Секция «Математика и механика»

О сложности тестирования криптографических функций на инверсные неисправности 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 $f(x_1, \dots, x_n)$, $i \in \{1, \dots, n\}$, если $\forall \tilde{\alpha} = (\alpha_1, \dots, \alpha_{i-1}, 0, \alpha_{i+1} \dots, \alpha_n) \in E_2^n$ при $\tilde{\beta} = (\alpha_1, \dots, \alpha_{i-1}, 1, \alpha_{i+1} \dots, d\alpha_n)$ выполняется равенство $f(\tilde{\alpha}) = f(\tilde{\beta})$. Определение. Пусть $F\colon E_2^{n+m} \to E_2^n$. Если $\forall k = (k_1, \dots, k_m) \in E_2^m \quad F(\cdot, k)$ – биекция и F не содержит фиктивных переменных, то F называется **криптографической**. Множество всех криптографических функций обозначим через $Cr(n, m)$. Определение. Классом **инверсных неисправностей** F_{in}^2 назовем множество всех ϕ_σ, $(\phi_\sigma(\alpha) = \alpha \oplus \sigma)$, $\sigma \in E_2^n \setminus \{0\}$. Через $F_{in}^2(p)$ обозначим класс всех таких ϕ_σ, что $||\sigma|| = p$. Для булевых функций от n переменных верно $L(n, F_{in}^2(1)) = n -]\log_2 n[$ ([1] Глава 3, Теорема 8). Тогда верно следующее утверждение: **Теорема 1.** $L(Cr(n, n), F_{in}^2(1)) = n - t$, *где* $2^{t-1} + t \leq n \leq 2^t + t$. **Доказательство.** Так как неисправность может произойти только на одном входе и в силу биективности $F(\cdot, k)$ любой один набор является тестовым для определения наличия инверсии одного входа у первых n переменных. Отсюда сложность тестирования не может превышать сложности тестирования функции с n входами (так как любой тест проверяет также и n первых входов). Получаем $L(Cr(n, n), F_{in}^2(1)) \leq n - t$. Построим функцию $F = (f_1, \dots, f_n)$ следующим образом:

$$f_i(x_1, \dots, x_{2n}) = x_i \oplus f_c(x_{n+1}, x_{n+2}, \dots, x_{2n})$$

$$f_c(x_1, \dots, x_n) = \bigvee_{i=t+1}^{n} x_i j_{\alpha_1^i}(x_1) \dots j_{\alpha_t^i}(x_t)$$

где набор $\tilde{\alpha}^i$ равен двоичному представлению числа i. По Предложению 12 в [1] Глава 3 сложность тестирования функции f_c равна $n - t$. Тогда имеем $L(F, F_{in}^2(1)) \geq n - t$. $\square$ Рассмотрим сложность тестирования на весь класс инверсных неисправностей. **Теорема 2.** $2\left[\frac{n-1}{2}\right] + 1 \leq L(Cr(n, n), F_{in}^2) \leq n + 1$. **Доказательство.** Рассмотрим произвольный набор $\tilde{\alpha}$ в качестве тестового. В силу биективности F при фиксированном $\tilde{k}$ имеем, что $\forall \tilde{k} \in E_2^n$ число наборов $\tilde{\beta} = (\beta_1, \dots, \beta_n, k_1, \dots, k_n)$ таких, что $F(\tilde{\beta}) \neq F(\tilde{\alpha})$, равно $2^n - 1$ (только на одном наборе значение должно совпадать). Получается, что число неисправностей $\phi_\sigma \in F_{in}^2$, на которые проверяет набор $\tilde{\alpha}$, равно $2^n(2^n - 1) = 2^{2n} - 2^n$. А значит, число непроверенных неисправностей равно $2^n - 1$. Далее, по лемме 24 (теорема

Погосяна) из Главы 3 [1] мощность минимального проверяющего теста не может превышать $n+1$. Нижняя оценка получается из Теоремы 7 из [1] и выбора $F = (f_1, \ldots, f_n)$ вида $f_i(x_1, \ldots, x_{2n}) = x_i \oplus f_{in}^n(x_{n+1}, \ldots, x_{2n})$. $\square$ Таким образом, сложность тестирования криптографических функций на инверсные неисправности асимптотически в 2 раза меньше, чем сложность класса всех функций от такого же числа переменных.

Литература

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

Слова благодарности

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