Differentially uniform mappings for cryptography

KAISA NYBERG*

Institute of Computer Technology, Vienna Technical University

Abstract. This work is motivated by the observation that in DES-like ciphers it is possible to choose the round functions in such a way that every non-trivial one-round characteristic has small probability. This gives rise to the following definition. A mapping is called differentially uniform if for every non-zero input difference and any output difference the number of possible inputs has a uniform upper bound. The examples of differentially uniform mappings provided in this paper have also other desirable cryptographic properties: large distance from affine functions, high nonlinear order and efficient computability.

1. Introduction

The most successful and widely used block cipher has been the DES algorithm which was designed in the seventies. By the time, however, it has become too small, the key size being only 56 bits, and all attempts to increase the security by extending the DES by parallel or serial implementetations have failed.

In recent years the DES has been extensively analyzed in order to capture its properties of strength. Special attention has been focused on the nonlinearity properties of the round function, which is composed of permutations and eight small parallel substitution transformations, the S-boxes. It seems that the security can be increased only by increasing the size of the S-boxes or possibly by replacing the set of small parallel substitutions by one large transformation with desirable properties.

The necessary criteria for a substitution transformation or a round function of DES-like cipher include the following.

(i) High nonlinearity, large distance from linear functions;
(ii) High nonlinear order, the degrees of the outputbit functions are large;
(iii) Resistance against the differential cryptanalysis; and
(iv) Efficient construction and computability.

To satisfy requirement (iii) it is enough that for every fixed nonzero input difference to the function no output difference occurs with high probability. In other words, it is required that there is a uniform upperbound to the probability of the possible output differences. If this holds no strong characteristics for the success of the differential cryptanalysis exist as was proven in [7].

The purpose of this paper is to give examples of transformations of $GF(2^n)$ with properties (i) - (iv). Moreover, all these transformations are extendable in the sense that if parametrized by the length of the input, the complexity of the construction and implementation is polynomial but the security is exponential with key of linear length.

*Current address: Prinz Eugen-Straße 18/6, A-1040 Vienna, Austria
The work of the author on this project is supported by the MATINE Board, Finland

T. Helleseth (Ed.): Advances in Cryptology - EUROCRYPT '93, LNCS 765, pp. 55-64, 1994.

2. The resistance of DES-like ciphers against differential attacks

Let $(G,+)$ be a finite Abelian group, G' a subgroup of G, $F_i : G \to G'$ mappings, and $E_i : G' \to G$ such that $E_i - E_i(0)$ is an injective group homomorphism, $i = 1,2,\ldots,r$. We define an r-round DES-like cipher over G as follows.

Given a plaintext $\mathbf{x} = (\mathbf{x}_L, \mathbf{x}_R) \in G' \times G'$ *and a key* $\mathbf{k} = (\mathbf{k}_1, \mathbf{k}_2, \ldots, \mathbf{k}_r) \in G^r$ *the ciphertext* $\mathbf{y} = (\mathbf{y}_L, \mathbf{y}_R)$ *is computed in* r *iterative rounds:*

Set $\mathbf{x}_L(0) = \mathbf{x}_L$ *and* $\mathbf{x}_R(0) = \mathbf{x}_R$ *and*
compute for $i = 1,2,\ldots,r$

$$\begin{aligned} \mathbf{x}(i) &= (\mathbf{x}_L(i), \mathbf{x}_R(i)), \quad \textit{where} \\ \mathbf{x}_L(i) &= \mathbf{x}_R(i-1) \quad \textit{and} \\ \mathbf{x}_R(i) &= F_i(E_i(\mathbf{x}_R(i-1)) + \mathbf{k}_i) + \mathbf{x}_L(i-1). \end{aligned}$$

Set $\mathbf{y}_L = \mathbf{x}_R(r)$ *and* $\mathbf{y}_R = \mathbf{x}_L(r)$.

An s-round *characteristic* $\chi = \chi(\boldsymbol{\alpha}(0),\ldots,\boldsymbol{\alpha}(s))$ of a DES-like cipher is a sequence of *differences* $\boldsymbol{\alpha}(i) = (\boldsymbol{\alpha}_L(i), \boldsymbol{\alpha}_R(i)) \in G' \times G'$, $i = 0,1,\ldots,s$, such that $\boldsymbol{\alpha}_L(i) = \boldsymbol{\alpha}_R(i-1)$, $i = 1,2,\ldots,s$.

Given $\mathbf{x}$, $\mathbf{x}^* \in G' \times G'$ and $\mathbf{k} = (\mathbf{k}_1,\ldots,\mathbf{k}_R) \in G^r$, $r \geq s$, we say that χ holds for $\mathbf{x}$ and $\mathbf{k}$ if $\mathbf{x}^* - \mathbf{x} = \boldsymbol{\alpha}(0)$ and

$$\mathbf{x}^*(i) - \mathbf{x}(i) = \boldsymbol{\alpha}(i),$$

for all $i = 1,2,\ldots,s$, or what is the same,

$$\begin{aligned} (1) \qquad & F_i(E_i(\mathbf{x}_R(i-1) + \boldsymbol{\alpha}_R(i-1)) + \mathbf{k}_i) - \\ & F_i(E_i(\mathbf{x}_R(i-1)) + \mathbf{k}_i) + \boldsymbol{\alpha}_L(i-1) = \boldsymbol{\alpha}_R(i) \end{aligned}$$

for all $i = 1,2,\ldots,s$.

In what follows we find it convenient to consider a characteristic χ as a Boolean function of $\mathbf{x}$ and $\mathbf{k} = (\mathbf{k}_1,\ldots,\mathbf{k}_s)$ defined as follows

$$\chi(\mathbf{x},\mathbf{k}) = \prod_{i=1}^{s} \chi_i(\mathbf{x},\mathbf{k}_i)$$

where for $i = 1,2,\ldots,s$ we set

$$\chi_i(\mathbf{x},\mathbf{k}_i) = 1$$

if and only if (1) holds.

The differential cryptanalysis of iterated ciphers [1] [4] makes use of s-round characteristics to carry forward the information of a fixed input difference from the first round to the s^{th} round *independently of the used key.* Given a plaintext pair $(\mathbf{x},\mathbf{x}^*)$, *chosen by the cryptanalyst*, and the round keys $\mathbf{k}_1,\ldots,\mathbf{k}_s$, *unknown*

to the cryptanalyst, a characteristic may or may not hold. The probability of the cryptanalyst's success, i.e., that a characteristic $\chi = \chi(\boldsymbol{\alpha}(0), \ldots, \boldsymbol{\alpha}(s))$ holds for a chosen plaintext pair $(\mathbf{x}, \mathbf{x}^*)$, $\mathbf{x} + \boldsymbol{\alpha}(0)$, is $P_K(\chi(\mathbf{x}, K) = 1)$, where the key $K = (K_1, \ldots, K_s) \in G^s$ is considered as a random variable. If the round keys $K_1, \ldots, K_s$ are independent then

$$P_K(\chi(\mathbf{x}, K) = 1) = \prod_{i=1}^{s} P_{K_i}(\chi_i(\mathbf{x}, K_i) = 1)$$

i.e., the probability of a characteristic is the product of the probabilities of its rounds.

To compute the one-round probabilities we assume that K_i is uniformly random. Let us denote

$$\boldsymbol{\alpha}'_R(i-1) = E_i(\boldsymbol{\alpha}_R(i-1)) - E_i(0).$$

Then

$$\begin{aligned} P_{K_i}(\chi(\mathbf{x}, K_i) = 1) =& P_{K_i}\{F_i(E_i(\mathbf{x}_R(i-1) + \boldsymbol{\alpha}_R(i-1)) + K_i) \\ & - F_i(E_i(\mathbf{x}_R(i-1)) + K_i) + \boldsymbol{\alpha}_L(i-1) = \boldsymbol{\alpha}_R(i)\} \\ =& P_{K_i}\{F_i(E_i(\mathbf{x}_R(i-1)) + K_i + \boldsymbol{\alpha}'_R(i-1)) \\ & - F_i(E_i(\mathbf{x}_R(i-1)) + K_i) + \boldsymbol{\alpha}_L(i-1) = \boldsymbol{\alpha}_R(i)\} \\ =& P_Z\{F_i(Z + \boldsymbol{\alpha}'_R(i-1)) - F_i(Z) + \boldsymbol{\alpha}_L(i-1) = \boldsymbol{\alpha}_R(i)\}, \end{aligned}$$

where $Z \in G$ is uniformly random. This shows, in particular, that the one-round probabilities are independent of $\mathbf{x}$. In the terminology of [4] this means that a DES-like cipher over an Abelian group is a Markov cipher with respect to the canonical difference.

Given $\mathbf{a}$, $\mathbf{b} \in G'$ let us denote

$$p_{F_i}(\mathbf{a}, \mathbf{b}) = P_Z\{F_i(Z + \mathbf{a}) - F_i(Z) = \mathbf{b}\}$$

where $Z \in G$ is uniformly random. Then

$$P_{K_i}(\chi(\mathbf{x}, K_i) = 1) = p_{F_i}(\boldsymbol{\alpha}'_R(i-1), \boldsymbol{\alpha}_R(i) - \boldsymbol{\alpha}_L(i-1)).$$

To prove resistance against differential cryptanalysis it suffices to show that for any given (or chosen) input pair $(\mathbf{x}, \mathbf{x}^*)$ the probability of guessing correctly the difference $\mathbf{x}^*(s) - \mathbf{x}(s)$, without any knowledge of the used key, is too small to be useful.

Given $\mathbf{x}$, $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ the probability of getting $\mathbf{x}^*(s) - \mathbf{x}(s) = \boldsymbol{\beta}$ from $(\mathbf{x}^*, \mathbf{x})$ with $\mathbf{x}^* = \mathbf{x} + \boldsymbol{\alpha}$ is the sum of the probabilities of the different characteristics $\chi(\boldsymbol{\alpha}(0), \ldots, \boldsymbol{\alpha}(s))$ with $\boldsymbol{\alpha}(0) = \boldsymbol{\alpha}$, $\boldsymbol{\alpha}(s) = \boldsymbol{\beta}$, that is

$$\sum_{\substack{\boldsymbol{\alpha}(0) = \boldsymbol{\alpha} \\ \boldsymbol{\alpha}(s) = \boldsymbol{\beta}}} P_K\{\chi(\boldsymbol{\alpha}(0), \boldsymbol{\alpha}(1), \ldots, \boldsymbol{\alpha}(s-1), \boldsymbol{\alpha}(s))(\mathbf{x}, K) = 1\}.$$

Theorem 1 of [7] can be generalized to hold for a DES-like cipher over any Abelian group with different round functions. We have the following result.

THEOREM. *Let the round keys of a DES-like cipher be independent and uniformly random. Then for all* $\boldsymbol{\alpha}, \boldsymbol{\beta} \in G' \times G'$, $\boldsymbol{\beta} \neq 0$ *and for all* $\mathbf{x} \in G' \times G'$

$$\sum_{\substack{\boldsymbol{\alpha}(0) = \boldsymbol{\alpha} \\ \boldsymbol{\alpha}(s) = \boldsymbol{\beta}}} P_K(\chi(\boldsymbol{\alpha}(0), \ldots, \boldsymbol{\alpha}(s))(\mathbf{x}, K) = 1) \leq 2(\max_{i, \mathbf{a}, \mathbf{b}, \mathbf{a} \neq 0} p_{F_i}(\mathbf{a}, \mathbf{b}))^2.$$

if $s \geq 4$. *If* $G' = G$ *and* F_i *is a permutation for all* $i = 1, 2, \ldots, r$, *then the estimate holds for* $s \geq 3$.

This motivates the following definition.

DEFINITION. *Let* G_1 *and* G_2 *be finite Abelian groups. A mapping* $F : G_1 \to G_2$ *is called differentially* δ*-uniform if for all* $\boldsymbol{\alpha} \in G_1$, $\boldsymbol{\alpha} \neq \mathbf{0}$, *and* $\boldsymbol{\beta} \in G_2$

$$|\{\mathbf{z} \in G_1 \mid F(\mathbf{z} + \boldsymbol{\alpha}) - F(\mathbf{z}) = \boldsymbol{\beta}\}| \leq \delta.$$

Now the result of the theorem can be stated as follows:

If the round functions of a DES-like cipher over G *are differentially* δ*-uniform and the round keys are independent and uniformly random then for every given input pair* $(\mathbf{x} + \boldsymbol{\alpha}, \mathbf{x})$, $\boldsymbol{\alpha} \neq 0$, *the average probability over the keys to obtain an output difference* $\boldsymbol{\beta} \neq 0$ *at the* s^{th} *round,* $s \geq 4$, *is less than or equal to* $2(\delta/|G|)^2$.

Examples of differentially 2-uniform mappings are the almost perfect nonlinear permutations of $GF(2^n)$ as defined in [7]. If $m - n$ output coordinates of a permutation of $GF(2^m)$ with property (P) (see [7]) are omitted the resulting mapping from $GF(2^m)$ to $GF(2^n)$ is differentially 2^{m-n+1}-uniform.

The purpose of this paper is to give other examples. The following two facts are useful.

PROPOSITION 1. *Let* $A : G_1 \to G_1$ *and* $B : G_2 \to G_2$ *be group isomorphisms and* $F : G_1 \to G_2$ *be differentially* δ*-uniform. Then* $B \circ F \circ A$ *is differentially* δ*-uniform.*

PROPOSITION 2. *Let* $F : G_1 \to G_2$ *be a differentially* δ*-uniform bijection. Then the inverse mapping of* F *is differentially* δ*-uniform.*

3. Power polynomials $F(\mathbf{x}) = \mathbf{x}^{2^k+1}$ in $GF(2^n)$ and their inverses

We shall first prove the following general results about the nonlinearity properties of power polynomial mappings.

PROPOSITION 3. *Let $F(\mathbf{x}) = \mathbf{x}^{2^k+1}$ be a power polynomial in $GF(2^n)$ and let $s = \gcd(k, n)$. Then F is differentially 2^s-uniform. If $\frac{n}{s}$ is odd, that is, F is a permutation, then the Hamming distance of the Boolean function $f_{\boldsymbol{\omega}}(\mathbf{x}) = tr(\boldsymbol{\omega}F(\mathbf{x}))$ from the set of linear Boolean functions is equal to $2^{n-1} - 2^{\frac{n+s}{2}-1}$, for all $\boldsymbol{\omega} \in GF(2^n), \boldsymbol{\omega} \neq \mathbf{0}$.*

PROOF: Given $\boldsymbol{\alpha}$, $\boldsymbol{\beta} \in GF(2^n)$, $\boldsymbol{\alpha} \neq \mathbf{0}$, the equation

$$(\mathbf{x}+\boldsymbol{\alpha})^{2^k+1} + \mathbf{x}^{2^k+1} = \boldsymbol{\beta} \tag{2}$$

has either zero or at least two solutions. Let $\mathbf{x}_1$ and $\mathbf{x}_2$ be two different solutions. Then

$$(\mathbf{x}_1 + \mathbf{x}_2)^{2^k}\boldsymbol{\alpha} + (\mathbf{x}_1 + \mathbf{x}_2)\boldsymbol{\alpha}^{2^k} = \mathbf{0}$$

or equivalently,

$$(\mathbf{x}_1 + \mathbf{x}_2)^{2^k-1} = \boldsymbol{\alpha}^{2^k-1}$$

from which it follows that

$$\mathbf{x}_1 + \mathbf{x}_2 \in \boldsymbol{\alpha}(G \setminus \{\mathbf{0}\})$$

where G is the subfield of $GF(2^n)$ of order 2^s. Hence given one solution $\mathbf{x}_0$ of (2) the set of all solutions is $\mathbf{x}_0 + \boldsymbol{\alpha}G$ of cardinality 2^s.

To prove the second part we make use of the technique of squared character sums. Let $\boldsymbol{\omega} \in GF(2^n), \boldsymbol{\omega} \neq \mathbf{0}$ and denote the Walsh transform of $f_{\boldsymbol{\omega}}$ by $\widehat{F}_{\boldsymbol{\omega}}$. It suffices to show that

$$\max_{\mathbf{t} \in GF(2^n)} |\widehat{F}_{\boldsymbol{\omega}}(\mathbf{t})| = 2^{\frac{n+s}{2}}.$$

Let $\mathbf{t} \in GF(2^n)$. Then

$$\begin{aligned}(\widehat{F}_{\boldsymbol{\omega}}(\mathbf{t}))^2 &= \sum_{\mathbf{x} \in GF(2^n)} (-1)^{f_{\boldsymbol{\omega}}(\mathbf{x})+\mathbf{t}\cdot\mathbf{x}} \sum_{\mathbf{y} \in GF(2^n)} (-1)^{f_{\boldsymbol{\omega}}(\mathbf{x}+\mathbf{y})+\mathbf{t}\cdot(\mathbf{x}+\mathbf{y})} \\ &= \sum_{\mathbf{y} \in GF(2^n)} (-1)^{\mathbf{t}\cdot\mathbf{y}} \sum_{\mathbf{x} \in GF(2^n)} (-1)^{f_{\boldsymbol{\omega}}(\mathbf{x}+\mathbf{y})+f_{\boldsymbol{\omega}}(\mathbf{x})}.\end{aligned}$$

Let $\mathbf{y} \neq \mathbf{0}$ and denote by $E_{\mathbf{y}}$ the range of the linear mapping

$$\mathbf{x} \mapsto F(\mathbf{x}+\mathbf{y}) + F(\mathbf{x}) + F(\mathbf{y}) = \mathbf{x}^{2^k}\mathbf{y} + \mathbf{y}^{2^k}\mathbf{x}.$$

Similarily as in the first part of the proof we see that the kernel of this linear mapping is $\mathbf{y}G$. Thus the dimension of the linear space $E_{\mathbf{y}}$ is $n - s$. For each $\mathbf{y} \neq \mathbf{0}$ either

$$tr(\boldsymbol{\omega}\boldsymbol{\beta}) = 0 \text{ for all } \boldsymbol{\beta} \in E_{\mathbf{y}}, \text{ or } \sum_{\boldsymbol{\beta} \in E_{\mathbf{y}}} (-1)^{\mathrm{tr}(\boldsymbol{\omega}\boldsymbol{\beta})} = 0.$$

The vectors $\mathbf{y}$ for which $\mathrm{tr}(\omega\beta) = 0$ for all $\beta \in E_{\mathbf{y}}$ or equivalently,

$$f_\omega(\mathbf{x}+\mathbf{y}) + f_\omega(\mathbf{x}) + f_\omega(\mathbf{y}) = \mathrm{tr}(\omega(\mathbf{x}^{2^k}\mathbf{y} + \mathbf{x}\mathbf{y}^{2^k})) = 0$$

for all $\mathbf{x} \in GF(2^n)$, form a linear subspace Y of $GF(2^n)$. So we have

$$\begin{aligned}(\widehat{F_\omega}(\mathbf{t}))^2 &= 2^n + \sum_{\mathbf{y}\neq\mathbf{0}} (-1)^{\mathbf{t}\cdot\mathbf{y}+f_\omega(\mathbf{y})} 2^s \sum_{\beta\in E_{\mathbf{y}}} (-1)^{\mathrm{tr}(\omega\beta)} \\ &= 2^n + 2^n \sum_{\mathbf{y}\in Y\setminus\{\mathbf{0}\}} (-1)^{\mathbf{t}\cdot\mathbf{y}+f_\omega(\mathbf{y})}\end{aligned}$$

By definition of Y the function f_ω is linear on Y. Hence it remains to show that Y has 2^s elements.

Let $\mathbf{y} \in Y$. Then

$$\mathrm{tr}(\omega\mathbf{y}\mathbf{x}^{2^k}) = \mathrm{tr}(\omega\mathbf{y}^{2^k}\mathbf{x}) = \mathrm{tr}(\omega^{2^k}\mathbf{y}^{2^{2k}}\mathbf{x}^{2^k})$$

for all $\mathbf{x} \in GF(2^n)$, which is equivalent to

$$\omega\mathbf{y} = \omega^{2^k}\mathbf{y}^{2^{2k}}$$

or, if $\mathbf{y} \neq \mathbf{0}$,

$$(\omega F(\mathbf{y}))^{2^k-1} = \mathbf{1},$$

from which we get exactly $2^s - 1$ nonzero solutions $\mathbf{y}$, since F is assumed to be a permutation. This completes the proof.

If n is odd, $1 < k < n$ and $\gcd(n,k) = 1$, then the power polynomial $F(\mathbf{x}) = \mathbf{x}^{2^k+1}$ in $GF(2^n)$ is a differentially 2-uniform permutation. The public key cryptosystem C^* [5] is based on power polynomial permutations with $n = (2\ell+1)2^r$ and $k = b2^r$, $1 \leq b \leq \ell$. By Proposition 3 the coordinate functions of these polynomials are the more linear the larger r is. Finally notice that for $n = 2^m$ the polynomial $F(\mathbf{x}) = \mathbf{x}^{2^k+1}$ in $GF(2^n)$ is never a permutation.

The *degree* of a Boolean function f is the polynomial degree of the algebraic normal form of f and is denoted by $\deg(f)$. Let us denote by $\mathrm{w}_2(k)$ the 2-weight of a non-negative integer k. One proof of the following well-known result can be found in [2].

PROPOSITION 4. *Let $\omega \in GF(2^n)$, $\omega \neq \mathbf{0}$ and let $\mathbf{x} \mapsto \mathbf{x}^e$ be a permutation of $GF(2^n)$. Then*

$$\deg(\mathrm{tr}(\omega\mathbf{x}^e)) = w_2(e).$$

The permutations $\mathbf{x} \mapsto \mathbf{x}^{2^k+1}$ in $GF(2^n)$, n odd, satisfy properties (i), (iii) and (iv) but their output coordinate functions are only quadratic. Their inverses, however, have degrees linearly growing with n.

PROPOSITION 5. *Let n be odd, $gcd(n,k) = 1$ and $F(\mathbf{x}) = \mathbf{x}^{2^k+1}$. Then $F^{-1}(\mathbf{x}) = \mathbf{x}^{\ell}$, where*

$$\ell = \frac{2^{k(n+1)}-1}{2^{2k}-1} = \sum_{i=0}^{\frac{n-1}{2}} 2^{2ik} \mod (2^n-1)$$

with

$$w_2(\ell) = \frac{n+1}{2}.$$

PROOF:

$$\begin{aligned}
\ell(2^k+1) &= \sum_{i=0}^{\frac{n-1}{2}} 2^{(2i+1)k} + \sum_{i=0}^{\frac{n-1}{2}} 2^{2ik} \mod (2^n-1) \\
&= \sum_{i=0}^{n} 2^{ik} \mod (2^n-1) \\
&= \sum_{i=0}^{n} 2^{i} \mod (2^n-1) \\
&= 2^{n+1}-1 \mod (2^n-1) = 1 \mod (2^n-1),
\end{aligned}$$

where the third equality follows from the fact that the mapping $i \mapsto ki$ permutes the integers modulo n if $\gcd(n,k) = 1$.

As a conclusion we list the following properties of the inverse of $F(\mathbf{x}) = \mathbf{x}^{2^k+1}$ in $GF(2^n)$ with n odd and $\gcd(n,k) = 1$.

(i) $\mathcal{N}(F^{-1}) = \min_{\omega \neq 0} \min_{L \text{ lin.}} \min_{\mathbf{x} \in GF(2^n)} d(\mathrm{tr}(\omega F^{-1}(\mathbf{x})), L(\mathbf{x})) = 2^{n-1} - 2^{\frac{n-1}{2}}$;

(ii) $\deg(\mathrm{tr}(\omega F^{-1}(\mathbf{x}))) = \mathrm{w}_2((2^k+1)^{-1} \mod (2^n-1)) = \frac{n+1}{2}$;

(iii) F^{-1} is differentially 2-uniform;

(iv) Using the fast exponentiation algorithm the computation of $F^{-1}(\mathbf{x})$ is of polynomial time requiring $\frac{n-1}{2}$ squarings and $\frac{n-1}{2}$ multiplications in $GF(2^n)$.

The first property follows from Theorem 1 of [6] which says that $\mathcal{N}(F^{-1}) = \mathcal{N}(F)$ and from Proposition 3.

4. The mapping $F(\mathbf{x}) = \mathbf{x}^{-1}$ in a finite field

Let $(\mathsf{F}, \cdot, +)$ be a finite field. Then the inversion mapping $F : \mathsf{F} \to \mathsf{F}$

$$F(\mathbf{x}) = \begin{cases} \mathbf{x}^{-1}, & \text{if } \mathbf{x} \neq \mathbf{0} \\ \mathbf{0}, & \text{if } \mathbf{x} = \mathbf{0} \end{cases}$$

is well defined.

PROPOSITION 6. *The inversion mapping is differentially 4-uniform in* $(\mathbf{F}, +)$.

PROOF: Let $\boldsymbol{\alpha}$, $\boldsymbol{\beta} \in \mathbf{F}$ and $\boldsymbol{\alpha} \neq \mathbf{0}$ and consider the equation

$$(\mathbf{x} + \boldsymbol{\alpha})^{-1} - \mathbf{x}^{-1} = \boldsymbol{\beta}. \tag{3}$$

Assume that $\mathbf{x} \neq \mathbf{0}$ and $\mathbf{x} \neq -\boldsymbol{\alpha}$. Then (3) is equivalent to

$$\boldsymbol{\beta}\mathbf{x}^2 + \boldsymbol{\alpha}\boldsymbol{\beta}\mathbf{x} - \boldsymbol{\alpha} = \mathbf{0}, \tag{4}$$

which has at most two solutions in $\mathbf{F}$. If either $\mathbf{x} = \mathbf{0}$ or $\mathbf{x} = -\boldsymbol{\alpha}$ is solution to (3), then both of them are solutions and $\boldsymbol{\beta} = \boldsymbol{\alpha}^{-1}$. In that case (4) is equivalent to

$$\mathbf{x}^2 + \boldsymbol{\alpha}\mathbf{x} - \boldsymbol{\alpha}^2 = 0, \tag{5}$$

which may give two more solutions to (3).

Let us solve (5) in the special case $\mathbf{F} = GF(2^n)$. By squaring (5) and substituting $\mathbf{x}^2 = \boldsymbol{\alpha}\mathbf{x} + \boldsymbol{\alpha}^2$ we obtain

$$\mathbf{x}(\mathbf{x}^3 + \boldsymbol{\alpha}^3) = \mathbf{0},$$

which has no other solutions than $\mathbf{x} = \mathbf{0}$ or $\boldsymbol{\alpha}$ if $\gcd(3, 2^n - 1) = 1$, or equivalently, if n is odd. If n is even then 3 divides $2^n - 1$. Let $d = \frac{1}{3}(2^n - 1)$. Then there are two more solutions, $\mathbf{x} = \boldsymbol{\alpha}^{1+d}$ and $\mathbf{x} = \boldsymbol{\alpha}^{1+2d}$.

We list the following properties of the inversion mapping in $GF(2^n)$.

(i) $\mathcal{N}(F) = \min_{\boldsymbol{\omega} \neq \mathbf{0}} \min_{L \text{ lin.}} \min_{\mathbf{x} \in GF(2^n)} d(\mathrm{tr}(\boldsymbol{\omega}\mathbf{x}^{-1}), L(\mathbf{x})) \geq 2^{n-1} - 2^{\frac{n}{2}}$;

(ii) $\deg(\mathrm{tr}(\boldsymbol{\omega}\mathbf{x}^{-1})) = \mathrm{w}_2(2^n - 2) = n - 1$;

(iii) F is differentially 2-uniform if n is odd and it is differentially 4-uniform if n is even;

(iv) The Euclidean algorithm computes $\mathbf{x}^{-1}$ in polynomial time with respect to n.

Acknowledgements. The author's attention to the mapping $\mathbf{x} \mapsto \mathbf{x}^{-1}$ was drawn by C. Carlet. He observed that the high nonlinearity property (i) was actually proven in the work of Carlitz and Uchiyama [3]. L. R. Knudsen provided the author with examples demonstrating the difference between the odd and even case in (iii).

5. A mapping derived from the exponent mapping in a prime field

Let p be a prime and consider the Abelian group $G = \{0, 1, \ldots, p-1\}$ with the modulo p addition. Let $\mathbf{u}$ be an element of order q in the finite field $GF(p)$. We define a mapping $F : G \to G$ as follows:

$$F(x) = \mathbf{u}^x, \quad \text{for } x \in G,$$

where the exponentiation is computed in $GF(p)$.

Let $\alpha, \beta \in G$ and $\alpha \neq 0$. Then the equation

$$\mathbf{u}^{(x+\alpha) \bmod p} - \mathbf{u}^x = \beta \tag{6}$$

is equivalent to

$$\begin{cases} \mathbf{u}^{x+\alpha} - \mathbf{u}^x = \beta \text{ and } 0 \leq x \leq p-\alpha-1 & (7) \\ \text{or} \\ \mathbf{u}^{x+\alpha-p} - \mathbf{u}^x = \beta \text{ and } p-\alpha \leq x \leq p-1. & (8) \end{cases}$$

Since the solution x of

$$\mathbf{u}^{x+\alpha} - \mathbf{u}^x = \beta$$

is unique modulo q it follows that (7) has at most $\lceil \frac{p-\alpha}{q} \rceil$ solutions in G. Similarily equation (8) has at most $\lceil \frac{\alpha}{q} \rceil$ solutions in G. Consequently equation (6) has at most

$$\lceil \tfrac{p-\alpha}{q} \rceil + \lceil \tfrac{\alpha}{q} \rceil = \tfrac{p-1}{q} + 1$$

solutions in G. We have proved the following.

PROPOSITION 7. *Let F be the mapping from the set of integers modulo a prime p to itself as defined above using exponentiation and an element of order q in $GF(p)$. Then F is differentially $(\frac{p-1}{q}+1)$-uniform.*

The mapping F defined in this section seems to be complex enough to be used as round function of a DES-like cipher over the integers modulo a prime with a small number of rounds. The computational complexity of such a cipher grows with the order of the base element $\mathbf{u}$. Proposition 7 shows the trade-off between the complexity of the enciphering (and deciphering) algorithm and the security against differential cryptanalysis.

6. Other security aspects.

Let us consider as an example a r-round DES-like cipher over $G = (GF(2^n), \oplus)$ with round functions $F_i(\mathbf{x}) = \mathbf{x}^{-1}$. From known plaintext-ciphertext pairs one gets polynomial equations of low degree (linear with the number of rounds) from which the round keys can be easily solved. The same is true if round functions $F_i(\mathbf{x}) = \mathbf{x}^3$ are used. Note the number of known plaintext-ciphertext pairs needed is constant with n. This number is at most linear with n if the inverses of $\mathbf{x} \mapsto \mathbf{x}^{2^k+1}$ are used as round functions.

However, the high nonlinear order of the inversion mapping and the inverses of $\mathbf{x}^{2^k+1}$ comes into effect if these mappings are combined with appropriately chosen linear or affine permutations which may vary from round to round and depend on the secret key. Hereby the virtues (i), (ii) and (iv) presented in §1 are not destroyed since they are linear invariants. By Proposition 1 the same is true for the differential uniformness that quarantees (iii).

An anonymous referee of this paper posed a natural question whether our approach is relevant to the situation where an attacker uses a notion of difference other than *xor* in his differential cryptanalysis attack. In our view, regarding DES-like ciphers, resistance against *xor*-differential analysis has no less crucial relevance as resistance against linear approximation.

Naturally, as well as a cryptanalyst may try any type of approximation he may try any type of differentials. Since all our examples of differentially uniform mappings in $GF(2^n)$ are multiplicative, we should consider differential cryptanalysis with respect to the multiplicative difference

$$\mathbf{x}^*\mathbf{x}^{-1}, \quad \text{for} \quad \mathbf{x}^*, \mathbf{x} \in GF(2^n).$$

Let us assume that F is a multiplicative permutation and A a linear permutation in $GF(2^n)$. Then for a DES-like cipher with $F \circ A$ as a round function, the probability of every one-round multiplicative differential with $\boldsymbol{\alpha} \neq \mathbf{1}$ is

$$P_K\{F(A(\mathbf{x}\boldsymbol{\alpha} \oplus K))F(A(\mathbf{x} \oplus K))^{-1} = \boldsymbol{\beta}\} =$$
$$P_K\{F((A(\mathbf{x}\boldsymbol{\alpha}) \oplus A(K))(A(\mathbf{x}) \oplus A(K))^{-1}) = \boldsymbol{\beta}\} =$$
$$2^{-n},$$

since the mapping

$$\mathbf{z} \mapsto (\mathbf{a} \oplus \mathbf{z})(\mathbf{b} \oplus \mathbf{z})^{-1}$$

is a permutation in $GF(2^n)$ if $\mathbf{a} \neq \mathbf{b}$ and we set $(\mathbf{a} \oplus \mathbf{z})(\mathbf{b} \oplus \mathbf{z})^{-1} = \mathbf{1}$ for $\mathbf{z} = \mathbf{b}$.

Recent related work.

Some of the results of this paper were independently obtained by T. Beth and C. Ding. They present also more examples of almost perfect nonlinear permutations in their paper which is the next to follow in these proceedings.

References

1. E. Biham, A. Shamir, *Differential Cryptanalysis of DES-like Cryptosystems*, J. Cryptology **4** (1991).
2. C. Carlet, *Codes de Reed-Muller, codes de Kerdock et de Preparata, thesis*, Publication of LITP, Institut Blaise Pascal, Université Paris 6, **90.59** (1990).
3. L. Carlitz and S. Uchiyama, *Bounds for exponential sums*, Duke Math. J. **24** (1957), 37-41.
4. X. Lai, J. L. Massey and S. Murphy, *Markov Ciphers and Differential Cryptanalysis*, Advances in Cryptology - Eurocrypt '91. Lecture Notes in Computer Science **547**, Springer-Verlag (1992).
5. T. Matsumoto and H. Imai, *Public quadratic polynomial-tuples for efficient signature-verification and message-encryption*, Advances in Cryptology - Eurocrypt '88. Lecture Notes in Computer Science **330**, Springer-Verlag (1988).
6. K. Nyberg, *On the construction of highly nonlinear permutations*, Advances in Cryptology - Eurocrypt '92. Lecture Notes in Computer Science **658**, Springer-Verlag (1993).
7. K. Nyberg and L. R. Knudsen, *Provable Security Against Differential Cryptanalysis*, Proceedings of Crypto '92 (to appear).