通信情報保護學會論文誌
第 8 卷 第 1 號, 1998. 3

The Linearity of algebraic Inversion and a Modification of Knudsen-Nyberg Cipher

ChangHyi,Lee*, JongIn,Lim**

Abstract

K. Nyberg and L.R. Knudsen showed a prototype of a DES-like cipher[1] which has a provable security against differential cryptanalysis. But in the last year, at FSE' 97 T. Jakobsen and L.R. Knudsen broke it by using higher order differential attack and interpolation attack[2]. Furthermore the cipher was just a theoretically proposed one to demonstrate how to construct a cipher which is provably secure against differential cryptanalysis[3] and it was suspected to have a large complexity for its implementation. In this paper the two improved results for the efficient hardware and software implementation and its security are presented. For the improvement, we proved that x^{-1} over GF(2^n), for any integer n, has its linearity (in the sense of linear cryptanalysis[6]) is bounded by $\frac{[1+2^{n/2+1}]_e}{2^n}$, where $[n]_e$ means the greatest even integer less than n. G. Lachaud and J. Wolfmann also showed a similar result in[9], but in this paper we achieve our result in a different approach, from the well known result on elliptic curve theory. Finally in section 4, we introduce a modified prototype cipher of Knudsen-Nyberg Cipher. **keywords** : differential cryptanalysis, linear cryptanalysis, DES-like cipher, basis of finite field

1. Introduction

In 1993, K. Nyberg and L.R. Knudsen suggested a prototype of a DES-like cipher which is 6-round iterated (we call this cipher *K.N* and it was published in the journal of cryptology(1995). In the journal[1] they showed that if the round function f in a DES-like cipher is a permutation which has maximal differential probability p_{max} and the round keys(k_i) are independent and uniformly random then the differential probability of an s-round differential for $s \geq 3$ is less than or equal to $2p^2_{max}$. And they showed that the permutations$f(x)=x^{2^k+1}$ of $\mathbf{GF}(2^d)^n$ with $k=0 \ mod \ d$, $gcd(k, n)=1$, and $n=odd$ have their differential

* *SAIT Digital Communication Lab.*
* *Korea University*

probability $2^{d(1-n)}$, in particular x^3 in **GF**(2^{33}) has its differential probability 2^{-30}.

Using these two results they showed that the cipher *K.N* is provably secure against a differential cryptanalysis. In fact, its *s*-round(s ≥ 3) iterated cipher has its differential probability 2^{-60}. But because of the simple type of algebraic function x^3, it was broken by higher order differential attack and interpolation attack[2] with only 512 chosen plaintexts. Moreover its software implementation complexity is suspected to be very high. *K.N*' s round function f is as the following :

$$GF(2^{32}) \xrightarrow{e} GF(2^{33}) \xrightarrow{x^3} GF(2^{33}) \xrightarrow{d} GF(2^{32}),$$

where e is a function which extends its argument by concatenation with an affine combination of the input bits, and d is a function which discards one bit from its argument. This is a provably secure cipher against conventional differential cryptanalysis, but it has two problems. The first is that it has very high complexity to construct or design the round function $f(x)=x^3$ in **GF**(2^{33}) and the second is that the non-linear order of the output is low with respective to the input and this can be exploited to amount an attack. In the following we overcome the two problems and get an implementation of a slightly modefied cipher from *K.N*.

2. Linearity of x^{-1}

In this section we prove that the linearity of x^{-1} in **GF**(2^n) is bounded by $2^{-\binom{n-1}{2}}$ for any integer n. For the proof we prepare some well known results(following 3 propositions).

Proposition 2.1 *The following quadratic polynomial equation of one variable X,*

$$X^2+aX+b=0,\ a\neq 0,\ b\in \mathbf{GF}(2^n)$$

is irreducible over **GF**(2^n) *if and only if* $\mathbf{Tr}\left(\frac{b}{a^2}\right)\neq 0$, where **Tr**( ) is an absolute trace mapping[4].

Proof. Dividing the above equation by a^2 and letting $T=\frac{x}{a^2}$ gives a new quadratic equation $T^2+T=\frac{x}{a^2}$. And noting that $L(x)=x^2+x$, $x\in \mathbf{GF}(2^n)$ is a linear transformation of which kernel consists of **GF**(2), we get the result.

Proposition 2.2 *Every basis* $B=\{\phi_1,\phi_2,\ldots,\phi_n\}$ *of* ***GF***(2^n) *over* ***GF***(2) *has its unique dual basis*[4] $B'=\{\psi_1, \psi_2, \ldots, \psi_n\}$ *such that*

$$Tr(\phi_i\, \psi_j)=\begin{cases}1 & \text{if } i=j\\ 0 & \text{if } i\neq j\end{cases}$$

The following definition and proposition can be refered to[5].

Definition 2.1 *The set* E *of points* $(x,y)\in \mathbf{GF}(2^n)\times \mathbf{GF}(2^n)$ *satisfying the following equation* $y^2+b_2xy+b_1y=a_3x^3+a_2x^2+a_1x+a_0, a_i, b_i\in \mathbf{GF}(2^n)$ *and the identity(null) element O is called elliptic curve over* **GF**(2^n) *and is denoted by* **E**(**GF**(2^n)). *And the number of elements of* **E** *is called the order of* **E**(**GF**(2^n)) and is denoted by #**E**(**GF**(2^n)).(see [5])

Proposition 2.3 (*Hasse*)
Let #**E**(**GF**(2^n))=$q+1-t$. *Then* $|t|\leq 2\sqrt{q}$

Definition 2.2[6]
The linearity $L(f)$ *of* $\mathbf{f}: \mathbf{GF}(2^n)\rightarrow \mathbf{GF}(2^n)$ *is defined by*

$$L(f)=\max_{\lambda,\omega}\frac{|\#\{x:\omega\cdot f(x)=\lambda\cdot x\}-2^{n-1}|}{2^{n-1}}$$

where **x**, **f(x)**, λ, *and* ω *are considered as binary represented vectors in* **GF**(2^n) *by some basis*

$B=\{\phi_1,\phi_2,\ldots,\phi_n\}$

and the notation '·'means the inner product operation.

Now we are ready to prove the following theorem.

Theorem 2.1 *The linearity of the permutation* x^{-1} *in* **GF**(2^n) *is bounded by*

$$\frac{[1+2^{n/2+1}]_e}{2^n}$$

where $[n]_e$ *means the greatest even integer less than* n.

Proof. Let $\mathbf{E}(\mathbf{GF}(2^n)): y^2+xy+\lambda x^3+\omega^2=0$ and let $S_{\lambda\omega}=\#\{x:\omega\cdot x^{-1}\}\lambda\cdot x$. If we regard the vectors x, x^{-1} as the binary represented elements in **GF**(2^n) with basis B and regard the vectors λ, ω as the binary vectors in **GF**(2^n) with the dual basis B', of B, then easily we get

$$\lambda\cdot x=\mathbf{Tr}(\lambda x) \text{ and } \omega\cdot x^{-1}=\mathbf{Tr}(\omega x^{-1}).$$

And so, by proposition 2.2, $S_{\lambda\omega}=\#\{x:\mathbf{Tr}(\lambda x+\omega x^{-1})=0\}$. Meanwhile, by proposition 2.1,

$$\begin{aligned}\#E &= 2\times\#\{x\mid \mathbf{Tr}\left(\tfrac{\lambda x^3+\omega^2}{x^2}\right)=0,\ x\neq 0\}+\#\{(0,w),0\}\\ &=2\times\#\{\mathbf{Tr}(\lambda x)+\mathbf{Tr}(\omega^2x^{-2})=0,\ x\neq 0\}+2\\ &=2\times\#\{\mathbf{Tr}(\lambda x)+\mathbf{Tr}(\omega x^{-1})=0,\ x\neq 0\}+2\\ &=2(S_{\lambda w}-1)+2=2S_{\lambda w}.\end{aligned}$$

Note, by proposition 2.3 and from the above result, that

$$2^n+1-2\sqrt{2^n}\le\#\mathbf{E}(\mathbf{GF}(2^n))=2S_{\lambda w}\le 2^n+1+2\sqrt{2^n} \quad (2.1)$$

and noting that the central value of eq.(2.1) is even integer, we got $|S_{\lambda w}-2^{n-1}|\le\dfrac{[1+2^{n/2+1}]_e}{2^n}$

Hence,

$$L(x^{-1})=max_{\lambda,w}\frac{|\#\{x:\omega x^{-1}+\lambda x\}-2^{n-1}|}{2^{n-1}}$$

$$=max_{\lambda,w}\frac{|S_{\lambda w}-2^{n-1}|}{2^{n-1}}$$

$$\le max_{\lambda,w}\frac{|1+2^{n/2+1}|}{2^n}$$

This completes the proof.

Since, in the case of n=*even*, in the equation(2.1) $2S_{\lambda\omega}$ is even and $2^n+1+2\sqrt{2^n}$ is odd integer, we get $2^n+2-2\sqrt{2^n}\le 2S_{\lambda\omega}\le 2^n+2\sqrt{2^n}$ and so $|S_{\lambda\omega}-2^{n-1}|\le 2^{n/2}$. From this $L(x^{-1})=2^{(-n/2-1)}$. For example, for the case of n=32, the permutation x^{-1} in **GF**(2^{32}) has its linearity 2^{-15} and so its squared linearity[8] is 2^{-30}. Moreover, from[1], we know that x^{-1} has its differential uniformity 4. Hence we got a permutation which is resistant against differential cryptanalysis and linear cryptanalysis. In the following section, using this permutation, we propose an efficient implementation of *K.N.*

3. IMPLEMENTATION

To begin with, for the implementation of x^{-1} in **GF**(2^{32})=**GF**(2^{25}) we will use a recursive method. Let $\psi_0=1\in\mathbf{GF}(2)$, $\psi_1^2+\psi_0\ \psi_1+1=0$, $\psi_1\in\mathbf{GF}(2^{21})$,

$$\psi_{n+1}^2+\psi_n\psi_{n+1}+1=0,\ \psi_{n+1}\in\mathbf{GF}(2^{n+1}),\ n=0,1,2,3,4.$$

Then each $\psi_{n+1}\mathbf{GF}(2^{2^{n+1}})$ is irreducible element over $\mathbf{GF}(2^{2^n})$[5, PP. 54]. Now we can take $\{1,\ \psi_{n+1}\}$ as a basis of $\mathbf{GF}(2^{2^{n+1}})$ over $\mathbf{GF}(2^{2^n})$ for each n=0, 1, 2, 3, 4 and so for $\alpha\in\mathbf{GF}(2^{2^{n+2}})$ can be represented by

$$\alpha=a_1+a_2\psi_{n+1},\ a_1,\ a_2\in\mathbf{GF}(2^{2^n})$$

$=(a_1, a_2)$ taking its coordinates in $GF(2^{2^n})$,

and again, by this way, a_i can be represented of form (b_1, b_2), $b_i \in GF(2^{2^{n-1}})$. We can do this process recusively down to the prime field $GF(2)$. and get a binary representation of α of n coordinates in $GF(2)$ For example, if we consider $\alpha=(1, 1, 0, 1)$ in $GF(2^4)$ then

$$\alpha=((1, 1), (0, 1))=(1, 1)+(0, 1)\psi_2=(1+\psi_1)+(0+\psi_1)\psi_2$$

Theorem 3.1 *Let* $\alpha=a_1+a_2\psi_{n+1}, a_1, a_2 \in GF(2^{2^n})$. *Then*

$$\alpha^{-1}=\delta^{-1}(a_1+a_2\psi_n+a_2\psi_{n+1})=(\delta^{-1}(a_1+a_2\psi_n), \delta^{-1}a_2),$$
where $\delta=a^2_2+a_1(a_1+a_2\psi_n)$.

Proof. Let $\alpha^{-1}=(x, y)=x+y\psi_{n+1}, x, y \in GF(2^{2^n})$. Then, using the formula $\psi^2_{n+1}=1+\psi_n\psi_{n+1}$ and noting that the expansion of the product $\alpha\alpha^{-1}=(a_1, a_2)(x, y)$ must equal to $(1, 0)=1$, we get a linear system of equations of x, y. Solving this linear system of equations, we easily get the result.

Note, from the above theorem, that inversion of an element in $GF(2^{2^{n+1}})$ can be calculated by one inversion in $GF(2^{2^n})$, one squaring in $GF(2^{2^n})$, two additions in $GF(2^{2^n})$, one multiplication of an element in $GF(2^{2^n})$ and $\psi_n \in GF(2^{2^n})$, and three products in $GF(2^{2^n})$. Let' s examine these operations in the same way.

[Multiplication in $GF(2^{2^{n+1}})$]

$$(a_1+a_2\psi_{n+1},)(b_1+b_2\psi_{n+1},)=t_1+t_1+(t_1+t_2+t_3+t_2\psi_n)\psi_{n+1},$$

where $t_1=a_1b_1$, $t_2=a_2b_2$, $t_3=(a_1+a_2)+(b_1+b_2)$

This operation needs 6 additions, 3 multiplications in $GF(2^{2^n})$, and 1 multiplication of an element in $GF(2^{2^n})$ and ψ_n

[Squaring in $GF(2^{2^{n+1}})$]

$$(a_1+a_2\psi_{n+1})^2=(a_1+a_2)^2+a^2_2\psi_n\psi_{n+1}$$

This operation needs 1 addition 2 squaring in $GF(2^{2^n})$, and 1 multiplication of an element in $GF(2^{2^n})$ and ψ_n.

[Multiplication of $\alpha=(a_1,a_2)$ and $\psi_{n+1,}$]

$$(a_1+a_2\psi_{n+1})\psi_{n+1}=a_2+(a_1+a_2)\psi_n\psi_{n+1,}$$

This operation needs 1 addition in $GF(2^{2^{n+1}})$, 1 multiplication of an element in $GF(2^{2^n})$ and ψ_n.

From the above results, we can calculate the total number of bit by bit operations in $GF(2)$ to get the inversion of an element in $GF(2^{2^n})$ by the way of iterating n=5 down to 0 as in the above. Some tedious calculation gives us that one inversion in $GF(2^{32})$ can be designed by about 1800 exclusive OR gates and 360 logic AND gates.

4. Network Structure and Performance

Here we slightly modify the cipher ***K.N***[1] to escape the interpolation attack[2]. We construct the round function, x^{-1} in $GF(2^{32})$, by using the quadratic recursived binary representation of 32-bit input text as in section 3.

Let $f=x^{-1}$ and let $P=(P_1, P_2, P_3, P_4) \in GF(2^{32})$, P_i:8-bit binary vectors, be a 32-bit text. Define a linear permutation T of $GF(2^{32})$ as $T(P)=(P_3, P_1, P_4, P_2)$. Then it' s very difficult to find any algebraic polynomial to represent T which is in

accord with the recursive representation in section3. We construct the cipher' s one round Feistel network structure as the following:

- XL, XR : 32-bit left and right half input texts
- $XL=XR, XR=XL\oplus T((XR\oplus K_i)^{-1})$

where k_i is a 32-bit round key. And iterating this by 6 rounds. Then, since the linearity and differential probability of T o x^{-1} preserves the linearity and differential probability of x^{-1}[6], the modified round function has its squared linearity and its differential probability 2^{-30} and by the result of [1] its 3 round iteration gives the cipher the total differential probability and the total linearity 2^{-60}. Moreover the composition of T and x^{-1} makes the structure more resistant against higher order and interpolation attacks, since, for the interpolation attack, we should get some algebraic polynomials or fractional representations for each round function, but T is a linear transformation and under the suggested basis representation it is hard to represent it as a polynomial type equation.

For the hardware implementation, to design the function x^{-1} in $\mathbf{GF}(2^{32})$ comes to be very efficient since, at least, the number of logic gates is lower than the one needed in the cipher, MISTY[7], and it uses a simple recursive structure.

For the software implementation, on the 120MHz pentium PC, it encrypts 3.5Mbytes/sec with precomputed tables of 1Kbytes.

5. Conclusion

We showed, in this paper, some linearity bound of x^{-1} and we suggested a method to implement x^{-1} in $\mathbf{GF}(2^{32})$ by using recursively generated irreducible elements through the quadratic extensions of the prime(base) field $\mathbf{GF}(2)$. In particular we have the very important result that x^{-1} in $\mathbf{GF}(2^n)$ is very robustic against both differential and linear cryptanalysis. And using this result we made a slightly modified prototype cipher from Knudsen and Nyberg' s which is still provably secure against DC and LC attacks. And moreover its 6-round encryption has some high speed performance, about 3.5 Mbytes/sec with memory cost, 1Kbytes, for software implementation on 120MHz pentium PC and is suspected to be very efficient also for hardware implementation.

REFERENCES

[1] K. Nyberg and L.R. Knudsen. *Provable Security Against a Differential Attack.* The Journal of Cryptology, 8(1): pp.27-38, 1995.

[2] T. Jakobsen and L.R Knudsen. *The Interpolation Attack on Block Ciphers.* Advances in cryptology - Fast Software Encryption'96, Lecture Notes in Computer Science, Springer - Verlag pp.28-40, 1996.

[3] E. Biham and A. Shamir. *Differential Cryptanalysis of the Data Encryption* Standard. Springer-Verlag, 1993.

[4] R. Lidl, H. Niederreiter, Finite Fields. Encyclopedia of Math. and its Application, #20.

[5] A. Menezes, *Elliptic Curve Public Key Cryptosystems*. Kluwer Academic Publishers, 1993.

[6] K. Nyberg. *S-Boxes and Round Functions with Controllable Linearity and Differential Uniformity*. Advances in Cryptology - Fast Software Encryption' 94, Lecture Notes in Computer Science 1008, Springer - Verlag pp.111-130, 1994.

[7] M. Matsui. *New Block Encryption Algorithm MISTY*. Advances in Cryptology - Fast Software Encryption' 96, Lecture Notes in Computer Science , Springer-Verlag, pp.53-67, 1996.

[8] M. Matsui. *Linear Cryptanalysis Method for DES cipher*, Advances in Cryptology - EUROCRYPT' 93, Lecture Notes in Computer Science 765, Springer-Verlag, 1994, pp.386-397.

[9] Gilles Lachaud and Jacques Wolfmann. *The weights of the orthogonals of the extended quadratic binary Goppa codes*, IEEE Transactions on Information Theory, vol.36, no.3, May 1990, pp.686-692.

□ 著者紹介

이 창 희

1989년 2월 고려대학교 수학과 학사
1991년 2월 고려대학교 대학원 수학과 석사
1996년 8월 고려대학교 대학원 수학과 이학박사
1996년 8월 ~현재 삼성종합기술원, MTS(Member of Technical Staff)

※ 주관심분야 : 대수기하학, 응용대수학, 암호이론

임 종 인

1980년 2월 고려대학교 수학과 학사
1982년 2월 고려대학교 대학원 수학과 석사
1986년 2월 고려대학교 대학원 수학과 이학박사
1996년 8월 ~현재 고려대학교 수학과 교수

※ 주관심분야 : 응용 대수학 및 정수론, 암호론