О. В. Ш е м я к и н а (Санкт-Петербург, РЦЗИ «ФОРТ»). **Некоторые структурные свойства криптографических преобразований.**

Рассматривается действие операции умножения в поле $\mathrm{GF}(2^n)$ на смежные классы по произвольной аддитивной подгруппе.

Пусть H — подгруппа аддитивной группы поля $\mathrm{GF}(2^n)$ мощности 2^{n-k}. Для произвольных $\alpha, \beta, \gamma \in \mathrm{GF}(2^n)$ нас интересует количество элементов из $(\alpha + H)(\beta + H)$, попадающих в класс $\gamma + H$, т. е. число решений следующей системы:

$$x_1 \in H, \quad x_2 \in H, \quad (\alpha + x_1)(\beta + x_2) + \gamma \in H. \tag{1}$$

Обозначим S число решений системы (1). Справедливы следующие оценки:

$$2^{2n-3k} - 2^n < S < 2^{2n-3k} + 2^n. \tag{2}$$

Оценка снизу является содержательной (неотрицательной) при условии $3k \leqslant n$.

Поскольку оценки (2) не зависят от значений α, β, γ, элементы произведения любых двух смежных классов по произвольной аддитивной подгруппе мощности не меньше $2^{2n/3}$ содержатся в каждом смежном классе по этой подгруппе.

Для некоторых подгрупп число S можно вычислить точно. Обозначим $\widetilde{H}$ подгруппу, состоящую из элементов $c \in \mathrm{GF}(2^n)$, для которых $\mathrm{TR}_{\mathrm{GF}(2^n)/\mathrm{GF}(2)} cx = 0$ для всех $x \in H$. Пусть F является подполем поля $\mathrm{GF}(2^n)$, W — подгруппа аддитивной группы поля F. Если подгруппа H такова, что $\widetilde{H} = aW$ и $\mathrm{TR}_{\mathrm{GF}(2^n)/F} a = 0$, то

$$S = \begin{cases} 2^{2n-3k} + 2^n - 2^{n-k}, & \text{если } \alpha, \beta, \gamma \in H, \\ 2^{2n-3k} - 2^{n-k}, & \text{если } \alpha, \beta \in H,\ \gamma \notin H, \\ 2^{2n-3k}, & \text{если } \alpha \notin H \text{ и (или) } \beta \notin H. \end{cases}$$