***Лисицкая И.В., Казимиров А.В.***
*Харьковский национальный университет радиоэлектроники, Харьков, Украина*

## Об участии S-блоков в формировании максимальных значений дифференциальных вероятностей блочных симметричных шифров

Многочисленные публикации последних лет придерживаются концепции, в соответствии с которой показатели доказуемой стойкости БСШ к атакам дифференциального и линейного криптоанализа непосредственно связаны с дифференциальными и линейными показателями входящих в шифры S-блоковых конструкций.

Цель работы привести дополнительные аргументы по обоснованию новой точки зрения к оценке безопасности блочных шифров к отмеченным атакам, пропагандируемой в работе [1].

Эта точка зрения сложилась на основе развития нового подхода в теории и методах криптоанализа, предложенного на кафедре БИТ ХНУРЭ [2]. Она основывается, с одной стороны, на использовании при определении ожидаемых показателей стойкости больших шифров результатов анализа уменьшенных их версий, а с другой, – на уточнённой в последнее время на основе изучения свойств и показателей случайных подстановок и уменьшенных моделей шифров, рассматриваемых как подстановочные преобразования, новой идеологии определения показателей стойкости БСШ к атакам дифференциального и линейного криптоанализа [1]. Эта новая идеология строится на подтвержденном многочисленными экспериментами с уменьшенными версиями современных шифров положении (факте), состоящем в том, что все современные шифры (и большие и малые их версии) через определенное число циклов независимо от используемых в шифрах S-блоков приобретают свойства случайных подстановок [3,4].

В докладе демонстрируются результаты оценки влияния на дифференциальные показатели современных шифров (их малых версий) максимальных значений таблиц XOR разностей используемых в шифрах S-блоков.

### Литература

1. Горбенко И.Д. Новая идеология оценки стойкости блочных симметричных шифров к атакам дифференциального и линейного криптоанализа / Горбенко И.Д., Долгов В.И., Лисицкая И.В., Олейников Р.В. // Прикладная радиоэлектроника. – 2010. – Т. 9, № 3. – С. 212–320.
2. Долгов В.И. Подход к криптоанализу современных шифров / Долгов В.И., Лисицкая И.В., Олейников Р.В. // Материалы второй международной конференции “Современные информационные системы”, Харьков-Туапсе, Украина, 2–5 октября. – 2007. – С. 435–436.
3. Олейников Р.В. Дифференциальные свойства подстановок / Олейников Р.В., Олешко О.И., Лисицкий К.Е., Тевяшев А.Д. // Прикладная радиоэлектроника. – 2010. – Т.9. – № 3. – С. 326–333.
4. Долгов В.И. Свойства таблиц линейных аппроксимаций случайных подстановок / Долгов В.И., Лисицкая И.В., Олешко О.И. // Прикладная радиоэлектроника. – 2010. – Т.9. – № 3. – С. 334–340.

International conference on System Analysis and Information Technologies SAIT 2011
Institute for Applied System Analysis of National Technical University of Ukraine “KPI”, Kyiv, Ukraine, May 23–28, 2011
ISBN 978-966-2153-57-6, revision 0.9 (2011.05.05), available at http://sait.kpi.ua/books/sait2011.ebook.pdf