ходимо подчеркнуть, что здесь для исследователя открывается широкое поле деятельности. Например, в качестве этой процедуры могут быть использованы суммирование и произведение результатов девиртуализации каналов. В первом случае алгоритм формирования развернутого ключа принимает вид, представленный выражением (3), во втором – выражением (4)

$$K_r^M(i) = \prod_{j=1}^{M} DVIR_j(K_V^j(t)) : \quad (3)$$

$$K_r^M(i) = \sum_{j=1}^{M} DVIR_j(K_V^j(t)) \quad (4)$$

Реализация приведенных алгоритмов позволила создать программный комплекс шифрования, открывающий возможность обеспечения абсолютной недешифруемости. Исследования, проводимые в направлении совершенствования данного комплекса дают обнадеживающие результаты, представляющий научный и практический интерес. Приведенные результаты получены в ходе исследований при поддержке гранта Министерства образования РФ Т02-03.1-816.

Список литературы

1. Котенко В.В., Поликарпов С.В. Стратегия формирования виртуальных выборочных пространств ансамблей ключа при решении задач защиты информации // Вопросы защиты информации. 2002. №2. С.47 − 52.

## ШИФРОВАНИЕ С ПОСЛЕДОВАТЕЛЬНЫМ УСЛОЖНЕНИЕМ ВИРТУАЛЬНЫХ ВЫБОРОЧНЫХ ПРОСТРАНСТВ АНСАМБЛЕЙ КЛЮЧА

Котенко В.В., Румянцев К.Е, Поликарпов С.В., Левендян И.Б.
*Таганрогский Государственный Радиотехнический Университет, Таганрог*

Актуальность решения проблемы обеспечения абсолютной недешифруемости в современных условиях определяется неуклонным возрастанием роли информационных технологий. В последнее время в этом направлении наметился определенный прогресс. Так, в [1] была предложена стратегия решении данной проблемы на основе виртуализации выборочных пространств ансамблей ключа. Последующие исследования позволили получить ряд вариантов реализации данной стратегии. Одним из таких вариантов является шифрование, основанное на последовательном усложнении виртуальных выборочных пространств ансамблей ключа. Его основу составляет рекуррентный алгоритм (1) формирования виртуального ключа:

$$K_V^j(t) = VIR_j(DVIR_{j-1}(K_V^{j-1}(t))), j = 1...N \quad (1)$$

где

$VIR_j(\,.\,)$ – процедура виртуализации;

$DVIR_j(\,.\,)$ – процедура девиртуализации;

j – порядок уровня усложнения.

Полученный алгоритм предполагает многократную последовательную виртуализацию и девиртуализацию ансамбля ключа. При этом на каждом шаге виртуализации в качестве исходного ключа выступает результат девиртуализации виртуального ключа, полученного на предыдущем шаге. Начальным условием $DVIR_0(K_V^0(t))$ функционирования данного алгоритма является исходный ключ $K_{nd}(i)$, формируемый на основании заданных ключевых данных $K_d$:

$$DVIR_0(K_V^0(t)) = K_{nd}(i) . \quad (2)$$

Развернутый ключ $K_n^N(i)$ формируется путем девиртуализации виртуального ключа, полученного на конечном N-ом шаге усложнения:

$$K_n^N(i) = DVIR_N(K_V^N(t)) \quad (3)$$

На основании приведенного подхода было получено семейство способов шифрования с последовательным усложнением виртуального ключа, открывающих возможность обеспечения абсолютной недешифруемости. Реализация данных способов позволила создать программный комплекс шифрования, обладающий уникальными возможностями. Экспериментальные исследования показали высокую надежность и эффективность данного комплекса.

Приведенные результаты получены в ходе исследований при поддержке гранта Министерства образования РФ Т02-03.1-816.

Список литературы

1. Котенко В.В., Поликарпов С.В. Стратегия формирования виртуальных выборочных пространств ансамблей ключа при решении задач защиты информации // Вопросы защиты информации. 2002. №2. С.47 − 52.

## ЭЛЕКТРОХИМИЧЕСКАЯ РАЗМЕРНАЯ ОБРАБОТКА ПОЛИГОНАЛЬНЫМ КАТОДОМ

Котляр Л.М., Миназетдинов Н.М., Хайруллин А.Х.
*Камский государственный политехнический институт, Набережные Челны*

Электрохимическая размерная обработка металлов – один из современных методов изготовления деталей из металлов и сплавов с заданной формой, размерами и качеством поверхности. Метод основан на принципе локального растворения анода – обрабатываемой заготовки в проточном электролите. Роль катода – обрабатывающего инструмента выполняет электрод с заданной геометрической формой поверхности. Протекание электрохимических процессов обеспечивается прокачкой раствора электролита через межэлектродный промежуток (МЭП) с целью выноса из зоны обработки продуктов реакции (газа, шлама) и выделившегося тепла

Наличие в задаче неизвестной границы приводит к большим трудностям, связанными с учетом изменения параметров задачи, для определения которых необходимо знать полную геометрию границ области. В связи с этим, в качестве первого приближения в теоретическом анализе процесса ЭХРО используется модель идеального процесса. Согласно этой модели, для условий ЭХРО постоянным током, электрическое поле в межэлектродном промежутке можно считать потенциальным, т.е. $\vec{\mathbf{E}} = -\operatorname{grad} u$, где $\vec{\mathbf{E}}$ - вектор напряженности электрического поля, $u$ - потенциал электрического поля. В идеальном процессе ЭХРО электрическое поле может быть описано уравнением Лапласа $\nabla^2 u = 0$. Значения потенциала $u_a$, $u_k$ на поверхности анода и катода величины постоянные.

В стационарном режиме форма обрабатываемой поверхности в подвижной системе координат, связанной с катодом, не изменяется. Это означает, что поверхность анода перемещается вместе с катодом с постоянной скоростью $V_k$. В этом случае линейная скорость анодного растворения $V_a = \eta \varepsilon i / \rho$ по нормали к поверхности анода в любой точке анода будет равна:

$$V_a = V_k \cdot \cos(\theta) = (\vec{\mathbf{V}}_k, \vec{\mathbf{n}}_a), \quad (1)$$

где $\theta$ угол между вектором скорости $\vec{\mathbf{V}}_k$ подачи катода и единичным вектором $\vec{\mathbf{n}}_a$ внешней нормали к аноду.

При постановке и решении задач ЭХРО используется гидродинамическая аналогия электрического поля, согласно которой плоское потенциальное электрическое поле моделируется фиктивным течением идеальной несжимаемой жидкости. При этом потенциалу поля ставиться в соответствие функция тока фиктивного течения, силовой линии электрического поля – эквипотенциальная линия. Если ввести комплексный потенциал электростатического поля $W = \varphi + i\psi$, где $\psi$ безразмерный потенциал электрического поля, то вдоль линии $\psi = const$ имеем $\partial\psi/\partial n = V$, где, в случае гидродинамической интерпретации задач ЭХРО, $\vec{\mathbf{V}}$ - вектор скорости фиктивного потока идеальной несжимаемой жидкости. Угол наклона скорости к оси абсцисс с точностью до знака совпадает с углом $\theta$. Тогда условие (1) имеет вид

$$V = a + b\cos\theta \quad (2)$$

и определяет годограф скорости указанного течения на неизвестной анодной границе, здесь $a, b$ - постоянные коэффициенты [1]. Гидродинамическая аналогия облегчает формулировку краевых задач теории ЭХРО и позволяет применять методы расчета, разработанные при решении задач гидродинамики.

Рассматривается плоская задача теории электрохимической размерной обработки металлов, состоящая в нахождении формы анодной границы, при электрохимической размерной обработке металлов полигональным катодом в установившемся режиме. Для решения задачи вводится прямоугольная система координат $x_1$, $y_1$, связанная с катодом-инструментом и считается, что движение катода осуществляется в направлении оси ординат.

В односвязной области плоскости $z = x + i\,y$ рассмотрим фиктивное течение идеальной жидкости, ограниченное твердой полигональной стенкой, соответствующей границе катода $\Gamma_k$, и свободной поверхностью, соответствующей анодной границе.

Пусть в плоскости вспомогательного комплексного переменного $t = \xi + i\eta$ области течения конформно соответствует область $D_t = \{|t| \le 1, \operatorname{Im} t \ge 0, \operatorname{Re} t \ge 0\}$, причем свободной поверхности соответствует дуга окружности $t = e^{i\sigma}$, $\sigma \in (0, \pi/2)$. Будем искать функцию $z(t)$, конформно отображающую область $D_t$ на область течения, причем точкам $z_m$ на полигоне, в которых скачком меняется направление вектора скорости, соответствуют точки $t_m = \xi_m$. Чтобы построить $z(t)$, достаточно найти производную комплексного потенциала $W(t)$ в плоскости вспомогательной переменной $t$ и функцию Жуковского

$$\chi(t) = \ln\left(\frac{1}{V_0}\frac{dW}{dz}\right) = r - i\theta, \quad r = \ln V/V_0,$$

где V – модуль скорости фиктивного течения, $V_0$ - значение V на бесконечности в точке A, $\theta$ - угол наклона вектора скорости к оси $x$, который равен (с точностью до знака) углу между вектором скорости $\vec{\mathbf{V}}_k$ подачи катода и вектором внешней нормали к аноду. На свободной поверхности из условия (2) получим граничное условие, связывающее вещественную и мнимую части функции $\chi(t) \quad (t = e^{i\sigma})$

$$V_0\, e^{r(\sigma)} = a + b\cos\theta(\sigma). \quad (3)$$

Будем искать функцию $\chi(t)$ в виде суммы $\chi(t) = \chi_*(t) + f(t)$, где $\chi_*(t) = r_* + i\theta_*,$. $r = \ln V_0/V_*$ - функция Жуковского для течения по той же схеме, но с условием $V_* = V_0$ на аноде, а $f(t)$ - аналитическая в $D_t$ и непрерывная в $\overline{D_t}$ функция.

Функцию $f(t)$, дающую решение краевой задачи можно представить в виде ряда

$$f(t) = \frac{1+t^2}{2}\sum_{k=0}^{\infty} c_{2k} \cdot t^{2k},$$ где $c_{2k}$ - вещественные постоянные, множитель введен для учета граничного условия $\operatorname{Re} f(i) = 0$.

В частном случае при обработке двугранным катодом-инструментом, функции $\chi_*(t)$ и $dW/dt$ имеют следующий вид

$$\chi_*(t) = -2(\alpha+\beta)\ln t + \beta\pi i,$$
$$dW/dt = 8t/\left(\pi\left(1-t^4\right)\right).$$

Для численного решения задачи задаются геометрические параметры $\alpha, \beta$ ,параметры $a, b$ характеризующие свойства электролита. Численные расчеты формы обрабатываемой границы для этого частного случая проведены при следующих значениях параметров:

$\alpha = 0.25, \beta = 0.25$ .1) – a=-0.301, b=2.401; 2) – a=-0.205, b=1.865; 3) – a=0.21, b=1.28; 4) – a=-0.127, b=1.467; 5) – a=0.141, b=1.104; 6) – a=0.077, b=0.931.

Список литературы

1. Котляр Л.М., Миназетдинов Н.М. Определение формы анода с учетом свойств электролита в задачах электрохимической размерной обработки металлов. //Прикладная механика и техническая физика, 2003, Т. 44, №3, С. 179-184

## ЭФФЕКТИВНОСТЬ ПРОТОКОЛА КВАНТОВОЙ КРИПТОГРАФИИ BB84 С КОДИРОВАНИЕМ ОДНОФОТОННЫХ СОСТОЯНИЙ ПО ОТНОСИТЕЛЬНОЙ ФАЗЕ

Румянцев К.Е., Хайров И.Е., Клочко К.В.
*Таганрогский государственный радиотехнический университет, Таганрог*

В основе наиболее распространенных криптографических систем положен принцип защиты, заключающийся в большой трудности расшифровывания криптограмм и требующих больших вычислительных мощностей. Однако они полностью не исключают возможность расшифровки криптограмм. Одним из наиболее перспективных и достаточно новых направлений в области криптографии является квантовая криптография. В отличие от большинства классических криптосистем, защищенность которых основывается на недоказанных математических предположениях, защищенность квантовых криптографических систем опирается на фундаментальные законы квантовой механики, что при надлежащей реализации таких систем делает принципиально невозможным чтение передаваемых сообщений третьими лицами. Как показывают исследования в данной области, сочетание квантово-криптографических методов распределения секретного ключа и классических методов шифрования позволит создать фундаментально защищенные системы передачи конфиденциальной информации.

Одним из наиболее распространенных в настоящее время протоколов квантовой криптографии является протокол BB84. В данном протоколе однофотонные состояния могут быть промодулированы по поляризации или по относительной фазе. Каждый из этих методов модуляции имеет свои преимущества и недостатки. В частности, поляризационная модуляция наиболее предпочтительна при передаче данных по открытому оптическому каналу, в то время как модуляция по относительной фазе может быть использована в волоконно-оптических системах связи. В случае модуляции фотонов по относительной фазе данный протокол использует 4 фазовых состояния. При этом в зависимости от разности фаз однофотонных импульсов передающего и приемного модулей возможна конструктивная, либо деструктивная интерференции, что определяет передаваемый бит информации.

Проведенные исследования методов съема информации в квантовых каналах с кодированием однофотонных импульсов по относительной фазе позволили выявить наиболее эффективные из них и сформулировать требования к методам защиты. Одним из методов съема является "мощная импульсная атака" [1], при которой нет необходимости напрямую взаимодействовать с квантами света. Следовательно, фазовые системы "Plug&Play" являются уязвимыми по отношению к атакам типа "Троянский конь" [1]. Действительно, Ева может послать сканирующий импульс для выяснения текущего состояния фазового модулятора Алисы (или Боба) и получить его обратно из-за сильного отражения, вызванного зеркалом на конце установки. Для предотвращения подобных видов атак Алиса устанавливает у себя аттенюатор для уменьшения количества света, проходящего через систему. Однако очевидно, что при внесении слишком сильного ослабления система сама окажется неработоспособной. Кроме того, необходимо отслеживать интенсивность принимаемого света при помощи классического детектора, чтобы отследить факт возможной атаки [1].

Так же недостатком системы "Plug&Play" является то, что они не могут работать с настоящими однофотонными источниками и, следовательно, не будут выигрывать от продвижений в области создания таких источников.

Таким образом, проведенные исследования подтвердили актуальность разработки новых методов противодействия атакам в квантовых каналах.

The bibliographic list

1. Vakhitov A.V., Makarov V., Hjelme D.R. Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography // Journal of modern optics. 2001.vol. 48. №13. p. 2023-2038.

## АНАЛИЗ ЭФФЕКТИВНОСТИ РЕАЛИЗАЦИИ ГОРОДСКОЙПРОГРАММЫ «ЭНЕРГОСБЕРЕЖЕНИЕ»

Тур В.И., Кузин Г.А., Кузина Г.М.
*АНО ОС «Ульяновскстройсертификация», Ульяновск*

Потенциал энергосбережения в России, по оценке специалистов, составляет 35% от уровня энергопотребления. Около 32% этого потенциала сосредоточено на хозяйствующих субъектах топливно-энергетического комплекса, еще столько же в промышленности, почти 20% в коммунально-бытовом секторе.

Федеральный закон «Об энергосбережении» определяет энергосбережение как реализацию правовых,