Locally Invertible Boolean Mappings*

O.A.Logachev

Information Security Institute,
Lomonosov University, Moscow
e-mail: logol@iisi.msu.ru

Abstract

The aim of this paper is to study a novel property of Boolean mappings called local intertibility. We focus on local invertibility of Boolean mappings which model filtering generators and study the case when filtering function is linear in the last variable.

Keywords: Boolean mapping, Boolean function, locally invertible mapping, resetable mapping.

1 Introduction

Local invertability of Boolean mappings which correspond to filtering generators is of primary importance for cryptanalysis. Usually to invert a mapping Φ amounts to compute for an image y of Φ any pre-image $\mathrm{x} \in \Phi^{-1}(\mathrm{y})$. We focus on the next problem: is there a value y in the range of Φ such that all points in $\Phi^{-1}(y)$ belong to the same affine plane. This property allows to write down a system of linear equations with key bits as unknowns.

2 Preliminaries

Let $\mathbb{F}_2 = GF(2)$ be the finite field with two elements and let $\mathbb{N}$ be the set of positive integers. We denote by $\mathrm{V}_n = \mathbb{F}_2^n,\ n \in \mathbb{N}$ the vector space of n-tuples $\mathrm{x} = (\mathrm{x}_1, \ldots, \mathrm{x}_n),\ \mathrm{x}_i \in \mathbb{F}_2,\ i = 1, \ldots, n$. Let $\mathcal{V} = \mathbb{F}_2^\infty$ be the set of all infinite sequences over $\mathbb{F}_2$. Elements of the set $\mathcal{V}$ we denote by $x = (x_i)_{i=1}^\infty$. We define a truncation operator on $\mathcal{V}$ as follows:

1. $(x)_{i,s} = (x_i, x_{i+1}, \ldots, x_{i+s-1}) \in \mathrm{V}_s,\ i = 1, 2, \ldots;\ s = 1, 2, \ldots.$
2. $(x)_{i,\infty} = (x_i, x_{i+1}, \ldots, x_{i+t}, \ldots) \in \mathcal{V},\ i = 1, 2, \ldots;\ s = \infty.$

*This research was partially supported by RFBR grant N 07-01-00154.

Analogously we define a truncation operator on V_n:

$$(\mathrm{x})_{i,s} = (\mathrm{x}_i, \mathrm{x}_{i+1}, \ldots, \mathrm{x}_{i+s-1}) \in \mathrm{V}_s,\ x \in \mathrm{V}_n,\ 1 \le i \le n,\ 1 \le s \le n-i+1.$$

Let $\mathcal{F}_n$ be the set of all Boolean functions in n variables. For any Boolean function $f : \mathrm{V}_n \to \mathbb{F}_2$ we define a mapping $f^* : \mathcal{V} \to \mathcal{V}$ as follows:

$$f^*(x) = \left(f\left((x)_{1,n}\right), f\left((x)_{2,n}\right), \ldots, f\left((x)_{t,n}\right), \ldots\right),$$

$x \in \mathcal{V}$. This mapping corresponds to binary shift register of length n without feedback with filtering Boolean function f.

Definition 2.1. Let $f \in \mathcal{F}_n$. A mapping f^* is called locally invertible if there exist $m \in \mathbb{N}$ and m-tuple $\mathrm{y} \in \mathrm{V}_m$, such that:

(i)
$$\mathcal{D}(f^*, \mathrm{y}) = \left\{z \in \mathcal{V} | (f^*)^{-1}(\mathrm{y}, z) \neq \varnothing\right\} \neq \varnothing; \tag{2.1}$$

(ii) for any $w, w' \in (f^*)^{-1}(\mathrm{y}, z)$, $z \in \mathcal{D}(f^*, \mathrm{y})$, an equation $(w)_{m+1,\infty} = (w')_{m+1,\infty}$ holds.

We denote by $\mathrm{Inv}(f^*)$ the set of all such m-tuples y of a mapping f^*.

Let $\rho_f(\cdot, \varepsilon) : \mathrm{V}_n \to \mathrm{V}_n$, $\varepsilon = 0, 1$ be mappings that correspond to non-autonomous binary shift register of length n with feedback function $f \in \mathcal{F}_n$:

$$\rho_f(\mathrm{x}, \varepsilon) = \rho_f\left((\mathrm{x}_1, \ldots, \mathrm{x}_n), \varepsilon\right) = (\mathrm{x}_2, \ldots, \mathrm{x}_n, f(\mathrm{x}_1, \ldots, \mathrm{x}_n) \oplus \varepsilon),$$

where $\mathrm{x} \in \mathrm{V}_n$, $\varepsilon \in \mathbb{F}_2$ and $\oplus$ denotes addition over $\mathbb{F}_2$. If $\mathrm{u} = (\mathrm{u}_1, \mathrm{u}_2, \ldots, \mathrm{u}_l)$, then

$$\rho_f(\mathrm{x}, \mathrm{u}) = \rho_f(\ldots, \rho_f(\rho_f(\mathrm{x}, \mathrm{u}_1), \mathrm{u}_2), \ldots, \mathrm{u}_l).$$

Definition 2.2. Let $f \in \mathcal{F}_n$. A mapping ρ_f is called resetable if there exist $l \in \mathbb{N}$, $\mathrm{y} \in \mathrm{V}_l$ and $\mathrm{z} = \mathrm{z}(\mathrm{y}) \in \mathrm{V}_n$ such that

$$\rho_f(\mathrm{x}, \mathrm{y}) = \mathrm{z} = \mathrm{z}(\mathrm{y})$$

for any $\mathrm{x} \in \mathrm{V}_n$. An n-tuple y is called reset tuple for the mapping ρ_f.

Resetable mappings were studied in [1].

Proposition 2.3. Let $f \in \mathcal{F}_n$. A mapping ρ_f is resetable iff for any $\mathrm{x}, \mathrm{x}' \in \mathrm{V}_n$, $\mathrm{x} \neq \mathrm{x}'$, there exist $\mathrm{y} = \mathrm{y}(\mathrm{x}, \mathrm{x}') \in \mathrm{V}_s$ and $s = s(\mathrm{x}, \mathrm{x}')$ such that $\rho_f(\mathrm{x}, \mathrm{y}) = \rho_f(\mathrm{x}', \mathrm{y})$.

Proof. Follows from the Definition 2.2. □

3 Main Result

Theorem 3.1.
Let $f \in \mathcal{F}_{n+1}$ be of the form

$$f(x_1, \ldots, x_n, x_{n+1}) = g(x_1, \ldots, x_n) \oplus x_{n+1}, \tag{3.1}$$

where $g \in \mathcal{F}_n$. The mapping f^* is locally invertible iff the mapping ρ_f is resetable.

Proof.

Note that a Boolean function f of the form (3.1) is perfectly balanced (see [2, 3]). Therefore for any sequence $z \in \mathcal{V}$ we have $\sharp(f^*)^{-1}(z) = 2^n$ ($\sharp C$ denotes cardinality of the set C) and for each $\mathrm{b} \in \mathrm{V}_n$ there exists a sequence $x \in (f^*)^{-1}(z)$ such that $(x)_{1,n} = \mathrm{b}$.

Necessity. Let $f \in \mathcal{F}_{n+1}$ be of the form (3.1). Suppose the mapping f^* is locally invertible. Hence for some $m \in \mathbb{N}$ there exists m-tuple y such that (2.1) holds. Let z be any sequence in $\mathcal{D}(f^*, \mathrm{y}) = \mathcal{V}$. Denote by $\mathrm{M}\,(f^*, (\mathrm{y}, z))$ an infinite table of sequences in $(f^*)^{-1}\,((\mathrm{y}, z))$:

$$\mathrm{M}\,(f^*, (\mathrm{y}, z)) = \begin{bmatrix} x^1 \\ x^2 \\ \vdots \\ x^{2^n} \end{bmatrix} = \begin{bmatrix} x_1^1 & x_2^1 & \dots & x_{m+1}^1 & \dots & x_{m+n}^1 & \dots \\ x_1^2 & x_2^2 & \dots & x_{m+1}^2 & \dots & x_{m+n}^2 & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ x_1^{2^n} & x_2^{2^n} & \dots & x_{m+1}^{2^n} & \dots & x_{m+n}^{2^n} & \dots \end{bmatrix} \tag{3.2}$$

Consider arbitrary but fixed ordering of these sequences. Rows restricted to first n columns of this table compose the vector space V_n. Using (2.1) we get $(x^1)_{m+1,\infty} = (x^2)_{m+1,\infty} = \ldots = (x^{2^n})_{m+1,\infty}$. Hence

$$\left(x_{m+1}^1, \ldots, x_{m+n}^1\right) = \left(x_{m+1}^2, \ldots, x_{m+n}^2\right) = \ldots = \left(x_{m+1}^{2^n}, \ldots, x_{m+n}^{2^n}\right) = a$$

for some $a \in \mathrm{V}_n$. Furthermore one has

$$\mathrm{y}_i = f(x_i^k, \ldots, x_{i+n}^k) = g(x_i^k, \ldots, x_{i+n-1}^k) \oplus x_{i+n}^k, \tag{3.3}$$

$k = 1, 2, \ldots, 2^n;\ i = 1, 2, \ldots, m$. Therefore

$$\rho_g\left((x_1^k, \ldots, x_n^k), y\right) = (x_{m+1}^k, \ldots, x_{m+n}^k) = a,$$

for any $k = 1, 2, \ldots, 2^n$. Hence ρ_g is a resetable mapping.

Sufficiency. Let $f \in \mathcal{F}_{n+1}$ be of the form (3.1). Suppose a mapping ρ_g is resetable. Then for some $m \in \mathbb{N}$ there exists a reset tuple y such that

$$\rho_f(\mathrm{x},\mathrm{y}) = \mathrm{b} = \mathrm{b}(\mathrm{y}),\ \mathrm{b} \in \mathrm{V}_n \tag{3.4}$$

for any $\mathrm{x} \in \mathrm{V}_n$. Let z be any sequence in $\mathcal{V}$. Since the function f is linear in the last variable it follows that $(f^*)^{-1}\,((\mathrm{y}, z)) = \left\{x^1, \ldots, x^{2^n}\right\}$ and $\left\{(x^1)_{1,n}, \ldots, (x^{2^n})_{1,n}\right\} = \mathrm{V}_n$. Using (3.3), 3.4) one gets

$$(x)_{m+1,n} = \mathrm{b} \tag{3.5}$$

for any $x \in (f^*)^{-1}\,((\mathrm{y}, z))$. Let $x, x' \in (f^*)^{-1}((\mathrm{y}, z)),\ x \neq x'$. Combining (3.1) and (3.5) we obtain $(x)_{m+1,\infty} = (x')_{m+1,\infty}$. □

4 Examples

Example 4.1. Let $f \in \mathcal{F}_n$ and $f(\mathrm{x}_1 \oplus 1, \ldots, \mathrm{x}_n \oplus 1) = f(\mathrm{x}_1, \ldots, \mathrm{x}_n)$. Then f^* is not locally invertible. If for a sequence $y \in \mathcal{V}$ one has $(f^*)^{-1}(y) \neq \varnothing$ and $x = (\mathrm{x}_1, \ldots, \mathrm{x}_t, \ldots) \in (f^*)^{-1}(y)$, then $x' = (\mathrm{x}_1 \oplus 1, \ldots, \mathrm{x}_t \oplus 1, \ldots) \in (f^*)^{-1}(y)$.

Example 4.2. Let $n \in \mathbb{N}$ be odd and let a function $g \in \mathcal{F}_n$ be of the form:

$$g(\mathrm{x}) = g(\mathrm{x}_1, \ldots, \mathrm{x}_n) = \begin{cases} 1, & \text{if } \sum\limits_{i=1}^{n} x_i \geq (n+1)/2; \\ 0, & \text{if } \sum\limits_{i=1}^{n} x_i \leq (n-1)/2. \end{cases}$$

Then f^* is locally invertible, where

$$f(\mathrm{x}_1, \ldots, \mathrm{x}_n, \mathrm{x}_{n+1}) = g(\mathrm{x}_1, \ldots, \mathrm{x}_n) \oplus \mathrm{x}_{n+1}.$$

Example 4.3. Let $g \in \mathcal{F}_n$ be a function of the form

$$g(\mathrm{x}) = g(\mathrm{x}_1, \ldots, \mathrm{x}_n) = \mathrm{x}_1 \oplus h(\mathrm{x}_1, \ldots, \mathrm{x}_n).$$

Then f^* is not locally invertible, where

$$f(\mathrm{x}_1, \ldots, \mathrm{x}_{n+1}) = g(\mathrm{x}_1, \ldots, \mathrm{x}_n) \oplus \mathrm{x}_{n+1} = \mathrm{x}_1 \oplus h(\mathrm{x}_2, \ldots, \mathrm{x}_n) \oplus \mathrm{x}_{n+1}.$$

References

[1] I.K.Ristsov. Reset Words of Solvable Automata. Kibernetika i Sistemnii Analis, №6, 1994, pp. 21-26 (in Russian).

[2] S.N.Sumarokov. Defects of Boolean Functions and Invertability of a Certain Class of Coding Circuits. Obozrenie Prikladnoi i Promyshlennoi Matematiki, v.1, no. 1, 1994, pp. 33-55 (in Russian).

[3] O.A. Logachev. On Perfectly Balanced Boolean Function.
http://eprint.iacr.org/2007/22.