ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 19 МАТЕМАТИКИ Выпуск 3
2012

М. А. Пудовкина (Москва, НИЯУ (МИФИ)). **О структурированности множеств итеративных алгоритмов блочного шифрования.**

Пусть $(X,+)$ — аддитивная абелева группа, $S(X)$ — множество всех подстановок на X, K — множество раундовых ключей, $g_{k_i}^{(i)}\colon X\to X$ есть раундовая функция i-го раунда, $l\in\mathbf{N}$, $n=|X|$, $n\geqslant 2$; э. о. — элементарная операция, $v^{(1)}$ — вероятность ошибки первого рода, $\sim_*$ — отношение эквивалентности на множестве $S(X)$, $U_*(s)=\{s'\in S(X)\,|\,s\sim_* s'\}$ — класс $\sim_*$-эквивалентности. Будем рассматривать такие разбиения, что $d=|U_*(s)|$ для всех $s\in S(X)$. Множество $\mathbf{R}\subseteq S(X)$ назовем $\sim_*$-*разбиением*, если оно является объединением некоторых классов $\sim_*$-эквивалентности, т. е. $R=\cup_{b\in\mathbf{R}}U_*(b)$. Рассмотрим множество итеративных алгоритмов шифрования $G^{(l)}=\{g_{k_1}^{(1)}g_{k_2}^{(2)}\cdots g_{k_l}^{(l)}|(k_1,k_2,\ldots,k_l)\in K^l\}$. Покажем, что нетривиальное отношение $\sim_*$ существует для большого класса алгоритмов блочного шифрования, основанных на XSL-сетях, схемах Фейстеля и Лэи–Месси.

Рассмотрим XSL-алгоритмы блочного шифрования с раундовой функцией $g_{k^{(i)}}^{(i)}\in S(X)$, заданной как $(\alpha)g_{k^{(i)}}^{(i)}=(\alpha+k^{(i)})^{g^{(i)}}$, $g^{(i)}\in S(X)$, $i=1,2,\ldots,l$. Положим $G^{(l,1)}=\{g_{k_1}^{(1)}g_{k_2}^{(2)}\cdots g_{k_l}^{(l)}|(k_1,k_2,\ldots,k_l)\in X^l\}$. Для $\beta,\alpha,k_1,k_2,\ldots,k_l\in X$ справедливо равенство $(\alpha+\beta)g_{k_1}^{(1)}g_{k_2}^{(2)}\cdots g_{k_l}^{(l)}-(\alpha)g_{k_1+\beta}^{(1)}g_{k_2}^{(2)}\cdots g_{k_l}^{(l)}=0$. Будем говорить, что множества $H\subseteq S(X)$ удовлетворяет условию (1) тогда и только тогда, когда для любых $\beta\in X$, $s\in H$ найдется такая подстановка $s'\in H$, что $(\alpha+\beta)^s=\alpha^{s'}$ для всех $\alpha\in X$. Положим $(\alpha+\beta)^s=\alpha^{s_\beta}$ для элементов $s\in S(X)$, $\beta,\alpha\in X$. На множестве $S(X)$ рассмотрим отношение $\sim_1$, полагая $s\sim_1 s'$ тогда и только тогда, когда $s'=s_\beta$ для некоторого элемента $\beta\in X$. Нетрудно убедиться, что $\sim_1$ есть отношение эквивалентности на множестве $S(X)$. Множество $S(X)$ разбивается на $(n-1)!$ эквивалентных классов, каждый мощности n. Тогда и только тогда $H\subseteq S(X)$ удовлетворяет условию (1), когда H есть $\sim_1$-разбиение. Таким образом, $G^{(l,1)}$ есть $\sim_1$-разбиение. Для различения случайного подмножества $\mathbf{R}\subseteq G^{(l,1)}$ от случайного подмножества $\underline{\mathbf{R}'\subseteq S(X)}$, $q=|R|=|R'|$ требуется: $T_q=-n^{l-1}\ln(v^{(1)})$ э. о., $q=1/2+\sqrt{2^{-2}-n^{l-1}\ln(v^{(1)})}$, вероятность ошибки второго рода равна $v^{(2)}=1-e^{\ln(v^{(1)})e^n n^{l-n-1/2}(2\pi)^{-1/2}}$.

Рассмотрим множество W с двумя бинарными операциями $+_1$, $+_2$, задающими аддитивные абелевы группы $(W,+_1)$ и $(W,+_2)$. Пусть $X=W\times W$. В этом случае i-раундовая функция схемы Фейстеля есть $g_{k^{(i)}}^{(i)}\colon(\alpha_1,\alpha_0)\to(\alpha_0,\alpha_1+_1(\alpha_0+_2k^{(i)})^{g^{(i)}})$, где $\alpha_1,\alpha_0,k^{(i)}\in W$, $g^{(i)}\colon W\to W$. Пусть $G^{(l,2)}=\{g_{k_1}^{(1)}g_{k_2}^{(2)}\cdots g_{k_l}^{(l)}|(k_1,k_2,\ldots,k_l)\in W^l\}$, $B^{(1)}(+_1,+_2)=\{\beta\in W|\exists\overline{\beta}\in W\colon\ (\lambda+_1\beta)+_2(\delta-_1\overline{\beta})=\lambda+_2\delta,\ \forall\lambda,\delta\in W\}$, $B^{(2)}(+_1,+_2)=\{\beta\in W|\exists\overline{\beta}\in W\colon\ (\lambda+_1\beta)-_2\overline{\beta}=\lambda,\ \forall\lambda\in W\}$.

В зависимости от четности числа раундов для любой подстановки $s\in G^{(l,2)}$ найдется такая подстановка $s'\in G^{(l,2)}$, что для всех элементов $\beta=(\beta_1,\beta_0)\in$

$(B^{(1)}(+_1,+_2))^2 \cup (B^{(2)}(+_1,+_2))^2$, $\alpha \in X$ имеем

$$(\alpha +_1 \beta)^{s'} = \begin{cases} \alpha^s +_1 \beta, & l \equiv 1\,(\mathrm{mod} 2), \\ \alpha^s +_1 (\beta_0, \beta_1), & l \equiv 0\,(\mathrm{mod} 2). \end{cases}$$

Пусть число раундов l нечетно. Для $s \in S(X)$ и $\beta \in X$ положим $(\alpha +_1 \beta)^{s_\beta} = \alpha^s +_1 \beta$. На множестве $S(X)$ рассмотрим отношение $\sim_2$, полагая $s \sim_2 s'$ тогда и только тогда, когда $s' = s_\beta$ для некоторого элемента $\beta \in X$. Нетрудно убедиться, что $\sim_2$ есть отношение эквивалентности на множестве $S(X)$ и множество $G^{(l,2)}$ есть $\sim_2$ - разбиение. Отметим, что четное l рассматривается похожим образом.

Таким образом, для ряда конструкций (схемы Фейстеля, Лэи–Месси, XSL-сети), используемых при синтезе блочных шифрсистем, для произвольного числа раундов $l < \log_{|K|} n!$ множество $G^{(l)}$ обладает структурой. Наличие такой структуры позволяет, например, различить случайное подмножество множества $G^{(l)}$ от множества случайных подстановок с трудоемкостью меньшей, чем n^l э. о. Кроме того, данная структура порождает классы слабых алгоритмов развертывания ключа блочной шифрсистемы. Также она может позволить с помощью связанных ключей построить различитель, отличающий алгоритм блочного шифрования от случайной подстановки с трудоемкостью, меньшей n э. о.