0.1. *Бучаев А.Я., Амаров А.А., Багандов А.М.* Аутентификация на основе физически неклонируемых функций

Информационная безопасность может быть надежно обеспечена только при условии применения средств защиты информации, в которых обеспечение секретности заключается в незнании злоумышленником некоторого секретного ключа. Секретность системы зависит от сложности ключей, и у злоумышленника не должно быть лучшей тактики для получения доступа к системе, чем полный перебор возможных значений ключей. При всех своих достоинствах, программно-аппаратные криптографические средства обладают одним существенным недостатком: энергонезависимая память вычислительной системы содержит секретный ключ. Данный факт позволяет злоумышленнику считать ключ при физическом доступе к вычислительной системе.

Физическая криптография, основанная на структурной сложности оптических и электронных физических систем, является одним из наиболее важных достижений в области защиты информации. В процессе производства элементов интегральной электроники неизбежны случайные технологические флуктуации, которые приводят к тому, что на микроуровне все интегральные элементы уникальны. Уникальность проявляется в том, что у идентичных с точки зрения топологии интегральных элементов электрофизические характеристики могут отличаться из-за вариации длины и ширины канала транзисторов, толщины подзатворного диэлектрика и др. Под физически неклонируемыми функциями (ФНФ) понимаются физические устройства, неотъемлемым свойством которых является неповторяемость (при изготовлении или моделировании, в том числе программном) некоторых их функций, свойств и характеристик. Важнейшим свойством ФНФ является то, что все измерения параметров устройства и формирование ключа происходит внутри ФНФ [1]. Ключ никогда не покидает устройства, но и не хранится в нем. С использованием этого ключа ФНФ, получив на вход запрос, выдает отклик, уникальный для данной системы.

Разработана методика аутентификации основанная на невоспроизводимости ФНФ [2], которая может быть использована при проверке оригинальности электронных устройств. Для этого в базе производителя регистрируются значения пар запрос-ответ ФНФ для случайных значений запросов, которые могут в дальнейшем использоваться для сравнения и однозначной идентификации ФНФ, являющеюся неотъемлемой частью устройства.

Список литературы

[1] Заливако С.С., Иванюк А.А. Использование физически неклонируемых функций для генерирования действительно случайных числовых последовательностей // Автоматика и вычислительная техника. 2013. № 3. С. 61–71.

[2] Mustafaev A.G., Buchaev A.Ya. A reliable authentication method for the Internet of Things devices // Intern. Conf. Inform. Tech. (InfoTech). Varna, Bulgaria, 2020. P. 1–3.