# Some properties of Boolean functions related to plane approximations

Alekseev E.K.[1], Kushchinskaya L.A.[2]

[1]CryptoPro LCC, [2]Lomonosov Moscow State University

May 28, 2018

- The filter generator key recovery method was introduced at the CTCrypt 2017.
- The paper *"Generalization of one method of filter generator key recovery"* was published in the *Discrete mathematics* in 2017 (in Russian).
- The method success essentially depends on the existence of cosets of subspaces of $V_n$ where function $f$ is close to a constant.

- The idea of a new more efficient method of key recovery.

- The idea of a new more efficient method of key recovery.
- An estimation of a function weight on an arbitrary coset $L \oplus u$ of subspace $L \subseteq V_n$ depending on nonlinearity $\mathrm{nl}(f)$ and weight $\mathrm{wt}(f)$.

- The idea of a new more efficient method of key recovery.
- An estimation of a function weight on an arbitrary coset $L \oplus u$ of subspace $L \subseteq V_n$ depending on nonlinearity $\mathrm{nl}(f)$ and weight $\mathrm{wt}(f)$.
- An estimation of a number of cosets $L \oplus u$ such that $|\mathrm{wt}(f|_{L \oplus u}) - \#L/2|$ is greater than a given value.

- The idea of a new more efficient method of key recovery.
- **An estimation of a function weight on an arbitrary coset $L \oplus u$ of subspace $L \subseteq V_n$ depending on nonlinearity $\mathrm{nl}(f)$ and weight $\mathrm{wt}(f)$.**
- An estimation of a number of cosets $L \oplus u$ such that $|\mathrm{wt}(f|_{L \oplus u}) - \#L/2|$ is greater than a given value.

**Theorem**

*Let $n, t \in \mathbb{N}$ such that $n \geqslant 2$ and $1 \leqslant t \leqslant n-1$. Then for any Boolean function $f$ of $n$ variables, for any subspace $L \subset V_n$ of dimension $n-t$ and for any vector $u \in V_n$ the following inequalities hold:*

$$\frac{\mathrm{wt}(f)}{2^t} - S \leqslant \mathrm{wt}(f|_{L \oplus u}) \leqslant \frac{\mathrm{wt}(f)}{2^t} + S,$$

*where $S = \frac{2^t-1}{2^t} \cdot (2^{n-1} - \mathrm{nl}(f))$.*

Experimental verification.

- $n = 10$, $f_d \in \mathcal{F}_n$ — filter function from LILI-128.
- $\mathrm{nl}(f) = 480$, $\mathrm{wt}(f) = 2^{n-1}$.

Method characteristics

| $\dim = n - t$ | theoretical limits | experimental limits | tests |
|---|---|---|---|
| 9 | $256 \pm 16$ | $256 \pm 16$ | $2^{10}$ |
| 8 | $128 \pm 24$ | $128 \pm 24$ | $2^{18}$ |
| 7 | $64 \pm 28$ | $64 \pm 20$ | $2^{18}$ |
| 6 | $32 \pm 30$ | $32 \pm 20$ | $2^{22}$ |
| 5 | $16 \pm 16$ | $16 \pm 16$ | $2^{22}$ |

Thank you for your attention!

alekseev@cryptopro.ru
lyudmila.kuschinskaja@yandex.ru