Bent functions on a Galois ring and Systematic Authentication Codes

J.C.Ku-Cauich and H. Tapia-Recillas*
Departamento de Matemáticas
Universidad Autónoma Metropolitana-I
09340 México, D.F., MEXICO
(jckc35@hotmail.com, htr@xanum.uam.mx)

Introduction

On a public communication channel there is a risk that an intruder can deliberately observe and even cause a disturbance in the communication. An authentication code provides a method for insuring the integrity of the information to be sent through this channel. These codes, first introduced by Gilbert, MacWilliams and Sloane, have since received attention by several authors and may be with secrecy and without secrecy; a subclass of the latter is the Systematic Authentication Codes (SACs). Several types of SACs have been constructed using various concepts such as highly nonlinear functions over finite fields or non-degenerated and rational functions on a Galois ring . By introducing a class of bent functions over a Galois ring of characteristic p^2, (p a prime) and using the Gray map on such ring, a class of SACs is presented and an example is given to illustrate the main results.

About Galois rings

Let $\mathbb{Z}_{p^t}$ be the ring of integers modulo p^t, where p is a prime and t a positive integer. A monic polynomial $f(x) \in \mathbb{Z}_{p^t}[x]$ is called *monic basic irreducible (primitive)* if its reduction modulo p is an irreducible (primitive) polynomial over $\mathbb{F}_p$. The Galois ring of characteristic p^t is defined as: $\mathrm{GR}(p^t, m) = \mathbb{Z}_{p^t}[x]/\langle f(x)\rangle$ where $f(x) \in \mathbb{Z}_{p^t}[x]$ is a monic basic irreducible polynomial of degree m and $\langle f(x)\rangle$ is the ideal of $\mathbb{Z}_{p^t}[x]$ generated by $f(x)$. The polynomial $f(x)$ can be taken such that it is a divisor of $x^{p^m-1} - 1$.

The ring $R = \mathrm{GR}(p^t, m)$ is local with maximal ideal $M = \langle p\rangle = pR$ generated by p and its residue field $\mathbb{F} = R/M$ is isomorphic to $\mathbb{F}_q$ where $q = p^m$. If $\omega \in R$ is a root of $f(x)$, the Teichmüller set of representatives of R can be taken as $T(R) = \{0, 1, \omega, \omega^2, ..., \omega^{q-2}\}$. Let $\mu : R \longrightarrow \mathbb{F}$, $\mu(\theta) = \overline{\theta}$ be the canonical residue mapping. Examples of Galois rings include $\mathrm{GR}(p, m) = \mathrm{GF}(p, m) = \mathbb{F}_{p^m}$ and $\mathrm{GR}(p^t, 1) = \mathbb{Z}_{p^t}$, and Galois rings are examples of finite chain rings.

There is an injective isometry $\Phi : (R^n, d_h) \longrightarrow (\mathbb{F}^{nq^{t-1}}, d_H)$, where d_H is the Hamming metric and d_h the homogeneous metric on R^n called the *Gray map.*

A class of bent functions

Let R be as above. We recall that a function $f : R^n \longrightarrow R$ is bent if $\left|\sum_{x\in R^n} e^{2\pi i(Tr(f(x)-\lambda\cdot x))/p^t}\right| = |R|^{n/2}$, for all $\lambda \in R^n$ where $\lambda \cdot x$ is the usual dot product in R^n and Tr is the trace function from R onto $\mathbb{Z}_{p^t}$.

The following result gives a class of bent functions on a Galois ring:

Proposition 1 *Let $R = GR(p^t, m)$ be the Galois ring of characteristic p^t with $t \geq 2$ and let $f : R \longrightarrow R$ be a bent function. Then for any unit u of $\mathbb{Z}_{p^t}$, (uf) is a bent function from R to R .*

A class of bent functions on a Galois ring of characteristic p^2 is given by

Proposition 2 *Let $R = GR(p^2, m)$, $r \geq 1$ be an integer such that $(r, p^m-1) = 1$ and let $f(x) = x^{pr+1} + \alpha x^p$ where $\alpha \in R$. Then for any unit u of R, (uf) is a bent function from R to R.*

General facts on SACs

A systematic authentication code is a quadruple: $(\mathbb{S}, \mathbb{T}, \mathbb{K}, \mathbb{E} = \{E_k : \mathbb{S} \to \mathbb{T},\ k \in \mathbb{K}\})$, where $\mathbb{S}$ is the source state space, $\mathbb{T}$ the tag space, $\mathbb{K}$ the key space and $E_k : \mathbb{S} \to \mathbb{T}$ is called an encoding rule. The sets $\mathbb{S}$, $\mathbb{T}$ and $\mathbb{K}$ are nonempty and finite.

A transmitter and receiver share a secret key $k \in \mathbb{K}$. The transmitter wishes to send a piece of information, $s \in \mathbb{S}$, called the source state, to the receiver. The transmitter computes $t = E_k(s) \in \mathbb{T}$ and sets the message $m = (s,t)$ into a public channel. Receiving $m' = (s',t')$, the receiver computes $E_k(s')$ and checks whether $E_k(s') = t'$. If yes, the receiver accepts the message as authentic, otherwise he rejects it.

It is assumed that an intruder can insert a message into the public channel or substitute an observed message m with another message m'. Thus two types of attacks can be considered: by impersonation and by substitution. Let P_I be the maximum probability that the message will be accepted as authentic in the impersonation case and let P_S be the maximum probability of this message being accepted as authentic in the substitution attack.

Assuming the key and source states are equiprobable these probabilities are defined as:

$$P_I = \max_{s \in \mathbb{S}, t \in \mathbb{T}} \frac{|\{k \in \mathbb{K} : E_k(s) = t\}|}{|\mathbb{K}|}, \quad P_S = \max_{\substack{s \in \mathbb{S} \\ t \in \mathbb{T}}} \max_{\substack{s' \in \mathbb{S}, s' \neq s \\ t' \in \mathbb{T}}} \frac{|\{k \in \mathbb{K} : E_k(s) = t, E_k(s') = t'\}|}{|\{k \in \mathbb{K} : E_k(s) = t\}|}.$$

For systematic authentication codes to be acceptable, both, P_I and P_S must be as small as possible.

The new SAC

Let f be a function on R as in Proposition 1 or Proposition 2. Let $S = \mathrm{GR}(p^t, mn)$ be a Galois ring, extension of $R = \mathrm{GR}(p^t, m)$ of degree n, and $T(S)$ (resp. $T(R)$ be the Teichmüller set of S (resp. R).

$$L = \{r_0 + r_1 p + \cdots + r_{t-2} p^{t-2} \mid r_0, \ldots, r_{t-2} \in T(R)\} \subset (R \backslash p^{t-1} R) \cup \{0\}.$$

The proposed Systematic Authentication Code, $\mathbb{A} = (\mathbb{S}, \mathbb{T}, \mathbb{K}, \mathbb{E})$, is the following:

$$\begin{aligned} \mathbb{S} &:= \{(a,b,c) \in T(S) \times S \times L \mid (a,b) \neq (0,0)\}, \\ \mathbb{T} &:= \mathbb{F}_q, \\ \mathbb{K} &:= \mathbb{Z}_{q^{t(n+1)}}, \\ \mathbb{E} &:= \{E_k(s) = pr_k(u_s),\ k \in \mathbb{K}, s \in \mathbb{S}\}. \end{aligned}$$

where for $x \in S$, $s = (a,b,c) \in \mathbb{S}$, $\beta \in p^{t-1}R = \{\beta_1, \beta_2, \ldots, \beta_q\}$: $v_{s,\beta}(x) = \beta + Tr_{(S/R)}(af(x) + bx) + c$, $u_{s,\beta} = (\Phi(v_{s,\beta}(x)))_{x \in S}$, $u_s = (u_{s,\beta})_{\beta \in p^{t-1}R}$, pr_k is the k-th projection map from $\mathbb{F}_q^{q^{t(n+1)}}$ onto $\mathbb{F}_q$, mapping u_s to its k-th coordinate, $Tr_{S/R}$ is the trace map from S onto R and Φ is the Gray map.

We have the following,

Theorem 3 *For the proposed systematic authentication code $\mathbb{A}$,*

$$P_I = \frac{1}{q} \quad \text{and} \quad P_S \leq \frac{1}{q} + \frac{q-1}{q^{\frac{tn+2}{2}}}.$$

An example

Let $R = GR(p^t, m)$ and $f : R \to R$ be a bent function. Then (af) is also bent for any unit a of $\mathbb{Z}_{p^t}$ (Proposition 1). Let $L = \{r_0 + r_1 p + \cdots + r_{t-2} p^{t-2} \neq 0 \mid r_0, ..., r_{t-2} \in T(R)\}$.

$$\begin{aligned} \mathbb{S} &:= \{(a,b,c) \in T(R) \times R \times L \mid (a,b) \neq (0,0)\}, \\ \mathbb{T} &:= \mathbb{F}_p, \\ \mathbb{K} &:= \mathbb{Z}_{p^{t(n+1)}}, \\ \mathbb{E} &:= \{E_k(s) = pr_k(u_s),\ k \in \mathbb{K}, s \in \mathbb{S}\}, \end{aligned}$$

and from Theorem 3,

$$P_I = \frac{1}{p} \quad \text{and} \quad P_S \leq \frac{1}{p} + \frac{p-1}{p^{\frac{tm+2}{2}}}.$$