Polyhedrons over Finite Abelian Groups and Their Cryptographic Applications*

Logachev O.A. Salnikov A.A. Yaschenko V.V.

Institute for Information Security Issues of Moscow University, RUSSIA
orfeo@rambler.ru

1 Introduction

The algebraic method for stream-cipher key recovering was developed in [5]. The essence of this method is in solving the system of nonlinear equations which are the simplified consequences of the enciphering equations. The different questions on this method were investigated in [5, 6, 7]. We are using the group-theory methods for justification of algebraic method in cryptanalysis. We are considering the case of general Abelian group transformations instead of elementary Abelian 2-groups transformations. On the group-theory setting we consider the embedding of a subset into a certain coset of Abelian group. We apply those results for investigation of Boolean functions cryptographic properties.

2 Polyhedrons over Finite Abelian Groups

Let G be a finite Abelian group with respect to the multiplicative operation; by N we denote the order of G. Let $\widehat{G}$ be the character group of G. For any set $D \subseteq G$ let Z_D be the complex-valued map of $\widehat{G}$ such that

$$Z_D(\chi) = \sum_{x \in D} \chi(x) \ ,$$

*Partially supported by Russian Found on Basic Research (project numbers 02-01-00581 and 02-01-00687)

for all $\chi \in \widehat{G}$. The set D is uniquely defined by Z_D since orthogonal relations for group characters (see [2]):

$$\frac{1}{N}\sum_{\chi\in\widehat{G}} Z_D(\chi)\chi(y^{-1}) = \begin{cases} 1, & \text{if } y \in D, \\ 0, & \text{if } y \notin D. \end{cases}$$

For values $Z_D(\chi)$ we have the equation similar to Parseval equation for Fourier coefficients of finite Abelian group (see [2]):

$$\sum_{\chi\in\widehat{G}} |Z_D(\chi)|^2 = \sum_{\chi\in\widehat{G}}\sum_{x,y\in D} \chi(x)\overline{\chi}(y) = \sum_{x,y\in D}\left(\sum_{\chi\in\widehat{G}} \chi\left(xy^{-1}\right)\right) = N \cdot \#D \ . \quad (1)$$

Using equation (1) we get

Lemma 1. *The set D coincides with the group G iff*

$$Z_D(\chi) = \sum_{x\in D} \chi(x) = 0 \quad \textit{for all } \chi \in \widehat{G},\ \chi \neq \chi_0.$$

Proof. If we distinguish in the sum $\sum\limits_{\chi\in\widehat{G}} |Z_D(\chi)|^2$ the summand for $\chi = \chi_0$ then from (1) we obtain

$$\sum_{\substack{\chi\in\widehat{G} \\ \chi\neq\chi_0}} |Z_D(\chi)|^2 = \#D\,(N - \#D) \ . \quad (2)$$

Therefor, $\#D = N$ iff

$$Z_D(\chi) = 0 \quad \text{for all } \chi \in \widehat{G},\ \chi \neq \chi_0.$$

$\blacksquare$

Any coset in finite Abelian group we will call *polyhedron* in order to distinguish them among all subsets. This term will help us to use in some cases geometric intuition. A useful tool for structure investigation of a finite Abelian group subset is it's "localization" by imbedding into the least possible polyhedron. More formally the task of "localization" is formulated in the following way: for any set $D \subseteq G$ find the least subgroup $H < G$ such that $D \subseteq x_0 H$ for some $x_0 \in D$. We will use the following notions.

$$\widehat{D} = \left\{\, \chi \in \widehat{G} \mid \chi(x) = \text{const for any } x \in D \,\right\} \ ,$$
$$A\left(\widehat{D}\right) = \left\{\, x \in G \mid \chi(x) = 1 \text{ for any } \chi \in \widehat{D} \,\right\} \ .$$

It is obvious that $\widehat{D}$ is subgroup in $\widehat{G}$ and that $A(\widehat{D})$ is subgroup in G.

Theorem 2. *$A(\widehat{D})$ is the least subgroup among all subgroups H of group G for which*

$$x_0^{-1}D \subseteq H \quad \textit{for some } x_0 \in D.$$

Proof. To each subgroup H of group G assign the subset H^* of group $\widehat{G}$

$$H^* = \left\{ \chi \in \widehat{G} \mid \chi(x) = 1 \text{ for any } x \in H \right\} \ .$$

It is well known [1] that the map $H \mapsto H^*$ is antiisomorphism for subgroups structures of group G and group $\widehat{G}$. For the set $D \subseteq G$ consider two set of subgroups

$$\mathfrak{G}(D) = \left\{ H < G \mid x_0^{-1}D \subseteq H \text{ for some } x_0 \in D \right\} \ ,$$
$$\widehat{\mathfrak{G}}(D) = \text{the set of all subgroups of the group } \widehat{D} \ .$$

Let's proof that the map $H \mapsto H^*$ is the antiisomorphism from $\mathfrak{G}(D)$ to $\widehat{\mathfrak{G}}(D)$. If $H \in \mathfrak{G}(D)$ then for any $\chi \in H^*$ and $y \in D$ we have $\chi(x_0^{-1}y) = 1$. The last equation holds iff any character $\chi \in H^*$ is constant on the set D and this means that $H^* \in \widehat{\mathfrak{G}}(D)$. It easy to check that the inverse inclusion is held. Note that

$$\left(A\left(\widehat{D}\right)\right)^* = \widehat{D} \ .$$

As the map $H \mapsto H^*$ is antiisomorphism and $\widehat{D}$ is the greatest element in $\widehat{\mathfrak{G}}(D)$ then $A\left(\widehat{D}\right)$ is the least element in $\mathfrak{G}(D)$. ■

Note that the function $Z_D(\chi)$ is helpful for searching the set $\widehat{D}$ due to the following evident equations

$$\widehat{D} = \left\{ \chi \in \widehat{G} \mid \ |Z_D(\chi)| = \#D \right\} \ .$$

The absolute value of function $Z_D(\chi)$ is constant on the cosets $\widehat{G}$ for $\widehat{D}$ because for any $\chi' \in \widehat{D}$ and any $\chi \in \widehat{G}$ and some $x_0 \in D$ we get

$$Z_D(\chi\chi') = Z_D(\chi)\chi'(x_0) \ .$$

It is evident that in the last equation it is sufficient to consider χ from the character group of the group $A(\widehat{D})$. Using the last remarks, lemma 1 and theorem 2 it is easy to proof the following theorem.

Theorem 3. *The set $D \subseteq G$ is polyhedron in group G iff the absolute value of function $Z_D(\chi)$ over $\widehat{G}$ takes only two values — 0 or $\#D$.*

3 Applications for Boolean Functions

Now we consider applications of those results for investigation of Boolean functions' cryptographic properties. We will use the notions and results from [8]. Let $G = V_n$ be n-dimensional vector space over the field of two elements, $\widehat{G} = \left\{ (-1)^{\langle \boldsymbol{\alpha}, \boldsymbol{x} \rangle} \mid \boldsymbol{\alpha}, \boldsymbol{x} \in V_n \right\}$, $\langle \boldsymbol{\alpha}, \boldsymbol{x} \rangle = \alpha_1 x_1 + \ldots + \alpha_n x_n$, $D = \{ \boldsymbol{x} \in V_n \mid f(\boldsymbol{x}) = 1 \}$, where $f(\boldsymbol{x})$ is a Boolean function. Then

$$
\begin{aligned}
Z_D(\chi) = Z_f(\boldsymbol{\alpha}) = \sum_{\boldsymbol{x}: f(\boldsymbol{x})=1} (-1)^{\langle \boldsymbol{\alpha}, \boldsymbol{x} \rangle} = \\
= \frac{1}{2} \left(\sum_{\boldsymbol{x} \in V_n} (-1)^{\langle \boldsymbol{\alpha}, \boldsymbol{x} \rangle} - \sum_{\boldsymbol{x} \in V_n} (-1)^{f(\boldsymbol{x}) + \langle \boldsymbol{\alpha}, \boldsymbol{x} \rangle} \right) = \\
= \begin{cases} 2^{n-1} - \dfrac{1}{2} W_f(\mathbf{0}), & \boldsymbol{\alpha} = \mathbf{0}; \\ -\dfrac{1}{2} W_f(\boldsymbol{\alpha}), & \boldsymbol{\alpha} \neq \mathbf{0}, \end{cases}
\end{aligned}
$$

where $W_f(\boldsymbol{\alpha})$ is the Walsh-Hadamard coefficients and then

$$
\widehat{D} = \left\{ \boldsymbol{\alpha} \in V_n \mid \boldsymbol{\alpha} \neq \mathbf{0},\ |W_f(\boldsymbol{\alpha})| = 2^n - W_f(\mathbf{0}) \right\} \cup \{ \mathbf{0} \} \ . \tag{3}
$$

Polyhedrons in V_n are cosets with respect to subspaces of V_n or in the terms of finite geometries they are plains.

Theorem 3 for Boolean case is formulated in the following way.

Corollary 4. *Function $f(\boldsymbol{x})$ is indication-function for a coset of k-dimensional subspace iff $|W_f(\boldsymbol{\alpha})|$ for all $\boldsymbol{\alpha} \in V_n$, $\boldsymbol{\alpha} \neq \mathbf{0}$ takes only two values 0 and 2^{k+1}.*

Let $\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_k \in V_n$ be a basis of subspace $\widehat{D}$ defined by (3), $\boldsymbol{x}_0 \in V_n$ is an arbitrary vector such that $f(\boldsymbol{x}_0) = 1$. Then

$$
A\left(\widehat{D}\right) = \{ \boldsymbol{x} \in V_n \mid \langle \boldsymbol{\alpha}_i, \boldsymbol{x} \rangle = 0,\ i = 1, \ldots, k \} \ ,
$$

and theorem 2 states, that if $f(\boldsymbol{x}) = 1$ then $\langle \boldsymbol{\alpha}_i, \boldsymbol{x} \rangle = \langle \boldsymbol{\alpha}_i, \boldsymbol{x}_0 \rangle$, $i = 1, \ldots, k$. In other words, the truth set of Boolean function $f(\boldsymbol{x})$ is embedded into the plain defined by the following linear equations

$$
\begin{cases} \langle \boldsymbol{\alpha}_1, \boldsymbol{x} \rangle = \langle \boldsymbol{\alpha}_1, \boldsymbol{x}_0 \rangle, \\ \ldots \\ \langle \boldsymbol{\alpha}_k, \boldsymbol{x} \rangle = \langle \boldsymbol{\alpha}_k, \boldsymbol{x}_0 \rangle. \end{cases} \tag{4}
$$

So, for Boolean functions theorem 2 can be reformulated in the following way.

Theorem 5. *For any Boolean function $f(\boldsymbol{x})$ there is a decomposition*

$$f\left(x_1,\ldots,x_n\right) = \\ = \left(\left\langle \boldsymbol{\alpha}_1, \boldsymbol{x}+\boldsymbol{x}_0\right\rangle+1\right)\cdot\ldots\cdot\left(\left\langle \boldsymbol{\alpha}_k, \boldsymbol{x}+\boldsymbol{x}_0\right\rangle+1\right)\psi\left(\left\langle \boldsymbol{\alpha}_{k+1}, \boldsymbol{x}\right\rangle,\ldots,\left\langle \boldsymbol{\alpha}_n, \boldsymbol{x}\right\rangle\right)\ . \tag{5}$$

Decomposition (5) for function $f(\boldsymbol{x})$ defined uniquely in the following sense

- $\boldsymbol{\alpha}_1,\ldots,\boldsymbol{\alpha}_k$ *is an arbitrary basis of a subspace uniquely defined for function $f(\boldsymbol{x})$;*
- $\boldsymbol{\alpha}_{k+1},\ldots,\boldsymbol{\alpha}_n$ *is an arbitrary complementation of $\boldsymbol{\alpha}_1,\ldots,\boldsymbol{\alpha}_k$ for basis of V_n;*
- $\boldsymbol{x}_0 \in V_n$ *is an arbitrary vector such that $f(\boldsymbol{x}) = 1$;*
- *Boolean function $\psi\big(\boldsymbol{y}_1,\ldots,\boldsymbol{y}_{n-k}\big)$ over $n-k$ variables can't be decomposed in the form of (5) and defined uniquely for the function $f(\boldsymbol{x})$.*

Clear that it is more easy to investigate the properties of function $f(\boldsymbol{x})$ when it is decomposed in the form (5). Particulary, decomposition (5) is connected with the annihilator group introduced in [5, 6, 7] for algebraic method of cryptanalysis. Function $\varphi(\boldsymbol{x})$ is called *annihilator* for function $f(\boldsymbol{x})$ if for all $\boldsymbol{x} \in V_n$ the following equation hold:

$$\varphi(\boldsymbol{x})f(\boldsymbol{x}) = 0\ .$$

From the previous the following statement is evident.

Corollary 6. *Let function $f(\boldsymbol{x})$ be decomposed in the form (5). Then the affine annihilator group for function $f(\boldsymbol{x})$ coincides with the linear span of the affine functions set $\langle \boldsymbol{\alpha}_1, \boldsymbol{x}\rangle + \langle \boldsymbol{\alpha}_1, \boldsymbol{x}_0\rangle, \ldots, \langle \boldsymbol{\alpha}_k, \boldsymbol{x}\rangle + \langle \boldsymbol{\alpha}_k, \boldsymbol{x}_0\rangle$, and function $\psi\big(\boldsymbol{y}_1,\ldots,\boldsymbol{y}_{n-k}\big)$ has a trivial affine annihilator group (i.e. only the zero-function).*

So, all the previous constructions lead to the algorithm for searching of all affine annihilator for a given Boolean function $f(\boldsymbol{x})$ from it's Walsh-Hadard coefficients $W_f(\boldsymbol{\alpha})$. It is interesting to find other annihilator for function $f(\boldsymbol{x})$ from it's Walsh-Hadard coefficients.

Theorem 7. *Boolean function $\varphi(\boldsymbol{x})$ is annihilator for function $f(\boldsymbol{x})$ iff one of two equivalent conditions hold:*

1. $W_f(\mathbf{0}) + W_\varphi(\mathbf{0}) - W_{f+\varphi}(\mathbf{0}) = 2^n$;

2. $W_f(\boldsymbol{\alpha}) + W_\varphi(\boldsymbol{\alpha}) - W_{f+\varphi}(\boldsymbol{\alpha}) = 0$ *for all* $\boldsymbol{\alpha} \in V_n$*,* $\boldsymbol{\alpha} \neq \mathbf{0}$*.*

Proof. From following evident equation

$$(-1)^{f(\boldsymbol{x})\varphi(\boldsymbol{x})} = \frac{(-1)^0 + (-1)^{f(\boldsymbol{x})} + (-1)^{\varphi(\boldsymbol{x})} - (-1)^{f(\boldsymbol{x})+\varphi(\boldsymbol{x})}}{2} \ ,$$

for all $\boldsymbol{\alpha} \in V_n$ we get

$$W_{f\varphi}(\boldsymbol{\alpha}) = \frac{1}{2}\left(W_0(\boldsymbol{\alpha}) + W_f(\boldsymbol{\alpha}) + W_\varphi(\boldsymbol{\alpha}) - W_{f+\varphi}(\boldsymbol{\alpha})\right) \ . \tag{6}$$

Equation $f(\boldsymbol{x})\varphi(\boldsymbol{x}) \equiv 0$ hold iff one of two equivalent conditions hold:

1. $W_{f\varphi}(\mathbf{0}) = 2^n$;
2. $W_{f\varphi}(\mathbf{0}) = 0$ for all $\boldsymbol{\alpha} \in V_n$, $\boldsymbol{\alpha} \neq \mathbf{0}$.

Then from (6) we get the theorem. ■

Sometimes it is more convenient to put down the terms of theorem 7 in the following symmetric form:

1. $W_{f+\varphi+1}(\mathbf{0}) = 2^n - \big(W_f(\mathbf{0}) + W_\varphi(\mathbf{0})\big)$;
2. $W_{f+\varphi+1}(\boldsymbol{\alpha}) = -\big(W_f(\boldsymbol{\alpha}) + W_\varphi(\boldsymbol{\alpha})\big)$ for all $\boldsymbol{\alpha} \in V_n$, $\boldsymbol{\alpha} \neq \mathbf{0}$.

It easy to see that if $f(\boldsymbol{x})\varphi(\boldsymbol{x}) \equiv 0$, then $W_f(\mathbf{0}) + W_\varphi(\mathbf{0}) \geqslant 0$. Moreover $W_f(\mathbf{0}) + W_\varphi(\mathbf{0}) = 0$ iff $f(\boldsymbol{x}) + \varphi(\boldsymbol{x}) \equiv 1$. Annihilator $f(\boldsymbol{x}) + 1$ is called *trivial*.

From theorem 7 it is easy to get

Corollary 8. *Function*

$$\varphi(\boldsymbol{x}) = \begin{cases} 1, & \textit{if } \boldsymbol{x} \in L + \boldsymbol{x}_0; \\ 0, & \textit{if } \boldsymbol{x} \notin L + \boldsymbol{x}_0, \end{cases}$$

is annihilator for Boolean function $f(\boldsymbol{x})$ *iff*

$$\sum_{\boldsymbol{\gamma} \in L^\perp} (-1)^{\langle \boldsymbol{\gamma}, \boldsymbol{x}_0 \rangle} W_f(\boldsymbol{\gamma}) = 2^n \ .$$

Corollary 9. *There are no affine annihilator for nonaffine plateatued and nonaffine balanced Boolean functions.*

Proof. All affine annihilator $\langle \boldsymbol{\alpha}, \boldsymbol{x} \rangle + \varepsilon$, $\boldsymbol{\alpha} \neq \mathbf{0}$ for function $f(\boldsymbol{x})$ are described by (3):

$$\left| W_f(\boldsymbol{\alpha}) \right| = 2^n - W_f(\mathbf{0}) \ .$$

If function f balanced, i.e. $W_f(\mathbf{0}) = 0$ and has affine annihilator then $\left| W_f(\boldsymbol{\alpha}) \right| = 2^n$ i.e. f is affine.

Plateaued of order $2r$ functions defined by the condition [3, 4]:

$$\left| W_f(\boldsymbol{\alpha}) \right| \text{ takes only two values } 0,\ 2^{n-r}.$$

Then it is evident that if $r \neq 0$, i.e. function is not affine, then condition (3) do not held for every $\boldsymbol{\alpha}$. ■

In particular quadratic Boolean functions do not have affine annihilator.

Corollary 10. *Two nonaffine plateaued functions with nonintersecting supports do not annihilate each other.*

Proof. Since the supports of f and φ don't intersect, i.e. $W_f(\boldsymbol{\alpha}) W_\varphi(\boldsymbol{\alpha}) = 0$ for all $\boldsymbol{\alpha} \in V_n$, then

$$W_{f+\varphi}(\mathbf{0}) = \frac{1}{2^n} \sum_{\boldsymbol{\alpha} \in V_n} W_f(\boldsymbol{\alpha}) W_\varphi(\boldsymbol{\alpha}) = 0 \ .$$

Hence f and φ annihilate each other iff

$$W_f(\mathbf{0}) + W_\varphi(\mathbf{0}) = 2^n \ .$$

It contradict to the conditions of 10. ■

Lemma 11. *Let $f(\boldsymbol{x})\varphi(\boldsymbol{x}) \equiv 0$ $f(\boldsymbol{x})$, $\varphi(\boldsymbol{x})$ be a bent-function $f(\boldsymbol{x}) + \varphi(\boldsymbol{x}) + 1 \not\equiv 0$. Then $f(\boldsymbol{x}) + \varphi(\boldsymbol{x}) + 1$ is indicator-function for coset of $n/2$-dimensional subspace.*

Proof. From conditions of theorem 7 the lemma we obviously get

$$\begin{aligned} &W_{f+\varphi+1}(\mathbf{0}) = 2^n - 2^{n/2+1}, \\ &W_{f+\varphi+1}(\boldsymbol{\alpha}) \in \left\{ 0, \pm 2^{n/2+1} \right\} \text{ for any } \boldsymbol{\alpha} \neq \mathbf{0}. \end{aligned}$$

The last equations and the conditions of 4 get lemma. ■

Corollary 12. *If $f(\boldsymbol{x})$, $\varphi(\boldsymbol{x})$ is bent-function, $\deg ff < n/2$ and $f(\boldsymbol{x}) + \varphi(\boldsymbol{x}) \not\equiv 1$ then functions $f(\boldsymbol{x})$ and $\varphi(\boldsymbol{x})$ do not annihilate each other.*

Lemma 13. *Let $f(\boldsymbol{x})$ be a plateaued of order $2r$ function and $\varphi(\boldsymbol{x})$ be a plateaued of order $2s$. If $r \geqslant 2$, $s \geqslant r+1$ or $r = 1$, $s \geqslant 3$ then functions $f(\boldsymbol{x})$ and $\varphi(\boldsymbol{x})$ do not annihilate each other.*

Proof. Suppose contrary. Then from the conditions of theorem 7 we get

$$|2^n - (W_f(\mathbf{0}) + W_\varphi(\mathbf{0}))| = |W_{f+\varphi+1}(\mathbf{0})| \leqslant \max_{\boldsymbol{\alpha} \in V_n} |W_\varphi(\boldsymbol{\alpha})| \ .$$
$$\frac{1}{2^n} \sum_{\boldsymbol{\alpha} \in V_n} |W_\varphi(\boldsymbol{\alpha})| = 2^{n-s} \cdot \frac{1}{2^n} \cdot 2^{n-r} \cdot 2^{2r} = 2^{n-s+r} \ . \tag{7}$$

Obviously there are 4 possible values of $W_f(\mathbf{0}) + W_f(\mathbf{0})$. Put them in increasing order:

$$2^{n-s} \leqslant 2^{n-r} - 2^{n-s} < 2^{n-r} < 2^{n-s} + 2^{n-r} \ .$$

Hence the least possible value for $|2^n - (W_f(\mathbf{0}) + W_\varphi(\mathbf{0}))|$ is $2^n - 2^{n-s} - 2^{n-r}$. If we proof inequality

$$2^n - \left(2^{n-s} + 2^{n-r}\right) > 2^{n-s+r} \ , \tag{8}$$

then we will get a contradiction with inequality (7) and hence we will proof lemma. Inequality (8) is equivalent to inequality

$$2^n - 2^{n-s+r} > 2^{n-s} + 2^{n-r} \ ,$$

which is equivalent to inequality

$$2^r > \frac{2^s + 2^r}{2^s - 2^r} = 1 + \frac{2}{2^{s-r} - 1} \ .$$

The right part of the last inequality monotone decreasing when $s - r$ increasing and hence inequality (7) is held. ∎

Remark 14. We have to consider two more cases to answer the question when do two plateaued functions annihilate each other:

1. $r = 1$, $s = 2$;

2. $r = s$.

References

[1] Birkhoff G. *Lattice Theory.* 3-d Edition, Amer. Math. Soc., Providence, R.I., 1967.

[2] Serre G.-P. *Representations Lineares des Groupes Finit.* Collection Methodes, Hermann, Paris, 1967.

[3] Zheng Y., Zhang X.-M. *On Plateaued Functions.* IEEE Trans. on Information Theory, **V. 47**, No. 3, Pp. 1215–1223, 2001.

[4] Carlet C., Prauff I.E. . *On Plateaued Functions and their Constructions.* FSE'2003.

[5] Courtois N.T., Meier W. *Algebraic Attacks on Stream Cipher with Linear Feedback.* EUROCRYPT'2003, LNCS 2656, PP. 345–369, 2003.

[6] Courtois N.T. *Fast Algebraic Attacks on Stream Cipher with Linear Feedback.* CRYPTO'2003, LNCS 2729, PP. 176–194, 2003.

[7] Meier W., Pasalic E., Carlet C. *Algebraic Attacks and Decomposition of Boolean Functions.* EUROCRYPT'2004, LNCS 3027, PP. 474–491, 2004.

[8] Logachev O.A., Salnikov A.A., Yaschenko V.V. *Boolean Functions in Coding Theory and Cryptology.* MCCME, Moscow, 2004. (in Russian)