On permutation polynomials of the shape

$$\mathbf{G(X) + \gamma\, Tr(\, H(X)\,)}$$

Gohar Kyureghyan
Otto-von-Guericke University of Magdeburg
Department of Mathematics – Germany

joint work with Pascale Charpin
SECRET – INRIA – France

Fq9 – Dublin, Ireland – July 13, 2009

A polynomial $F(X) \in \mathbb{F}_{p^n}[X]$ is called a permutation polynomial of $\mathbb{F}_{p^n}$ if the induced mapping $x \mapsto F(x)$ is a permutation of $\mathbb{F}_{p^n}$.

Let $\gamma \in \mathbb{F}_{p^n}$ and $G(X),\ H(X) \in \mathbb{F}_{p^n}[X]$. We consider the permutation polynomials of the shape

$$F(X) = G(X) + \gamma\, Tr(\, H(X)\,),$$

where $Tr(X) = X + X^p + \ldots + X^{p^{n-1}}$.

Claim: If $G(X) + \gamma\, Tr(\, H(X)\,)$ is a permutation polynomial of $\mathbb{F}_{p^n}$, then for any $\alpha \in \mathbb{F}_{p^n}$ the equation $G(x) = \alpha$ has at most p solutions.

Let $\boldsymbol{G(x)}$ be a permutation of $\mathbb{F}_{p^n}$. Then

$$\boldsymbol{G(x) + \gamma\, Tr(\, H(x)\,) = \Big(x + \gamma\, Tr\big(\, H\big(G^{-1}(x)\big)\big)\Big) \circ G(x)}$$

is a permutation of $\mathbb{F}_{\boldsymbol{p^n}}$ if and only if for any $\boldsymbol{c} \in \mathbb{F}_{\boldsymbol{p}}^*$ the mapping $R(x) = H \circ G^{-1}(x)$ satisfies

$$\sum_{\boldsymbol{x}\in\mathbb{F}_{\boldsymbol{p^n}}} \boldsymbol{\xi^{Tr(cR(x)+\lambda x)} = 0} \tag{1}$$

for all $\boldsymbol{\lambda} \in \mathbb{F}_{\boldsymbol{p^n}}$ with $\boldsymbol{Tr(\gamma\lambda) = c}$.

The mappings $\boldsymbol{R(x)}$, such that $\boldsymbol{Tr\big(R(x)\big)}$ has a linear structure, satisfy (1). This concept appears in several works in Cryptology.

Mappings with a linear structure

Let $b \in \mathbb{F}_p$ and $f : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_p$. An element $\gamma \in \mathbb{F}^*_{p^n}$ is said to be a b-linear structure of the mapping f if

$$f(x+\gamma) - f(x) = b$$

for all $x \in \mathbb{F}_{p^n}$. (Dubuc, Everste, Lai, Yashchenko)

Example:

Let $\gamma \neq 0$, $\beta \in \mathbb{F}_{p^n}$ and $H(X) \in \mathbb{F}_{p^n}[X]$ be arbitrary. Then γ is a $Tr(\beta\gamma)$-linear structure of the mapping defined by

$$Tr\left(H(X^p - \gamma^{p-1}X) + \beta X\right).$$

Theorem. Let $\gamma \in \mathbb{F}_{p^n}$ be a b-linear structure of $f : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_p$. Then the mapping

$$F(x) = x + \gamma f(x)$$

(1) is a permutation of $\mathbb{F}_{p^n}$ if and only if $b \neq -1$;

(2) is a complete mapping of $\mathbb{F}_{p^n}$ if and only if $b \neq -1, -2$;

(3) is p-to-1 on $\mathbb{F}_{p^n}$ if $b = -1$.

(4) The inverse mapping of $F(x)$ is $F^{-1}(x) = x - \frac{\gamma}{b+1} f(x)$.

Corollary. Let $p = 2$ and $1 \leq d, t \leq 2^n - 2$. Then

$$X^d + Tr(X^t)$$

is a permutation polynomial over $\mathbb{F}_{2^n}$ if and only if the following conditions are satisfied:

- n is even and $gcd\,(d, 2^n - 1) = 1$
- $t = d \cdot s \pmod{2^n - 1}$ for some s such that $1 \leq s \leq 2^n - 2$ and has binary weight 1 or 2.

The proof uses the complete characterization of the monomial Boolean functions $Tr(\delta x^s)$ having a linear structure.

$G(X)$ is a linearized polynomial

Theorem. Let $G : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_{p^n}$ be a linear p-to-1 mapping with kernel $\alpha\mathbb{F}_p$ and $H : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_{p^n}$. Then the mapping

$$G(x) + \gamma\, Tr(H(x)), \quad \gamma \in \mathbb{F}_{p^n},$$

is a permutation of $\mathbb{F}_{p^n}$ if and only if

- γ does not belong to the image set of G
- $Tr\big(H(x+\delta) - H(x)\big) \neq 0$ for any $x \in \mathbb{F}_{p^n}$ and $\delta \in \alpha\mathbb{F}_p^*$.

Corollary. Let $H : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_{p^n}$ be arbitrary and $\beta, \gamma \in \mathbb{F}_{p^n}$. Then

$$X^p - \alpha^{p-1}X + \gamma\, Tr(H(X^p - \alpha^{p-1}X) + \beta X)$$

is a permutation polynomial of $\mathbb{F}_{p^n}$ if and only if $Tr(\gamma\alpha^{-p}) \neq 0$ and $Tr(\alpha\beta) \neq 0$.

Lifting of permutations

Theorem. Let $h : \mathbb{F}_p \longrightarrow \mathbb{F}_p$ and $\gamma \in \mathbb{F}_{p^n}$ be a b-linear structure of $f : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_p$. Then

$$x + \gamma\, h\big(f(x)\big)$$

permutes $\mathbb{F}_{p^n}$ if and only if

$$x + b\, h(x)$$

permutes $\mathbb{F}_p$.

Remark. A prime number p can be replaced by a prime power q.

Conclusions

We found a link between permutation polynomials of the shape

$$G(X) + \gamma\, Tr(\, H(X)\,)$$

and the concept of a linear structure. The mappings with a linear structure allow

- to construct large families of permutation polynomials of $\mathbb{F}_q$
- to lift permutation polynomials of $\mathbb{F}_q$ to those of $\mathbb{F}_{q^n}$

Open Problems

- general $G(X)$