КОНСТРУИРОВАНИЕ КЛАССИЧЕСКИХ ЭНДОМОРФНЫХ СОВЕРШЕННЫХ ШИФРОВ И ИХ СОВРЕМЕННЫХ АНАЛОГОВ

С.С. Коновалова, С.С. Титов

Уральский государственный университет путей сообщения,
Колмогорова 66, 620034 Екатеринбург, Россия
svetlanak@e1.ru
sergey.titov@usaaa.ru

В работе в качестве объекта исследования взяты классические эндоморфные совершенные шифры и их современные аналоги — $U(L)$- и $O(L)$-стойкие шифры. Предмет исследования — комбинаторные конструкции данных шифров. Цель работы — расширить знания о классических эндоморфных совершенных шифрах и их современных аналогах.

В работе найдены решения трех задач о трех конструкциях линейных совершенных шифров, поставленных западными криптографами в 1987 году и описанных в [1]. Решение данных трех задач позволило уточнить связи между различными конструкциями линейных совершенных шифров. Также в работе получен целый ряд следующих серьезных результатов по эндоморфным $O(L)$- и $U(L)$-стойким шифрам [2, 3].

Установлена связь $O(L)$-стойких шифров с конечными плоскостями для $L = 2$, а также с пороговой схемой разделения секрета $(L, 2L-1)$. Построены массивы зашифрования для $O(2)$-, $U(2)$-, $O(3)$-, $U(3)$-стойких шифров. Найден целый класс $O(3)$-стойких шифров на основе дробно-линейных подстановок в почти-полях. Получены условия для проверки линейных шифров на совершенность, а линейных и циклических шифров — на $O(2)$- и $U(2)$-стойкость. Доказана одна теорема о взаимосвязи линейных, другая — циклических — $O(2)$- и $U(2)$-стойких шифров. Созданы основания для построения обобщенной теоремы о взаимосвязи $U(2)$- и $O(2)$-стойких шифров, содержащих инволюцию.

Исследованы конкретные системы Веблена-Веддерберна, такие как система Холла, почти-поля, не сводящиеся к полям, а также группы Матье, для возможности построения $O(L)$- и $U(L)$-стойких шифров на их основе; установлены связи между ними. В том числе доказана невозможность построения $O(3)$-стойких шифров на основе системы Холла определенного вида (что, вместе с другими отрицательными результатами, позволит сократить перебор вариантов уравнений зашифрования при построении $U(L)$- и $O(L)$-стойких шифров), а также определены частные случаи выделения $U(2)$-стойких шифров из $O(2)$-стойких для систем Холла и почти-полей.

Развитие существующих методов и привлечение более тонких комбинаторных, алгебраических, геометрических свойств может привести к эффективным критериям существования совершенных шифров и их современных аналогов, применимым на практике; к исследованию более имитостойких совершенных шифров. Полученные выводы означают, что необходимо выходить за традиционные рамки, в пределах которых исследуются совершенные шифры, с целью повышения защиты информации, сохранения ее конфиденциальности и целостности, что особенно важно для критичной информации (например, коротких, но очень важных сообщений). Результаты работы имеют научную и методическую ценность, так как расширяют существующую теорию совершенных шифров.

Литература

1. *Зубов А. Ю.* Совершенные шифры. М.: Гелиос АРВ, 2003. 160 с.

2. *Гутарин Д.С., Коновалова С.С., Тимин В.И., Титов Е.С., Титов С.С.* Комбинаторные проблемы существования совершенных шифров // Труды Института математики и механики. Екатеринбург: УрО РАН. Т. 13. № 4. 2007. С. 61–73.

3. *Коновалова С.С., Титов С.С.* Построение $O(L)$- и $U(L)$-стойких шифров в конечных плоскостях // Материалы Третьей межд. науч. конф. по проблемам безопасности и противодействия терроризму. МГУ им. М.В. Ломоносова. 25-27 октября 2007 г. М.: МЦНМО, 2008. С. 191–209.