Lattices from Totally Real Number Fields with Large Regulator

Ong Soon Sheng

Division of Mathematical Sciences
Nanyang Technological University(NTU), Singapore
(Joint work with Prof. Frédérique Oggier, NTU, Singapore)

April 18, 2013

WCC 2013: International Workshop on Coding and Cryptography

Bergen, Norway

Outline

- Introduction
  - Coding Strategy for the Wiretap Rayleigh Fading Channel
  - Code Design Criterion
- Ideal Lattices
- Some Number fields with Prescribed Ramification
  - Norms and Ramification
- Units and Regulator
- Conclusion

Introduction

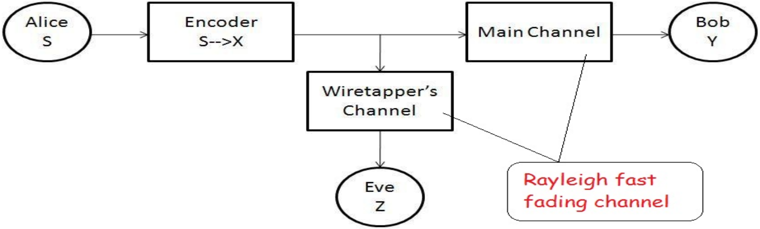

Figure : Wiretap Channel

Introduction

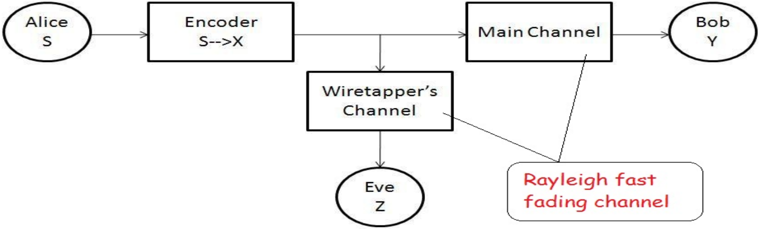

Figure : Wiretap Channel

Goals of coding for a wiretap channel:

Introduction

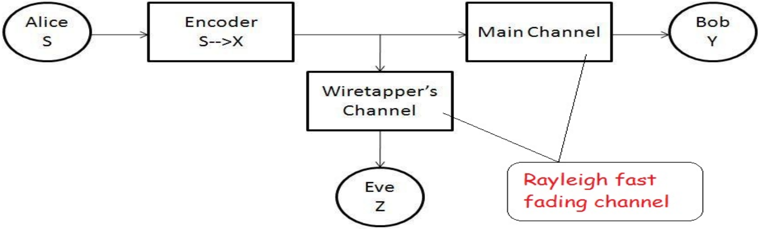

Figure : Wiretap Channel

Goals of coding for a wiretap channel:

- to increase reliability for Bob

Introduction

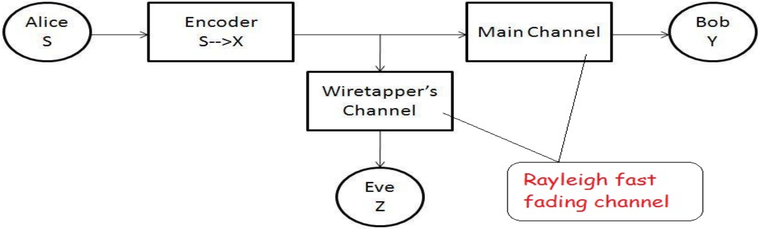

Figure : Wiretap Channel

Goals of coding for a wiretap channel:

- to increase reliability for Bob
- to increase confidentiality for Bob

Coding Strategy for the Wiretap Rayleigh Fading Channel

Coset encoding:

Coding Strategy for the Wiretap Rayleigh Fading Channel

Coset encoding:a sublattice Λ_e of Λ_b and partition Λ_b into a union of disjoint cosets of the form

$$\Lambda_e + \mathbf{c}$$

where $\mathbf{c} = (c_1, c_2, ..., c_n) \in \Lambda_b \subset \mathbb{R}^n$.

Coding Strategy for the Wiretap Rayleigh Fading Channel

Coset encoding:a sublattice Λ_e of Λ_b and partition Λ_b into a union of disjoint cosets of the form

$$\Lambda_e + \mathbf{c}$$

where $\mathbf{c} = (c_1, c_2, ..., c_n) \in \Lambda_b \subset \mathbb{R}^n$.

The message intended for Bob, s is labelled by $s \mapsto \Lambda_e + \mathbf{c}_{(\mathbf{s})}$.

Coding Strategy for the Wiretap Rayleigh Fading Channel

Coset encoding:a sublattice Λ_e of Λ_b and partition Λ_b into a union of disjoint cosets of the form

$$\Lambda_e + \mathbf{c}$$

where $\mathbf{c} = (c_1, c_2, ..., c_n) \in \Lambda_b \subset \mathbb{R}^n$.

The message intended for Bob, s is labelled by $s \mapsto \Lambda_e + \mathbf{c}_{(\mathbf{s})}$.

Lattice encoding: The transmitted lattice point $\mathbf{x} \in \Lambda_e + \mathbf{c}_{(\mathbf{s})} \subset \Lambda_b$ is chosen randomly.

Coding Strategy for the Wiretap Rayleigh Fading Channel

Coset encoding:a sublattice Λ_e of Λ_b and partition Λ_b into a union of disjoint cosets of the form

$$\Lambda_e + \mathbf{c}$$

where $\mathbf{c} = (c_1, c_2, ..., c_n) \in \Lambda_b \subset \mathbb{R}^n$.

The message intended for Bob, s is labelled by $s \mapsto \Lambda_e + \mathbf{c}_{(\mathbf{s})}$.

Lattice encoding: The transmitted lattice point $\mathbf{x} \in \Lambda_e + \mathbf{c}_{(\mathbf{s})} \subset \Lambda_b$ is chosen randomly.

$$\mathbf{x} = \mathbf{r} + \mathbf{c}_{(\mathbf{s})} \in \Lambda_e + \mathbf{c}_{(\mathbf{s})}$$

Coding Strategy for the Wiretap Rayleigh Fading Channel

Coset encoding:a sublattice Λ_e of Λ_b and partition Λ_b into a union of disjoint cosets of the form

$$\Lambda_e + \mathbf{c}$$

where $\mathbf{c} = (c_1, c_2, ..., c_n) \in \Lambda_b \subset \mathbb{R}^n$.

The message intended for Bob, s is labelled by $s \mapsto \Lambda_e + \mathbf{c}_{(\mathbf{s})}$.

Lattice encoding: The transmitted lattice point $\mathbf{x} \in \Lambda_e + \mathbf{c}_{(\mathbf{s})} \subset \Lambda_b$ is chosen randomly.

$$\mathbf{x} = \mathbf{r} + \mathbf{c}_{(\mathbf{s})} \in \Lambda_e + \mathbf{c}_{(\mathbf{s})} \Leftrightarrow \text{random vector } \mathbf{r} \in \Lambda_e$$

Code Design Criterion

(J.C. Belfiore and F.Oggier, 2011)

$$\bar{P}_{c,e} \approx (\frac{\gamma_e}{4})^{\frac{n}{2}} \text{Vol}(\Lambda_b) \frac{1}{\gamma_e^{\frac{3}{2}d_{\mathbf{x}}}} \sum_{\mathbf{x}\in\Lambda_e, \mathbf{x}\neq 0} \prod_{x_i \neq 0} \frac{1}{|x_i|^3}$$

where

Λ_b (resp.Λ_e) is the lattice intended for Bob (resp.Eve),
γ_e is Eve's average Signal to Noise Ratio(SNR),
$\mathbf{x} = (x_1, x_2, ..., x_n)$,
Vol(Λ_b) is the volume of Λ_b,
$d_{\mathbf{x}} = |\{x_i : x_i \neq 0\}|$ is the minimum diversity of $\mathbf{x}$.

Code Design Criterion

(J.C. Belfiore and F.Oggier, 2011)

$$\bar{P}_{c,e} \approx (\frac{\gamma_e}{4})^{\frac{n}{2}} \text{Vol}(\Lambda_b) \frac{1}{\gamma_e^{\frac{3}{2}d_{\mathbf{x}}}} \sum_{\mathbf{x}\in\Lambda_e, \mathbf{x}\neq 0} \prod_{x_i \neq 0} \frac{1}{|x_i|^3}$$

where
Λ_b (resp.Λ_e) is the lattice intended for Bob (resp.Eve),
γ_e is Eve's average Signal to Noise Ratio(SNR),
$\mathbf{x} = (x_1, x_2, ..., x_n)$,
Vol(Λ_b) is the volume of Λ_b,
$d_{\mathbf{x}} = |\{x_i : x_i \neq 0\}|$ is the minimum diversity of $\mathbf{x}$.

Coding criterion:

To minimize

$$\sum_{\mathbf{x}\in\Lambda_e, \mathbf{x}\neq 0} \prod_{x_i \neq 0} \frac{1}{|x_i|^3}$$

Ideal Lattices

Let K be a totally real number field of degree n, with ring of integers $\mathcal{O}_K$, and real embeddings $\sigma_1, ..., \sigma_n$.

Ideal Lattices

Let K be a totally real number field of degree n, with ring of integers $\mathcal{O}_K$, and real embeddings $\sigma_1, ..., \sigma_n$.

If $\{\omega_1, \dots, \omega_n\}$ is a $\mathbb{Z}$-basis of $\mathcal{I}$, the generator matrix M of the corresponding ideal lattice $(\mathcal{I}, q_\alpha) = \{\mathbf{x} = \mathbf{u}M | \mathbf{u} \in \mathbb{Z}^n\}$ is given by

$$M = \begin{pmatrix} \sqrt{\alpha_1}\sigma_1(\omega_1) & \sqrt{\alpha_2}\sigma_2(\omega_1) & \dots & \sqrt{\alpha_n}\sigma_n(\omega_1) \\ \vdots & \vdots & \dots & \vdots \\ \sqrt{\alpha_1}\sigma_1(\omega_n) & \sqrt{\alpha_2}\sigma_2(\omega_n) & \dots & \sqrt{\alpha_n}\sigma_n(\omega_n) \end{pmatrix}$$

where $\alpha_j = \sigma_j(\alpha)$, for all j.

Ideal Lattices

$\mathbf{x} = (x_1, \ldots, x_n) = (\sqrt{\alpha_1}\sigma_1(x), \ldots, \sqrt{\alpha_n}\sigma_n(x))$ for some $x = \sum_{i=1}^{n} u_i\omega_i \in \mathcal{I} \subseteq \mathcal{O}_K$ where $(u_1, ..., u_n) \in \mathbb{Z}^n$.

Ideal Lattices

$\mathbf{x} = (x_1, \ldots, x_n) = (\sqrt{\alpha_1}\sigma_1(x), \ldots, \sqrt{\alpha_n}\sigma_n(x))$ for some $x = \sum_{i=1}^{n} u_i\omega_i \in \mathcal{I} \subseteq \mathcal{O}_K$ where $(u_1, ..., u_n) \in \mathbb{Z}^n$.

$$\sum_{\mathbf{x} \in \Lambda_e} \prod_{x_i \neq 0} \frac{1}{|x_i|^3}$$

Ideal Lattices

$\mathbf{x} = (x_1, \ldots, x_n) = (\sqrt{\alpha_1}\sigma_1(x), \ldots, \sqrt{\alpha_n}\sigma_n(x))$ for some $x = \sum_{i=1}^{n} u_i \omega_i \in \mathcal{I} \subseteq \mathcal{O}_K$ where $(u_1, ..., u_n) \in \mathbb{Z}^n$.

$$\sum_{\mathbf{x} \in \Lambda_e} \prod_{x_i \neq 0} \frac{1}{|x_i|^3} = \sum_{x \in \mathcal{I}, x \neq 0} \prod_{i=1}^{n} \frac{1}{(\sqrt{\alpha_i})^3 |\sigma_i(x)|^3}$$

Ideal Lattices

$\mathbf{x} = (x_1, \ldots, x_n) = (\sqrt{\alpha_1}\sigma_1(x), \ldots, \sqrt{\alpha_n}\sigma_n(x))$ for some $x = \sum_{i=1}^{n} u_i\omega_i \in \mathcal{I} \subseteq \mathcal{O}_K$ where $(u_1, ..., u_n) \in \mathbb{Z}^n$.

$$\sum_{\mathbf{x}\in\Lambda_e} \prod_{x_i \neq 0} \frac{1}{|x_i|^3} = \sum_{x\in\mathcal{I}, x\neq 0} \prod_{i=1}^{n} \frac{1}{(\sqrt{\alpha_i})^3 |\sigma_i(x)|^3}$$

$$= \sum_{x\in\mathcal{I}, x\neq 0} \frac{1}{(N_{K/\mathbb{Q}}(\alpha))^{\frac{3}{2}} |N_{K/\mathbb{Q}}(x)|^3}$$

where $\alpha_j = \sigma_j(\alpha)$, for all j and $N_{K/\mathbb{Q}}(\beta) = \prod_{i=1}^{n} \sigma_i(\beta)$ for $\beta \in K$.

Ideal Lattices

In addition to K as a totally real number field,

Ideal Lattices

In addition to K as a totally real number field,

- K is a Galois extension.
- Class number of K is 1.

Ideal Lattices

In addition to K as a totally real number field,

- K is a Galois extension.
- Class number of K is 1.

Thus $x' \in \mathcal{I} = (\beta)\mathcal{O}_K$, $N_{K/\mathbb{Q}}(x') = N_{K/\mathbb{Q}}(\beta)N_{K/\mathbb{Q}}(x)$ for some $x \in \mathcal{O}_K$.

Ideal Lattices

In addition to K as a totally real number field,

- K is a Galois extension.
- Class number of K is 1.

Thus $x' \in \mathcal{I} = (\beta)\mathcal{O}_K$, $N_{K/\mathbb{Q}}(x') = N_{K/\mathbb{Q}}(\beta)N_{K/\mathbb{Q}}(x)$ for some $x \in \mathcal{O}_K$.

Hence,

$$\sum_{x' \in \mathcal{I}, x' \neq 0} \frac{1}{|N_{K/\mathbb{Q}}(x')|^3} \Rightarrow \sum_{x \in \mathcal{O}_K, x \neq 0} \frac{1}{|N_{K/\mathbb{Q}}(x)|^3}. \tag{1}$$

$$
\begin{aligned}
\sum_{x\in\mathcal{O}_K, x\neq 0} \frac{1}{|N_{K/\mathbb{Q}}(x)|^3} &= \frac{A_1}{1^3} + \frac{A_2}{2^3} + \frac{A_{2^2}}{(2^2)^3} + \frac{A_{2^3}}{(2^3)^3} + \ldots \\
&+ \frac{A_3}{3^3} + \frac{A_{3^2}}{(3^2)^3} + \frac{A_{3^3}}{(3^3)^3} + \ldots \\
&+ \frac{A_5}{5^3} + \frac{A_{5^2}}{(5^2)^3} + \frac{A_{5^3}}{(5^3)^3} + \ldots \\
&+ \frac{A_7}{7^3} + \frac{A_{7^2}}{(7^2)^3} + \frac{A_{7^3}}{(7^3)^3} + \ldots
\end{aligned}
$$

where A_i refers to number of algebraic integers with a norm of $\pm i$.

In practice, we consider finite constellation so that only finitely many integers are considered in the sum.

In practice, we consider finite constellation so that only finitely many integers are considered in the sum.

Instead we will consider in analysing the following

$$\sum_{x \in \mathcal{O}_K \cap \mathcal{R}, x \neq 0} \frac{1}{|N_{K/\mathbb{Q}}(x)|^3}$$

where $\mathcal{R}$ decides the shape of the finite constellation.

Norms and Ramification

Norms and Ramification

Dominant terms in $\sum_{x \in \mathcal{O}_K \cap \mathcal{R}, x \neq 0} \frac{1}{|N_{K/\mathbb{Q}}(x)|^3}$ are those integers with small norms and units.

Norms and Ramification

Dominant terms in $\sum_{x \in \mathcal{O}_K \cap \mathcal{R}, x \neq 0} \frac{1}{|N_{K/\mathbb{Q}}(x)|^3}$ are those integers with small norms and units.

Integers with norms at least 2 depend on

Norms and Ramification

Dominant terms in $\sum_{x \in \mathcal{O}_K \cap \mathcal{R}, x \neq 0} \frac{1}{|N_{K/\mathbb{Q}}(x)|^3}$ are those integers with small norms and units.

Integers with norms at least 2 depend on

- ramification in K
- the class number of K
- density of units

Norms and Ramification

Let p be a prime, then $p \in p\mathcal{O}_K$.

Norms and Ramification

Let p be a prime, then $p \in p\mathcal{O}_K$.

$$N(p\mathcal{O}_K) = N(\prod_{i=1}^{g} \mathfrak{p}_i^{e_i}) = \prod_{i=1}^{g} N(\mathfrak{p}_i)^{e_i} = |N_{K/\mathbb{Q}}(p)| = p^n$$

where all $\mathfrak{p}_i$ are distinct prime ideals and $e_i = e$ for all i.

Norms and Ramification

Let p be a prime, then $p \in p\mathcal{O}_K$.

$$N(p\mathcal{O}_K) = N(\prod_{i=1}^{g} \mathfrak{p}_i^{e_i}) = \prod_{i=1}^{g} N(\mathfrak{p}_i)^{e_i} = |N_{K/\mathbb{Q}}(p)| = p^n$$

where all $\mathfrak{p}_i$ are distinct prime ideals and $e_i = e$ for all i.

In particular, if p is totally ramified($g = 1$ and $e_1 = n$) or if p totally splits($g = n$ and $e = 1$), then

Norms and Ramification

Let p be a prime, then $p \in p\mathcal{O}_K$.

$$N(p\mathcal{O}_K) = N(\prod_{i=1}^{g} \mathfrak{p}_i^{e_i}) = \prod_{i=1}^{g} N(\mathfrak{p}_i)^{e_i} = |N_{K/\mathbb{Q}}(p)| = p^n$$

where all $\mathfrak{p}_i$ are distinct prime ideals and $e_i = e$ for all i.

In particular, if p is totally ramified($g = 1$ and $e_1 = n$) or if p totally splits($g = n$ and $e = 1$), then

$$N(\mathfrak{p})^n = p^n, \text{ or } \prod_{i=1}^{n} N(\mathfrak{p}_i) = p^n.$$

Norms and Ramification

Let p be a prime, then $p \in p\mathcal{O}_K$.

$$N(p\mathcal{O}_K) = N(\prod_{i=1}^{g} \mathfrak{p}_i^{e_i}) = \prod_{i=1}^{g} N(\mathfrak{p}_i)^{e_i} = |N_{K/\mathbb{Q}}(p)| = p^n$$

where all $\mathfrak{p}_i$ are distinct prime ideals and $e_i = e$ for all i.

In particular, if p is totally ramified($g = 1$ and $e_1 = n$) or if p totally splits($g = n$ and $e = 1$), then

$$N(\mathfrak{p})^n = p^n, \text{ or } \prod_{i=1}^{n} N(\mathfrak{p}_i) = p^n.$$

This shows the existence of an ideal above p of norm p.

Norms and Ramification

Let p be a prime, then $p \in p\mathcal{O}_K$.

$$N(p\mathcal{O}_K) = N(\prod_{i=1}^{g} \mathfrak{p}_i^{e_i}) = \prod_{i=1}^{g} N(\mathfrak{p}_i)^{e_i} = |N_{K/\mathbb{Q}}(p)| = p^n$$

where all $\mathfrak{p}_i$ are distinct prime ideals and $e_i = e$ for all i.

In particular, if p is totally ramified($g = 1$ and $e_1 = n$) or if p totally splits($g = n$ and $e = 1$), then

$$N(\mathfrak{p})^n = p^n, \text{ or } \prod_{i=1}^{n} N(\mathfrak{p}_i) = p^n.$$

This shows the existence of an ideal above p of norm p.

We can further identify a generator with norm p.

Norms and Ramification

Moreover, if we have $e = g = 1$, we will force the smallest norm involving only the prime p to be at least p^n.

Norms and Ramification

Moreover, if we have $e = g = 1$, we will force the smallest norm involving only the prime p to be at least p^n.

This kind of prime p, we call it inert prime and it is desirable to have those smaller primes remain inert.

Norms and Ramification

Moreover, if we have $e = g = 1$, we will force the smallest norm involving only the prime p to be at least p^n.

This kind of prime p, we call it inert prime and it is desirable to have those smaller primes remain inert.

Example

If 2 is inert prime, then $x \in \mathcal{O}_K$ with $N(x) = 2^k$ for $k \geq n$.

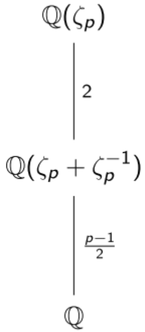

Figure : Cyclotomic Field and its Maximal Real Subfield

Theorem

(D.A.Marcus,1977)
Let q *be a rational prime different from* p, *then* q *is unramified in* $\mathbb{Q}(\zeta_p)$ *and in fact*

$$(q)\mathbb{Z}[\zeta_p] = \mathfrak{q}_1 ... \mathfrak{q}_g$$

with mutually distinct prime ideals $\mathfrak{q}_i$ *and each of inertial degree* $f = f(\mathfrak{q}_i/q)$ *equal to the order of* q *in* $(\mathbb{Z}/p)^\times$*,i.e.,* f *is the least natural number such that*

$$q^f \equiv 1 \pmod p.$$

Consider the special case when $p = 2p' + 1$, with p' a prime.

Consider the special case when $p = 2p' + 1$, with p' a prime.

Lemma

Suppose that $p = 2p' + 1$, where both p and p' are prime (such a prime p' is called a Sophie Germain prime). Then the primes smaller than p are inert in $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$.

Consider the special case when $p = 2p' + 1$, with p' a prime.

Lemma

Suppose that $p = 2p' + 1$, where both p and p' are prime (such a prime p' is called a Sophie Germain prime). Then the primes smaller than p are inert in $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$.

Example

Consider $\mathbb{Q}(\zeta_{23})$, with $23 = 2 \cdot 11 + 1$. The primes 2, 3, 5, 7, 11, 13, 17, 19 are all inert in $\mathbb{Q}(\zeta_{23} + \zeta_{23}^{-1})$.

Units and Regulator

Let L be a number field of degree n and signature (r_1, r_2). Set $r = r_1 + r_2 - 1$. The density of units in K is related to its regulator R.

Units and Regulator

Let L be a number field of degree n and signature (r_1, r_2). Set $r = r_1 + r_2 - 1$. The density of units in K is related to its regulator R.

Definition

Given a basis $e_1, \ldots, e_r$ for the group of units modulo the group of roots of unity. The *regulator* of K is

$$R = |\det(\log|\sigma_i(e_j)|)_{1 \leq i,j \leq r}|,$$

where $|\sigma_i(e_j)|$ denotes the absolute value for the real embeddings, and the square of the complex absolute value for the complex ones.

Theorem

(G.R.Everest, J.H.Loxton, 1993)
Let w be the number of roots of unity in L. The number of units $U(q)$ such that $\max_{1\le i\le d}|\sigma_i(u)| < q$ in K is given by

$$U(q) = \frac{w(r+1)^r}{Rr!}(\log q)^r + O((\log q)^{r-1-(cR^{2/r})^{-1}})$$

as $q \to \infty$ and $c = 6 \cdot 2 \times 10^{12} d^{10}(1 + 2\log d)$.

Table : Some totally real number fields K of Cyclotomic Fields.

$K \subset \mathbb{Q}(\zeta_p)$	R	$p(X)$	primes
$\mathbb{Q}(\zeta_{11})$	1.63	$x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1$	11 ramifies
$\mathbb{Q}(\zeta_{31})$	30.36	$x^5 - 9x^4 + 20x^3 - 5x^2 - 11x - 1$	5 splits
$\mathbb{Q}(\zeta_{41})$	123.32	$x^5 - x^4 - 16x^3 - 5x^2 + 21x + 9$	3 splits
$\mathbb{Q}(\zeta_{23})$	1014.31	$x^{11} + x^{10} - 10x^9 - 9x^8 + 36x^7 + 28x^6$	
		$-56x^5 - 35x^4 + 35x^3 + 15x^2 - 6x - 1$	23 ramifies
$\mathbb{Q}(\zeta_{67})$	330512.24	$x^{11} - x^{10} - 30x^9 + 63x^8 + 220x^7 - 698x^6$	
		$-101x^5 + 1960x^4 - 1758x^3 + 35x^2 + 243x + 29$	29 splits

Table : Some totally real number fields K of Cyclotomic Fields.

$K \subset \mathbb{Q}(\zeta_p)$	R	$p(X)$	primes
$\mathbb{Q}(\zeta_{11})$	1.63	$x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1$	11 ramifies
$\mathbb{Q}(\zeta_{31})$	30.36	$x^5 - 9x^4 + 20x^3 - 5x^2 - 11x - 1$	5 splits
$\mathbb{Q}(\zeta_{41})$	123.32	$x^5 - x^4 - 16x^3 - 5x^2 + 21x + 9$	3 splits
$\mathbb{Q}(\zeta_{23})$	1014.31	$x^{11} + x^{10} - 10x^9 - 9x^8 + 36x^7 + 28x^6$ $-56x^5 - 35x^4 + 35x^3 + 15x^2 - 6x - 1$	23 ramifies
$\mathbb{Q}(\zeta_{67})$	330512.24	$x^{11} - x^{10} - 30x^9 + 63x^8 + 220x^7 - 698x^6$ $-101x^5 + 1960x^4 - 1758x^3 + 35x^2 + 243x + 29$	29 splits

For the case of degree 5,

$$\frac{2 \cdot 5^4}{4!R}(\log q)^4 = \frac{625}{12R}(\log q)^4$$

yielding respectively

$$\sim 32(\log q)^4, \quad \sim 0.4(\log q)^4$$

for the smallest and biggest regulators shown in Table 1.

Conclusion

- Code design criterion for fast fading channel is analysed in designing the lattice code that provides confusion to the eavedropper.

Conclusion

- Code design criterion for fast fading channel is analysed in designing the lattice code that provides confusion to the eavedropper.
- Identifying totally real number fields with prescribed ramification and regulator provide some thought in the design of wiretap codes for fast fading channels.

$\sim$ Thank you for your attention! $\sim$