УВАЖАЕМЫЕ ЧИТАТЕЛИ!

Настоящий выпуск журнала «Прикладная радиоэлектроника» является тематическим и посвящен проблемным вопросам кибербезопасности, в основном в части криптографической защиты информации. Ряд статей, которые представлены в журнале, являются заказными, их тематика определяется практическими приложениями. В основном они подготовлены специалистами и молодыми соавторами по тематике, ориентируясь на задачи, которые решаются спонсором издания журнала – ПАТ «Институт информационных технологий», г. Харьков.

При отборе статей делалась ориентация авторов на оценку стойкости существующих криптографических преобразований для их применения в постквантовый период, а также на разработку предложений относительно совершенствования криптографических преобразований с учетом возникающих требований. Анализ и оценка, в первую очередь, были направлены на принятые в Украине, в качестве национальных, международные стандарты.

Дело в том, что в среде криптографов возникли волнения, связанные с наличием прогнозов относительно создания в перспективе квантового компьютера. Так, в случае появления квантового компьютера, на котором будут эффективно запущены квантовые алгоритмы криптоанализа Шора или алгоритм поиска Гроувера и др., могут возникнуть большие проблемы относительно стойкости как симметричных, так и ассиметричных криптографических преобразований.

Учитывая указанное, сегодня в технологически развитых государствах развернуты серьезные исследования и ведутся разработки в двух направлениях – создании квантового компьютера, а также разработки квантовых алгоритмов осуществления квантового криптоанализа.

Существенный импульс этим работам, по нашему мнению, придала публикация в Интернет статьи «A RIDDLE WRAPPED IN AN ENIGMA», авторы NEAL KOBLITZ AND ALFRED J. MENEZES. По мнению авторов, опубликованное агентством национальной безопасности правительства США (NSA) крупное политическое заявление о необходимости разработки стандартов для постквантовой криптографии, является мощным толчком для теоретических исследований и практических разработок в криптологии. В заявлении также указывается, что стандарты для новых постквантовых алгоритмов еще не изобретены.

Среди кандидатов на постквантовую криптографию авторами статьи называются:

- симметрические криптографические преобразования (блочные и поточные);
- криптопреобразования, основанные на алгебраических решетках;
- преобразования, основанные на хеш-функциях;
- криптография, основанная на кодах исправления ошибок;
- криптография на основе трудности вычисления изогения определенной степени между двумя изогенными суперсингулярными эллиптическими кривыми над конечным полем.

Публикуемые в этом журнале статьи, конечно без особых претензий авторов, в определенной мере ориентированы на решение задач синтеза и анализа постквантовых преобразований.

Так, в первом разделе представлены статьи, посвященные ассиметричным криптопреобразованиям направленного шифрования и электронной подписи. Они, в определенной мере, по крайней мере для авторов, отвечают на вызовы относительно требований к постквантовой криптографии, а также позволяют сделать определенные шаги к ней.

Во втором разделе мы продолжаем публикации, посвященные алгоритмам симметричных блоковых преобразований. Мы считаем, что принятием в Украине национальных стандартов ДСТУ 7624:2014 и ДСТУ 7564:2014, уже создана постквантовая криптография в части симметричных блочных преобразований и функций хеширования.

В третьем разделе представлены в основном статьи, посвященные электронной идентификации и и аутентификации.

С уважением и пожеланиями успехов,
профессор ***И.Д. Горбенко***