➔ Regular Research Paper – NS

Cryptanalytical Invertibility of Functions of Four Variables

Moustapha Sylla
Department of Computer Engineering, Institute of Natural Sciences,
Suleyman Demirel University, Turkey
yl2130138005@ogr.sdu.edu.tr

Anar Adiloğlu Nabiyev
Department of Computer Engineering, Faculty of Engineering and Natural Sciences,
Suleyman Demirel University, Turkey
anaradiloglu@sdu.edu.tr

Abstract

Tests of cryptanalytic invertibility for functions of four arguments are proposed. Algorithms for constructing a recovery function and generating invertible functions are formulated.

Keymords *:* Invertibility of a function with respect to a variable, cryptanalytic invertibility, invertibility test, recovery function, *Mathematics Subject Glassification 2010:* 68W01, 68Q45.

1. INTRODUCTION

The concept of cryptanalytic invertibility of a function was introduced in [1, 2] as a generalization, on the one hand, of the concept of ordinary inverse of a function, and on the other, of cryptanalytic invertibility of a finite automaton [1 ,2]. The generalization of the concept of inverse of a function is made in two directions. Firstly, the inversion is made with respect to some variable where not the entire set of values of arguments is restored by the value of the function, but only the value of some variables; Secondly, quantifiers are used for restoration of the value of a variable, but it is not necessarily possible for all values of the remaining variables.

Definition 1 [1] A function $g(x_1, x_2, ..., x_n)$ is called invertible with respect to the variable $x_k(k = 1, 2, ..., n)$ of type $Q_1Q_2...Q_n$, where $Q_i \in \{\forall, \exists\}$ and $Q_k = \forall$ if there exists the restoring function f such that the formula

$$Q_1x_1Q_2x_2...Q_nx_n\ (f(g(x_1, x_2... x_n)\ = x_k) \qquad (1)$$

is true. It is clear that if a function is invertible in all variables of type ∀ then it is invertible in the classical sense. Let D_i be the range of x_i and y_i for $i \in \{1... n\}$. Also let $g(x_1... x_n)$ be a function in variables $x_1, ..., x_n$ with a range D_g, $k_0 \in \{1, ..., n\}$, and $Qk_0 = \forall$. Finally, let $f : D_g \to D_{h0}$ denotes an arbitrary function with the domain D_g and the range D_{h0} .The following lemmas from [1, 2] answers the existence questions of the invertible functions in the sense of Definition 1.

Lemma 1 [1] If $Q_k = \forall$ for all $k = 1, 2, ..., n$ then the function f with the property (1) exists if and only if

$$(g(x_1, x_2, ..., x_n)\ = g(y_1, y_2, ..., y_n) \Rightarrow x_{k0}\ = y_{k0}\ )$$

For some $x_1, x_2, ..., x_n$ and $y_1, y_2, ..., y_n$.

Lemma 2 [1] for any true quantifier logic formulas in a normal form $Q_1z_1...Q_m z_m A(z_1, ..., z_m)$ and $R_1z_1...R_m z_m B(z_1, ..., z_m)$, where $Q_i, R_i \in \{\forall, \exists\}$ and $Q_i R_i = \exists\exists$ for every $i \in \{1, ..., m\}$, there exist some values $c_1, ..., c_m$ of variables $z_1, ..., z_m$ respectively such that $A(c_1, ..., c_m) = B(c_1, ..., c_m)$ =true.

Lemma 3. For any function g, if there exists a function f with the property (1), then

$$Q_1x_1Q_2x_2...Q_nx_nQ_1y_1Q_2y_2...Q_ny_n\ (x_k0 \neq y_k0\ ) \Rightarrow g(x_1, x_2, ..., x_n) = g(y_1, y_2, ..., y_n).$$

For each type of invertibility, we have some important questions as a development of a invertibility test; development of an algorithm for constructing a recovery function; development of algorithms for generating invertible functions; counting or estimating the number of invertible functions. In [3] and [4] some of the above task are considered for the case $n = 2$ and $n = 3$. Our task in this paper to consider these problems for the case $n = 4$. Consider

$$g : D_1 \times D_2 \times D_3 \times D_4 \rightarrow D$$

where D_k, $(k = 1, 2, 3, 4,)$, D are arbitrary sets. Let us introduce the following notations: $|M|$ is the cardinality of the set M (finite or infinite); G_a is the set of values of the subfunction obtained from g by fixing the variable $x_1 = a$:

$$G_a = g(a, x_2, x_3, x_4) : x_k \in D_k,\ \ k = 2, 3, 4.$$

Some types of invertibility for $n = 4$ can be reduced to the cases $n = 2$ and $n = 3$. By the commutative law of quantifiers with the same symbols it is not necessity for considering all cases with different variables. All invertibiliy types for $n = 4$ are given in the following table:

Type of invertibility	Variable	Equivalent case for $n = 3$	Equivalent case for $n = 2$
∀∀∀∀	x_1	∀∀∀	∀∀
∀∀∀∃	x1	—	—
∀∀∃∀	x1, x4	—	—
∀∀∃∃	x1	∀∀∃	—
∀∃∀∀	x1, x3	—	—
∀∃∀∃	x1, x3	—	—
∀∃∃∀	x1, x4	∀∃∀	—
∀∃∃∃	x1	∀∃∃	∀∃
∃∀∀∀	x2	—	—
∃∀∀∃	x2	—	—
∃∀∃∀	x2,x4	—	—
∃∀∃∃	x2	∃∀∃	—
∃∃∀∀	x3	∃∀∀	—
∃∃∀∃	x3	∃∀∃	—
∃∃∃∀	x4	∃∃∀	∃∀

2. INVERTIBILITIES OF EQUIVALENT TYPES

From the above tables we see that equivalent types of invertibilities are

$$\forall\forall\forall\forall,\ \forall\forall\exists\exists,\ \forall\exists\exists\forall,\ \forall\exists\exists\exists,\ \exists\forall\exists\exists,\ \exists\exists\forall\forall,\ \exists\exists\forall\exists,\ \exists\exists\exists\forall.$$

Consider the first invertibility ∀∀∀∀. We see that

$$\forall x_1 \in D_1 \forall x_2 \in D_2 \forall x_3 \in D_3 \forall x_4 \in D_4 \simeq \forall x_1 \in D_1 \forall\, (x_2, x_3, x_4) \in D_2 \times D_3 \times D_4 \simeq \forall\, (x_1, x_2) \in D_1 \times D_2 6\, (x_3, x_4) \in D_3 \times D_4,$$

so firstly we needn't consider invertibility with respect x_1 x_2, x_3, x_4 separately and secondly we can reduce the problem to the invertibility of type 66 for the function $g(x, y)$ with $x \in D_1 \times D_2$ and $y \in D_3 \times D_4$. Analogously, for the type ∀∀∃∃ we have

$$\forall x_1 \in D_1 \forall x_2 \in D_2 \forall x_3 \in D_3 \forall x_4 \in D_4 \simeq \forall x_1 \in D_1 \forall x_2 \in D_2 \exists\, (x_3, x_4) \in D_3 \times D_4,$$

so we can reduce the problem to the invertibility of type ∀∀∃ for the function $g(x, y, z)$ with $x \in D_1$, $y \in D_2$ and $z \in D_3 \times D_4$. Note that by the similar way the remained equivalent invertibility types can be reduced to three or two variables cases.

3. INVERTIBILITY OF TYPE ∀∀∀∃ WITH RESPECT TO x_1

The function $g(x_1, x_2, x_3, x_4)$ is invertible of type 666I with respect to x_1 if

$$\exists f \forall x_1 \forall x_2 \forall x_3 \exists x_4\ \ (f(g(x_1, x_2, x_3, x_4)) = x_1).$$

Propsoition 1. A function $g : D_1 \times D_2 \times D_3 \times D_4 \to D$ is invertible of type 666∃ with respect to $x_1$if and only if there exists the map

$$\varphi\ : D_1 \times D_2 \times D_3 \to D_4$$

for which the condition

$$\forall a, \tilde{a} \in D_1 \forall b, \tilde{b} \in D_2, \forall c, \tilde{c} \in D_3, a \neq \tilde{a} \Rightarrow g(a, b, c, '(a, b, c)) \neq g\,(\tilde{a}, \tilde{b}, \tilde{c},\ '(\tilde{a}, \tilde{b}, \tilde{c})).\ (2)$$

The restoring function $f : D \to D_1$ is constructing by the following steps :

Step 1 $f(g(a, b, c, '(a, b, c)) = a$ for all $a \in D_1$, $b \in D_2$, $c \in D_3$;

Step 2 For $x \in D$ which is not defined on Step 1 $f(x)$ is equal to any value from the set D_1.

From (2) we have that Step 1 and Step 2 define the function f correctly.

The method for generating an invertible function

$$g : D_1 \times D_2 \times D_3 \times D_4 \to D$$

is described in algorithm 1.

Algorithm 1. Generating a function invertible of type 66I with respect to variable x_1

```
1 : Construct an arbitrary partition of set $D$ into classes $H_a$, $a \in D_1$.
```

```
2 : For all $a \in D_1$ :
3 : For all $b \in D_2$ :
4 : For all $c \in D_3$ :
5 : Choose $d \in D_4$, $z \in H_a$;
5 : Put $g(a, b, c, d) := z$;
∀ : For all $x_4 \in D_3 \backslash \{d\}$ choose an arbitrary $y \in D_1$ for the value of $g(a, b, c, x_4)$.
```

Algorithms for generating functions of other types of invertibility are similar and are not given here.

4. INVERTIBILITY OF TYPE ∀∀∃∀ WITH RESPECT TO x_1

The function $g(x_1, x_2, x_3, x_4)$ is invertible of type ∀∃ with respect to x_1

$$\exists f \forall x_1 \forall x_2 \exists x_3 \forall x_4 \ (f(g(x_1, x_2, x_3, x_4)) = x_1).$$

Proposition 2. A function $g : D_1 \times D_2 \times D_3 \times D_4 \rightarrow D$ is invertible of type 66I6 with respect to $x_1$if and only if there exists the map

$$\varphi : D_1 \times D_2 \rightarrow D_3$$

for which the condition

$$\forall a, \tilde{a} \in D_1 \forall b, \tilde{b} \in D_2, \forall d, \tilde{d} \in D_4, a \neq \tilde{a} \Rightarrow g(a, b, '(a, b), d) \neq g(\tilde{a}, \tilde{b}, '(\tilde{a}, \tilde{b}), \tilde{d}). \ (3)$$

The restoring function $f : D \rightarrow D_1$ is constructing by the following steps:
Step 3 $f(g(a, b, '(a, b), d) = a$ for all $a \in D_1, b \in D_2, d \in D_4$;
Step 4 For $x \in D$ which is not defined on Step 3 $f(x)$ is equal to any value from the set D_1.

From (3) we have that Step 3 and Step 4 define the function f correctly.

5. INVERTIBILITY OF TYPE ∀∀∃∀ WITH RESPECT TO x_4

The function $g(x_1, x_2, x_3, x_4)$ is invertible of type ∀∀∃∀ with respect to x_1 $\exists f$ $\forall x_1 \forall x_2 \exists x_3 \forall x_4 \ (f(g(x_1, x_2, x_3, x_4)) = x_4)$.

Proposition 3. A function $g : D_1 \times D_2 \times D_3 \times D_4 \rightarrow D$ is invertible of type ∀∀∃∀ with respect to x_4 if and only if there exists the map

$$\varphi : D_1 \times D_2 \rightarrow D_3$$

for which the condition

$$\forall a, \tilde{a} \in D_1 \forall b, \tilde{b} \in D_2, \forall d, \tilde{d} \in D_4, d \neq \tilde{d} \Rightarrow g(a, b, '(a, b), d) \neq g(\tilde{a}, \tilde{b}, '(\tilde{a}, \tilde{b}), \tilde{d}). \ (3)$$

The restoring function $f : D \rightarrow D_4$ is constructing by the following steps: Step 5 $f(g(a, b, '(a, b), d) = d$ for all $a \in D_1, b \in D_2, d \in D_4$;

Step ∀ for $x \in D$ which is not defined on Step 5 $f(x)$ is equal to any value from the set D_4.

From (3) we have that Step 5 and Step 6 define the function f correctly.

6. INVERTIBILITY OF TYPE ∀∃∀∀ WITH RESPECT TO x_1

The function $g(x_1, x_2, x_3, x_4)$ is invertible of type 6I66 with respect to x_1

$$\exists f \forall x_1 \exists x_2 \forall x_3 \forall x_4 \;\; (f(g(x_1, x_2, x_3, x_4)) = x_1).$$

Proposition 3. A function $g : D_1 \times D_2 \times D_3 \times D_4 \to D$ is invertible of type 6∃66 with respect to x_4 if and only if there exists the map

$$\varphi : D_1 \to D_2$$

For which the condition

$$\forall a, \tilde{a} \in D_1 \forall c, \tilde{c} \in D_3, \forall d, \tilde{d} \in D_4, a \neq \tilde{a} \Rightarrow g(a, '(a), c, d) \neq g(\tilde{a}, \; '(\tilde{a}), \tilde{c}, \tilde{d}). \quad (4)$$

The restoring function $f : D \to D_1$ is constructing by the following steps :

Step 7 $f(g(a, '(a), c, d) = a$ for all $a \in D_1, c \in D_3, d \in D_4$;

Step 8 for $x \in D$ which is not defined on Step 5 $f(x)$ is equal to any value from the set D_1.

From (4) we have that Step 7 and Step 8 define the function f correctly.

7. INVERTIBILITY OF TYPE ∀∃∀∀ WITH RESPECT TO x_3

The function $g(x_1, x_2, x_3, x_4)$ is invertible of type 6I66 with respect to x_3

$$\exists f \forall x_1 \exists x_2 \forall x_3 6 x_4 \;\; (f(g(x_1, x_2, x_3, x_4)) = x_3).$$

Proposition 4. A function $g : D_1 \times D_2 \times D_3 \times D_4 \to D$ is invertible of type ∀∃∀∃ with respect to x_3 if and only if there exists the map

$$\varphi : D_1 \to D_2$$

For which the condition

$$\forall a, \tilde{a} \in D_1 \forall c, \tilde{c} \in D_3, \forall d, \tilde{d} \in D_4, c \neq \tilde{c} \Rightarrow g(a, '(a), c, d) \neq g(\tilde{a}, \; '(\tilde{a}), \tilde{c}, \tilde{d}). \quad (5)$$

The restoring function $f: D \to D_3$ is constructing by the following steps:

Step 9 $f(g(a, '(a), c, d) = c$ for all $a \in D_1, c \in D_3, d \in D_4$;

Step 10 for $x \in D$ which is not defined on Step 5 $f(x)$ is equal to any value from the set D_3.

From (5) we have that Step 9 and Step 10 define the function f correctly.

By the similar way we can construct an invertible function g for the remained invertibility types in the table.

The proposed tests of invertibility are not constructive, since they require checking the existence of suitable values $a \in D_1$ and/or mappings $'$. It is necessary to develop algorithms for searching (constructing) such values and mappings. Finally It is interesting to count (or at least estimate) the number of reversible functions of different types. The task does not seem trivial, since with different choices of parameters, generation algorithms can produce the same invertible functions.

REFERENCES

[1] Agibalov G.P. Cryptanalytical finite automaton invertibility with finite delay. Applied discreet mathematics,2019,46,.27-37.

[2] Agibalov G.P. Cryptanalytic concept of finite automaton invertibility with finite delay. Applied discreet mathematics, 2019,44, 34-42.

[3] Berdnikova N.Yu., Pankratova I.A. Cryptanalytical invertibility of functions of two variables. Applied discret mathematics, Applications, 2021,14,67-71.

[4] Pankratova I.A., .Sorokoumova A.D. Cryptanalytical invertibility of functions of two variables. Applied discreet mathematics, Applications, 2024,17,44-48.

JOMUDE
http://www.jomude.com