УДК 004.056.5

АЛГОРИТМ ПРОВЕРКИ ПОДЛИННОСТИ ПОЛЬЗОВАТЕЛЯ, ОСНОВАННЫЙ НА ГРАФИЧЕСКИХ КЛЮЧАХ

А. В. Мазуренко, Н. С. Архангельская, Н. В. Болдырихин

Донской государственный технический университет, Ростов-на-Дону, Российская Федерация

mazurencoal@gmail.com
arh.iv@bk.ru
boldyrikhin@mail.ru

В данной работе представлен алгоритм проверки подлинности пользователя, основанный на построении системы путей в Евклидовом пространстве размерности два. Описанный алгоритм базируется на идее создания графического пароля для обеспечения защиты данных пользователя от несанкционированного доступа. Дана оценка стойкости построенной системы ко взлому путем полного перебора. Приведены подробные примеры реализации описанного алгоритма.

Ключевые слова: графический пароль, распознавание пользователя, Евклидово пространство.

UDC 004.056.5

USER AUTHENTICATION ALGORITHM BASED ON PATTERN LOCKS

A. V. Mazurenko, N. S. Arkhangelskaya, N. V. Boldyrikhin

Don State Technical University, Rostov-on-Don, Russian Federation

mazurencoal@gmail.com
arh.iv@bk.ru
boldyrikhin@mail.ru

This paper details with the user authentication algorithm based on creation of system of paths in two-dimensional Euclidean space. The described algorithm is based on generation of the unlock patterns, which are used to protect user's data from malefactor. The article gives the estimation of resistance to cracking by exhaustive search of constructed system. The paper provides detailed examples of the implementation of the described algorithm.

Keywords: Pattern lock, user authentication, Euclidian space.

Введение. Графический ключ (пароль) — довольно распространенный способ блокировки современных гаджетов. Основное его назначение — исключить несанкционированный доступ злоумышленника к защищаемой информации пользователя [1]. Таким образом, электронное устройство и графический ключ можно рассматривать как систему проверки подлинности пользователя для доступа к ресурсам.

Постановка задачи. На данный момент существует множество аппаратных способов обхода и сброса графического пароля при рассмотрении его как приложения для операционной системы Android [2, 3, 4]. Пользователи часто выбирают удобные, но ненадежные пароли, подобрать которые злоумышленнику не составляет труда [5]. При использовании графической комбинации знаков размер поля для ввода, как правило, является фиксированным, что также ограничивает возможности выбора наиболее безопасного пароля. Итак, необходимо усложнить злоумышленнику задачу и добиться повышения защищенности информации пользователя.

Решение. Рассмотрим графический ключ как математический объект. Предположим, что размер поля для введения графического ключа не фиксирован и его выбирает пользователь.

Рассмотрим решетку L в Евклидовом пространстве $\mathbb{Z}^2$, ортогональным базисом которой служат векторы $e_1 = (1,0)$ и $e_2 = (0,1)$. Путем от точки P_1 до точки P_k в L назовем упорядоченное множество точек $P = \{P_1, P_2, \dots, P_k\}$.

Назовем горизонтальную прямую, соединяющую точки (i,j) и $(i+1,j)$, горизонтальным единичным шагом. Назовем вертикальную прямую, соединяющую точки (i,j) и $(i,j+1)$, вертикальным единичным шагом.

Пусть $L(m,n) = \{(i,j) \in \mathbb{Z}^2 | 0 \le i \le m, 0 \le j \le n\}$, где $m,n \in \mathbb{Z}_+$.

Пример.

$$L(4,3) = \{(0,0),(0,1),(0,2),(0,3),(1,0),(1,1),(1,2),(1,3),$$
$$(2,0),(2,1),(2,2),(2,3),(3,0),(3,1),(3,2),(3,3),(4,0),(4,1),(4,2),(4,3)\}.$$

На рис. 1 изображены пути $P_1 = \{(1,0),(1,1),(2,1),(2,2),(3,2),(3,3)\}$, $P_2 = \{(1,2),(1,3),(2,3)\}$ и $P_3 = \{(3,1),(4,1),(4,2),(4,3)\}$.

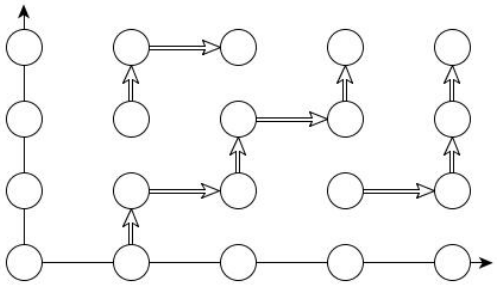

Рис. 1. Пути P_1, P_2 и P_3в $L(4,3)$

Далее под путями будут подразумеваться пути, состоящие из горизонтальных и вертикальных единичных шагов.

Теорема 1. Количество путей в $L(m,n)$ равно

$P_1(m,n) = \sum_{i=0}^{m}\sum_{j=0}^{n} W(i,j,m,n)$, где $W(k,l,m,n) = \sum_{i=k}^{m}\sum_{j=l}^{n}\binom{i+j-k-l}{j-l}$

при $0 \le k \le m$, $0 \le l \le n$.

Доказательство. Количество путей от точки (k,l) до точки(r,s), где $0 \le k \le r$, $0 \le l \le s$ равно $\binom{r+s-k-l}{s-l}$. Тогда количество путей от точки (k,l) до всех остальных точек, лежащих в $L(m,n)$, равно $W(k,l,m,n) = \sum_{i=k}^{m}\sum_{j=l}^{n}\binom{i+j-k-l}{j-l}$. Таким образом, общее количество путей в $L(m,n)$ равно $P_1(m,n) = \sum_{i=0}^{m}\sum_{j=0}^{n} W(i,j,m,n)$.

Пример.

Количество путей в $L(4,3)$ равно

$$P_1(4,3) = \sum_{i=0}^{4}\sum_{j=0}^{3} W(i,j,4,3) = 125 + 55 + 20 + 5 + 69 + 34 + 14 + 4+$$
$$+34 + 19 + 9 + 3 + 14 + 9 + 5 + 2 + 4 + 3 + 2 + 1 = 431.$$

Пусть $\underline{R_k(\alpha,\beta;\gamma,\delta) = (R_1,R_2,\dots,R_k)}$ — набор k различных путей, где $\alpha,\beta,\gamma,\delta \in$ $\in \mathbb{Z}_+^n$, если R_i путь от (α_i,β_i) к (γ_i,δ_i) при $\alpha_i \le \gamma_i$, $\beta_i \le \delta_i$.

Очевидно, что при рассмотрении путей в $L(n,m)$ должно выполняться условие $k \le (n+1)(m+1)$.

Пусть $S^h_{L(m,n)}$ — множество всех h-подмножеств $L(m,n)$, где $h \in \mathbb{N}$.

Теорема 2. Количество путей в $L(m,n)$ вида $R_k(\alpha,\beta;\gamma,\delta)$ для фиксированного $k \in \mathbb{N}$, равно:

$$P_k(m,n)=\sum_{\{(\alpha_1,\beta_1),(\alpha_2,\beta_2),\dots,(\alpha_k,\beta_k)\}\subseteq S^k_{L(m,n)}}\ \sum_{\substack{\alpha_1\le\gamma_1\le m,\alpha_2\le\gamma_2\le m,\dots,\alpha_k\le\gamma_k\le m,\\ \beta_1\le\delta_1\le n,\beta_2\le\delta_2\le n,\dots,\beta_k\le\delta_k\le n}}\ \prod_{i=1}^{k}\binom{\gamma_i+\delta_i-\alpha_i-\beta_i}{\delta_i-\beta_i} \quad (1)$$

Доказательство. Рассмотрим $R_k(\alpha,\beta;\gamma,\delta)$ для некоторых фиксированных $\alpha,\beta,\gamma,\delta\in\mathbb{Z}_+^2$. Тогда $|R_k(\alpha,\beta;\gamma,\delta)|=\prod_{i=1}^{k}\binom{\gamma_i+\delta_i-\alpha_i-\beta_i}{\delta_i-\beta_i}$. Таким образом,

$$P_k(m,n)=\sum_{\{(\alpha_1,\beta_1),(\alpha_2,\beta_2),\dots,(\alpha_k,\beta_k)\}\subseteq S^k_{L(m,n)}}\ \sum_{\substack{\alpha_1\le\gamma_1\le m,\alpha_2\le\gamma_2\le m,\dots,\alpha_k\le\gamma_k\le m,\\ \beta_1\le\delta_1\le n,\beta_2\le\delta_2\le n,\dots,\beta_k\le\delta_k\le n}}|R_k(\alpha,\beta;\gamma,\delta)|=$$

$$=\sum_{\{(\alpha_1,\beta_1),(\alpha_2,\beta_2),\dots,(\alpha_k,\beta_k)\}\subseteq S^k_{L(m,n)}}\ \sum_{\substack{\alpha_1\le\gamma_1\le m,\alpha_2\le\gamma_2\le m,\dots,\alpha_k\le\gamma_k\le m,\\ \beta_1\le\delta_1\le n,\beta_2\le\delta_2\le n,\dots,\beta_k\le\delta_k\le n}}\ \prod_{i=1}^{k}\binom{\gamma_i+\delta_i-\alpha_i-\beta_i}{\delta_i-\beta_i}.$$

Пример. Найдем количество путей, лежащих в $L(3,2)$. Согласно формуле (1),

$$P_1\big(L(3,2)\big)=105,\ P_2\big(L(3,2)\big)=4579,\ P_3\big(L(3,2)\big)=57076,\ P_4\big(L(3,2)\big)=$$
$$=295149,\ P_5\big(L(3,2)\big)=738269,\ P_6\big(L(3,2)\big)=966261,\ P_7\big(L(3,2)\big)=673153,\ P_8\big(L(3,2)\big)=$$
$$247324,\ P_9\big(L(3,2)\big)=47187,\ P_{10}\big(L(3,2)\big)=4290,\ P_{11}\big(L(3,2)\big)=143 \text{ и } P_{12}\big(L(3,2)\big)=1.$$

Зададим вероятностное пространство $(\Omega,\mathcal{A},\mathrm{P})$, где

$$\Omega=\left\{R_k(\alpha,\beta;\gamma,\delta)\subseteq 2^{2^{L(m,n)}}\,|\,k\in\mathbb{N},\alpha,\beta,\gamma,\delta\in\mathbb{Z}_+^k,\alpha\le\gamma,\beta\le\delta\right\},\ \mathcal{A}=\{A|A\subseteq\Omega\}$$

и $\mathrm{P}=\{P(A)=D/N|A\in\mathcal{A}\}$, D — число элементарных событий, составляющих A, N — число точек Ω.

Ключ пользователя K представляет собой некоторое множество

$$K\in\left\{R_k(\alpha,\beta;\gamma,\delta)\subseteq 2^{2^{L(m,n)}}\,|\,k\in\mathbb{N},\alpha,\beta,\gamma,\delta\in\mathbb{Z}_+^k,\alpha\le\gamma,\beta\le\delta\right\}.$$

Пусть $c\in\mathbb{N}$ — число попыток построения верного K.

Теорема 3. Пусть $K\in\left\{R_k(\alpha,\beta;\gamma,\delta)\subseteq 2^{2^{L(m,n)}}\,|\,k\in\mathbb{N},\alpha,\beta,\gamma,\delta\in\mathbb{Z}_+^k,\alpha\le\gamma,\beta\le\delta\right\}$. Тогда вероятность $p(K)$ — построения верного ключа аутентификации K злоумышленником равна

$$p(K)=\frac{c}{\sum_{k=1}^{(n+1)(m+1)}P_k(m,n)}.$$

Доказательство. Поскольку у злоумышленника есть c попыток построить ключ K, то из формулы (1) следует

$$p(K)=\frac{c}{\sum_{k=1}^{(n+1)(m+1)}P_k(m,n)}. \quad (2)$$

Пример. Рассмотрим пути, лежащие в $L(3,2)$. Пусть

$K=\{\{(0,1),(1,1),(2,2),(2,3)\},\{(3,1),(3,2)\},\{(0,0),(0,1),(0,2)\},\{(1,2)\}\}$.

На рис. 2 изображен K.

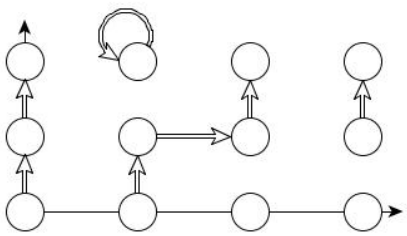

Рис. 2. Ключ K

Пусть $c=30$. Тогда из формулы (2) следует, что

$$p(K)=\frac{30}{105+4579+57076+295149+738269+966261+673153+247324+47187+4290+143+1}=$$
$$=\frac{30}{3033537}\approx 9{,}889*10^{-6}.$$

Выводы. Таким образом, приведен алгоритм проверки подлинности пользователя, основанный на построении системы путей в Евклидовом пространстве размерности два. Представленный алгоритм базируется на создании графического пароля для обеспечения защиты данных пользователя от несанкционированного доступа. Приведена оценка стойкости алгоритма проверки подлинности ко взлому путем полного перебора. Удалось добиться повышения защищенности информации пользователя при использовании графических ключей.

Библиографический список

1. Рябко, Б. Я. Криптографические методы защиты информации / Б. Я. Рябко, А. Н. Фионов. — 2-е изд. — Москва : Горячая линия — Телеком, 2013. — 229 с.

2. Молдовян, А. А. Криптография / А. А. Молдовян, Н. А. Молдовян, Б. Я. Советов. — Санкт-Петербург : Лань, 2000. — 227 с.

3. Рябко, Б. Я. Основы современной криптографии для специалистов в информационных технологиях / Б .Я. Рябко, А. Н. Фионов. — Москва : Научный мир, 2004. — 285 с.

4. Бабаш, А. В. История криптографии. Часть I / А. В. Бабаш, Г. П. Шанкин. — Москва : Гелиос АРВ, 2002. — 240 с.

5. Романец, Ю. В. Защита информации в компьютерных системах и сетях / Ю. В. Романец, П. А. Тимофеев, В. Ф. Шаньгин. — Москва : Радио и связь, 1999. — 230 с.