VERSITA

Tatra Mountains
Mathematical Publications
DOI: 10.2478/v10127-012-0041-9
Tatra Mt. Math. Publ. **53** (2012), 103–117

NOTES ON A PREIMAGE-RESISTANT HASH FUNCTION

János Folláth

ABSTRACT. Bérczes, Folláth and Pethő constructed a preimage-resistant hash function. In this paper to investigate the avalanche criterion of this function, we will generalize the results of Coulter and Mathews regarding planar polynomials. At the same time a necessary and sufficient condition for being planar is given for Dembowski-Ostrom monomials. In the even characteristic case both a weaker asymptotic statement and practical test results are presented regarding the avalanche criterion.

1. Introduction

One of the most basic notions for cryptographic applications is the hash function. These functions are important building blocks for most of the protocols and play a fundamental role in verifying passwords and creating digital signatures. Their use is important for constructing cryptographically secure pseudo-random--number generators. There is an extensive literature on hash functions and their applications. We refer here only to two fundamental books on cryptography [19] and [22].

An important requirement against a cryptographic hash function is the preimage-resistance. A preimage-resistant or one-way function is a function which is "easy" to compute but "hard" to invert. Complexity theoretical point of view this means, that a preimage-resistant function can be computed in polynomial time, but all of its inverses only in exponential time. If a function belongs to the **P** (polynomial) class, then its inverses belong to the **NP** class and there can exist a preimage-resistant function in the above sense only if $\mathbf{P} \neq \mathbf{NP}$ (see, e.g., [20]).

2010 Mathematics Subject Classification: 14G50.

Keywords: hash function, finite field, strict avalanche criterion, planar polynomial, Dembowski-Ostrom polynomial.

Research supported in part by the TÁMOP 4.2.1./B-09/1/KONV-2010-0007 project. The project is implemented through the New Hungary Development Plan, cofinanced by the European Social Fund and the European Regional Development Fund.

Despite the lack of the safe theoretical background, there appeared in the literature several suggestions for the construction of one-way functions. The papers [6], [14] [18] and [23], show how to construct a one-way function. O. Goldreich, L. Levin and N. Nisan [13] make a one-to-one one-way function based on the hardness of inverting RSA and the discrete log problem.

J. Buchmann and S. Paulus [5] use results from algebraic number theory to construct a one-way function. It is based on the hardness of the discrete logarithm problem with respect to the ideal class group of algebraic number fields.

Bérczes, Ködmön and Pethő [4] constructed a family of preimage--resistant functions based on norm functions, well studied in the theory of Diophantine equations. Bérczes and Járási [3] extended this result to a family based on index forms. In both cases the functions were reduced modulo m, where m is the product of two large primes. For security reason m should have at least 1024 binary digits. The first construction was implemented by the company Crypto Ltd. under the name Codefish. J.-P. Aumasson [1] pointed out some vulnerability of the implemented algorithm.

Later in [2] we defined a family of polynomials $\mathcal{F}$ that is large, and under mild and easily decidable conditions the members of this family are nearly permutation polynomials.

Theorem 1 ([2, Theorem 2.1.]). *Let $f(\overline{X}) \in \mathbb{F}_q[X_1, \dots, X_m]$ be a polynomial such that*

$$f(\overline{X}) := b(X_1, \dots, X_m) + a(X_1, \dots, X_m)$$

with homogeneous polynomials $a(\overline{X}), b(\overline{X})$ satisfying $k = \deg a(\overline{X}) < \deg b(\overline{X}) = n$, $\deg_{X_i} b(\overline{X}) = n$ for $1 \le i \le m$. Further, suppose that there exist indices $1 \le j_1 < j_2 \le n$ such that the binary form

$$b_0(X_{j_1}, X_{j_2}) := b(0, \dots, 0, X_{j_1}, 0, \dots, 0, X_{j_2}, 0, \dots, 0) \tag{1}$$

has no multiple zero.

Let $N(f, \gamma, q)$ denote the number of solutions of the equation

$$f(X_1, \dots, X_m) = \gamma$$

in $X_1, \dots, X_m \in \mathbb{F}_q$. Then

$$\left|N(f, \gamma, q) - q^{m-1}\right| \le (n-1)(n-2)q^{m-3/2} + 5n^{13/3}q^{m-2}. \tag{2}$$

Moreover, if $q > 15n^{13/3}$, then

$$|N(f, \gamma, q) - q^{m-1}| \le (n-1)(n-2)q^{m-3/2} + (5n^2 + n + 1)q^{m-2}. \tag{3}$$

For $f \in \mathcal{F}$ the preimage-resistance means that for any $\gamma \in \mathbb{F}_q$ it is infeasible to find $\overline{X} \in \mathbb{F}_q^m$ such that $f(\overline{X}) = \gamma$. Our result implies that if q is large enough, then the solution of this equation by chance is computationally infeasible.

(In [2] there are also some informal arguments, that the direct solving algorithms in this magnitude are also computationally infeasible.)

In [2] we also defined a subfamily $\mathcal{F}_1$ such that their members are easy to evaluate.

Proposition 1 ([2, Proposition 5.1.]). *Let $f(\overline{X}) = b(\overline{X}) + a(\overline{X})$ such that $b(\overline{X}) = \beta_1 X_1^r + \dots + \beta_m X_m^r$, $a(\overline{X}) = \alpha_1 X_1^s + \dots + \alpha_m X_m^s$ and $\alpha_1, \dots, \alpha_m \neq 0$, $\beta_1, \dots, \beta_m \neq 0$. If $0 < s < r < q$ and r is odd if $q = 2^f$, then $f(\overline{X})$ satisfies all assumptions of Theorem 1.*

The main subject of this paper is the avalanche criterion of the polynomials of Proposition 1, which is in close connection with the planar polynomials. In Section 2 we will overview the definitions of the avalanche criterion and planar polynomials and present a result regarding their connection.

In Section 3, to investigate the avalanche criterion first we will generalize the results of Coulter and Mathews [9, Theorems 3.3, 4.1 and 4.2] regarding planar polynomials over a finite field (Theorems 6 and 8). An important part of Theorem 8 is, that the type of polynomials presented in [9, Theorems 4.1 and 4.2] (and more generally in Theorem 8 itself) are planar only over fields of characteristic 3. Thus one can reformulate the question first stated in [10]: "Is there any planar polynomial over a field of characteristic greater than 3, that is not Dembowski-Ostrom polynomial?"

With the help of these results large families of polynomials of the form prescribed in Proposition 1 is given, which members all satisfy the strict avalanche criterion of order less than m.

In Section 4 a construction satisfying Proposition 1 is given over fields of even characteristic, for which a weaker, asymptotic form of the avalanche criterion holds.

In Section 5 some practical test results are presented for polynomials over fields of even characteristic also satisfying Proposition 1, but for which the result of Section 4 does not hold.

2. Avalanche criterion

An important desirable property for hash functions is the avalanche effect. Loosely speaking it means, if we change the input slightly the output changes significantly. The notion of the strict avalanche criterion was introduced by Webster and Tavares [24] for Boolean functions. Forrè [11] extended this concept by defining multiple orders of the strict avalanche criterion. Recently Li and Cusick [16] extended and studied these concepts for functions over prime fields of odd characteristic.

It is natural to formulate the strict avalanche criterion for an arbitrary finite field $\mathbb{F}_q$ with $q = p^k$ and p prime

$f(\overline{X})\colon \mathbb{F}_q^n \to \mathbb{F}_q$ fulfills the *strict avalanche criterion* (SAC) if the probability $P\big(f(\overline{X}+\overline{A}) - f(\overline{X}) = \gamma\big) = \frac{1}{q}$ for any fixed $\gamma \in \mathbb{F}_q$ and $\overline{A} \in \mathbb{F}_q^n$ with $wt(\overline{A}) = 1$, where $wt(\overline{A})$ denotes the number of nonzero components of $\overline{A}$ (i.e., the Hamming weight of $\overline{A}$), and $\overline{X}$ is a random variable distributed uniformly over $\mathbb{F}_q^n$.

$f(\overline{X})\colon \mathbb{F}_q^n \to \mathbb{F}_q$ is said to fulfill the *strict avalanche criterion of order m* (SAC(m)) if any function obtained from $f(\overline{X})$ by keeping m of its input components constant fulfills the SAC as well (this must be true for any choice of the position, and any values of the m constant components).

To study the avalanche effect of the hash function defined in Proposition 1 we will use the theory of planar polynomials.

A polynomial $f \in \mathbb{F}_q[X]$ is called a *permutation polynomial* of $\mathbb{F}_q$ if the associated polynomial function $f\colon c \to f(c)$ from $\mathbb{F}_q$ into $\mathbb{F}_q$ is a permutation of $\mathbb{F}_q$.

A polynomial $f \in \mathbb{F}_q[X]$ is called a *planar polynomial* over $\mathbb{F}_q$ if the *difference operator* $\triangle_{f,a} = f(X+a) - f(X)$ is a permutation polynomial over $\mathbb{F}_q$ for each $a \in \mathbb{F}_q^*$.

Any polynomial $f \in \mathbb{F}_q[X]$ may be reduced mod $X^q - X$ to yield a polynomial of degree less than q which induces on $\mathbb{F}_q$ the same function as f. It is called the *reduced form* of f.

We can also extend the notion of permutation polynomial to multivariate polynomials.

A polynomial $f \in \mathbb{F}_q[X_1, \dots, X_n]$ is called *permutation polynomial in n indeterminate* over $\mathbb{F}_q$ if the equation $f(X_1, \dots, X_n) = \alpha$ has q^{n-1} solutions in $\mathbb{F}_q^n$ for each $\alpha \in \mathbb{F}_q$.

Theorem 2 ([17, Theorem 7.42]). *Suppose $f \in \mathbb{F}_q[X_1, \dots, X_n]$ is of the form*

$$f(X_1, \dots, X_n) = g(X_1, \dots, X_m) + h(X_{m+1}, \dots, X_n), \qquad 1 \le m < n.$$

If at least one of g and h is a permutation polynomial over $\mathbb{F}_q$, then f is a permutation polynomial over $\mathbb{F}_q$. If q is prime, then the converse holds as well.

The following statement follows from the corresponding definitions and Theorem 2 by induction.

Theorem 3. *If $f(\overline{X}) = f_1(X_1) + \dots + f_n(X_n)$, such that $f_i \in \mathbb{F}_q[X]$ is planar over $\mathbb{F}_q$ for every $0 < i \le n$, then $f(\overline{X})$ satisfies the strict avalanche criterion of order m for every $m < n$.*

It is natural to try to choose the exponents and the coefficients in Proposition 1 so, that the binomials

$$\beta_i X_i^r + \alpha_i X_i^s \tag{4}$$

are planar.

In the following sections these binomials will be investigated and good parameter choices will be proposed.

Obviously if $s = p^l$, then the binomial (4) will be a sum of a monomial and a linearized polynomial. Since the constant terms disappear in the difference operator and the linear members will appear as a constant, in this case it is enough to choose the parameters of the $\beta_i X_i^r$ monomial such that it will be planar. Only a few necessary conditions are known in the general case, even for monomials (for a survey of the stronger results see [7]).

3. Odd characteristic case

In [12] [15] and [21] the authors independently showed, that any planar polynomial over a prime field must reduce to a quadratic. Consequently if we work over a prime field and set the parameters of the monomial $\beta_i X_i^r$ so that it is planar, it will reduce to a quadratic. Unfortunately this will be weak in the sense, that the direct inverting algorithms will become efficient in the case of such a low degree polynomials.

In [10] Dembowski and Ostrom described a class of polynomials which sometimes give rise to planar functions. As the authors in [9] I will refer to these polynomials as Dembowski-Ostrom polynomials.

Suppose $f \in \mathbb{F}_q[X]$. Then f is a *Dembowski-Ostrom polynomial* if the reduced form of f has the following shape

$$f(X) = \sum_{i,j=0}^{k-1} a_{ij} X^{p^i + p^j}.$$

To give a necessary and sufficient condition for being planar in the case of Dembowski-Ostrom monomials we will need the following results.

Proposition 2 ([9, Proposition 2.4]). *The polynomial X^n is planar over $\mathbb{F}_q$ if and only if $(X+1)^n - X^n$ is a permutation polynomial over $\mathbb{F}_q$. Further, if X^n is a planar polynomial over $\mathbb{F}_q$, then $n \equiv 2 \pmod{p-1}$ and $gcd(n, q-1) = 2$.*

Theorem 4 ([17, Theorem 7.8]).

(1) *Every linear polynomial over $\mathbb{F}_q$ is a permutation polynomial of $\mathbb{F}_q$.*

(2) *The monomial X^n is a permutation polynomial of $\mathbb{F}_q$ if and only if $gcd(n, q-1) = 1$.*

Theorem 5 ([17, Theorem 7.9]). *Let $\mathbb{F}_q$ be of characteristic p. Then the p-polynomial*

$$L(X) = \sum_{i=0}^{m} a_i X^{p^i} \in \mathbb{F}_q[X]$$

is a permutation polynomial of $\mathbb{F}_q$ *if and only if its only root in* $\mathbb{F}_q$ *is* 0.

Now we can state the following

Theorem 6. *Let* $f \in \mathbb{F}_q[X]$, $f(X) = X^{p^i+p^j}$ *with* $i < j$ *and* $q = p^k$, p *an odd prime. Then* f *is planar over* $\mathbb{F}_q$ *if and only if* $k/gcd(i-j,k)$ *is odd.*

Proof. Due to Proposition 2 we only need to determine when the polynomial $(X+1)^{p^i+p^j} - X^{p^i+p^j} = (X^{p^{i-j}} + X + 1)^{p^j}$ is a permutation polynomial over $\mathbb{F}_q$. Permutation polynomials form a group under the operation of composition and subsequent reduction modulo $X^q - X$ and since according to Theorem 4 both X^{p^j} and $X + 1$ is a permutation polynomial over $\mathbb{F}_q$, $(X^{p^{i-j}} + X + 1)^{p^j}$ will be a permutation polynomial over $\mathbb{F}_q$ if and only if $X^{p^{i-j}} + X$ is one. Now according to Theorem 5 $X^{p^{i-j}} + X$ will be a permutation polynomial over $\mathbb{F}_q$ if and only if it has no other roots in $\mathbb{F}_q$ than 0, that is $X^{p^{i-j}-1} \neq -1$ for all $x \in \mathbb{F}_q$. Let α be a primitive element of $\mathbb{F}_q$. Then $\alpha^{t(p^{i-j}-1)} \neq \alpha^{\frac{q-1}{2}}$ for any integer t. So $X^{p^i+p^j}$ is planar over $\mathbb{F}_q$ if and only if the congruence

$$t(p^{i-j} - 1) \equiv (p^k - 1)/2 \pmod{p^k - 1}$$

has no integer solution t. Now $iu \equiv v \,(\mathrm{mod}\ n)$ has an integer solution t if and only if $(u,n)|v$. So we have a solution t if and only if

$$gcd(p^{i-j} - 1, p^k - 1) \not| (p^k - 1)/2$$

or equivalently $p^{gcd(i-j,k)} - 1 \not| (p^k - 1)/2$. Let $d = gcd(i-j,k)$. Then there is no integer solution t if and only if the 2-adic order of $p^d - 1$ is greater than the 2-adic order of $p^k - 1$. But

$$p^k - 1 = (p^d - 1)\big(1 + p^d + p^{2d} + \cdots + p^{((k/d)-1)d}\big).$$

Here the second factor on the right side has (k/d) members each of which are odd, so this condition is equivalent to $k/gcd(i-j,k)$ being odd. □

This result is a generalization in [9, Theorem 3.3] where the authors gave a similar condition for monomials of the form $f(X) = X^{p^i+1}$.

Proposition 3. *Let* $f(\overline{X}) = b(\overline{X}) + a(\overline{X})$ *such that* $b(\overline{X}) = \beta_1 X_1^r + \cdots + \beta_m X_m^r$, $a(\overline{X}) = \alpha_1 X_1^s + \cdots + \alpha_m X_m^s$ *and* $\alpha_1, \ldots, \alpha_m \neq 0$, $\beta_1, \ldots, \beta_m \neq 0$, $\alpha_i, \beta_i \in \mathbb{F}_q$, *where* $q = p^k$, p *an odd prime and* $0 < i \leq m$.

If $r = p^i + p^j$ *such that* $k/gcd(i-j,k)$ *is odd and* $s = p^l$, *then* $f(\overline{X})$ *will satisfy the strict avalanche criterion of every order* $n < m$.

Proof. It is an immediate consequence of Theorem 3 and Theorem 6. □

In [21] it was conjectured, that up to addition of an additive polynomial, every planar polynomial on $\mathbb{F}_q$ is a Dembowski-Ostrom polynomial. Later in [9] two counterexamples to this conjecture were given. Both of these examples are monomials over fields of characteristic 3. In the following we will generalize these results regarding the characteristic 3 case, and prove that these type of monomials are not planar in fields of higher characteristic. Thus one can restate the conjecture: Up to addition of an additive polynomial, every planar polynomial on $\mathbb{F}_{p^k}$, $k > 3$ is a Dembowski-Ostrom polynomial.

To prove the next result we will need the notion of the Dickson polynomials. This is a well studied class of polynomials, and over the complex numbers they are in correspondence with the Chebyshev polynomials of the first kind. Regarding the following facts about the Dickson polynomials we refer to the book [17]. The explicit form of the Dickson polynomials over a field $\mathcal{F}$ is the following

$$g_k(x,a) = \sum_{j=0}^{\lfloor k/2 \rfloor} \frac{k}{k-j} \binom{k-j}{j} (-a)^j x^{k-2j}.$$

In the field of the rational functions over $\mathcal{F}$ in the indeterminate y we have the identity

$$g_k\left(y + \frac{a}{y}, a\right) = y^k + \frac{a^k}{y^k}.$$

Theorem 7 ([17, Theorem 7.16]). *The Dickson polynomial $g_k(x,a)$, $a \in \mathbb{F}_{q^*}$, $q = p^e$, p prime, is a permutation polynomial of $\mathbb{F}_q$ if and only if $gcd(k, q^2–1) = 1$.*

Theorem 8. *Let $q = p^e$ and $\alpha, \beta \in \mathbb{N}$. The polynomial $X^{(p^\alpha + p^\beta)/2}$ is planar over $\mathbb{F}_q$ if and only if $p = 3$ and $(\alpha - \beta, 2e) = 1$.*

Proof. Firstly we will notice, that the polynomial X^n is planar over $\mathbb{F}_q$ if and only if $\triangle_{f,4}(X) = (X+4)^n - X^n$ is a permutation polynomial over $\mathbb{F}_q$. Indeed

$$(X+a)^n - X^n = a^n c^n \Big(\big(X/(ac) + 4\big)^n - \big(X/(ac)\big)^n \Big),$$

where $4c \equiv 1 \pmod{p}$ (there will always be such a c, because $(4,p)|1$).

Suppose $f(X) = X^n$ and define $h(X)$ to be $\triangle_{f,4}(X-2) = (X+2)^n - (X-2)^n$. Since permutation polynomials form a group under the operation of composition and subsequent reduction modulo $X^q - X$, $\triangle_{f,4}(X)$ will be a permutation polynomial of $\mathbb{F}_q$ if and only if $h(X)$ is one. Then $f(X)$ is planar over $\mathbb{F}_q$ if and only if $h(X)$ is a permutation polynomial over $\mathbb{F}_q$. Let $\eta \in \mathbb{F}_{q^2}$ the root of the polynomial $Z^2 - xZ + 1$. Then $x = \eta + \eta^{-1}$ and

$$\begin{aligned} h(x) &= \big(\eta + \eta^{-1} + 2\big)^n - \big(\eta + \eta^{-1} - 2\big)^n \\ &= \frac{(\eta^2 + 1 + 2\eta)^n - (\eta^2 + 1 - 2\eta)^n}{\eta^n} \\ &= \frac{(\eta + 1)^{2n} - (\eta - 1)^{2n}}{\eta^n}. \end{aligned}$$

If $n = (p^\alpha + p^\beta)/2$, then

$$\begin{aligned} h(x) &= \frac{(\eta + 1)^{p^\alpha + p^\beta} - (\eta - 1)^{p^\alpha + p^\beta}}{\eta^{(p^\alpha + p^\beta)/2}} \\ &= \frac{2\eta^{p^\alpha} + 2\eta^{p^\beta}}{\eta^{(p^\alpha + p^\beta)/2}} \\ &= 2(\eta^{(p^\alpha - p^\beta)/2} + \eta^{-(p^\alpha - p^\beta)/2}) \\ &= 2g_{(p^\alpha - p^\beta)/2}(x, 1). \end{aligned}$$

Thus X^n is planar if and only if, the Dickson polynomial $g_{(p^\alpha - p^\beta)/2}(X, 1)$ is a permutation polynomial over $\mathbb{F}_q$. According to Theorem 7 it will occur if and only if $gcd\big((p^\alpha - p^\beta)/2, q^2 - 1\big) = 1$. Since $q^2 - 1 \equiv -1 \pmod p$ this is equivalent to $gcd\big((p^{\alpha-\beta} - 1)/2, q^2 - 1\big)$. Since $q^2 \equiv 1 \pmod 4$, this holds if and only if $gcd\big((p^{\alpha-\beta} - 1), p^{2e} - 1\big) = p^{gcd(\alpha-\beta,2e)} - 1 = 2$, which holds if and only if $p = 3$ and $(\alpha - \beta, 2e) = 1$. □

Proposition 4. *Let $f(\overline{X}) = b(\overline{X}) + a(\overline{X})$ such that $b(\overline{X}) = \beta_1 X_1^r + \dots + \beta_m X_m^r$, $a(\overline{X}) = \alpha_1 X_1^s + \dots + \alpha_m X_m^s$ and $\alpha_1, \dots, \alpha_m \neq 0$, $\beta_1, \dots, \beta_m \neq 0$, $\alpha_i, \beta_i \in \mathbb{F}_q$ where $q = 3^k$ and $0 < i \le m$.*

Let $r = (3^a + 3^b)/2$, where $a, b \in \mathbb{N}$, $gcd(a - b, 2k) = 1$ and $s = p^l$. Then $f(\overline{X})$ will satisfy the strict avalanche criterion of every order $n < m$.

Proof. It is an immediate consequence of Theorem 3 and Theorem 8. □

4. Even characteristic case

From the implementation point of view the most advantageous options are big prime fields and fields of characteristic two. As stated in the previous section prime fields are not the best choice because of the small degree of the planar polynomials.

It is easy to see that there are no planar polynomials over fields of even characteristic. Consequently the binomial

$$\beta_i X_i^r + \alpha_i X_i^s \tag{5}$$

also cannot be planar over fields of even characteristic. In this section a weaker asymptotic statement will be proven.

We will need the following result.

Theorem 9 ([8, Theorem 3]). *Let $q = p^k$, n be a non-negative integer and $f \in \mathbb{F}_q[X]$ be the trinomial $f(X) = X^{p^n} - aX - b$ where $a \in \mathbb{F}_q^*$. Set $d = gcd(n,k)$ and $m = k/d$. Let Tr_d be the trace function from $\mathbb{F}_q$ onto $\mathbb{F}_{q^d}$. For $0 \le i \le m-1$ define $t_i = \sum_{j=i}^{m-2} p^n(j+1)$. Put $\alpha_0 = a$ and $\beta_0 = b$. If $m > 1$, then for $1 \le r \le m-1$, set $\alpha_r = a^{1+p^n+\cdots+p^{nr}}$ and*

$$\beta_r = \sum_{i=0}^{r} a^{s_i} b^{p^{ni}},$$

where $s_i = \sum_{j=i}^{r-1} p^{n(j+1)}$ for $0 \le i \le r-1$ and $s_r = 0$. The trinomial f has no roots in $\mathbb{F}_q$ if and only if $\alpha_{m-1} = 1$ and $\beta_{m-1} \ne 0$. When $\alpha_{m-1} \ne 1$ then f has a unique root in $x \in \mathbb{F}_q$, namely, $x = \beta_{m-1}/(1-\alpha_{m-1})$. Otherwise f has p^d roots in $\mathbb{F}_q$ given by $x + \delta\tau$ where $\delta \in \mathbb{F}_{p^d}$, τ is a fixed element of $\mathbb{F}_q$ satisfying $\tau^{p^n-1} = a$ and, for any $c \in \mathbb{F}_q^*$ satisfying $Tr_d(c) \in \mathbb{F}_{p^d}$,

$$x = \frac{1}{Tr_d(c)} \sum_{i=0}^{m-1} \left(\sum_{j=0}^{i} c^{p^{nj}} \right) a^{t_i} b^{p^{ni}}.$$

Theorem 10. *Let us define $f \in \mathbb{F}_q[x_1, \ldots, x_m]$ as*

$$f(x_1, \ldots, x_m) = \sum_{i=1}^{m} \alpha_i x_i^n + \sum_{i=1}^{m} \beta_i x_i,$$

where $q = 2^k$ and $n = 2^l + 1$ such that $gcd(l,k) = 1$. Let Tr be the absolute trace function of $\mathbb{F}_q$, and $\delta, \gamma \in \mathbb{F}_q$.

$$f(x_1, \ldots, x_m) - f(x_1, \ldots, x_j + \delta, \ldots, x_m) = \gamma$$

holds if and only if $Tr\big((\beta_j\delta + \gamma)\alpha_j^{-1}\delta^{-n} + 1\big) = 0$, and only for exactly two distinct values of x_j.

Proof. By the definition

$$f(x_1, \ldots, x_m) = \sum_{i=1}^{m} \alpha_i x_i^n + \sum_{i=1}^{m} \beta_i x_i,$$

and since only the jth term changes

$$f(x_1, \ldots, x_j + \delta, \ldots, x_m) = \sum_{\substack{i=1 \\ i \ne j}}^{m} \alpha_i x_i^n + (x_j + \delta)^n \alpha_j + \sum_{\substack{i=1 \\ i \ne j}}^{m} \beta_i x_i + (x_j + \delta)\beta_j,$$

we conclude

$$f(x_1,\dots,x_m)-f(x_1,\dots,x_j+\delta,\dots,x_m)=\alpha_j\bigl(x_j^n+(x_j+\delta)^n\bigr)+\beta_j\delta.$$

Consequently, $f(x_1,\dots,x_m)-f(x_1,\dots,x_j+\delta,\dots,x_m)=\gamma$ holds exactly if the value of x_j is a zero of the following polynomial

$$p(x)=x^n+(x+\delta)^n+\gamma',$$

where $\gamma'=(\beta_j\delta+\gamma)\alpha_j^{-1}$. Since $p(x)=\delta^n\bigl(y^n+(y+1)^n+\gamma''\bigr)$, where $y=x\alpha_j^{-1}$ and $\gamma''=\gamma'\delta^{-n}$ the zeros of

$$p'(y)=y^n+(y+1)^n+\gamma''$$

has to be determined. Since $n=2^l+1$,

$$p'(y)=y^n+(y+1)(y^{n-1}+1)+\gamma''=y^{2^l}+y+(\gamma''+1).$$

According to Theorem 9 if $gcd(l,k)=1$, then $p'(y)$ either has 2 or 0 roots depending on γ''. Since $gcd(l,k)=1$, $a=1$ and $b=\gamma''+1$,

$$\beta_{k-1}=\sum_{i=0}^{k-1}(\gamma''+1)^{2^{li}}.$$

The integers $1,\dots,k-1$ constitute a complete residue system modulo k. $gcd(l,k)=1$ consequently $l,\dots,(k-1)l$ is also a complete residue system modulo k. Since $\delta^{2^k}=\delta$ holds for every $\delta\in\mathbb{F}_q$

$$\beta_{k-1}=\sum_{i=0}^{k-1}(\gamma''+1)^{2^i}=Tr\bigl((\beta_j\delta+\gamma)\alpha_j^{-1}\delta^{-n}+1\bigr).$$

□

Although the hash function in question does not satisfy the strict avalanche criterion, a weaker asymptotic statement holds.

Theorem 11. *Let us define $f\in\mathbb{F}_q[x_1,\dots,x_m]$ as*

$$f(x_1,\dots,x_m)=\sum_{i=1}^{m}\alpha_i x_i^n+\sum_{i=1}^{m}\beta_i x_i,$$

where $q=2^k$ and $n=2^l+1$ such that $(l,k)=1$. Then

$$(1-q\varepsilon)^{m-1}\left(\frac{1}{q}-\varepsilon\right)\le P\bigl(f(x_1,\dots,x_m)-f(x_1+\delta_1,\dots,x_m+\delta_m)=\gamma\bigr)$$
$$\le(1+q\varepsilon)^{m-1}\left(\frac{1}{q}+\varepsilon\right),$$

where $0\le\varepsilon\le nq^{-\frac{3}{2}}$.

Proof. Let D_{γ_i} be the event that

$$f(x_1,\dots,x_m)-f(x_1,\dots,x_i+\delta_i,\dots,x_m)=\gamma_i.$$

According to Theorem 10

$$\begin{aligned}P(D_{\gamma_i}|\delta_i\in A_{\gamma_i})&=0,\\ P(D_{\gamma_i}|\delta_i\in B_{\gamma_i})&=\frac{1}{2^{k-1}},\end{aligned}$$

where

$$\begin{aligned}A_{\gamma_i}&=\Big\{\delta|Tr\big((\beta_i\delta+\gamma)\alpha_i^{-1}\delta^{-n}+1\big)=1\Big\},\\ B_{\gamma_i}&=\Big\{\delta|Tr\big((\beta_i\delta+\gamma)\alpha_i^{-1}\delta^{-n}+1\big)=0\Big\}.\end{aligned}$$

Let $g(x)=(\beta_jx+\gamma)\alpha_j^{-1}x^{-n}+1$ and $h(x)=\alpha_j^{-}1\beta_jx^{n+1}+\gamma\alpha_i^{-1}x^n+1$. Let χ be a nontrivial additive character of $\mathbb{F}_q$. Since $\chi\big(g(x)\big)=\chi\big(h(x^{-1})\big)$ for every $x\neq 0$ and $\chi\big(g(0)\big)=\chi\big(h(0)\big)$, using Weil's theorem ([17, Theorem 5.38])

$$||A_{\gamma_i}|-|B_{\gamma_i}||=\left|\sum_{\delta\in\mathbb{F}_q}\chi\big(g(x)\big)\right|\leq nq^{1/2}$$

follows. $P(\delta_i\in A_{\gamma_i})+P(\delta_i\in B_{\gamma_i})=1$, consequently

$$P(A_{\gamma_i})=\frac{1}{2}\pm\epsilon_{\gamma_i},\qquad P(B_{\gamma_i})=\frac{1}{2}\mp\epsilon_{\gamma_i},$$

where $\epsilon_{\gamma_i}\leq\frac{n}{2q^{1/2}}$. By the theorem of total probability

$$P(D_{\gamma_i})=P(D_{\gamma_i}|A_{\gamma_i})P(A_{\gamma_i})+P(D_{\gamma_i}|B_{\gamma_i})P(B_{\gamma_i})=\frac{1}{q}\pm\varepsilon_{\gamma_i},$$

where $\varepsilon_{\gamma_i}\leq nq^{-3/2}$. Notice, that due to the structure of $f(x_1,\dots,x_m)$, the events D_{γ_i} are independent, moreover $f(x_1,\dots,x_m)-f(x_1+\alpha_1,\dots,x_m+\alpha_m)=\gamma$ holds if and only if the events D_{γ_i} $(i=1,\dots,m)$ hold with $\gamma_1+\dots+\gamma_m=\gamma$. Therefore

$$\begin{aligned}&P\big(f(x_1,\dots,x_m)-f(x_1+\alpha_1,\dots,x_m+\alpha_m)=\gamma\big)\\ &=\sum_{\substack{i_1,\dots,i_m\\ \gamma_{i_1}+\dots+\gamma_{i_m}=\gamma}}\prod_{j=1}^{m}P(D_{\gamma_{i_j}}).\end{aligned}$$

According to Theorem 2 $h(x_1,\dots,x_m)=x_1+\dots+x_m$ is a permutation polynomial and as such, it has q^{m-1} solutions. Consequently

$$\sum_{\substack{i_1,\dots,i_m\\ \gamma_{i_1}+\dots+\gamma_{i_m}=\gamma}}\prod_{j=1}^{m}P(D_{\gamma_{i_j}})\leq q^{m-1}\left(\frac{1}{q}+\varepsilon\right)^m=(1+q\varepsilon)^{m-1}\left(\frac{1}{q}+\varepsilon\right)$$

and

$$\sum_{\substack{i_1,\dots,i_m \\ \gamma_{i_1}+\dots+\gamma_{i_m}=\gamma}} \prod_{j=1}^{m} P(D_{\gamma_{i_j}}) \geq q^{m-1}\left(\frac{1}{q}-\varepsilon\right)^m = (1-q\varepsilon)^{m-1}\left(\frac{1}{q}-\varepsilon\right)$$

hold, where $\varepsilon = \max_{\gamma_i} \varepsilon_{\gamma_i}$ and the maximum is taken over all γ_i appearing in the solution vectors of $h(x_1,\dots,x_m)$. $\square$

5. Test results

Unfortunately the conditions of Theorem 11 are quite strict, and therefore there has been also some practical testing, to investigate the behavior of the hash function with other exponents. The effect of changing an input bit to the output bits were tested for multiple choice of exponents and coefficients of the polynomial. There were 1500–1500 random input samples in each test.

On the figures the x-axis stands for the input bits, the y-axis represents the output bits and the points on the z-axis mean the number of samples. An (x,y,z) point on the figure means, that with changing the xth input bit, the yth output bit changed in the case of z samples:

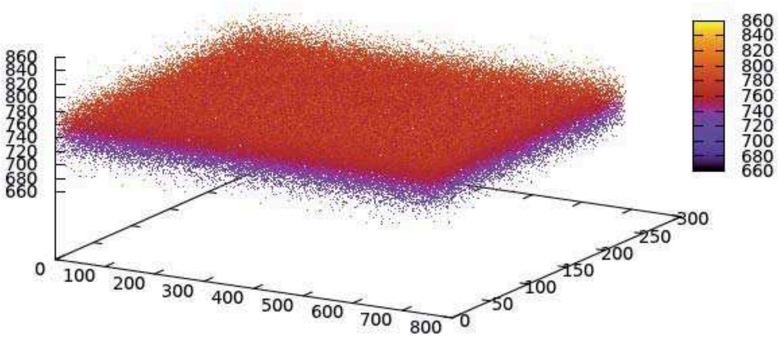

Figure 1. Base test results.

$r = 286295073$; $s = 1$.
The values of β_i
3d1b58ba507ed7ab625558ec238e1f2974b0dc5119495cff327b23c6643c9869,
519b500d431bd7b76b68079a4e6afb667fdcc2331befd79f3352255a109cf92e,
3a95f874081386412ca886110836c40e189a769b54e49eb479838cb24353d0cd.
The values of α_i
1190cde766ef438d4db127f80216231b515f007c5bd062c241b71efb79e2a9e3,
6763845e75a2a8d4721da3172443a858436c6125628c895d7c83e458257130a3,
440badfc05072367614fd4a1419ac24122221a704516dde97c3dbd3d737b8ddc.

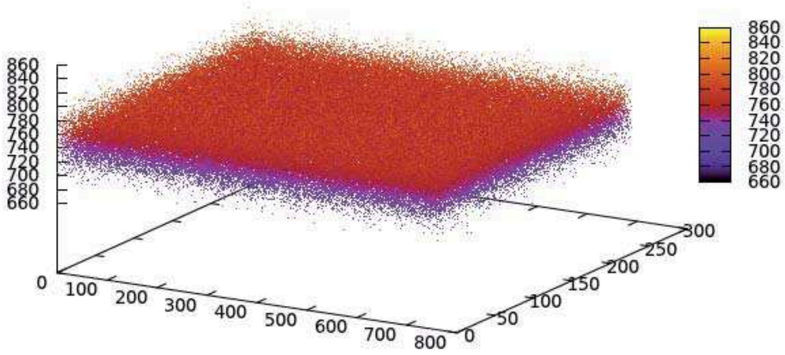

Figure 2. Test results with changed coefficients.

$r = 286295073$; $s = 1$.
The values of β_i
680c1b62443d8e597a1c574377d02f4866613afa24a7c25e0eed54217fcf7bf2,
6d5e56326881ca2d1642e53a02208f331e81e2ee73333b123d5c5c2d37cd332f,
2df5b11c2fdc7fd51ad7b7c6115a9ce6651e5e3b53fe40b97e8820947c2e42da.
The values of α_i
57cffdde091852a979ef5e9e462d4a4336cc7f001ad4086200c828696a5674f1,
1c1463c6023ee43c7e674f6b4b72653c27954eaa4aaa3cd33c9179df629e2171,
6453d5b017a483cb6a9868e9700f352168ad2b6a337dbb410b69b04a461f650f.

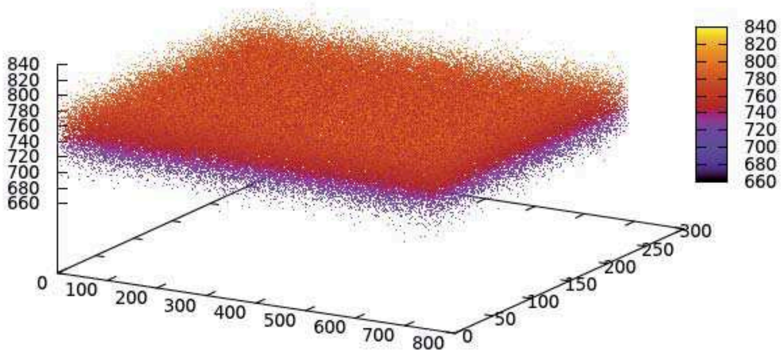

Figure 3. Test results with small exponent.

$r = 127$; $s = 1$.
The values of β_i**.**
3d1b58ba507ed7ab625558ec238e1f2974b0dc5119495cff327b23c6643c9869,
519b500d431bd7b76b68079a4e6afb667fdcc2331befd79f3352255a109cf92e,
3a95f874081386412ca886110836c40e189a769b54e49eb479838cb24353d0cd.
The values of α_i
1190cde766ef438d4db127f80216231b515f007c5bd062c241b71efb79e2a9e3,
6763845e75a2a8d4721da3172443a858436c6125628c895d7c83e458257130a3,
440badfc05072367614fd4a1419ac24122221a704516dde97c3dbd3d737b8ddc.

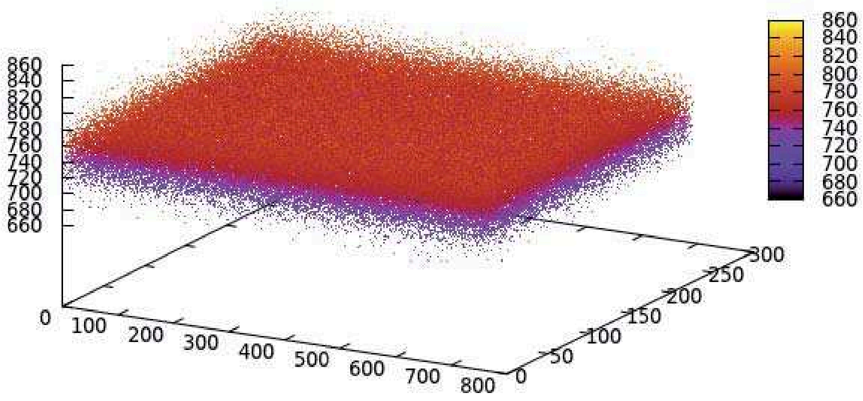

Figure 4. Test results with low-weight exponent.

$r = 268435459$ $(2^{28} + 2^1 + 2^0)$; $s = 1$.
The values of β_i.
3d1b58ba507ed7ab625558ec238e1f2974b0dc5119495cff327b23c6643c9869,
519b500d431bd7b76b68079a4e6afb667fdcc2331befd79f3352255a109cf92e,
3a95f874081386412ca886110836c40e189a769b54e49eb479838cb24353d0cd.
The values of α_i
1190cde766ef438d4db127f80216231b515f007c5bd062c241b71efb79e2a9e3,
6763845e75a2a8d4721da3172443a858436c6125628c895d7c83e458257130a3,
440badfc05072367614fd4a1419ac24122221a704516dde97c3dbd3d737b8ddc.

It is clear, that on the figures the points are in the neighborhood of the plane $x = 750$, that is, the empiric probability is near to the $\frac{1}{2}$ required by the avalanche effect.

Though these polynomials do not satisfy the strict avalanche criterion of any order, these test results give a hope that they also possesses the avalanche property in some weaker sense, like the special case in Theorem 11.

REFERENCES

[1] AUMASSON, J.-P.: *Cryptanalysis of a hash function based on norm form equations*, Cryptologia **33** (2009), 1–4.

[2] BÉRCZES, A.—FOLLÁTH, J.—PETHŐ, A.: *On a family of preimage-resistant functions*, Tatra Mt. Math. Publ. **47** (2010), 1–13.

[3] BÉRCZES, A.—JÁRÁSI, I.: *An application of index forms in cryptography*, Period. Math. Hungar. **58** (2008), 35–45.

[4] BÉRCZES, A.—KÖDMÖN, J.—PETHŐ, A.: *A one-way function based on norm form equations*, Period. Math. Hungar. **49** (2004), 1–13.

[5] BUCHMANN, J.—PAULUS, S.: *A one-way function based on ideal arithmetic in number fields*, Lecture Notes in Comput. Sci. **1294** (1997), 385–394.

[6] CHAO, L. R.—LIN, Y. C.: *Associative one-way function and its significances to cryptographics*, Internat. J. Inform. Management Sci. **5** (1994), 53–59.

[7] COULTER, R. S.: *Planar monomials over fields of prime square order*, Proc. Amer. Math. Soc. **134** (2006), 3373–3378.

[8] COULTER, R. S.—HENDERSON, M.: *A note on the roots of trinomials over a finite field*, Bull. Austral. Math. Soc. **69** (2004), 429–432.

[9] COULTER, R. S.—MATTHEWS R. W.: *Planar functions and planes of Lenz-Barlotti class II*, Des. Codes Cryptogr. **10** (1997), 167–184.

[10] DEMBOWSKI, P.—OSTROM, T. G.: *Planes of order n with collineation groups of order n^2*, Math. Z. **103** (1968), 239–258.

[11] FORRÈ, R.: *The strict avalanche criterion: spectral properties of Boolean functions and an extended definition*, in: CRYPTO '88—Advances in Cryptology (S. Goldwasser, ed.), Santa Barbara, California, USA, 1988, Lecture Notes in Comput. Sci., Vol. 403, Springer--Verlag, New York, NY, USA, 1990, pp. 450–468.

[12] GLUCK, D.: *A note on permutation polynomials and finite geometries*, Discrete Math. **80** (1990), 97–100.

[13] GOLDREICH, O.—LEVIN, L.—NISAN, N.: *On constructing 1-1 one-way functions*, in: Proc. of the Electronic Colloquium on Computational Complexity (ECCC), Vol. 2, 1995, pp. 1–11.

[14] HEMASPAANDRA, L. A.—ROTHE, J.: *Creating strong, total, commutative, associative one-way functions from any one-way function in complexity theory*, J. Comput. System Sci. **58** (1999), 648–659.

[15] HIRAMINE, Y.: *A conjecture on affine planes of prime order*, J. Combin. Theory Ser. A **52** (1989), 44–50.

[16] LI, Y.—CUSICK, T. W.: *Strict avalanche criterion over finite fields*, Math. Cryptology **1** (2008) 65–78.

[17] LIDL, R.—NIEDERREITER, H.: *Finite Fields*. Cambridge University Press, Cambridge, 1997.

[18] MERKLE, R. C.: *A fast software one-way hash function*, J. Cryptology **3** (1990), 43–58.

[19] MENEZES, A. J.—VAN OORSCHOT, P. C.—VANSTONE, S. A.: *Handbook of Applied Cryptography*. CRC Press, Boca Raton, 1997.

[20] PAPADIMITRIOU, C. H.: *Computational complexity*. Addison-Wesley Publ. Comp., Reading, MA, 1994.

[21] RÓNYAI, L.— SZŐNYI, T.: *Planar functions over finite fields*, Combinatorica **9** (1989), 315–320.

[22] SCHNEIER, B.: *Applied Cryptography*. John Wiley & Sons, New York, 1996.

[23] SUN, Q.: *A kind of trap-door one-way function over algebraic integers*, J. Sichuan Univ., Nat. Sci. Ed. **2** (1986), 22–27.

[24] WEBSTER, A. F.—TAVARES, S. E.: *On the design of S-boxes*, in: Advances in Cryptology—CRYPTO '85 (H. C. Williams, ed.), Santa Barbara, 1985, Lecture Notes in Comput. Sci., Vol. 218, Springer-Verlag, New York, 1986, pp. 523–534.

Received October 18, 2012

Department of Computer Science
Faculty of Informatics
University of Debrecen
Egyetem tér 1.
HU–4032 Debrecen
HUNGARY
E-mail: janos.follath@inf.unideb.hu