УДК 681.3

АНАЛИЗ ВОЗМОЖНОСТИ ПРОВЕДЕНИЯ АТАКИ НА АЛГОРИТМ ECDSA ЧЕРЕЗ ПОБОЧНЫЕ КАНАЛЫ С ИСПОЛЬЗОВАНИЕМ ДАННЫХ О ПОТРЕБЛЯЕМОЙ ВЫЧИСЛИТЕЛЬНЫМ ПРОЦЕССОРОМ МОЩНОСТИ

Магистрант ПСФ Короткевич О.С.,
кандидат техн. наук, доцент Артамонов В.А.
Белорусский национальный технический университет

Для осуществления атак на криптографические протоколы и алгоритмы в последнее время все чаще используются так называемые побочные каналы. Утечка информации через такие каналы чаще всего не предусматривается в классической модели безопасности протокола.

В данном докладе продемонстрирована возможность проведения атаки на аппаратное устройство, реализующее алгоритм ECDSA – стандарт создания электронной цифровой подписи, базирующийся на арифметике эллиптических кривых.

Как правило, для создания аппаратной реализации устройств шифрования и выработки ЭЦП используются логические элементы на базе КМОП технологии. Основываясь на физических принципах работы КМОП микросхем и получив доступ к ненадежному источнику питания, используемому аппаратным устройством для осуществления генерации ЭЦП, можно провести анализ потребляемой им мощности (см. рисунок).

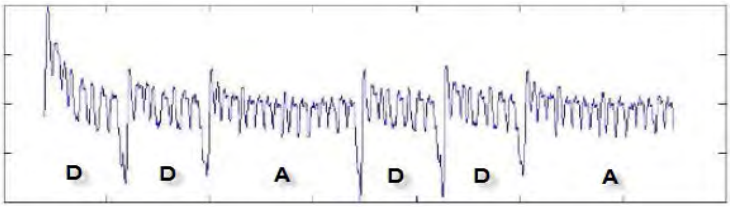

Рисунок – Потребление мощности устройством при проведении операции сложения (A) и удвоения (D) на эллиптической кривой

Допуская, что известны: модуль кривой P и подписываемое сообщение, можно, используя известный алгоритм, восстановить используемый закрытый ключ.

Помимо описания возможности проведения успешной атаки на алгоритм ECDSA с использованием данных о потреблении мощности аппаратным криптографическим устройством, в докладе предлагаются способы борьбы с уязвимостями такого рода.