hsiang Tsai.* A data hiding method based on information sharing via PNG images for applications of color image authentication and metadata embedding (англ.) // Signal Processing : Journal. — Amsterdam, The Netherlands: Elsevier North-Holland, Inc., 2013. — Vol. 93, no. 7. — P. 2010—2025. — ISSN 0165-1684 (https://www.worldcat.org/search?fq=x0:jrnl&q=n2:0165-1684). — DOI:10.1016/j.sigpro.2013.01.009 (https://dx.doi.org/10.1016%2Fj.sigpro.2013.01.009).
10. *Goubin L., Martinelli A.* Protecting AES with Shamir's Secret Sharing Scheme (http://rd.springer.com/content/pdf/10.1007%2F978-3-642-23951-9_6.pdf) // *Cryptographic Hardware and Embedded Systems — CHES 2011: 13th International Workshop, Nara, Japan, September 28 — October 1, 2011, Proceedings* / B. Preneel, T. Takagi — Springer Science+Business Media, 2011. — P. 79–94. — 524 p. — (Lecture Notes in Computer Science; Vol. 6917) — ISBN 978-3-642-23950-2 — ISSN 0302-9743 (https://www.worldcat.org/issn/0302-9743) — doi:10.1007/978-3-642-23951-9_6 (http://dx.doi.org/10.1007/978-3-642-23951-9_6)
11. *Xiao S., Ling H., Zou F. et al.* Secret Sharing Based Video Watermark Algorithm for Multiuser // *Digital Watermarking: 7th International Workshop, IWDW 2008, Busan, Korea, November 10-12, 2008, Selected Papers* / H. J. Kim, S. Katzenbeisser, Anthony T. S. Ho — Springer Berlin Heidelberg, 2009. — P. 303–312. — 472 p. — (Lecture Notes in Computer Science; Vol. 5450) — ISBN 978-3-642-04437-3 — ISSN 0302-9743 (https://www.worldcat.org/issn/0302-9743) — doi:10.1007/978-3-642-04438-0_26 (http://dx.doi.org/10.1007/978-3-642-04438-0_26)
12. *A. Teoh, D. Ngo, A. Goh.* Personalised cryptographic key generation based on FaceHashing (англ.) // Computers and Security : Journal. — Elsevier Advanced Technology Publications Oxford, 2004. — Vol. 23, no. 7. — P. 606—614. — ISSN 0167-4048 (https://www.worldcat.org/search?fq=x0:jrnl&q=n2:0167-4048). — DOI:10.1016/j.cose.2004.06.002 (https://dx.doi.org/10.1016%2Fj.cose.2004.06.002).

Литература

- *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)
- *Шнайер Б.* 23.2 Алгоритмы разделения секрета. Схема интерполяционных полиномов Лагранжа // Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си = Applied Cryptography. Protocols, Algorithms and Source Code in C. — М.: Триумф, 2002. — С. 588—589. — 816 с. — 3000 экз. — ISBN 5-89392-055-4.
- *Чмора А.Л.* Современная прикладная криптография. — 2-е изд., стер.. — М.: Гелиос АРВ, 2002. — С. 123—124. — 256 с. — ISBN 5-85438-046-3.
- *Под общ. ред. Ященко В.В.* Введение в криптографию. — 2-е изд., испр.. — М.: МЦНМО: «ЧеРо», 1999. — С. 118—125. — 272 с. — ISBN 5-900916-40-5.

Ссылки

ssss: реализация схемы разделения секретов Шамира с интерактивной демонстрацией. (http://point-at-infinity.org/ssss/)