количествах и располагаются исключительно по границам зерен, где находятся области кристаллизации аморфной анодной оксидной пленки. Увеличение формирующего напряжения более 160 В приводит к возрастанию числа пор, увеличению их диаметра, а при 220 В наблюдаемая поверхность имеет сходство с поверхностью пористых оксидных пленок. Полученные данные позволяют скорректировать максимальное напряжение формовки для получения бездефектного диэлектрика, содержащего редкоземельные металлы.

Анализ профиля распределения элементов анионов электролита в анодных оксидных пленках, содержащих иттрий, полученных при напряжении формовки 70 В и при различных pH, свидетельствует, что pH электролита практически не оказывает влияния на характер распределения P^{31} в анодной оксидной пленке. Наибольшее количество P^{31} фиксируется на поверхности пленки, далее оно несколько снижается и остается практически постоянным, на расстоянии, соответствующем 30% толщины оксида. Максимальное содержание Y^{89} при всех исследованных значениях pH фиксируется на поверхности пленок, а затем убывает, достигая минимума на глубине около 100 нм. Подобный характер распределения наблюдается в оксидных пленках с редкоземельными металлами, введенными методом термодиффузии и характеризует замещение алюминия иттрием в оксиде сложного состава.

ШИФРОВАНИЕ ДАННЫХ НА ОСНОВЕ ДИСКРЕТНЫХ ХАОТИЧЕСКИХ СИСТЕМ И ОТОБРАЖЕНИЙ

А.В. СИДОРЕНКО, К.С. МУЛЯРЧИК

Одним из перспективных направлений в современной криптографии является разработка и исследование алгоритмов шифрования на основе динамического хаоса. Динамический хаос и криптография имеют ряд общих фундаментальных свойств, среди которых чувствительность к начальным условиям и апериодичность траекторий в фазовом пространстве динамических систем, что позволяет реализовать такие свойства криптографических систем как запутывание и рассеяние.

Нами разработан алгоритм шифрования, основанный на использовании дискретных хаотических отображений, сети Фейстеля в качестве базового преобразования и четырех режимов работы алгоритма — ECB, CBC, CFB, OFB. Использование сети Фейстеля в алгоритме шифрования позволяет применять одно базовое преобразование для зашифрования и расшифрования, что повышает скорость работы алгоритма, снижает структурную сложность, а, следовательно, и потребность в вычислительных ресурсах.

В базовом преобразовании в качестве нелинейной функции используется дискретное хаотическое отображение. При этом выбор хаотического отображения приобретает принципиальное значение, что обусловлено необходимостью целочисленного представления информации.

Для анализа алгоритмов шифрования на основе динамического хаоса используются специализированные методы: метод задержанной координаты и метод построения фазовых диаграмм. Так, для зашифрованной последовательности вычисляются значения корреляционной размерности и энтропии Колмогорова. Данные параметры позволяют в динамике оценить область локализации и степень расходимости фазовых траекторий в пространстве и определить минимально необходимое число итераций базового преобразования, которое обеспечивает криптостойкость алгоритма.

Библиотека БГУИР