План статьи журнала «Современная электроника» №2, 2014

Алексей Смирнов, главный редактор,
Владимир Вычужанин, автор статьи
«СТА - ПРЕСС», издательство

Защита данных в ИТ – системах.

1. Использование аппаратных и программных средств в защите данных ИТ – систем.
2. Криптографические алгоритмы.
3. Классификация современных FPGA с точки зрения хранения информации.

Тезисы статьи журнала «Современная электроника» №2, 2014

Алексей Смирнов, главный редактор,
Владимир Вычужанин, автор статьи
«СТА - ПРЕСС», издательство

Защита данных в ИТ – системах.

В настоящее время защита данных в ИТ – системах осуществляется за счет совместного использования аппаратных и программных средств. Обычно второй вариант кажется более простым и привлекательным, однако из – за большого объема вычислений в алгоритмах шифрования/дешифрования применение программных средств ограничивается случаями, когда система рассчитана на одного пользователя/клиента.

Фактически единственным методом защиты от SPA и DPA атак является конструктивное решение криптографического модуля, которое не позволяет их производить. Без адекватной защиты FPGA не может быть обеспечена ее эффективная конструкционная безопасность или защита данных от SPA или DPA атак.

Современные FPGA с точки зрения хранения информации можно классифицировать следующим образом:

- ПЛИС с аутентификацией шифрования
- ПЛИС с битовыми потоками шифрования
- FPGA без криптографических функций