А. Ф. Ронжин, Расширения информационных протоколов, основанных на отображениях конечных множеств, *Дискрет. матем.*, 2005, том 17, выпуск 4, 18–28

DOI: 10.4213/dm126

Дискретная математика

том 17 выпуск 4 * 2005

УДК 519.7

Расширения информационных протоколов, основанных на отображениях конечных множеств

© 2005 г. А. Ф. Ронжин

Вводятся понятия информационного протокола на конечном множестве, его расширения и разложения. Приводятся примеры махинаций злоумышленника с информационными протоколами. Предлагается система защиты информационных протоколов, допускающих разложение на большое количество расширений, и вычисляются некоторые вероятностные характеристики ее качества.

1. Определения и основные свойства

Зафиксируем конечное непустое множество S. Пусть $C(S)$ — множество всех отображений множества S в себя. Далее всюду полагаем, что $\varnothing$ — пустое множество, для любого подмножества $X \subset S$ и отношения $\rho \in C(S)$ запись $|X|$ обозначает мощность множества X, $\rho(X)$ и $\rho^{-1}(X)$ — образ и прообраз множества X, соответственно.

Пару отображений (φ, ψ), где $\varphi, \psi \in C(S)$, будем называть информационным протоколом на S (далее всюду протоколом). Протокол (φ, ψ) будем называть прозрачным, если $|\varphi(S)| = |\psi(\varphi(S))|$, и мутным, если $|\varphi(S)| > |\psi(\varphi(S))|$.

Протокол (φ_r, ψ_r) будем называть расширением протокола (φ, ψ), если

$$\varphi_r(S) \subset \varphi(S), \tag{1}$$

$$\psi(\varphi_r(s)) = \psi(\varphi(s)) \text{ для всех } s \in S. \tag{2}$$

Расширение (φ_r, ψ_r) протокола (φ, ψ) будем называть строгим, если

$$|\psi_r(\varphi_r(S))| = |\psi(\varphi(S))|,$$

и противоречивым, если

$$|\psi_r(\varphi_r(S))| > |\psi(\varphi(S))|. \tag{3}$$

Из соотношений (1) и (2) следует, что для расширения (φ_r, ψ_r) справедливы неравенства

$$|S| \geqslant |\varphi(S)| \geqslant |(\varphi_r(S))| \geqslant |\psi(\varphi(S))| \geqslant 1. \tag{4}$$

Для противоречивого расширения из (3) и (4) следует, что

$$|S| \geqslant |\varphi(S)| \geqslant |(\varphi_r(S))| \geqslant |\psi_r(\varphi_r(S))| > |\psi(\varphi(S))| \geqslant 1. \tag{5}$$

Семейство расширений протокола (φ, ψ)

$$R(\varphi, \psi) = \{(\varphi_r, \psi_r),\ r \in R\},$$

где R — конечное множество, назовем разложением протокола (φ, ψ), если

$$\varphi(S) = \bigcup_{r \in R} \varphi_r(S), \quad \varphi_{r_1}(S) \cap \varphi_{r_2}(S) = \varnothing, \quad r_1 \neq r_2. \tag{6}$$

Разложение $R(\varphi, \psi)$ назовем регулярным, если $|\varphi_r(S)| = |\psi(\varphi(S))|$ для всех $r \in R$.

Кроме того, пусть ξ — некоторая случайная величина с значениями на S, вероятностями $\mathbf{P}\{\xi = s\} > 0$, $s \in S$, и

$$\mathbf{P}_{\varphi,\psi}(x, y) = \mathbf{P}_{\varphi,\psi}\{\varphi(\xi) = x,\ \psi(\varphi(\xi)) = y\}$$

— совместное распределение пары случайных величин $(\varphi(\xi), \psi(\varphi(\xi)))$, $x \in \varphi(S)$, $y \in \psi(\varphi(S))$. Очевидно, что $\mathbf{P}_{\varphi,\psi}(x, y) = \mathbf{P}\{\varphi(\xi) \in \varphi^{-1}(x)\}$, если $y = \psi(x)$, и 0 в противном случае.

По аналогии с [1] введем обозначения

$$\mathbf{P}_{\psi}(y) = \sum_{x \in \varphi(S)} \mathbf{P}_{\varphi,\psi}(x, y),$$

$$\mathbf{P}_{\psi}(x) = \sum_{y \in \psi(\varphi(S))} \mathbf{P}_{\varphi,\psi}(x, y),$$

и определим среднюю взаимную информацию протокола (φ, ψ) как величину

$$\mathbf{I}(\varphi, \psi) = \sum_{x,y} \mathbf{P}_{\varphi,\psi}(x, y) \ln(\mathbf{P}_{\varphi,\psi}(x, y)/\mathbf{P}_{\psi}(y)\mathbf{P}_{\varphi}(x)).$$

Вычисления показывают, что

$$\mathbf{P}_{\varphi}(x) = \mathbf{P}\{\varphi(\xi) = x\}, \qquad \mathbf{P}_{\psi}(y) = \mathbf{P}\{\psi(\varphi(\xi)) = y\}$$

и

$$\mathbf{I}(\varphi, \psi) = -\sum_{y \in \psi(\varphi(S))} \mathbf{P}_{\psi}(y) \ln \mathbf{P}_{\psi}(y). \tag{7}$$

Для $\mathbf{I}(\varphi, \psi)$ справедливы неравенства

$$0 \leqslant \mathbf{I}(\varphi, \psi) \leqslant -\sum_{x \in \varphi(S)} \mathbf{P}\{\varphi(\xi) = x\} \ln \mathbf{P}\{\varphi(\xi) = x\}, \tag{8}$$

причем слева равенство достигается тогда и только тогда, когда

$$|\psi(\varphi(S))| = 1,$$

а равенство справа тогда и только тогда, когда протокол (φ, ψ) прозрачный.

Теорема 1 (теорема расширения). *Протокол (φ, ψ) имеет противоречивое расширение (φ_r, ψ_r) тогда и только тогда, когда он мутный. При этом существует его расширение (φ_r, ψ_r) такое, что средняя взаимная информация $\mathbf{I}(\varphi, \psi)$ меньше средней взаимной информации этого расширения $\mathbf{I}(\varphi_r, \psi_r)$.*

Доказательство. Необходимость условий утверждения следует из соотношений (5).

Докажем достаточность. Пусть протокол (φ, ψ) является мутным. Существуют $y_1, y_2, \ldots, y_k \in \varphi(S)$, где $k \geqslant 2$, такие, что $\psi(y_1) = \ldots = \psi(y_k) = z_1$, и существуют $z_2, \ldots, z_k \in \varphi(S) \setminus \psi(\varphi(S))$. Пусть $\psi_r(y_j) = z_j$ для всех $j = 1, \ldots, k$, и $\psi_r(s) = \psi(s)$, если $s \in S \setminus \{y_1, \ldots, y_k\}$.

Очевидно, что

$$|\psi_r(\varphi_r(S))| = |\psi(\varphi(S))| + k - 1 > |\psi(\varphi(S))|.$$

Это неравенство завершает доказательство достаточности условий теоремы.

Средняя взаимная информация протокола (φ_r, ψ_r) вычисляется по формуле

$$\mathbf{I}(\varphi_r, \psi_r) = \mathbf{I}(\varphi, \psi) + \mathbf{P}\{\psi(\xi) \in \{y_1, y_2, \ldots, y_k\}\} \ln \mathbf{P}\{\psi(\xi) \in \{y_1, y_2, \ldots, y_k\}\} + \sum_{i=1}^{k} (-\mathbf{P}\{\varphi(\xi) = y_i\} \ln \mathbf{P}\{\varphi(\xi) = y_i\}).$$

Сумма последних двух слагаемых положительна.

Доказательство теоремы завершено.

Следствие 1. *Любой протокол имеет расширение, являющееся прозрачным.*

Теорема 2 (теорема разложения). *Протокол (φ, ψ) имеет разложение на m расширений тогда и только тогда, когда*

$$m \leqslant \min_{y \in \psi(\varphi(S))} |\psi^{-1}(y) \cap \varphi(S)|.$$

Доказательство. Пусть существует разложение (φ, ψ) на m расширений. Тогда для всех s из S

$$\psi(\varphi(s)) = \psi(\varphi_{r_1}(s)) = \cdots = \psi(\varphi_{r_m}(s)), \quad r_i \in R, \quad i = 1, \ldots, m. \tag{9}$$

В силу (6) для всех s из S и $i \neq j$

$$\varphi_{r_i}(s) \neq \varphi_{r_j}(s). \tag{10}$$

Пусть $y_m \in \psi(\varphi(S))$ таково, что

$$|\psi^{-1}(y_m) \cap \varphi(S)| = \min_{y \in \psi(\varphi(S))} |\psi^{-1}(y) \cap \varphi(S)|.$$

Тогда в y_m переходят не более, чем $|\psi^{-1}(y_m)|$ элементов из $\varphi(S)$, следовательно, среди $\varphi_{r_1}(s), \ldots, \varphi_{r_m}(s)$ при $s \in \varphi^{-1}(\psi^{-1}(y_m))$ не более $|\psi^{-1}(y_m)|$ различных элементов из S, и для выполнения (10) необходимо выполнение условия

$$m \leqslant |\psi^{-1}(y_m)|.$$

Необходимость доказана.

Докажем достаточность. Пусть

$$|\psi(\varphi(S))| = \{y_1, \ldots, y_k\}, \qquad m_i = |\psi^{-1}(y_i) \cap \varphi(S)|,$$
$$X_i = \{x_{i,1} \ldots, x_{i,m_i}\} = \psi^{-1}(y_i) \cap \varphi(S), \quad i = 1, \ldots, k, \quad m \leqslant \min_i m_i.$$

Определим отображения $\varphi_r(s) = x_{i,r}$, $\psi_r(s) = s$, если $\varphi(s) \in X_i$, $r = 1, \ldots, m$. Из построения видно, что (φ_r, ψ_r) является расширением (φ, ψ) и $\psi_{r_i}(S) \cap \psi_{r_j}(S) = \varnothing$ при $i \neq j$. Если $\varphi_1(S) \cup \ldots \cup \varphi_m(S) = \varphi(S)$, то утверждение доказано. Это означает, что $m_1 = \ldots = m_k = m = |\varphi(S)|/|\psi(\varphi(S))|$, и построенное разложение является регулярным.

В противном случае построим протокол (φ_0, ψ_0) следующим образом. Обозначим через X все элементы $\varphi(S)$, не вошедшие в $\varphi_1(S) \cup \ldots \cup \varphi_m(S)$. Положим $\varphi_0(s) = \varphi(s)$, если s принадлежит $\varphi^{-1}(X)$, и $\varphi_0(s) = \varphi_m(s)$, если s не принадлежит $\varphi^{-1}(X)$, $\psi_0(s) = s$. По построению (φ_0, ψ_0) является расширением (φ, ψ), $\varphi_0(S) \cup \ldots \cup \varphi_{m-1}(S) = \varphi(S)$, и значит, $\{(\varphi_r, \psi_r), r = 0, 1, \ldots, m-1\}$ является требуемым разложением.

Теорема доказана.

2. Примеры махинаций в мутных протоколах

Прикладной смысл данного в предыдущем пункте определения протокола применительно к информационным системам заключается в следующем.

Система информацию о своем состоянии s из S передает участнику системы в виде $\varphi(s)$, который, в свою очередь, принимает некоторое решение $\psi(\varphi(s))$. Использование мутных протоколов может привести к нарушению безопасности системы посредством действий злоумышленника (нарушителя безопасности системы), находящегося в системе, возможно в сговоре с сообщником (агентом), находящимся у участника системы.

К примерам таких нарушений можно отнести махинации в системах нотариальной заверки цифровых подписей [2], организации скрытых [3], потайных [4] каналов для обмена данными между злоумышленником и сообщником.

2.1. Махинации в системах нотариальной заверки цифровых подписей

Рассматривается сеть передачи сообщений x из конечного множества всех сообщений X между абонентами из множества $I = \{0, 1, \ldots, N\}$, $N > 2$. Абонент 0 объявлен нотариусом. Каждый абонент i имеет набор секретных функций $d_{i,j}(x)$, $x \in X$, которые принимают значения из множества D, $j \in I$. Они используются абонентом i для создания цифровой подписи сообщений x абонентам j. Кроме того, i имеет набор секретных функций $b_{j,i}(x, d)$, $x \in X$, $d \in D$, которые принимают значение из множества D, $j \in I$. Они используются абонентом i для проверки правильности цифровой подписи d под сообщением x от абонента j. Абонент $i \in \{1, \ldots, N\}$ знает только функции $d_{i,j}(x)$, $b_{j,i}(x, d)$, $j \in I$, $d \in D$. Нотариус знает все функции. Получив от абонента i вектор (i, j, x, d) нотариус создает вектор $s = (i, j, x, d, b_{i,j}(x, d))$ и через сеть передает его абоненту j. Обратим внимание на то, что функция $b_{i,j}(x, d)$ известна лишь нотариусу и абоненту j. Абоненту i она неизвестна.

Абонент j, получив через сеть вектор $s = (i, j, x, d, b)$, принимает решение о том, что сообщение x с подписью d подписано правильно, если вычисленное им значение $b_{i,j}(x, d)$ совпадает с b, и отображает его в себя. В противном случае, считает его неподписанным и отображает в вектор (i, i, x, d, b).

Выше описан протокол (φ, ψ) для общения системы с участником j, в котором

$$S = \{(i, j, x, d, b)\}, \quad i \in I, \quad x \in X, \quad d \in D, \quad b \in B, \quad \varphi(s) = s,$$

$\psi(s) = s$, если $b_{i,j}(x, d) = b$, и $\psi(s) = (i, i, x, d, b)$, если $b_{i,j}(x, d) \neq b$.

Одна из функций механизма электронной цифровой подписи — это разрешение конфликта, в котором абонент j утверждает, что получил от i сообщение x, подписанное подписью d, а абонент i от этого отказывается. Обычно, условием разрешения конфликта в пользу абонента i является справедливость неравенства $d_{i,j}(x) \neq d$.

Пусть S_0 — множество тех состояний системы из S, для которых соответствующие им сообщения x приняты абонентом j как подписанные правильно.

Рассмотрим ограничение описанного выше протокола на множество S_0.

Из приведенных выше определений видно, что для всех x

$$s_u = (i, j, x, d_{i,j}(x), b_{i,j}(x, d_{i,j}(x))) \in \psi(\varphi(S_0)).$$

Пусть для некоторых i, x эффективно вычислены при неизвестных функциях $b_{i,j}$, $b_{i_1,j}$ такие i_1, x_1, d_1, что

$$b_{i,j}(x, d_{i,j}(x)) = b_{i_1,j}(x_1, d_1), (i_1, x_1, d_1) \neq (i, x, d_{i,j}(x)). \tag{11}$$

В силу условия (11) абонент j примет решение о том, что сообщение x_1 от абонента i_1 с подписью d_1 подписано правильно, то есть

$$\psi(\varphi(s_f)) = S_f.$$

В случае возникновения конфликта абонент i_1 будет отказываться от сообщения x_1 с подписью d_1. Он сможет это сделать, если $d_{i,j}(x_1) \neq d_1$.

Замечание 1. Пусть функция $b_{i,j}(x, d)$ не зависит от d. Тогда любой абонент i_1 откажется от любого сообщения x_1 с подписью $d_1 \neq d_{i_1,j}(x_1)$, проведя описанную выше махинацию при $i = i_1, x = x_1$, если подменит

$$S_n = (i_1, j, x_1, d_{i_1,j}(x_1), b_{i_1,j}(x_1))$$

вектором

$$S_f = (i_1, j, x_1, d_1, b_{i_1,j}(x_1)).$$

Замечание 2. Пусть функция $b_{i,j}(x, d)$ не зависит от i. Тогда любой абонент i_1 откажется от любого сообщения x_1 с подписью $d_1 = d_{i,j}(x_1) \neq d_{i_1,j}(x)$, проведя описанную выше махинацию при $x = x_1$ в сговоре с абонентом i.

2.2. Потайные, скрытые каналы

Пусть протокол (φ, ψ) имеет разложение (6). Тогда злоумышленник (возможно, это программно-аппаратная закладка) может организовать канал передачи команд своему сообщнику (возможно, программно-аппаратной закладке), находящемуся у участника, следующим образом.

Не ограничивая общности, полагаем $R \subset S$.

Пусть злоумышленник желает передать сообщнику команду с именем r. Тогда, при передаче системой участнику сообщения о своем состоянии $\varphi(s)$, злоумышленник подменяет $\varphi(s)$ на $\varphi_r(s)$. В силу условий (1) и (2) на расширения (φ_r, ψ_r) участник не заметит такой подмены. Сообщник же примет решение об исполнении команды с именем r на том основании, что полученное им сообщение $\varphi_r(s)$ принадлежит множеству $\varphi_r(S)$. В силу условий (6) его решение будет однозначным и правильным. Конечно, такая подмена имеет смысл лишь в случае $|R| \geqslant 2$.

Далее рассмотрим довольно общий пример, встречающихся в практике ситуаций. На конечном промежутке времени T в фиксированные моменты времени в системе происходят события с признаками $0, 1, \ldots, N$. Например, передаются сообщения со значениями атрибута $0, 1, \ldots, N$ (см. [5]). Система передает информацию о событиях своему участнику. Информация о характере события (сообщения) недоступна никому, кроме системы и участника, а вот признаки (значения атрибутов) наблюдаемы. Рассмотрим в качестве модели наблюдений за передачей признаков событий выборку без возвращений.

Пусть множеством состояний системы S является множество выборов без возвращения из урны с $n + h_0$ шарами, содержащей $h_i \geqslant 1$ шаров цвета i, $i = 0, 1, \ldots, N$, где $h_1 + \ldots + h_N = n$. Будем обозначать это множество $S(h_0, \ldots, h_N)$, а его элементы

$$s = (x_1, \ldots, x_{n+h_0}), \quad x_j = 0, 1, \ldots, N, \quad j = 1, \ldots, n + h_0.$$

Решения участника могут не зависеть от порядка следования всех событий или событий с некоторыми признаками. Поэтому для дальнейших обсуждений определим еще ряд множеств. Пусть

$I(n, h_0)$ — множество всех наборов целых чисел $i = (i_1, \ldots, i_n)$ таких, что $1 \leqslant i_1 < \ldots < i_n \leqslant n + h_0$;

$S(h_1, \ldots, h_N)$ — множество всех выборов без возвращения из урны с n шарами, содержащей $h_i \geqslant 1$ шаров цвета i, $i = 1, \ldots, N$, которые будем обозначать $a = (a_1, \ldots, a_n,\ a_j = 1, \ldots, N,\ j = 1, \ldots, n)$;

$T(i)$, $i \in I(n, h_0)$ — это множество всех элементов $S(h_1, \ldots, h_N)$, у которых на местах i не стоит элемент цвета 0;

$P(a)$, $a \in S(h_1, \ldots, h_N)$ — множество всех элементов $S(h_0, \ldots, h_N)$, у которых есть подпоследовательность a, то есть существует $i \in I(n, h_0)$ такое, что $x_{i_\nu} = a_\nu$, $\nu = 1, \ldots, n$.

Для $s \in S$ определим следующие отображения:

$\varepsilon(s) = s$ отображает элемент s в себя;

$\tau_t(s) = t$ отображает все элементы S в фиксированный элемент $t \in S$;

$\mu_i(s)$ отображает s в элемент, у которого шары цветов $1, \ldots, N$ стоят в том же порядке, как в s, но на местах $i \in I(n, h_0)$;

$\pi_a(s)$ отображает s в элемент, у которого на тех местах, где стояли шары цветов $1, \ldots, N$, стоит последовательность шаров $a \in S(h_1, \ldots, h_N)$;

$\chi(s)$ принимает фиксированное значение на всех элементах множества S (это значит, что участнику важен лишь факт передачи информации о всех событиях за период T);

$\omega(s)$ принимает одно фиксированное значение на всех элементах множества P_a, $a \in S(h_1, \ldots, h_N)$, причем, разные значения при разных a (это означает, что участнику важен лишь порядок, в котором следуют события с признаками $1, \ldots, N$);

$\lambda(s)$ принимает одно фиксированное значение на всех элементах множества $T(i)$, $i \in I(n, h_0)$, причем, разные значения при разных i (это означает, что участнику важно лишь, в какие моменты времени происходили события с признаками $1, \ldots, N$).

Теорема 3. *Семейство протоколов* $\{(\tau_t, \varepsilon), t \in S\}$ *является регулярным разложением протокола* (ε, χ) *на* $(n + h_0)!/(h_0! \ldots h_n!)$ *расширений.*

Семейство протоколов $\{(\mu_i, \varepsilon), i \in I(n, h_0)\}$ *является регулярным разложением протокола* (ε, ω) *на* $(n + h_0)!/(h_0! n!)$ *расширений.*

Семейство протоколов $\{(\pi_a, \varepsilon), a \in S(h_1, \ldots, h_N)\}$ *является регулярным разложением протокола* (ε, λ) *на* $n!/(h_1! \ldots h_N!)$ *расширений.*

Справедливость утверждений теоремы следует из построения соответствующих отображений.

3. Использование расширений информационных протоколов для их защиты

По-видимому, наилучший способ не допускать нарушения безопасности информационных систем — это использовать только прозрачные протоколы. Однако, это не всегда возможно в связи с наличием таких требований к информационным системам как оперативность и ограниченность технических ресурсов.

Одним из возможных подходов к решению задач безопасности использования мутных протоколов, допускающих разложение на большое количество расширений, является следующий.

Пусть (φ, ψ) допускает разложение (6) и Q — подмножество R. Тогда, перед входом участника используется программно-техническое средство безопасности, которое случайным образом выбирает элемент r из Q и осуществляет преобразование его входа при помощи φ_r.

Рассмотрим далее лишь те протоколы (φ, ψ), у которых отображения φ удовлетворяют условию

$$\varphi(\varphi(s)) = \varphi(s), \qquad s \in S. \tag{12}$$

Такое ограничение логично, так как подготовленное для передачи состояние не имеет смысла еще раз изменять. Кроме того, для произвольного протокола (φ, ψ) существует взаимно однозначное отображение (подстановка) π множества S на себя такое, что отображение $\pi(\varphi(s))$ удовлетворяет условию (12), и $(\pi(\varphi(s))), \psi(\pi^{-1}(s))$ эквивалентен протоколу (φ, ψ) с точки зрения конечных пользователей.

Введем обозначения

$$\{y_1, \ldots, y_m\} = \psi(\varphi(S)), \qquad W_j = \varphi^{-1}(\psi^{-1}(y_j)),$$
$$V_j = \psi^{-1}(y_j) \cap \varphi(S), \qquad j = 1, \ldots, m.$$

Лемма 1. *Пусть для протокола* (φ, ψ) *выполнено условие* (12). *Тогда протокол* (φ_r, ψ_r) *является расширением протокола* (φ, ψ) *тогда и только тогда, когда для всех* $j = 1, \ldots, m$

$$\varphi_r(W_j) \subset V_j.$$

При этом $\varphi_r(V_j) \subset V_j$.

Доказательство. Из условия (12) следует,что

$$S = W_1 \cup \ldots \cup W_m, \qquad \varphi(S) = V_1 \cup \ldots \cup V_m$$

являются такими разбиениями на непересекающиеся множества, что $W_j \supset V_j$, $j = 1, \ldots, m$. Пусть (φ_r, ψ_r) является расширением и $s \in W_j$, $j = 1, \ldots, m$. Тогда $\varphi(s) \in V_j$, $\varphi_r(s) \in \varphi(S)$, $\psi(\varphi_r(s)) = \psi(\varphi_r(s)) = y_j$, и следовательно, $\varphi_r(s) \in V_j$. Необходимость доказана. Достаточность доказывается проверкой условий (1) и (2).

Разложение

$$\{(\xi_z, \zeta_z), z \in Z\}, \quad \varphi(S) = \bigcup_{z \in Z} \xi_z(S), \quad \xi_{z_1}(s) \cap \xi_{z_2}(s) = \varnothing, \quad z_1 \neq z_2, \tag{13}$$

протокола (φ, ψ) будем называть вложенным по отношению к разложению (6), если выполнение условия $\xi_z(S) \cap \phi_r(S) \neq \varnothing$ влечет выполнение условия $\xi_z(S) \supset \phi_r(S)$.

Замечание 3. Если разложение (6) регулярное и $|\psi(\varphi(S))| = 1$, то любое разложение протокола (φ, ψ) будет вложенным по отношению к разложению (6).

Замечание 4. Пусть $S = S(h_0, h_1, \ldots, h_N)$, $(\varphi, \psi) = (\varepsilon, \omega)$, $(\varphi_r, \psi_r) = (\mu_i, \varepsilon)$ (см. теорему 3) и в разложении (13) $\xi_z(S)$ переставляет все шары из $T(i)$, $i \in I(n, h_0)$, одним и тем же способом, тогда разложение (13) является вложенным по отношению к (ε, ω).

Теорема 4. *Пусть протокол* (φ, ψ) *имеет разложения* (6) *и* (13), *отображение* φ *удовлетворяет условию* (12), ρ *— некоторая случайная величина, принимающая значения из множества* R.

Тогда для любых $s \in S$, $z \in Z$ *справедливы соотношения*

$$\mathbf{P}\{\rho \in \{r : \psi(\varphi_r(\varphi(s))) = \psi(\varphi(s))\}\} = 1, \tag{14}$$

$$\mathbf{P}\{\rho \in \{r : \psi(\varphi_r(\xi_z(s))) = \psi(\varphi(s))\}\} = 1. \tag{15}$$

Пусть, кроме того, разложение (13) *является вложенным по отношению к разложению* (6).

Тогда существуют такие множества $R(z) \subset R$, $z \in Z$, *что* $R(z_1) \cap R(z_2) = \varnothing$ *при* $z_1 \neq z_2$ *и*

$$R = \bigcup_{z \in Z} R(z), \xi_z(S) = \bigcup_{r \in R(z)} \varphi_r(S), \tag{16}$$

и для любых $s \in S$, $z_1, z_2 \in Z$ *справедливо равенство*

$$\mathbf{P}\{\rho \in \{r : \varphi_r(\xi_{z_1}(s)) \in \xi_{z_2}(S)\}\} = \mathbf{P}\{\rho \in R(z_2)\}. \tag{17}$$

Доказательство. Для любых $r \in R$, $z \in Z$, $s \in W_j$, $j = 1, \ldots, m$, из (2) и (12) следует справедливость цепочек равенств

$$\psi(\varphi_r(\varphi(s))) = \psi(\varphi(\varphi(s))) = \psi(\varphi(s)),$$
$$\psi(\varphi_r(\xi_z(s))) = \psi(\varphi(\xi_z(s))) = \psi(\xi_z(\xi_z(s))) = \psi(\xi_z(s)) = \psi(\varphi(s)).$$

Из леммы 1 следует, что $\xi_z(\xi_z(s))$ и $\xi_z(s)$ лежат в V_j, а это означает совпадение двух крайних членов последних цепочек. Утверждения теоремы (14) и (15) доказаны.

Для каждого $z \in Z$ существует такое $R(z)$, что

$$\xi_z(S) = \bigcup_{r \in R(z)} \varphi_r(S)$$

и для любого подмножества $Q \subset R(z)$, не равного $R(z)$, объединение

$$\bigcup_{r \in Q} \varphi_r(S)$$

не включает $\xi_z(S)$. Если $R(z) = R$, то $\xi_z(S) = \varphi(S)$, $|Z| = 1$, и соотношения (16) и (17) доказаны.

Пусть существуют такие $r \in R$, z_1, z_2, что

$$\varphi_r(S) \cap \xi_{z_1}(S) \neq \varnothing, \qquad \varphi_r(S) \cap \xi_{z_2}(S) \neq \varnothing.$$

Тогда в силу того, что разложение (13) является вложенным по отношению к разложению (6),

$$\xi_{z_1}(S) \cap \xi_{z_2}(S) \subset \varphi_r(S).$$

Это возможно лишь при $z_1 = z_2$, что, в свою очередь, означает, что множества $R(z)$, не пересекаются при разных $z \in Z$. В силу (6) и (13) справедливо (16). А это означает, что

$$\{r : \varphi_r(\xi_{z_1}(S)) \in \xi_{z_2}(S)\} = R(z_2).$$

Это влечет справедливость (17).

Теорема доказана.

Теорема 5. *Пусть семейство расширений $\{(\varphi_r, \psi_r), r \in R\}$ является регулярным разложением протокола (φ, ψ), $\{(\xi_z, \eta_z), z \in Z\}$ — некоторое разложение протокола (φ, ψ), отображение φ удовлетворяет условию* (12), *и ρ — некоторая случайная величина, принимающая значения из R.*

Тогда для любых $s \in S$, $z_1, z_2 \in Z$ справедливо равенство

$$\mathbf{P}\{\rho \in \{r : \varphi_r(\xi_{z_1}(s)) \in \xi_{z_2}(S)\}\} = \mathbf{P}\{\rho \in \{r : \xi_{z_2}(S) \cap \varphi_r(S) \cap \psi^{-1}(\psi(\varphi(s))) \neq \varnothing\}\}.$$

Доказательство. Из соотношения (14) следует, что $\varphi_r(\xi_{z_1}(s)) \in \psi^{-1}(\psi(\varphi(s)))$ и, кроме того, $\varphi_r(\xi_{z_1}(s)) \in \varphi_r(S)$. В силу регулярности разложения

$$|\varphi_r(S) \cap \psi^{-1}(\psi(\varphi(s)))| = 1. \tag{18}$$

Это, наряду со сказанным выше, означает, что

$$\varphi_r(\xi_{z_1}(s)) = \varphi_r(S) \cap \psi^{-1}(\psi(\varphi(\xi))),$$

и в силу (18)

$$\{r:\varphi_r(\xi_{z_1}(s)) \in \xi_{z_2}(S)\} = \{r:\varphi_r(S) \cap \psi^{-1}(\psi(\varphi(s))) \in \xi_{z_2}(S)\}$$
$$= \{r:\xi_{z_2}(S) \cap \varphi_r(S) \cap \psi^{-1}(\varphi(s)) \neq \varnothing\}.$$

Последнее соотношение завершает доказательство теоремы.

Следствие 2. *Пусть в условиях теоремы* 5 *случайная величина* ρ *имеет равномерное распределение на* R. *Тогда справедливо соотношение*

$$\mathbf{P}\{\rho \in \{r:\varphi_r(\xi_{z_1}(s)) \in \xi_{z_2}(S)\}\} = \frac{|\psi(\varphi(S))|}{|\varphi(S)|}|\xi_{z_1}(S) \cap \psi^{-1}(\psi(\varphi(s)))|.$$

Если, кроме того $|\varphi(S)| = |S|$, *то*

$$\frac{1}{|S|}\sum_{s\in S}\mathbf{P}\{\rho \in \{r:\varphi_r(\xi_{z_1}(s)) \in \xi_{z_2}(S)\}\} = \frac{|\xi_{z_2}(S)|}{|S|}.$$

Замечание 5. Пусть для защиты протокола (φ, ψ), допускающего разложение (6), используется защита, основанная на разложении (13). Тогда смысл фигурирующих в теоремах 4 и 5 вероятностей заключается в следующем.

Решения, принимаемые участником не изменяются ни от действия защиты, ни при подмене протокола (φ, ψ) на протоколы (ξ_z, η_z), $z \in Z$.

Вероятность решения сообщника z_2 не зависит от передаваемой ему команды злоумышленника z_1.

Замечание 6. Рассмотрим результаты применения описанной выше защиты к одному примеру построения процедуры скрытого общения злоумышленника с сообщником из [5].

Описание процедуры дается в терминах раздела 2.2.

Пусть $S = (h_0, h_1)$, t_0 — фиксированный элемент из S. Рассмотрим пару протоколов (ξ_0, η_0), (ξ_1, η_1), в которых $\xi_0 = \tau_{t_0}$, $\eta_0 = \eta_1 = \varepsilon$, ξ_1 — произвольное отображение множества S на множество $S \setminus t_0$.

Тогда, по построению, определенная выше пара является разложением протокола (ε, χ), которое в силу первого утверждения теоремы 3 и замечания 3 является вложенным по отношению к разложению $\{(\tau_t, \varepsilon),\ t \in S\}$. Злоумышленник использует пару (ξ_0, η_0), (ξ_1, η_1) для передачи сообщнику команды на начало действия t_0.

Из теоремы 4 и замечания 5 при равномерном распределении ρ на множестве S следует, что вероятность правильного решения на начало действий равна

$$\frac{h_0!\,h_1!}{(h_0+h_1)!}$$

Отсюда следует, что вероятность правильного решения в процедуре (активизации агента) [5], даже в том случае, когда он знает систему адресации сегментов и внутренних адресов, при применении описанной выше защиты будет стремиться к 0 с ростом $h_0 + h_1$.

Автор выражает признательность И. А. Круглову за внимание к работе и ряд конструктивных замечаний. В частности, им предложена лемма 1, которая существенно расширяет границы применимости теоремы 4.

Список литературы

1. Шеннон К., *Работы по теории информации и кибернетике.* ИЛ, Москва, 1963.
2. Князев А. В., Ронжин А. Ф., О простейших махинациях в некоторых системах нотариального заверивания цифровых подписей. *Обозрение прикладной и промышленной математики* (2003) **10**, №2, 481–482.
3. Lampson B. W., A note of the confinement problem. *Commun. ACM* (1973) **16**, №10, 613–615.
4. Schneier B., *Applied cryptography: protocols, algorithms and source code in C.* Wiley, New York, 1996.
5. Грушо А. А., Тимонина Е. Е., Оценка времени, требуемого для организации скрытого канала. *Дискретная математика* (2003) **15**, №2, 40–46.

Статья поступила 23.03.2004.