Mathematics and Statistics 6(3): 34-45, 2018 http://www.hrpub.org
DOI: 10.13189/ms.2018.060302

Discrete Logarithm in Galois Rings

Samuel Bertrand Liyimbeme Mouchili

African Institute for Mathematical Sciences (AIMS)-Cameroon alumnus, Cameroon

Abstract Since Galois rings are the generalization of Galois fields, the question we tried to answer is: How to move from the discrete logarithm in Galois fields to the one in Galois rings? That concept of the discrete logarithm in Galois rings is a little bit different from the one in Galois fields. Here, the discrete logarithm of an element is the tuple, which is not the case in Galois fields. However, thanks to the multiplicative representation of elements in Galois rings, each element α can be uniquely represented in the form: $\alpha = \varepsilon^{(x_0,x_1,\cdots,x_{k-1})}$; where k is a nonnegative integer, ε is a generator of the Galois ring (the definition of a generator in a Galois ring will be given later on). Then the tuple $(x_0, x_1, \cdots, x_{k-1})$ will be called: the discrete logarithm of α. The notion of generators in Galois rings comes from the one in the group theory. The Knowledge of the generators in multiplicative groups $(\mathbb{Z}/p\mathbb{Z})^*$ allows, as well to determine the generators in Galois rings $GR(p^k, m)$; p is a prime number and m is a nonnegative integer greater than or equal to two. These new concepts of discrete logarithm and generators in Galois rings will help to securely share common information and to perform ElGamal encryption in Galois rings.

Keywords Galois Ring, Discrete Logarithm, ElGamal Encryption

1 Introduction

The ElGamal encryption is an asymmetric scheme like RSA. It was invented by Taher ElGamal in 1984 and it is generally based on discrete logarithm in finite groups [7]. To build that encryption, one has to find a finite group in which it is not easy to solve the discrete logarithm problem.

More often, people work with extensions of Galois fields $\mathbb{F}_p(\xi) \cong \mathbb{F}_{p^m}$, where ξ is a primitive element of $\mathbb{F}_p$; (see [6]). That is just because they want to increase the number of elements in the fields of characteristic p. For instance the field $\mathbb{Z}_p$ (stands for $\mathbb{Z}/p\mathbb{Z}$) has only p elements whereas the field $\mathbb{Z}_p(\xi)$ has p^m elements. ξ is the primitive root of the minimal polynomial of degree m and with coefficients in $\mathbb{Z}_p$. See [1] for details. One could just take the ring $\mathbb{Z}_{p^m}$ because it also has p^m elements. But the problem is that it has no strucure of a field. That is why it is needed to work with field extensions of $\mathbb{Z}_p$ in order to performed ELGamal encryptions and to have the same number of elements (p^m in this case).

In this paper, we present a new idea on how it is possible to stay in the ring $\mathbb{Z}_{p^m}$ with no field structure on it and to still have the right to perform ElGamal encryptions as well. That is mainly because the ring $\mathbb{Z}_{p^m}$ and its extensions (with respect to B-polynomials) have a structure of Galois rings.

Galois rings are the generalisation of the finite fields [1], in the sense that they are built from the field $\mathbb{Z}_p$. They are denoted by $GR(p^k, m)$. To construct a Galois ring $GR(p^k, m)$, one can move from $\mathbb{Z}_p$ to $\mathbb{Z}_{p^k}$, which is the Galois ring $GR(p^k, 1)$, where k is a nonnegative integer. The extensions of Galois rings are constructed using B-polynomials P of degree m. B-polynomials are irreducible and unitary polynomials with coefficients in $\mathbb{Z}_{p^k}$. One can use the Hensel lemma to have such polynomials.

It is worth while to recall that, in a multiplicative (or additive) cyclic group G generated by an element g, any element h in G is a power of g. For more details in finite groups, see [8].
That is $h = g^x$ for some $x \in \{0, 1, \cdots, \mid G \mid -1\}$. Such a x is called the discrete logarithm of h in basis g.
For instance in $\mathbb{Z}_5^*$, where 3 is a generator (since $1 = 3^0,\ 2 = 3^3,\ 3 = 3^1,\ 4 = 3^2$),
2 is the discrete logarithm of 4 in basis 3: $\log_3(4) = 2$. Likewise 3 is the discrete logarithm of 2 in basis 3: $\log_3(2) = 3$.
Even in field extensions $\mathbb{F}_p(\xi) \cong \mathbb{F}_{p^m} = \{0, \xi, \xi^2, \cdots, \xi^{p^m-1}\}$, where m is the degree of the extension, the finite groups $\mathbb{F}_p(\xi)^\times$ are generated by ξ. [9]

The security of ElGamal encryption schemes rely on p: for a good security, p has to be of around 1024 bits [2]. And we claim that the security has to be better when m is larger enough.

In Galois rings, the multiplicative representation of elements allows to define the notion of discrete logarithm. Nevertheless, before that definition, Galois ring theory has to be briefly recalled. In this work, p is a prime number; k, m are positive integers greater than or equal to 2.

1.1 Basis irreducible polynomials

Lemma 1.2. *Factorization in $\mathbb{Z}_{p^k}[X]$ [5]:*
Let p be a prime number and k an integer, $k \geq 2$.
Let P be a unitary polynomial with coefficients in $\mathbb{Z}_{p^k}$, and such that
$P \equiv QR \mod p$, where $Q, R \in \mathbb{Z}_p[X]$ are two unitary and coprine polynomials.
Then there exists a unique couple $\left(Q^{(k)}, R^{(k)}\right)$ of unitary and coprime polynomials in $\mathbb{Z}_{p^k}[X]$ such that:

1. $P = Q^{(k)}R^{(k)}$
2. $Q^{(k)} \equiv Q \mod p$ *and* $R^{(k)} \equiv R \mod p$.

Moreover $Q^{(k)}$ and Q have the same degree.
Likewise, $R^{(k)}$ and R have the same degree.

Definition 1.3. *Let Q and R be two polynomials with coefficients in Z_p such that :*
$X^n - 1 = Q(X)R(X)$ where n and p are coprime.
A Hensel lifting of order k of polynomial Q is the polynomial $Q^{(k)}$ in the couple $(Q^{(k)}, R^{(k)})$ in the previous lemma.
When Q is irreducible and primitive, its Hensel lifting are called B-polynomials. B stands for basic (in basic polynomial).

Proposition 1.4. *[5]*
Let $Q \in Z_2[X]$ a factor of $X^{2^m-1} - 1$.
Let $Q^{(k)} \in Z_{2^k}[X]$ be its Hensel lifted of order k.
Set $Q^{(k)} = P(X) - I(X)$, where P contains even degree polynomials and I contains odd degree polynomials.
Then:

$$Q^{(k+1)}(X^2) = \pm\left(P^2(X) - I^2(X)\right).$$

Computations are performed in $Z_{p^k}[X]$ and signs are chosen in order to make $Q^{(k+1)}$ unitary.

Example 1.5.

$$X^7 - 1 = (X^3 + X + 1)(X^3 + X^2 + 1)(X - 1).$$

Set $Q = Q^{(1)} = X^3 + X^2 + 1 \in Z_2[X]$ and let us compute its Hensel lifting of order 3 using the previous proposition:

$$P_1(X) = \left(X^2 + 1\right) \mod 2,\ I_1(X) = \left(-X^3\right) \mod 2,$$
$$\left(P_1(X)\right)^2 = \left(X^4 + 2X^2 + 1\right) \mod 4,\ \left(I_1(X)\right)^2 = X^6 \mod 4.$$

And

$$Q^{(2)}\left(X^2\right) = \left(X^6 - X^4 - 2X^2 - 1\right) \mod 4 = \left(X^6 + 3X^4 + 2X^2 + 3\right) \mod 4.$$

It follows that the Hensel lifting of order 2 of the polynomial Q is

$$Q^{(2)}(X) = \left(X^3 + 3X^2 + 2X + 3\right) \mod 4.$$

Similarly, to compute $Q^{(3)}$, it has to be splited into two parts as well.

$$P_2(X) = \left(3X^2 + 3\right) \mod 4,\ I_2 = \left[-(X^3 + 2X)\right] \mod 4.$$
$$\left(P_2(X)\right)^2 = \left(X^4 + 2X^2 + 1\right) \mod 8,\ \left(I_2(X)\right)^2 = \left(X^6 + 4X^4 + 4X^2\right) \mod 8.$$

Then

$$Q^{(3)}\left(X^2\right) = \left(X^6 + 3X^4 + 2X^2 + 7\right) \mod 8.$$

Which amounts to

$$Q^{(3)}(X) = \left(X^3 + 3X^2 + 2X + 7\right) \mod 8.$$

Which is the Hensel lifting of order 3 of the polynomial Q.

$X^4 + 2X^3 + 7X^2 + 5X + 1$ *is the Hensel lifting of* $\left(X^3 + X^2 + 1\right)(X - 1)$.

Example 1.6. *Consider the polynomial* $X^3 - 1 \in Z_2[X]$.

$$X^3 - 1 = (X^2 + X + 1)(X - 1).$$

Set $Q = Q^1 = X^2 + X + 1$ *in* $Z_2[X]$. *As it is done in the previous example,*

$$P_1(X) = (X^2 + 1) \mod 2 \text{ and } I_1(X) = -X \mod 2$$

$$(P_1(X))^2 = (X^4 + 2X^2 + 1) \mod 4 \text{ and } (I_1(X))^2 = X^2 \mod 4$$

$$Q^{(2)}(X^2) = (X^4 + X^2 + 1) \mod 4.$$

Finally

$$Q^{(2)}(X) = (X^2 + X + 1) \mod 4.$$

2 Galois rings

Definition 2.1. *A ring* R *is said to be a Galois ring if it is unitary, commutative, local and finite.*

Example 2.2. $\mathbb{Z}_{p^k}$ *understood as* $\mathbb{Z}/p^k\mathbb{Z}$ *is a Galois ring; where* p *is a prime number,* k *a positive integer.*

Let ξ be a root of a basis irreducible polynomial P of degree $m > 1$.
$\mathbb{Z}_{p^k}[X]/(P(X))$ is the ring extention of $\mathbb{Z}_{p^k}$. It is also a Galois ring. See [5] for more details.
All the Galois rings are isomorphic to $\mathbb{Z}_{p^k}[X]/(P(X))$ and they are denoted by $GR(p^k, m)$; where m is the degree of the B-polynomial.
The equivalence class of X under the equivalence relation $\mathcal{R}$, understood by

$$(a, b) \in \mathcal{R} \Leftrightarrow a = b \mod p,$$

is denoted by ξ,
which means that $\xi = X \mod P$.
The B-polynomial used to construct an extension of Z_{p^k} will always be appointed by P.
Let

$$\begin{array}{rccc} \chi: & Z_{p^k}[X]/(P) & \longrightarrow & \mathbb{F}_{p^m} \\ & \alpha & \longmapsto & \alpha + (p) \end{array}$$

χ is a ring morphism.

Remark 2.3. $ker\chi = (p)$. *Then* $A/(p)$ *and* $\chi(A)$ *are isomorphic; where* $A = Z_{p^k}[X]/(P)$.
But $\chi(A) = \mathbb{F}_{p^m}$ *because* χ *is surjective. So* $A/(p)$ *and* $\mathbb{F}_{p^m}$ *are isomorphic.*

Proposition 2.4. *With the previous hypotheses, the element* $\xi = X \mod P$ *has the following properties:*

1. $P(\xi) = 0$;
2. $\chi(\xi)$ *is a primitive element in* F_{p^m};
3. ξ *generates a group of order* $p^m - 1$.

Let α in $GR(p^k, m)$. α can be expressed in two different ways: additively and multiplicatively.
See [5] for more details.
Additive representation:

$$\alpha = \sum_{i=0}^{m-1} \lambda_i \xi^i, \ \lambda \in \{0, 1, 2, \cdots, m-1\}.$$

Multiplicative representation:

$$\alpha = \sum_{i=0}^{k-1} \nu_i p^i, \ \nu_i \in \mathcal{T} = \{0, 1, \xi, \cdots, \xi^{p^m - 2}\}.$$

$\mathcal{T}$ is called the Teichmüller set.

3 Discrete logarithm in Galois rings

3.1 Discrete logarithm in $\mathbb{Z}_{p^k}$

For all $\alpha \in \mathbb{Z}_{p^k}$, there exist unique integers $0 \leq \alpha_i \leq p-1$ such that

$$\alpha = \sum_{i=0}^{k-1} \alpha_i p^i.$$

It is a representation of α in basis p.
Now we consider p to be an odd prime.
$\forall i \in \{0, 1, \cdots, k-1\},$ if $\alpha_i \neq 0,$ then $\alpha_i = g^{x_i},$ otherwise, $\alpha_i = 0$. And we represent 0 by $g^- : \ 0 = g^-$.
where g is a generator of the multiplicative group $\mathbb{F}_p^*$, and $x_i \in \{0, 1, \cdots, p-1\}, \ \forall i \in \{0, 1, \cdots, k-1\}$.
x_i is the discrete logarithm of α_i in the basis g, $\forall i \in \{0, 1, \cdots, k-1\}$.
α can then be expressed as $\alpha = \sum_{i=0}^{k-1} g^{x_i} p^i$. One can just write $\alpha = g^{(x_0, x_1, \cdots, x_{k-1})}$.

Before we can give the definition of the discrete logarithm in a Galois ring $\mathbb{Z}_{p^k}$, let us consider the following mapping:

$$\begin{array}{rccc} f: & \mathbb{Z}_{p^k} \times \{-, 0, 1, \cdots, p-1\}^k & \longrightarrow & \mathbb{Z}_{p^k} \\ & (\alpha, X) & \longmapsto & \alpha^X \end{array}$$

$\forall \alpha \in \mathbb{Z}_{p^k}$, there is a unique tuple $Y = (y_0, y_1, \cdots, y_{k-1})$ such that: $\alpha = g^Y$, where g is a generator of $\mathbb{Z}_p$. Note that:

$$(g^x)^- = \left(g^-\right)^x = 0, \ \forall x \in \{-, 0, 1, \cdots, p-1\}.$$

And

$$(g^x)^y = g^{xy \mod (p-1)}, \ \forall x, y \in \{0, 1, \cdots, p-1\}.$$

Therefore

$$\forall X, Y \in \{-, 0, 1, \cdots, p-1\}, \ \left(g^Y\right)^X = \left(g^X\right)^Y.$$

Definition 3.2. *With the previous hypotheses, the tuple $(x_0, x_1, \cdots, x_{k-1})$ in the expression $\alpha = \sum_{i=0}^{k-1} g^{x_i} p^i$, is the discrete logarithm of α in the basis $b = g^{(1,1,\cdots,1)}$.*
To avoid confusion with the discrete logarithm in finite groups,
it will be called the Galois logarithm of α in the basis $b = g^{(1,1,\cdots,1)}$,
where g is a generator of the finite group $\mathbb{Z}_p$.
Such an element b will be called a generator of the Galois ring $\mathbb{Z}_{p^k}$.

Notation 3.3. *The Galois logarithm of an element $\alpha = g^{(x_0, x_1, \cdots, x_{k-1})}$ in the basis b is denoted by: $\log_b \alpha$ and it is equal to $(x_0, x_1, \cdots, x_{k-1})$.*

The following computations allows to determine generators in Galois rings $\mathbb{Z}_{p^k}$:

$$\begin{aligned} b &= g^{(1,1,\cdots,1)} \\ &= g + g \cdot p + g^2 \cdot p^2 + \cdots + g^{k-1} \cdot p^{k-1} \\ &= g\left(1 + p + p^2 + \cdots + p^{k-1}\right) \\ &= g\left(\tfrac{1-p^k}{1-p}\right) \\ &= g\left(\tfrac{1}{1-p}\right), \end{aligned}$$

where $\frac{1}{1-p}$ is the inverse of $1-p$ in $\mathbb{Z}_{p^k}$.

Example 3.4. *The ring $\mathbb{Z}_{25}$ is a Galois ring since $25 = 5^2$. Let us compute the Galois logarithm of $14 \in \mathbb{Z}_{25}$ in the basis $b = 3^{(1,1)} = 3 + 3 \times 5 = 18$;*

$14 = 4 + 2 \times 5 = 3^2 + 3^3 \times 5$.
Then
$14 = 3^{(2,3)}$. *And*
$\log_{18} 14 = (2, 3)$.
If we change the basis and take $b = 2^{(1,1)}$, *we should have* $\log_b 14 = (2, 1)$.
Indeed $b = 2^{(1,1)} = 2 + 2 \times 5 = 12$,
$14 = 4 + 2 \times 5 = 2^2 + 2 \times 5 = 2^{(2,1)}$.
So the Galois logarithm of 14 *in the Galois ring* $\mathbb{Z}_{25}$ *in the basis* 12 *is* $(2, 1)$.

3.5 Discrete logarithm in $GR(p^k, m)$

Let $\alpha \in GR(p^k, m)$, then $\alpha = \sum_{i=0}^{k-1} \nu_i p^i,\ \nu_i \in \mathcal{T}$.
And $\mathcal{T}^* = \langle \xi \rangle$ is a group of order $p^m - 1$ and generated by ξ.
Therefore for all $\nu \in \mathcal{T}^*,\ \nu = \xi^x$ for a certain $x \in \{0, 1, \cdots, p^m - 2\}$.
And 0 will be represented by ξ^-.

So the following mappig is a bijection:

$$\begin{array}{rccc} \varphi: & GR(p^k, m) & \longrightarrow & \{-, 0, 1, \cdots, p^m - 2\}^k \\ & \alpha & \longmapsto & (x_0, x_1, \cdots, x_{k-1}) \end{array}$$

Then each element α in the Galois ring $GR(p^k, m)$ can be represented by:

$$\alpha = (\xi, p)^{(x_0, x_1, \cdots, x_{k-1})}.$$

Or simply by:

$$\alpha = \xi^{(x_0, x_1, \cdots, x_{k-1})}.$$

Remark 3.6. *For all* $x, y \in \{-, 0, 1, \cdots, p^m - 2\}$, *we should have:*

$$(\xi^x)^y = (\xi^y)^x = \xi^{xy \mod (p^m - 1)}.$$

Note that:

$$(\xi^x)^- = (\xi^-)^x = 0^x = 0,\ \forall x \in \{-, 0, 1, \cdots, p^m - 2\}.$$

Definition 3.7. *Let* $X, Y \in \{-, 0, 1, \cdots, p^m - 2\}^k$,
$X = (x_0, x_1, \cdots, x_{k-1}),\ Y = (y_0, y_1, \cdots, y_{k-1})$. *Then*

$$\left((\xi, p)^X\right)^Y = \xi^{z_0} + \xi^{z_1} p + \xi^{z_2} p^2 + \cdots + \xi^{z_{k-1}} p^{k-1},$$

where $\forall i \in \{0, 1, \cdots, k-1\}$

$$z_i = \begin{cases} - & \text{if } x_i = - \text{ or } y_i = - \\ x_i y_i \mod (p^m - 1) & \text{otherwise} \end{cases}$$

Then the following mapping is well defined.

$$\begin{array}{rccc} \phi: & GR(p^k, m) \times \{-, 0, 1, 2, \cdots, p^m - 2\}^k & \longrightarrow & GR(p^k, m) \\ & (\alpha, Y) & \longmapsto & \alpha^Y \end{array}$$

For all $(\alpha, Y) \in GR(p^k, m) \times \{-, 0, 1, \cdots, p^m - 2\}^k$, there exists a unique $X \in \{-, 0, 1, 2, \cdots, p^m - 2\}^k$ such that

$$\phi(\alpha, Y) = \alpha^Y = \left(\xi^X\right)^Y.$$

Remark 3.8. $\left(\xi^X\right)^Y = \left(\xi^Y\right)^X,\ \forall X, Y \in \{-, 0, 1, \cdots, p^m - 2\}^k$.

Definition 3.9. *With the previous hypotheses, the tuple* $(x_0, x_1, \cdots, x_{k-1})$ *in the following representation:*
$\alpha = \xi^{(x_0, x_1, \cdots, x_{k-1})}$ *is the discrete logarithm of* α *in the basis* ε *in the Galois ring* $GR(p^k, m)$.
Note that $\varepsilon = \xi^{(1,1,\cdots,1)}$. *Each component* x_i *in the tuple* $(x_0, x_1, \cdots, x_{k-1})$, *different from* $-$, *is exactly the discrete logarithm in the multiplicative group* $\mathbb{F}_p(\xi)^\times$, *of the corresponding component* ξ^{x_i} *in the tuple* $(\xi^{x_0}, \xi^{x_1}, \cdots, \xi^{x_{k-1}})$.

Notation 3.10. *The Galois logarithm of an element* $\alpha = \xi^{(x_0,x_1,\cdots,x_{k-1})}$ *in the Galois ring* $GR(p^k,m)$ *in the basis* ε *is denoted by* $\log_\varepsilon \alpha$. *So* $\log_\varepsilon \alpha = \varphi(\alpha) = (x_0, x_1, \cdots, x_{k-1})$.

Remark 3.11. $\forall (x_0, x_1, \cdots, x_{k-1}) \in (-, 0, 1, \cdots, p^m - 2)$,

$$\varepsilon^{(x_0,x_1,\cdots,x_{k-1})} = \left(\xi^{(1,1,\cdots,1)}\right)^{(x_0,x_1,\cdots,x_{k-1})} = \left(\xi^{(x_0,x_1,\cdots,x_{k-1})}\right)^{(1,1,\cdots,1)} = \xi^{(x_0,x_1,\cdots,x_{k-1})}.$$

Example 3.12. *a)* $A = \mathbb{Z}_{2^2}[X]/(P);\ p = 2;\ k = 2$ *and* $P = X^2 + X + 1$.
Let ξ *be a primitive root of* P *in* A: $\xi^2 + \xi + 1 = 0$.
Let $\alpha = 3 + \xi$ *and* $\beta = \xi$ *be two elements in* A.
The question is to find the discrete logarithm of α *and* β *in the Galois ring* A. *The two following tables are needed.*

$\underline{Table\ 1}$: *Additive form of the powers of* ξ *in* $\mathbb{Z}_{2^2}[X]/(X^2 + X + 1)$

$$\xi = \xi$$

$$\xi^2 = -\xi - 1 = 3\xi + 3$$

$$\xi^3 = 3\xi^2 + 3\xi = 3(3\xi + 3) + 3\xi = \xi + 3\xi + 1 = 1.$$

$\underline{Table\ 2}$: χ *correspondance of the powers of* ξ *in* $\mathbb{Z}_{2^2}[X]/(X^2 + X + 1)$

$$\chi(\xi) = \chi(\xi)$$

$$\chi(\xi^2) = 1 + \chi(\xi)$$

$$\chi(\xi^3) = 1.$$

The multiplicative representation of α *is obtained following these steps:*

1) $\chi(\alpha) = 1 + \chi(\xi) = \chi(\xi^2)$.
It is necessary, first of all, to check whether α *is already on the multiplicative representation or not. If it is the case, then there is nothing else to do. Otherwise, do:*

2) $\alpha - \xi^2 = 3 + \xi - \xi^2 = 3 + \xi - 3\xi - 3 = -2\xi = 2\xi$.

3) $\alpha = \xi^2 + 2\xi$ *which is the multiplicative form of* α.
Therefore $\alpha = \xi^{(2,1)}$ *and* $\log_\varepsilon \alpha = (2, 1)$ *Since* β *is already on the multiplicative form, then* $\xi = \xi^{(1,-)}$ *and* $\log_\varepsilon \xi = (1, -)$.

b) Let $A := Z_{2^3}[X]/(P);\ p = 2; k = 3$ *and* $P = X^3 + 3X^2 + 2X + 7$.
Let ξ *be a primitive root of* P.
The two following tables will be helpful in establishing the multiplicative representations of elements in the Galois ring A. *The first table will be exclusively used in the additive representation; whereas the second one combined with the first will help in the multiplicative representation.*

$\underline{Table\ 3}$: *Additive form of the powers of* ξ *in* $\mathbb{Z}_{2^3}[X]/(X^3 + 3X^2 + 2X + 7)$

$$\xi = \xi$$

$$\xi^2 = \xi^2$$

$$\xi^3 = -3\xi^2 - 2\xi - 7 = 5\xi^2 + 6\xi + 1$$

$$\xi^4 = 5\xi^3 + 6\xi^2 + \xi = 5(5\xi^2 + 6\xi + 1) + 6\xi^2 + \xi = 7\xi^2 + 7\xi + 5$$

$$\xi^5 = 7\xi^3 + 7\xi^2 + 5\xi = 7(5\xi^2 + 6\xi + 1) + 7\xi^2 + 5\xi = 2\xi^2 + 7\xi + 7$$

$$\xi^6 = 2\xi^3 + 7\xi^2 + 7\xi = 2(5\xi^2 + 6\xi + 1) + 7\xi^2 + 7\xi = \xi^2 + 3\xi + 2$$

$$\xi^7 = \xi^3 + 3\xi^2 + 2\xi = 5\xi^2 + 6\xi + 1 + 3\xi^2 + 2\xi = 1.$$

Table 4 : χ *correspondance of the powers of* ξ *in* $\mathbb{Z}_{2^3}[X]/(X^3+3X^2+2X+7)$

$\chi(\xi) = \chi(\xi)$

$\chi(\xi^2) = \chi(\xi^2)$

$\chi(\xi^3) = \chi(\xi^2) + 1$

$\chi(\xi^4) = \chi(\xi^2) + \chi(\xi) + 1$

$\chi(\xi^5) = \chi(\xi) + 1$

$\chi(\xi^6) = \chi(\xi^2) + \chi(\xi)$

$\chi(\xi^7) = 1.$

Let $\alpha = 3 + 5\xi$ *and* $\beta = 1 + \xi^2$ *in A. They are given in their additive representation.*
To have the multiplicative representation of α*, one can follow the following steps:*

1) $\chi(\alpha) = 1 + \chi(\xi) = \chi(\xi^5)$*, by making use of the second table above.*

2) $\alpha - \xi^5 = 3 + 5\xi + 6\xi^2 + \xi + 1 = 6\xi^2 + 6\xi + 4 = 2(3\xi^2 + 3\xi + 2)$.

3) Check whether $\alpha - \xi^5$ *is already given on a multiplicative representation. In this example it is not the case. Then set* $\alpha' = 3\xi^2 + 3\xi + 2$ *and:*

$$\begin{aligned} \chi(\alpha') &= \chi(\xi^2) + \chi(\xi) = \chi(\xi^6) \\ \alpha' - \xi^6 &= 3\xi^2 + 3\xi + 2 - \xi^2 - 3\xi - 2 = 2\xi^2 \\ 2\xi^2 & \quad \textit{is a multiplicative representation; then} \\ \alpha' &= \xi^6 + 2\xi^2 \end{aligned}$$

4) $\alpha = \xi^5 + 2\alpha' = \xi^5 + 2\left(\xi^6 + 2\xi^2\right) = \xi^5 + 2\xi^6 + 2^2\xi^2 = \xi^5 + 2\xi^6 + 2^2\xi^2$.
So $\alpha = \varepsilon^{(5,6,2)}$. *And* $log_\varepsilon \alpha = (5, 6, 2)$.

For β*, one has:*

1) $\chi(\beta) = 1 + \chi(\xi^2) = \chi(\xi^3)$.

2) $\beta - \xi^3 = 1 + \xi^2 - \xi^3 = 1 + \xi^2 - 5\xi^2 - 6\xi - 1 = -4\xi^2 - 6\xi = 4\xi^2 + 2\xi$
The last equality gives the multiplicative representation of $\beta - \xi^3$.

3) $\beta = \xi^3 + 4\xi^2 + 2\xi = \xi^3 + 2\xi + 2^2\xi^2 = \xi^{(3,1,2)} = \varepsilon^{(3,1,2)}$.
So $\beta = \varepsilon^{(3,1,2)}$.
And $log_\varepsilon \alpha = (3, 1, 2)$.

4 Invertible elements in Galois rings

Lemma 4.1. *In the finite ring* $\mathbb{Z}_n$*,* $n \in \mathbb{N}$*, an element is either an invertible or a zero divisor.*

Proof. Set $A = \mathbb{Z}_n$, $n \geq 2$. Let $x \in A \setminus \{0\}$.
the multiplication mapping

$$\begin{array}{rccc} m_x : & A & \longrightarrow & A \\ & z & \longmapsto & xz \end{array}$$

is an endomorphism of Abelian groups.
If m_x is surjective, then $1 \in m_x(A)$.

So there is $y \in A$ such that $1 = xy$.
Then x is an invertible element in A.
If m_x is not surjective, then m_x is not injective since A is finite.
Therefore $ker(m_x) \neq \{0\}$.
So there is $z \in ker(m_x)$ such that $z \neq 0$; which means that $xz = 0$.
Then x is a zero divisor in A. □

Proposition 4.2. *The invertible elements in Galois rings $GR(p^k, m)$ are of the form:*

$$\xi^{(x_0, x_1, \cdots, x_{k-1})}, \text{ with } x_0 \neq -.$$

Proof. Let $\alpha = \xi^{(-, x_1, \cdots, x_{k-1})} \in GR(p^k, m)$. Then

$$\alpha = \xi^{x_1} p + \cdots + \xi^{x_{k-1}} p^{k-1} = p\left(\xi^{x_1} + \xi^{x_2} p + \cdots + \xi^{x_{k-1}} p^{k-2}\right),$$

is a zero divisor in $GR(p^k, m)$. When $x_0 \neq -$ in the tuple $(x_0, x_1, \cdots, x_{k-1})$, then α cannot be a zero divisor.
So it is invertible.
For all invertible element $\alpha = \xi^{(x_0, x_1, \cdots, x_{k-1})}$ in $GR(p^k, m)$, x_0 has to be different from $-$. □

5 Discrete logarithm problem in Galois rings

Definition 5.1. *Let $GR(p^k, m)$ be a Galois ring in which ξ in a root of the B-polynomial which generates $\mathcal{T}^*$; $\mathcal{T}$ is a Teichmüller set.*
The discrete logarithm problem (DLP) in Galois rings is the problem of finding the tuple $(x_0, x_1, \cdots, x_{k-1}) \in \{-, 0, 1, \cdots, p^m - 2\}^k$ such that $\alpha = \xi^{(x_0, x_1, \cdots, x_{k-1})}$ for a given α in $GR(p^k, m)$.
In other words, it is the problem of finding the discrete logarithm of a given α in $GR(p^k, m)$ in the basis ε.

It is difficult to compute the discrete logarithm x_i of ξ^{x_i} in the multiplicative group $\mathbb{F}_p(\xi)^\times$:
knowing as the discrete logarithm problem in finite groups. See [3]
So, moving from additive representations of elements in Galois rings to multiplicative representations is very difficult, since it is exactly the problem of solving discrete logarithm problem in some multiplicative groups $\mathbb{F}_p(\xi)^\times$; p prime of around 1024 bits. See [4] for more details.

6 Keys exchange

The following key exchange method is based on the Diffie-Hellman key exchange.
Let denoted by G a Galois ring $GR(p^k, m)$; $\mathcal{T}$ a Techmüller set. $\mathcal{T}^* = \langle \xi \rangle$.

Alice and Bob want to safely share a common key.

Alice chooses a tuple $X = (x_0, x_1, \cdots, x_{k-1})$ in $\{-, 0, 1, \cdots, p^m - 2\}^k$.
X is her private key.
She computes her public key $A = \xi^X \in G$, and sends the coordinates (in the additive form) of A: $(\xi^{x_0}, \xi^{x_1}, \cdots, \xi^{x_{k-1}})$ to Bob.

Set $(\xi^{x_i})_{0 \leq i \leq k-1} = (\xi^{x_0}, \xi^{x_1}, \cdots, \xi^{x_{k-1}}) = (\alpha_i)_{0 \leq i \leq k-1} = \alpha$.
$(\alpha_i)_{0 \leq i \leq k-1}$ is the additive form of $(\xi^{x_0}, \xi^{x_1}, \cdots, \xi^{x_{k-1}})$.

On his side, Bob does the same. He chooses a tuple $Y = (y_0, y_1, \cdots, y_{k-1})$ in $\{-, 0, 1, \cdots, p^m - 2\}^k$.
Y is his private key.
He computes his public key $B = \xi^Y \in G$, and sends the coordinates (in the additive form) of B: $(\xi^{y_0}, \xi^{y_1}, \cdots, \xi^{y_{k-1}}) = (\beta_i)_{0 \leq i \leq k-1} = \beta$ to Alice.

Therefore Alice and Bob now have the same key $K = \xi^Z$,
where $Z = (z_0, z_1, \cdots, z_{k-1}) \in \{-, 0, 1, \cdots, p^m - 2\}^k$.

Explanation:

When Alice receives β, she computes $\beta^X = (\beta_i^{x_i})_{0\leq i\leq k-1}$.

$$\beta^X = ((\xi^{y_i})^{x_i})_{0\leq i\leq k-1} = ((\xi^{x_i})^{y_i})_{0\leq i\leq k-1}\,.$$

$\forall i \in \{0, 1, \cdots, k-1\},\ x_i y_i$ is computed modulo $p^m - 1$.
β^X is the tuple which represents the coordinates of K.
After receiving Alice's public key, Bob does exactly the same computations as Alice did.
He computes $\alpha^Y = (\alpha_i^{y_i})_{0\leq i\leq k-1}$.

$$\alpha^Y = ((\xi^{x_i})^{y_i})_{0\leq i\leq k-1} = ((\xi^{y_i})^{x_i})_{0\leq i\leq k-1}\,,$$

which is the coordinates of K.

An eavesdropper who sees α and β of the additive form, will have difficulties to recover X and Y.
That is because it is an instance of the discrete logarithm problem in Galois rings $GR(p^k, m)$.

The same process is also applied in Galois rings $\mathbb{Z}_{p^k}$.

Table 1. Diffie Helman key exchange in Galois rings $GR(p^k, m)$

Alice	$GR(p^k, m)$	Bob
Private key: X X=$(x_0, x_1, \cdots, x_{k-1})$	$- - - \longrightarrow \xi^X$ $\xi^Y \longleftarrow - - -$	Private key: Y Y=$(y_0, y_1, \cdots, y_{k-1})$
$(\xi^Y)^X$	$(\xi^Y)^X = (\xi^X)^Y$	$(\xi^X)^Y$

6.1 Example

Example 6.2. *Alice and Bob want to use the Galois ring $GR(2^3, 2)$ to share common key.*
Alice chooses $(5, 6, 3)$ and computes:
$A = \xi^{(5,6,3)} = \xi^5 + 2\xi^6 + 2^2\xi^3$ *and sends to Bob the coordinates of A, (ξ^5, ξ^6, ξ^3) in their additive forms:*
$(2\xi^2 + 7\xi + 7,\ \xi^2 + 3\xi + 2,\ 5\xi^2 + 6\xi + 1)$.

Bob chooses $(3, 4, 6)$ and computes:
$B = \xi^{(3,4,6)} = \xi^3 + 2\xi^4 + 2^2\xi^6$ *and sends to Alice the coordinates of B, (ξ^3, ξ^4, ξ^6) in their additive forms:*
$(5\xi^2 + 6\xi + 1, 7\xi^2 + 7\xi + 5, \xi^2 + 3\xi + 2)$.

When Alice receives $(5\xi^2 + 6\xi + 1,\ 7\xi^2 + 7\xi + 5,\ \xi^2 + 3\xi + 2)$, she computes
$\Big(\big(5\xi^2 + 6\xi + 1\big)^5, \big(7\xi^2 + 7\xi + 5\big)^6, \big(\xi^2 + 3\xi + 2\big)^3\Big)$;
which is equal to $\big(\xi, \xi^3, \xi^4\big)$. It is the element $\xi^{(1,3,4)}$.

Likewise, When Bob receives $\big(2\xi^2 + 7\xi + 7,\ \xi^2 + 3\xi + 2,\ 5\xi^2 + 6\xi + 1\big)$, he computes
$\Big(\big(2\xi^2 + 7\xi + 7\big)^3, \big(\xi^2 + 3\xi + 2\big)^4, \big(5\xi^2 + 6\xi + 1\big)^6\Big)$;
which is equal to $\big(\xi, \xi^3, \xi^4\big)$.

So their common key is $\xi^{(1,3,4)}$.

Example 6.3. *Alice and Bob want to use the Galois ring $\mathbb{Z}_{25}$ to share common key.*
Alice chooses $(2, 3)$ and computes:
$A = 3^{(2,3)} = 3^2 + 3^3 \times 5 = 4 + 2 \times 5 = 14$ *and sends to Bob the coordinates of 14: $(3^2, 3^3)$ in their additive forms: $(4, 2)$.*

Bob chooses $(3, 2)$ and computes:
$B = 3^{(3,2)} = 3^3 + 3^2 \times 5 = 2 + 4 \times 5 = 22$ *and sends to Alice the coordinates of 22: $(3^3, 3^2)$ in their additive forms: $(2, 4)$.*

When Alice receives $(2, 4)$, she computes $(2^2, 4^3) \mod 5$;
which is equal to $(4, 4)$. It is the element $= 4 + 4 \times 5 = 24$.
Likewise, When Bob receives $(4, 2)$, he computes
$(4^3, 2^2) \mod 5 = (4, 4)$;

which is equal to $4 + 4 \times 5 = 24$.
So their common key is 24.

7 ElGamal encryption in Galois rings

The concept of ElGamal encryption can be transfered from finite fields $\mathbb{F}_p(\xi)$ to Galois rings $GR(p^k, m)$.

Alice (A) and Bob (B) want to use ElGamal encryption in Galois rings.
Public parameters: A Galois ring $GR(p^k, m)$; a basis ε.

1) A chooses a random tuple $X_a = (x_0, x_1, \cdots, x_{k-1})$ in $\{-, 0, 1, \cdots, p^m - 2\}^k$ such that $x_0 \neq -$.
X_a is the private key of A.

2) A computes $K_a = \varepsilon^{X_a}$ in $GR(p^k, m)$ and broadcasts it.
K_a is the public key of A.

3) B wants to send a message M to A.
M is assumed to be an element in $GR(p^k, m)$.
B picks a random tuple $Y = (y_0, y_1, \cdots, y_{k-1})$ in $\{-, 0, 1, \cdots, p^m - 2\}^k$ such that $y_0 \neq -$.
B sends the cipher text $C = \left[\varepsilon^Y, M \cdot K_a^Y\right]$ to A in the additive form.
ε^Y is the Bob's puplic key.

4) A receives C and A can recover the message M because of the following computations:

$$\begin{aligned} M \cdot K_a^Y \cdot \left(\left(\varepsilon^Y\right)^{X_a}\right)^{-1} &= M \cdot \left(\varepsilon^{X_a}\right)^Y \cdot \left(\left(\varepsilon^Y\right)^{X_a}\right)^{-1} \\ &= M \cdot \left(\varepsilon^{X_a}\right)^Y \cdot \left(\left(\varepsilon^{X_a}\right)^Y\right)^{-1} \\ &= M. \end{aligned}$$

$\left(\varepsilon^{X_a}\right)^Y$ is invertible since $x_0 \neq -$ and $y_0 \neq -$.
And the second equality holds because $\left(\varepsilon^{X_a}\right)^Y = \left(\varepsilon^Y\right)^{X_a}$.

Example 7.1. *In the Galois ring* $GR(2^2, 2)$, $\xi^2 + \xi + 1 = 0$.
Alice (A) and Bob (B) want to use ElGamal encryption.

1) A chooses $X_a = (2, 1)$*;*

2) $K_a = \xi^{(2,1)} = \xi^2 + 2\xi$*;*

3) B is about to send a message $M_1 = \xi$ *and* $M_2 = 1 + \xi$ *to A.*
B picks a random $Y = (1, 2)$ *and sends* $C_1 = \left[\xi^Y, M_1 \cdot K_a^Y\right]$ *and* $C_2 = \left[\xi^Y, M_2 \cdot K_a^Y\right]$ *to A.*
$\xi^Y = \xi^{(1,2)} = \xi + 2\xi^2$*;*
$K_a^Y = \left(\xi^{X_a}\right)^Y = \left(\xi^2 + 2\xi\right)^{(1,2)} = \xi^2 + 2\xi^2$

$M_1 \cdot K_a^Y = \xi\left(\xi^2 + 2\xi^2\right) = \xi^3 + 2\xi^3 = 1 + 2 = 3$.
Then $C_1 = \left[\xi + 2\xi^2, 3\right]$.

$M_2 \cdot K_a^Y = (1 + \xi)\left(\xi^2 + 2\xi^2\right) = \xi^2 + 2\xi^2 + \xi^3 + 2\xi^3 = 3\xi^2 + 3$.
Then $C_2 = \left[\xi + 2\xi^2, 3\xi^2 + 3\right]$.

4) A receives C_1, C_2 *and computes* $M_1 \cdot K_a^Y \cdot \left(\left(\xi^Y\right)^{X_a}\right)^{-1}$ *and* $M_2 \cdot K_a^Y \cdot \left(\left(\xi^Y\right)^{X_a}\right)^{-1}$.
$\left(\xi + 2\xi^2\right)^{X_a} = \left(\xi + 2\xi^2\right)^{(2,1)} = \xi^2 + 2\xi^2 = \left(\xi^Y\right)^{X_a}$.

A computes the inverse $a+b\xi$ *of* $\left(\xi^Y\right)^{X_a}$*:*

$$\begin{aligned} 1=\left(\xi^2+2\xi^2\right)(a+b\xi) &= (1+\xi)(a+b\xi) \\ &= a+(a+b)\xi+b\xi^2 \\ &= a+(a+b)\xi+b(3+3\xi) \\ &= a+3b+(a+4b)\xi \end{aligned}$$

Then $a=0$ *and* $b=3$*. So the inverse of* $\xi^2+2\xi^2$ *is* 3ξ*.*
Finally, the messages were $M_1=3\times(3\xi)=\xi$*.*
And $M_2=(3\xi^2+3)(3\xi)=\xi^3+\xi=1+\xi$*.*

Example 7.2. *In the Galois ring* $\mathbb{Z}_{7^2}$*, choose for example* $g=3$*.*
And a generator of $\mathbb{Z}_{7^2}$ *is* $b=3^{(1,1)}=3+3\times 7=24$*.*
Alice (A) and Bob (B) want to use ElGamal encryption.

1) A chooses $X_a=(4,3)$*;*

2) $K_a=3^{(4,3)}=3^4+3^3\times 7=4+6\times 7=46$*;*

3) B wants to send a message $M=45$ *to A.*
B picks a random $Y=(2,5)$ *and sends* $C=\left[3^Y, M\cdot K_a^Y\right]$ *to A.*
$3^Y=3^{(2,5)}=3^2+3^5\times 7=2+5\times 7=37$*;*
$K_a^Y=(46)^Y=4^2+6^5\times 7=3^2+3^3\times 7=2+6\times 7=44$*.*

$M\cdot K_a^Y=45\times 44 \mod 49=20$*. Then* $C=[37,20]$*.*

4) A receives C and computes $M\cdot K_a^Y\cdot\left(\left(b^Y\right)^{X_a}\right)^{-1}$
$(37)^{X_a}=\left(3^2+3^5\times 7\right)^{(4,3)}=3^2+3^3\times 7=2+6\times 7=44$*.*
A computes the inverse of 44 *and finds* 39*:*
Finally, the message was $M=20\times 39=45$*.*

8 Conclusion

In this paper, it is explained how one can use Galois rings to perform ElGamal encryption through the concept of the discrete logarithm and the generators. That encryption is based on the Diffie-Hellman key exchange and it was made possible thanks to Teichmüller sets. With such sets, the multiplicative representation of elements in Galois rings $\left(GR(p^k,m)\right)$ allows to express each element $\alpha\in GR(p^k,m)$ in the form: $\alpha=\xi^{(x_0,x_1,\cdots,x_k)}$, where $(x_0,x_1,\cdots,x_k)$ is called the discrete logarithm of α in the basis $\varepsilon=\xi^{(1,1,\cdots,1)}$, which is a generator of the Galois ring $\left(GR(p^k,m)\right)$.

REFERENCES

[1] Micheal Calder bank. An introduction to linear and cyclic codes. *Lecture*, 22 August 2008.

[2] John C. Bowman. Coding theory and cryptograhy. *University of Alberta, Edmonton Canada*, 2015.

[3] Johannes Buchmann. Introduction à la cryptographie. *Dunod*, Avril 2006.

[4] Renaud Dumont. Cryptographie et sécurité informatique. *Université de liège*, 2010.

[5] Fabien Galand. Codes $\mathbb{Z}_{2^k}$-lineaires. *Institut National de Recherche en Informatique et en Automatique; numero 5073; Rapport de recherche*, Janvier 2004.

[6] Wade Trappe; Wireless Information Network Laboratory, the Electrical, and Lawrence C. Washington Department of Mathematics University of Maryland Computer Engineering Department, Rutgers University. Introduction to cryptography with coding theory. *Pearson Education International*, page Second edition, 2006.

[7] Keijo Ruohonen. Mathematical gryptology. *Translation: Jussi Kangas and Paul Coughlan*, 2014.

[8] Jean-Pierre Serre. Groupes finis. *Cours à l'École Normale Supérieur de Jeunes filles*, Montrouge, 1979.

[9] L. Washington. Elliptic curves: Number theory and cryptography. *Chapman and Han/CRC Press*, 2003.