The Multivariate Method strikes again: New Power Mappings with Low Differential Uniformity in odd Characteristic

P. Felke

BFA 2019

The Differential Uniformity

Equivalence Relations

Mappings over Fields of odd Characteristic in Cryptography

The Multivariate Method

Conclusion & Open Problems

The Differential Uniformity

Equivalence Relations

Mappings over Fields of odd Characteristic in Cryptography

The Multivariate Method

Conclusion & Open Problems

Δ-Mapping

Let p be a prime and $\mathbb{F}_{p^n}$ a field of degree n. Let f be a mapping $f : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$.

- For $c \in \mathbb{F}_{p^n}$ we define $\Delta_{f,c}(x) := f(x + c) - f(x)$.

Δ-Mapping

Let p be a prime and $\mathbb{F}_{p^n}$ a field of degree n. Let f be a mapping $f : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$.

- For $c \in \mathbb{F}_{p^n}$ we define $\Delta_{f,c}(x) := f(x+c) - f(x)$.
- $N_f(c,a)$ is defined as $\#\Delta_{f,c}^{-1}(a)$ for $a, c \in \mathbb{F}_{p^n}$, i.e. the number of solutions of $f(x+c) - f(x) - a = 0$.

Δ-Mapping

Let p be a prime and $\mathbb{F}_{p^n}$ a field of degree n. Let f be a mapping $f : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$.

- For $c \in \mathbb{F}_{p^n}$ we define $\Delta_{f,c}(x) := f(x+c) - f(x)$.
- $N_f(c,a)$ is defined as $\#\Delta_{f,c}^{-1}(a)$ for $a, c \in \mathbb{F}_{p^n}$, i.e. the number of solutions of $f(x+c) - f(x) - a = 0$.
- The family $(N_f(c.a))_{c,a\in\mathbb{F}_{p^n}}$ is called the difference spectrum.
- The (differential) uniformity of f is $\mathcal{U}_f := \max\{N_f(c,a) | a, c \in \mathbb{F}_{p^n}, c \neq 0\}$.
- A mapping f is called (differentially) k-uniform if $\mathcal{U}_f = k$.
- If f is a power mapping x^d we write $N_d(c,a), \Delta_{d,c}(x), \ldots$

Δ-Mapping

Let p be a prime and $\mathbb{F}_{p^n}$ a field of degree n. Let f be a mapping $f : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$.

- For $c \in \mathbb{F}_{p^n}$ we define $\Delta_{f,c}(x) := f(x+c) - f(x)$.
- $N_f(c,a)$ is defined as $\#\Delta_{f,c}^{-1}(a)$ for $a, c \in \mathbb{F}_{p^n}$, i.e. the number of solutions of $f(x+c) - f(x) - a = 0$.
- The family $(N_f(c.a))_{c,a\in\mathbb{F}_{p^n}}$ is called the difference spectrum.
- The (differential) uniformity of f is $\mathcal{U}_f := \max\{N_f(c,a) | a, c \in \mathbb{F}_{p^n}, c \neq 0\}$.
- A mapping f is called (differentially) k-uniform if $\mathcal{U}_f = k$.
- If f is a power mapping x^d we write $N_d(c,a), \Delta_{d,c}(x), \ldots$

- If $k = 1$, then f is called perfect nonlinear (PN) or planar.
- If $k = 2$, then f is called almost perfect nonlinear (APN).

The Differential Uniformity

Equivalence Relations

Mappings over Fields of odd Characteristic in Cryptography

The Multivariate Method

Conclusion & Open Problems

Equivalence Relations preserving the Difference Properties

The seminal equivalence relation which preserves the difference spectrum $(N_f(c,a))_{c,a\in\mathbb{F}_{p^n}}$ is

Carlet-Charpin-Zinoviev equivalence - CCZ-equivalence

Two functions f, h from $\mathbb{F}_{p^n}$ to itself are called CCZ-equivalent if for some affine permutation $\mathcal{L}$ of $\mathbb{F}_{p^n}^2$
$\mathcal{L}(\Gamma_f) = \Gamma_h$, where
$\Gamma_f = \{(x, f(x)) | x \in \mathbb{F}_{p^n}\}$ and $\Gamma_h = \{(x, h(x)) | x \in \mathbb{F}_{p^n}\}$.

Equivalence Relations preserving the Difference Properties

The seminal equivalence relation which preserves the difference spectrum $(N_f(c,a))_{c,a\in\mathbb{F}_{p^n}}$ is

Carlet-Charpin-Zinoviev equivalence - CCZ-equivalence

Two functions f, h from $\mathbb{F}_{p^n}$ to itself are called CCZ-equivalent if for some affine permutation $\mathcal{L}$ of $\mathbb{F}_{p^n}^2$
$\mathcal{L}(\Gamma_f) = \Gamma_h$, where
$\Gamma_f = \{(x, f(x))|x \in \mathbb{F}_{p^n}\}$ and $\Gamma_h = \{(x, h(x))|x \in \mathbb{F}_{p^n}\}$.

- Differentially k-uniform mappings are classified according to CCZ-equivalence.
- Helleseth, Rong and Sandberg conducted extensive computer search in the 90th to classify k-uniform power mappings. These numerical results are well-known as the H-R-S tables.

For power mappings we have the following results

U. Dempwolff

Let $\mathbb{F}_{p^n}$ be a finite field of characteristic p and x^k and x^l be power functions on $\mathbb{F}_{p^n}$. Then x^k and x^l are CCZ-equivalent, if and only if there exists a positive integer $0 \leq m < n$, such that
$l = p^m k \bmod (p^n - 1)$ or $kl = p^m \bmod (p^n - 1)$.

☞Note, that the latter condition means that $x^{p^{n-m}k}$ and x^l are inverse to each other.

- For power mappins x^d the difference spectrum is completely determined by the difference spectrum $(N_d(1,a))_{a \in \mathbb{F}_{p^n}}$.
- x^d is CCZ-equivalent to $(x - \frac{1}{2})^d$ over $\mathbb{F}_{p^n}, p$ odd.
  Thus we will consider $\Delta_{d,1}\left(x - \frac{1}{2}\right)$ because this is often more convenient.

The Differential Uniformity

Equivalence Relations

Mappings over Fields of odd Characteristic in Cryptography

The Multivariate Method

Conclusion & Open Problems

$\mathbb{F}_{3^n}$ matters in Cryptography

$\mathbb{F}_{3^n}$ matters in Cryptography

- The proprietary hash function Curl employed in the cryptocurrency IOTA makes use of ternary S-boxes and is vulnerable to differential cryptanalysis.

$\mathbb{F}_{3^n}$ matters in Cryptography

- The proprietary hash function Curl employed in the cryptocurrency IOTA makes use of ternary S-boxes and is vulnerable to differential cryptanalysis.
- The IOTA foundation substituted it by the new ternary hash function Troika in collaboration with Cybercrypt (Bogdanov et al.) and initiated a crypto challenge over 200.000 €.

$\mathbb{F}_{3^n}$ matters in Cryptography

- The proprietary hash function Curl employed in the cryptocurrency IOTA makes use of ternary S-boxes and is vulnerable to differential cryptanalysis.
- The IOTA foundation substituted it by the new ternary hash function Troika in collaboration with Cybercrypt (Bogdanov et al.) and initiated a crypto challenge over 200.000 €.
- The foundation is currently developing new computer chips built around base-3 logic (`https://cryptobriefing.com/iota-new-hash-function/`).

$\mathbb{F}_{3^n}$ matters in Cryptography

- The proprietary hash function Curl employed in the cryptocurrency IOTA makes use of ternary S-boxes and is vulnerable to differential cryptanalysis.
- The IOTA foundation substituted it by the new ternary hash function Troika in collaboration with Cybercrypt (Bogdanov et al.) and initiated a crypto challenge over 200.000 €.
- The foundation is currently developing new computer chips built around base-3 logic (`https://cryptobriefing.com/iota-new-hash-function/`).
- In this context research on bijective power mappings with low uniformity over $\mathbb{F}_{3^n}$ is of particular interest as they can be also employed in S-boxes for SPN- and streamciphers.

$\mathbb{F}_{3^n}$ matters in Cryptography

- The proprietary hash function Curl employed in the cryptocurrency IOTA makes use of ternary S-boxes and is vulnerable to differential cryptanalysis.
- The IOTA foundation substituted it by the new ternary hash function Troika in collaboration with Cybercrypt (Bogdanov et al.) and initiated a crypto challenge over 200.000 €.
- The foundation is currently developing new computer chips built around base-3 logic (`https://cryptobriefing.com/iota-new-hash-function/`).
- In this context research on bijective power mappings with low uniformity over $\mathbb{F}_{3^n}$ is of particular interest as they can be also employed in S-boxes for SPN- and streamciphers.
- Planar functions cannot be bijective. Thus mappings of uniformity ≥ 2 are of interest (see also AES).

☞As $p = 3$ is of interest other primes will follow(?).

We contribute to this development and prove

Theorem 1: Bijective Power Mapping over $\mathbb{F}_{3^n}, n$ odd with Low Uniformity

1. The family $x^{d'_n}, d'_n = \frac{3^n-1}{2} + 3^{\frac{n+1}{2}} - 1$ over $\mathbb{F}_{3^n}, n$ odd is bijective.
2. The inverse is x^{d_n}, where
$$d_n = \begin{cases} \frac{3^{\frac{n+1}{2}}+1}{2}, n \equiv 3 \bmod 4 \\ \frac{3^n-1}{2} + \frac{3^{\frac{n+1}{2}}+1}{2}, n \equiv 1 \bmod 4. \end{cases}$$
3. It is $\mathcal{U}_{d_n} = \mathcal{U}_{d'_n} = 4$ for $n > 1$.

This explains the following entries in the H-R-S tables

p^n	d	uniformity
3^5	49	4
3^7	391	4
3^5	5	4
3^7	41	4

- d is min $\{d \cdot 3^i \bmod (3^n - 1) | 0 \leq i \leq n-1\}$.
- The first two entries are new and result from $x^{d'_n}$.
- The last two entries are explained by x^{d_n} which was discovered by Felke in 2006.

This explains the following entries in the H-R-S tables

p^n	d	uniformity
3^5	49	4
3^7	391	4
3^5	5	4
3^7	41	4

- d is min $\{d \cdot 3^i \bmod (3^n - 1) | 0 \leq i \leq n-1\}$.
- The first two entries are new and result from $x^{d'_n}$.
- The last two entries are explained by x^{d_n} which was discovered by Felke in 2006.
- Theorem 1 can be proven by the multivariate method which will be shown later.
- It is enough to compute the uniformity for one of these families, e.g. by the result of Dempwolff.

Theorem 2

Let $x^{d_n}, d_n = \frac{p^n-1}{2} + p^{\frac{n+1}{2}} + 1$ be a power function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^n}$, p an odd prime and n odd. Then

1. $\mathcal{U}_{d_n} \leq 3, p \equiv 1 \mod 4,$
2. $\mathcal{U}_{d_n} = 3, p = 3, n = 1,$
3. $\mathcal{U}_{d_n} \in \{2, 4, 6\}$ else.

.

- Theorem 2 is a generalization of the power mapping $x^{d_n}, d_n = \frac{5^n-1}{2} + 5^{\frac{n+1}{2}} + 1, n$ odd with $\mathcal{U}_{d_n} = 3$ (Felke 2006).
- The bound in 1 is still tight if we exclude $p = 5$ as it is e.g. assumed over $\mathbb{F}_{13}$.
- The set in 3 cannot be narrowed in this general setting and theorem 2 covers some open entries in the H-R-S tables (next table).

p	n	d	uniformity	H-R-S entry
7	1	5	4	no H-R-S table
7	3	179	4	open H-R-S entry
7	5	8453	6	no H-R-S table
7	7	412115	6	no H-R-S table
11	1	7	2	no H-R-S table
11	3	677	4	open H-R-S entry
11	5	80647	6	no H-R-S table

- Again d is min $\{d \cdot p^i \bmod (p^n - 1) | 0 \leq i \leq n - 1\}$.

p	n	d	uniformity	H-R-S entry
7	1	5	4	no H-R-S table
7	3	179	4	open H-R-S entry
7	5	8453	6	no H-R-S table
7	7	412115	6	no H-R-S table
11	1	7	2	no H-R-S table
11	3	677	4	open H-R-S entry
11	5	80647	6	no H-R-S table

- Again d is min $\{d \cdot p^i \bmod (p^n - 1) | 0 \leq i \leq n-1\}$.
- No known family shares the difference properties given in the theorem. Therefore this family is new and not CCZ-equivalent to known ones.
- Theorem 2 can be proven as well by the above mentioned multivariate method.

The Differential Uniformity

Equivalence Relations

Mappings over Fields of odd Characteristic in Cryptography

The Multivariate Method

Conclusion & Open Problems

The Multivariate Method (Dobbertin, Felke)

Problem: Many proofs dealing with k-uniform mappings make use of a „rabbit out of the hat“.

- The multivariate method aims to give systematic approach to compute the uniformity of certain families of mappings over $\mathbb{F}_{p^n}$.

  ☞The uniformity deals with the formal derivative. In analogy to calculus standard techniques to study the derivative for certain families of power mappings and to compute the uniformity are developed.

The Multivariate Method (Dobbertin, Felke)

Problem: Many proofs dealing with k-uniform mappings make use of a „rabbit out of the hat“.

- The multivariate method aims to give systematic approach to compute the uniformity of certain families of mappings over $\mathbb{F}_{p^n}$.

  ☞The uniformity deals with the formal derivative. In analogy to calculus standard techniques to study the derivative for certain families of power mappings and to compute the uniformity are developed.
- The proofs presented here give such standard techniques when a certain resultant can be resolved by certain radicals and linearized polynomials.

The Multivariate Method (Dobbertin, Felke)

Problem: Many proofs dealing with k-uniform mappings make use of a „rabbit out of the hat“.

- The multivariate method aims to give systematic approach to compute the uniformity of certain families of mappings over $\mathbb{F}_{p^n}$.

  ☞The uniformity deals with the formal derivative. In analogy to calculus standard techniques to study the derivative for certain families of power mappings and to compute the uniformity are developed.
- The proofs presented here give such standard techniques when a certain resultant can be resolved by certain radicals and linearized polynomials.
- These techniques are applicable to many families with low uniformity found in the past, e.g. $x^{\frac{5^{\frac{n+1}{2}}+1}{2}}$, n odd (inverse of a already proven conjecture by Dobbertin et al.)

From now on we consider $\mathbb{F}_{p^n}$ with n odd.

From now on we consider $\mathbb{F}_{p^n}$ with n odd.

Theorem and Definition

- The conjugation $x^{p^{\frac{n+1}{2}}}$ is denoted by x^*. It is $x^{**} = x^p$.

From now on we consider $\mathbb{F}_{p^n}$ with n odd.

Theorem and Definition

- The conjugation $x^{p^{\frac{n+1}{2}}}$ is denoted by x^*. It is $x^{**} = x^p$.
- The quadratic character $x \mapsto x^{\frac{p^n-1}{2}}, x \in \mathbb{F}_{p^n}$ is denoted by $\chi_{p,n}(x)$. We skip p, when it is clear.

From now on we consider $\mathbb{F}_{p^n}$ with n odd.

Theorem and Definition

- The conjugation $x^{p^{\frac{n+1}{2}}}$ is denoted by x^*. It is $x^{**} = x^p$.
- The quadratic character $x \mapsto x^{\frac{p^n-1}{2}}, x \in \mathbb{F}_{p^n}$ is denoted by $\chi_{p,n}(x)$. We skip p, when it is clear.
  - It is $\chi_{p,n}(\alpha) = 1$ iff $\alpha = r^2, r \in \mathbb{F}^*_{p^n}$.
  - It is $\chi_{p,n}(-1) = 1$ iff $\frac{p^n-1}{2}$ is even.
  - As n is odd it is $\chi_{p,n}(-1) = 1$ iff $p \equiv 1$ mod 4.

From now on we consider $\mathbb{F}_{p^n}$ with n odd.

Theorem and Definition

- The conjugation $x^{p^{\frac{n+1}{2}}}$ is denoted by x^*. It is $x^{**} = x^p$.
- The quadratic character $x \mapsto x^{\frac{p^n-1}{2}}, x \in \mathbb{F}_{p^n}$ is denoted by $\chi_{p,n}(x)$. We skip p, when it is clear.
  - It is $\chi_{p,n}(\alpha) = 1$ iff $\alpha = r^2, r \in \mathbb{F}^*_{p^n}$.
  - It is $\chi_{p,n}(-1) = 1$ iff $\frac{p^n-1}{2}$ is even.
  - As n is odd it is $\chi_{p,n}(-1) = 1$ iff $p \equiv 1$ mod 4.
- For $\alpha \in \mathbb{F}_{p^n}$ we define $\sqrt{\alpha} := r \in \mathbb{F}_{p^{n'}}$, where $\alpha = r^2$ and $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^{n'}}$ is smallest field extension containing r.
  If $p \equiv 3 \bmod 4$ and $r \in \mathbb{F}_{p^n}$ we set $\sqrt{\alpha} := r$, where r is s.t. $\chi(r) = 1$.
  This way the root becomes unique.

From now on we consider $\mathbb{F}_{p^n}$ with n odd.

Theorem and Definition

- The conjugation $x^{p^{\frac{n+1}{2}}}$ is denoted by x^*. It is $x^{**} = x^p$.
- The quadratic character $x \mapsto x^{\frac{p^n-1}{2}}, x \in \mathbb{F}_{p^n}$ is denoted by $\chi_{p,n}(x)$. We skip p, when it is clear.
  - It is $\chi_{p,n}(\alpha) = 1$ iff $\alpha = r^2, r \in \mathbb{F}^*_{p^n}$.
  - It is $\chi_{p,n}(-1) = 1$ iff $\frac{p^n-1}{2}$ is even.
  - As n is odd it is $\chi_{p,n}(-1) = 1$ iff $p \equiv 1$ mod 4.
- For $\alpha \in \mathbb{F}_{p^n}$ we define $\sqrt{\alpha} := r \in \mathbb{F}_{p^{n'}}$, where $\alpha = r^2$ and $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^{n'}}$ is smallest field extension containing r.
  If $p \equiv 3 \bmod 4$ and $r \in \mathbb{F}_{p^n}$ we set $\sqrt{\alpha} := r$, where r is s.t. $\chi(r) = 1$.
  This way the root becomes unique.
- It is $\sqrt{\alpha\alpha^*}^* = \sqrt{\alpha^p\alpha^*} = \chi(\alpha^{\frac{p-1}{2}})\alpha^{\frac{p-1}{2}}\sqrt{\alpha\alpha^*} \in \mathbb{F}_{p^n}$ for $p \equiv 3 \bmod 4$.

We will now prove

Theorem 1: Bijective Power Mapping over $\mathbb{F}_{3^n}, n$ odd with Low Uniformity

1. The family $x^{d'_n}, d'_n = \frac{3^n-1}{2} + 3^{\frac{n+1}{2}} - 1$ over $\mathbb{F}_{3^n}, n$ odd is bijective.
2. The inverse is x^{d_n}, where
$$d_n = \begin{cases} \frac{3^{\frac{n+1}{2}}+1}{2}, n \equiv 3 \bmod 4 \\ \frac{3^n-1}{2} + \frac{3^{\frac{n+1}{2}}+1}{2}, n \equiv 1 \bmod 4. \end{cases}$$
3. It is $\mathcal{U}_{d_n} = \mathcal{U}_{d'_n} = 4$ for $n > 1$.

We start to prove $\mathcal{U}_{d_n} = 4$ with the multivariate method.

Step 1:Transform $\Delta_{d_n}(x - \frac{1}{2}) = a$ into a System of Multivariate Equations

- Set $y := x^* = x^{3^{\frac{n+1}{2}}}$ then $x^{d_n} = \chi_n(x)\sqrt{yx}$.
- The equation $\Delta_{d_n}(x - \frac{1}{2}) = a$ has the multivariate representation: $\chi_n(x-1)\sqrt{(y-1)(x-1)} - \chi_n(x+1)\sqrt{(y+1)(x+1)} = a$ and it is $\Delta_{d_n}(x-1) = \Delta_{d_n}(-x-1)$.
- We get by successive squaring and conjugation with * the system

$$\begin{array}{rcl} F_1 : x^2 - (a^2+1)xy + y^2 + a^4 - a^2 & = & 0 \\ F_2 : y^2 - (b^2+1)x^3y + x^6 + b^4 - b^2 & = & 0. \end{array}$$

Step 2: Compute the Resultant and Factorize it

This gives

$$\begin{aligned}\phi_1(x) &:= x^2 + abx + a^2 + b^2 - 1\\ \phi_2(x) &:= x^2 - abx + a^2 + b^2 - 1\\ \phi_3(x) &:= x^4 + (ab-1)x^2 + a^2 + ab + b^2\\ \phi_4(x) &:= x^4 - (ab+1)x^2 + a^2 - ab + b^2.\end{aligned}$$

Step 3: Determine the symbolic Roots and finally the Solutions of $\Delta_{d_n}(x-\frac{1}{2})=a$

The polynomials split over $\mathbb{F}_{p^{n'}}, n'=n$ or $2n$ as listed below

$$\phi_1(x) = \left(x - ab - \sqrt{(a^2-1)(b^2-1)}\right)\left(x - ab + \sqrt{(a^2-1)(b^2-1)}\right)$$
$$\phi_2(x) = \left(x + ab + \sqrt{(a^2-1)(b^2-1)}\right)\left(x + ab - \sqrt{(a^2-1)(b^2-1)}\right)$$
$$\phi_3(x) = \left(x - \sqrt{ab - 1 + \sqrt{(a^2-1)(b^2-1)}}\right)\cdot\ldots$$
$$\phi_4(x) = \left(x - \sqrt{-ab - 1 + \sqrt{(a^2-1)(b^2-1)}}\right)\cdot\ldots$$

Step 3: Determine the symbolic Roots and finally the Solutions of $\Delta_{d_n}(x - \frac{1}{2}) = a$

The polynomials split over $\mathbb{F}_{p^{n'}}, n' = n$ or $2n$ as listed below

$$\phi_1(x) = \left(x - ab - \sqrt{(a^2-1)(b^2-1)}\right)\left(x - ab + \sqrt{(a^2-1)(b^2-1)}\right)$$

$$\phi_2(x) = \left(x + ab + \sqrt{(a^2-1)(b^2-1)}\right)\left(x + ab - \sqrt{(a^2-1)(b^2-1)}\right)$$

$$\phi_3(x) = \left(x - \sqrt{ab - 1 + \sqrt{(a^2-1)(b^2-1)}}\right) \cdot \ldots$$

$$\phi_4(x) = \left(x - \sqrt{-ab - 1 + \sqrt{(a^2-1)(b^2-1)}}\right) \cdot \ldots$$

- The next step is to determine which of these roots yield solutions of $\Delta_{d_n}(x - \frac{1}{2}) = a$.

Step 3: Determine the symbolic Roots and finally the Solutions of $\Delta_{d_n}(x - \frac{1}{2}) = a$

The polynomials split over $\mathbb{F}_{p^{n'}}, n' = n$ or $2n$ as listed below

$$
\begin{aligned}
\phi_1(x) &= \left(x - ab - \sqrt{(a^2-1)(b^2-1)}\right)\left(x - ab + \sqrt{(a^2-1)(b^2-1)}\right) \\
\phi_2(x) &= \left(x + ab + \sqrt{(a^2-1)(b^2-1)}\right)\left(x + ab - \sqrt{(a^2-1)(b^2-1)}\right) \\
\phi_3(x) &= \left(x - \sqrt{ab - 1 + \sqrt{(a^2-1)(b^2-1)}}\right)\cdot \ldots \\
\phi_4(x) &= \left(x - \sqrt{-ab - 1 + \sqrt{(a^2-1)(b^2-1)}}\right)\cdot \ldots
\end{aligned}
$$

- The next step is to determine which of these roots yield solutions of $\Delta_{d_n}(x - \frac{1}{2}) = a$.

  ☞Step 3 is crucial. In analogy to treating derivatives in calculus we will show that this step yields to a standard technique by using . . .

Rational Parameterizations

- The elements $\chi_n(\alpha) = \pm 1, \chi_n(\alpha - 1) = \pm 1, \alpha, \alpha - 1 \in \mathbb{F}_{3^n}^*$ can be parameterized by rational parameterizations.

...

Rational Parameterizations

- The elements $\chi_n(\alpha) = \pm 1, \chi_n(\alpha - 1) = \pm 1, \alpha, \alpha - 1 \in \mathbb{F}_{3^n}^*$ can be parameterized by rational parameterizations.
- E.g. since n is odd we have $\chi_n(-1) = -1$ and the elements $\chi_n(\alpha) = \chi_n(\alpha - 1) = 1$ can be parametrized by $\alpha = \left(u + \frac{1}{u}\right)^2, u \in \mathbb{F}_{3^n} \setminus \{0, \pm 1\}$.
  The parameterization maps 4-to-1 and is in 1 to 1 correspondence with the cyclotomic numbers.

...

Rational Parameterizations

- The elements $\chi_n(\alpha) = \pm 1, \chi_n(\alpha - 1) = \pm 1, \alpha, \alpha - 1 \in \mathbb{F}_{3^n}^*$ can be parameterized by rational parameterizations.
- E.g. since n is odd we have $\chi_n(-1) = -1$ and the elements $\chi_n(\alpha) = \chi_n(\alpha - 1) = 1$ can be parametrized by $\alpha = \left(u + \frac{1}{u}\right)^2, u \in \mathbb{F}_{3^n} \setminus \{0, \pm 1\}$. The parameterization maps 4-to-1 and is in 1 to 1 correspondence with the cyclotomic numbers.

and

Weil estimate (quadratic case over $\mathbb{F}_{3^n}$)

Let $f(x) \in \mathbb{F}_{3^n}[x]$ be a quadratic polynomial with 2 distinct zeros in its splitting field then it is $\left|\sum_{\alpha \in \mathbb{F}_{3^n}} \chi_n(f(\alpha))\right| \leq 1$.

Exemplary we treat the zeros of ϕ_1, ϕ_2

- The radicals in ϕ_1, ϕ_2 are of the form $\sqrt{(a^2-1)(b^2-1)}$ and it is $\phi_1(-x) = \phi_2(x)$.
- Since our mapping is of the form $\chi(x)\sqrt{yx}$ it is $\Delta_{d_n}(-x) = \Delta_{d_n}(x)$.
- Obviously the conjugation $\sqrt{(a^2-1)(b^2-1)}^* = \chi_n(a^2-1)(a^2-1)\sqrt{(a^2-1)(b^2-1)}$ plays a crucial role.
- This leads to the case distinction $\chi_n(a^2-1) = \pm 1$ and it is sufficient to consider ϕ_1.

Case 1: $\chi_n(a^2-1)=1, a \notin \mathbb{F}_3$
Then a can be paramterized by $u+\frac{1}{u}$ and $\Delta_{d_n}(x-1)=a$ becomes equal to
$\chi_n(x-1)\sqrt{(y-1)(x-1)}-\chi_n(x+1)\sqrt{(y+1)(x+1)}=u+\frac{1}{u}.$

Case 1: $\chi_n(a^2-1)=1, a \notin \mathbb{F}_3$

Then a can be paramterized by $u+\frac{1}{u}$ and $\Delta_{d_n}(x-1)=a$ becomes equal to

$$\chi_n(x-1)\sqrt{(y-1)(x-1)} - \chi_n(x+1)\sqrt{(y+1)(x+1)} = u+\frac{1}{u}.$$

- With the above substitution $\phi_1(x) \quad = \quad (x+\frac{u}{u^*}+\frac{u^*}{u})(x+uu^*+\frac{1}{uu^*})$ splits over $\mathbb{F}_3(u,u^*) \subset \mathbb{F}_{3^n}$.

Case 1: $\chi_n(a^2-1)=1, a \notin \mathbb{F}_3$
Then a can be paramterized by $u+\frac{1}{u}$ and $\Delta_{d_n}(x-1)=a$ becomes equal to
$\chi_n(x-1)\sqrt{(y-1)(x-1)} - \chi_n(x+1)\sqrt{(y+1)(x+1)} = u+\frac{1}{u}$.

- With the above substitution $\phi_1(x) = (x+\frac{u}{u^*}+\frac{u^*}{u})(x+uu^*+\frac{1}{uu^*})$ splits over $\mathbb{F}_3(u,u^*) \subset \mathbb{F}_{3^n}$.
- These zeros are plugged into $\Delta_{d_n}(x-1)=u+\frac{1}{u}$ giving rational expresssions in $R(u,u^*)$ depending on $\chi_n(u)$, e.g. for $\chi_n(u)=-1$ we get

$$\begin{aligned} \chi_n(x-1)\sqrt{(x-1)(y-1)} &= \frac{(u-u^*)(u^*-u^3)}{u^2u^*} \\ \chi_n(x+1)\sqrt{(x+1)(y+1)} &= \frac{(u+u^*)(u^3+u^*)}{u^2u^*}. \end{aligned}$$

Case 1: $\chi_n(a^2-1)=1, a \notin \mathbb{F}_3$
Then a can be paramterized by $u+\frac{1}{u}$ and $\Delta_{d_n}(x-1)=a$ becomes equal to
$\chi_n(x-1)\sqrt{(y-1)(x-1)} - \chi_n(x+1)\sqrt{(y+1)(x+1)} = u+\frac{1}{u}$.

- With the above substitution $\phi_1(x) = (x+\frac{u}{u^*}+\frac{u^*}{u})(x+uu^*+\frac{1}{uu^*})$ splits over $\mathbb{F}_3(u,u^*) \subset \mathbb{F}_{3^n}$.
- These zeros are plugged into $\Delta_{d_n}(x-1)=u+\frac{1}{u}$ giving rational expresssions in $R(u,u^*)$ depending on $\chi_n(u)$, e.g. for $\chi_n(u)=-1$ we get

$$\begin{aligned} \chi_n(x-1)\sqrt{(x-1)(y-1)} &= \frac{(u-u^*)(u^*-u^3)}{u^2u^*} \\ \chi_n(x+1)\sqrt{(x+1)(y+1)} &= \frac{(u+u^*)(u^3+u^*)}{u^2u^*}. \end{aligned}$$

  We skip the remaining technical but simple details here.
- Analogously we treat the case $\chi_n(a^2-1)=1$.

This yields the following proposition.

Proposition 1

- $\Delta_d(x-1) = a, a \notin \mathbb{F}_{3^3}$ has exactly two solutions from ϕ_1, ϕ_2 iff $\chi_n(a^2-1) = 1$ and $\chi_n(u) = -1$, where u is such that $a = u + \frac{1}{u}$.
  Such u exists for $n > 3$ and in this case the solutions are given by $\pm\left(uu^* + \frac{1}{uu^*}\right)$
- In all other cases it has no solutions from ϕ_1 and ϕ_2.

- The polynomials ϕ_3, ϕ_4 are treated in the same way by successively applying again the rational parametrizations for elements of the form $\chi(\alpha) = \pm 1, \chi_n(\alpha - 1) = \pm 1, \alpha \in \mathbb{F}_{3^n}$.
- We get

Proposition 2

Given $a \notin \mathbb{F}_{3^9}$, then ϕ_3 and ϕ_4 contribute solutions only if $\chi_n(a^2-1) = -1$ (in opposite to proposition 1).

- It is $\#\Delta_{d_n}^{-1}(a) = 4$ iff a can be parameterized by $-\frac{(s^2+1)(s^2+s-1)}{(s^2-s-1)^2}$ with $\chi_n(s^2-s-1) = -1$.
- In all other cases ϕ_3, ϕ_4 contribute no solutions.

- From the Weil estimate we get that such an a or s exists respectively .
- The exceptional cases $\mathbb{F}_3, \mathbb{F}_{3^3}, \mathbb{F}_{3^9}$ can be inspected easily „by hand“.
- Combining this with proposition 1 yields x^{d_n} is 4-uniform for $\mathbb{F}_{3^n}, n > 1$.

To complete the proof of theorem 1 we have to show that $x^{d'_n} = x^{\frac{3^n-1}{2}+3^{\frac{n+1}{2}}-1}$ is the inverse of x^{d_n}.

Sketch of Proof.

$n \equiv 3 \bmod 4:$

$$\begin{aligned}
x^{d_n \cdot d'_n} &= x^{\left(\frac{3^{\frac{n+1}{2}}+1}{2}\right)\left(\frac{3^n-1}{2}+3^{\frac{n+1}{2}}-1\right)} \\
&= x^{1+\left(\frac{3^n-1}{2}\right)\left(\frac{3^n-1}{2}\right)} \\
&= x
\end{aligned}$$

□

Proof of Theorem 2

Recall

Theorem 2

Let $x^{d_n}, d_n = \frac{p^n-1}{2} + p^{\frac{n+1}{2}} + 1$ be a power function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^n}$, p an odd prime and n odd. Then

1. $\mathcal{U}_{d_n} = 3, p = 3, n = 1$,
2. $\mathcal{U}_{d_n} = 3, p \equiv 1 \bmod 4$,
3. $\mathcal{U}_{d_n} \in \{2, 4, 6\}$ else.

Step 1: Describe $\Delta_{d_n}(x-\frac{1}{2})=a$ as a System of Multivariate Equations

It is $x^{d_n}=\chi_n(x)yx$, where $y=x^*, x^{**}=x^p$.

Thus by setting $b=a^*$

$$F_1:\chi_n\left(x+\tfrac{1}{2}\right)\left(y+\tfrac{1}{2}\right)\left(x+\tfrac{1}{2}\right)-\chi_n\left(x-\tfrac{1}{2}\right)\left(y-\tfrac{1}{2}\right)\left(x-\tfrac{1}{2}\right)=a$$
$$F_2:\chi_n\left(x+\tfrac{1}{2}\right)\left(y+\tfrac{1}{2}\right)\left(x^p+\tfrac{1}{2}\right)-\chi_n\left(x-\tfrac{1}{2}\right)\left(y-\tfrac{1}{2}\right)\left(x^p-\tfrac{1}{2}\right)=b.$$

Case distinction according to the values of χ_n gives:

Case 1: $\chi(x-\frac{1}{2})=1, \chi(x+\frac{1}{2})=1$

$$\begin{aligned} F_{11} &: & x+y-a &= 0 \\ F_{12} &: & x^p+y-b &= 0 \end{aligned}$$

Case 2: $\chi(x-\frac{1}{2})=-1, \chi(x+\frac{1}{2})=1$

$$\begin{aligned} F_{21} &: & xy-\frac{1}{2}a+\frac{1}{4} &= 0 \\ F_{22} &: & x^py-\frac{1}{2}b+\frac{1}{4} &= 0 \end{aligned}$$

Case 3: $\chi(x-\frac{1}{2})=1, \chi(x+\frac{1}{2})=-1$

$$\begin{aligned} F_{31} &: & xy+\frac{1}{2}a+\frac{1}{4} &= 0 \\ F_{32} &: & x^py+\frac{1}{2}b+\frac{1}{4} &= 0 \end{aligned}$$

Case 4: $\chi(x-\frac{1}{2})=-1, \chi(x+\frac{1}{2})=-1$

$$\begin{aligned} F_{41} &: & x+y+a &= 0 \\ F_{42} &: & x^p+y+b &= 0. \end{aligned}$$

The above case distinction does not capture the 2 cases $a=\pm 1$.

☞Simple exception handling.

Step 2: Compute the Resultants and Factorize it

This gives the following resultants:

Case 1: $\chi(x-\frac{1}{2}) = 1, \chi(x+\frac{1}{2}) = 1$

$\phi_1(x) := x^p - x + a - b$

Case 2: $\chi(x-\frac{1}{2}) = -1, \chi(x+\frac{1}{2}) = 1$

$\phi_2(x) := x\left(x^{p-1} - \frac{b-\frac{1}{2}}{a-\frac{1}{2}}\right)$

Case 3: $\chi(x-\frac{1}{2}) = 1, \chi(x+\frac{1}{2}) = -1$

$\phi_3(x) := x\left(x^{p-1} - \frac{b+\frac{1}{2}}{a+\frac{1}{2}}\right)$

Case 4: $\chi(x-\frac{1}{2}) = -1, \chi(x+\frac{1}{2}) = -1$

$\phi_4(x) := x^p - x - a + b$

Step 2: Compute the symbolic Roots and finally the Solutions of $\Delta_{d_n}(x - \frac{1}{2}) = a$

$$\phi_1(x) = (x-\alpha)\,(x-\alpha-1)\ldots(x-\alpha-p-1)$$
$$\phi_4(x) = (x+\alpha)\,(x+\alpha+1)\ldots(x+\alpha+p-1)$$

over $\mathbb{F}_{p^n}$ by the famous Hilbert 90.

Step 2: Compute the symbolic Roots and finally the Solutions of $\Delta_{d_n}(x - \frac{1}{2}) = a$

$$\phi_1(x) = (x - \alpha)\,(x - \alpha - 1)\ldots(x - \alpha - p - 1)$$
$$\phi_4(x) = (x + \alpha)\,(x + \alpha + 1)\ldots(x + \alpha + p - 1)$$

over $\mathbb{F}_{p^n}$ by the famous Hilbert 90.

It is $p^{\frac{n+1}{2}} - 1$ always divisible by $p - 1$ and therefore

$\phi_2(x) =$

$x\left(x - \omega^0(a - \frac{1}{2})^{\frac{p^{\frac{n+1}{2}}-1}{p-1}}\right)\ldots\left(x - \omega^{p-2}(a - \frac{1}{2})^{\frac{p^{\frac{n+1}{2}}-1}{p-1}}\right)$ and

$\phi_3(x) =$

$x\left(x - \omega^0(a + \frac{1}{2})^{\frac{p^{\frac{n+1}{2}}-1}{p-1}}\right)\ldots\left(x - \omega^{p-2}(a + \frac{1}{2})^{\frac{p^{\frac{n+1}{2}}-1}{p-1}}\right)$, $\omega \in \mathbb{F}_p$

a $p - 1$-th root of unity.

☞Step 3 yields again in analogy to calculus standard techniques to treat the radicals and the linear polynomials ϕ_1, ϕ_2 occuring in many situation when applying this method.

The Contribution of ϕ_1, ϕ_4

- It is $\phi_1(x) = 0$ iff $\phi_4(-x) = 0$.
- It is $\chi(-x - \frac{1}{2}) = \chi(-1)\chi(x + \frac{1}{2})$ and $\chi(-x + \frac{1}{2}) = \chi(-1)\chi(x - \frac{1}{2})$.
  - If $p \equiv 3 \mod 4$ then a zero $\alpha + \beta_i, \beta_i \in \mathbb{F}_p$ of ϕ_1 yields a solution of equation F_{11} iff $-(\alpha + \beta_i)$ extends to a solution of equation F_{41}.
  - If $p \equiv 1 \mod 4$ then either ϕ_1 or ϕ_4 contribute a solution.

- ϕ_1 contributes at most 1 suitable solution. Assume the contrary. Then $\alpha + \beta_i + \alpha^* + \beta_i^* = 0$
  and
  $\alpha + \beta_j + \alpha^* + \beta_j^* = 0, \beta_i \in \mathbb{F}_p$.
- Subtracting both equations gives $\beta_i - \beta_j + (\beta_i - \beta_j)^* = 0$.
  As $\beta_i - \beta_j \in \mathbb{F}_p$ it is $(\beta_i - \beta_j)^* = (\beta_i - \beta_j)$.
  Consequently $\beta_i - \beta_j + (\beta_i - \beta_j)^* = 2(\beta_i - \beta_j) = 0$. It follows $\beta_i = \beta_j$.

Thus ϕ_1 and ϕ_4 contribute either 0 or 1 solution when $p \equiv 1$ mod 4 and 0 or 2 solutions when $p \equiv 3$ mod 4 to F_1.

The contribution of ϕ_2 and ϕ_3

- It is $xy = x^2$ over $\mathbb{F}_p$ and therefore plugging $\omega^i(a - \frac{1}{2})^{\frac{p^{\frac{n+1}{2}}-1}{p-1}}$ into xy gives $\omega^{2i}(a - \frac{1}{2})^{1+\frac{p^n-1}{p-1}}, 0 \leq i \leq p-2.$
- It follows that the possible solutions of F_{21} are $\pm\omega^{i_n}(a - \frac{1}{2})^{\frac{p^{\frac{n+1}{2}}-1}{p-1}}$, where $\omega^{2i_n} = \frac{1}{2}(a - \frac{1}{2})^{-\frac{p^n-1}{p-1}} \in \mathbb{F}_p.$
Such an i_n exists iff $\chi_n\left(\frac{1}{2}\left(a - \frac{1}{2}\right)\right) = 1, a \neq \frac{1}{2}.$

In the same vein ϕ_3 is treated. We skip the details.

- Remember that $\chi(-x-\frac{1}{2})=\chi(-1)\chi(x+\frac{1}{2})$ and $\chi(-x+\frac{1}{2})=\chi(-1)\chi(x-\frac{1}{2})$.
- This gives that ϕ_2 and ϕ_3 contribute either 0 or 1 solution each when $p \equiv 1 \bmod 4$ and 0 or 2 solutions each when $p \equiv 3 \bmod 4$ to F_1.
- In total they contribute either at a most 2 or 4 solutions respectively.

Exception handling by using gives the corresponding theorem. The results are summed up in the following tables.

$p \equiv 1 \bmod 4$

	$\chi(x-\frac{1}{2})$	$\chi(x+\frac{1}{2})$	No. of solutions
Case 1	1	1	0 or 1
Case 2	-1	1	0 or 1
Case 3	1	-1	0 or 1
Case 4	1	1	0 or 1 (1 sol. if case 1 has 0 sol. and vice versa
Exceptions $a = \pm 1$	1/0	0/1	≤ 3
Exceptions $a = \pm\frac{1}{2}$			≤ 3

$p \equiv 3 \bmod 4$

	$\chi(x-\frac{1}{2})$	$\chi(x+\frac{1}{2})$	No. of solutions
Case 1	1	1	0 or 1
Case 2	-1	1	0 or 2
Case 3	1	-1	0 or 2
Case 4	1	1	0 or 1 (1 sol. iff case 1 has 1 sol.)
Exceptions $a = \pm 1$	1/0	0/1	≤ 5
Exceptions $a = \pm\frac{1}{2}$	0/1	1/0	≤ 6

$p \equiv 3 \bmod 4$

	$\chi(x-\frac{1}{2})$	$\chi(x+\frac{1}{2})$	No. of solutions
Case 1	1	1	0 or 1
Case 2	-1	1	0 or 2
Case 3	1	-1	0 or 2
Case 4	1	1	0 or 1 (1 sol. iff case 1 has 1 sol.)
Exceptions $a = \pm 1$	1/0	0/1	≤ 5
Exceptions $a = \pm\frac{1}{2}$	0/1	1/0	≤ 6

From this theorem 2 follows.
$\mathcal{U}_{d_n} = 3$ for $p = 3, n = 1$ is computed directly.

The Differential Uniformity

Equivalence Relations

Mappings over Fields of odd Characteristic in Cryptography

The Multivariate Method

Conclusion & Open Problems

Conclusion & Open Problems

Conclusion & Open Problems

- We introduced two families of power mappings of low uniformity in theorem 1 and 2. The family in theorem 1 is bijective over $\mathbb{F}_3$ and therefore of particular interest as a building block for cryptography over odd characteristic (Cryptocurrency IOTA).
  ☞Compute the crosscorrelation for this family.
  ☞Cryptanalysis based on quadratic characters.

Conclusion & Open Problems

- We introduced two families of power mappings of low uniformity in theorem 1 and 2. The family in theorem 1 is bijective over $\mathbb{F}_3$ and therefore of particular interest as a building block for cryptography over odd characteristic (Cryptocurrency IOTA).

  ☞Compute the crosscorrelation for this family.

  ☞Cryptanalysis based on quadratic characters.
- In analogy to calculus we gave standard techniques for the multivariate method, where the corresponding resultants can be resolved by certain radicals and linearized polynomials. This simplifies and unifies the proofs for many families (in opposite to „rabbit out of the hat").

Conclusion & Open Problems

- We introduced two families of power mappings of low uniformity in theorem 1 and 2. The family in theorem 1 is bijective over $\mathbb{F}_3$ and therefore of particular interest as a building block for cryptography over odd characteristic (Cryptocurrency IOTA).

  ☞Compute the crosscorrelation for this family.

  ☞Cryptanalysis based on quadratic characters.
- In analogy to calculus we gave standard techniques for the multivariate method, where the corresponding resultants can be resolved by certain radicals and linearized polynomials. This simplifies and unifies the proofs for many families (in opposite to „rabbit out of the hat“).
- Improve the bound of theorem 2 for concrete primes p, e.g. it is conjectured that $\mathcal{U}_{d_n} = 4$ for $d_n = \frac{3^n-1}{2} + 3^{\frac{n+1}{2}} + 1, n > 3$.

  ☞Could be doable with the multivariate method presented here as a basis.

  Work in progress and joint work is welcome.