Gaussian Wiretap Codes

Fuchun Lin (Joint work with
Frédérique Oggier)

School of Physical and Mathematical Sciences,

Nanyang Technological University, Singapore

ITW 2011, Paraty

Outline

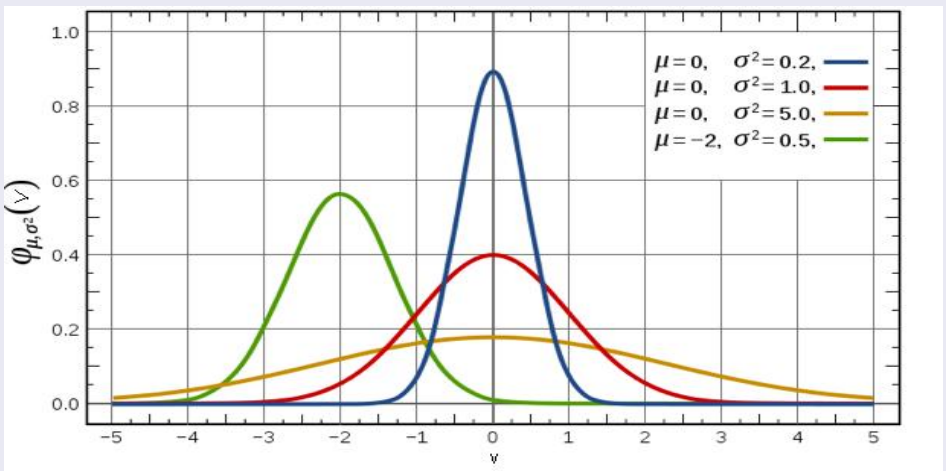
1. Introduction: Secrecy Gain, a new code design criterion
2. Main results: Codes from unimodular lattices
3. Future Work: Codes from modular lattices

Additive White Gaussian Noise channel

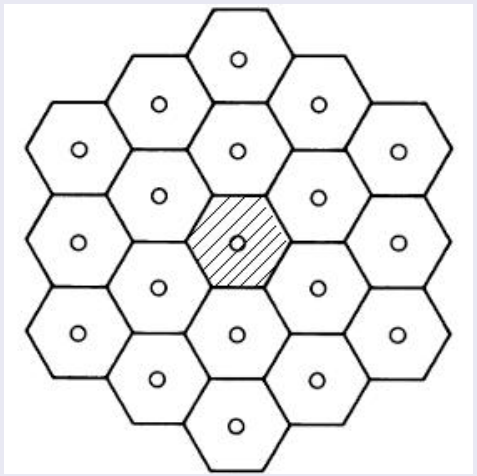
Channel model:

$$\mathbf{y} = \mathbf{x} + \mathbf{v},$$

every component of $\mathbf{v}$ is i.i.d. and drawn from a zero-mean Gaussian distribution with variance σ: $\varphi_{0,\sigma^2}(v) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{v^2}{2\sigma^2}}$



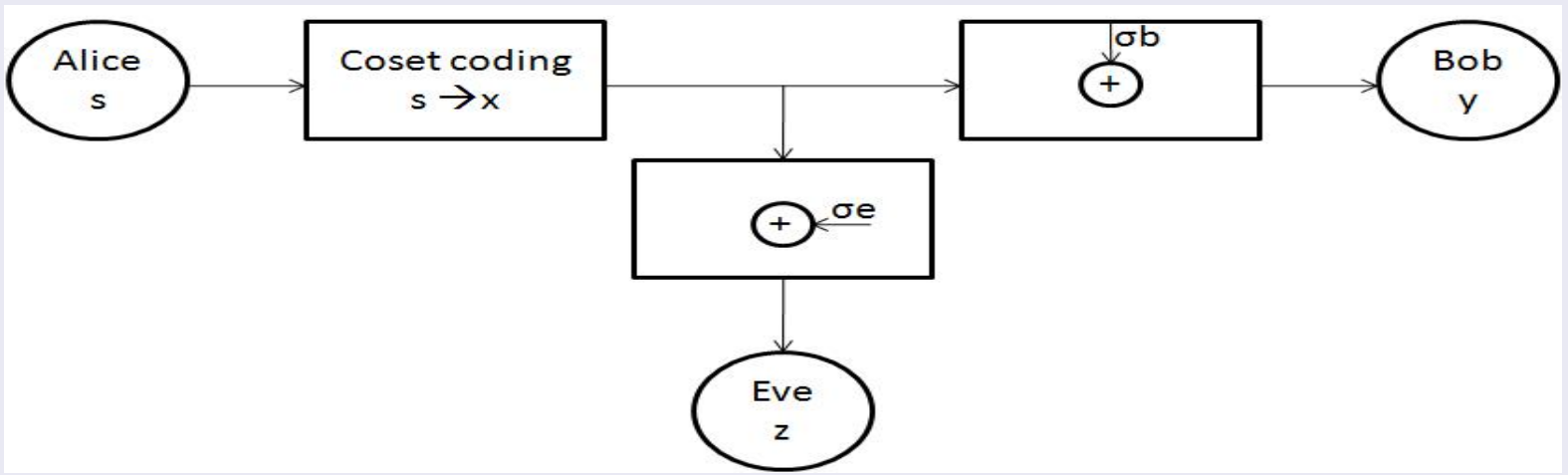
Probability of correct dicision



y falls in $\mathcal{V}_\Lambda(\mathbf{x})$, the **Voronoi cell** of **x**:

$$P_c = \frac{1}{(\sigma\sqrt{2\pi})^2} \int_{\mathcal{V}_\Lambda(\mathbf{x})} e^{-||\mathbf{y}-\mathbf{x}||^2/2\sigma^2} d\mathbf{y}$$

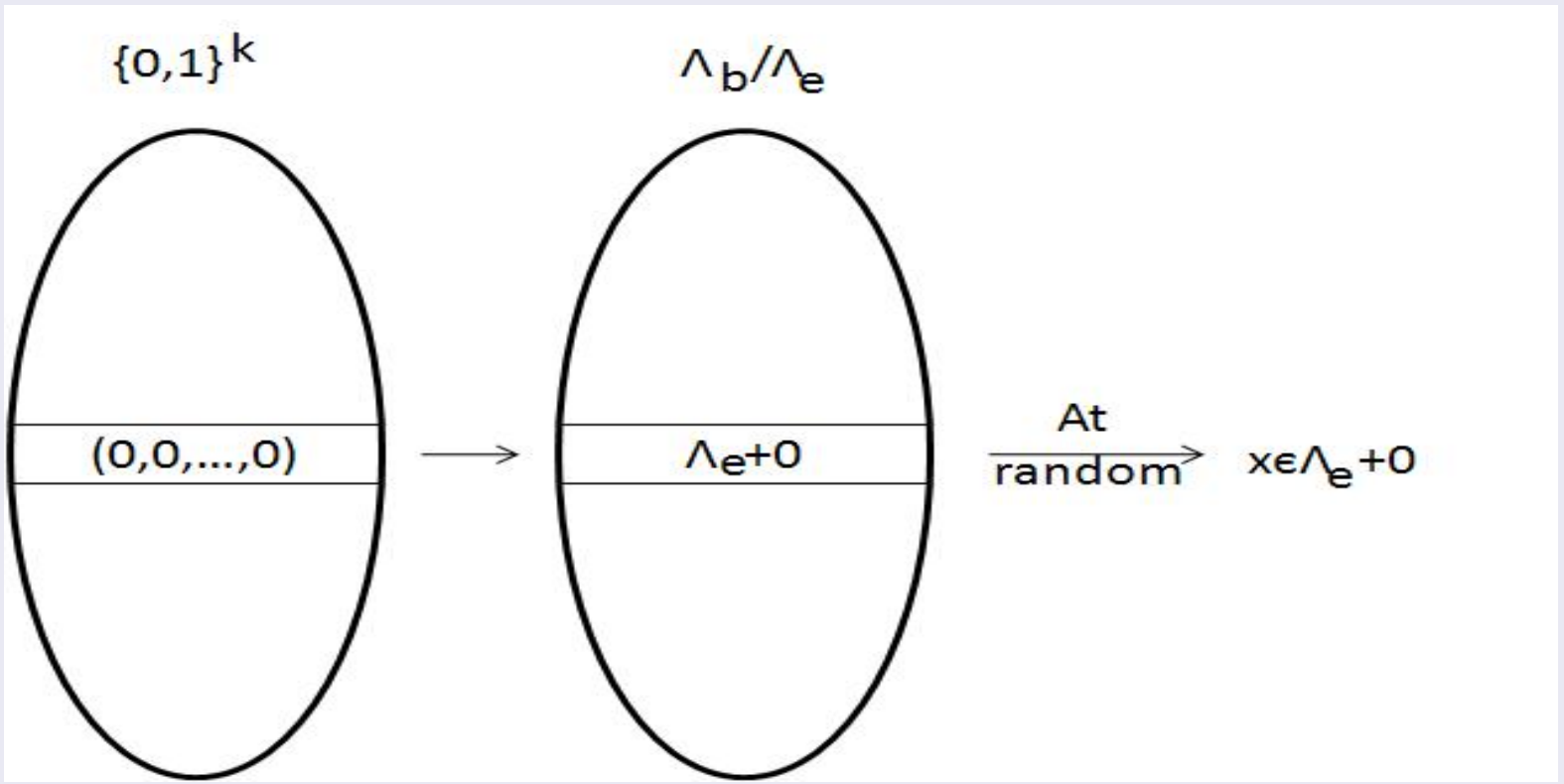
Gaussian Wiretap Channel ($\sigma_b < \sigma_e$)



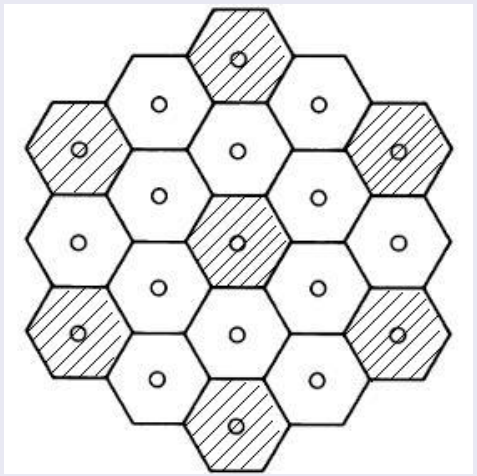
$$\mathbf{y} = \mathbf{x} + \mathbf{v}_b$$
$$\mathbf{z} = \mathbf{x} + \mathbf{v}_e$$

Coset Coding

$\Lambda_e \subset \Lambda_b$ and $|\Lambda_b/\Lambda_e| = 2^k$



Probability of correct dicision



$$P_c \approx \frac{1}{(\sigma\sqrt{2\pi})^2} \sum_{\mathbf{t}\in\Lambda_e} \int_{\mathcal{V}_{\Lambda_b}} e^{-||\mathbf{u}+\mathbf{t}||^2/2\sigma^2} d\mathbf{u}$$

We want to minimize $P_{c,e}$

Taylor expansion of $e^{-||\mathbf{u}+\mathbf{t}||^2/2\sigma_e^2}$ at order 2

$$\begin{aligned} P_{c,e} &\approx \frac{1}{(\sigma_e\sqrt{2\pi})^n}\sum_{\mathbf{t}\in\Lambda_e}\int_{\mathcal{V}_{\Lambda_b}} e^{-||\mathbf{u}+\mathbf{t}||^2/2\sigma_e^2}d\mathbf{u} \\ &\approx \frac{1}{(\sigma_e\sqrt{2\pi})^n}\sum_{\mathbf{t}\in\Lambda_e}\int_{\mathcal{V}_{\Lambda_b}} e^{-||\mathbf{t}||^2/2\sigma_e^2}\left(1+\frac{-1}{\sigma_e^2}\langle\mathbf{t},\mathbf{u}\rangle+\frac{-1}{2\sigma_e^2}||\mathbf{u}||^2\right)d\mathbf{u} \\ &= \frac{1}{(\sigma_e\sqrt{2\pi})^n}\mathrm{vol}(\mathcal{V}_{\Lambda_b})\left(1+\frac{-1}{2\sigma_e^2}\frac{\mathcal{U}(\mathcal{V}_{\Lambda_b})}{\mathrm{vol}(\mathcal{V}_{\Lambda_b})}\right)\cdot\overline{\left|\sum_{\mathbf{t}\in\Lambda_e}e^{-||\mathbf{t}||^2/2\sigma_e^2}\right|} \end{aligned}$$

Since $\mathrm{vol}(\mathcal{V}_{\Lambda_b})$ and $\mathcal{U}(\mathcal{V}_{\Lambda_b})$ are invariants of Λ_b, to minimize $P_{c,e}$ is to minimize the **theta series** of Λ_e at $z=\frac{i}{2\pi\sigma_e^2}$:

$$\Theta_{\Lambda_e}(z)=\sum_{\mathbf{t}\in\Lambda_e}q^{||\mathbf{t}||^2},\ q=e^{\pi iz},\ \mathrm{Im}(z)>0$$

Secrecy Gain

The **secrecy function** of a lattice Λ is defined by

$$\Xi_\Lambda(y) = \frac{\Theta_{\lambda\mathbb{Z}^n}(y)}{\Theta_\Lambda(y)},\ y = \mathrm{Im}(z) > 0,$$

where λ is a scaling factor such that $\mathrm{vol}(\lambda\mathbb{Z}^n) = \mathrm{vol}(\Lambda)$.
The **secrecy gain** of Λ is then

$$\chi_\Lambda = \sup_{y>0}\Xi_\Lambda(y).$$

Why unimodular lattices?

Jacobi's formula:

$$\Theta_\Lambda(y) = |\det(M)|^{-1}(\frac{1}{\sqrt{y}})^n \Theta_{\Lambda^*}(\frac{1}{y}),$$

where Λ^* is the dual of Λ. Specially, when $\Lambda \sim \Lambda^*$,

$$\begin{cases} \Theta_{\mathbb{Z}^n}(y) = (\frac{1}{\sqrt{y}})^n \Theta_{\mathbb{Z}^n}(\frac{1}{y}) \\ \Theta_\Lambda(y) = (\frac{1}{\sqrt{y}})^n \Theta_\Lambda(\frac{1}{y}) \end{cases}$$

$$\Longrightarrow \Xi_\Lambda(y) = \frac{\Theta_{\mathbb{Z}^n}(y)}{\Theta_\Lambda(y)} = \Xi_\Lambda(\frac{1}{y})$$

A proven conjecture and some known results

$$\chi_\Lambda = \Xi_\Lambda(1), \text{ for } \Lambda \sim \Lambda^*$$

ANNE-MARIA ERNVALL-HYTÖNEN
"On A Conjecture by Belfiore and Solé on Some Lattices"
ArXiv Apr 2011. (Done only for extremal even lattices.)

- Extremal even unimodular lattices: $\chi_{E_8} = \frac{4}{3}$, $\chi_{\Lambda_{24}} = \frac{256}{63}$, $\chi_{BW_{32}} = \frac{64}{9}$, $\chi_{P_{48}} = \frac{524288}{19467}$, $\chi_{\Lambda_{72}} = \frac{134217728}{685881}$, $\chi_{\Lambda_{80}} = \frac{536870912}{1414413}$.
- Even unimodular lattices: $\chi_{\Lambda_n} \longrightarrow \infty, n \longrightarrow \infty$.

F. Oggier, P. Solé, and J.C. Belfiore,
"Lattice Codes for the Wiretap Gaussian Channel: Construction and Analysis,"
IWCC 2011.

Unimodular lattices in small dimensions

Odd	Even
$\mathbb{Z}^8$	E_8
$\mathbb{Z}^9, E_8+\mathbb{Z}$	
$\mathbb{Z}^{10}, E_8+\mathbb{Z}^2$	
$\mathbb{Z}^{11}, E_8+\mathbb{Z}^3$	
$\mathbb{Z}^{12}, E_8+\mathbb{Z}^4, D_{12}^+$	
$\mathbb{Z}^{13}, E_8+\mathbb{Z}^5, D_{12}^+ + \mathbb{Z}$	
$\mathbb{Z}^{14}, E_8+\mathbb{Z}^6, D_{12}^+ + \mathbb{Z}^2, E_7^{2+}$	
$\mathbb{Z}^{15}, A_{15}^+, E_8+\mathbb{Z}^7, D_{12}^+ + \mathbb{Z}^3, E_7^{2+} + \mathbb{Z}$	
$\mathbb{Z}^{16}, A_{15}^+ + \mathbb{Z}, E_8+\mathbb{Z}^8, D_{12}^+ + \mathbb{Z}^4, E_7^{2+} + \mathbb{Z}^2, D_8^{2+}$	E_8^2, D_{16}^+
$\cdots$	
$\mathbb{Z}^{23}, \cdots, (A_{15}E_8)^+, (A_{19}A_4)^+, (D_{11}A_{11}O_1)^+, \cdots, O_{23}$	
	Niemeier lattices

Hecke's Theorem

For any unimodular lattice Λ,

$$\Theta_\Lambda(y) = \sum_{r=0}^{\lfloor \frac{n}{8} \rfloor} a_r \vartheta_3^{n-8r}(y)\Delta_8^r(y), a_r \in \mathbb{Z},$$

where

$$\begin{cases} \vartheta_3(y) & = 1 + 2q + 2q^4 + \cdots \\ \Delta_8(y) & = q - 8q^2 + 28q^3 - 64q^4 + \cdots \end{cases}$$

First result:

$$\chi_\Lambda = \Xi_\Lambda(1) = \frac{1}{\sum_{r=0}^{\lfloor \frac{n}{8} \rfloor} a_r (\frac{1}{2^6})^r}$$

Extremal lattices

$$\Theta_\Lambda(y) = 1 + 0q + \cdots + 0q^t + A_{t+1}q^{t+1} + \cdots, \; t = \lfloor \frac{n}{8} \rfloor$$

Example:

$$\begin{cases} \Theta_{O_{23}}(y) & = 1 + 0q + 0q^2 + A_3 q^3 + \cdots \\ \Theta_{O_{23}}(y) & = \vartheta_3^{23}(y) + a_1 \vartheta_3^{15}(y)\Delta_8(z) + a_2 \vartheta_3^{7}(z)\Delta_8^2(z) \end{cases}$$

$$\Longrightarrow \begin{cases} \Theta_{O_{23}}(y) & = 1 + 0q + 0q^2 + A_3 q^3 + \cdots \\ \Theta_{O_{23}}(y) & = 1 + (46 + a_1)q + (1012 + 22a_1 + a_2)q^2 + \cdots \end{cases}$$

then

$$\begin{cases} 46 + a_1 & = 0 \\ 1012 + 22a_1 + a_2 & = 0 \end{cases} \Longrightarrow \begin{cases} a_1 & = -46 \\ a_2 & = 0 \end{cases}$$

Secrecy gains

Second result:

dim	lattices	theta series	secrecy gain
12	D_{12}^{+}	$\vartheta_3^{12} - 24\vartheta_3^4\Delta_8$	$\frac{8}{5}$
14	E_7^{2+}	$\vartheta_3^{14} - 28\vartheta_3^6\Delta_8$	$\frac{16}{9}$
15	A_{15}^{+}	$\vartheta_3^{15} - 30\vartheta_3^7\Delta_8$	$\frac{32}{17}$
23	O_{23}	$\vartheta_3^{23} - 46\vartheta_3^{15}\Delta_8$	$\frac{32}{9}$

Unimodular lattices in small dimensions

Odd	Even
$\mathbb{Z}^8$	E_8
$\mathbb{Z}^9, E_8+\mathbb{Z}$	
$\mathbb{Z}^{10}, E_8+\mathbb{Z}^2$	
$\mathbb{Z}^{11}, E_8+\mathbb{Z}^3$	
$\mathbb{Z}^{12}, E_8+\mathbb{Z}^4, D_{12}^+$	
$\mathbb{Z}^{13}, E_8+\mathbb{Z}^5, D_{12}^++\mathbb{Z}$	
$\mathbb{Z}^{14}, E_8+\mathbb{Z}^6, D_{12}^++\mathbb{Z}^2, E_7^{2+}$	
$\mathbb{Z}^{15}, A_{15}^+, E_8+\mathbb{Z}^7, D_{12}^++\mathbb{Z}^3, E_7^{2+}+\mathbb{Z}$	
$\mathbb{Z}^{16}, A_{15}^++\mathbb{Z}, E_8+\mathbb{Z}^8, D_{12}^++\mathbb{Z}^4, E_7^{2+}+\mathbb{Z}^2, D_8^{2+}$	E_8^2, D_{16}^+
$\cdots$	
$\mathbb{Z}^{23}, \cdots, (A_{15}E_8)^+, (A_{19}A_4)^+, (D_{11}A_{11}O_1)^+, \cdots, O_{23}$	

Root lattices in dimensions $16 \leq n \leq 23$(except O_{23})

$$\Theta_\Lambda(y) = 1 + 0q + K(\Lambda)q^2 + \cdots$$

Example:

$$\begin{cases} \Theta_{D_8^{2+}}(y) & = 1 + 0q + 224q^2 + A_3q^3 + \cdots \\ \Theta_{D_8^{2+}}(y) & = \vartheta_3^{16}(y) + a_1\vartheta_3^8(z)\Delta_8(z) + a_2\Delta_8^2(z) \end{cases}$$

$$\Longrightarrow \begin{cases} \Theta_{D_8^{2+}}(y) & = 1 + 0q + 224q^2 + A_3q^3 + \cdots \\ \Theta_{D_8^{2+}}(y) & = 1 + (32 + a_1)q + (480 + 8a_1 + a_2)q^2 + \cdots \end{cases}$$

then

$$\begin{cases} 32 + a_1 & = 0 \\ 480 + 8a_1 + a_2 & = 224 \end{cases} \Longrightarrow \begin{cases} a_1 & = -32 \\ a_2 & = 0 \end{cases}$$

Secrecy gains

Third result:

lattice	secrecy gain	lattices	secrecy gain
E_8^2	$\frac{16}{9}$	D_{16}^+	$\frac{16}{9}$
D_8^{2+}	2	$(A_{11}E^6)^+$	$\frac{32}{15}$
$(A_{17}A_1)^+$	$\frac{32}{15}$	$(D_{10}E_7A_1)^+$	$\frac{32}{15}$
D_6^{3+}	$\frac{16}{7}$	A_9^{2+}	$\frac{16}{7}$
$(E_6^3O_1)^+$	$\frac{64}{27}$	$(A_{11}D_7O_1)^+$	$\frac{64}{27}$
$(A_7^2D_5)^+$	$\frac{32}{13}$	D_{20}^+	$\frac{32}{17}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
$(A_2^6A_1^6O_5)^+$	$\frac{256}{75}$	$(A_1^{16}O_7)^+$	$\frac{128}{37}$

Odd v.s. Even

- Same secrecy gain:
  $\chi = \frac{16}{9}$ is achieved by E_7^{2+} in dimension 14;
  $\chi = \frac{16}{9}$ is achieved by E_8^2 and D_{16}^+ in dimension 16.
- Same dimension:
  In dimension 16, $\chi_{D_8^{2+}} = 2$;
  In dimension 16, $\chi_{E_8^2} = \chi_{D_{16}^+} = \frac{16}{9}$.

Lattices and codes

Construction A

$$\Lambda_C := \frac{1}{\sqrt{2}}\rho^{-1}(C),$$

$\rho : \mathbb{Z}^n \to \mathbb{F}_2^n$ is the component-wise reduction modulo 2.

- C is a type I code iff Λ_C is an odd unimodular lattice;
- C is a type II code iff Λ_C is an even unimodular lattice.

Lattices and codes

Fourth result:

odd lattice $\sim$ type I code	even lattice $\sim$ type II code
	$E_8 \sim [8,4,4]$
$D_{12}^{+} \sim [12,6,4]$	
$E_7^{2+} \sim [14,7,4]$	
$D_8^{2+} \sim [16,8,4]$	$E_8^2 \sim [16,8,4]^{\dagger}$ $D_{16}^{+} \sim [16,8,4]^{\ddagger}$

Modular Lattices

When $\Lambda \sim \alpha\Lambda^*$,

$$\Xi_\Lambda(\mathrm{vol}(\mathcal{V}(\Lambda))^{-\frac{2}{n}} y) = \Xi_\Lambda(\frac{\mathrm{vol}(\mathcal{V}(\Lambda))^{-\frac{2}{n}}}{y}).$$

- Prove the conjecture for modular lattices (Stephanie)
- Compute the secrecy gain for modular lattices
- Find the corresponding code for modular lattices


谢谢！