ISSN 2658 – 7505
Выпуск №1, 2019
Электронный научный журнал «Вестник молодёжной науки России»

УДК 519.7

О СИСТЕМЕ РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ НА ОСНОВЕ ДИЗАЙНОВ АДАМАРА

В.М. Деундяк*[1,2], *vl.deundyak@gmail.com*, *А.А. Таран*[1], *fraktal-at@yandex.ru
Южный Федеральный Университет (ЮФУ), г. Ростов-на-Дону
ФГНУ «НИИ «Спецвузавтоматика», г. Ростов-на-Дону

В работе изучается возможность применения дизайнов Адамара к задаче распределения ключей в сообществе для обеспечения безопасности переписки каждой пары членов сообщества. Исследуются построенные на дизайнах Адамара системы предварительного распределения ключей, позволяющие участникам вычислить общие секретные ключи для переписки с помощью предварительно распределенной ключевой информации. Однако, в системах такого типа возможно проведение коалиционных атак на общие секретные ключи, при этом гарантируется безопасность ключей при условии, что мощность коалиции злоумышленников не превышает некоторого фиксированного граничного значения. Для построенных систем исследуется устойчивость к коалиционным атакам в случае превышения предусмотренного значения мощности коалиции. Вычисляются вероятности возможности проведения атаки на общий ключ переписки произвольной пары участников.

Ключевые слова: системы распределения ключей, комбинаторные дизайны, коалиционные атаки.

ON THE KEY DISTRIBUTION SYSTEM BASED ON HADAMARD DESIGNS

***V.M. Deundyak*[1,2], *A.A. Taran*[1]**
Southern Federal University (SFedU), Rostov-on-Don
FSSO «SRI «Spetsvuzavtomatika», Rostov-on-Don

This article discusses the applicability of Hadamard designs to the task of key distribution within a community for secure communication between each pair of users. Key predistribution systems based on Hadamard designs, that allow users to calculate shared secret keys using previously distributed key information, are studied. Collusive attacks on shared secret keys are possible in such systems, but the security of key is guaranteed in case when cardinality of the coalition does not exceed specified threshold. Resilience of these systems to collusive attacks in the case when cardinality of the coalition exceeds this threshold is studied. Probabilities of successful attacks on shared secret key of arbitrary pair of users are calculated.

Keywords: key distribution systems, combinatorial designs, collusive attacks.

Введение

Для обеспечения безопасной передачи данных в сообществе участникам обмена требуется наличие общего секретного ключа. Алгоритмы, с помощью которых эти общие ключи могут быть получены, можно разделить на три группы [1]. В алгоритмах выработки общего секретного ключа, таких как [2], участники обмениваются открытыми ключами по публичным каналам связи и на основе них вычисляют общие секретные ключи. В системах распределения ключей, таких как [3], участники могут получить общий секретный ключ в результате обмена данными с некоторым доверенным сервером. Однако в некоторых случаях обмен данными с другими участниками сообщества или с доверенным сервером может быть невозможен или непрактичен. В таких случаях могут использоваться системы предварительного распределения ключей [4], в которых каждому участнику системы заранее предоставляется некая ключевая информация, на основе которой он затем может независимо от других участников системы вычислить необходимые общие секретные ключи. Однако системы такого типа могут быть подвержены коалиционным атакам: находящиеся в системе злоумышленники могут объединиться в коалицию и получить возможность вычислить

ISSN 2658 – 7505
Выпуск №1, 2019
Электронный научный журнал «Вестник молодёжной науки России»

общие секретные ключи других участников системы с помощью ключевой информации всех членов коалиции.

Примерами систем предварительного распределения ключей являются системы, построенные с помощью шаблонов распределения ключей [5]. В качестве основы для их построения могут использоваться различные комбинаторные структуры [6,7], такие как ортогональные массивы и комбинаторные дизайны [8]. Эти системы гарантируют безопасность ключей при условии, что мощность коалиции злоумышленников не превышает некоторого определяемого конструкцией системы значения. Но т.к. коалиция злоумышленников может сформироваться уже после построения системы, когда максимальное значение допустимой мощности будет зафиксировано, то представляется актуальным исследование безопасности общих секретных ключей пользователей системы в случае превышения этого значения.

В данной работе изучается система распределения ключей, построенная на дизайнах Адамара, и вычисляются вероятности возможности проведения успешной коалиционной атаки в случае, когда мощность коалиции превышает предусмотренное системой значение.

Построение системы

Предположим, что имеется сообщество из $n = 2^a, a > 2$ пользователей. Система распределения ключей в этом сообществе будет строиться на основе шаблонов распределения ключей [5,6], которые определяются следующим образом. Доверенный сервер генерирует множество U из n идентификационных номеров пользователей системы и множество блоков $B = \{B_i\}_{i=1}^{|B|}$, где каждый B_i является подмножеством U. Множества U и B являются открытой информацией и известны всем пользователям системы. Для каждого B_i сервер генерирует ключ k_i из ключевого пространства K. Каждый пользователь системы получает ключ k_i, если соответствующий ему идентификационный номер лежит во множестве B_i. Таким образом, каждый пользователь может получить несколько ключей, и каждый ключ k_i может быть одновременно получен несколькими пользователями системы. Множество ключей k_i, полученных пользователем системы, составляет его приватную ключевую информацию.

Пара (U, B) называется (t, w)-*KDP* (*Key Distribution Pattern*), т.е. шаблоном распределения ключей, обеспечивающим безопасность конференций из t участников при условии наличия в системе коалиции злоумышленников из не более чем w пользователей системы, если выполняются следующие условия: для любой конференции $P \subset U, |P| = t$ множество $B_P = \{B_i \in B : P \subseteq B_i\}$ непусто, т.е. все участники конференции P принадлежат, по крайней мере, одному общему блоку B_i, а значит, имеют, по крайней мере, один общий ключ k_i; для любой конференции $P \subset U, |P| = t$ и для любой коалиции $F \subset U \setminus P, |F| \le w$ множество

$$\{B_i \in B : P \subseteq B_i, F \cap B_i = \varnothing\} \neq \varnothing, \quad (1)$$

т.е. существует, по крайней мере, один блок B_i, в который входят все участники конференции P, но не входит ни один из злоумышленников из коалиции F, а значит, у всех участников коалиции P есть, по крайней мере, один общий ключ k_i, который неизвестен коалиции F. Тогда каждый из участников конференции,

зная U, B и P, может получить множество B_P и соответствующее ему множество ключей $K_P = \{k_i : B_i \in B_P\}$, общих для всех участников конференции, и вычислить общий секретный ключ $k_P = f(K_P)$ конференции P с помощью заранее оговоренной функции f. Если в качестве f использовать такую функцию, для которой нельзя получить никакой информации о ключе k_P, если не известен хотя бы один ключ из множества K_P, то, согласно (1), никакая коалиция $F \subset U \setminus P, |F| \le w$ не сможет вычислить общий секретный ключ k_P. Например, в качестве такой функции может использоваться побитовая сумма всех ключей из множества K_P.

В [6] показано, что в качестве шаблона распределения ключей может использоваться комбинаторный дизайн. v-(n,m,λ)-дизайном называется пара (U,B), где $|U| = n$, $B = \{B_i \subset U\}_{i=1}^{|B|}, |B_i| = m$, для которой выполняется условие, что любые v элемента из U содержатся ровно в λ блоках из B. В [6], с. 223, доказана теорема, что $(t+1)$-(n,m,λ)-дизайн является (t,w)-*KDP* при

$$w < \frac{n-t}{k-t}. \qquad (2)$$

Мы будем рассматривать описанную систему, построенную на 3-$(n, n/2, n/4-1)$-дизайне Адамара, который может быть получен из матрицы Адамара-Сильвестра размера $n \times n$ [8]. Согласно (2), этот дизайн является $(2,2)$-*KDP*, т.е. позволяет обеспечить безопасность переписки пары пользователей системы при наличии коалиций из не более чем двух злоумышленников.

Вычисление вероятностей проведения атак

Для описанной выше системы распределения ключей на 3-дизайнах Адамара было доказано следующее утверждение.

Теорема 1. Коалиция $F \subset U$ может получить общий секретный ключ k_P переписки $P \subset U$ тогда и только тогда, когда у коалиции F имеются все приватные ключи по крайней мере одного из участников P.

Благодаря этой теореме можно свести задачу определения вероятности того, что коалиция сможет вычислить общий секретный ключ конференции, к задаче определения вероятности того, что коалиция получит все приватные ключи какого-то пользователя системы.

Зафиксируем коалицию злоумышленников F мощности $|F|$. Для описанной системы распределения ключей можно показать, что коалиция всегда будет получать все приватные ключи ровно 2^d пользователей системы (включая самих злоумышленников из F) для некоторого целого d. Поэтому рассмотрим вспомогательную систему гипотез $\{H(|F|,d)\}_{d=0}^{a}$, состоящих в том, что коалиция из $|F|$ злоумышленников получила все ключи 2^d пользователей системы. Вероятности наступления гипотез могут быть вычислены рекуррентно по формуле

$$p(H(|F|,d)) = \frac{p(H(|F|-1,d-1)) \cdot (n - 2^{d-1}) + p(H(|F|-1,d) \cdot (2^d - (|F|-1))}{n - (|F|-1)} \qquad (3)$$

со следующими начальными значениями:

$$p(H(1,0)) = 1;\ p(H(r,0)) = 0, r \ne 1;\ p(H(1,d)) = 0, d \ne 0. \qquad (4)$$

Из этих формул, а также из формул гипергеометрического распределения и полной вероятности, вытекает следующее утверждение.

Теорема 2. Рассмотрим $(2,2)$-систему распределения ключей для $n = 2^a$ пользователей, построенную на 3-дизайнах Адамара, полученных из матриц Адамара-Сильвестра. Вероятность события $A(|F|)$, состоящего в том, что коалиция злоумышленников F мощности $|F|$ может вычислить общий секретный ключ произвольной переписки (с учетом тех переписок, в которых один из участников – это член коалиции F) вычисляется по формулам

$$p(A(|F|)) = \sum_{d=0}^{a} p(A(|F|) \mid H(|F|,d)) \cdot p(H(|F|,d)),$$

$$p(A(|F|) \mid H(|F|,d)) = 1 - \frac{C_{n-2^d}^2}{C_n^2},$$

где $p(H(|F|,d))$ вычисляется по формулам (3), (4).

Заключение. В работе на основе применения теории дизайнов построены системы предварительного распределения ключей, позволяющие участникам сообщества вычислять общие секретные ключи для защищенной переписки каждой пары членов сообщества с помощью предварительно распределенной ключевой информации. В системах подобного типа возможны коалиционные атаки на общие секретные ключи, но, несмотря на это, система гарантирует безопасность ключей при условии, что мощность коалиции злоумышленников не превышает некоторого фиксированного граничного значения. Для построенных в работе систем распределения ключей вычислены вероятности возможности проведения атаки на общий ключ переписки произвольной пары участников, что позволяет оценить риски при внедрении представленной системы на практике.

Список цитируемой литературы

1. Martin K.M. The Combinatorics of Cryptographic Key Establishment. // Surveys in Combinatorics, 2007. – pp.223-273
2. Diffie W., Hellman M. New Directions in Cryptography // IEEE Transactions on Information Theory, vol. 22, 1976. – pp.644-654
3. Needham R.M., Schroeder M.D. Using Encryption for Authentication in Large Networks of Computers // Communications of the ACM, vol. 21, 1978. – pp.993-999
4. Matsumoto T., Imai I. On the Key Predistribution Systems: A Practical Solution to the Key Distribution Problem // Advances in Cryptology: CRYPTO'87 (LNCS 293), 1987. – pp.185-193
5. Mitchell C.J., Piper F.C. Key Storage in Secure Networks // Discrete Applied Mathematics, vol. 21, 1988. – pp.215-228
6. Stinson D.R. On Some Methods for Unconditionally Secure Key Distribution and Broadcast Encryption // Designs, Codes and Cryptography, vol. 12, 1997. – pp.215-243
7. Stinson D.R., Trung T.V. Some New Results on Key Distribution Patterns and Broadcast Encryption // Designs, Codes and Cryptography, vol. 14, 1998. – pp.261-279
8. Таранников Ю.В. Комбинаторные свойства дискретных структур и приложения к криптологии. – М.: МЦНМО, 2011. – 152 с.