2024年度特別研究期間における研究活動

2025年5月27日

経営学部　永田清

2024年4月1日～2025年3月31日 特別研究期間制度取得

- 申請書における研究課題（以下の各課題を並行して研究する）
  - 整数の剰余環上における誤り訂正符号生成手法の耐量子暗号への応用
  - 工学オントロジーを用いた多言語対応情報セキュリティポリシー作成システムの研究と開発
  - 情報セキュリティe-Learningシステムへの多言語自然言語処理の組込み

研究計画（当初予定）

- 2024年7月～8月
  - 場所：　Philippine University, Diliman校, Manila, Philippine
  - 内容：　Philippine大学のFidel Nemenzo教授との共同研究である，整数の剰余環上における誤り訂正符号生成手法の応用として，耐量子暗号への適用可能性を研究する．
    情報セキュリティe-Learningシステムのアジア言語化を検討する
- 2024年10月～11月
  - 場所：　Indraprastha Institute of Information Technology(IIIT-Delhi)，New Delhi, India
  - 内容：　IIIT-Delhi数学科の*Anuradha Sharma*教授との共同研究として，一般Galois環上の誤り訂正符号の実用化を研究する
    ITによって発展を目指すインドの情報セキュリティ現状調査を行う
- 2025年1月～2月
  - 場所：　The University of Tabuk, Tabuk, Saudi Arabia
  - 内容：　Tabuk大学の*Hassan Hijry*准教授とのプロジェクトに参加し，情報セキィリティマネージメントの研究を行う

7月29日～8月26日
Philippine University, Diliman校, Manila, Philippine

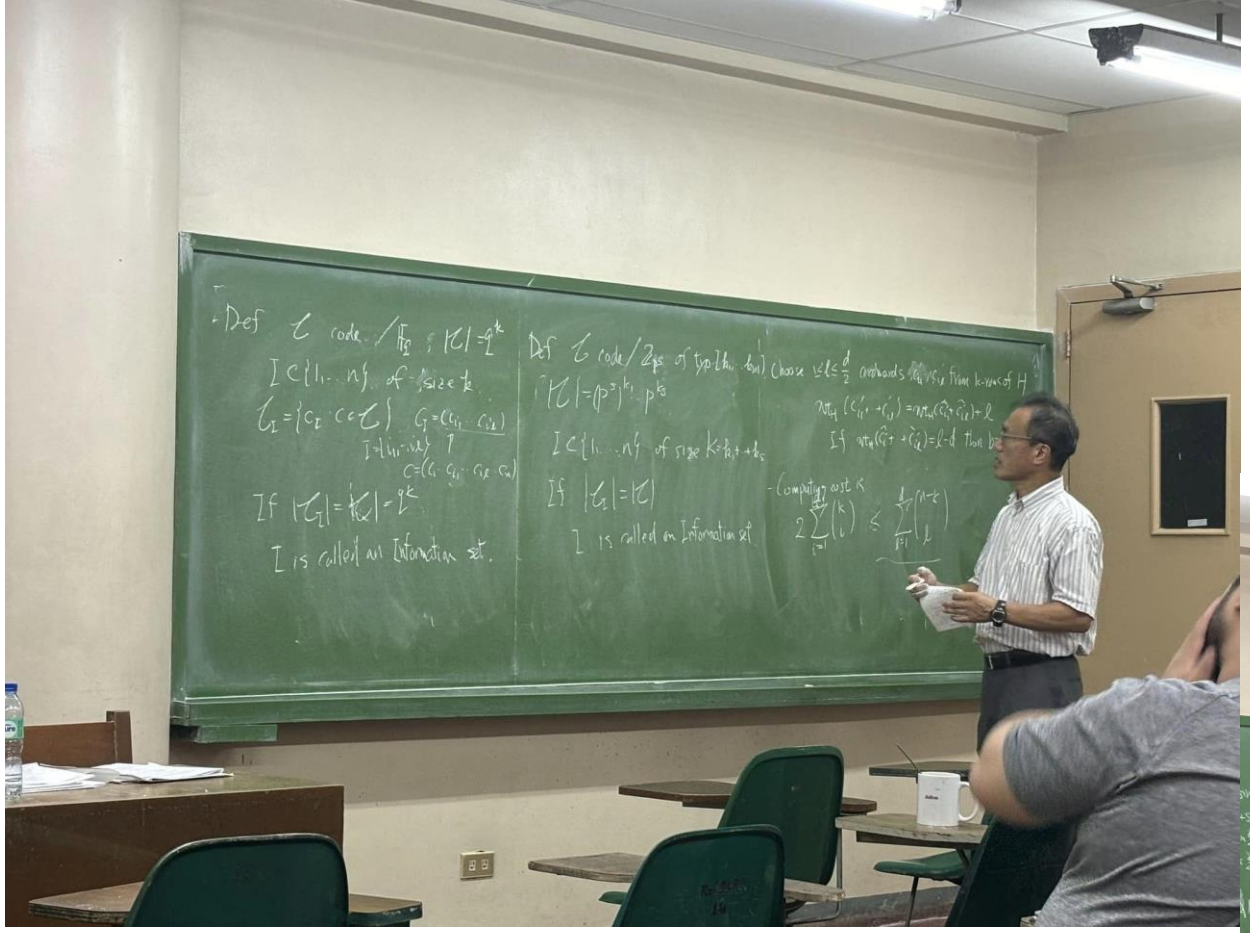
- 整数の剰余環上における誤り訂正符号生成手法の応用
- Fidel Nemenzo教授との共同研究
- 耐量子暗号(PQCC：Post Quantum Computer Cryptography)への適用可能性に関する研究
- 教員及び大学院生との研究会に5回参加・発表

University of the Philippines Los Baños校 and Diliman校

Rico C. Ancog, PhD DEAN School of Environmental Science and Management

Fidel Nemanzo, PhD Former Chanceller of UP Diliman

UP Diliman校, Mathematic Department




Prange's Algorithm over
Information Set Decoding
Def

Survey on PQCC with Self Dual Code over Integer Modulo Ring

[**Key generation**] Let G be a generator matrix of $[n, k, 2t+1]$-linear binary code $\mathcal{C}$ with t-errors correcting capability. For randomly chosen S from $GL_k(\mathbb{F}_2)$ and P from S_n (n-permutation matrix), $\tilde{G} = SGP$ is the public key and (S, G, P) is the private key.

[**Encryption**] For a plain text m of size k, the cipher text $c = m\tilde{G}+e = mSGP+e$, where e is a random binary vector of weight t and length n.

[**Decryption**] For the transmitted binary vector c, the owner of the private key (S, G, P) calculates $\bar{c} = cP^{-1} = mSG + eP^{-1}$.
Since $\bar{c}$ can be considered as the coded text of mS with t errors in eP^{-1}, mS can be decoded by applying the error correcting capability of G. When it works, the plaintext $m = (mS)S^{-1}$ can be given.

[**Security**] The security of the system is based on the quasi-randomness of $\tilde{G}$ under the binary version of LWE hypothesis called Learning with Parity Noise (LPN). Under the McEliece assumption shown below the quasi-randomness is guaranteed.

[McEliece Assumption] For any generator matrix G of $[n, k]$-linear binary code $\mathcal{C}$, the difference between

$$|Pr[S \leftarrow GL_k(\mathbb{F}_2), P \leftarrow S_n : \mathcal{A}(1^n, \tilde{G} = SGP) = 1] \tag{1}$$

and

$$Pr[G \leftarrow M_{n\times k}(\mathbb{F}_2) : \mathcal{A}(1^n, G) = 1]| \tag{2}$$

can be negligible compared to n. Here, the notation $\mathcal{A}(1^n, G) = 1$ implies that the calculated vector c in $\mathbb{F}_2^n$ from one of two messages m_0, m_1 applying G can be correctly distinguished using algorithm $\mathcal{A}$.

Operational Cost Calculation

[Operational cost Algorithm 3]

$$\frac{\binom{2n}{t}}{\binom{2m_1}{v}\binom{2m_2}{v}\binom{2(n-k_1-k_2-l)}{t-2v}}$$

$$\Bigg(2(n-k)^2(n+1)+$$

$$2l\left(L(2m_1,v)+L(2m_2,v)-\ 2m_1-2m_2+\binom{2m_2}{v}\right)+$$

$$k_2\left(L(m_1,v)+L(m_2,v)-\ m_1-m_2+\binom{2m_2}{v}\right)+$$

$$\frac{1}{2^{k_2+2l-1}}\binom{2m_1}{v}\binom{2m_2}{v}(t-2v+1)(2v+1)\Bigg)$$

Algorithm 3 Collision ISD (Stern's algorithm) over $\mathbb{Z}_4$

Require: Parity check matrix $H \in M_{n-k_1,n}(\mathbb{Z}_4)$, the syndrome $s \in \mathbb{Z}_4^{n-k_1}$, positive integers v, m_1, m_2, l, such that $k_1 + k_2 = m_1 + m_2$, $v \leq min\{2m_1, 2m_2\}, 2v \leq t$, and $t - 2v \leq 2(n - k_1 - k_2 - l)$.

Ensure: $e \in \mathbb{Z}_4^n$ with the same syndrome as s with $wt_L(e) = t$.

1: Choose a quaternary information set $I \subset \{1, \ldots, n\}$ of size $k_1 + k_2$

2: Choose a set $Z \subset \{1, \ldots, n\} \setminus I$ of size l and let $J = \{1, \ldots, n\} \setminus (I \cup Z)$.

3: Partition I into X and Y of size m_1 and m_2 respectively

4: Find $U \in GL_{n-k_1}(\mathbb{Z}_4)$ such that $UH = \begin{pmatrix} A & Id_l & 0 \\ B & 0 & Id_{n-k_1-k_2-l} \\ 2C & 0 & 0 \end{pmatrix}$ by permuting $k_1 + k_2$ columns in I first, l columns in Z second, and $n - k_1 - k_2 - l$ columns in J last, where $A \in M_{l,k_1+k_2}(\mathbb{Z}_4)$, $B \in M_{n-k_1-k_2-l,k_1+k_2}(\mathbb{Z}_4)$, and $C \in M_{k_2,k_1+k_2}(\mathbb{F}_2)$.

5: Compute $Us^t = \begin{pmatrix} s_1^t \\ s_2^t \\ 2s_3^t \end{pmatrix}$, where $s_1 \in \mathbb{Z}_4^l$, $s_2 \in \mathbb{F}_2^{n-k_1-k_2-l}$, and $s_3 \in \mathbb{F}_2^{k_2}$

6: Compute
$S = \{(\pi_I(e_X)A^t, 2\pi_I(e_X)C^t, e_X);$
$e_X \in \mathbb{Z}_4^n(X)$ and $wt_L(e_X) = v\}$,
where $\mathbb{Z}_4^n(X)$ is the set of all vectors in $\mathbb{Z}_4^n$ whose support is in X, and π_I is the projection to $\mathbb{Z}_4^{k_1+k_2}$ corresponding to I's coordinates.

7: Compute
$T = \{(s_1 - \pi_I(e_Y)A^t, 2s_3 - 2\pi_I(e_Y)C^t, e_Y);$
$e_Y \in \mathbb{Z}_4^n(Y)$ and $wt_L(e_Y) = v\}$

8: **for** $(a, b, e_X) \in S$ **do**

9: **for** $(a, b, e_Y) \in T$ **do**

10: **if** $wt_L(s_2 - \pi_I(e_X + e_Y)B^t) = t - 2w$ **then**

11: Output:
$e = e_X + e_Y + \sigma_J(s_2 - \pi_I(e_X + e_Y)B^t)$,
where σ_J is the canonical embedding to $\mathbb{Z}_4^n$.

12: **end if**

13: **end for**

14: **end for**

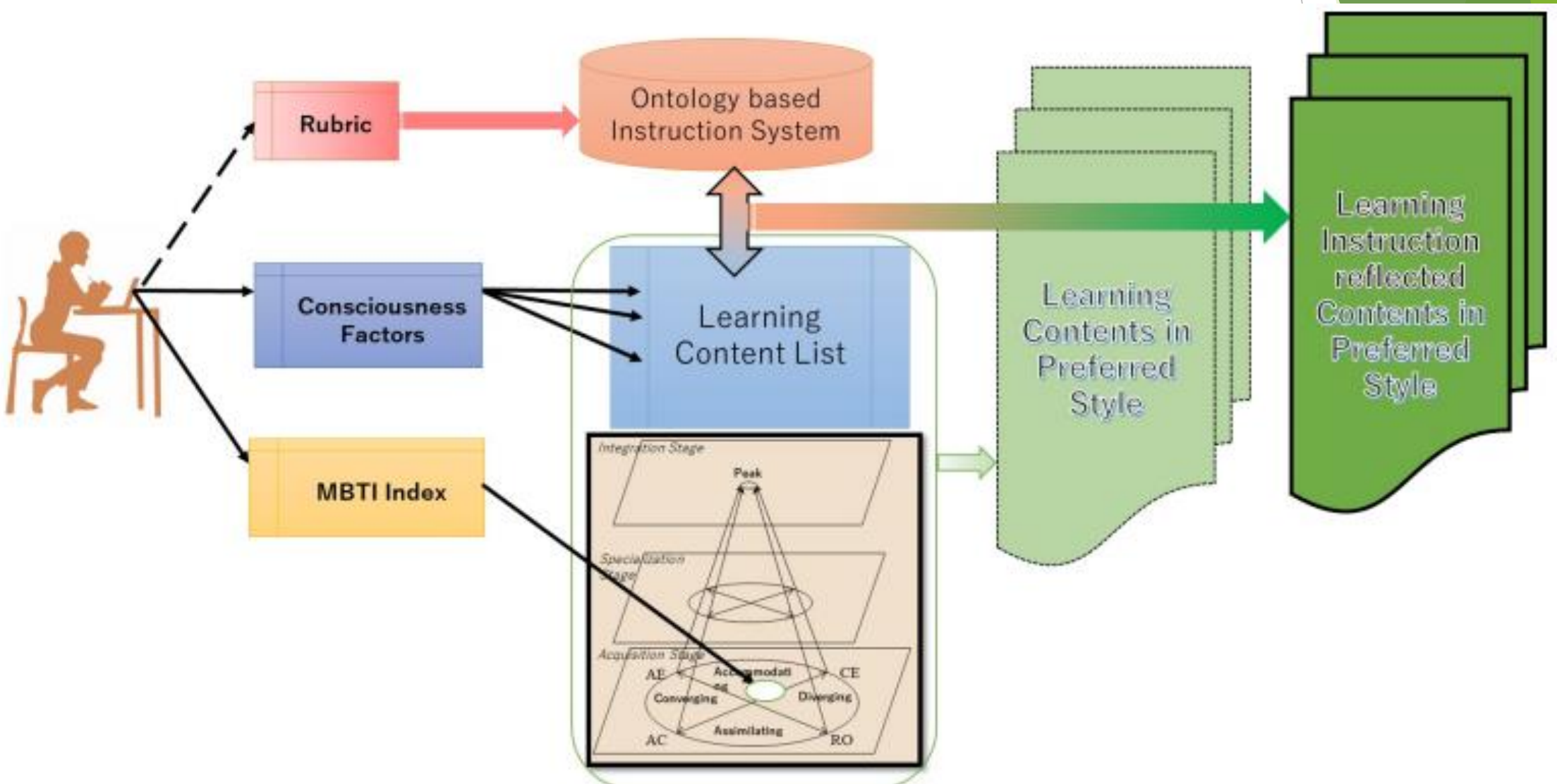
15: **return** Step 1 with a new selection of I

(Souce: Anna-Lena Horlemann and Violetta Weger, p. 14)

9月23日～9月27日
Tallinn University of Technology，Estonia
International Conference on Learning ICL2024

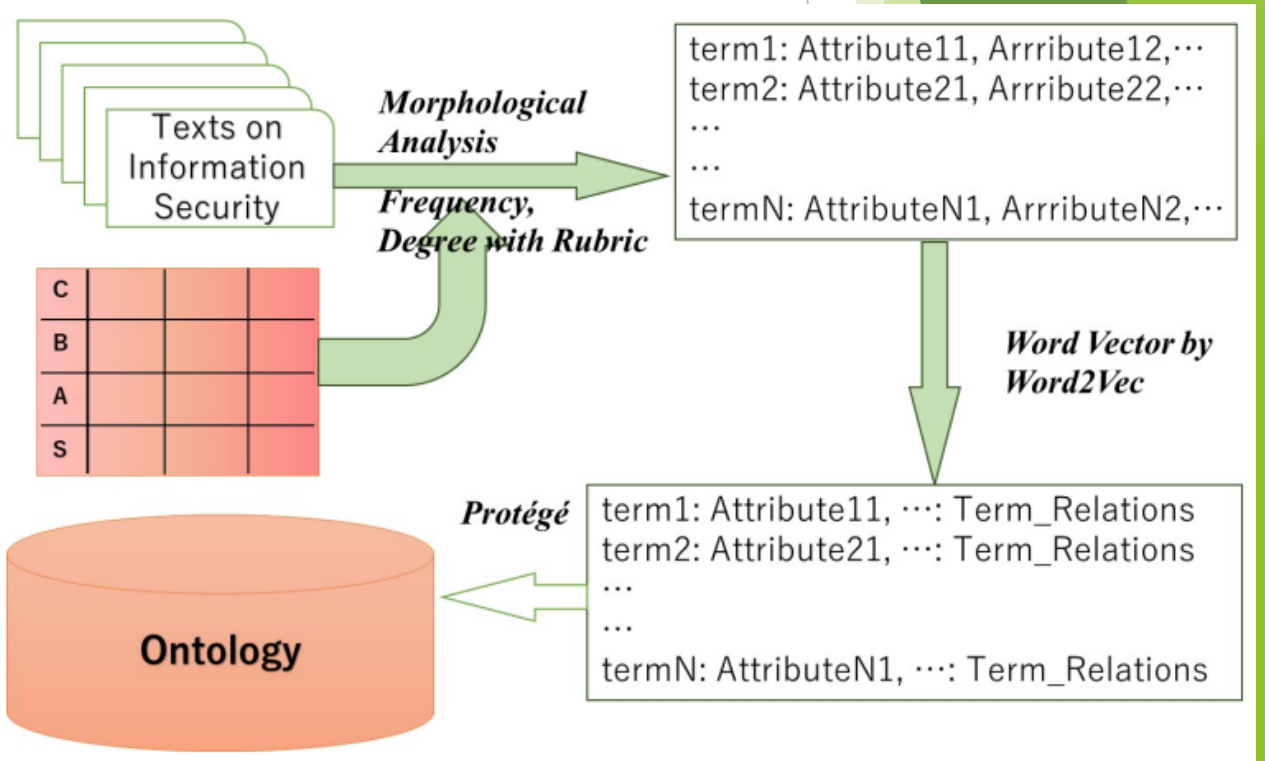
- “Learning Styles and Ontological Approach for Information Security e-Learning System”の発表
- 論文：Futureproofing Engineering Education for Global Responsibility. (ICL 2024), Lecture Notes in Networks and Systems, Springer, Cham. Vol 1261,207-218

“Learning Styles and Ontological Approach for Information Security e-Learning System”



Ontology Configuring Method for “Learning Styles and Ontological Approach for Information Security e-Learning System”

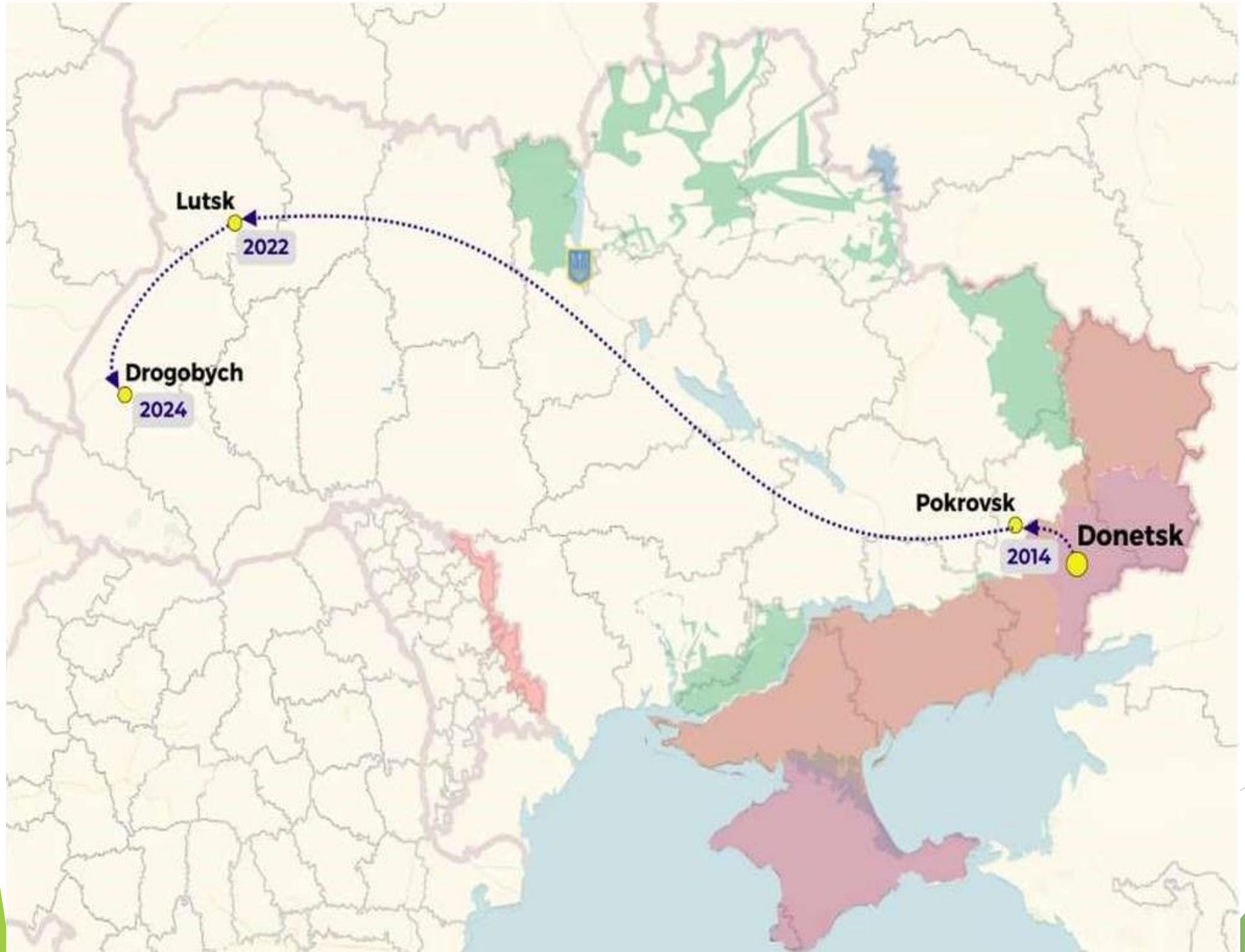
1. Choose one or some textbook on information security management
2. Extract words (terms or terminologies) and their relationships using morphological analysis software, such as *Tree Tagger*
3. Analise the frequency of each term and make a list of them with the relationship between them
4. Provides each of terms the importance degree in common formation security by using *Word2Vec*
5. Configure an ontology using *Protégé*



ICL2024 in タリン工科大学

エストニア，タリン工科大学

国立ドネツク工科大学
DonNTU副校長 Viktoriya Voropayeva氏の発表


Lutsk
2022
Drogobych
2024
Pokrovsk
2014
Donetsk

10月28日～11月12日
Indraprastha Institute of Information Technology(IIIT-Delhi), New Delhi, India

- IIIT-Delhi数学科のAnuradha Sharma教授との共同研究
- 一般Galois環上の誤り訂正符号の実用化に関する研究
- 教員及び大学院生との研究会に3回参加・発表

IIIT-Delhi
Anuradha Sharma教授の大学院生

Indraprastha Institute of Information Technology(IIIT-Delhi)

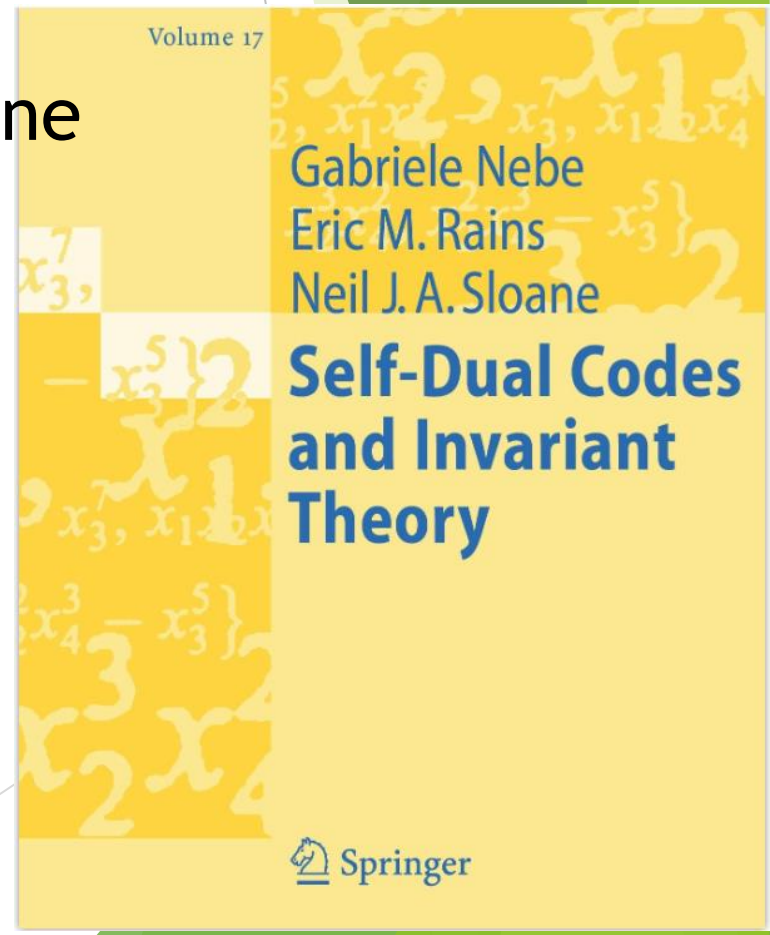
Indraprastha Institute of Information Technology, Delhi

The campus in 2024

Other name	IIIT-D, IIIT Delhi
Type	State university
Established	2008; 17 years ago
Chairperson	Rajesh Srivastava
Chancellor	Lieutenant Governor of Delhi
Director	Ranjan Bose
Address	Okhla Industrial Estate, Phase III, New Delhi, 110020, India 28°32′40″N 77°16′21″E
Campus	Urban, 25 acres (10 ha)
Language	English
Colours	
Website	www.iiitd.ac.in

Text Book

- Self-Dual Codes and Invariant Theory (Algorithms and Computation in Mathematics Book 17) (English Edition) 2006th 版, Kindle版
- (著) Gabriele Nebe, Eric M. Rains, Neil J. A. Sloane
- Chapter 13 Quantum Codes
  - 13.1 Definitions
  - 13.2 **Additive and symplectic quantum codes**
  - 13.3 Hamming weight enumerators
  - 13.4…



研究成果概要（1）

- 整数の剰余環上における誤り訂正符号生成手法の耐量子暗号への応用
  - University of PhilippinesのFidel Nemenzo教授やIndraprastha Institute of Information Technology(IIIT-Delhi)のAnuradha Sharma教授との共同研究活動によってこの分野における課題が明らかになった
  - 今後の方向性が示されたが，具体的に論文として発表するまでには至っていない

研究成果概要（２）

- 工学オントロジーを用いた多言語対応情報セキュリティポリシー作成システムの研究と開発
  - 情報セキュリティに関する現状やセキュリティポリシー作成システムの概要に関してまとめIntech Open BookのChapter2で公表することができた
  - ネット上のオープンダウンロードシステムに公開されており，2025年3月現在までに120ダウンロード
  - 工学オントロジーの組込みに関しては概要だけを示しており，今後その具体化を行う予定

研究成果概要（３）

- 情報セキュリティe-Learningシステムへの多言語自然言語処理の組込み
  - ICL2024においては，多言語言語処理に対応した情報セキュリティe-Learningシステムについてオントロジーの活用を含めた発表を行った
  - 実際のオントロジー作成とその処理を組込んだアプリケーションソフト作成が今後の課題として重要であることがわかった

発表論文等

- “Learning Styles and Ontological Approach for Information Security e-Learning System” ,
  ICL2024－Futureproofing Engineering Education for Global Responsibility
- “Survey on PQCC with Self Dual Code over Integer Modulo Ring”,
  The 2nd International Conference on ICT Application Research, Aomori, Japan
- “Learning Style Recognition in relation with MBTI and FSLSM”,
  The 2nd International Conference on ICT Application Research, Aomori, Japan
- “Establishing Information Security Policy as an Organizational Risk Management”,
  in The Future of Risk Management, IntechOpen, 2025-01-29, Chapter 2, pp. 17-37,
  DOI: 10.5772/intechopen.1004563

反省

- フィリピンやインドにおいて情報セキュリティやe-Learningに関する調査を予定していたが実施はできなかった
- Tabuk UniversityのHassan Hijry准教授との共同研究は実行できなかった
- 2012年度に1年間滞在したHeilbronn University, Department of Industrial Engineering and ManagementのRainald Kasprik教授から連絡をもらったが訪問することができなかった