разделить на несколько характерных участков, характеризующих определенную область в АОП, каждая из которых имеет свою среднюю скорость травления. Можно выделить три характерных участка на кривых. Первый участок — вблизи границы раздела «оксид-электролит», второй участок, где ЭП постоянен и диэлектрическая пленка однородна по толщине и третий участок — вблизи границы раздела «оксид-металл».

Анализ полученных результатов позволяет говорить о том, что первый участок представляет собой область с максимальным количеством внедренных анионов. Причем в этой области наблюдается резкое уменьшение ЭП при приближении к границе раздела «оксид-электролит». Такой вид кривой характерен и для профиля распределения РЗМ в АОП. Скорость травления области АОП (Eu) в семь раз ниже, чем у АОП (Yb) и АОП (Gd). По мере травления первого участка АОП ЭП уменьшается и принимает значение –1,2 В, что соответствует потенциалу «чистого» оксида.

Исследования также показывают, что толщина однородного или «чистого» оксида зависит от состава электролита и его pH. Наибольшей толщине «чистого» оксида соответствует pH формовочного электролита 4,0 не зависимо от природы РЗМ, а наилучшим элементом с этой точки зрения является европий, у которого толщина однородной области составляет 74% при концентрации кислоты 1 масс. %.

ЛАВИННЫЙ ЭФФЕКТ В АЛГОРИТМАХ ШИФРОВАНИЯ НА ОСНОВЕ ДИСКРЕТНЫХ ХАОТИЧЕСКИХ ОТОБРАЖЕНИЙ

К.С. МУЛЯРЧИК

Одним из условий обеспечения стойкости алгоритма шифрования к дифференциальному криптоанализу, является наличие в преобразованиях лавинного эффекта. Суть эффекта заключается в значительном — «лавинном» — изменении бит в выходной последовательности преобразования при малом изменении («возмущении») бит во входной последовательности преобразования по сравнению с исходными («невозмущенными») значениями.

Выделяют несколько критериев стойкости алгоритма шифрования, основанные на лавинном эффекте: лавинный критерий (AVAL) — требует изменения в среднем половины бит в зашифрованном значении при изменении каждого отдельно взятого бита в исходном значении; строгий лавинный критерий (SAC) — требует изменения с вероятностью ½ каждого отдельно взятого бита в выходном значении при изменении каждого отдельно взятого бита во входном значении. При анализе алгоритма шифрования указанные критерии могут быть применены, в общем случае, как к S-блоку (таблице подстановки, дискретному отображению), так и к базовому преобразованию.

В данной работе представлены результаты исследования значений «лавинных параметров» — численные значения отклонения вероятностей изменения бит в выходной последовательности от требуемого значения, равного ½. Данные параметры являются более наглядной характеристикой степени лавинного эффекта в преобразовании.

В результате проведенных исследований — при анализе характера лавинного эффекта в паре «входное значение — выходное значение» обусловлен выбор базового преобразования в виде дискретного тент-отображения. Этот же вид хаотического отображения выбирается при анализе характера лавинного эффекта в паре «управляющий параметр — выходное значение» в процессе генерации раундовых ключей.