УДК 621.391:519.7:510.5

Алексейчук А. Н., Конюшок С. Н., Скрыпник Л. В.

БЕЗУСЛОВНО СТОЙКИЕ СХЕМЫ РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ, ПОСТРОЕННЫЕ ПО КОНГРУЭНЦИЯМ УНИВЕРСАЛЬНЫХ АЛГЕБР

Предложена комбинаторная модель схемы предварительного распределения ключей, с использованием которой получено описание таких схем в терминах определенных систем отношений эквивалентности на конечном множестве. Предложен метод построения схем предварительного распределения ключей по системам конгруэнций конечных универсальных алгебр, обобщающий известный способ их синтеза на основе линейных отображений конечных векторных пространств.

Одним из перспективных направлений современной криптографии, активно развивающихся на протяжении последних 15 – 20 лет, является построение криптографически стойких протоколов (схем) распределения ключей в системах защищенной многоадресной связи. Характерная особенность таких систем заключается в наличии большого числа авторизованных абонентов, образующих наделенные различными правами группы (коалиции), состав которых может динамически изменяться [1, 2].

Говоря неформально, схема распределения ключей (СРК) представляет собой криптографический протокол, с ипользованием которого доверенная сторона (центр распределения ключей (ЦРК) или дилер) передает абонентам сети связи некоторую вспомогательную секретную информацию так, что со временем абоненты, входящие в определенную привилегированную коалицию, могут вычислить общий (групповой) ключ. Схема распределения ключей называется безусловно стойкой, если каждая запрещенная (для данной привилегированной) коалиция абонентов не может получить никакой информации об этом ключе даже при наличии неограниченных вычислительных ресурсов [3, 4].

Подробные сведения об известных методах построения, анализа и различных аспектах практического применения СРК можно найти в обзорных работах [3, 5, 6].

Настоящая статья посвящена изучению специального класса безусловно стойких СРК, а именно, схем предварительного распределения ключей (СПРК). Центральной задачей исследования таких схем является разработка конструктивных методов синтеза СПРК, имеющих оптимальные или близкие к оптимальным характеристики эффективности (так называемые информационную скорость и полную информационную скорость) [3 – 7].

В настоящее время конструкции оптимальных СПРК известны лишь для отдельных типов структур спецификаций (совокупностей пар привилегированных и запрещенных коалиций участников схемы) [3, 7]. При этом, несмотря на разнообразие конкретных видов СПРК, общая теория построения и анализа схем предварительного распределения ключей для произвольных структур спецификаций находится в состоянии становления. Отметим статью [7], в которой предложена конструкция так называемых линейных СПРК, включающих в себя большинство известных видов схем предварительного распределения ключей.

В настоящей статье предложена комбинаторная модель СПРК, позволяющая, по мнению авторов, более наглядно и, практически, без потери общности выразить существенные свойства произвольной схемы предварительного распределения ключей. С использованием данной модели получено формальное описание СПРК в терминах определенных систем отношений эквивалентности (ОЭ) на конечном множестве.

Предложен метод построения СПРК по системам конгруэнций конечных универсальных алгебр, обобщающий конструкцию линейных схем предварительного распределения ключей [7]. Отметим, что решения аналогичных задач для другого класса протоколов распределения ключей (так называемых совершенных схем разделения секрета) получены ранее в [8].

Далее в статье свободно используются понятия универсальной алгебры, определения которых можно найти в [9, 10]. Более подробная информация о схемах предварительного распределения ключей приведена в [3 – 5, 7].

Перейдем к изложению основных результатов статьи.

Пусть $V=\{1,2,..,v\}$ – множество абонентов сети связи, $\Gamma\subseteq 2^V\times 2^V$ – структура спецификации на множестве V [7]. Обозначим $\Re(\Gamma) = \{P\subseteq V\,|\,\exists C\subseteq V:(P,C)\in\Gamma\}$ совокупность Γ-привилегированных коалиций абонентов. Для любого $P\in\Re(\Gamma)$ обозначим $\Im_\Gamma(P) = \{C\subseteq V\,|\,(P,C)\in\Gamma\}$ множество всех P-запрещенных коалиций абонентов. Отметим, что $\Im_\Gamma(P)$ является монотонно невозрастающим классом множеств, каждое из которых не пересекается с P.

Опишем предлагаемую комбинаторную модель схемы предварительного распределения ключей со структурой спецификации Γ (Γ-СПРК).

Пусть U, $U_1,...,U_v$ – конечные множества, где $U\subseteq U_1\times...\times U_v$. Пусть, далее, для любого $P\in\Re(\Gamma)$ задано конечное множество K_P такое, что $|K_P|\geq 2$, и сюръективное отображение $\varphi_P: U\to K_P$. Будем говорить, что набор $D=(U,(U_i)_{i\in V},(K_P,\varphi_P)_{P\in\Re(\Gamma)})$ задает Γ-СПРК на множестве V, если выполняются следующие условия:

$$\forall P\in\Re(\Gamma)\ \forall i\in P\ \forall u=(u_1,...,u_v),\ \tilde{u}=(\tilde{u}_1,...,\tilde{u}_v)\in U:\ (u_i=\tilde{u}_i)\Rightarrow(\varphi_P(u)=\varphi_P(\tilde{u}))\,, \quad (1)$$

$$\forall (P,C)\in\Gamma:\ |\{(u_C,\varphi_P(u)):u\in U\}| = |\{u_C:u\in U\}|\cdot|\{\varphi_P(u):u\in U\}|\,, \quad (2)$$

где u_C обозначает подвектор вектора u с координатами, номера которых принадлежат множеству C.

Для любых $i\in V$, $P\in\Re(\Gamma)$ множества U_i и K_P называются соответственно множеством вспомогательных секретных данных i-го абонента и множеством групповых ключей коалиции P.

Протокол распределения ключей абонентам из множества V с использованием заданной СПРК D описывается следующим образом. На первом этапе в ЦРК случайно и равновероятно выбирают элемент $u=(u_1,...,u_v)\in U$ и передают каждому абоненту $i\in V$ значение u_i по защищенному каналу связи. На втором этапе, согласно условию (1), каждый участник произвольной привилегированной коалиции P может однозначно вычислить групповой ключ $k_P=\varphi_P(u)$. При этом на основании равенства (2) участники произвольной P-запрещенной коалиции $C\in\Im_\Gamma(P)$ не получат никакой (апостериорной) информации об этом ключе.

Стандартными показателями эффективности СПРК D являются ее информационная скорость ρ и полная информационная скорость ρ_T [3, 4, 7], которые, в рассматриваемом случае, определяются по формулам

$$\rho=\min\{\frac{\log|K_P|}{\log|U_i|}:i\in P,P\in\Re(\Gamma)\}\,, \quad (3)$$

$$\rho_T = \min\{\frac{\log|K_P|}{\log|U|} : P \in \Re(\Gamma)\}. \quad (4)$$

Отметим, что данное выше формальное определение является переложением на комбинаторный язык (без существенной потери общности) общепринятого вероятностного определения схемы предварительного распределения ключей (см., например, [3, 4, 7]).

Покажем, что произвольная Γ-СПРК может быть, по существу, однозначно задана определенной системой отношений эквивалентности на конечном множестве.

Обозначим $\Im(U)$ решетку отношений эквивалентности на множестве U. Символы $\bullet$, $\vee$ и $\wedge$ обозначают соответственно произведение, точную верхнюю грань и точную нижнюю грань (пересечение) ОЭ на множестве U [9]. Каждое ОЭ $\pi \in \Im(U)$ отождествляется с фактормножеством (разбиением) U/π, число элементов (блоков) которого обозначается $n(\pi)$. Символ 1_U обозначает наибольший элемент решетки $\Im(U)$, равный U^2.

Справедливо следующее утверждение.

Утверждение 1. Тогда и только тогда существует Γ-СПРК на множестве V, имеющая информационную скорость (3) и полную информационную скорость (4), когда существуют конечное множество U и система ОЭ π_i, $\theta_P \in \Im(U)$, $i \in V$, $P \in \Re(\Gamma)$, которые удовлетворяют следующим соотношениям:

$$\bigvee_{i \in P} \pi_i \subseteq \theta_P \neq 1_U, \ P \in \Re(\Gamma), \quad (5)$$

$$(\bigwedge_{j \in C} \pi_j) \bullet \theta_P = 1_U, \ (P, C) \in \Gamma, \quad (6)$$

$$\rho = \min\{\frac{\log n(\theta_P)}{\log n(\pi_i)} : i \in P, P \in \Re(\Gamma)\}, \quad (7)$$

$$\rho_T = \min\{\frac{\log n(\theta_P)}{\log|U|} : P \in \Re(\Gamma)\}. \quad (8)$$

Сформулированное утверждение доказывается аналогично утверждению 1 в статье [8]. Отметим, что для заданной Γ-СПРК $D = (U, (U_i)_{i \in V}, (K_P, \varphi_P)_{P \in \Re(\Gamma)})$ ОЭ π_i, θ_P можно определить по формулам $\pi_i = \mathrm{Ker}(pr_i)$, $i \in V$, $\theta_P = \mathrm{Ker}(\varphi_P)$, $P \in \Re(\Gamma)$, где $pr_i : U \to U_i$ – проекция множества U на множество U_i, $\mathrm{Ker}(f)$ – ядро произвольного отображения f (см. [9]). При этом соотношение (5) равносильно условию (1) и неравенству $|K_P| \geq 2$, $P \in \Re(\Gamma)$, а соотношения (6), (7) и (8) равносильны соотношениям (2), (3) и (4) соответственно.

Полученное утверждение позволяет предложить общий метод построения СПРК, исходя из определенных наборов конгруэнций конечных универсальных алгебр. Сущность метода раскрывается в формулировках следующих результатов.

Пусть Γ – произвольная структура спецификации на множестве V. Обозначим $\Im_{\max}(P)$ множество всех максимальных элементов класса $\Im_\Gamma(P)$. Будем говорить, что

система ОЭ $\pi_1,\ldots,\pi_v \in \mathfrak{I}(U)$ порождает Γ-СПРК на множестве V, если существуют отношения $\theta_P \in \mathfrak{I}(U)$, $P \in \mathfrak{R}(\Gamma)$, удовлетворяющие условиям (5), (6).

Утверждение 2. Система ОЭ $\pi_1,\ldots,\pi_v \in \mathfrak{I}(U)$ порождает некоторую Γ-СПРК на множестве V в том и только в том случае, когда существует подрешетка $\mathfrak{I}$ решетки $\mathfrak{I}(U)$, содержащая отношения $\pi_1,\ldots,\pi_v$, и для любого $P \in \mathfrak{R}(\Gamma)$ существует максимальный элемент μ_P решетки $\mathfrak{I}$ такой, что

$$\bigvee_{i\in P}\pi_i \subseteq \mu_P,\ \bigwedge_{j\in C}\pi_j \not\subset \mu_P,\ (\bigwedge_{j\in C}\pi_j)\bullet\mu_P = \mu_P\bullet(\bigwedge_{j\in C}\pi_j),\ C \in \Im_{\max}(P). \tag{9}$$

Справедливость утверждения 2 вытекает из предыдущего утверждения и известного критерия перестановочности отношений эквивалентности на множестве U (см. [9], стр. 104).

Рассмотрим теперь конечную универсальную алгебру A с носителем U. Обозначим $\mathfrak{I}_A(U)$ подрешетку решетки $\mathfrak{I}(U)$, состоящую из всех конгруэнций алгебры A [9, 10]. Напомним, что A называется конгруэнц-перестановочной алгеброй, если для любых $\pi_1, \pi_2 \in \mathfrak{I}_A(U)$ выполняется равенство $\pi_1 \bullet \pi_2 = \pi_2 \bullet \pi_1$.

Непосредственно из утверждения 2 вытекает следующий результат.

Утверждение 3. Пусть $\pi_1,\ldots,\pi_v \in \mathfrak{I}_A(U)$ – различные конгруэнции конечной конгруэнц-перестановочной алгебры A. Пусть, далее, Γ – структура спецификации на множестве V такая, что для любого $P \in \mathfrak{R}(\Gamma)$ существует максимальная конгруэнция алгебры A, содержащая конгруэнцию $\bigvee_{i\in P}\pi_i$ и не содержащая конгруэнцию $\bigwedge_{j\in C}\pi_j$ для любого $C \in \Im_{\max}(P)$. Тогда ОЭ $\pi_1,\ldots,\pi_v$ порождают Γ-СПРК на множестве V, информационная скорость ρ и полная информационная скорость ρ_T которой удовлетворяют неравенствам

$$\rho \ge \left(\max\{\log n(\pi_i) : i \in V\}\right)^{-1},\ \rho_T \ge \left(\log|U|\right)^{-1}. \tag{10}$$

В качестве одного из возможных применений утверждения 3, рассмотрим следующую конструкцию СПРК, основанную на подпространствах n-мерного векторного пространства U над полем из q элементов.

Пусть $V_1,\ldots,V_v$ – все k-мерные подпространства векторного пространства U, $2 \le k \le n-2$, $n \ge 4$. Обозначим $M_1,\ldots,M_m$ и $L_1,\ldots,L_m$ соответственно все максимальные и все минимальные подпространства пространства U. Справедливы равенства [11]

$$v = \frac{(q^n-1)\cdots(q^{n-k+1}-1)}{(q^k-1)\cdots(q-1)},\ m = \frac{q^n-1}{q-1}.$$

Построим СПРК $D_{n,k}$ на множестве участников $V = \{V_1,\ldots,V_v\}$ со структурой спецификации Γ следующего вида:

$$\mathfrak{R}(\Gamma) = \{P_1,\ldots,P_m\},\ \Im_{\max}(P_i) = \{C_i(L_s) \mid L_s \cap M_i = 0,\ s \in \overline{1,m}\},\ i \in \overline{1,m},$$

где

$$P_i = \{V_l \mid V_l \subseteq M_i,\ l \in \overline{1,\nu}\},\ C_i(L_s) = \{V_l \mid V_l \supseteq L_s,\ l \in \overline{1,\nu}\},\ i,s \in \overline{1,m}.$$

Другими словами, для любой пары подпространств (M_i, L_s) таких, что $L_s \cap M_i = 0$, определим привилегированную коалицию P_i как множество всех k-мерных подпространств V_l, $l \in \overline{1,\nu}$, сумма которых равна M_i, и максимальную P_i-запрещенную коалицию $C_i(L_s)$ как множество всех k-мерных подпространств V_l, $l \in \overline{1,\nu}$, пересечение которых равно L_s, $i,s \in \overline{1,m}$.

Ясно, что все максимальные запрещенные коалиции СПРК $D_{n,k}$ имеют одинаковую мощность

$$\nu\left(\frac{q^k-1}{q^n-1}\right) = \frac{(q^{n-1}-1)\cdots(q^{n-k+1}-1)}{(q^{k-1}-1)\cdots(q-1)}. \qquad (11)$$

При этом для любой привилегированной коалиции $P_i \in \Re(\Gamma)$ существует ровно q^{n-1} максимальных запрещенных коалиций.

Информационная скорость ρ и полная информационная скорость ρ_T СПРК $D_{n,k}$ определяются по формулам $\rho = (n-k)^{-1}$, $\rho_T = n^{-1}$. По существу это означает, что для формирования группового ключа $k_{P_i} \in \mathbf{GF}(q)$ произвольной привилегированной коалиции P_i, $i \in \overline{1,m}$, на первом этапе протокола распределения ключей потребуется сгенерировать ровно n секретных значений, принадлежащих полю $\mathbf{GF}(q)$. При этом каждый абонент будет хнанить в сектрете $n-k$ элементов данного поля. На втором этапе абоненты произвольной привилегированной коалиции смогут вычислить групповой ключ, секретный для любой из q^{n-1} максимальных запрещенных коалиций абонентов, каждая из которых имеет мощность (11).

В целом, полученные результаты позволяют строить разнообразные схемы предварительного распределения ключей, исходя из определенных систем ОЭ на конечных множествах, в частности, систем конгруэнций конечных конгруэнц-перестановочных алгебр (луп, ассоциативных колец, модулей над кольцом с единицей, векторных пространств над полем и др. [10]). В частном случае, когда алгебра A является векторным пространством, схемы распределения ключей, описанные в формулировке утверждения 3, совпадают с линейными СПРК, предложенными ранее в [7]. Разнообразие и особенности строения конкретных классов конечных универсальных алгебр свидетельствуют о возможности синтеза новых видов схем предварительного распределения ключей, имеющих практически удовлетворительные характеристики эффективности.

Список литературы

1. Canetti R., Malkin T., Nissim K. Effcient communication-storage tradeoffs for multicast encryption // Advances in Cryptology – EUROCRYPT'99, Lecture Notes in Computer Science. – 1999. – P. 459 – 474.
2. Canetti R., Garay J., Itkis G., Micciancio D., Naor M., Pinkas B. Issue in multicast security: a taxonomy and efficient constructions // INFOCOM'99. – 1999. – P. 708 – 716.
3. Stinson D.R. On some methods for unconditionally secure key distribution and broadcast encryption // Designs, Codes and Cryptography. – 1997. – Vol. 12. – P. 215 – 243.

4. Stinson D.R., van Trung T. Some new results on key distribution patterns and broadcast encryption // Designs, Codes and Cryptography. – 1998. – Vol. 15. – P. 261 – 279.
5. Конюшок С.М., Олексійчук А.М. Безумовно стійки схеми розподілу ключів в інформаційних та телекомунікаційних системах з великою кількістю абонентів: I. Схеми попереднього розподілу й узгодження ключів // Прикладная радиоэлектроника. – 2006. – Т. 5. – № 1. – С. 83 – 93.
6. Конюшок С.М., Олексійчук А.М. Безумовно стійки схеми розподілу ключів в інформаційних та телекомунікаційних системах з великою кількістю абонентів: II. Схеми багатоадресного розподілу ключів // Прикладная радиоэлектроника. – 2006. – Т. 5. – № 1. – С. 94 – 104.
7. Padro C., Gracio I., Martin S., Morillo P. Linear key predistribution schemes // Designs, Codes and Cryptography. – 2002. – Vol. 25. – P. 281 – 298.
8. Алексейчук А.Н. Схемы разделения секрета и конечные универсальные алгебры // Реєстрація, зберігання і обробка даних, 2005. – Т. 7. – № 2. – С. 55 – 65.
9. Кон П. Универсальная алгебра / Пер. с англ. – М.: Мир, 1968. – 351 с.
10. Биркгоф Г. Теория решеток / Пер. с англ. – М.: Наука, 1984. – 568 с.
11. Сачков В.Н. Введение в комбинаторные методы дискретной математики. – М.: Наука, 1982. – 384 с.