Distinguishing Attacks on a Kind of Generalized Unbalanced Feistel Network

Ruilin Li, Bing Sun, and Chao Li

Department of Mathematics and System Science, Science College,
National University of Defense Technology,
Changsha, 410073, China
securitylrl@gmail.com, happy_come@163.com
lichao_nudt@sina.com

Abstract. Recently, a new kind of Generalized Unbalanced Feistel Network, denoted as GUFN-n, is proposed by Choy *et al.* at ACISP 2009. The advantages of this structure are that it allows parallel computations for encryption and it can provide provable security against traditional differential and linear cryptanalysis given that the round function is bijective. For this new structure, the designers also found a $(2n-1)$-round impossible differential and $(3n-1)$-round integral distinguisher.

In this paper, we study distinguishing attacks on GUFN-n. We find an n^2-round integral distinguisher and show that it can be simply extended to an (n^2+n-2)-round higher-order integral distinguisher. Moreover, we point out that the n^2-round integral distinguisher corresponds to an n^2-round truncated differential with probability 1, based on which an impossible differential with up to (n^2+n-2)-round can be constructed. At last, we describe a variant structure of GUFN-n, denoted as GUFN*-n, where the round function is $F(x,K) = F(x \oplus K)$. For this variant structure, we present a new kind of n^2-round non-surjective distinguisher and use it to attack GUFN*-n with very low data complexity.

Key Words: Generalized Unbalanced Feistel Network, Integral Distinguisher, Impossible Differential, Non-surjective Distinguisher

1 Introduction

For attacking block ciphers, one mainly refers to distinguishing attacks or key recovery attacks, of which distinguishing attacks are the basis. To mount a key recovery attack, the adversary always firstly distinguish the r-round cipher from a random permutation, and then finish his key recovery attack on $(r+r')$-round algorithm.

Differential cryptanalysis (DC) and linear cryptanalysis (LC) are the two most powerful known attacks on block ciphers since 1990s. For a new block cipher algorithm, designers must guarantee that it can resist these two attacks. In [3,4], Knudsen and Nyberg firstly presented the idea of provable security against DC and LC. Based on the Feistel structure and the assumption of uniformly random

and independent round keys, the upper bound of the differential (linear hull) probability for the iterative algorithm after several rounds can be provided as a polynomial expression of $p(q)$, where $p(q)$ denotes the upper bound of differential (linear hull) probability of the round function. As long as $p(q)$ is small enough, the iterative algorithm can resistant against DC and LC. Since it is easy to design round functions with good differential (linear hull) probability, choosing which kind of structure to provide security against DC and LC becomes a hot issue [5-10].

However, even the security against DC and LC can be proved, the algorithm maybe suffers other attacks, such as truncated differential and higher-order differential attacks [11,12], impossible differential attack [13], integral attack [14], boomerang attack [15], rectangle attack [16], interpolation attack [17], algebraic attack [18], related-key attack [19], and slide attack [20] etc. For example, considering the round numbers of the well-known byte-oriented block cipher Rijndael, six rounds is sufficient for resisting DC and LC. However, by integral cryptanalysis, one can break six, seven, even eight rounds [21,22].

Generally speaking, it is necessary to provide its security against all known attacks for a new algorithm, but this is not sufficient, since we don't know whether there exists any other new distinguishers or key recovery attacks. Thus one must give more delicate cryptanalysis combined with the speciality of the algorithm.

At ACISP 2009, Choy *et.al.* proposed a new block cipher structure [23], called "KASUMI-FO" like structure. In fact, it is a new generalized unbalanced Feistel network [24] containing n sub-blocks, denoted as GUFN-n. The advantages of this structure are that it allows parallel computations for encryption and it can provide provable security against traditional differential and linear cryptanalysis given that the round function is bijective. In the same paper, a block cipher Four-Cell is designed as an application of the theoretical model of GUFN-4.

In this paper, we study distinguishing attacks on GUFN-n. We find an n^2-round integral distinguisher and show that it can be simply extended to an $(n^2 + n - 2)$-round higher-order integral distinguisher. Moreover, we point out that the n^2-round integral distinguisher corresponds to an n^2-round truncated differential with probability 1, based on which an impossible differential with up to (n^2+n-2)-round can be constructed. At last, we describe a variant structure of GUFN-n, denoted as GUFN*-n, where the round function is $F(x, K) = F(x \oplus K)$. For this structure, we present a new kind of non-surjective distinguisher and use it to attack GUFN*-n with very low data complexity.

One should note that the idea of non-surjective attack was firstly introduced by Rijmen *et.al* [26]. It is appropriate for Feistel ciphers with non-surjective round function and the principle is analyzing the statistical bias of some expression derived by the round function. However, the proposed non-surjective attack in this paper is based on a non-surjective function deduced by a bijective round function. Thus these two attacks have basic difference in essence.

This paper is organized as follows: we begin with a brief description of GUFN-n in Section 2, then presents an n^2-round integral distinguisher and an $(n^2 + n - 2)$-round impossible differential distinguisher in Section 3 and Section 4, respectively. Section 5 describes a variant structure of GUFN-n, followed by a new n^2-round non-surjective distinguisher and its corresponding key recovery attack. Section 6 applies the non-surjective attack to a toy cipher based on GUFN*-4 and the Sbox of AES. Section 7 concludes this paper.

2 Description of GUFN-n

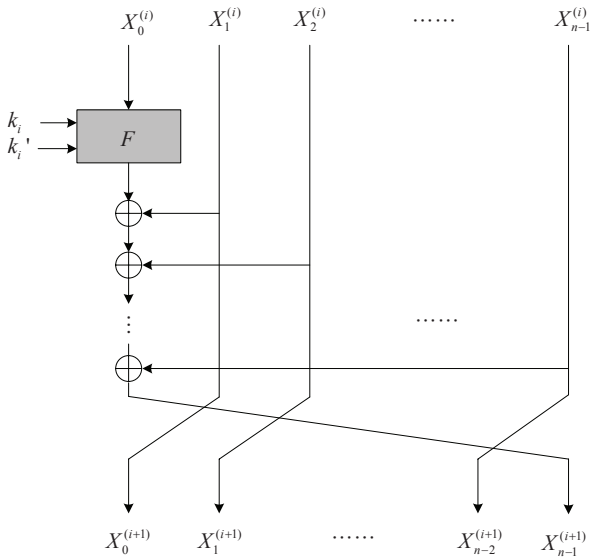

Fig. 1. The i-th Round Transformation of GUFN-n

As shown in Fig.1, assume the input, output and round key to the i-th round of GUFN-n is $(x_0^{(i)}, x_1^{(i)}, \ldots, x_{n-1}^{(i)}) \in \mathbb{F}_{2^b}^n$, $(x_0^{(i+1)}, x_1^{(i+1)}, \ldots, x_{n-1}^{(i+1)}) \in \mathbb{F}_{2^b}^n$, and $K_i = (k_i, k_i')$, then the round transformation can be described as following:

$$(X_0^{(i)}, X_1^{(i)}, \ldots, X_{n-2}^{(i)}, X_{n-1}^{(i)}) \rightarrow (X_0^{(i+1)}, X_1^{(i+1)}, \ldots, X_{n-2}^{(i+1)}, X_{n-1}^{(i+1)})$$

where

$$\begin{cases} X_l^{(i+1)} = X_{l+1}^{(i)}, \quad l = 0, 1, \ldots, n-2 \\ X_{n-1}^{(i+1)} = F(X_0^{(i)}, K_i) \oplus X_1^{(i)} \oplus X_2^{(i)} \oplus \ldots \oplus X_{n-1}^{(i)} \end{cases}$$

and $F_{K_i}(\cdot)$ is a permutation on $\mathbb{F}_{2^b}$.

In [23], the authors showed that there exist a $(2n-1)$-round impossible differential: $(0,0,0,\ldots,\alpha) \not\rightarrow (\psi,\psi,0,\ldots,0)$, where $\alpha \neq 0$, $\psi \neq 0$, and a $(3n-1)$-round integral distinguisher:$(A,C,C,\ldots,C) \rightarrow (C,?,?,\ldots,?)$, where A is active in $\mathbb{F}_{2^b}$, $C \in \mathbb{F}_{2^b}$ is constant.

3 n^2-round Integral Distinguisher of GUFN-n

In this section, the round function $F_{K_i}(x)$ is seemed as a permutation polynomial over $\mathbb{F}_{2^b}$.

Proposition 1. *Let the input of the i-th round of* GUFN-n *be $(x_0,x_1,\ldots,x_{n-1})$, the output of the $(i+n-1)$-th round be $(y_0,y_1,\ldots,y_{n-1})$. Then*

$$\begin{cases} y_0 = F_{K_i}(x_0) \oplus x_1 \oplus \ldots \oplus x_{n-1} \\ y_m = F_{K_{i+m-1}}(x_{m-1}) \oplus F_{K_{i+m}}(x_m) \oplus x_m \quad \text{if } 1 \leq m \leq n-1. \end{cases}$$

and

$$\bigoplus_{j=0}^{n-1} y_j = F_{K_{i+n-1}}(x_{n-1}).$$

Proposition 1 can be verified directly by the definition of GUFN-n. Based on this result, we can get the following proposition:

Proposition 2. *Let the input to* GUFN-n *be $(x,C_1,\ldots,C_{n-1})$, and the output of the r-round be $(y_0^{(r)}(x),y_1^{(r)}(x),\ldots,y_{n-1}^{(r)}(x))$, where $r = m \times n$ and $1 \leq m \leq n-1$, Then*

(1) $y_i^{(m\times n)}(x)$ *is a permutation polynomial over $\mathbb{F}_{2^b}$ if $i = m$;*
(2) $y_i^{(m\times n)}(x)$ *is a constant if $i > m$.*

Table 1 shows the output of every n rounds of GUFN-n, where the first column denotes the round number, C denotes some constant, and $P_m(x)$ is a permutation polynomial over $\mathbb{F}_{2^b}$, $m = 1,2,\ldots,n-1$.

Theorem 1. *There is an n^2-round integral distinguisher of* GUFN-n*:*

$$(A,C,\ldots,C) \rightarrow (S_0,S_1,\ldots,S_{n-1})$$

where A is active, C is constant and $(S_0 \oplus S_1 \oplus \ldots \oplus S_{n-1})$ is active.

Proof. Let the input of GUFN-n be $(x,c_1,\ldots,c_{n-1})$ and the output of the $(n-1)\times n$-th round be $\left(y_0^{((n-1)\times n)}(x),y_1^{((n-1)\times n)}(x),\ldots,y_{n-1}^{((n-1)\times n)}(x)\right)$, then $y_{n-1}^{((n-1)\times n)}(x)$ is a permutation polynomial by Proposition 2.

Table 1. Output of every n rounds of GUFN-n

0	x	C	C	$\dots$	C	$\dots$	C	C
n		$P_1(x)$	C	$\dots$	C	$\dots$	C	C
$\vdots$			$\ddots$		$\vdots$		$\vdots$	$\vdots$
$(m-1)\times n$				$P_{m-1}(x)$	C	$\dots$	C	C
$m\times n$					$P_m(x)$	$\dots$	C	C
$\vdots$						$\ddots$	$\vdots$	$\vdots$
$(n-2)\times n$							$P_{n-2}(x)$	C
$(n-1)\times n$								$P_{n-1}(x)$

Assume the output of the n^2-round is $\left(y_0^{(n^2)}(x), y_1^{(n^2)}(x), \dots, y_{n-1}^{(n^2)}(x)\right)$, according to Proposition 1,

$$y_0^{(n^2)}(x) \oplus y_1^{(n^2)}(x) \oplus \dots \oplus y_{n-1}^{(n^2)}(x) = F_{K_{n^2}}\left(y_{n-1}^{((n-1)\times n)}(x)\right).$$

Since $y_{n-1}^{((n-1)\times n)}(x)$ is a permutation polynomial, so is $F_{K_{n^2}}\left(y_{n-1}^{((n-1)\times n)}(x)\right)$, which ends the proof. □

Table 3 lists the 16-round integral distinguisher for GUFN-4, where C_i, $4 \le i \le 19$ is constant, y, z, w, u, v is active on $\mathbb{F}_2^b$, t_j, $1 \le j \le 5$ are some unknown intermediate values. It can be easily verified that $(t_3 \oplus t_1 \oplus y \oplus z \oplus C_{16}) \oplus (t_4 \oplus t_3 \oplus t_2 \oplus t_1 \oplus y \oplus z \oplus w \oplus C_{17}) \oplus (t_5 \oplus t_4 \oplus t_2 \oplus w \oplus u \oplus C_{18}) \oplus (t_5 \oplus u \oplus v \oplus C_{19}) = v \oplus C_{16} \oplus C_{17} \oplus C_{18} \oplus C_{19} = v \oplus C_{20}$.

From the idea of higher-order integral, the above n^2-round integral can be extended to (n^2+n-2)-round higher-order integral.

Theorem 2. *There is an (n^2+n-2)-round higher-order integral distinguisher of* GUFN-n*:*

$$(A_0, A_1, \dots, A_{n-2}, C) \to (S_0, S_1, \dots, S_{n-1})$$

where $(A_0, A_1, \dots, A_{n-2})$ is active in $\mathbb{F}_{2^b}^{n-1}$, C is constant and $(S_0 \oplus S_1 \oplus \dots \oplus S_{n-1})$ is balanced.

4 (n^2+n-2)-round Impossible Differential of GUFN-n

Theorem 3. *The n^2-round integral distinguisher corresponds to the following truncated differential with probability 1:*

$$(\delta, 0, \dots, 0) \to (\delta_0, \delta_1, \dots, \delta_{n-1})$$

where $\delta \neq 0$ and $\delta_0 \oplus \delta_2 \oplus \dots \oplus \delta_{n-1} \neq 0$.

Proof. Let the input of the GUFN-n be $(x, c_1, c_2, \ldots, c_{n-1})$, after n^2 rounds, the output is $(q_0(x), q_1(x), \ldots, q_{n-1}(x))$, then according to Proposition 2, $q_0(x) \oplus q_1(x) \oplus \ldots \oplus q_{n-1}(x) \triangleq q(x) \in \mathbb{F}_{2^b}[x]$ is a permutation polynomial.

Assume two inputs are $(x_1, c_1, c_2, \ldots, c_{n-1})$ and $(x_2, c_1, c_2, \ldots, c_{n-1})$ with $x_1 \neq x_2$, thus $q(x_1) \neq q(x_2)$. Now the input difference is $(\delta, 0, \ldots, 0)$ with $\delta = x_1 \oplus x_2 \neq 0$, and the output difference is $(\delta_0, \delta_1, \ldots, \delta_{n-1})$, satisfying $\delta_0 \oplus \delta_1 \oplus \ldots \oplus \delta_{n-1} = q(x_1) \oplus q(x_2) \neq 0$. □

Theorem 4. *There exists an* (n^2+n-2)*-round impossible differential in* GUFN-n *of the following form:*

$$(\delta, 0, \ldots, 0) \nrightarrow_{n^2+n-2} (\psi, \psi, 0, \ldots, 0)$$

where $\delta \neq 0$ *and* $\psi \neq 0$.

Proof. From the encrypt direction, the n^2-round differential

$$(\delta, 0, \ldots, 0) \rightarrow (\delta_0, \delta_1, \ldots, \delta_{n-1})$$

is with probability 1, where $\delta \neq 0$ and $\delta_0 \oplus \delta_2 \oplus \ldots \oplus \delta_{n-1} \neq 0$.

From the decrypt direction, the $(n-2)$-round differential

$$(0, \ldots, 0, \psi, \psi) \leftarrow (\psi, \psi, 0, \ldots, 0)$$

is with probability 1.

Since $\psi \oplus \psi = 0$, as shown in Fig 2, we find a contradiction. □

$$
\begin{array}{l}
(\delta,\ 0,\ \cdots,\ 0,\ 0) \\
\qquad \downarrow n^2 \\
(\delta_0, \delta_1, \cdots, \delta_{n-2}, \delta_{n-1}) \\
\\
\qquad \Updownarrow \quad \delta_0 \oplus \delta_1 \oplus \cdots \oplus \delta_{n-2} \oplus \delta_{n-1} \neq 0 \ \ \textit{contradiction}! \\
\\
(0, \cdots, 0,\ \psi,\ \psi) \\
\qquad \uparrow n-2 \\
(\psi,\ \psi,\ 0, \cdots,\ 0)
\end{array}
$$

Fig. 2. Impossible Differential Found By Meet-in-the-middle Technique

From the proof of Theorem 4, one can easily deduce the following r-round impossible differential

$$(\delta, 0, \ldots, 0) \nrightarrow_r (\psi, \psi, 0, \ldots, 0),$$

where $n^2 + 1 \leq r \leq n^2 + n - 2$.

5 n^2-round Non-surjective Distinguisher of GUFN*-n

In this section, we describe a variant structure of GUFN-n, denoted as GUFN*-n. As shown in Fig 3, the main difference is the round function $F(x, K)$. In GUFN*-n, we always assume that $F_K(x) = F(x \oplus K)$. One can demonstrate that, for GUFN*-n, the provable security against differential and linear cryptanalysis can also be provided.

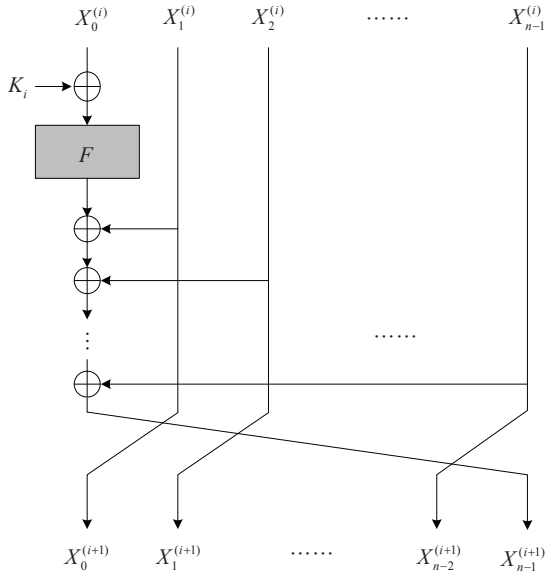

Fig. 3. The i-th Round Transformation of GUFN*-n

If the input of GUFN*-n is $(x, c_1, \ldots, c_n)$, then $y_{n-1}^{((n-2)\times n)}$ is a constant, say C. According to Proposition 1:

$$\bigoplus_{j=0}^{n-1} y_j^{(n^2-n)} = F_{K_{n^2-n}}(C) \triangleq C'.$$

Thus $y_0^{(n^2-n)} = C' \oplus \bigoplus_{j=1}^{n-1} y_j^{(n^2-n)}$.

Assume the output of n^2-round is $(q_0(x), q_1(x), \ldots, q_{n-1}(x))$, from Proposition 1, we have

$$q_0(x) = F\left(y_0^{(n^2-n)} \oplus K_{n^2-n+1}\right) \oplus \bigoplus_{j=1}^{n-1} y_j^{(n^2-n)},$$

Let $t = y_0^{(n^2-n)} \oplus K_{n^2-n+1}$, then

$$\begin{aligned} q_0(x) &= F(t) \oplus t \oplus K_{n^2+n-1} \oplus C' \\ &= F(t) \oplus t \oplus C^*, \end{aligned}$$

where $C^* = K_{n^2+n-1} \oplus C'$ represents some unknown constant.

Let $f(t) = F(t) \oplus t$, define $\mathcal{D}_f = \{y | y = f(t),\, t \in \mathbb{F}_{2^b}\}$, considering the above fact, we have the following n^2-round distinguisher:

Theorem 5. *Let the input to* GUFN-n *be* $(x, c_1, \ldots, c_{n-1})$*, where* c_i *is constant, and the output of the* n^2*-th round be* $(q_0(x), q_1(x), \ldots, q_{n-1}(x))$*. Then there exists some constant* $C^* \in \mathbb{F}_{2^b}$*, such that for any* $x \in \mathbb{F}_{2^b}$*,* $q_0(x) \oplus C^* \in \mathcal{D}_f$*.*

Considering the distinguisher in Theorem 5, in this situation, the input to the (n^2+1)-th round function F is $q'(x) = q_0(x) \oplus K_{n^2+1}$, let $c^* = C^* \oplus K_{n^2+1}$, then $q'(x) \oplus c^* = q_0(x) \oplus C^*$. In other words, for all $x \in \mathbb{F}_{2^b}$, there exists some constant c^*, s.t., $q'(x) \oplus c^* \in \mathcal{D}_f$. Thus we could get the following theorem.

Theorem 6. *Let the input to* GUFN-n *be* $(x, c_1, \ldots, c_{n-1})$*, where* c_i *is constant, and the input of the* (n^2+1)*-th round function* F *be* $q'(x)$*. Then there exists some constant* $c^* \in \mathbb{F}_{2^b}$*, such that for any* $x \in \mathbb{F}_{2^b}$*,* $q'(x) \oplus c^* \in \mathcal{D}_f$*.*

One should note that if $\mathcal{D}_f = \mathbb{F}_{2^b}$, $f(x)$ is an *orthormorphic permutation*. Since the number of all orthormorphic permutations is small, in general, for a randomly chosen permutation $F(x)$, $f(x) = F(x) \oplus x$ can be seen as a random function(as the D-M construction in hash function), thus $\mathcal{D}_f \subsetneq \mathbb{F}_{2^b}$. From now on, we will call the above distinguisher the *non-surjective distinguisher*, since the domain of f generated by a permutation F is only a subset of $\mathbb{F}_{2^b}$.

By using the above non-surjective distinguisher, one can attack $(n^2 + n')$-round GUFN*-n by Algorithm 1, where $n' > 1$.

Algorithm 1: Non-surjective Attack on GUFN*-n

Step 1	Compute and store $\mathcal{D}_f$.
Step 2	Given t plaintexts $(x_i, c_1, \ldots, c_{n-1})$, obtain the corresponding $(n^2 + n')$-round ciphertexts, $i = 1, \ldots, t$.
Step 3	Guess the last $(n' - 1)$ round-keys $rk = (rk_1, rk_2, \ldots, rk_{n'-1})$, decrypt the ciphertext to get the input of the $(n^2 + 1)$-round function F, denoted by $q'_{rk}(x_i)$.
Step 4	For all x_i in Step 2, test whether there exists some constant c^* satisfying $q'_{rk}(x_i) \oplus c^* \in \mathcal{D}_f$. If not, the guessed round-keys rk must be wrong.
Step 5	If necessary, repeat Step 2 $\sim$ Step 5 to further filter the wrong round keys until only one left.

In order to estimate the complexity of the above attack, we need the following two lemmas.

Lemma 1. *Given $A \subseteq \mathbb{F}_{2^b}$, $|A|$ denotes the number of different elements in A. For a random chosen set $X \subseteq \mathbb{F}_{2^b}(|X| \leq |A|)$, let p be the probability that there exists $c \in \mathbb{F}_{2^b}$, such that $X \oplus c = \{x \oplus c | x \in X\} \subseteq A$, then*

$$p < 2^b \times \frac{|A|}{2^b} \times \frac{|A|-1}{2^b-1} \times \ldots \times \frac{|A|-(|X|-1)}{2^b-(|X|-1)}.$$

Lemma 2. *Let $f(x)$ be a random function from $\mathbb{F}_q$ to $\mathbb{F}_q$, $\mathcal{D}_f = \{f(x)|x \in \mathbb{F}_q\}$, $\epsilon = E(|\mathcal{D}_f|)$ and $\sigma^2 = V(|\mathcal{D}_f|)$ be the expectation and variance of $|\mathcal{D}_f|$, respectively. Then*

(1) $\lim\limits_{q\to\infty} \dfrac{\epsilon}{q} = 1 - \dfrac{1}{e} \approx 0.632$

(2) $\lim\limits_{q\to\infty} \dfrac{\sigma^2}{q} = \dfrac{e-2}{e^2} \approx 0.097$

If $|X| \ll |A|$, from Lemma 1, the upper bound of p can be approximated by $2^b \times \left(|A|/2^b\right)^{|X|}$. This implies that, for a random chosen $X \subseteq \mathbb{F}_{2^b}$, the probability that there exists $c \in \mathbb{F}_{2^b}$, s.t. $X \oplus c \subseteq A$ is very low.

When q is large, from Lemma 2, the *Chebyshev Inequality* [27] indicates

$$P(|\ |\mathcal{D}_f\ | - \epsilon| \leq l\sigma) \geq 1 - \frac{1}{l^2}.$$

Choose $q = 2^b$ and $l = 10$, then for a randomly chosen f,

$$P\left(0.63 \times 2^b - 3 \times 2^{b/2} \leq |\mathcal{D}_f| \leq 0.63 \times 2^b + 3 \times 2^{b/2}\right) \geq 0.99.$$

So we can estimate with high probability that $|\mathcal{D}_f|$ is less than $0.63 \times 2^b + 3 \times 2^{b/2}$. Moreover, when b is large, $|\mathcal{D}_f|$ can be approximated by 0.63×2^b.

Now we can analysis the attack complexity as follow:

First we note that when applying integral attack on GUFN*-n, one must choose at least a structure of all possible $(x, c_1, c_2, \ldots, c_{n-1})$, where c_is are constants. While for the non-surjective attack, only a fraction of them are needed.

Assume the number of chosen plaintexts as $(x, c_1, c_2, \ldots, c_{n-1})$ is t, let $\mathcal{T}$ denote the set of their corresponding ciphertexts, $\mathcal{T}_{rk}$ denote the set of the input to the (n^2+1)-round F function from decrypting the ciphertexts in $\mathcal{T}$ by guessing the last $n'-1$ round keys rk.

The crucial step in Algorithm 1 is to check whether there exists a constant $c^* \in \mathbb{F}_{2^b}$ such that $\mathcal{T}_{rk} \oplus c^* \subseteq \mathcal{D}_f$. Assume wrong key values can pass such test with probability P_{err}, then from Lemma 1,

$$P_{err} \leq (2^{(n'-1)b} - 1) \times 2^b \times \binom{|\mathcal{D}_F|}{t} / \binom{2^b}{t} \triangleq P_t,$$

thus in order to identify the right keys for the last $n'-1$ rounds, P_{err} must be small enough. If b is large, and $t << |\mathcal{D}_F|$,

$$P_t \approx 2^{n'b} \times \left(|\mathcal{D}_F|/2^b\right)^t \approx 2^{n'b} \times 0.63^t.$$

Let $P_t \leq 2^{-\lambda}$, then $P_{err} \leq P_t \leq 2^{-\lambda}$, which indicates that the probability that the wrong key can pass the test in Step 4 is less than $2^{-\lambda}$. From $2^{n'b} \times 0.63^t \leq 2^{-\lambda}$, we get $t \geq \frac{3}{2}n'b + \frac{3}{2}\lambda$, where the parameter λ is related to the successful probability, and can be deduced by experiments.

Thus for attacking $(n^2 + n')$-round GUFN*-n, the data complexity is about $\frac{3}{2}n'b + \frac{3}{2}\lambda$. Since one must store $\mathcal{D}_f$, the space complexity is about 0.63×2^b. As explained before, Step 4 of Algorithm 1 needs to verify whether there exists a constant $c^* \in \mathbb{F}_{2^b}$, s.t. $\mathcal{T}_{rk} \oplus c^* \subseteq \mathcal{D}_f$ for each possible r_k. Assume for each possible c^*, the time complexity for testing whether $\mathcal{T}_{rk} \oplus c^* \subseteq \mathcal{D}_f$ is equivalent to u encryptions, then the time complexity is about $\left(\frac{3}{2}n'b + \frac{3}{2}\lambda\right) \times (2^{(n'-1)b}) \times 0.63 \times 2^b \times u \approx (n'b + \lambda) \times 2^{n'b} \times u$, thus a good algorithm for testing whether one set is included in another is required.

6 Non-surjective Attack on GUFN*-4

In this section, we design a 32-bit toy cipher based on GUFN*-4, where the round function F is defined by $F(x, k) = S(x \oplus k)$ with S as the Sbox of AES. In this case, $b = 8$ and $|\mathcal{D}_f| = 163 \approx 0.63 \times 2^8$. We use the method in Section 5 to mount a non-surjective attack on the 18-round toy cipher.

Table 2 lists our experimental results. For each $\lambda = 2, 4, 6, 8, 10$, t denotes the number of chosen plaintexts. We do 200 times attacks each and the successful probability is $0.455, 0.705, 0.865, 0.925, 0.995$, where the "successful" means the adversary can uniquely recover the right 18-th round key.

Table 2. Results of Non-surjective Attack on GUFN*-4 with AES Sbox

paramater λ	chosen plaintext $t = 3b + 1.5\lambda$	successful probability
2	27	0.455
4	30	0.705
6	33	0.865
8	36	0.925
10	39	0.995

7 Conclusion

This paper studies distinguishing attacks on a new kind of generalized unbalanced Feistel network GUFN-n. We find that there exists an n^2-round integral distinguisher, which can be easily extended to an (n^2+n-2)-round higher-order integral distinguisher. Based on the n^2-round integral distinguisher, an impossible differential with up to $n^2 + n - 2$ rounds can be constructed. These results implies that the security of GUFN-n must be carefully re-evaluated.

Moreover, if the round function of GUFN-n is defined as $F(x, K) = F(x \oplus K)$, we can present a new non-surjective distinguisher by which a key recovery attack can be mounted. Some experimental results are given for the non-surjective attack on a toy cipher based on GUFN*-4 and Sbox of AES. Since our non-surjective attack is different in essence with the one proposed by Rijmen *et.al.* It is an interesting problem that whether this new non-surjective attack can be extended to other block ciphers.

References

1. E.Biham and A. Shamir. Differential Cryptanalysis of DES-like Cryptosystems. Journal of Cryptology, Vol 3, pp. 3-72, Springer-Verlag, 1991.
2. M.Matsui. Linear cryptanalysis method for DES cipher. In EUROCRYPT 1993, LNCS 765, pp. 386–397, Springer-Verlag, 1993.
3. K. Nyberg and L.R. Knudsen. Provable Security Against Differential Cryptanalysis. In Crypto 1992, LNCS 740, pp. 566-574, Springer-Verlag, 1992.
4. K. Nyberg. Linear Approximation of Block Ciphers. In Eurocrypt 1994, LNCS 950, pp. 439-444, Springer-Verlag, 1994.
5. K. Nyberg. Generalized Feistel Networks. In Asiacrypt 1996, LNCS 1163, pp. 91-104, Springer-Verlag, 1996.
6. M. Matsui. New structure of block ciphers with provable security against differential and linear cryptanalysis. In FSE 1996, LNCS 1039, pp. 205-218, Springer-Veralg, 1996.
7. J. Sung, S. Lee, J. Lim, S. Hong, and S. Park. Provable Security for the skipjack-like structure against differential cryptanalysis and linear cryptanalysis. In Asiacrypt 2000, LNCS 1976, pp. 274-288, Springer-Verlag, 2000.
8. S. Hong, S. Lee, J. Lim, J. Sung, D. Chen, and I. Cho. Provable Security against Differential and Linear Cryptanalysis for the SPN Structure. In FSE 2000, LNCS 1978, pp. 273-283, Springer-Verlag, 2001.
9. C. Lee, J. Kim, J. Sung, S. Hong, and S. Lee. Provable Security for an RC6-like structure and a MISTY-FO-like Structure against Differential Cryptanalysis. In ICCSA 2006, LNCS 3982, pp. 446-455, Springer-Verlag, 2006.
10. J. Kim, C. LEE, J. SUNG, S. HONG, S. LEE, and J. LIM. Seven New Block Cipher Structures with Provable Security against Differential Cryptanalysis. In IEICE TRANS. FUNDAMENTALS, VOL. E91-A, NO. 10 October 2008, 3047-3058.
11. L. Knudsen. Truncated and high order differentials. In FSE 1995, LNCS 1008, pp. 196–211, Springer-Verlag 1995.
12. X. Lai. High order derivatives and differential cryptanalysis. Communications and Cryptography. 1994, 227-233
13. E. Biham , A. Biryukov, A. Shamir. Cryptanalysis of Skipjack reduced to 31 rounds using impossible differentials. In EUROCRYPT 1999, LNCS 1592, pp. 12–23, Springer-Verlag, 1999.
14. L. Knudsen. D. Wagner. Integral Cryptanalysis. In FSE 2002, LNCS 2365, pp. 112–127, Springer-Verlag, 2002.
15. D. Wanger. The Boomerang Attack. In FSE 1999, LNCS 1636, pp.156-170, Springer-Verlag, 1999.
16. E. Biham, O. Dunkelman, and N. Keller. The Rectangle Attack- Rectangling the Serpent. In EUROCRYPT 2001, LNCS 2045, pp. 340-357, Springer-Verlag, 2001

17. T. Jackobsen, L. Knudsen. The interpolation attack on block cipher. In FSE 1997, LNCS 1008, pp. 28–40, Springer-Verlag, 1997.
18. N. Courtois and J. Pieprzyk. Cryptanalysis of Block Ciphers with overdefined systems of equations. In ASIACRYPT 2002, LNCS 2501, pp. 267-287, Springer-Verlag, 2002.
19. E. Biham. New Types of Cryptanalytic Attacks Using Related Keys. In EUROCRYPT 1993, LNCS 765, pp. 398-409, Springer-Verlag, 1994.
20. A. Biryukov and D. Wagner. Slide Attack. In FSE 1999, LNCS 1636, pp. 245-259, Springer-Verlag, 1999.
21. J. Daemen , L. Knudsen, V. Rijmen. The block cipher Square. In FSE 1997, LNCS 1267, pp. 149–165, Springer-Verlag, 1997.
22. N. Ferguson, J. Kelsey, S. Lucks, B. Schneier, M. Stay, D. Wagner, and D. Whiting. Improved cryptanalysis of Rijndael. In FSE 2000, LNCS 1978, pp. 213–230, Springer-Verlag, 2001.
23. J. Choy G. Chew, K. Khoo and H. Yap. Cryptographic Properties and Application of a Generalized Unbalanced Feistel Network Structure. In ACISP 2009, LNCS 5594, pp. 73-89, Springer-Verlag, 2009.
24. B. Schneier, J. Kelsey. Unbalanced Feistel Networks and Block Cipher Design. In FSE 1996, LNCS 1039, pp.121-144, Springer-Verlag, 1996.
25. J. Kim, S. Hong, J. Sung, S. Lee, J. Lim, and S. Sung. Impossible Differential Cryptanalysis for Block Cipher Structures. Indocrypt 2003, LNCS 2904, pp. 82-96, Springer-Verlag 2003.
26. V. Rijmen, B. Preneel and E. De Win. On Weaknesses of Non-surjective Round Functions. In Designs, Codes, and Cryptography, VOL 12, pp. 253-266, Springer-Verlag, 1997.
27. W. Feller. An Introduction to Probability Theory and Its Applications, 3rd Edition. Wiley, New York, 1968.

Table 3. The 16-round Integral Distinguisher of GNFN-4

0	x	C_1	C_2	C_3
1	C_1	C_2	C_3	$y \oplus C_4$
2	C_2	C_3	$y \oplus C_4$	$y \oplus C_5$
3	C_3	$y \oplus C_4$	$y \oplus C_5$	C_6
4	$y \oplus C_4$	$y \oplus C_5$	C_6	C_7
5	$y \oplus C_5$	C_6	C_7	$y \oplus z \oplus C_8$
6	C_6	C_7	$y \oplus z \oplus C_8$	$y \oplus z \oplus w \oplus C_9$
7	C_7	$y \oplus z \oplus C_8$	$y \oplus z \oplus w \oplus C_9$	$w \oplus C_{10}$
8	$y \oplus z \oplus C_8$	$y \oplus z \oplus w \oplus C_9$	$w \oplus C_{10}$	C_{11}
9	$y \oplus z \oplus w \oplus C_9$	$w \oplus C_{10}$	C_{11}	$t_1 \oplus y \oplus z \oplus C_{12}$
10	$w \oplus C_{10}$	C_{11}	$t_1 \oplus y \oplus z \oplus C_{12}$	$t_2 \oplus t_1 \oplus y \oplus z \oplus w \oplus C_{13}$
11	C_{11}	$t_1 \oplus y \oplus z \oplus C_{12}$	$t_2 \oplus t_1 \oplus y \oplus z \oplus w \oplus C_{13}$	$t_2 \oplus w \oplus u \oplus C_{14}$
12	$t_1 \oplus y \oplus z \oplus C_{12}$	$t_2 \oplus t_1 \oplus y \oplus z \oplus w \oplus C_{13}$	$t_2 \oplus w \oplus u \oplus C_{14}$	$u \oplus C_{15}$
13	$t_2 \oplus t_1 \oplus y \oplus z \oplus w \oplus C_{13}$	$t_2 \oplus w \oplus u \oplus C_{14}$	$u \oplus C_{15}$	$t_3 \oplus t_1 \oplus y \oplus z \oplus C_{16}$
14	$t_2 \oplus w \oplus u \oplus C_{14}$	$u \oplus C_{15}$	$t_3 \oplus t_1 \oplus y \oplus z \oplus C_{16}$	$t_4 \oplus t_3 \oplus t_2 \oplus t_1 \oplus y \oplus z \oplus w \oplus C_{17}$
15	$u \oplus C_{15}$	$t_3 \oplus t_1 \oplus y \oplus z \oplus C_{16}$	$t_4 \oplus t_3 \oplus t_2 \oplus t_1 \oplus y \oplus z \oplus w \oplus C_{17}$	$t_5 \oplus t_4 \oplus t_2 \oplus w \oplus u \oplus C_{18}$
16	$t_3 \oplus t_1 \oplus y \oplus z \oplus C_{16}$	$t_4 \oplus t_3 \oplus t_2 \oplus t_1 \oplus y \oplus z \oplus w \oplus C_{17}$	$t_5 \oplus t_4 \oplus t_2 \oplus w \oplus u \oplus C_{18}$	$t_5 \oplus u \oplus v \oplus C_{19}$