線形符号の Relative Generalized Rank Weightと，そのセキュアネットワーク符号への応用

栗原 淳

SITA2014 ワークショップ
2014年12月10日

今日の発表内容

1. セキュアネットワーク符号化の紹介
2. この発表で紹介する研究の狙い
3. 新しい符号パラメータの紹介
4. 符号パラメータとセキュアネットワーク符号化の安全性

今回の発表の内容は，東工大 植松先生・松本先生との共同成果

ネットワーク符号化 [ACLY00, LY03]

複数ノードで構成されたネットワーク上でのデータの転送において,

- 従来方式(ルーティング)： 中間ノードは，受信データをコピー・転送
- ネットワーク符号化： 中間ノードは，受信データを(線形)演算して出力

ネットワーク符号化は，ルーティングと比べてネットワーク上でのデータ伝送効率が良いなどのメリットがある

ネットワーク符号化の広がり

理論面での展開の例:

- 分散ストレージ用符号・再生成符号への拡張,
- Index Coding with Side Information, Coded-Caching との関係性,
- など.

実際の適用が期待できそうな応用研究分野の例:

- TCP/IPの輻輳制御への適用[1]
- Information-Centric Networkingでの符号化キャッシュ方式への適用[2]
- など.

---

[1] TCP/NC, Coded-TCP
[2] CodingCacheなど

本発表は，「ネットワーク符号化されたネットワークに【盗聴者が存在した場合】のセキュリティ対策技術」について．

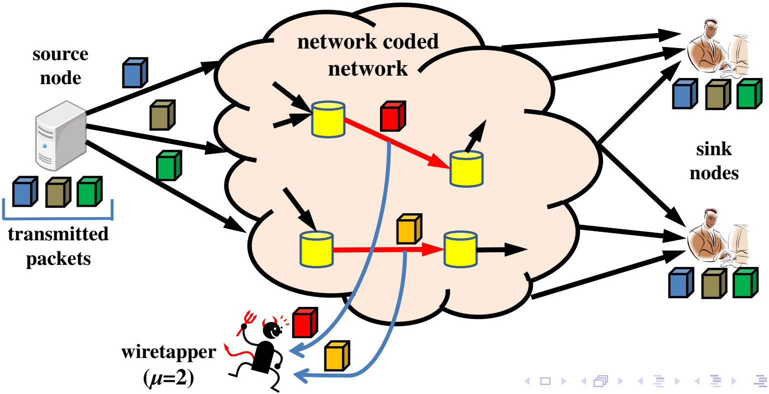
⇒ セキュアネットワーク符号化

セキュアネットワーク符号化問題 [CC11, CY02]

【仮定】

- 単一ソースでの(ネットワーク符号化による)マルチキャスト
- ネットワーク上のμリンクを盗聴する盗聴者が存在

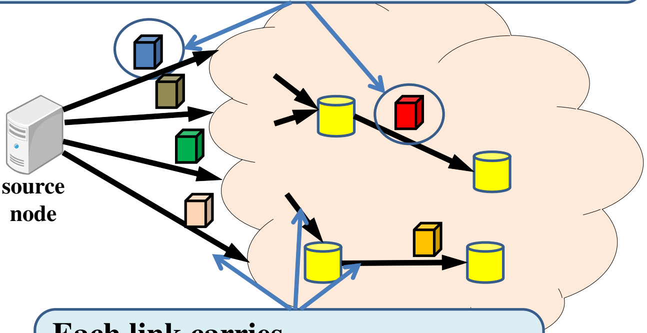
【ゴール】秘密メッセージSを，盗聴者へは漏らさずに，正規のシンクノードへマルチキャストする



もうすこし詳しく：ネットワークの仮定

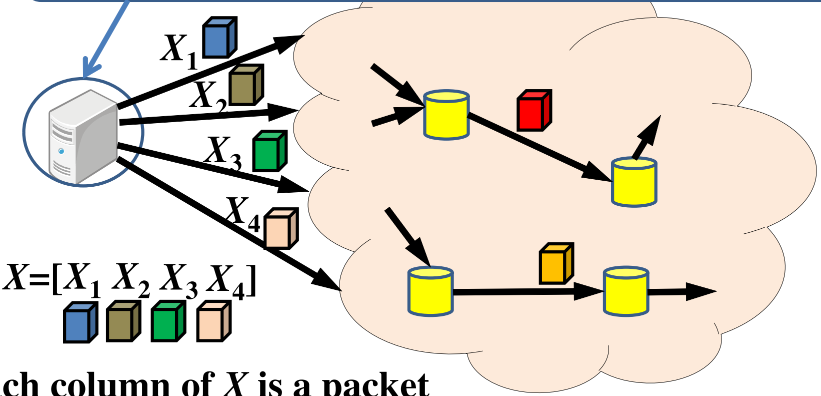
有向非巡回グラフで表された，遅延のないネットワーク上で，
単一ソースでのマルチキャスト

packet: sequence of m symbols in $\mathbb{F}_q$,
represented by a vector $[x_1, x_2, \ldots, x_m]^{\mathrm{T}} \in \mathbb{F}_q^{m\times 1}$

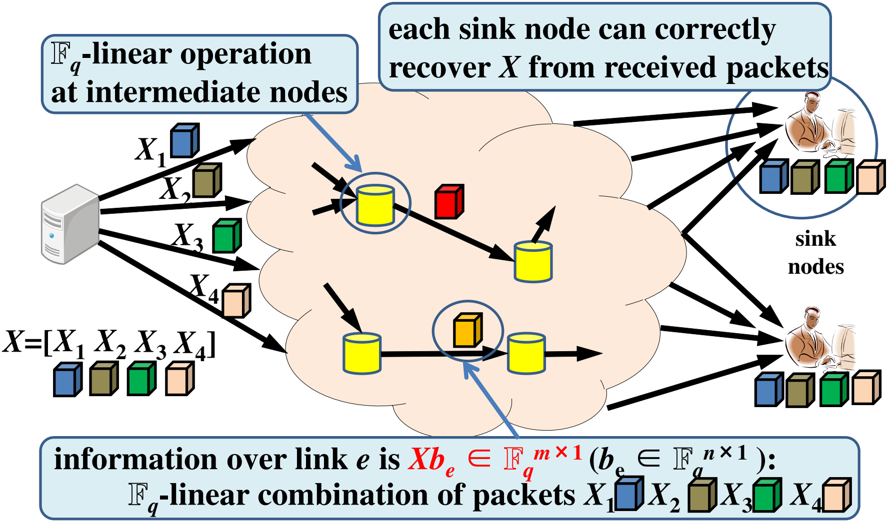


Each link carries
- **single $\mathbb{F}_q$-symbol per one time slot,**
- **a packet over m time slots.**

n packets is transmitted from n outgoing links, represented by an $m \times n$ matrix $X \in \mathbb{F}_q^{m \times n}$

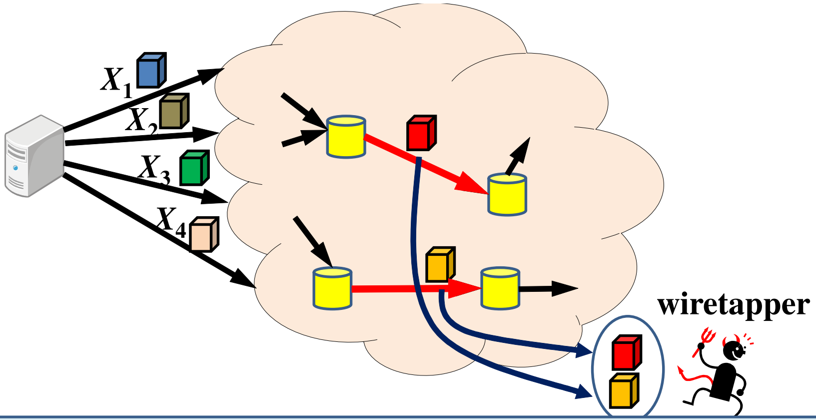


each column of X is a packet


$\mathbb{F}_q$-linear operation at intermediate nodes
each sink node can correctly recover X from received packets
X_1
X_2
X_3
X_4
$X=[X_1\ X_2\ X_3\ X_4]$
sink nodes
information over link e is $Xb_e \in \mathbb{F}_q^{m\times 1}$ ($b_e \in \mathbb{F}_q^{n\times 1}$):
$\mathbb{F}_q$-linear combination of packets X_1 X_2 X_3 X_4

もうすこし詳しく：盗聴者が得る情報

盗聴者は任意に選んだμリンクを盗聴する



information obtained by the wiretapper is $W=XB \in \mathbb{F}_q^{m\times\mu}$:

μ $\mathbb{F}_q$-linear combinations of packets X_1 X_2 X_3 X_4

- 送信パケット：$X = [X_1, \ldots, X_n] \in \mathbb{F}_q^{m \times n}$
- ネットワーク上のリンクeに対して定まるベクトル：$b_e = [b_1, \ldots, b_n] \in \mathbb{F}_q^{n \times 1}$
- 盗聴者がアクセスするμリンク：$e_1, \ldots, e_\mu$

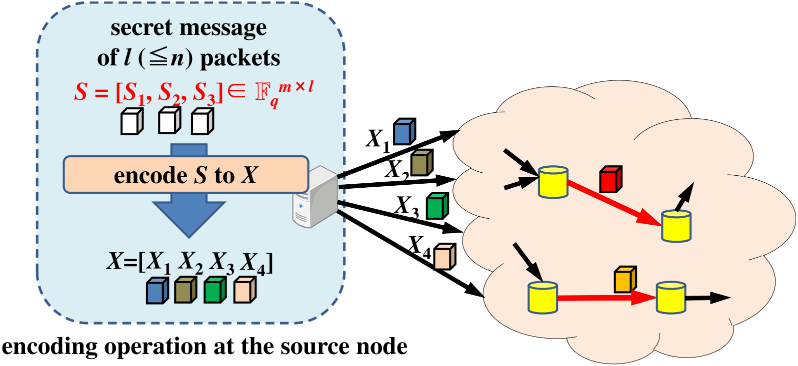
このとき，盗聴者が得る情報Wは以下のように表される

$$W = X \underbrace{\left[b_{e_1}, \ldots, b_{e_\mu} \right]}_{= B \in \mathcal{B} \text{ (盗聴行列)}} \in \mathbb{F}_q^{m \times \mu}$$

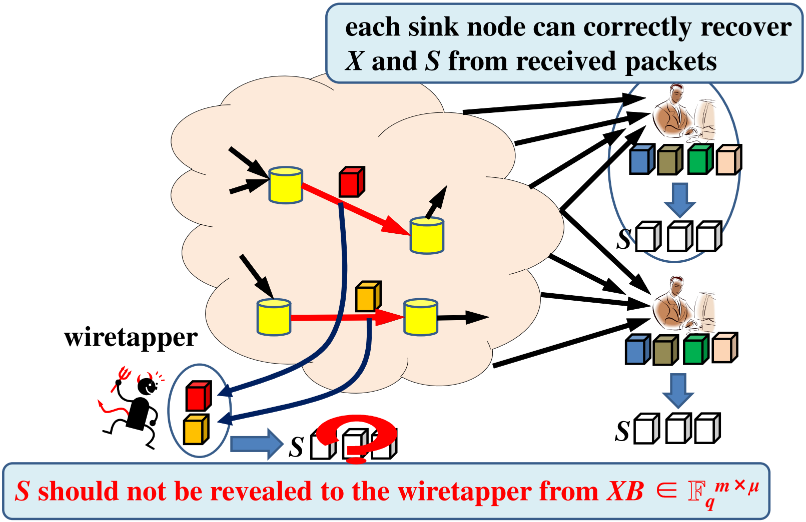
$\mathcal{B}$: 盗聴されるμリンクの組み合わせで決まる盗聴行列Bの集合

もうすこし詳しく：セキュアネットワーク符号化とは

盗聴行列の集合$\mathcal{B}$に応じた符号化によりlパケットの秘密メッセージ$S \in \mathbb{F}_q^{m\times l}$ $(l \leq n)$からXを生成し



シンクノードは正しくSを復号でき，盗聴者はSに関する情報を得られないようにする手法のこと



1. セキュアネットワーク符号化の紹介
2. この発表で紹介する研究の狙い
3. 新しい符号パラメータの紹介
4. 符号パラメータとセキュアネットワーク符号化の安全性

セキュアネットワーク符号化でできたらうれしい事

【符号化手法の設計の問題】

- ネットワーク構造 = 盗聴行列の集合$\mathcal{B}$ を元に符号化方法を設計するのは計算量が多い
- さらに，ネットワーク構造が未知の場合や時変の場合[3]に対応できない

$\Rightarrow$ 【常に同じ符号化方法】で，【どんなネットワークでも一定の安全性を保てる】やり方があると，とてもうれしい（ユニバーサルなセキュアネットワーク符号化方法）

[3] ランダムネットワーク符号化[HMK+06]

Silva-Kschischang ユニバーサルセキュアネットワーク符号化 [SK11]

【情報理論的な意味で安全】な[4]【ユニバーサル】な手法.
基づく構成要素とその条件は,

- $\mathbb{F}_{q^m}$-線形符号(部分空間) $\mathcal{C}_1 \subseteq \mathbb{F}_{q^m}^n$, $m \geq n$
- その$\mathbb{F}_{q^m}$-線形部分符号 $\mathcal{C}_2 \subsetneq \mathcal{C}_1$, $\dim_{\mathbb{F}_{q^m}} \mathcal{C}_2 = \dim_{\mathbb{F}_{q^m}} \mathcal{C}_1 - l$
- ただし$\mathcal{C}_1$と$\mathcal{C}_2$はMaximum Rank Distance (MRD) 符号.

[4]かつ誤り訂正能力もある

Silva-Kschischang法[SK11]の安全性

$\mathbb{F}_{q^m}$-線形MRD符号: C_1 and C_2
$(C_2 \subsetneq C_1 \subseteq \mathbb{F}_{q^m}^n,\ m \geq n,\ \dim_{\mathbb{F}_{q^m}} C_2 = \dim_{\mathbb{F}_{q^m}} C_1 - l)$

[SK11, Theorem 7]

Silva-Kschischangの$S \in \mathbb{F}_q^{m \times l}$から$X \in \mathbb{F}_q^{m \times n}$の生成手法は，ネットワーク構造に依存せず，任意の$\mu \leq \dim_{\mathbb{F}_{q^m}} C_2 = \dim_{\mathbb{F}_{q^m}} C_1 - l$リンクの盗聴について S の情報を一切漏洩しない.

ついでにユニバーサルな誤り訂正能力もある[5]

[SK11, Theorem 12]

Silva-Kschischangの$S \in \mathbb{F}_q^{m\times l}$から$X \in \mathbb{F}_q^{m\times n}$の生成手法は，　ネットワーク構造に依存せず，任意の$t < \lfloor (n - \dim_{\mathbb{F}_{q^m}} C_1)/2 \rfloor$リンクで発生した(挿入された)誤りを訂正・正しく$S$を復号できる．

[5]この定理はネットワーク符号そのものをfeasible(誤りがなければ必ず復号できる)だと仮定して書き換えています

疑問

- C_1, C_2がMRD符号ではない場合，安全性（と誤り訂正能力）はどうなるのか？
- C_1とC_2のどんなパラメータが，セキュアネットワーク符号化の安全性を表しているのか？

私たちの研究の狙いは，これらの疑問を解消し，線形符号の世界とネットワーク符号化の世界をつなげること．そして古典的な符号理論の文脈でセキュアネットワーク符号化を捉える道筋を作ること．

ざっくり成果

⇒ 任意の$C_2 \subsetneq C_1 \subsetneq \mathbb{F}_{q^m}^n$の新しい(相対)符号パラメータを提案し;

⇒ その符号パラメータを使って，安全性・誤り訂正能力を厳密に見積もれることを示した

Silva-Kschischang法[SK11]の符号化手法

$C_2 \subsetneq C_1 \subseteq \mathbb{F}_{q^m}^n$: $\mathbb{F}_{q^m}$-線形MRD符号[6] with $m \geq n$.

秘密メッセージのパケット数 : $l = \dim_{\mathbb{F}_{q^m}} C_1 - \dim_{\mathbb{F}_{q^m}} C_2$
秘密メッセージ : $S = [S_1, \ldots, S_l] \in \mathbb{F}_{q^m}^l = \mathbb{F}_q^{m \times l}$

Nested Coset Coding

1. 任意の同型写像$\psi : \mathbb{F}_{q^m}^l \to C_1/C_2$で, $S = [S_1, \ldots, S_l]$をコセット$\psi(S) \in C_1/C_2$に対応させる.
2. $\psi(S)$から$X = [X_1, \ldots, X_n] \in \psi(S) \subsetneq \mathbb{F}_{q^m}^n$をランダムに選択.

得られた$X_1, \ldots, X_n \in \mathbb{F}_{q^m}$のそれぞれを$m$次元ベクトル=1パケットとみなして送信

[6]まだMRDの性質は気にしなくて大丈夫

Silva-Kschischang法[SK11]のC_1, C_2の直感的役割

$C_2 \subsetneq C_1 \subseteq \mathbb{F}_{q^m}^n$: $\mathbb{F}_{q^m}$-線形MRD符号
秘密メッセージ$S \in \mathbb{F}_{q^m}^l \leftrightarrow$ コセット$\psi(S) \in C_1/C_2$.

- C_1 - 誤り訂正能力を与える．XとしてC_1に属すベクトルのみを使うことで，誤り訂正が可能となる．ただし，$C_1 = \mathbb{F}_{q^m}^n$とすることで誤り訂正機能はオフにできる．
- C_2 - 秘密メッセージの秘匿能力を与える．Xをコセット$\psi(S) \in C_1/C_2$からランダム選択することで，秘匿を行っている．$C_2 = \{0\}$とすることで秘匿機能はオフにできる．

1. セキュアネットワーク符号化の紹介
2. この発表で紹介する研究の狙い
3. 新しい符号パラメータの紹介
4. 符号パラメータとセキュアネットワーク符号化の安全性

$\mathbb{F}_{q^m}$-線形部分空間のq乗 [Sti90]

ベクトル$x = [x_1, \ldots, x_n] \in \mathbb{F}_{q^m}^n$について，$x^q \triangleq [x_1^q, \ldots, x_n^q]$.
$\mathbb{F}_{q^m}$-線形部分空間$V \subseteq \mathbb{F}_{q^m}^n$について，$V^q \triangleq \{x^q : x \in V\}$.

$\Gamma \triangleq \left\{V \subseteq \mathbb{F}_{q^m}^n : V \text{ is } \mathbb{F}_{q^m}\text{-linear}, V = V^q\right\}$.
$V^* \triangleq V + V^q + V^{q^2} + \cdots + V^{q^{m-1}}$.

1. $V \subseteq \mathbb{F}_{q^m}^n$が$V \in \Gamma \Leftrightarrow V$の基底が$\mathbb{F}_q^n$の要素で書ける.
   すなわち$B \in \mathbb{F}_q^{n\times\mu}$の$\mathbb{F}_{q^m}$-線形の列空間を$\langle B \rangle$として，

$$\left\{\langle B \rangle \subseteq \mathbb{F}_{q^m}^n : B \in \mathbb{F}_q{}^{n\times\mu}\right\} = \left\{V \subseteq \mathbb{F}_{q^m}^n : V \in \Gamma, \dim_{\mathbb{F}_{q^m}} V \le \mu\right\}.$$

2. V^*は，Vを包含するΓ中の最小の$\mathbb{F}_{q^m}$-線形部分空間

Relative Generalized Rank Weight (RGRW)

i-th RGRW

$\mathbb{F}_{q^m}$-線形符号$C_1 \subseteq \mathbb{F}_{q^m}^n$および部分符号$C_2 \subsetneq C_1$について，

$$
\begin{aligned}
&M_{R,i}(C_1, C_2)\\
&\triangleq \min\left\{\dim_{\mathbb{F}_{q^m}} V : V \in \Gamma, \dim_{\mathbb{F}_{q^m}}(C_1 \cap V) - \dim_{\mathbb{F}_{q^m}}(C_2 \cap V) \geq i\right\}\\
&= \min\left\{\dim_{\mathbb{F}_{q^m}} V : V \in \Gamma, \dim_{\mathbb{F}_{q^m}}(C_1 \cap V) - \dim_{\mathbb{F}_{q^m}}(C_2 \cap V) = i\right\},
\end{aligned}
$$

ただし， $0 \leq i \leq \dim C_1/C_2 = l$.

Gabidulinのランク重み

$x = [x_1, \ldots, x_n] \in \mathbb{F}_{q^m}^n$

$\mathfrak{S}(x) \subseteq \mathbb{F}_{q^m}$: $x_1, \ldots, x_n$で張られる$\mathbb{F}_{q^m}$の$\mathbb{F}_q$-線形部分空間

ランク重み [Gab85]

$x \in \mathbb{F}_{q^m}^n$について, $w_R(x) \triangleq \dim_{\mathbb{F}_q} \mathfrak{S}(x)$.

最小ランク重み [Gab85]

$\mathbb{F}_{q^m}$-線形部分空間$C \subseteq \mathbb{F}_{q^m}^n$について $d_R(C) = \min\{w_R(x) : x \in C \setminus \{0\}\}$.

MRD符号：$d_R(C) = n - \dim_{\mathbb{F}_{q^m}} C + 1$を満たす符号$C \subseteq \mathbb{F}_{q^m}^n$

RGRWと最小ランク重みの関係

1st RGRW $M_{R,1}(C_1, C_2)$は，w_Rを使って以下のように表せる．

$$M_{R,1}(C_1, C_2) = \min\{w_R(x) : x \in C_1 \setminus C_2\}.$$

$\Rightarrow$

RGRWと最小ランク重みの関係

$\mathbb{F}_{q^m}$-線形符号$C \subseteq \mathbb{F}_{q^m}^n$に対して，　$M_{R,1}(C, \{0\}) = d_R(C).$

RGRWはGabidulinの最小ランク重みの一般化

Relative Generalized Hamming Weightとの関係

$V_{\mathcal{I}} = \{x \in \mathbb{F}_{q^m}^n : x_i = 0 \text{ if } i \notin \mathcal{I}\}$ for $\mathcal{I} \subseteq \{1, \ldots, n\}$. $\dim_{\mathbb{F}_{q^m}} V_{\mathcal{I}} = |\mathcal{I}|$.

$\mathbb{F}_{q^m}$-線形符号$C_2 \subsetneq C_1 \subseteq \mathbb{F}_{q^m}^n$の i-th Relative Generalized Hamming Weight (RGHW) [LMHC05]:

$$\min_{\mathcal{I} \subseteq \{1,\ldots,n\}} \left\{ \dim_{\mathbb{F}_{q^m}} V_{\mathcal{I}} : \dim_{\mathbb{F}_{q^m}} (C_1 \cap V_{\mathcal{I}}) - \dim_{\mathbb{F}_{q^m}} (C_2 \cap V_{\mathcal{I}}) \geq i \right\}.$$

C_1のi-th Generalized Hamming Weight (GHW) [Wei91]:

$$\min_{\mathcal{I} \subseteq \{1,\ldots,n\}} \left\{ \dim_{\mathbb{F}_{q^m}} V_{\mathcal{I}} : \dim_{\mathbb{F}_{q^m}} (C_1 \cap V_{\mathcal{I}}) \geq i \right\}.$$

そしてRGRWは,

$$\min \left\{ \dim_{\mathbb{F}_{q^m}} V : V \in \Gamma, \dim_{\mathbb{F}_{q^m}} (C_1 \cap V) - \dim_{\mathbb{F}_{q^m}} (C_2 \cap V) \geq i \right\}.$$

RGRWとRGHWの違いは，C_1, C_2との共通集合を取る部分空間の集合だけ.

まとめると

- RGRWはGabidulinの最小ランク重みの一般化
- RGRWとRGHWの違いはC_1, C_2との共通集合を取る部分空間の集合だけ

⇒ これらから「Relative Generalized Rank Weight」という名前に.

1. セキュアネットワーク符号化の紹介
2. この発表で紹介する研究の狙い
3. 新しい符号パラメータの紹介
4. 符号パラメータとセキュアネットワーク符号化の安全性

ネットワーク構造に依存しない安全性

ネットワーク構造に依存せず保障される安全性の評価とは，任意の$B \in \mathbb{F}_q^{n\times\mu}$についての$S$と$XB$の相互情報量の最大値

$$\max\left\{I(S\,;XB) : B \in \mathbb{F}_q^{n\times\mu}\right\},$$

を評価すること．すなわち盗聴者の行列の集合が$\mathcal{B} = \mathbb{F}_q^{n\times\mu}$のネットワークを考慮する．

以降，log底はq^mとする．

RGRWのセキュアネットワーク符号化への応用

定理 (RGRWのセキュアネットワーク符号への応用)

盗聴者がSの情報を$j \log_2 q^m$ $(1 \leq j \leq \dim_{\mathbb{F}_{q^m}} C_1/C_2)$ビット以上得る

$$\max \left\{ I(S; XB) : B \in \mathbb{F}_q^{n \times \mu} \right\} \geq j.$$

$$\Updownarrow$$

盗聴リンク数μが双対符号$C_2^\perp, C_1^\perp$のj-th RGRW 以上

$$\mu \geq M_{R,j}(C_2^\perp, C_1^\perp).$$

系

盗聴リンク数が$M_{R,1}(C_2^\perp, C_1^\perp)$未満であればネットワーク構造に依存せず$S$の情報は一切得られない

C_1, C_2を線形MRD符号に固定した時，Silva-Kschischangの定理と一致する．つまり，

$$M_{R,1}(C_2^{\perp}, C_1^{\perp}) = \dim_{\mathbb{F}_{q^m}} C_2 + 1.$$

シンクノードでの誤り訂正能力

N本の入力リンクを持つ1つのシンクノードを固定.
$A \in \mathbb{F}_q^{n \times N}$: ソースノードからシンクノードへの遷移行列（誤りがなければXAが受信される）
シンクノードはAを知っていると仮定.
送信経路の途中のtリンクから誤りが乗ってくると仮定.

定理 (RGRWのセキュアネットワーク符号の誤り訂正能力への応用)

シンクノードは，いかなる遷移行列$A \in \mathbb{F}_q^{n \times N}$, rank$A \geq n - \rho$に対しても，

$$M_{R,1}(C_1, C_2) > 2t + \rho$$

が満たされれば，あらゆるtリンク誤りを訂正しSを正しく復号できる.

これも，C_1, C_2を線形MRD符号に固定した時,
Silva-Kschischangの定理と一致する．　つまり,

$$M_{R,1}(C_1, C_2) = n - \dim_{\mathbb{F}_{q^m}} C_1 + 1$$

発表のまとめ

まとめ：今日の発表内容

線形符号によるセキュアネットワーク符号化についての最新[7]の結果の紹介

- j-th RGRW $M_{R,j}(C_1, C_2)$という符号パラメータを提案
- RGRWはGabidulinの提案した最小ランク重みの一般化
- $\max_{B \in \mathbb{F}_q^{n \times \mu}} I(S; XB) \geq j \Leftrightarrow$ 盗聴リンク数$\mu \geq M_{R,j}(C_2^{\perp}, C_1^{\perp})$

[7]そうでもない…

おまけ：産業界でのネットワーク符号化

今現在は，鳴かず飛ばずです.

- ネットワークの人は基盤ネットワークに入れたくない
- 分散ストレージ符号も，広く使われているHadoopなどに入れ込むのは難しい
- etc....

課題点は【既存システムへの導入の難しさ】【システムデザインから符号化を前提にしなければならない】【符号化・復号処理の計算量もバカにならない】など.

それでもネットワーク・無線分野の人なども符号化の有用性は重々わかっているので，未来はある（と信じている）し，Hetero-genius network, 5G, ICN などの新しいキーワードに関連してくる可能性もある（と信じたい）

補足情報

すべての詳細な証明は以下の原稿に記載.

J. Kurihara, R. Matsumoto, and T. Uyematsu, “Relative Generalized Rank Weight and Its Applications to Network Coding,” Jan. 2013. [Online]. Available: arXiv:1301.5482 [cs.IT]

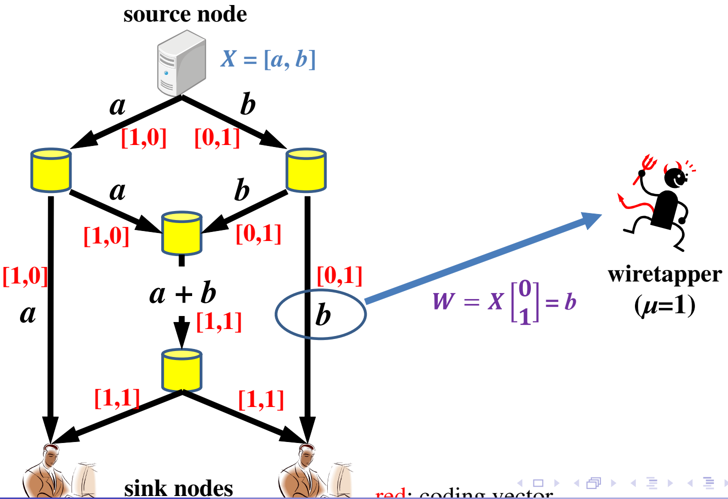
また、GRW (non-relative version, i.e., $C_1 = \mathbb{F}_{q^m}^n$)は同時期・独立に以下の文献でも提案.

F. Oggier and A. Sboui, “On the existence of generalized rank weights,” in Proc. ISITA 2012, Honolulu, Hawaii, USA, Oct. 2012, pp. 406–410.

Appendix

セキュアネットワーク符号化の具体例

$\mathbb{F}_q = \mathbb{F}_5$, $n = 2$, $m = 1$のネットワーク符号化において盗聴者は任意の$\mu = 1$リンクを盗聴． 盗聴行列の集合:$\mathcal{B} = \{[1,0],[0,1],[1,1]\}$.

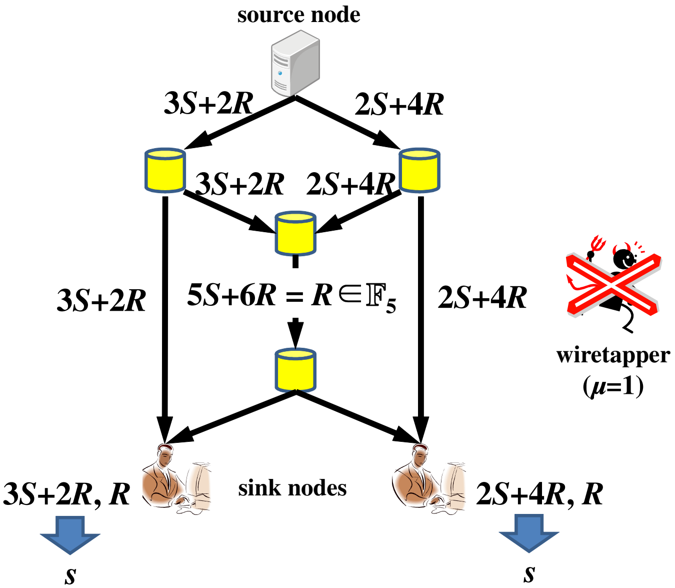


目的：秘密メッセージ$S \in \mathbb{F}_5$ $(l = 1)$を盗聴者に漏らすことなく正しくすべてのシンクノードに送信する.

このときは，例えば一様乱数$R \in \mathbb{F}_5$を用いて，$S \in \mathbb{F}_5$をXへ以下のように符号化してみる.

$$X = [3S + 2R, 2S + 4R]$$

すると，どの$\mu = 1$リンクからもSの情報は一切漏洩しない.



Relative Network Generalized Hamming Weight (RNGHW)

(R)GHWをネットワーク符号用に拡張しようという研究はすでに存在 [NYZ11, ZZ09].
ただし，ユニバーサルな設定ではない.

- ネットワーク構造を固定, $m = 1$.
- $\mathcal{F} \triangleq$そのネットワークのすべてのリンクeの符号化ベクトルb_eの集合
- $\Upsilon_{\mathcal{F}} \triangleq \mathcal{F}$の部分集合で張られる線形部分空間の集合

i-th RNGHW:

$$\min \left\{ \dim_{\mathbb{F}_{q^m}} V : V \in \Upsilon_{\mathcal{F}}, \dim_{\mathbb{F}_{q^m}}(C_1 \cap V) - \dim_{\mathbb{F}_{q^m}}(C_2 \cap V) \right\}$$

RGRWのΓ(ネットワーク非依存)を$\Upsilon_{\mathcal{F}}$(ネットワーク依存)に変えることでRNGHWになる.

RGHWとWiretap Channel II (秘密分散)

Wiretap Chanell II [OW84], 秘密分散 [Sha79]:

- 秘密メッセージ$S \in \mathbb{F}_{q^m}^l$を$X \in \mathbb{F}_{q^m}^n$に符号化して伝送路を送信
- 盗聴者はXの任意のμシンボルを盗聴
- Sに関する情報を盗聴者に漏らさぬように伝送することが目的

SからXへの符号化方法は$C_2 \subsetneq C_1 \subseteq \mathbb{F}_{q^m}^n$によるNested Coset Coding.
セキュアネットワーク符号化の特殊なケースとみなせる.

$X = [X_1, \ldots, X_n] \in \mathbb{F}_{q^m}^n$, $X_{\mathcal{I}} \triangleq (X_i : i \in \mathcal{I})$ for $\mathcal{I} \subseteq \{1, \ldots, n\}$.

定理 (RGHWのWiretap Chanell II・秘密分散への応用)

盗聴者がSの情報を$j \log_2 q^m$ $(1 \leq j \leq \dim_{\mathbb{F}_{q^m}} C_1/C_2)$ビット以上得る

$$\max\{I(S; X_{\mathcal{I}}) : \mathcal{I} \subseteq \{1, \ldots, n\}\} \geq j.$$

$$\Updownarrow$$

盗聴シンボル数μが双対符号$C_2^\perp, C_1^\perp$のj-th RGHW 以上

$$\mu \geq j\text{-th RGHW of } C_2^\perp \text{ and } C_1^\perp.$$

系

盗聴シンボル数が$C_2^\perp, C_1^\perp$の1st RGHW未満であればSの情報は一切得られない

上記の結果は DOI: 10.1587/transfun.E95.A.2067 [KUM11]で報告

私たちの研究の位置づけ

- Wiretap Channel II(WC2)・秘密分散: セキュアネットワーク符号化の特殊ケース
- 線形符号のRelative Generalized Hamming Weight (RGHW) [LMHC05, Wei91]: WC2・秘密分散における符号化の安全性を示す符号パラメータ

$$\Downarrow$$

ネットワーク符号化の世界で，WC2・秘密分散とRGHWの関係性と同様の理論を，符号パラメータの提案から全て構築

漏洩情報量に関する定理

[準備] 条件付きエントロピー[CT06]:

$$
\begin{aligned}
H(A|B) &\triangleq \sum_{a\in\mathcal{A},b\in\mathcal{B}} P_{A,B}(a,b)\log\frac{1}{P_{A|B}(a|b)} \\
&= \sum_{b\in\mathcal{B}} P_B(b)H(A|B=b) \\
&= H(A) - I(A;B)
\end{aligned}
$$

$I(S;XB) = H(XB) - H(XB|S)$.
SとXの一様分布を仮定していると，XはC_1の全要素を実現値として取りうる一様分布の確率変数．このことから，以下が成立．[8]

$$\begin{aligned} H(XB) &= \log_{q^m} \text{the number of possible } XB \\ &= \log_{q^m} |\text{image of map } C_1 \to \{XB : X \in C_1\}| \\ &= \dim_{\mathbb{F}_{q^m}} C_1 - \dim_{\mathbb{F}_{q^m}} (C_1 \cap \text{Ker}\,(B)), \end{aligned}$$

$$\begin{aligned} H(XB|S) &= \log_{q^m} \text{the number of possible } XB \text{ given } S = s \\ &= \log_{q^m} \text{the number of possible } XB \text{ given } \psi(S) = C_2 \\ &= \log_{q^m} |\text{image of map } C_2 \to \{XB : X \in C_2\}| \\ &= \dim_{\mathbb{F}_{q^m}} C_2 - \dim_{\mathbb{F}_{q^m}} (C_2 \cap \text{Ker}\,(B)). \end{aligned}$$

よって，
$$\begin{aligned} I(S;XB) &= H(XB) - H(XB|S) \\ &= \dim_{\mathbb{F}_{q^m}} C_1 - \dim_{\mathbb{F}_{q^m}} C_2 \\ &\quad - (\dim_{\mathbb{F}_{q^m}} (C_1 \cap \text{Ker}\,(B)) - \dim_{\mathbb{F}_{q^m}} (C_2 \cap \text{Ker}\,(B))). \end{aligned}$$

[8] 任意の分布だと相対エントロピー[CT06]を使って上界・下界を導出．

Extension of Forney's second duality lemma

$\mathbb{F}_{q^m}$-線形部分空間$C_1 \subseteq \mathbb{F}_{q^m}^n$とその部分符号$C_2 \subsetneq C_1$, 任意の部分空間$V \subseteq \mathbb{F}_{q^m}^n$について

$$\begin{aligned}&\dim_{\mathbb{F}_{q^m}}(C_1 \cap V) - \dim_{\mathbb{F}_{q^m}}(C_2 \cap V)\\ &\quad = \dim_{\mathbb{F}_{q^m}} C_1/C_2 - \dim_{\mathbb{F}_{q^m}}(C_2^\perp \cap V^\perp) + \dim_{\mathbb{F}_{q^m}}(C_1^\perp \cap V^\perp).\end{aligned}$$

$$\begin{aligned}I(S;XB) &= \dim_{\mathbb{F}_{q^m}} C_1 - \dim_{\mathbb{F}_{q^m}} C_2\\ &\quad - \underbrace{(\dim_{\mathbb{F}_{q^m}}(C_1 \cap \text{Ker }(B)) - \dim_{\mathbb{F}_{q^m}}(C_2 \cap \text{Ker }(B)))}_{=\dim_{\mathbb{F}_{q^m}} C_1/C_2 - \dim_{\mathbb{F}_{q^m}}(C_2^\perp \cap \text{Ker }(B)^\perp) + \dim_{\mathbb{F}_{q^m}}(C_1^\perp \cap \text{Ker }(B)^\perp)}\\ &= \dim_{\mathbb{F}_{q^m}}(C_2^\perp \cap \text{Ker }(B)^\perp) - \dim_{\mathbb{F}_{q^m}}(C_1^\perp \cap \text{Ker }(B)^\perp)\\ &= \dim_{\mathbb{F}_{q^m}}(C_2^\perp \cap \langle B \rangle) - \dim_{\mathbb{F}_{q^m}}(C_1^\perp \cap \langle B \rangle)\end{aligned}$$

$\cdots \text{Ker }(B)^\perp = \mathbb{F}_{q^m}$-線形列空間$\langle B \rangle \triangleq \{Bx : x \in \mathbb{F}_{q^m}^{\mu \times 1}\} \subseteq \mathbb{F}_{q^m}^n$.

RGRWのセキュアネットワーク符号化への応用の定理の証明

相互情報量を$I(S\,;XB) = j$得るために必要な盗聴リンク数の最小値は,

$$
\begin{aligned}
&\min_{B\in\mathbb{F}_q^{n\times\mu}} \{\mu : I(S\,;XB) = j\} \\
&= \min_{B\in\mathbb{F}_q^{n\times\mu}} \left\{\mu : \dim_{\mathbb{F}_{q^m}}(C_2^{\perp} \cap \langle B\rangle) - \dim_{\mathbb{F}_{q^m}}(C_1^{\perp} \cap \langle B\rangle) = j\right\} \\
&= \min_{V\in\Gamma} \left\{\dim_{\mathbb{F}_{q^m}} V : \dim_{\mathbb{F}_{q^m}}(C_2^{\perp} \cap V) - \dim_{\mathbb{F}_{q^m}}(C_1^{\perp} \cap V) = j\right\} \\
&= M_{R,j}(C_2^{\perp}, C_1^{\perp})
\end{aligned}
$$

Relative Dimension/Intersection Profile (RDIP)

漏洩情報量の定理の一般化と$\mathbb{F}_{q^m}$-線形部分空間のq乗の性質から，

$$
\begin{aligned}
&\max\left\{I(S;XB) : B \in \mathbb{F}_q^{n\times\mu}\right\}\\
&= \max_{B\in\mathbb{F}_q^{n\times\mu}} \left\{\dim_{\mathbb{F}_{q^m}}(C_2^{\perp} \cap \langle B\rangle) - \dim_{\mathbb{F}_{q^m}}(C_1^{\perp} \cap \langle B\rangle)\right\}\\
&= \max_{V\in\Gamma, \dim_{\mathbb{F}_{q^m}} V\le\mu} \left\{\dim_{\mathbb{F}_{q^m}}(C_2^{\perp} \cap V) - \dim_{\mathbb{F}_{q^m}}(C_1^{\perp} \cap V)\right\}\\
&= \max_{V\in\Gamma, \dim_{\mathbb{F}_{q^m}} V=\mu} \left\{\dim_{\mathbb{F}_{q^m}}(C_2^{\perp} \cap V) - \dim_{\mathbb{F}_{q^m}}(C_1^{\perp} \cap V)\right\}
\end{aligned}
$$

i-th RDIP

$\mathbb{F}_{q^m}$-線形符号$C_1 \subseteq \mathbb{F}_{q^m}^n$および部分符号$C_2 \subsetneq C_1$について，　$K_{R,i}(C_1, C_2) \triangleq \max\left\{\dim_{\mathbb{F}_{q^m}}(C_1 \cap V) - \dim_{\mathbb{F}_{q^m}}(C_2 \cap V) : V \in \Gamma, \dim_{\mathbb{F}_{q^m}} V = i\right\}$.

定理 (RDIPのセキュアネットワーク符号への応用)

μ本の盗聴リンクから漏洩するSの情報量の最大値は,

$$\max\left\{I(S\,;XB) : B \in \mathbb{F}_q^{n\times\mu}\right\} = K_{R,\mu}(C_2^{\perp}, C_1^{\perp}).$$

非一様分布への拡張

確率変数$A, B \in \mathcal{X}$の確率分布P_A, P_B間の相対エントロピー[CT06]:

$$D(A\|B) \triangleq \sum_{a \in \mathcal{X}} P_A(a) \log \frac{P_A(a)}{P_B(a)}.$$

確率変数$C \in \mathcal{Y}$が与えられたときの$A, B \in \mathcal{X}$の条件付き確率分布$P_{A|C}, P_{B|C}$間の相対エントロピー[CT06]:

$$D(A\|B|C) \triangleq \sum_{y \in \mathcal{Y}} P_C(y) \sum_{x \in \mathcal{X}} P_{A|C}(x|y) \log \frac{P_{A|C}(x|y)}{P_{B|C}(x|y)}.$$

$U_{\mathcal{A}}$: $\mathcal{A}$上の一様分布の確率変数．任意の分布に従うS, Xに対して,

$$I(S; XB) \leq \dim_{\mathbb{F}_{q^m}}(C_2^\perp \cap \langle B \rangle) - \dim_{\mathbb{F}_{q^m}}(C_1^\perp \cap \langle B \rangle) + D(X\|U_{\psi(S)}|S),$$

および

$$I(S; XB) \geq \dim_{\mathbb{F}_{q^m}}(C_2^\perp \cap \langle B \rangle) - \dim_{\mathbb{F}_{q^m}}(C_1^\perp \cap \langle B \rangle) - D(S\|U_{\mathbb{F}_{q^m}^l}),$$

が成立する．

参考文献 I

[ACLY00] R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung, "Network information flow," IEEE Trans. Inf. Theory, vol. 46, no. 4, pp. 1204–1216, Jul. 2000.

[CC11] N. Cai and T. Chan, "Theory of secure network coding," Proc. IEEE, vol. 99, no. 3, pp. 421–437, Mar. 2011.

[CT06] T. M. Cover and J. A. Thomas, Elements of Information Theory, 2nd ed. Wiley-Interscience, Jan. 2006.

[CY02] N. Cai and R. W. Yeung, "Secure network coding," in Proc. IEEE ISIT 2002, Lausanne, Switzerland, Jun. 2002.

[Gab85] E. M. Gabidulin, "Theory of codes with maximum rank distance," Probl. Inf. Transm., vol. 21, no. 1, pp. 1–12, 1985.

[HMK+06] T. Ho, M. Médard, R. Koetter, D. R. Karger, M. Effros, J. Shi, and B. Leong, "A random linear network coding approach to multicast," IEEE Trans. Inf. Theory, vol. 52, no. 10, pp. 4413–4430, Oct. 2006.

[KUM11] J. Kurihara, T. Uyematsu, and R. Matsumoto, "Secret sharing schemes based on linear codes can be precisely characterized by the relative generalized Hamming weight," IEICE Trans. Fundamentals, vol. E95-A, no. 11, pp. 2067–2075, Nov. 2011.

[LMHC05] Y. Luo, C. Mitrpant, A. J. Han Vinck, and K. Chen, "Some new characters on the wire-tap channel of type II," IEEE Trans. Inf. Theory, vol. 51, no. 3, pp. 1222–1229, Mar. 2005.

[LY03] S.-Y. R. Li and R. W. Yeung, "Linear network coding," IEEE Trans. Inf. Theory, vol. 49, no. 2, pp. 371–381, Feb. 2003.

[NYZ11] C.-K. Ngai, R. W. Yeung, and Z. Zhang, "Network generalized Hamming weight," IEEE Trans. Inf. Theory, vol. 57, no. 2, pp. 1136–1143, Feb. 2011.

[OW84] L. H. Ozarow and A. D. Wyner, "The wire-tap channel II," AT&T Bell Labs. Tech. J., vol. 63, no. 10, pp. 2135–2157, Dec. 1984.

[Sha79] A. Shamir, "How to share a secret," Commun. ACM, vol. 22, no. 11, pp. 612–613, 1979.

参考文献 II

[SK11] D. Silva and F. R. Kschischang, “Universal secure network coding via rank-metric codes,” IEEE Trans. Inf. Theory, vol. 57, no. 2, pp. 1124–1135, Feb. 2011.

[Sti90] H. Stichtenoth, “On the dimension of subfield subcodes,” IEEE Trans. Inf. Theory, vol. 36, no. 1, pp. 90–93, 1990.

[Wei91] V. K. Wei, “Generalized Hamming weights for linear codes,” IEEE Trans. Inf. Theory, vol. 37, no. 5, pp. 1412–1418, May 1991.

[ZZ09] Z. Zhang and B. Zhuang, “An application of the relative network generalized Hamming weight to erroneous wiretap networks,” in Proc. IEEE ITW 2009, Taormina, Sicily, Italy, Oct. 2009, pp. 70–74.