Идеи Шеннона по перемешиванию и рассеиванию в свете линейного и разностного методов в криптографии

Ф.М. Малышев

Математический институт им. В.А.Стеклова, Москва, Россия

Основой доклада является работа автора: *Методы линейных и разностных соотношений в криптографии. Диск. мат.* **34***:1 (2022), 36–63.*

Для теоретической криптографии типичной является ситуация, когда для отображения двоичных векторных пространств $F\colon V_N \to V_M$, $a \mapsto b = F(a)$, $a \in V_N = GF(2)^N$, $b \in V_M$, рассматриваются вероятностные линейные и разностные соотношения. *Вероятностное линейное соотношение* представляем парой вектор-столбцов $L' \in V_N^*$, $L'' \in V_M^* \diagdown \{0\}$, и записываем в виде $aL' \simeq bL''$. Оно характеризуется величиной $\delta_{L',L''} = \delta^F_{L',L''} = 2\mathbf{P}\{aL' = bL''\} - 1$, где вероятность вычисляется в условиях равномерного распределения вектор-строк a на V_N. *Вероятностное разностное соотношение* представляем векторами $D' \in V_N \diagdown \{0\}$, $D'' \in V_M$ и обозначаем как $D' \rightsquigarrow D''$. Оно оценивается вероятностью $p_{D',D''} = p^F_{D',D''} = \mathbf{P}\{F(a+D') + F(a) = D''\}$. Использующие эти соотношения соответственно линейный и разностный методы криптографического анализа характеризуются следующими особенностями.

1) Предварительно получаемые вероятностные соотношения относятся к отображениям F, задаваемым сложно устроенными конкретными *функциональными схемами* (ф.с.) $\mathcal{F}$, реализующими глубокие и разветвлённые суперпозиции большого числа *локальных* нелинейных отображений $f_i : V_{n_i} \to V_{m_i}$, $x_i \mapsto y_i = f_i(x_i)$, $i = 1, \dots, k$, составляющих *нелинейную часть* ф.с. $\mathcal{F}$. Переменные a, x_i, y_i, b линейно выражаются друг через друга: $(a, y_1, \dots, y_k)C_{\mathcal{F}} = (x_1, \dots, x_k, b)$. Здесь $C_{\mathcal{F}}$ верхнетреугольная матрица *линейной среды*, состоящей из линейных отображений ф.с. $\mathcal{F}$.

2) При построении вероятностных соотношений в качестве целевых функций, подлежащих максимизации, используют не точные значения $|\delta_{L',L''}|$ и $p_{D',D''}$, а некоторые их "приближения" : $|\tilde{\delta}_{\mathfrak{L}}| = \prod_{i=1}^k |\delta^{f_i}_{l'_i,l''_i}|$, $\tilde{p}_{\mathfrak{D}} = \prod_{i=1}^k p^{f_i}_{d'_i,d''_i}$, где $\mathfrak{L} = ((l'_i, l''_i),\ i = 1, \dots, k)$, $\mathfrak{D} = ((d'_i, d''_i),\ i = 1, \dots, k)$ – множества *локальных вероятностных соотношений*, относящихся к отдельным f_i. Элементы множеств $\mathfrak{L}$ и $\mathfrak{D}$ должны быть согласованы линейной средой. Если, например, $x_i = y_j$, $i > j$, то $l''_j = l'_i$, $d'_i = d''_j$. Замены $|\delta_{L',L''}|$ на $|\tilde{\delta}_{\mathfrak{L}}|$ и $p_{D',D''}$ на $\tilde{p}_{\mathfrak{D}}$ производятся в отсутствии каких-либо утверждений о степени близости этих пар величин.

3) При окончательных расчётах эффективности методов анализа вместо требуемых величин $|\delta_{L',L''}|$ и $p_{D',D''}$ используют $|\widetilde{\delta}_{\mathfrak{L}}|$ и $\widetilde{p}_{\mathfrak{D}}$.

При максимизации $|\tilde{\delta}_{\mathfrak{L}}|$ и $\tilde{p}_{\mathfrak{D}}$ ориентируются на множества $\mathfrak{L}$ и $\mathfrak{D}$, в которых как можно больше номеров $i \in \{1, \dots, k\}$, для которых $l'_i = l''_i = 0$ или $d'_i = d''_i = 0$. Минимально возможные (при некоторых $\mathfrak{L}$ и $\mathfrak{D}$ соответственно) мощности совокупностей остальных значений i являются показателями рассеивания θ_C и θ_C^* линейной среды $C = C_{\mathcal{F}}$, соответственно относительно линейного и разностного методов.

Приведённые особенности являются источником справедливой критики линейного и разностного методов. Имеется даже пример семейства функциональных схем $\mathcal{F}_c$ с линейной средой независящей от c, реализующих любое отображение $F_c\colon V_N \to V_M$. Параметр c принимает 2^{M2^N} значений. Локальные отображения $f_{i,c}$ зависят от c, но участвующие в поиске "лучших" вероятностных соотношений величины $|\delta^{f_{i,c}}_{l'_i,l''_i}|$ и $p^{f_{i,c}}_{d'_i,d''_i}$ от c не зависят. Это позволяет получать примеры самых экзотических соотношений между $\tilde{\delta}_{\mathfrak{L}}$ и $\delta_{L'_{\mathfrak{L}},L''_{\mathfrak{L}}}$, и между $\tilde{p}_{\mathfrak{D}}$ и $p_{D'_{\mathfrak{D}},D''_{\mathfrak{D}}}$.

Теоремы о точных значениях $\delta^F_{L',L''}$ и $p^F_{D',D''}$, привлекающие в своих формулировках все возможные согласованные совокупности локальных соотношений $\mathfrak{L}$ и $\mathfrak{D}$, дополнительно вскрывают недостатки методов:

4) находятся не самые лучшие соотношения, а какие получатся,

5) ориентация на $\tilde{\delta} = \max_{\mathfrak{L}} |\tilde{\delta}_{\mathfrak{L}}|$ и $\tilde{p} = \max_{\mathfrak{D}} \tilde{p}_{\mathfrak{D}}$ уводит из областей, где реализуются $\max |\delta_{L',L''}|$ и $\max p_{D',D''}$.

Последние недостатки очень ярко демонстрируются на одной конкретной ф.с. с решёточной структурой.

Не смотря на приведённые недостатки, величины $\tilde{\delta}$ и $\tilde{p}$, зависящие кстати от ф.с. $\mathcal{F}$, являются признанными характеристиками отображения F как шифрпреобразования. При синтезе ф.с. $\mathcal{F}$, предназначаемых для шифраторов, формирование нелинейной части и линейной среды ф.с. $\mathcal{F}$ осуществляется исходя из минимизации характеристик $\tilde{\delta}$ и $\tilde{p}$, что сопряжено с максимизацией показателей рассеивания θ_C, θ_C^* и с минимизацией максимальных значений $|\delta^{f_i}_{l'_i,l''_i}|$ по всем l'_i, l''_i и $p^{f_i}_{d'_i,d''_i}$ по всем d'_i, d''_i. Перечисленные требования практически повторяют предложения Шеннона по рассеиванию и перемешиванию при разработке шифраторов. Они упреждали опасность от двойственных друг другу линейного и разностного методов криптографического анализа, которые появятся спустя полвека.