УДК 621.391:519.72

АНАЛИТИЧЕСКОЕ ОБОСНОВАНИЕ ИСПОЛЬЗОВАНИЯ GFSR-ГЕНЕРАТОРОВ В ЗАДАЧАХ КРИПТОГРАФИИ

Казакова Н. Ф.

АНАЛІТИЧНЕ ОБГРУНТУВАННЯ ЩОДО ЗАСТОСУВАННЯ GFSR-ГЕНЕРАТОРІВ В ЗАДАЧАХ КРИПТОГРАФІЇ

Казакова Н. Ф.

ANALYTICAL BASIS FOR USE GFSR-GENERATOR IN THE TASKS OF CRYPTOGRAPHY

Kazakova N.

Проведено аналіз проблем, пов'язаних з теоретичним та практичним обґрунтуванням принципів побудови комбінованих генераторів псевдовипадкових послідовностей на основі регістрів зсуву з узагальненим зворотнім зв'язком. Визначено проблеми, які пов'язані з проектуванням та оцінкою якості рекурентних генераторів псевдовипадкових послідовностей комбінованого типу, які об'єднують рекурентні способи формування шифруючих послідовностей з нелінійною фільтрацією вихідного потоку.

Ключові слова: потоковий шифр, комбінований генератор, фільтр з пам'яттю, GFSR-генератор, вихор Мерсенна

Проведен анализ проблем, связанных с теоретическим и практическим обоснованием принципов построения комбинированных генераторов псевдослучайных последовательностей на основе регистров сдвига с обобщенной обратной связью. Определены проблемы, связанные с проектированием и оценкой качества рекурентных генераторов псевдослучайных последовательностей комбинированного типа, которые объединяют рекуррентные способы формирования шифрующих последовательностей с нелинейной фильтрацией выходного потока

Ключевые слова: потоковый шифр, комбинированный генератор, фильтр с памятью, GFSR-генератор, вихрь Мерсенна

1. Вступление

Генераторы (ГН) псевдослучайных последовательностей (ПСП) применяются в задачах криптографии и моделирования. Они являются частью многих криптографических систем: формирование ключей, шифрование сообщений и т.д. Их эффективность при моделировании доказана давно. Что касается криптографии, то

здесь требования к равномерности распределения вероятностей формируемых чисел выше [1-3]. Этим определяется тот факт, что в настоящее время в этой области появилось большое число новых идей и подходов. Ранее для формирования ПСП использовались различные методы, среди которых наиболее значимый основан на линейных сдвиговых регистрах с обратной связью (англ.: *Linear Feedback Shift Register* – LFSR). Они экономичны, поскольку для реализации применяют сдвиговые, логические и линейные операции. Однако, для обеспечения заданной криптографической стойкости в их состав необходимо введение нелинейных функций и, т.о., они представляют собой некоторый инженерный компромисс между указанным подходом и ГН со сложными нелинейными преобразованиями. Следовательно, обоснованием актуальности является анализ проблем, связанных с проектированием и оценкой качества рекуррентных ГН ПСП комбинированного типа [1, 2, 8], объединяющих рекуррентные способы формирования шифрующих последовательностей с нелинейной фильтрацией выходного потока [3].

2. Анализ литературных данных и постановка проблемы

В [5] сказано, что многие алгоритмы не обеспечивает приемлемой равномерности распределения вероятностей чисел, формируемых на выходе ГН ПСП. Там же приведен анализ проблем, связанных с усовершенствоанием алгоритмов, построенных на основе LFSR, а также краткая аннотация по нелинейным алгоритмам. Показано, что к ГН 1-го типа применениима некоторая общая математическая теория, а в основу алгоритмов 2-го типа заложены обособленные математические задачи. В [4-8] показано, что поскольку экономия вычислительных ресурсов, криптостойкость и производительность формирования ПСП являются наиболее актуальными задачами, разработчики потоковых систем шифрования склонны к построению алгоритмов, сочетающих достоинства линейных и нелинейных преобразований. Исходя из этого и учитывая [1-3], целью является выявление наиболее перспективных способов построения составных устройств, представляющих компромиссное сочетание между LFSR и ГН с нелинейными мультипликативными фильтрами, обладающими собственной конечной памятью.

3. Результаты исследований

Известно [1-3], что большинство потоковых шифров используют LFSR. Проблема лежит в том, что их программная реализация неэффективна [6]: при выборе образующих полиномов необходимо избегать разреженных многочленов обратной связи, которые облегчают их корреляционное вскрытие. Так, например, учитывая, что выход потокового шифра – побитовый, то такой алгоритм как DES, за одну итерацию шифрует столько же текста, сколько потоковый шифр – за 64 итерации.

Целесообразным является в качестве ячеек регистра рассматривать не битовые ячейки, а блоки памяти, равные по размеру величине машинного слова w. Обычно $w = 32$. Такие ГН являются регистрами сдвига с обобщённой обратной связью (англ.: *Generalized Feedback Shift Register* – GFSR). В их основе лежит тезис о том, что для удобства анализа, всякий рекуррентный ГН может быть пред-

ставлен как автомат с памятью $A=(S,F,O,o)$ с конечным числом состояний без входа, где S – конечное множество его состояний, отображение $f:S\to S$ – это функция переходов из текущего состояния в следующее, O – набор символов выходного алфавита и $o:S\to O$ – это выходная функция, отображающая его внутренние состояния в символы выходного алфавита. Вид формируемой последовательности определяется начальным состоянием автомата s_0, а переходы в следующие состояния происходят в соответствии с рекуррентным соотношением $s_i=f(s_{i-1})(n=1,2,3,...)$, где при этом $o(s_0),o(s_1),o(s_2),...\in O$.

Задание начального состояния GFSR-генератора – отдельная проблема. Так, генератор, основанный на «вихре Мерсенна» [7], требует заполнения 623 w-битных ячеек памяти. Для этого необходимо использовать отдельный ГН-инициализатор, формирующий на основе некоторой функции инициализации $\text{init}:K\to S$ значение $s_0=\text{init}(k_i)$ из ключа $k_i\in K$, где K – пространство ключей. Обычно эта проблема решается путем выбора линейной функции перехода в двоичном поле Галуа $GF(2)$.

Чтобы получить безопасный ГН с наибольшим периодом T, желательно, чтобы функции f и o были достаточно сложными. Однако для сложной функции f, анализ ее периода и распределения вероятностей в выходной последовательности представляет собой сложную задачу. Поэтому сначала определяют пространство состояний ГН – $S=GF\left(2^w\right)^n$, где n – степень образующего полинома GFSR, а, затем, выбрают функцию перехода f, период которой может быть определен методами линейной алгебры в полиномиальном исчислении. В общем случае, для GFSR, построенного на основе образующего полинома степени n, число его внутренних состояний равно $2^{wn}-1$. Линейное отображение множества состояний ГН во множество его выходных слов $g:GF\left(2^w\right)^n\to GF\left(2^w\right)$ есть функция обратной связи, а его переход из одного состояния в другое, эквивалентен рекурсии $x_{i+n}=$ $=g(x_i,x_{i+1},...,x_{i+n-1})$, $i=0,\ 1,\ 2,\ ...$. При этом выход GFSR задается отображением $o:S\to GF\left(2^w\right),\ (x_1,...,x_n)\to x_1$, которое не является секретным.

Оценка нелинейности функции определяется ее алгебраической степенью, под которой понимается полиномиальная булева функция $h(c_1,c_2,...,c_n)$ с переменными из поля $GF(2)$, определяемая как $h:GF\left(2^n\right)\to GF(2)$ или $h=\sum_{i\subset\{1,2,...,n\}}a_ic_i$, где $a_i\in GF(2)$, а c_i – это состояния ячеек памяти GFSR [7, 9].

Для достижения высокой производительности ГН, преобразованию o_i недостаточно количества доступных бит, составляющих состояния s_i и, кроме того, алгебраическая степень такого преобразования, также ограничивается числом доступных бит. Это уменьшает достоинства большого пространства состояний S.

Проблема решается введением в состав ГН дополнительного конечного автомата с входом, представляющим собой фильтр с памятью, который, в отличие от автомата без входа, может быть представлен в виде кортежа $A=(S,U,f,O,o)$, где компоненты S, f, O и o имеют те же значения, что и в случае автомата без входа, а U есть множество символов входного алфавита. При этом функция переходов имеет вид $f:U\times S\to S$. При начальном состоянии s_0 и входной последовательности $u_0,u_1,...\in U$, изменения внутреннего состояния автомата с входом определяется рекурсией $s_i=f\left(u_{j-1},s_{j-1}\right),\ (i=1,2,3,...)$.

Формально, комбинированный ГН с фильтром можно описать следующим образом. Пусть автомат без входа $A_M=(S_M,f_M,O_M,o_M)$ – это основной ГН на основе GFSR, порождающий некоторую ПСП. Автомат с входом $A_F=(S_F,U_F,f_F,O_F,o_F)$ будем использовать, как фильтр с памятью. Поскольку символы ПСП поступают на вход фильтра, алфавиты O_M и U_F совпадают, то $O_M=U_F$. Для формирования выходной последовательности следует инициализировать и основной ГН и фильтр. Для этого требуется пара начальных состояний $s_{M,0}\in S_M$ и $s_{F,0}\in U_F$. Фильтр A_F преобразует выходную последовательность основного ГН o_M в собственную выходную последовательность o_F. В итоге, вся конструкция в целом является автоматом C без входа, т.е. комбинированным ГН. При этом пространство внутренних состояний такого ГН составляет $S_M\times S_F$, переходная функция имеет вид: $f_C:(s_M,s_F)\to$ $\to\left(f_M(s_M),\ f_F\left(o_M(s_M),s_F\right)\right)$, а выходная функция – $o_C:(s_M,s_F)\to o_F(s_F)\in O_F$ [10].

4. Выводы

Перспективным способом построения составных ГН на основе GFSR, является их компромиссное сочетание с нелинейными мультипликативными фильтрами, обладающими собственной конечной памятью. Применение такого подхода обосновано тем фактом, что при достаточно большом периоде формируемых GFSR-генераторами последовательностей, число порождающих полиномов, определяющих тип обратной связи, относительно невелико, что облегчает задачу криптоаналитикам. Введение же некоторой нелинейности является экономичным способом решения проблемы.

Литература

1. Скопа, О. О. Аналіз моделей первинних датчиків псевдовипадкових чисел [Текст] / Н. М. Білик, О. О. Скопа // Системи обробки інформації. – 2009. – №7 (79). – С. 56-59. – ISSN 1681-7710.

2. Скопа, О. О. Статистичне тестування симетричних криптографічних перетворень [Текст] / О. О. Скопа // Східноєвропейський журнал передових технологій. – 2011. – №4/9 (52). – С. 15-18. – ISSN 1729-4061.

3. Скопа, О. О. Інструментальні засоби статистичного тестування криптогра-

фічних перетворень [Текст] / О. О. Скопа // Вісник Національного технічного університету «ХПІ». – 2011. – №33. – С. 77-83. – ISSN 2079-0023.

4. Безпека банківської діяльності [Текст] : монографія / Казакова Н. Ф., Панфілов В. І., Скачек Л. М., Скопа О. О., Хорошко В. О. ; за ред. проф. Хорошко В. О. – К. : ПВП «Задруга», 2013. – 282 с. – ISBN 978-966-2970-82-1.

5. Кнут, Д. Искусство программирования для ЭВМ [Текст] : пер. з англ. [Ю. В. Козаченко] / Д. Кнут. – М. : Мир, 1977. – Т. 2. – 727 с. – ISBN 978-5-8459-0081-4.

6. Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си [Текст] : пер. з англ. / Брюс Шнайер. – М. : Триумф, 2002. – 816 с. – ISBN 5-89392-055-4, 0-471-11709-9.

7. Казакова, Н. Ф. Проблемы построения комбинированных линейных генераторов псевдослучайных чисел [Текст] / Н. Ф. Казакова, Ю. В. Щербина // Інформаційна безпека. – 2013. – № 2(10). – С.58-64. – ISSN 2224-9613.

8. Щербина, Ю. В. Проблемы оценки защищенности автоматизированных систем [Текст] / Ю. В. Щербина, А.А. Скопа // Захист інформації. – 2008. – №4(41). – С.23-29. – ISSN 2221-5212.

9. Courtois, N. Fast algebraic attacks on stream ciphers with linear feedback Advances in Cryptology [Текст] / N. Courtois // CRYPTO-2003. – Springer-Verlag. – 2003. – №2729. – P. 176-194. – ISSN 0302-9743, ISBN 3-540-40674-3.

10. Ekdahl, P. SNOW-a new stream cipher [Текст] / P. Ekdahl, T. Johansson // Proc. of First Open NESSIE Workshop. – KU-Leuven, 2000. – 230 p. – ISSN відсутній.

References

1. Skopa, O. O., Bilik, N. M. (2009). Analiz modelej pervynnyh datchykiv psevdovypadkovyh chysel. *Systemy obrobky informacii, №7 (79)*, 56-59.

2. Skopa, O. O. (2011). Statystychne testuvannja simetrychnyh kryptografichnyh peretvoren'. *Shidnoevropejs'kyj zhurnal peredovyh tehnolohij, №4/9 (52)*, 15-18.

3. Skopa, O. O. (2011). Instrumental'ni zasoby statystychnogo testuvannja kryptografichnyh peretvoren'. *Visnyk Nacional'noho tehnichnogo universytetu «HPI», №33*, 77-83.

4. Kazakova, N. F., Panfilov, V. I., Skachek, L. M., Skopa, O. O., Horoshko, V. O. (2013). Bezpeka bankivs'koi' dijal'nosti. Kyi'v. : PVP Zadruga, 282.

5. Knut, D. (1977). Iskusstvo programmirovanija dlja EVM. Moskva: Mir, 727.

6. Shnajer, B. (2002). Prikladnaja kriptografija. Protokoly, algoritmy, ishodnye teksty na jazyke Si. – Moskva: Triumf, 816.

7. Kazakova, N. F., Shherbina, Ju. V. (2013). Problemy postroenija kombinirovannyh linejnyh generatorov psevdosluchajnyh chisel. *Informacijna bezpeka, № 2(10)*, 58-64.

8. Shherbina, Ju. V., Skopa, A. A. (2008). Problemy ocenki zashhishhennosti avtomatizirovannyh sistem. *Zahiyst informacii, №4(41)*, 23-29.

9. Courtois, N. (2003). Fast algebraic attacks on stream ciphers with linear feedback Advances in Cryptology. *CRYPTO-2003, №2729*, 176-194.

10. Ekdahl, P., Johansson, T. (2000). SNOW-a new stream cipher. *Proc. of First Open NESSIE Workshop*. – KU-Leuven, 230.

Проведен анализ проблем, связанных с теоретическим и практическим обоснованием принципов построения комбинированных генераторов псевдослучайных последовательностей на основе регистров сдвига с обобщенной обратной связью. Показано, что одним из перспективных способов построения составных генераторов псевдослучайных последовательностей является компромиссное сочетание принципов, положенных в основу синтеза GFSR-генераторов, с нелинейными мультипликативными фильтрами, обладающими собственной конечной памятью. Применение такого подхода обосновано тем фактом, что при достаточно большом периоде последовательностей, формируемых GFSR-генераторами, число порождающих полиномов, определяющих тип обратной связи, относительно невелико, что облегчает задачу криптоаналитикам. Введение же некоторой нелинейности является экономичным способом решения проблемы повышения криптозащиты и может быть использовано при проектировании современных систем защиты информации и при разработке новых криптошифров.

Ключевые слова: потоковый шифр, комбинированный генератор, фильтр с памятью, GFSR-генератор, вихрь Мерсенна

Казакова Надія Феліксівна
доцент кафедри Інформаційних систем в економіці
кандидат технічних наук, доцент
Одеський національний економічний університет
вул. Преображенська, 8, Одеса, Україна, 65082
Контактний телефон 094-955-94-18
E-mail: kaz2003@ukr.net

Надежда Феликсовна Казакова
доцент кафедры Информационных систем в экономике
кандидат технических наук, доцент
Одесский национальный экономический университет
ул. Преображенская, 8, Одесса, Украина, 65082
Контактный телефон 094-955-94-18
E-mail: kaz2003@ukr.net

Nadezhda Kazakova
Associate Professor of Department of information systems in economics
Ph.D., associate professor
Odessa State Economic University
8, str. Preobrazhens'ka, Odessa, Ukraine, 65082
Contact phone 094-955-94-18
E-mail: kaz2003@ukr.net