Секция «Математика и механика»

О сложности тестирования криптографических функций на неисправности типа слипания на входах

Икрамов Алишер Акрамович
Студент
Филиал МГУ имени М.В.Ломоносова в г. Ташкенте, Факультет прикладной математики и информатики, Ташкент, Узбекистан
E-mail: melan44@mail.ru

Определение. **Неисправностью** называется отображение $\phi\colon E_2^n \to E_2^n$, если $\exists\tilde{\alpha} \in E_2^n \quad \phi(\tilde{\alpha}) \neq \tilde{\alpha}$.

Определение. **Проверяющим тестом** для семейства $\Phi = \{\phi$ – неисправность$\}$ и функции f называется $T \subset E_2^n$ такое, что $\forall\phi \in \Phi \quad (f(\phi(\cdot)) \not\equiv f(\cdot)) \Rightarrow (\exists\tilde{\alpha} \in T \quad f(\phi(\tilde{\alpha})) \neq f(\tilde{\alpha}))$.

Определение. **Сложностью** тестирования функции f на класс неисправностей K называется минимальное $|T|$, где T – проверяющий тест для K и f. Обозначение: $L(f, K)$. Сложностью тестирования множества функций N на класс неисправностей K называется величина $L(N, K) = \max\limits_{f\in N} L(f, K)$.

Определение. Переменная x_i называется **фиктивной** для функции $f(x_1, \ldots, x_n)$, $i \in \{1, \ldots, n\}$, если $\forall\tilde{\alpha} = (\alpha_1, \ldots, \alpha_{i-1}, 0, \alpha_{i+1} \ldots, \alpha_n) \in E_2^n$ при $\tilde{\beta} = (\alpha_1, \ldots, \alpha_{i-1}, 1, \alpha_{i+1} \ldots, \alpha_n)$ выполняется равенство $f(\tilde{\alpha}) = f(\tilde{\beta})$.

Определение. Пусть $F\colon E_2^{n+m} \to E_2^n$. Если $\forall k = (k_1, \ldots, k_m) \in E_2^m \quad F(\cdot, k)$ — биекция и F не содержит фиктивных переменных, то F называется **криптографической**. Множество всех криптографических функций обозначим через $Cr(n, m)$. Переменные $k_1, \ldots, k_m$ назовем ключом.

Определение. Неисправности типа **дизъюнктивного слипания** (обозначение $S^2_\vee$) разбивают множество переменных X^n на непустые подмножества $Z_1(\phi), \ldots, Z_{q_\phi}(\phi)$, $q_\phi \in \{1, \ldots, n-1\}$ так, что для любого $\tilde{\alpha} \in E_2^n, \tilde{\alpha} = (\alpha_1, \ldots, \alpha_n)$ полагаем $\phi(\tilde{\alpha}) = (\beta_1, \ldots, \beta_n)$, где $\beta_i = \max\{\alpha_j\colon x_j \in Z_l(\phi)\}$, если $x_i \in Z_l(\phi)$, $i = \overline{1, n}$.

Определение. Неисправности типа **конъюнктивного слипания** (обозначение $S^2_\&$) разбивают множество переменных X^n на непустые подмножества $Z_1(\phi), \ldots, Z_{q_\phi}(\phi)$, $q_\phi \in \{1, \ldots, n-1\}$ так, что для любого $\tilde{\alpha} \in E_2^n, \tilde{\alpha} = (\alpha_1, \ldots, \alpha_n)$ полагаем $\phi(\tilde{\alpha}) = (\beta_1, \ldots, \beta_n)$, где $\beta_i = \min\{\alpha_j\colon x_j \in Z_l(\phi)\}$, если $x_i \in Z_l(\phi)$, $i = \overline{1, n}$.

Определение. **Разнотипными** неисправностями называется объединение нескольких классов неисправностей. На входе логического устройства может присутствовать не более одной неисправности, принадлежащей хотя бы одному из исходных классов.

Теорема 1. $m - 1 +]\log_2(n-1)[\leq L(Cr(n, m), S^2_\vee) \leq m +]\log_2 n[$

Доказательство. Возьмем набор, у которого первые n компонент равны 0, а остальные компоненты равны 1. Данный набор назовем "разделяющим", так как он по определению криптографической функции позволит определить любое слипание каких-либо из первых n переменных с любыми из последующих m переменных. Далее с помощью логарифмической системы наборов, у которых компоненты с $n+1$ по $n+m$ равны 1, проверяем слипание первых n переменных. Логарифмической называется система из $]\log_2 n[$ наборов, чей вес по первым n компонентам равен $n/2$ (в случае нечётного n

равен $[n/2]$ или $]n/2[$), а также вес первых n значений покомпонентной суммы по модулю 2 любых двух наборов из этой системы равен $n/2$ (то есть на месте половины единиц одного набора у второго набора стоят единицы, на месте оставшихся единиц первого набора у второго набора стоят нули, аналогично половине нулей первого набора у второго набора соответствуют единицы, оставшимся нулям первого набора — нули у второго набора).

Логарифмическая система позволяет на каждом шаге уменьшать количество непроверенных неисправностей слипания первых n переменных в 2 раза. В силу биективности по первым n переменным любое изменение в наборе приведет к изменению значения. По лемме 20 [1] строим тест для проверки m переменных ключа (зная по предыдущим тестам, что других слипаний в исследуемом логическом устройстве заведомо нет). Для этого потребуется не более $m-1$ наборов (по Предложению 6 [1]). Поэтому построенное множество является проверяющим тестом, в котором $m+]\log_2 n[$ наборов.

Построим функцию, сложность тестирования которой будет давать нам оценку снизу. Пусть $F(x_1,\dots,x_n,x_{n+1},\dots,x_{n+m}) = (f_1,\dots,f_n)$ задается $f_1(x_1,x_2,\dots,x_n,\dots,x_{n+m}) = x_1 \oplus x_2\&\dots\&x_{n+m}$, $f_i(x_1,\dots,x_{n+m}) = x_i$ для $2 \le i \le n$. Тогда любой проверяющий на неисправности типа $S^2_\vee$ должен содержать попарно различные наборы $\tilde\beta^1,\dots,\tilde\beta^{m-1}$, у которых выполняются следующие свойства: $\|\tilde\beta^i\| \ge n+m-2$, $\beta^i_2 = \beta^i_3 = \dots = \beta^i_n = 1$, ровно одна компонента из $\beta^i_{n+1},\dots,\beta^i_{n+m}$ равна 0. Иначе существует неисправность φ слипания двух переменных из $x_{n+1},\dots,x_{n+m}$, которая данным тестом не проверяется, так как только при $(x,1,\dots,1)$ значения F отличаются по ключу. Отсюда $L(F,S^2_\vee) \ge m-1$. Так как среди упомянутых наборов нет ни одного, проверяющего на слипания переменных $x_2,\dots,x_n$, то понадобится ещё минимум $]\log_2(n-1)[$ наборов для проверки этих неисправностей (по логарифмической системе). Таким образом $L(F,S^2_\vee) \ge m-1+]\log_2(n-1)[$. $\square$

Следствие 1. $m-1+]\log_2(n-1)[\le L(Cr(n,m),S^2_\&) \le m+]\log_2 n[$

Доказательство. По принципу двойственности в качестве "разделяющего" набора будет взят набор, у которого первые n компонент равны 1, а последующие m компонент равны 0. Функция, дающая нижнюю оценку, отличается от теоремы 1 в $f_1(x_1,\dots,x_{n+m}) = x_1 \oplus \overline{x}_2\&\dots\&\overline{x}_{n+m}$. $\square$

Теорема 2. $2(m-1)+]\log_2(n-1)[\le L(Cr(n,m),S^2_\vee \cup S^2_\&) \le 2m+]\log_2 n[$

Доказательство. В начале тест формируется из двух "разделяющих" наборов, описанных в доказательствах теоремы 1 и следствия 1. Так как на входе может быть только одна неисправность либо из $S^2_\vee$, либо из $S^2_\&$ (по определению разнотипных неисправностей), то эти два набора заведомо разделяют переменные. Теперь для проверки слипания первых n переменных достаточно одной логарифмической системы, в которой все компоненты с $n+1$ по $n+m$ наборов равны одной и той же константе (что исключает влияние слипаний на этих позициях). Далее добавляются наборы, отдельно проверяющие на конъюнктивное слипание и отдельно на дизъюнктивное слипание переменных $x_{n+1},\dots,x_{n+m}$ (по теореме 4 [2]). Вместе получаем $L(Cr(n,m),S^2_\vee \cup S_\&) \le 2+]\log_2 n[+2(m-1) = 2m+]\log_2 n[$.

В качестве функции, дающей нижнюю оценку возьмем F: $f_1(x_1,\dots,x_{n+m}) = x_1 \oplus x_2\&\dots\&x_{n+m} \oplus \overline{x}_2\&\dots\&\overline{x}_{n+m}$, $f_i(x_1,\dots,x_{n+m}) = x_i$ для $2 \le i \le n$. Так как функция F меняет свое поведение только при ключах $(0,\dots,0)$, $(1,\dots,1)$ и только на значениях, когда компоненты со второй по n равны между собой и равны компонентам ключа, то

проверяющий тест на слипание переменных $x_{n+1}, \ldots, x_{n+m}$ будет прямой суммой тестов на конъюнктивное слипание и на дизъюнктивное слипание, то есть $L(F, S^2_\vee \cup S^2_\&) \geq 2(m-1)$. Логарифмическая система переменных с 2 по n проверит их и конъюнктивное, и дизъюнктивное слипание. В сумме $L(F, S^2_\vee \cup S^2_\&) \geq 2(m-1)+]\log_2(n-1)$. $\square$

Рассмотрим вопрос обобщения неисправностей типа слипания. Множество переменных разбивается на непустые непересекающиеся подмножества. В результате интерпретации каждая переменная из подмножества равна значению функции от переменных этого подмножества. Но для слипаний не существенен вопрос последовательности переменных в функции. А значит, наиболее общий случай, когда функция слипания является симметрической.

Класс неисправностей типа **симметрических слипаний** обозначим через S^2_{sym}. Тогда верно следующее утверждение:

Теорема 3. $L(n, S^2_{sym}) = 2^n$

Доказательство. Верхняя оценка очевидна.

Рассмотрим функцию $f(x_1, \ldots, x_n) = x_1 \vee \ldots \vee x_n$. Теперь покажем, что необходим каждый набор из E^n_2 для проверки на наличие неисправностей из S^2_{sym}. Введём неисправности $f_k(x_1, \ldots, x_k)$ следующим образом: $\forall \tilde{\alpha} \in E^k_2 \quad (0 < \|\tilde{\alpha}\| < k) \Rightarrow (f_k(\tilde{\alpha}) = 1)$, $f_k(0, \ldots, 0) = f_k(1, \ldots, 1) = 0$. Данные функции являются симметрическими. Предположим, что набор $\tilde{\beta}$ не входит в тест. Пусть $t = \|\tilde{\beta}\|$, $i_1, \ldots, i_t$ – номера компонент, которые равны 1 в наборе $\tilde{\beta}$. Тогда неисправность $f_t(x_{i_1}, \ldots, x_{i_t})$ не проверена, так как её можно проверить лишь положив $x_{i_1} = \ldots = x_{i_t} = 1$, но при этом все остальные переменные должны быть равны 0 (в силу f). Следовательно, все наборы веса не меньше 2 входят в тест.

По определению симметрических слипаний может происходить слипание одной переменной. В этом случае мы получаем либо константную неисправность кратности 1, либо инверсную неисправность кратности 1. Тогда необходимо проверить все наборы, в которых только одна компонента равна 1. Получаем вхождение в тест всех наборов веса 1. Наконец, для проверки установления какой-то переменной в константу 1, необходим также нулевой набор. Получаем нижнюю оценку 2^n. $\square$

Литература

1. Кудрявцев В.Б., Гасанов Э.Э., Долотова О.А., Погосян Г.Р., Теория тестирования логических устройтсв, М.: Физматлит, 2006 г.

2. Икрамов А.А., О сложности тестирования логических устройств на некоторые типы неисправностей, "Интеллектуальные системы Том 17, выпуск 1-4, 2013 г. http://intsys.msu.ru/magazine/archive/v17(1-4)/

Слова благодарности

Выражаю благодарность своему научному руководителю В.Б. Кудрявцеву за постановку задачи и внимание к проделанной работе.