

поле служит для разделения зарядов и их фокусировки, так как скорость частиц вблизи горизонта может быть сколь угодно близка к скорости света. Таким образом, из окрестностей сверхмассивной черной дыры выбрасываются электронный протонный джеты в противоположных направлениях. В отличие от моделей, представленных в [3], данная модель обладает простотой, использует более реалистичные допущения и ее основные положения подтверждаются экспериментально на других астрофизических системах.

### **Литература**

1. *Ferrarese L., Ford H. C.* Supermassive Black Holes in Galactic Nuclei: Past, Present and Future Research // *Mon. Not. Roy. Astron. Soc.* 2004. Vol. 351. P. 1187.
2. *Bekenstein J. D.* Black Holes: Physics and Astrophysics // Preprint astro-ph/0407560. 2004.
3. *Wang R.-Y., Ye Y.-C., Ma R.-Y.* A Toy Model for Magnetic Extraction of Energy from Black Hole Accretion Disc // *New Astron.* 2004. Vol. 9. P. 585-597.
4. *Chakrabarty S.K.* Study of Accretion Processes on Black Holes // Preprint astro-ph/0402562. 2004.
5. *Ландау Л. Д., Лифшиц Е. М.* Теоретическая физика. Теория поля, Т. 2. М.: Наука, 1988.
6. *Мизнер Ч., Торн К., Уилер Дж.* Гравитация. М.: Мир, 1977. Т. 1, Т. 2, Т. 3.

## **РАЗРАБОТКА ПОТОЧНОГО КОДЕРА НА ОСНОВЕ ХАОТИЧЕСКОГО ШИФРОВАНИЯ**

**А. Г. Потапенко**

### **ВВЕДЕНИЕ**

При сетевой передаче конфиденциальных данных важно обеспечить их безопасность и целостность. Особенно это актуально для систем мобильной, сотовой связи. Используемые в таких системах криптографические алгоритмы шифрования (блочные и поточные) должны быть быстродействующими и надежными.

Поточные шифры, как правило, имеют более высокое быстродействие, чем блочные шифры, при этом аппаратно реализуются менее сложно [1]. Поточные шифры обладают преимуществом в случае, если буферизация данных ограничена и высока вероятность возникновения ошибок. При этом символы данных должны обрабатываться отдельно.

В последнее время широкое распространение получили поточные способы шифрования, основанные на использовании хаоса (например, полиморфный способ шифрования [2]).

Для хаотических шифров важны следующие проблемы.

1. Скорость шифрования. По сравнению с традиционными алгоритмами у большинства хаотических шифров скорость меньше [3]. Существует несколько разных способов объяснить эту проблему. Это неоднократные итерации для шифрования, использование арифметики с плавающей точкой и сложных хаотических отображений.

2. Используемое хаотическое отображение. Большинство хаотических шифров должны использовать особые хаотические отображения для гарантии безопасности, что ограничивает их дальнейшее использование. Желательно, чтобы хаотический шифр мог хорошо функционировать с большим числом хаотичных отображений.

3. Реализация алгоритмов аппаратным или программным способом. Хороший хаотический шифр будет хорошо реализовываться как аппаратно, так и программно с низкой стоимостью.

В данной работе представлены результаты разработки кодера на основе хаотического шифрования. При этом задачами разработки являлись: максимизация скорости шифрования; обеспечение достаточной стойкости по отношению к современным видам криптоанализа; создание генератора потока гаммы ключа, который близок по показателям к одноразовому блокноту.

### **ПОТОЧНЫЙ КОДЕР НА ОСНОВЕ ПОЛИМОРФНОГО СПОСОБА ШИФРОВАНИЯ**

В основу кодера был положен полиморфный способ шифрования [2], т.к. он обладает высокими показателями криптостойкости и скорости шифрования.

Кодер является симметричным. При зашифровании входной поток формируется из байтов открытого текста. При расшифровании входной поток формируется из байтов шифртекста. В выходном потоке образуется открытый текст. Блок обратной связи связан с шифртекстом.

Блоки кода представляют собой наборы определенных инструкций. Счетчик вызывает процедуру шифрования символа. Датчик псевдослучайных чисел рандомизирует процесс шифрования.

### **ОПИСАНИЕ АЛГОРИТМА И ПРОГРАММНОЙ РЕАЛИЗАЦИИ КОДЕРА**

Зашифрование происходит путем сложения по модулю два битов открытого текста и битов массива внутреннего состояния кодера. Расшифрование происходит аналогично, но с битами шифртекста.

Массив внутреннего состояния кодера первоначально заполняется с помощью основного генератора псевдослучайных чисел. Затем происходит срабатывание алгоритма некоторое количество раз, которое зависит

от ключевой фразы, без шифрования (для увеличения криптостойкости). В итоге данные массива рандомизируются. В процессе шифрования, после обработки определенного числа битов, данные гаммы циклически сдвигаются и при этом изменяются с помощью одного из блоков инструкций.

Блоки инструкций представляют собой перестановки, замены и генераторы псевдослучайных чисел. Блоки вызываются с помощью основного датчика псевдослучайных чисел старшими битами выдаваемых чисел. При срабатывании функции обратной связи биты инвертируются. Таким образом, действительный алгоритм оказывается практически непредсказуемым.

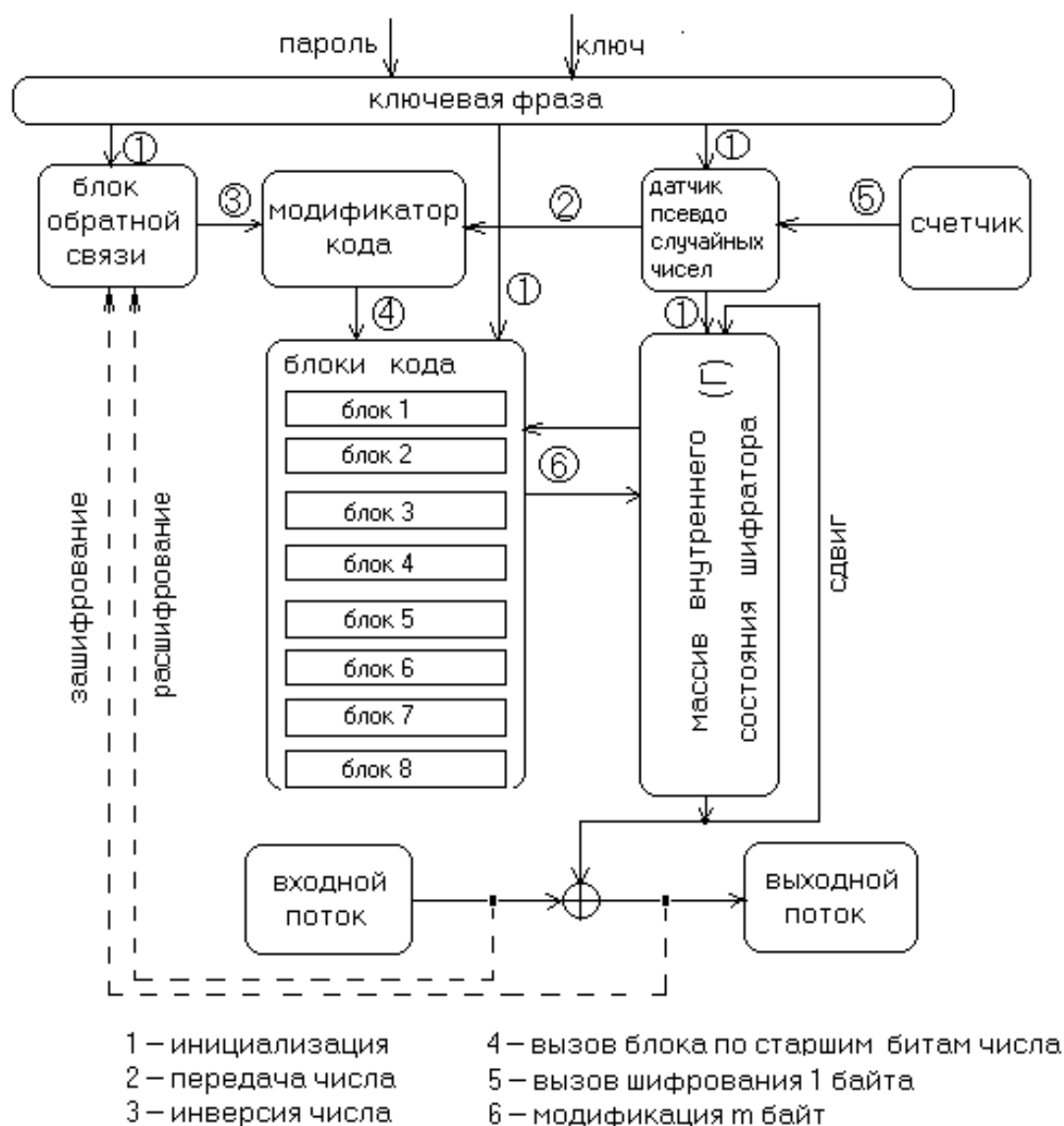


Рис. 1. Функциональная схема кодера

Обратная связь возникает в том случае, если в определенном количестве байтов шифртекста встречается комбинация символов, которая зависит от ключевой фразы.

Полиморфное поведение реализуется с помощью динамического связывания [4]. Т.е. имеется абстрактный базовый класс с чисто виртуальной функцией, предназначением которой является изменение данных массива внутреннего состояния кодера. Классы-потомки реализуют в рамках этой функции какой-либо блок инструкций (блок замены, блок перестановки, блок-генератор псевдослучайных чисел или их комбинация). Затем создаются указатели базового класса на объекты производных классов. Таким образом, при вызове функции абстрактного базового класса выполняются функции классов-потомков.

Моделью потока служат два файла.

На рис.2 изображен результат работы кодера по зашифрованию открытого текста, состоящего из нулевых битов.

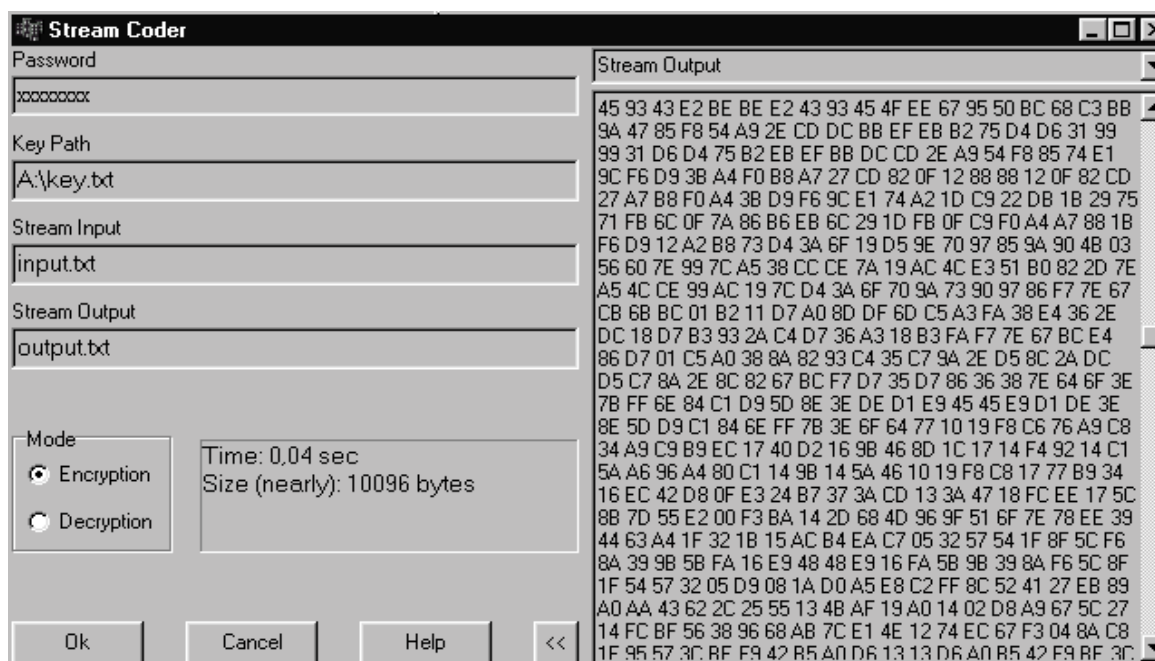


Рис.2. Окно программы

## ЗАКЛЮЧЕНИЕ

В данной работе были представлены некоторые результаты разработки кодера на основе хаотического шифрования с использованием полиморфного способа шифрования. Свойства полиморфизма позволяют обеспечить адаптивную перестройку, что ведет к некоторому усложнению алгоритма и повышению его криптостойкости, но без существенного уменьшения быстродействия.

Были кратко описаны алгоритм и программная реализация, выполненная на языке C++ с использованием среды Borland C++ Builder 6. В результате тестирования получены оценочные показатели скорости шифрования: 1,9 МБит/с на процессоре Celeron 333 МГц.

#### Литература

1. Menezes A., Van Oorschot P. Handbook of applied cryptography. CRC Press, 1996.
2. Roellgen. The polymorphic cipher. <http://www.pmc-ciphers.com>.
3. Li S., Zheng X. Chaotic encryption scheme for real-time digital video. <http://citeseer.ist.psu.edu>.
4. Дейтель Х., Дейтел П. Как программировать на C++. М., 1998.

### ИССЛЕДОВАНИЕ СЕГРЕГАЦИИ GE И SN В СТРУКТУРЕ SiO<sub>2</sub>/Si

С. Л. Прокопьев, А. Г. Новиков, К. В. Яцко

#### ВВЕДЕНИЕ

Кремний является базовым материалом современной микроэлектроники, что связано с удачным сочетанием ряда физических и технологических параметров. Вместе с тем, дальнейшее развитие кремниевой микроэлектроники требует, в частности, поиска новых способов внутрисхемных коммуникаций. Одним из возможных путей решения этой проблемы является использование оптоэлектронных элементов. Кремний является непрямозонным материалом с низким квантовым выходом, поэтому в настоящее время ведется интенсивный поиск новых прямозонных материалов, совместимых с кремниевой технологией.

В ряде работ было установлено, что недеформированные сплавы  $Ge_{1-x}Sn_x$  в определенном композиционном интервале могут иметь прямую запрещенную зону. Так, в теоретических работах [1] показано, что прямая запрещенная зона характерна для сплава  $Ge_{1-x}Sn_x$  при  $0,09 < x < 0,15$ . Указанные выводы теоретических расчетов затем подтверждены экспериментально. В частности, в работе [2,3] было установлено, что сплавы  $Ge_{1-x}Sn_x$  в композиционном интервале  $0,09 < x < 0,15$  являются прямозонными. В дополнение к этому в работе [2] с использованием метода измерения коэффициента поглощения ИК излучения подтверждено наличие прямой зоны для сплавов  $Ge_{1-x}Sn_x$  в интервале  $0,035 < x < 0,115$ . Суммируя указанные результаты, можно предполагать, что сплавы  $Ge_{1-x}Sn_x$  в композиционном интервале  $0,035 < x < 0,15$  являются перспективными для применения в электронике, базирующейся на Si и соединениях SiGe. Таким образом, цель настоящей работы заключалась в исследовании воз-