ЗАЩИТА КРИПТОГРАФИЧЕСКИХ УСТРОЙСТВ АЛГЕБРАИЧЕСКИМИ КОДАМИ ОБНАРУЖЕНИЯ МАНИПУЛЯЦИЙ

С.Б. Саломатин

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Рассматривается проблема обнаружения алгебраических манипуляций (AMD) [1] по каналу связи, который частично передает информацию противнику. Модель предполагает, что злоумышленник вычислительно неограничен, и между отправителем и получателем нет общего ключа или коррелированной случайности.

Криптографические методы внедрения ошибок. Усовершенствованная модель злоумышленника, в которой злоумышленник знает каждую деталь криптографического устройства, включая код обнаружения ошибок, используемый для защиты устройства. Злоумышленник может выбрать определенные входы для устройства во время атак с внедрением ошибок. Более того, злоумышленник также может внедрить любой конкретный шаблон ошибки на выходе устройства. В этом случае злоумышленник имеет полный контроль не только над ненулевой ошибкой, но также над безошибочным выходом y и ошибочным [2].

Определим архитектуру, которая по-прежнему может обеспечить гарантированную вероятность обнаружения ошибок в рамках приведенной выше модели злоумышленника, строго защищенной криптографической архитектурой.

Конструкции АМД-кодов, основанные на введении случайности в информационные биты кода. В кодовой архитектуре избыточные биты кода определяются не только выходом y исходного устройства, но и случайными данными x, сгенерированными генератором истинных случайных чисел, который по умолчанию встроен в большинство криптографических устройств для инициализации ключа [3]. В основе кодовых структур лежат обобщенные коды Рида–Маллера и Рида-Соломона. Криптографические устройства, защищенные кодами AMD, имеют высокую вероятность обнаружения ошибки (сбоя).

Список литературы

1. Cramer R., Dodis Y., Fehr S. [et al.] Detection of algebraic manipulation with applications to robust secret sharing and fuzzy extractors // Proceedings of the theory and applications of cryptographic techniques 27th annual international conference on Advances in cryptology, ser. EUROCRYPT'08. 2008. P. 471–488.

2. Bar-El, H., Choukri H., Naccache D. [et al.] The sorcerer's apprentice guide to fault attacks // Proceedings of the IEEE. 2006. Vol. 94, no. 2. P. 370–382.

3. Sunar B., Martin W.J., Stinson D.R. A provably secure true random number generator with built-in tolerance to active attacks // IEEE Trans. Comput. 2007. Vol. 56, no. 1. P. 109–119.