

СООТНОШЕНИЯ НЕОПРЕДЕЛЕННОСТИ ДЛЯ НЕКОТОРЫХ КЛАССОВ КРИПТОГРАФИЧЕСКИХ ФУНКЦИЙ

Кадирова Ильвира Февзиевна

Студент

Факультет ВМК МГУ имени М. В. Ломоносова, Москва, Россия

E-mail: elviramus@yandex.ru

Изучение алгебраических, комбинаторных, криптографических и иных свойств дискретных функций, используемых в качестве примитивов при синтезе криптосистем, является одним из основных направлений исследований в области криптографии.

В рамках указанного выше направления исследований сформировалась область изучения свойств дискретных функций на конечных группах, описываемых так называемыми соотношениями неопределенности. Соотношение неопределенности — математическое соотношение между параметрами дискретной функции, задающее границы совместных изменений этих параметров.

Пусть $f, g \in \mathcal{F}_n$ — булевы функции. $N\Delta_{f,g}$ — число векторов $u \in \mathcal{F}_n$ таких, что функция взаимной корреляции $\Delta_{f,g}(u) \neq 0$. $NW_{f,g}$ — число векторов $u \in \mathcal{F}_n$ таких, что произведение коэффициентов Уолша-Адамара $W_f(u)W_g(u) \neq 0$.

Была рассмотрена теорема, сформулированная в [1], представляющая собой соотношение неопределенностей для булевых функций (на конечной абелевой 2-группе), связывающее параметры $N\Delta_{f,g}$ и $NW_{f,g}$. В работе было доказано, что оценка в данной теореме может быть улучшена:

Теорема 1. *Для любых $f, g \in \mathcal{F}_n$ выполнено неравенство*

$$N\Delta_{f,g} \cdot NW_{f,g} \geq 2^n.$$

Следствие 1. *Для любых $f, g \in \mathcal{F}_n$ выполнено неравенство*

$$N\Delta_f \cdot NW_f \geq 2^n.$$

В работе приведена криптографическая интерпретация следствия 1. В криптографии считается, что функции, используемые при синтезе криптосистем, должны иметь как можно большее значение нелинейности. Булева функция имеет высокую нелинейность, если функция автокорреляции $\Delta_f(u)$ имеет много нулевых значений, то

есть $N\Delta_f$ мало. Так же считается, что функции, используемые при синтезе криптосистем, должны иметь как можно больший порядок корреляционной иммунности, что соответствует большому числу нулевых значений функции $W_f(u)$, то есть малому NW_f . Однако, следствие 1 показывает, что значения $N\Delta_f$ и NW_f не могут быть малыми одновременно. Поэтому функция, используемая для синтеза криптосистем, не может одновременно иметь высокую нелинейность и порядок корреляционной иммунности.

В работе было получено обобщение теоремы из [1], представляющее собой соотношение неопределенностей для комплекснозначных функций на произвольной конечной абелевой группе.

Пусть $L^2(G)$ - векторное пространство над $\mathbb{C}$ всех комплекснозначных функций на конечной абелевой группе G с заданным скалярным произведением. Пусть f, g из $L^2(G)$. S - характер конечной абелевой группы G . $\hat{G}$ - группа характеров. $\hat{f}(S) = \sum_{x \in G} f(x) \overline{S(x)}$ — дискретное преобразование Фурье функции f . Свертка $f * g(x) = \sum_{y \in G} f(y)g(x-y)$, $x \in G$. $N(f * g)$ — число $s \in G$ таких, что $f * g(s) \neq 0$. $N(f \hat{*} g)$ — число $S \in \hat{G}$ таких, что $f \hat{*} g(S) \neq 0$.

Теорема 2. Пусть G — конечная абелева группа, $f, g \in L^2(G)$ такие, что $|f(s)| \leq 1, |g(s)| \leq 1$ для любого $s \in G$. Тогда выполнено неравенство

$$N(f * g) \cdot N(f \hat{*} g) \geq \max_{s \in G} |f * g(s)|.$$

На основании теоремы 1 была сформулирована и доказана теорема с улучшенной оценкой:

Теорема 3. Пусть G — конечная абелева группа, $f, g \in L^2(G)$ такие, что $|f(s)| \leq 1, |g(s)| \leq 1$ для любого $s \in G$. Тогда выполнено неравенство

$$N(f * g) \cdot N(f \hat{*} g) \geq |G|.$$

Литература

1. Логачев О. А., Сальников А. А., Смышляев С. В., Яценко В. В. Булевы функции в теории кодирования и криптологии. М.: МЦНМО, 2012. С.96–97.