ПАК оценки защищенности ПЛИС от стороннего воздействия по электромагнитному излучению и энергопотреблению

Обнаружение уязвимостей программируемых логических интегральных схем к скрытым каналам утечки конфиденциальных данных

ПАК включает осциллограф, антенны для снятия сигнала, анализируемое устройство (ПЛИС - программируемую логическую интегральную схему) и разработанное ПО. Комплекс анализирует физические каналы утечки конфиденциальной информации при работе ПЛИС, в частности, электромагнитное излучение и колебания энергопотребления.
В основе работы лежит CPA-атака на основе подобранного открытого текста. Суть метода заключается в сборе данных электромагнитного излучения и энергопотребления, которые затем используются в качестве шаблонов для выявления корреляции с обрабатываемой информацией.

ЦЕННОСТНОЕ ПРЕДЛОЖЕНИЕ

Повышение безопасности продуктов, использующих ПЛИС, за счет аудита их физических особенностей, обеспечивающего объективный измерительный контроль и своевременное детектирование уязвимостей

ОБЛАСТИ ПРИМЕНЕНИЯ

Разработчики и производители электроники, криптографического оборудования, банковских терминалов, телекоммуникационного оборудования и другого оборудования с повышенными требованиями к безопасности

КОНКУРЕНТНЫЕ ПРЕИМУЩЕСТВА

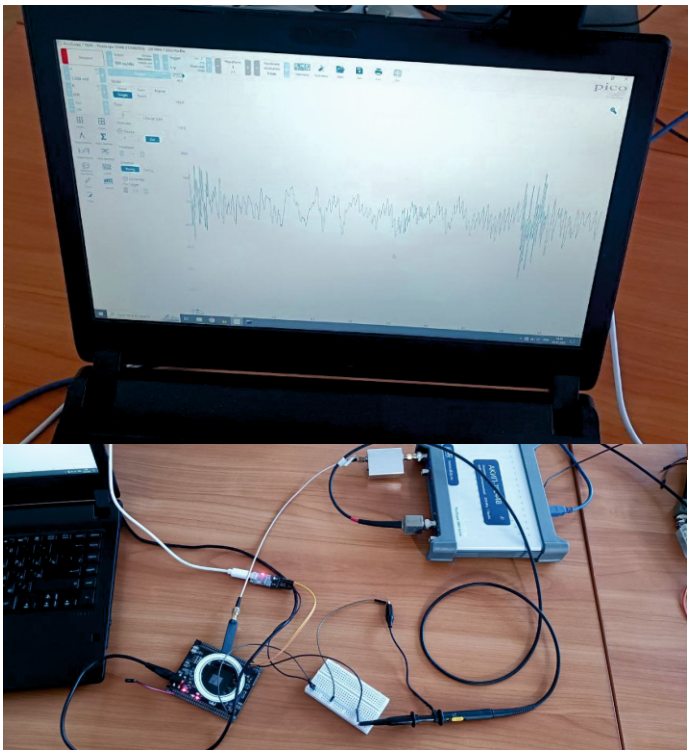
Высокая точность обнаружения уязвимости (87%)

СТАДИЯ РАЗРАБОТКИ

- Разработан ПАК по детектированию уязвимостей, на базе которого создан MVP
- Работа ПАК протестирована на атакуемой плате - QMTECH-XC7A100T_200T-CORE-BOARD

ОСНОВНЫЕ ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ

- Встроенное CPA-тестирование
- Время тестирования: 40 минут
- Кол-во трассировок – 40000
- Кол-во правильно вычисленных байт – 16
- Осциллограф: Picoscope 5244A



ПАК оценки защищенности ПЛИС