Q_j – число срабатываний j-го ФУ на одном цикле работы,

$$t^*(\chi_3(t(j,q)+\Delta t_j \cdot k)) = 1(t-(t(J,q)+\Delta t \cdot k+\tau))-1(t-(t(J,q)+\Delta t \cdot k)),$$

при $\tau \to 0$ – момент окончания интервала длительностью $t(j,k)+\Delta t \cdot k$, определяющий время q-го включения j-го ФУ на k-ом цикле его функционирования и вычисляемый по выражению (1) или (2). Здесь $1(.)$ – единичная функция Хевисайда.

Выражения (3) могут быть преобразованы к виду, удобному для их представления графом вычислительного алгоритма, последовательные преобразования которого методами теории графов (добавление вершин, элементарный гомоморфизм и др.) могут быть алгоритмизированы, что предоставляет возможности для автоматизации синтеза БУ АСКПП.

ЛИТЕРАТУРА

1 Воеводин, В.В. Математические методы и модели в параллельных процессах / В.В. Воеводин. - М.: Наука, 1986.

2 Кобайло, А.С. Основы теории синтеза вычислительных структур реального времени / А.С. Кобайло. - Минск: БГУИР, 2001.

УДК 681.3.006

Е.В. Лисица, магистрант; П.П. Урбанович, д-р техн. наук
(БГТУ, г. Минск)

МОДЕЛИРОВАНИЕ КРИПТОГРАФИЧЕСКИХ СИСТЕМ НА ОСНОВЕ НЕЙРОННЫХ СЕТЕЙ

Основная идея использования нейронных сетей в криптографии заключается в возможности синхронизации двух систем со случайным начальным набором весовых коэффициентов, в результате чего образуется общий для обеих систем вектор значений, который может быть использован в качестве секретного ключа в симметричных системах шифрования. Поскольку по общественным каналам передаются только входные и выходные значения двух сетей, то возможная атакующая сторона не в состоянии получить текущие значения их весовых коэффициентов, однако она также может попробовать синхронизировать свою сеть, на основе полученных данных.

Впервые идея использования нейронных сетей в криптографических системах – архитектура TPM (Tree Parity Machine, древовидная машина четкости) – была описана В. Кинцелем и И. Кантером в 2002 г. [1]. Позже А. Климовым, А. Митягиным и А. Шамиром была доказана безопасность этой системы только при простой атаке [2]. Для защиты протокола при геометрической атаке как минимум необходимо значительное увеличение синаптической глубины, что также

приводит к увеличению на порядок времени, необходимому для синхронизации. Таким образом, для обеспечения безопасности протокола при указанном способе атаки необходимы альтернативные способы защиты.

Одним из таких способов стала разработка М. Плонковски системы, использующей комплексные числа – протокол TPCM (Tree Parity Complex Machine, древовидная машина четкости на основе комплексных чисел). Проведенные исследования показали, что применение геометрической атаки опасно для процесса синхронизации сетей на основе архитектуры TPM, в то время как модель на основе TPCM характеризуется очень высокой степенью устойчивости к данному виду атак. Поскольку в основе процесса синхронизации лежит способность сетей к взаимообучению, актуальными также являются направления в изучении надежности протокола в зависимости от используемых правил обучения. Для экспериментального изучения эффективности и оценки надежности работы классического протокола TPM при различных параметрах: значений синаптических глубин, количестве персептронов, входных значений и правил обучения, – было создано программное средство [3]. В ходе исследований экспериментальным путем было найдено правило обучения «Modified rule» (модифицированное правило «Hebbian»), позволяющее защитить классическую архитектуру от геометрической атаки. В таблице представлены результаты надежности протокола при геометрической атаке и различных параметрах.

Таблица - Результат надежности протокола при геометрической атаке

Правило	Количество успешных атак	Параметры	Количество испытаний
Hebbian	31	K=3, N=5, L=3	100
	27	K=3, N=5, L=4	100
	25	K=3, N=5, L=5	100
Random walk	16	K=3, N=5, L=3	100
	10	K=3, N=5, L=4	100
	8	K=3, N=5, L=5	100
Modified rule	4	K=3, N=5, L=3	100
	1	K=3, N=5, L=4	100
	0	K=3, N=5, L=5	200
Примечание - K – количество персептронов, N – количество входов, L – значение синаптической глубины			

Таким образом, протокол Кинцеля-Кантера является безопасным при простой атаке. Для защиты протокола от геометрической атаки целесообразно использование архитектуры TPCM или архитек-

туры TPM с правилом обучения «Modified rule» и значением синаптической глубины больше 4.

ЛИТЕРАТУРА

1 W. Kinzel, I. Kanter. Interacting neural networks and cryptography. [Electronic resource]. – 2002. – Mode of access: http://theorie.physik.uni-wuerzburg.de/~ruttor/neurocrypt.html.

2 A. Klimov, A. Mityagine. Analysis of Neural Cryptography. [Electronic resource]. – 2003. – Mode of access: http://theorie.physik.uni-wuerzburg.de/~ruttor/neurocrypt.html.

3 D. Karchmarski, M. Plonkovski, E. Lisitsa. Methods and algorithms of modeling cryptographic systems based on neural networks technologies / D. Karchmarski // Proc. of the BSTU. - Mn: Proc. of the BSTU, 2008. - pp. 137-140.