Constructions of Almost Resilient Functions

Pin-Hui Ke[1,2,3], Tai-Lin Liu[1,4], and Qiao-Yan Wen[1]

[1] School of Science,
Beijing University of Posts and Telecommunications,
Beijing,100876, P.R. China
keph@eyou.com, tlinliu@sina.com, wqy@bupt.edu.cn
[2] State Key Laboratory of Information Security, Chinese Academy of Sciences,
Beijing 100039, P.R. China
[3] School of Mathematics and Computer Science,Fujian Normal University,
Fujian 350007, P.R. China
[4] School of Literature and Science , Shandong Finance Institute,
Shandong 250014, China

Abstract. The relation between almost resilient function and its component functions is investigated in this paper. We prove that if each nonzero linear combination of $f_1, f_2, \cdots, f_m$ is an ε-almost$(n, 1, k)$-resilient function, then $F = (f_1, f_2, \cdots, f_m)$ is a $\frac{2^m-1}{2^m-1}\varepsilon$-almost$(n, m, k)$-resilient function. In the case ε equals 0, the theorem gives another proof of Linear Combination Lemma for resilient functions. As applications of this theorem, we introduce a method to construct a balanced $\frac{9}{2}\varepsilon$–almost $(3n, 2, 2k+1)$-resilient function from a balanced ε-almost $(n, 1, k)$-resilient function and present a method of improving the degree of the constructed functions with a small trade-off in the nonlinearity and resiliency. At the end of this paper, the relation between balanced almost CI function and its component functions are also concluded.

1 Introduction

An ε-almost(n, m, k)-resilient function is an n-input m-output function f with the property that the deviation of output's distribution from uniform distribution is not great than ε when k arbitrary inputs are fixed and the remaining $n - k$ inputs run through all the 2^{n-k} input tuples. The concept of almost resilient functions was introduced by K.Kurosawa et al.[1] and is the generalization of the concept of resilient function. It was showed to have parameters superior to resilient functions. The notations of independent sample space was introduced by Naor and Naor [2], which has been proved to have many cryptographic applications, such as multiple authentication codes[3], almost security cryptographic boolean functions[4] and so on. In [1], the relations between the almost resilient functions and the large sets of almost independent sample spaces were established. So if some efficient methods to construct almost resilient functions are found, more large sets of almost independent sample spaces are also obtained. However up to the present, the only construction method is by using almost independent sample space. So we wish to investigate the relations between the

Y.G. Desmedt et al. (Eds.): CANS 2005, LNCS 3810, pp. 236–246, 2005.
© Springer-Verlag Berlin Heidelberg 2005

almost resilient functions and its component functions and look for some other construction methods.

Linear Combination Lemma , which is also called XOR-*lemma* in binary case, establishs a bridge which links the vector resilient function and its component functions and plays an important role in the characterization and construction of vector resilient functions[5]. It is also expressed in terms of independence of random variables in [6]. However, the proof method cannot be directly adapted to the almost case. So in this paper we firstly present a useful lemma , which will be used to look insight into the relation between a vector function and its component function. If F is an ε-almost(n, m, k)-resilient function , it is easy to prove that each nonzero linear combination of $f_1, f_2, \cdots, f_m$ is a $2^{m-1}\varepsilon$-almost$(n, 1, k)$-resilient function. Furthermore it is naturally for us to consider the opposite direction which has never been discussed before. We prove that if each nonzero linear combination of $f_1, f_2, \cdots, f_m$ is ε-almost$(n, 1, k)$-resilient function then F is a $\frac{2^m-1}{2^{m-1}}\varepsilon$-almost$(n, m, k)$-resilient function. The proof of the theorem depends on some technical observations. Especially in the case ε equals 0, the theorem gives another proof of Linear Combination Lemma. Then we present a method to construct a balanced $\frac{9}{2}\varepsilon$-almost$(3n, 2, 2k + 1)$-resilient function from a balanced ε-almost$(n, 1, k)$-resilient function. As pointed out in [7], one important task of construction of vector resilient functions is to construct (n, m, k)-resilient functions with degree $d > m$ and high nonlinearity. By above theorem, we will describe a method of improving the degree of the constructed functions with a small trade-off in the nonlinearity and resiliency. Almost correlation immune (for simplicity, CI) functions is the generalization of CI functions, which was introduced by K.Kurosawa[1] and the case of single output also independently introduced by Yi-Xian Yang [8]. At the end of this paper, the relation between balanced almost CI function and its component functions are also concluded.

2 Preliminaries

The vector spaces of n-tuples of elements from GF(2) is denoted by F_2^n. Let F be a function from F_2^n to F_2^m.

Definition 1. *The function F is called an (n, m, k)-resilient function if*

$$Pr[F(x_1, \cdots, x_n) = (y_1, \cdots, y_m)|x_{i_1}x_{i_2}\cdots x_{i_k} = \alpha] = 2^{-m}$$

for any k positions $i_1 < i_2 < \cdots < i_k$, for any k-bit string $\alpha \in F_2^k$, and for any $(y_1, \cdots, y_m) \in F_2^m$, where the values $x_j (j \notin \{i_1, i_2, \cdots, i_k\})$ are chosen independently at random.

Following proposition is well-known and useful in understanding the relationship between a resilient functions and its component functions. It has appeared in many references (see, for example, [5]).

Proposition 1. *Let $F = (f_1, \cdots, f_m)$ be a function from F_2^n to F_2^m, where n and m are integers with $n \geq m \geq 1$, and each f_i is a function on F_2^n. Then*