Кафедра 42
Криптология и дискретная математика
Тел. 324-7334; факс. 323-9137; e-mail: kaf42@mail.ru.

О перемешивающих графах частного класса модифицированных аддитивных генераторов [1]

Аспирант каф.42 НИЯУ МИФИ, Дорохова А.М.

РусКрипто 2015

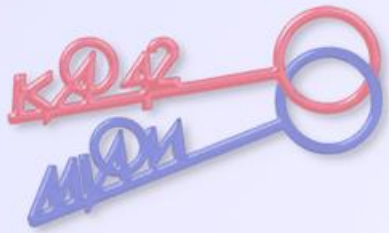
[1]: Работа выполнена в рамках программы поддержки научных кадров «ИнфоТеКС Академия 2014».

Актуальность

Итеративные функции векторных пространств, где каждый бит выхода зависит от всех битов входа, используются:

- в системах аутентификации для выработки кодов аутентификации;

- в симметричных криптосистемах для противодействия криптоаналитическим атакам типа последовательного опробования частей ключа.



Матрично-графовый подход

Пусть $\varphi(z_1,\ldots,z_n)=(z_2,\ldots,z_n,f(z_1,\ldots,z_n))$ – преобразование регистра левого сдвига длины n над V_r (есть преобразование φ множества $V_{nr}=\{(z_1,\ldots,z_n)\}$, где $z_1,\ldots,z_n\in V_r$); $f:V_{nr}\to V_r$ – функция обратной связи регистра сдвига.

Преобразование φ задается системой nr булевых координатных функций

$$\{\varphi_1(x_1,\ldots,x_{nr}),\ldots,\varphi_{nr}(x_1,\ldots,x_{nr})\},$$

где функция $\varphi_{v+kr}(x_1,\ldots,x_{nr})$ вычисляет v-й бит x_{v+kr} вектора z_{k+1}, $v=1,\ldots,r$, $k=0,1,\ldots,n-1$.

Перемешивающие свойства регистрового преобразования φ определяются системой множеств $\{E(\varphi_1),\ldots,E(\varphi_{nr})\}$, где $E(\varphi_j)$ – множество номеров существенных переменных координатной функции $\varphi_j(x_1,\ldots,x_{nr})$, $j=1,\ldots,nr$.

Функции φ соответствует **перемешивающий** nr-вершинный **орграф** $\Gamma(\varphi)$ (**перемешивающая 0,1-матрица** $M(\varphi)=(m_{ij})$ смежности его вершин), где $i\in E(\varphi_j)$ $\Leftrightarrow$ (i,j) дуга в $\Gamma(\varphi)$ ($m_{ij}=1$), $i,j\in\{1,\ldots,nr\}$.

Задача: определить **условия примитивности** и **экспонент** графа $\Gamma(\varphi)$.

Аддитивные генераторы

Обозначим:

- $Z/2^r$ – кольцо вычетов по модулю 2^r, где $r>1$;
- n – длина регистра сдвига с номерами ячеек $0,\ldots,n-1$;
- $X_0,X_1,\ldots,X_{n-1}$ – знаки начального состояния генератора (элементы $Z/2^r$);
- $\delta(X_i)$ – двоичное представление числа $X_i \in Z/2^r$; младшими битами вектора $\delta(X_i) \in V_r$ положим r–е биты.

Знак X_i образуется при $i \geq n$ в соответствии с законом рекурсии:

$$X_i = \left(\sum_{j=0}^{n-1} a_j X_{j+i-n}\right) \bmod 2^r, \qquad (1)$$

где $a_0,\ldots,a_{n-1} \in \{0,1\}$.

Аддитивный генератор есть регистр сдвига длины n с функцией обратной связи $f(y_0,\ldots,y_{n-1}) = \left(\sum_{j=0}^{n-1} a_j y_j\right) \bmod 2^r$.

При $a_0=1$ (в противном случае длина регистра меньше n) $f(y_1,\ldots,y_n)$ биективна по переменной y_0, то есть регистр реализует подстановку множества состояний генератора.

На основе аддитивных генераторов построены алгоритмы Fish, Pike, Mush.

Модификации аддитивных генераторов (1)

Перемешивающий nr-вершинный граф аддитивного генератора обозначим $\Gamma(\varphi)$.

В соответствии с законом рекурсии (1), k-е разряды двоичного представления каждого из чисел $X_0, X_1, \ldots, X_{n-1}$ текущего состояния зависят только от 1-го,…,k-го разрядов чисел предыдущего состояния, $k=1,\ldots,r$. Следовательно, граф $\Gamma(\varphi)$ не сильно связный, что исключает хорошие перемешивающие свойства преобразования аддитивного генератора.

Для достижения хороших перемешивающих свойств необходима сильная связность перемешивающего орграфа $\Gamma(\varphi)$.

В связи с этим исследуем модификации аддитивного генератора, полученные с помощью определенных преобразований множества V_r.

Модификации аддитивных генераторов (2)

Первый вид модификации (***I*-модификация**) состоит в применении к векторам из V_r инволюции I: $I(x_1,\ldots,x_r)=(x_r,\ldots,x_1)$.

Второй вид модификации (***S*-модификация**) состоит в применении к векторам из V_r нелинейного совершенного преобразования S, моделирующего s-бокс.

Для I-, S-модификаций закон рекурсии (1) соответственно имеет вид, $i \geq n$:

$$\delta(X_i)=I(\delta((X_{i-n}+\sum_{j=1}^{n-1} a_j X_{j+i-n}) \bmod 2^r)).$$

$$\delta(X_i)=S(\delta((X_{i-n}+\sum_{j=1}^{n-1} a_j X_{j+i-n}) \bmod 2^r)).$$

Схема модифицированных генераторов представлена на рисунке 1. Выходная последовательность имеет вид $(X_0, X_1,\ldots,X_i,\ldots)$.

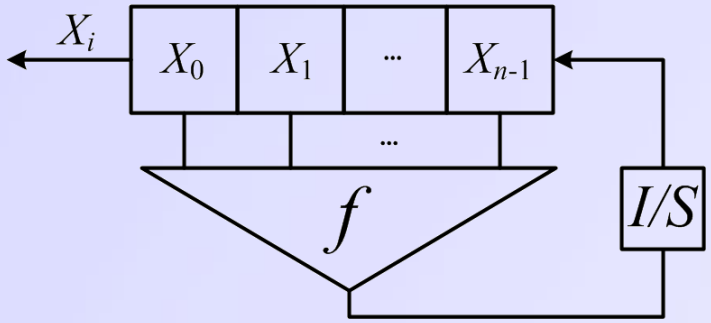


Рисунок 1. Схема модификаций аддитивного генератора

Модификации аддитивных генераторов (3)

Обозначим модифицированные с помощью I и S регистровые подстановки над V_r соответственно $\varphi^I(X_0,\ldots,X_{n-1})$ и $\varphi^S(X_0,\ldots,X_{n-1})$, $\Gamma(\varphi^I)$ и $\Gamma(\varphi^S)$ – перемешивающие орграфы подстановок φ^I и φ^S.

Номера существенных переменных функции обратной связи регистра сдвига будем называть точками съема.

Обозначим D множество точек съема регистра, на основе которого построен аддитивный генератор: $D=\{d_0,d_1,\ldots,d_q\}$, где $0<q<n$ и $0=d_0<d_1<\ldots<d_q<n$.

Обозначим $\rho(D)=\max\{d_1,d_2-d_1,\ldots,d_q-d_{q-1}\}$ – максимум расстояний между двумя соседними точками съема регистра.

Условия примитивности

Теорема *(достаточные условия примитивности перемешивающих орграфов* $\Gamma(\varphi^l)$ *и* $\Gamma(\varphi^S)$*)*: Перемешивающие графы $\Gamma(\varphi^l)$ и $\Gamma(\varphi^S)$ модифицированных аддитивных генераторов являются примитивными, если

$$\gcd(n,d_1,\ldots,d_q)=1.$$

Пусть $d \in D$ – наибольшее из чисел d_i, $i=1,\ldots,q$, тогда:

1. $\exp\Gamma(\varphi^l) \le (n-d)^2-2(n-d)+2nr-1$, если $d_i-d_{i-1}=1$.
2. $\exp\Gamma(\varphi^l) \le n^2+(2r-3-d)n+2d$, если $(n,d)=1$; $\exp\Gamma(\varphi^l) \le 2n-2$ при $d=n-1$.
3. $\exp\Gamma(\varphi^S) \le \rho(D)+(n-d)(n-1)$, если $(n,d)=1$.

Пример

Пример. Пусть n=11, r=32, D={0,5,6,10}.

Оценки	[*Wielandt H. Unzerlegbare nicht negative Matrizen*]:	[*Фомичев В. М. Оценки экспонентов примитивных графов*]:	[*Сачков В.Н., Тараканов В.Е. Комбинаторика неотрицательных матриц*]:	[*Оценки Теоремы*]
	$\exp\Gamma \le (nr)^2-2nr+2$	$\exp\Gamma \le l\lambda-l-3\lambda+h+2n$	$\exp\Gamma \le nr+l(nr-2)$	$\exp\Gamma(\varphi^l) \le 2n-2$ $\exp\Gamma(\varphi^S) \le \rho(D)+(n-d)(n-1)$
$\exp\Gamma(\varphi^l)$	123202	718 (l=6,λ=5,h=5)	702 (l=1)	20
$\exp\Gamma(\varphi^S)$	123202	718 (l=6,λ=5,h=5)	702 (l=1)	15

Рекомендации по выбору параметров

Выбор параметров модифицированного аддитивного генератора позволяет достичь полное перемешивание за число итераций, существенно меньшее размера состояний генератора (в битах).

Для *I*-модификации: если параметры регистра сдвига связаны соотношением $n-m=r$, то

$$\exp\Gamma(\varphi^I)\le 2nr+r^2-2r-1,$$

оценка достигает минимума при $n-m=2$ и равна $2nr-1$.

Для *S*-модификации: наименьшее число итераций для полного перемешивания достигается при четном значении n длины регистра сдвига и множестве точек съема $D=\{0,2,4,\ldots,n-1\}$. В этом случае

$$\exp\Gamma_S(\varphi)\le n+1.$$

Оценка экспонента не зависит от r, что может быть использовано при построении *S*-модификации аддитивного генератора с небольшой длиной n регистра сдвига при любых значениях r.

Спасибо за внимание!