УДК 661.3.06.004

Формирование криптографических ключей на базе нескольких алгоритмов без использования односторонних функций

Пивоваров В.Л., Голиков В.Ф.
Белорусский национальный технический университет

Задача конфиденциальной доставки ключевой информации в настоящее время решается методами ассиметричной криптографии, в основе которой лежит использование односторонних функций. Широкое применение нашел алгоритм прямого распределения ключей, предложенный Диффи и Хеллманом. Однако, несмотря на внешнее благополучие ассиметричной криптографии, развитие математической науки и компьютерной техники вносит существенные коррективы в ее параметры. Представляет интерес поиск других решений, которые в определенных ситуациях могут быть использованы как альтернативные.

И. Кантером и В. Кинцелем был предложен алгоритм формирования криптографических ключей с использованием синхронизируемых искусственных нейронных сетей. Основным недостатком названного метода является большое количество итераций, требуемое для полной синхронизации двух сетей.

Еще одним перспективным методом формирования криптографических ключей является алгоритм, предложенный в работе Ф Абдольванда. Недостатком данного метода является очень большая длина исходной последовательности по отношению к длине получаемого ключа. Так, для получения длины итоговой последовательности 128 бит требуемая длина исходной последовательности превышает 10^6 бит. Также предполагается, что в итоговой последовательности есть возможность определить значения некоторых бит на определенных позициях с вероятностью более 0,5.

Для того чтобы избавиться от недостатков двух описанных выше методов предлагается комбинированное решение, смысл которого заключается в том, что для независимого формирования «сырых» последовательностей у абонентов А и В, содержащих количество несовпадающих битов гарантированно менее 50%, использовать синхронизируемые искусственные нейронные сети.

Предлагаемый алгоритм нуждается в серьезном анализе криптостойкости и может найти применение, например, при формирования криптографического ключа для системы «точка-точка», имеющих аутентифицированный, но незащищенный от прослушивания канал связи или криптостойкой модификации устаревших ключей, распространенных другим способом.