ATLANTIS PRESS
Advances in Computer Science Research (ACRS), volume 54
International Conference on Computer Networks and Communication Technology (CNCT2016)

A New Method for Construction of Orthomorphic Permutations with the Highest Degree

Zi-dong LU[1] and Xue-jia LAI[1,*]

[1]Institute of Cryptology and Information Security, Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai, 200240, China

*Corresponding author (email: lai-xj@cs.sjtu.edu.cn)

Keywords: Information Security, Cryptography, orthomorphic permutation, Boolean function

Abstract. Orthomorphic permutation is proposed in 1942, which is a special permutation with many good cryptographic properties. Orthomorphic permutation has similar structure with a one-way function used in hash functions called Davies-Meyer construction. However, the algebraic degrees of previous constructions of orthomorphic permutations by Boolean functions are not the highest, which can be attacked by higher order differential attack. In this paper, we develop a new method for construction of orthomorphic permutations with the highest degree so that they are resistant to higher order differential analysis. We also generalize the construction from four aspects to generate more orthomorphic permutations with the highest degree. Moreover, we give the total number of orthomorphic permutations constructed after applying these generalizations. Our improvement on the degree of orthomorphic permutation can be used as a reference of designing S-box with great cryptographic properties in new algorithms.

Introduction

Orthomorphic permutation is proposed in 1942 by Mann [1]. It is a special permutation such that the bitwise exclusive OR (XOR) of an identical permutation and it is still a permutation. Orthomorphic permutation has several good cryptographic properties [2,3]. Orthomorphic permutations are perfectly balanced permutations [2]. It is also proved in [3] that if the input differential is not zero, the output differential of orthomorphic permutation is not equal to the input differential. Therefore, orthomorphic permutations can be used to design s-boxes in block ciphers [4,5], design bent functions and Boolean functions [6,7], design and analysis of hash functions [8,9], etc. The first application of orthomorphic permutations is the design of block substitutions by Mittenthal [10]. These primitives are fundamental of cryptography and information security.

As the total number of orthomorphic permutations is quite large when the number of bits is greater than 5, we can hardly generate one orthomorphic permutation by the enumerating algorithm in [11]. It is necessary to develop constructions of orthomorphic permutations for practical applications. Previous works [12,13,14,15] have developed several constructions of orthomorphic permutations. However, those constructions failed to generate orthomorphic permutations with the highest degree, although most of n-bit orthomorphic permutations have degree of n-1. After enumerating all the orthomorphic permutations of 4-bit, we find that most of them have degree of 3. Permutations with lower degree can be attacked by higher order differential analysis

[16]. Therefore, finding a construction of orthomorphic permutations with the highest degree is of cryptographic significance.

Our contribution. First, we develop a new method for constructing orthomorphic permutations with the highest degree by adding two more bits to existed ones. Then, we generalize our construction to produce more orthomorphic permutations with the highest degree. Finally, we give the total number of orthomorphic permutations constructed by this method based on the number of orthomorphic permutations of fewer bits.

Preliminaries

Definitions

This section introduces the definition of orthomorphic permutation and degree of permutations.

Definition 1 The permutation σ on F_2^n is an *orthomorphic permutation*, if and only if $\sigma \oplus I$ is also the permutation on F_2^n. I is an identical permutation on F_2^n.

Definition 2 Degree of a monomial is the sum of all the exponents of the variables in the monomial, where all the exponents are 1 on F_2^n.

Definition 3 Degree of a Boolean function is the highest degree of all the monomials in the algebraic normal form of the Boolean function, denoted as *deg(f)*, where f is a Boolean function.

Definition 4 Degree of a permutation is the highest degree of all the Boolean functions in the Boolean representation of the permutation.

Theorems

This section introduces two theorems of permutations.

Theorem 1[13] $F(x) = (f_1(x), f_2(x), \ldots, f_n(x))$ is a permutation on F_2^n if and only if any nonzero linear combination of $f_1(x), f_2(x), \ldots, f_n(x)$ is a balanced Boolean function.

Theorem 2 The highest degree of n-bit permutations is n-1.

Proof: From Theorem 1, we can conclude that $F(x) = (f_1(x), f_2(x), \ldots, f_n(x))$ is a n-bit permutation only if $f_i(x)$, where $i \in [1, n]$, are all balanced Boolean functions. Then $f_i(x)$ is the sum of even monomials in the sense of add on F_2. For each monomial, it can be represented as $x_1x_2\ldots x_n \oplus f(x_1, x_2, \ldots, x_n)$, where $x = ((x_1, x_2, \ldots, x_n)$ and f is a function with degree lower or equal to n-1. Sum of even numbers of $x_1x_2\ldots x_n$ is 0. So we can conclude that degree of $f_i(x)$ is lower or equal to n-1.

Theorem 3 The smallest number of bits of orthomorphic permutations is 2.

Previous Constructions of Orthomorphic Permutations and Their Degree

This section introduces three constructions of orthomorphic permutations and give the highest degree of them respectively. The degree of constructions in [14,15] is also lower than n-1.

Method 1[12] Let F be an orthomorphic permutation on F_2^n and G be an orthomorphic permutation on F_2^m. Then

$$(F(x_1, x_2, \ldots, x_n), G(y_1, y_2, \ldots, y_m)) \quad (1)$$

is an orthomorphic permutation on F_2^{n+m}.

The degree of this construction is max{deg(F), deg(G)}. Based on Theorem 1 and Theorem 3, max{deg(F), deg(G)} < max{n-1, m-1} < n+m-1. Therefore, the highest degree of this construction is lower than n+m-1.

Method 2[13] Let F be an orthomorphic permutation on F_2^n and G be an orthomorphic permutation on F_2^m. for any $H(y_1, y_2, \ldots, y_m): F_2^m \to F_2^n$ or $H(x_1, x_2, \ldots, x_n): F_2^n \to F_2^m$, we have

$$(F(x_1, x_2, \ldots, x_n) \oplus H(y_1, y_2, \ldots, y_m), G(y_1, y_2, \ldots, y_m)): F_2^{n+m} \to F_2^{n+m} \quad (2)$$

or

$$(F(x_1, x_2, \ldots, x_n), G(y_1, y_2, \ldots, y_m) \oplus H(x_1, x_2, \ldots, x_n)): F_2^{n+m} \to F_2^{n+m} \quad (3)$$

is an orthomorphic permutation on F_2^{n+m}.

The degree of this construction is similar as Method 1.

Method 3[12] Select a (n-2)-bit Boolean function $h_2(x_3, x_4, \ldots, x_n)$, a (n-3)-bit Boolean function $h_3(x_4, x_5, \ldots, x_n)$, …, a 1-bit Boolean function $h_{n-1}(x_n)$. Let

$$f_1(x) = f_1(x_1, x_2, \ldots, x_n) = x_n \oplus d,\ d \in F_2,$$

$$f_2(x) = f_2(x_1, x_2, \ldots, x_n) = x_1 \oplus x_2 \oplus c,\ c \in F_2,$$

$$f_3(x) = f_3(x_1, x_2, \ldots, x_n) = x_2 \oplus h_2(x_3, x_4, \ldots, x_n),$$

$$f_4(x) = f_4(x_1, x_2, \ldots, x_n) = x_3 \oplus h_3(x_4, x_5, \ldots, x_n), \quad (4)$$

…

$$f_n(x) = f_n(x_1, x_2, \ldots, x_n) = x_{n-1} \oplus h_{n-1}(x_n),$$

then $\sigma(x) = (f_1(x), f_2(x), \ldots, f_n(x))$ is an orthomorphic permutation on F_2^n.

The degree of this construction is max{deg(h_2), deg(h_3), …, deg(h_{n-1})}. The possible highest degree can be achieved by choosing h_2 with the highest degree, which is n-2. Therefore, the highest degree of this construction is lower than n-1.

The New Construction of Orthomorphic Permutations

Construction

There are a great number of orthomorphic permutations with the highest degree, but previous constructions are failed to generate them. So we try to find a new construction to generate orthomorphic permutations with the highest degree. This section introduces the new construction.

Construction 1 Let $\sigma(x_1, x_2, \ldots, x_{n-2}) = (f_1(x), f_2(x), \ldots, f_{n-2}(x))$ be an orthomorphic permutation on F_2^{n-2}, and

$$g(x_1, x_2, \ldots, x_n) = x_{n-1} \oplus x_n \oplus x_1x_2 \ldots x_{n-2}\, x_{n-1} \quad (5)$$

$$h(x_1, x_2, \ldots, x_n) = x_{n-1} \oplus x_1x_2 \ldots x_{n-2}\, x_n \quad (6)$$

Then $\delta = (f_1(x), f_2(x), \ldots, f_{n-2}(x), g(x), h(x))$ is an orthomorphic permutation on F_2^n with the degree of n-1, which is the highest degree.

Proof of Correctness

In this section, we prove the correctness of such construction.

Firstly, we prove that δ is a permutation. Because the domain of δ is F_2^n, δ is a permutation if and only if the following proposition holds.

Proposition 1 For any $\{x_1, x_2, \ldots, x_n\} \neq \{y_1, y_2, \ldots, y_n\} \in F_2^n$, $\delta(x_1, x_2, \ldots, x_n) \neq \delta(y_1, y_2, \ldots, y_n)$

We discuss the following four cases:

1) $\exists\, i \in [1, n-2]$. $x_i \neq y_i$, for σ is a permutation, then $\exists\, j \in [1,n-2]$, $f_j(x_1, x_2, \ldots, x_{n-2}) \neq f_j(y_1, y_2, \ldots, y_{n-2})$. So $\delta(x_1, x_2, \ldots, x_{n-2}) \neq \delta(y_1, y_2, \ldots, y_{n-2})$.
2) $\forall\, i \in [1, n-2]$, $x_i = y_i$, $x_{n-1} \neq y_{n-1}$, $x_n = y_n$, then $h(x_1, x_2, \ldots, x_{n-2}) \neq h(y_1, y_2, \ldots, y_{n-2})$. So $\delta(x_1, x_2, \ldots, x_{n-2}) \neq \delta(y_1, y_2, \ldots, y_{n-2})$.
3) $\forall\, i \in [1, n-2]$, $x_i = y_i$, $x_{n-1} = y_{n-1}$, $x_n \neq y_n$, then $g(x_1, x_2, \ldots, x_{n-2}) \neq g(y_1, y_2, \ldots, y_{n-2})$. So $\delta(x_1, x_2, \ldots, x_{n-2}) \neq \delta(y_1, y_2, \ldots, y_{n-2})$.
4) $\forall\, i \in [1, n-2]$, $x_i = y_i$, $x_{n-1} \neq y_{n-1}$, $x_n \neq y_n$, then we have Table 1:

Table 1. Value of g and h

x_{n-1}	x_n	y_{n-1}	y_n	g(x)	g(y)	h(x)	h(y)
0	0	1	1	0	$x_1x_2\ldots x_{n-2}$	0	$1\oplus x_1x_2\ldots x_{n-2}$
0	1	1	0	1	$1\oplus x_1x_2\ldots x_{n-2}$	$x_1x_2\ldots x_{n-2}$	1

We may easily verify either $g(x) \neq g(y)$ or $h(x) \neq h(y)$ when $x_1x_2\ldots x_{n-2} = 0$ or $x_1x_2\ldots x_{n-2} = 1$.

After discussing four cases, we have finished proving δ is a permutation. The second step is to prove $\delta \oplus I$ is a permutation. The last 2 bits of $\delta \oplus I$ is

$$g'(x_1, x_2, \ldots, x_n) = x_n \oplus x_1x_2 \ldots x_{n-2}\, x_{n-1} \quad (7)$$

$$h'(x_1, x_2, \ldots, x_n) = x_{n-1} \oplus x_n \oplus x_1x_2 \ldots x_{n-2}\, x_n \quad (8)$$

We can prove $\delta \oplus I$ in the same way. Therefore, $\delta \oplus I$ is an orthomorphic permutation.

General Form and Counting

The construction introduced in the first part is a special form, we can generalize our construction in four aspects.

1) According to Eq. 7 and Eq. 8, it is obvious that $\delta' = (f_1, f_2, \ldots, f_{n-2}, g', h')$ is also an orthomorphic permutation.
2) According to Theorem 1, $\delta_{INV} = (f_1, f_2, \ldots, f_{n-2}, g \oplus r_{n-1}, h \oplus r_n)$, where $r_{n-1} = 0$ or $r_{n-1} = 1$, $r_n = 0$ or $r_n = 1$, is also an orthomorphic permutation.

3) According to Theorem 1, $\delta_{SWAP} = (f_1, f_2, \ldots, f_{j-1}, g, f_j, \ldots, f_{k-2}, h, f_{k-1}, \ldots, f_{n-2})$, where j, k are the indices of g, h respectively, is also an orthomorphic permutation.
4) Let $mono(x_1, x_2, \ldots, x_{n-2})$ be any monomial of $\{x_1, x_2, \ldots, x_n\}$, if we substitute $x_1x_2\ldots x_n$ in Eq. 5 and Eq. 6 into $mono(x_1, x_2, \ldots, x_{n-2})$, $\delta_{MONO} = (f_1, f_2, \ldots, f_{n-2}, g, h)$ is also an orthomorphic permutation.

After generalizing our construction in these four aspects, we have the total number of orthomorphic permutations constructed is $2^{n+1} * n(n-1) * |O_{n-2}(F_2)|$, where $|O_{n-2}(F_2)|$ is the total number of n-2-bit orthomorphic permutations.

Summary

In this paper, we introduced a new method for construction of orthomorphic permutations with the highest degree. This construction resists higher order differential analysis. Furthermore, proof of correctness, general form and counting result were given. The cryptographic properties of orthomorphic permutations deserve to be further studied in future.

Acknowledgement

This work was supported by the National Natural Science Foundation of China (61272440, 61472251, U1536101), China Postdoctoral Science Foundation (2013M531174, 2014T70417), and Science and Technology on Communication Security Laboratory.

References

[1] Mann H B. The construction of orthogonal latin squares. The Annals of Mathematical Statistics, 1942, 13(4): 418-423.

[2] Mittenthal L. Nonlinear dynamic substitution devices and methods for block substitutions: U.S. Patent 5,214,704. 1993-5-25.

[3] Wu Z P, Ye D F. Composite properties of orthomorphic permutations (in Chinese) Progress in Nature Science, 2006(11):1517-1520.

[4] Feng D, Feng X, Zhang W, et al. Loiss: A byte-oriented stream cipher. Coding and Cryptology. Springer Berlin Heidelberg, 2011: 109-125.

[5] Liu X, FEND D. Construction of S-Boxes with Sorm Cryptographic Properties. Journal of Software, 2000, 11(10): 1299-1302.

[6] Dawu G, Guozhen L J X. Construction of cryptographic functions based on orthomorphic permutation. Jounal of Xidian University, 1999.

[7] Zhang F, Hu Y, Zhao Y, et al. Constructions of Two-Output Bent Functions. Journal of Computational Information Systems, 2011, 7(12): 4178-4184.

[8] Schnorr C P, Vaudenay S. Black box cryptanalysis of hash networks based on multipermutations. Advances in Cryptology—EUROCRYPT'94. Springer Berlin Heidelberg, 1994: 47-57.

[9] Vaudenay S. On the need for multipermutations: Cryptanalysis of MD4 and SAFER. Fast Software Encryption. Springer Berlin Heidelberg, 1994: 286-297.

[10] Mittenthal L. Block substitutions using orthomorphic mappings. Advances in Applied Mathematics, 1995, 16(1): 59-71.

[11] Zhou, Jianqin. A Note on the Constructions of Orthomorphic Permutations. IJ Network Security, 2010, 10.1: 57-61.

[12] Feng D G, Liu Z H. On the construction of orthomorphic permutations (in Chinese). Communication Privacy, 1996(02):61-64.

[13] Feng D G, Liu Z H. An iterated method of constructing orthomorphic permutations (in Chinese). Communication Privacy, 1998(02):53-54+59.

[14] Guo J J. Property and Construction of Orthomorphic Permutations (in Chinese). Zhengzhou: PLA Information Engineering University, 2010.

[15] Zheng H R, Zhang H M, Fan D. Correction of Construction Method of Orthomorphic Permutations and Improvement of its enumeration lower Bound (in Chinese). Journal on Communications, 2009, 30(12): 45-50.

[16] Lai X. Higher order derivatives and differential cryptanalysis, Communications and Cryptography. Springer US, 1994: 227-233.