ПРОТОКОЛ ОБМЕНА КЛЮЧАМИ С ИСПОЛЬЗОВАНИЕМ НЕЙРОННЫХ СЕТЕЙ

Е.А. Охрименко, В.А. Липницкий

В 2002 г. немецкие физики Кантер, Кинцель и Кантер предложили принципиально новый протокол обмена ключами между двумя абонентами, который предназначен для незащищенного от прослушивания, но защищенного от подмены данных канала связи. Он основан на хаотической синхронизации двух нейронных сетей особой конфигурации, называемых древовидными машинами четности (tree parity machine).

Можно провести аналогию между данным протоколом и алгоритмом обмена ключами Диффи–Хеллмана. в каждом из них абоненты начинают со случайных, несвязанных значений. Алгоритм Диффи–Хеллмана подразумевает единичный обмен данными, в результате которого стороны приходят к одинаковым значениям. Протокол ККК, в свою очередь, рассчитан на множество итераций обмена данными, на каждой из которых стороны узнают несущественную информацию о текущем состоянии друг друга, и, используя ее, обновляют свои состояния. В ходе итераций разница между значениями абонентов хаотично изменяется, однако имеет тенденцию снижаться, вплоть до полного исчезновения. Для стороны, наблюдающей за ходом синхронизации, состояния сторон являются быстро меняющимися целями, при этом он получает незначительную информацию о них. В частности, эмпирически установлено, что взломщик, который прослушивает все пересылаемые в ходе синхронизации сторон данные, обладает нейронной сетью той же конфигурации и использует аналогичное правило обновления, имеет очень низкую вероятность получить значения абонентов.

В 2004 г. Климов, Митягин и Шамир провели более детальный анализ рассматриваемого протокола и сделали выводы о том, что он является совершенно незащищенным, и может быть взломан, по крайней мере, 3-мя видами атак: геометрической, вероятностной, а также атакой с использованием генетического алгоритма.

В данном докладе проводится критическая оценка указанных выводов, основанная на независимых эмпирических исследованиях предложенных видов атак.