Projective polynomials in cryptography

Faruk Göloğlu

University of Tartu

BFA Workshop, Rosendal
September 3, 2014

Projective polynomials

Projective polynomials

Projective polynomials are polynomials of type (Abhyankar-Cohen-Zieve 2000)

$$X^{2^k+1} + AX^{2^k} + BX + C$$

on $\mathbb{F}_{2^m}[X]$.

Applications in finite fields:

- Difference sets (Dillon-Dobbertin 2004, Dillon 2002)
- Cross-correlation of sequences (Dobbertin-Felke-Helleseth-Rosendahl 2006, Helleseth-Kholosha 2007)
- Error-correcting codes (Bracken-Helleseth)
- APN functions (Budaghyan-Carlet 2008)

In this talk:

- Discrete logarithm problem
- APN functions

The Discrete Logarithm Problem

In a cyclic group G, with given generator g, the DLP is the following problem:

DLP problem

Given $h \in G$, find i such that $h = g^i$.

In other words, find $\log_g(h)$.

Remark

The map g^i can be computed efficently (Square-and-Multiply) but (considered as) difficult to invert — one-way function*.*

In cryptography, the following groups are of interest:

1. The multiplicative group of a finite field $\mathbb{F}_q$
2. The group of $\mathbb{F}_q$-rational points on an elliptic curve, $E(\mathbb{F}_q)$
3. The Jacobian of a hyperelliptic curve over $\mathbb{F}_q$.

DLP in cryptography

- Key exchange: Diffie-Hellman
- Encryption: ElGamal
- Signature: Schnorr, ElGamal
- Homomorphic encryption: Pallier
- Pairing-based Cryptography: Joux

Generic algorithms:

- Baby Step/Giant Step
- Pohlig-Hellmann
- Pollard Rho

Principle of the Index Calculus Method

The computation of $\log_\alpha \beta$ in a group consists of three steps.

1. *Relation Generation.*

   Choose a subset S of the group, called factor base, and find multiplicative relations between factor base elements, which correspond to linear relations among their discrete logarithms.

2. *Linear Algebra.*

   After sufficiently many relations have been generated, obtain the DLP for all factor base elements by solving a linear system.

3. *Individual Logarithms.*

   Find an expression of the target element as a product of factor base elements, e.g., by a descent method.

Index calculus over a prime field $\mathbb{Z}_p$

The factor base S consists of the first t prime numbers. Relations are generated by computing $\alpha^k \bmod p$ and then using trial division to check whether this integer is a product of primes in S.

Example. Let $p = 229$. The element $\alpha = 6$ is a generator of $\mathbb{Z}_{229}$ of order $n = 228$. Choose factor base $S = \{2, 3, 5, 7, 11\}$.

Index calculus over a prime field $\mathbb{Z}_p$

The factor base S consists of the first t prime numbers. Relations are generated by computing $\alpha^k \bmod p$ and then using trial division to check whether this integer is a product of primes in S.

Example. Let $p = 229$. The element $\alpha = 6$ is a generator of $\mathbb{Z}_{229}$ of order $n = 228$. Choose factor base $S = \{2, 3, 5, 7, 11\}$.

1. The following relations are obtained:

$$\begin{aligned}
6^{100} \bmod 229 &= 180 = 2^2 \cdot 3^2 \cdot 5 \\
6^{18} \bmod 229 &= 176 = 2^4 \cdot 11 \\
6^{12} \bmod 229 &= 165 = 3 \cdot 5 \cdot 11 \\
6^{62} \bmod 229 &= 154 = 2 \cdot 7 \cdot 11 \\
6^{143} \bmod 229 &= 198 = 2 \cdot 3^2 \cdot 11 \\
6^{206} \bmod 229 &= 210 = 2 \cdot 3 \cdot 5 \cdot 7
\end{aligned}$$

Index calculus over a prime field $\mathbb{Z}_p$

The factor base S consists of the first t prime numbers. Relations are generated by computing $\alpha^k \bmod p$ and then using trial division to check whether this integer is a product of primes in S.

Example. Let $p = 229$. The element $\alpha = 6$ is a generator of $\mathbb{Z}_{229}$ of order $n = 228$. Choose factor base $S = \{2, 3, 5, 7, 11\}$.

1. The following relations are obtained:

$$\begin{aligned}
6^{100} \bmod 229 &= 180 = 2^2 \cdot 3^2 \cdot 5 \\
6^{18} \bmod 229 &= 176 = 2^4 \cdot 11 \\
6^{12} \bmod 229 &= 165 = 3 \cdot 5 \cdot 11 \\
6^{62} \bmod 229 &= 154 = 2 \cdot 7 \cdot 11 \\
6^{143} \bmod 229 &= 198 = 2 \cdot 3^2 \cdot 11 \\
6^{206} \bmod 229 &= 210 = 2 \cdot 3 \cdot 5 \cdot 7
\end{aligned}$$

Index calculus over a prime field $\mathbb{Z}_p$

The factor base S consists of the first t prime numbers. Relations are generated by computing $\alpha^k \bmod p$ and then using trial division to check whether this integer is a product of primes in S.

Example. Let $p = 229$. The element $\alpha = 6$ is a generator of $\mathbb{Z}_{229}$ of order $n = 228$. Choose factor base $S = \{2, 3, 5, 7, 11\}$.

1. These yield the following equations $\bmod 228$:

$$\begin{aligned}
100 &\equiv 2\log_6 2 + 2\log_6 3 + \log_6 5 \\
18 &\equiv 4\log_6 2 + \log_6 11 \\
12 &\equiv \log_6 3 + \log_6 5 + \log_6 11 \\
62 &\equiv \log_6 2 + \log_6 7 + \log_6 11 \\
143 &\equiv \log_6 2 + 2\log_6 3 + \log_6 11 \\
206 &\equiv \log_6 2 + \log_6 3 + \log_6 5 + \log_6 7
\end{aligned}$$

The factor base S consists of the first t prime numbers. Relations are generated by computing $\alpha^k \bmod p$ and then using trial division to check whether this integer is a product of primes in S.

Example. Let $p = 229$. The element $\alpha = 6$ is a generator of $\mathbb{Z}_{229}$ of order $n = 228$. Choose factor base $S = \{2, 3, 5, 7, 11\}$.

1. We can write this linear system in matrix form as:

$$\begin{bmatrix} 100 \\ 18 \\ 12 \\ 62 \\ 143 \\ 206 \end{bmatrix} = \begin{bmatrix} 2 & 2 & 1 & 0 & 0 \\ 4 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 \\ 1 & 2 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{bmatrix}.$$

2. Solving this linear system yields the solutions:
   $x_1 = \log_6 2 = 21$, $x_2 = \log_6 3 = 208$, $x_3 = \log_6 5 = 98$, $x_4 = \log_6 7 = 107$, and $x_5 = \log_6 11 = 162$.

3. Consider $\beta = 13$. Then $\log_6 13$ is computed as follows. We find for $k = 77$ that

$$\beta \cdot \alpha^k = 13 \cdot 6^{77} \mod 229 = 147 = 3 \cdot 7^2 ,$$

   hence it follows that

$$\begin{aligned} \log_6 13 &= (\log_6 3 + 2\log_6 7 - 77) \bmod 228 \\ &= (208 + 214 - 77) \bmod 228 = 117 . \end{aligned}$$

The Function Field Sieve (Joux-Lercier '06)

- In the FFS, we work on polynomials over $\mathbb{F}_q[X]$. Factor base is small degree (degree 1) polynomials.
- Choose $g_1, g_2 \in \mathbb{F}_q[X]$ of degrees $d_1, d_2 \approx \sqrt{n}$ such that $X - g_1(g_2(X))$ has a degree n irreducible factor $f(X)$ over $\mathbb{F}_q$, and represent $\mathbb{F}_{q^n}$ as $\mathbb{F}_{q^n} \cong \mathbb{F}_q(x) \cong \mathbb{F}_q[X]/\langle f(X) \rangle$. For $y := g_2(x)$ we then have $g_1(y) = x$.

The Function Field Sieve (Joux-Lercier '06)

- In the FFS, we work on polynomials over $\mathbb{F}_q[X]$. Factor base is small degree (degree 1) polynomials.
- Choose $g_1, g_2 \in \mathbb{F}_q[X]$ of degrees $d_1, d_2 \approx \sqrt{n}$ such that $X - g_1(g_2(X))$ has a degree n irreducible factor $f(X)$ over $\mathbb{F}_q$, and represent $\mathbb{F}_{q^n}$ as $\mathbb{F}_{q^n} \cong \mathbb{F}_q(x) \cong \mathbb{F}_q[X]/\langle f(X) \rangle$. For $y := g_2(x)$ we then have $g_1(y) = x$.
- We set the factor base as $S = \{x + a \mid a \in \mathbb{F}_q\} \cup \{y + b \mid b \in \mathbb{F}_q\}$.

The Function Field Sieve (Joux-Lercier '06)

- In the FFS, we work on polynomials over $\mathbb{F}_q[X]$. Factor base is small degree (degree 1) polynomials.
- Choose $g_1, g_2 \in \mathbb{F}_q[X]$ of degrees $d_1, d_2 \approx \sqrt{n}$ such that $X - g_1(g_2(X))$ has a degree n irreducible factor $f(X)$ over $\mathbb{F}_q$, and represent $\mathbb{F}_{q^n}$ as $\mathbb{F}_{q^n} \cong \mathbb{F}_q(x) \cong \mathbb{F}_q[X]/\langle f(X)\rangle$. For $y := g_2(x)$ we then have $g_1(y) = x$.
- We set the factor base as $S = \{x + a \mid a \in \mathbb{F}_q\} \cup \{y + b \mid b \in \mathbb{F}_q\}$.

Relation generation:

- We consider elements $xy + ay + bx + c$ for $a, b, c \in \mathbb{F}_q$ to obtain two expressions for an element of $\mathbb{F}_{q^n}$

$$xg_2(x) + ag_2(x) + bx + c = yg_1(y) + ay + bg_1(y) + c\ .$$

The Function Field Sieve (Joux-Lercier '06)

- If for some (a, b, c) triple, the corresponding polynomials

$$Xg_2(X) + ag_2(X) + bX + c, Yg_1(Y) + aY + bg_1(Y) + c$$

  both split, one obtains a relation by evaluating the polynomials at x and y respectively. That is,

$$\prod_i (x + \alpha_i) = \prod_j (y + \beta_j)$$

  gives us a relation.
- In the original Joux-Lercier approach, the probability of either polynomial

$$Xg_2(X) + ag_2(X) + bX + c, Yg_1(Y) + aY + bg_1(Y) + c \, .$$

  splitting is $1/(d_2 + 1)!$ and $1/(d_1 + 1)!$ respectively.
- Can we choose g_1, g_2 such that we can control the splitting behaviour?

Projective polynomials

- Let $q = 2^m$, $m = kk'$. Consider the family of polynomials

$$x^{2^k+1} + ax^{2^k} + bx + c.$$

- If $ab \neq c$ and $ba^{2^k} \neq b$, this may be transformed into

$$f_B(y) = y^{2^k+1} + By + B$$

via $x = \frac{ab+c}{a^{2^k}+b} y + a$.

Theorem (Bluher; Helleseth-Kholosha)

The number of elements $B \in \mathbb{F}_q^*$ such that the polynomial $f_B(x)$ splits completely over $\mathbb{F}_q$ equals

$$\frac{2^{m-k} - 1}{2^{2k} - 1} \quad \text{if } k' \text{ is odd}, \qquad \frac{2^{m-k} - 2^k}{2^{2k} - 1} \quad \text{if } k' \text{ is even}.$$

- Recall the polynomials

$$Xg_2(X) + ag_2(X) + bX + c,\ Yg_1(Y) + aY + bg_1(Y) + c\ .$$

- Choose $g_2(X) = X^{2^k}$

- Recall the polynomials

$$Xg_2(X) + ag_2(X) + bX + c, Yg_1(Y) + aY + bg_1(Y) + c \,.$$

- Choose $g_2(X) = X^{2^k}$
- LHS becomes

$$X^{2^k+1} + aX^{2^k} + bX + c$$

- LHS splits with a probability $1/2^{3k}$ which is much better then $1/(2^k + 1)!$.

- Recall the polynomials

$$Xg_2(X) + ag_2(X) + bX + c, Yg_1(Y) + aY + bg_1(Y) + c\ .$$

- Choose $g_2(X) = X^{2^k}$
- LHS becomes

$$X^{2^k+1} + aX^{2^k} + bX + c$$

- LHS splits with a probability $1/2^{3k}$ which is much better then $1/(2^k+1)!$.
- Of course choosing g_2 imposes a condition on g_1, but one can choose $2^k >> d_1$ making splitting probability very high.
- One can even get more greedy and choose $g_1(X) = \gamma X$ then RHS become quadratic and splits with probability $1/2!$.

Relation generation

- The irreducible factor then becomes $X^{2^k-1} + \gamma$, an example of a Kummer extension.
- Our setting: $k' = 3$ and $k = 8$. Therefore our field is: $\mathbb{F}_{2^{8 \cdot 3 \cdot 2^8 - 1}} = \mathbb{F}_{2^{6120}}$.
- This setting guarantees existence of splitting projective polynomials.
- Our method is the **first polynomial time relation generation method**. The relation generation was the bottleneck before.

Factor base preserving automorphisms

- The linear algebra step (we use Lanczos) requires matrix-vector multiplications $\mathbf{Ax}$ where $\mathbf{A}$ is an $|S| \times |S|$ matrix.
- The automorphisms which preserves the factor base helps us shrink the size of $\mathbf{A}$.
- Choice of $g_2(X) = X^{2^k}$ implies $y = x^{2^k}$ and

$$(y + b) = (x + b^{2^{-k}})^{2^k} \implies \log(y + b) = 2^k \log(x + b^{2^{-k}})$$

  which halves the factor base size.
- $\alpha \mapsto \alpha^q$ is another automorphism which preserves the factor base, shrinking A further, all thanks to properties of projective polynomials.

Other niceties implied by projective polynomials

- The matrix-vector multiplications normally is too expensive (lots of finite fields multiplications)
- A property of projective polynomials is that when they split, repeated roots have multiplicity powers of 2.
- This implies entries in A are all powers of 2.
- Therefore instead of field multiplications, we have “rotations”.

The descent

- Now, given a random polynomial in $\mathbb{F}_q[X]$ (e.g. an element in $\mathbb{F}_{q^n}$ whose logarithm is to be found) we use standard methods to represent it by a product of smaller degree polynomials, hence the descent – a recursive algorithm.
- For degree 2 elimination we try to equate a given quadratic polynomial

$$Q(x) = x^2 + A_1 x + A_0 = x^{2^k+1} + ax^{2^k} + bx + c$$

where RHS splits (again high probability).

- Since $x^{2^k-1} = \gamma$, RHS becomes

$$\gamma \left(x^2 + \left(a + \frac{b}{\gamma} \right) x + \frac{c}{\gamma} \right)$$

and using Bluher-parametrization we get

$$(a^{2^k} + \gamma a + \gamma A_1)^{2^k+1} + B(\gamma a^2 + \gamma A_1 a + \gamma A_0)^{2^k} = 0$$

which we solve via a Gröbner basis computation.

Algorithmic optimizations

- Matrix-Vector multiplication
  - Matrix of size 1000000×1000000, each entry 1000s of bits.
  - If entries are powers of 2 – shift instead of multiplication.
- GMP - GNU Multi-Precision Library
- Parallelization and Vectorization

Algorithmic optimizations

- Matrix-Vector multiplication
  - Matrix of size 1000000×1000000, each entry 1000s of bits.
  - If entries are powers of 2 – shift instead of multiplication.
- GMP - GNU Multi-Precision Library
- Parallelization and Vectorization
- Some algorithms *embarassingly parallel*
- Lanczos (finding a solution to a linear system) – parallelisation (not very good) depends on parameters
- OpenMP and MPI

Algorithmic optimizations

- Matrix-Vector multiplication
  - Matrix of size 1000000×1000000, each entry 1000s of bits.
  - If entries are powers of 2 – shift instead of multiplication.
- GMP - GNU Multi-Precision Library
- Parallelization and Vectorization
- Some algorithms *embarassingly parallel*
- Lanczos (finding a solution to a linear system) – parallelisation (not very good) depends on parameters
- OpenMP and MPI
- Registers up to 512 bits
- Vectorization means exploit the *length* of the registers

Solving the DLP in $\mathbb{F}_{2^{6120}}$

- Let $\mathbb{F}_{2^8} = \mathbb{F}_2[T]/ < T^8 + T^4 + T^3 + T + 1 >$,
- Let $\mathbb{F}_{2^{24}} = \mathbb{F}_{2^8}[W]/ < W^3 + t >$,
- Let $\mathbb{F}_{2^{6120}} = \mathbb{F}_{2^{24}}[X]/ < X^{255} + w + 1 >$.

We took as generator $\alpha = x + w$ and target

$$\beta_\pi = \sum_{i=0}^{254} \tau(\lfloor \pi q^{i+1} \rfloor \bmod q)\, x^i \, .$$

The computation took:

- 15 seconds for relation generation using Magma
- 60.5 core-hours for the parallelized C/GMP Lanczos implementation on four of the Intel (Westmere) Xeon E5650 hex-core processors ICHEC's SGI Altix ICE 8200EX Stokes cluster
- 689 core-hours for the descent, giving a total of 750 core-hours.

Solving the DLP in $\mathbb{F}_{2^{6120}}$

On 11/4/13 we announced that $\log_\alpha(\beta_\pi) =$

138587598363978692625475711283123171009236361503896992366495931704517700280127178022234894098617
581360131441835074256363730624426814293233474272521598166126957928116825443110965404253837938808
595404111035238027107772178822939281873403451999731815140073481766513715358449279314556797352446
246860317946750124475689474406274942356035936501674050933448909201029834522226732247771897083223
217282051573645013603613042367782716361877817938374393824313019073624786387618414037541681120284
044659383192907436852526392087724304775451631271825250968111451400502733404381769675255289127346
639350098221570844400380788516332496583882522436381918008200167032186350245107751346979596314696
153666716168951481948091060066730184766758137773944303875429830867205463918144256843911730747265
146154193438041627833661739775057161236346096236566875251277843062329973044475486561062204356908
568471471279383781038538818884463796989906076079843248127252020839705886436071213650575186707456
948584072378916942925369140868417196479573481032711481021729162865973588174096389913305607677858
033996361734905537150362024720515772660781208855505434331055766570014211875602940633575763850457
503079087074376585304470520411320246292255375711457573555286060236699317039454479326718281128961
423275142787569425690532833283344049635521302596000897192512036695298807294032964530959691377087
204546348960132760095544105980198255245493202412831593891984788152417957691939817112366182063687
529915365150361180214451234387656883256149355994405051149585969163075307026647956035683671589546
448539955132726112034938655961291856203422247680387029078473520951160334472525475071680672623661
587292720329606182512044312194357156139201340952037872975243254476081554937002122953415949407262
137232099852298394838422907643191397673290238344183046040975859915928536530445697145317668044973
7096483324156185041

World record progress:

bitlength	who/when	running time
127	Coppersmith 1984	N/A
...		
521	Joux-Lercier 2001	$>$ 3000 core hours
607	Thomé 2001	$>$ 800000 core hours
...		
923	Hayashi et al. 2010	$>$ 800000 core hours
1175	Joux Dec. 2012	$>$ 30000 core hours
1425	Joux Jan. 2013	$>$ 30000 core hours
1778	Joux 11/2/2013	215 core hours

World record progress:

bitlength	who/when	running time
127	Coppersmith 1984	N/A
...		
521	Joux-Lercier 2001	$>$ 3000 core hours
607	Thomé 2001	$>$ 800000 core hours
...		
923	Hayashi et al. 2010	$>$ 800000 core hours
1175	Joux Dec. 2012	$>$ 30000 core hours
1425	Joux Jan. 2013	$>$ 30000 core hours
1778	Joux 11/2/2013	215 core hours
1971	GGMZ 19/2/2013	3132 core hours

World record progress:

bitlength	who/when	running time
127	Coppersmith 1984	N/A
...		
521	Joux-Lercier 2001	$>$ 3000 core hours
607	Thomé 2001	$>$ 800000 core hours
...		
923	Hayashi et al. 2010	$>$ 800000 core hours
1175	Joux Dec. 2012	$>$ 30000 core hours
1425	Joux Jan. 2013	$>$ 30000 core hours
1778	Joux 11/2/2013	215 core hours
1971	GGMZ 19/2/2013	3132 core hours
4080	Joux 22/3/2013	14100 core hours

World record progress:

bitlength	who/when	running time
127	Coppersmith 1984	N/A
...		
521	Joux-Lercier 2001	$>$ 3000 core hours
607	Thomé 2001	$>$ 800000 core hours
...		
923	Hayashi et al. 2010	$>$ 800000 core hours
1175	Joux Dec. 2012	$>$ 30000 core hours
1425	Joux Jan. 2013	$>$ 30000 core hours
1778	Joux 11/2/2013	215 core hours
1971	GGMZ 19/2/2013	3132 core hours
4080	Joux 22/3/2013	14100 core hours
6120	GGMZ 11/4/2013	750 core hours

World record progress:

bitlength	who/when	running time
127	Coppersmith 1984	N/A
...		
521	Joux-Lercier 2001	$>$ 3000 core hours
607	Thomé 2001	$>$ 800000 core hours
...		
923	Hayashi et al. 2010	$>$ 800000 core hours
1175	Joux Dec. 2012	$>$ 30000 core hours
1425	Joux Jan. 2013	$>$ 30000 core hours
1778	Joux 11/2/2013	215 core hours
1971	GGMZ 19/2/2013	3132 core hours
4080	Joux 22/3/2013	14100 core hours
6120	GGMZ 11/4/2013	750 core hours
6168	Joux 21/5/2013	550 core hours (subgroup)

World record progress:

bitlength	who/when	running time
127	Coppersmith 1984	N/A
...		
521	Joux-Lercier 2001	$>$ 3000 core hours
607	Thomé 2001	$>$ 800000 core hours
...		
923	Hayashi et al. 2010	$>$ 800000 core hours
1175	Joux Dec. 2012	$>$ 30000 core hours
1425	Joux Jan. 2013	$>$ 30000 core hours
1778	Joux 11/2/2013	215 core hours
1971	GGMZ 19/2/2013	3132 core hours
4080	Joux 22/3/2013	14100 core hours
6120	GGMZ 11/4/2013	750 core hours
6168	Joux 21/5/2013	550 core hours (subgroup)
9234	GKZ 31/01/2014	400000 core hours

Theoretical breakthrough and open problems

Barbulescu, Gaudry, Joux and Thome 2014: A heuristic quasi-polynomial time algorithm. Theoretically much better than any previous algorithm for smalll characteristic fields.

Problem

What are the implications in medium prime case?

Problem

A heuristic-free algorithm for small characteristic.

APN functions

Let

- $n = 2m$, $q = 2^m$, $\mathbb{F} = \mathbb{F}_{q^2}$, $\mathbb{K} = \mathbb{F}_q$
- $\mathcal{P}_{q-1} = \{X^{q-1} \ : \ X \in \mathbb{F}\}$
- $\mathcal{T}_1 = \{X \in \mathbb{F} \ : \ X + X^q = 1\}$

Budaghyan and Carlet proved:

Theorem

Let $C \in \mathbb{F}$ and $A \in \mathbb{F} \setminus \mathbb{K}$. If

$$P_{C,k}(X) = X^{2^k+1} + CX^{2^k} + C^q X + 1 = 0$$

has no solutions $X \in \mathcal{P}_{q-1}$, then the polynomial

$$g_{C,k}(X) = X(X^{2^k} + X^q + CX^{2^k q}) + X^{2^k}(C^q X^q + AX^{2^k q}) + X^{(2^k+1)q}$$

is differentially $2^{\gcd(k,m)}$-uniform on $\mathbb{F}$. Thus, $g_{C,k}$ is APN if and only if $\gcd(k, m) = 1$.

When does $P_{C,k}$ have no solutions in $\mathcal{P}_{q-1}$

- Bracken, Tan and Tan (2014): constructed some elements C when $m \equiv 2$ or $4 \pmod 6$ such that P_{C_k} has no roots in $\mathcal{P}_{2^m-1}$ (in the $\gcd(m,k) = 1$ case).
- Qu, Tan and Li (2014): constructed some elements when $m \equiv 0 \pmod 6$ (in the $\gcd(m,k) = 1$ case).
- Bluher (2013): characterized those (m,k) pairs for which such a $P_{C,k}$ exists for any $\gcd(m,k)$.

A Trace-0/Trace-1 decomposition

Recall that

- $\mathcal{P}_{q-1} = \{X^{q-1} \ : \ X \in \mathbb{F}^*\}$
- $\mathcal{T}_1 = \{X \in \mathbb{F} \ : \ X + X^q = 1\}$

We have the following decompositions:

- Polar coordinate decomposition: Any $X \in \mathbb{F}^*$ can be written as $X = xu$ where $x \in \mathbb{K}$ and $u \in \mathcal{P}_{q-1}$.
- Trace-0/Trace-1 decomposition: Any $X \in \mathbb{F}^*$ can be written as $X = xg$ where $x \in \mathbb{K}$ and $g \in \mathcal{T}_1 \cup \{1\}$.

Observe that $xg = yh$ implies $\mathrm{Tr}_m^n(xg) = \mathrm{Tr}_m^n(yh)$ implies $x = y$ and $g = h$.
Notice that $\mathcal{P}_{q-1} = \{g^{q-1} \ : \ g \in \mathcal{T}_1 \cup \{1\}\}$.

Characterization of $P_{C,k}$

Let

$$\Gamma_k : \mathbb{K} \to \mathbb{K}$$
$$\Gamma_k : x \mapsto x^{2^k+1} + x.$$

Write

$$g^{(q-1)(2^k+1)} + Cg^{(q-1)2^k} + C^q g^{q-1} + 1$$

instead of

$$u^{2^k+1} + Cu^{2^k} + C^q u + 1$$

and after some steps you get

Theorem

Let $C \in \mathbb{F}$ and $1 \leq k < n$. The polynomial

$$P_{C,k}(X) = X^{2^k+1} + CX^{2^k} + C^q X + 1$$

has no solutions $X \in \mathcal{P}_{q-1}$ if and only if each of the three following conditions holds

- $k \neq m$,
- $C \notin \mathbb{K}$, *and*
- $$\frac{\mathrm{Tr}^n_m(h^3) + 1 + \frac{1}{b}}{\mathrm{Tr}^n_m(h^{2^k+1})^{2^{n-k}+1}} \notin \mathrm{Im}(\Gamma_k)$$

  where $C^q + 1 = bh$ with $b \in \mathbb{K}^*$ and $h \in \mathcal{T}_1 \setminus Z_{k,1}$.

- This is not **that** cumbersome.
- Equivalent to

$$\frac{1}{b} \neq A_h(y^{2^k+1} + y) + B_h.$$

- The image set of $\Gamma_k(y) = y^{2^k+1} + y$ is well-studied (Bluher 2007, Helleseth-Kholosha, Bracken-Tan-Tan 2014).
- Even the counts are given (HK), helping to prove:

Theorem

If $\gcd(k, m) = 1$ *(i.e.,* $g_{C,k}$ *is APN), then the number of elements* $C \in \mathbb{F}$ *for which the polynomial* $P_{C,k}(X)$ *has no solutions* $X \in \mathcal{P}_{q-1}$ *is*

$$N_{m,k} = \begin{cases} (q-2)\frac{q+1}{3} & \text{if } m \text{ is odd,} \\ q\frac{q-1}{3} & \text{if } m \text{ is even.} \end{cases}$$

APN permutations

- There are many APN permutations on $\mathbb{F}_{2^{2m+1}}$, e.g. monomials
- The only known APN permutation (up to equivalence) on $\mathbb{F}_{2^{2m}}$ is (when $m = 3$) CCZ-equivalent to

$$\kappa(X) = X^3 + X^{10} + AX^{24},$$

  where A is a generator of $\mathbb{F}_{2^6}^*$. (Browning-Dillon-McQuistan-Wolfe 2009)
- Does there exist another APN permutation on even dimensions?
- Why not mimic the behaviour of κ?

Properties of κ

- An APN function f on $\mathbb{F}_{2^n}$ is CCZ-equivalent to a permutation if the Walsh zeroes of f contains two subspaces of dimension n intersecting only trivially.
- The *Walsh transform* of f

$$\widehat{f}(A,B) = \sum_{X \in \mathbb{F}} \chi(Af(X) + BX)$$

and Walsh zeroes WZ_f of f is

$$WZ_f = \{(X,Y) \ : \ \widehat{f}(X,Y) = 0\} \cup \{(0,0)\}.$$

- Walsh zeroes of κ has more structure with respect to some subspaces, i.e.,

$$\{(u_1 x, v_1 y) \ : \ x, y \in \mathbb{K}\}, \{(u_2 x, v_2 y) \ : \ x, y \in \mathbb{K}\} \subseteq WZ_f$$

for some $u_1, u_2, v_1, v_2 \in \mathcal{P}_7$.

Subspace property

- The function κ satisfies the *subspace property*, which is defined as

$$f(aX) = a^{2^k+1} f(X), \qquad \forall a \in \mathbb{K}. \tag{1}$$

  for some integer k.

- According to Browning-Dillon-McQuistan-Wolfe this explained some of the simplicity of why κ is equivalent to a permutation, viz.

$$\begin{aligned}\widehat{f}(au, bv) &= \sum_{X \in \mathbb{F}} \chi\,(au\ f(X) + bv\ X) \\ &= \sum_{X \in \mathbb{F}} \chi\left(ac^{2^k+1}u\ f(X) + bcv\ X\right) \\ &= \widehat{f}(ac^{2^k+1}u, bcv).\end{aligned}$$

Which functions satisfy the subspace property

- κ
- Gold exponents

Remark

If the exponents of f are in $\{2^k+1, q+2^k, (2^k+1)q, 2^kq+1\}$ then f satisfies subspace property.

- *$g_{C,k}$ necessarily has exponents $\{q+1, 2^kq\}$ which disturbs the subspace property.*
- *Carlet 2011 and Zhou-Pott 2013 has bivariate constructions which necessitates the exponents $\{2, q+1, 2q\}$. These constructions have also close connections to projective polynomials*

Quoting Browning-Dillon-McQuistan-Wolfe

> *[T]he highly structured decomposition of the κ code raise the hope that much of the structure, if not all, should generalize to higher dimensions. Does it?*

New APN family satisfying the subspace property

Theorem

Let $f_k(X) = X^{2^k+1} + (\mathrm{Tr}^n_m(X))^{2^k+1}$. Then f_k is APN if and only if m is even and $\gcd(k, n) = 1$.

Proof.

Use Trace-0/Trace-1 decomposition.
Write $X = xg + y$.
Derivatives $L_{ag}(X) = a^{2^k+1}(A(x, y)g + B(x, y))$.
$L(X)$ are two-to-one maps.

□

Remark

Unfortunately f_k are not equivalent to permutations on $\mathbb{F}_{2^8}$ and does not seem to be on $\mathbb{F}_{2^{12}}$.

Hyperplane spectrum

Crooked functions

For a crooked function f, the hyperplane spectrum $\mathcal{H}_f$ is defined by the multiset

$$\mathcal{H}_f = \{* \ \beta \in \mathbb{F}^* \ : \ \mathrm{Im}(D_A f) = H_\beta \ *\}.$$

where $H_\beta = \{X \in \mathbb{F} \ : \ \mathrm{Tr}\,(\beta X) = 0\}$

Hyperplane spectrum

Crooked functions

For a crooked function f, the hyperplane spectrum $\mathcal{H}_f$ is defined by the multiset

$$\mathcal{H}_f = \{* \ \beta \in \mathbb{F}^* \ : \ \mathrm{Im}(D_A f) = H_\beta \ *\}.$$

where $H_\beta = \{X \in \mathbb{F} \ : \ \mathrm{Tr}\,(\beta X) = 0\}$

For Gold exponents X^{2^k+1}

$$\mathcal{H}_{f_{\mathrm{Gold}}} = \{* \ \beta^{2^k+1} \ : \ \beta \in \mathbb{F}^* \ *\}$$

Hyperplane spectrum

Crooked functions

For a crooked function f, the hyperplane spectrum $\mathcal{H}_f$ is defined by the multiset

$$\mathcal{H}_f = \{\!*\ \beta \in \mathbb{F}^* \ :\ \mathrm{Im}(D_A f) = H_\beta\ *\!\}.$$

where $H_\beta = \{X \in \mathbb{F} \ :\ \mathrm{Tr}\,(\beta X) = 0\}$

For Gold exponents X^{2^k+1}

$$\mathcal{H}_{f_{\mathrm{Gold}}} = \{\!*\ \beta^{2^k+1} \ :\ \beta \in \mathbb{F}^*\ *\!\}$$

Theorem

Let $A = ag$ where $a \in \mathbb{K}^*$ and $g \in \mathcal{T}_1$. Then the derivatives $D_A f_k$ of f_k satisfy

$$\mathrm{Im}(D_A f_k) = H_{\beta_A}$$

where

$$\beta_A = \frac{1}{a^{2^k+1}} \frac{\mathrm{Tr}^n_m(g^{2^k+1})}{\mathrm{Tr}^n_m(g^3)^{2^k+1}} \left(g + 1 + \frac{\mathrm{Tr}^n_m(g^3)}{\mathrm{Tr}^n_m(g^{2^k+1})} \right).$$

Corollary

We have

(i) *The Walsh spectrum* $\mathcal{W}_{f_k}$ *of* f_k *satisfies* $\mathcal{W}_{f_k} = \{0, \pm 2^m, \pm 2^{m+1}\}$,

(ii) *If* $A \in \mathbb{F}^*$ *and* $A^{-1} \notin \mathcal{H}_f$, *then the binomial (monomial if* $A \in \mathbb{K}^*$*) Boolean function* $\mathrm{Tr}\left(AX^{2^k+1} + (A^q + A)X^{q2^k+1}\right)$ *is bent. The number of such bent functions is* $2^{\frac{q^2-1}{3}}$.

Remark

- *If* $k = 1$ *then* $\beta_A = \frac{g}{a^3 \mathrm{Tr}_m^n(g^3)^2}$ *becomes very simple.*
- *This also tells us finding zeroes of Walsh transform of* f_k *is rather easy.*
- *The functions* f_k *are not CCZ-equivalent to any known functions on* $\mathbb{F}_{2^{12}}$.

More functions with subspace property?

- Let $g = X^3$
- Consider $L_1(g(L_2(X))) = h(X)$ where

$$L_i(X) = AX + BX^q$$

- Difficult to check with computers
- It does not seem to exist on $\mathbb{F}_{2^{10}}$ and $\mathbb{F}_{2^{14}}$
- Restriction to odd dimension subfield important?

Switching construction

- Recall the similarity to the infinite family of Budaghyan-Carlet-Leander

$$X^3 + \mathrm{Tr}\left(X^9\right)$$

- Adding a Boolean function to a known family is a highly exploited method (Dillon, Budaghyan-Carlet-Leander, Edel-Pott, ...)
- New family can be seen as adding a "vectorial Boolean function" to the Gold family.

Some problems

Problem

Find an infinite family of APN functions which includes the Kim function and which satisfies the subspace property.

Problem

Show that the Gold functions (or any existing family) are not equivalent to permutations.

Problem

Describe the zeroes of the Walsh transform of known APN families.

Problem

Are there APN permutations on $\mathbb{F}_{2^{2m}}$ for $m > 3$?

Thanks for your attention.