УДК 519.7

О РАСШИРЕНИЯХ ОТОБРАЖЕНИЙ, СОХРАНЯЮЩИХ СВОЙСТВО ИДЕНТИФИЦИРУЕМОСТИ[1]

Л. Н. Андреева

Пусть $A = \{0, 1, \ldots, k-1\}$, $k \geqslant 2$, n — натуральное число, Q — множество всех отображений $q\colon A^n \to A^n$ и для каждого отображения q в Q определены функции $q_i\colon A^n \to A$, $i = 1, 2, \ldots, n$, так, что $q(x) = q_1(x)q_2(x)\ldots q_n(x)$ для всех x в A^n, т. е. $q = q_1q_2\ldots q_n$. Пусть также $B = \{i_1, i_2, \ldots, i_{|B|}\} \subseteq \{1, \ldots, n\}$, $i_1 < i_2 < \ldots < i_{|B|}$ и $a[B] = a_{i_1}a_{i_2}\ldots a_{i_{|B|}}$ для любого вектора $a = a_1a_2\ldots a_n$.

Говорят, что отображение q в Q *идентифицируется на* B, если для любого отображения $t \in Q$ из $q[B] = t[B]$ следует $q = t$.

По определению, если отображение q в Q идентифицируется на B, то оно идентифицируется и на любом множестве $F \subseteq \{1, \ldots, n\}$, таком, что $B \subseteq F$.

Построим отображение $g\colon A^{n+1} \to A^{n+1}$ как расширение отображения q следующим образом. Возьмём произвольную функцию $\sigma\colon A \to A$ и элемент $j \in \{1, \ldots, n+1\} \setminus B$ и положим $g_j(x_1, \ldots, x_j, \ldots, x_{n+1}) = \sigma(x_j)$, $g_i(x_1, \ldots, x_j, \ldots, x_{n+1}) = q_i(x_1, \ldots, x_{j-1}, x_{j+1}, \ldots, x_{n+1})$ для всех $i \neq j$. Пусть наконец $D = B \cup \{j\}$.

Теорема 1. Отображение q идентифицируется на B, если и только если отображение g идентифицируется на D. Отображение g не идентифицируется на множестве $\{1, \ldots, n+1\} - \{j\}$.

Доказательство. Пусть отображение q идентифицируется на B. Предположим, что его расширение g не идентифицируется на D. Тогда найдётся такое отображение $t' : A^{n+1} \to A^{n+1}$, что $t'[D] = g[D]$ и $g \neq t'$, и для $t \in Q$, полученного из t' вычёркиванием j-й компоненты, будет $q[B] = t[B]$ и $q \neq t$, что противоречит идентифицируемости q на B. Следовательно, g идентифицируется на D.

Обратно, пусть отображение g идентифицируется на D. Предположим, что q не идентифицируется на B. Тогда найдётся такое отображение $t\colon A^n \to A^n$, что $t[B] = q[B]$ и $q \neq t$. Построим расширение t' для t, положив $t'_j = g_j$, и как результат получим $g[D] = t'[D]$ и $g \neq t'$, что противоречит идентифицируемости g на D. Следовательно, q идентифицируется на B.

Пусть g' — такое расширение отображения q, что $g'_j(x) = \sigma'(x_j) \neq \sigma(x_j) = g_j(x)$. Тогда $g_1g_2\ldots g_{j-1}g_{j+1}\ldots g_{n+1} = g'_1g'_2\ldots g'_{j-1}g'_{j+1}\ldots g'_{n+1}$ и $g \neq g'$, т. е. отображение g не идентифицируется на множестве $\{1, \ldots, n+1\} - \{j\}$. ■

Пусть далее $V \subseteq Q$ есть множество всех инволюций на A^n, т. е. подстановок $q\colon A^n \to A^n$ со свойством инволютивности: $\forall x, y \in A^n(q(x) = y \Rightarrow q(y) = x)$. Непосредственно проверяется, что если расширение g инволюции $q \in V$ построено с помощью подстановки $\sigma\colon A \to A$, то $g \in V$, т. е. расширение инволюции по подстановке является инволюцией; в этом случае теорема 1 остаётся в силе, если в её формулировке вместо отображений в Q рассматриваются инволюции в V. Таким образом, для любой инволюции $q \in V$ можно построить $k!(n+1)$ различных инволюций, являющихся расширениями инволюции q, сохраняющими свойство идентифицируемости последней.

Эти результаты могут быть использованы в инволюционных схемах разделения секрета [1], когда в множество участников схемы вводится новый участник и требуется,

[1]Работа выполнена в рамках реализации ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009–2013 гг. (гос. контракт № П1010).

чтобы неавторизованные множества новой схемы включали в себя неавторизованные множества прежней схемы.

В этой связи, а также в связи с криптоанализом инволюционных шифров [2, 3] представляет интерес следующий тест идентифицируемости произвольной инволюции.

Теорема 2. Инволюция $q \in V$ идентифицируется на B, если и только если для любых x и y в A^n, $x \neq y$, выполняется $q(x)[B] \neq q(y)[B]$.

Доказательство. Необходимость. Пусть инволюция q идентифицируется на B. Предположим, что в A^n найдутся такие x и y, что $x \neq y$ и $q(x)[B] = q(y)[B]$. Построим инволюцию $t \in V$, $t \neq q$, такую, что $q(x) = t(y)$ и $q(y) = t(x)$, а на остальных элементах в A^n инволюции t и q совпадают. Тогда $t(y)[B] = q(x)[B] = q(y)[B] = t(x)[B]$. Имеем $t[B] = q[B]$ и $t \neq q$, что противоречит идентифицируемости q на B.

Достаточность. Пусть для любых x и y в A^n, где $x \neq y$, выполняется $q(x)[B] \neq \neq q(y)[B]$. Предположим, что инволюция q не идентифицируется на B. Тогда в Q найдется инволюция t, что $t \neq q$ и $q[B] = t[B]$. Если же $t \neq q$, то в A^n найдутся такие x и y, что $x \neq y$, $q(x) = t(y)$ и $q(y) = t(x)$. Следовательно, $q(x)[B] = t(x)[B] = q(y)[B] = = t(y)[B]$, что противоречит условию. ■

ЛИТЕРАТУРА

1. *Андреева Л. Н.* Инволюционные схемы разделения секрета // Вестник Томского госуниверситета. Приложение. 2007. № 23. С. 99.
2. *Андреева Л. Н.* К криптоанализу шифров инволюционной подстановки // Вестник Томского госуниверситета. Приложение. 2005. № 14. С. 43–44.
3. *Андреева Л. Н.* К криптоанализу инволютивных шифров с частично известными инволюциями // Вестник Томского госуниверситета. Приложение. 2006. № 17. С. 109–112.

УДК 004.056.55

ДОКАЗУЕМО БЕЗОПАСНАЯ ДИНАМИЧЕСКАЯ СХЕМА ГРУППОВОЙ ПОДПИСИ

А. В. Артамонов, П. Н. Васильев, Е. Б. Маховенко

В ряде прикладных задач для защиты сообщений от фальсификации требуется выполнение следующих условий:

— возможности создания электронной цифровой подписи одним лицом от имени группы лиц;
— невозможности идентификации автора такой подписи проверяющей стороной;
— возможности раскрытия автора подписи уполномоченным лицом.

Этим условиям удовлетворяют схемы групповой подписи. В зависимости от решаемой прикладной задачи к ним могут быть предъявлены дополнительные требования:

— возможность добавления новых членов в группу без необходимости изменения открытого ключа группы;
— возможность отзыва права подписи у определенных членов группы.

Анализ современных схем групповой подписи позволил выделить признаки, по которым такие схемы можно классифицировать и сравнивать, а на их основе построить обобщенную классификационную схему схем групповой подписи [1]. По совокупности этих признаков, в частности свойств безопасности, обеспечиваемых схемой, эффективности процедур формирования, проверки и раскрытия подписи, ее длины, а также