УДК 681. 327

А.К. Шилов, А.А. Валуев, А.Е. Умрихин

ИНЖЕНЕРНЫЕ ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

В докладе обсуждается проект документа [1], предложенного NIST (Национальным институтом стандартов и технологий США). Проект содержит базовые принципы, которые должны применяться при проектировании безопасных информационных систем. Принципы адресованы разработчикам и пользователям защищенных систем, государственного и частного сектора. Основа подхода состоит в определении набора базовых моделей безопасности. Цели защиты определяются связанными между собой требованиями по доступности, целостности, конфиденциальности и ответственности, а также гарантированности их реализации. Модели содержат следующие категории служб безопасности: поддержания, предотвращения и восстановления. На службы первой категории возлагаются функции идентификации, управления криптоключами, администрирования безопасностью и системной защиты. Функции служб второй категории: защищенный обмен, аутентификация, авторизация, управление доступом, невозможность отказа, секретная пересылка деловой информации. Службы третьей категории ориентированы на аудит, определение причин нарушения безопасности и содержания ответных действий, доказательство факта ненарушения защиты, восстановление безопасного состояния. В докладе дается анализ содержащихся в проекте тридцати одного принципа, предложения по их уточнению и детализации с учетом функциональных требований к механизмам защиты и требованиям по гарантированности их реализации в соответствии с международным стандартом [2].

ЛИТЕРАТУРА

1. Engineering Principles for IT Security (EP-ITS). A technical baseline for achieving security capabilities. Draft. - National Institute of Standards and Technology. United States Department of Commerce.- 10/23/2000. - 33 p. - www//nist.gov.
2. Common Criteria for Information Technology Security Evaluation. International Standard ISO/IEC 15408:1999.

УДК 681. 325.5

А.К. Шилов, П.А. Федоров

СИСТОЛИЧЕСКАЯ РЕАЛИЗАЦИЯ КРИПТОАЛГОРИТМОВ

В докладе обсуждаются проблемы реализации на СБИС различных криптосистем на основе систолических вычислений. Известные подходы к решению этой задачи связаны с выполнением криптоалгоритмов в СБИС целиком либо наиболее вычислительно сложных их частей [1]. Основная проблема организации вычислений в СБИС-архитектурах состоит в достижении пространственно-временного компромисса, то есть минимизации времени выполнения алгоритма при оптимальном использовании площади кристалла [2]. Такие особенности криптоалгоритмов, как ограниченный на-

бор криптопреобразований (базовых операций), возможности рекурсивной, конвейерной и потоковой обработки элементов массивов делают возможным их эффективное систолическое выполнение. В докладе предлагается методика проектирования СБИС-архитектур для аппаратной поддержки криптосистем, которая включает следующие этапы:

- Декомпозиция исходного криптоалгоритма и выделение набора базовых криптопреобразований.
- Проектирование систолических криптопроцессоров (базового набора СБИС) для реализации этого набора.
- Пространственно-временное согласование систолических криптопроцессоров при выполнении криптопреобразований большой размерности.
- Реализация криптосиситем произвольной размерности на основе базового набора СБИС в реальном времени.

ЛИТЕРАТУРА

1. *Zhang Chang N., Martin Herold L., Yun David Y.Y.* Parallel algoritms and systolic array design for RSA cryptosystem // Int. Conf. Sysolic Arrays, San Diego, Calif., Vay 25-27, 1988: Proc. - Washington (D.C.), 1988. P.341–350.
2. *Walter Colin D.* Space/time trade-off for higher radix modular multiplication using repeated addition//IEEE Trans. Comput. 1997. Vol.46. N2. P.139–141.