情報理論的安全性に基づく放送型暗号

～古典的結果と最近の進展～

渡邉 洋平（電気通信大学）

情報理論研究会
2017/9/8

自己紹介

- 渡邉 洋平 (わたなべ ようへい)
- 学位: 博士 (情報学) (横浜国立大学)
- 専門: 現代暗号理論
  - 特に (計算量的) 公開鍵暗号及び情報理論的暗号

[略歴]

- 2007/4-2011/3 横浜国立大学 工学部 電子情報工学科
- 2011/4-2013/3 同大学大学院環境情報学府 博士課程前期
- 2013/4-2016/3 同大学大学院環境情報学府 博士課程後期
- 2013/4-2016/3 JSPS特別研究員(DC1) @横浜国立大学
- **2016/4-現在 JSPS特別研究員(PD) @電気通信大学**
- **2016/4-現在 産業技術総合研究所 情報技術研究部門 協力研究員**
- 2016/9 4th Heidelberg Laureate Forum 招待

Heidelberg Laureate Forum（HLF）

Laureates of Mathematics and Computer Sciences Meet the Next Generation

Laureates: Turing, Abel, Fields賞受賞者(20~30名)

Next Generation: 審査を通過した若手研究者 (約200名)

目的：Laureatesと若手研究者の交流
開催時期：毎年9月半ば〜9月末
場所：ハイデルベルク大学 (ドイツ)

2013年から開催され, 2017年で5回目

ⓘ http://ohta-lab.jp/users/y.watanabe/ja/activity/#HLF

具体的に何をするのか？

6日間に渡り，以下のプログラムを共に過ごす

- ✓ Laureatesによる講演 (45分×15~17名)
- ✓ ほぼ毎日豪華なランチ&ディナー
- ✓ 多数のSocial Events
  - ハイデルベルク市街地ツアー
  - Boat Trip (ネッカー川)
  - Speyer City Tour
  - ハイデルベルク城ツアー
- ✓ パネルディスカッション
  - 2015年はビッグデータ，2016年は人工知能，今年は量子計算
- ✓ その他，ワークショップ，企業訪問等

ⓘ http://ohta-lab.jp/users/y.watanabe/ja/activity/#HLF

どうすれば参加できるのか？

Webサイトから申請 (**次回申請締切: 2018年2月中旬**)

- ✓ **大学院生〜ポスドク研究者**が申請可能
  - ✓ 申請資格は厳密ではなく，それ以上のポジションでも申請可能
  - ✓ **企業研究者**でも申請可能
  - ✓ 修士学生，博士学生，(ポスドク) 研究者の3回申請可能とのこと
- ✓ 参加費用は**ほぼ全て無料** (交通費以外)
  - ✓ HLF参加費
  - ✓ 宿泊費
  - ✓ 食事代
  - ✓ 保険費用
- ✓ 交通費をサポートしてくれる団体

  JDC財団，NEC C&C財団

ⓘ http://ohta-lab.jp/users/y.watanabe/ja/activity/#HLF

JDC財団について

1. **若手研究者の海外学会活動の支援**
2. 算額の再興と国際的認知度の向上

運営委員会

委員長	今井 秀樹	東京大学　名誉教授
委員	平田 康夫	(株)国際電気通信基礎技術研究所 代表取締役
委員	安田 豊	(財)KDDI 元理事長
委員	舩橋 晴雄	(株)シリウスインスティチュート 代表取締役
委員	四方 順司	横浜国立大学　教授
委員	井沼 学	城西大学　准教授
委員	竹内 新	ジャパンデータコム(株) 代表取締役
委員	石田 祐子	ジャパンデータコム(株) 会長
委員	梶川 仁美	一般財団法人JDC学術研究奨励会 副理事長

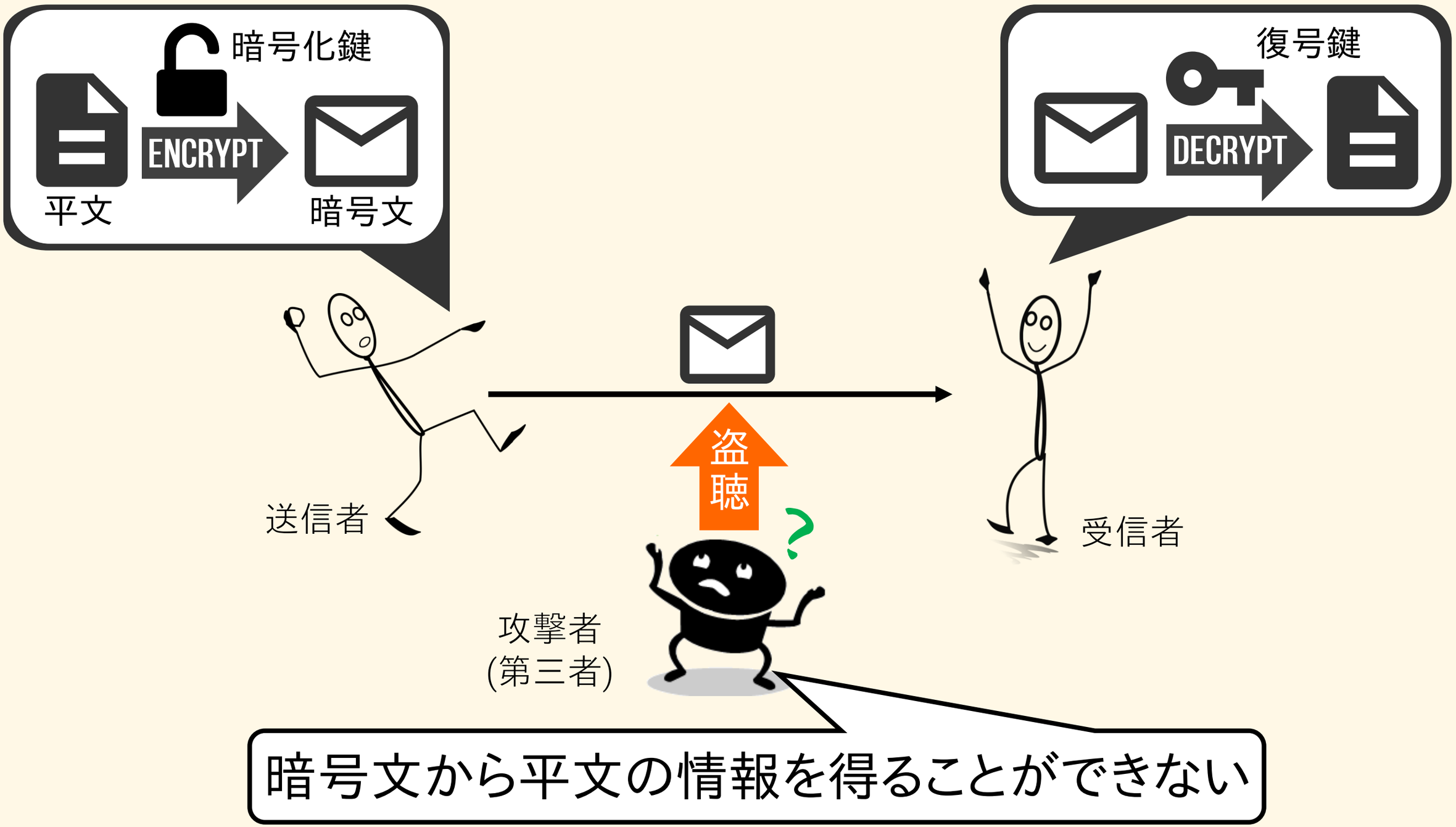
ⓘ http://ohta-lab.jp/users/y.watanabe/ja/activity/#HLF

OUTLINE

- ☑ 準備と本発表の位置づけ
- ☑ 放送型暗号 (Broadcast Encryption: BE)
  - ☐ $(t, \leq \omega)$-secure BEと$(\leq n, \leq \omega)$-secure BE
- ☑ Key Predistribution System (KPS) との関係
- ☑ 暗号文長と秘密鍵長のトレードオフ
  - ☐ $(t, \leq \omega)$-secure BEにおける鍵長の下界と構成法
  - ☐ $(\leq n, \leq \omega)$-secure BEにおける鍵長の下界と構成法
- ☑ 放送型暗号の拡張
  - ☐ BE for Cloud Environments
  - ☐ BE with Specific Broadcast Channels
  - ☐ BE with Relaxed Security Definitions

暗号化方式(ENCRYPTION)とは

- Goal: 通信路上の平文(データ)が漏洩することを防ぐ



安全性基準

計算量的安全性 (Computational Security)

攻撃者: **多項式時間アルゴリズム (実世界における計算機)**

- 😐 保証期間: **高々数十年**
- ☹ 量子計算機への耐性: **多くの方式が耐性なし**
- ☺ 公開鍵方式: **実現可能**
- ☺ 鍵長: (比較的) **短い**

実用性
(効率性)

Trade-off

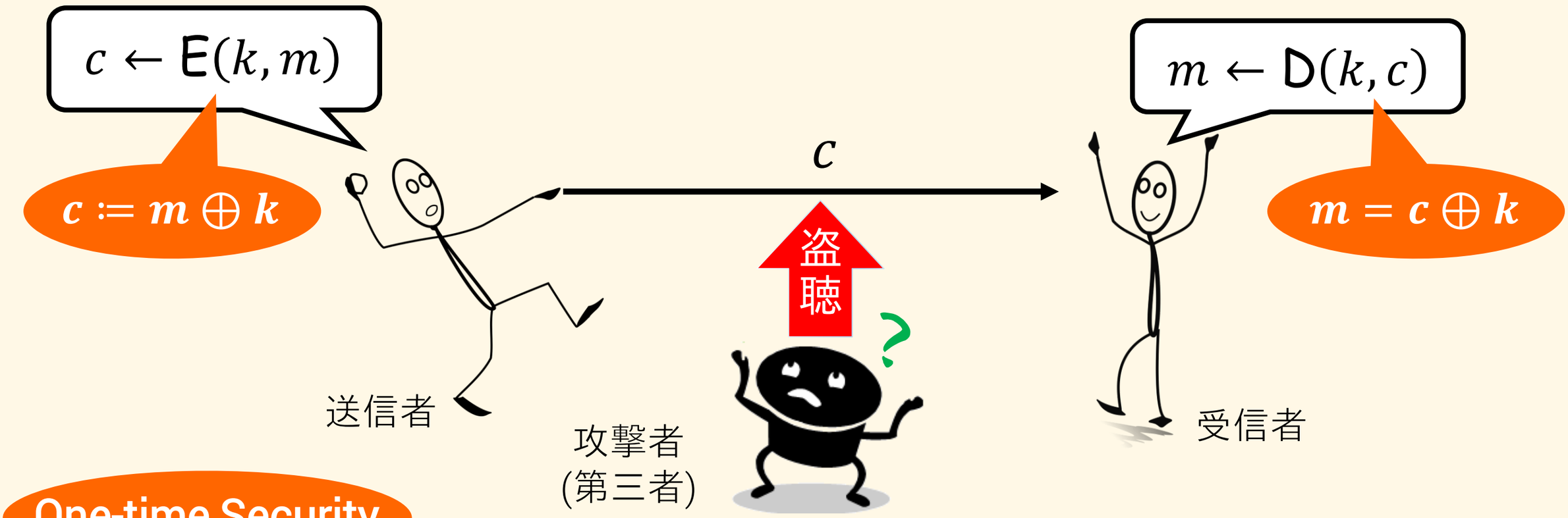
安全性
レベル

情報理論的安全性 (Information-Theoretic Security)

攻撃者: **あらゆるアルゴリズム (量子計算機を含む)**

- ☺ 保証期間: **長期 (理論上限界なし)**
- ☺ 量子計算機への耐性: **耐性有り (安全性が崩れない)**
- ☹ 公開鍵方式: **実現不可能**
- ☹ 鍵長: (非常に) **長い**

共通鍵暗号 (SYMMETRIC-KEY ENCRYPTION: SKE)



One-time Security

完全秘匿性 (Perfect Secrecy) [Shannon49]

$$H(M \mid C) = H(M)$$

鍵長の下界 [Shannon49]

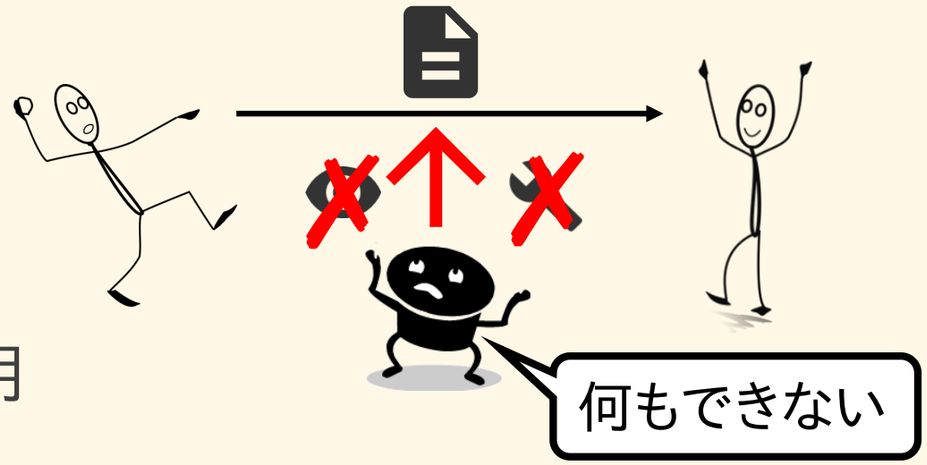
$$H(K) \geq H(M)$$

最適な構成法: ワンタイムパッド (One-Time Pad: OTP) [Vernam26]

通信路

☑ Secure Channel

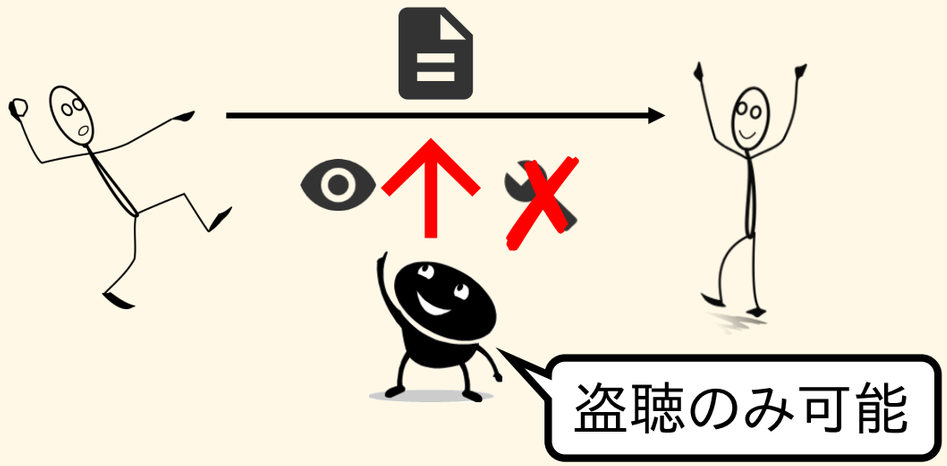
- ✓ 秘匿性:有
- ✓ 完全性:有
- ✓ (初期) 秘密情報の配布等に利用



暗号化方式の目的

☑ Authenticated Channel

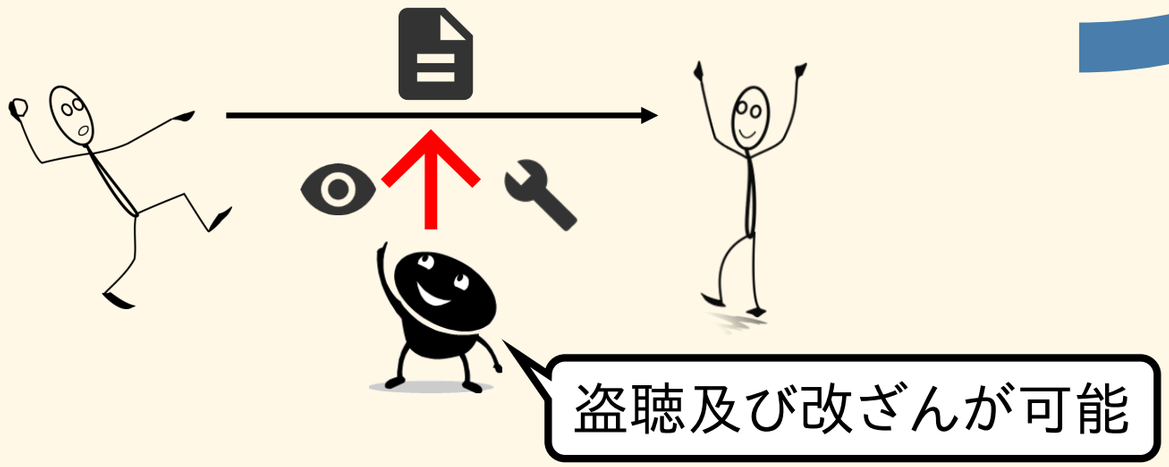
- ✓ 秘匿性:無
- ✓ 完全性:有
- ✓ 主に暗号化方式で仮定



認証方式の目的

☑ Insecure Channel

- ✓ 秘匿性:無
- ✓ 完全性:無
- ✓ 主に認証方式で仮定



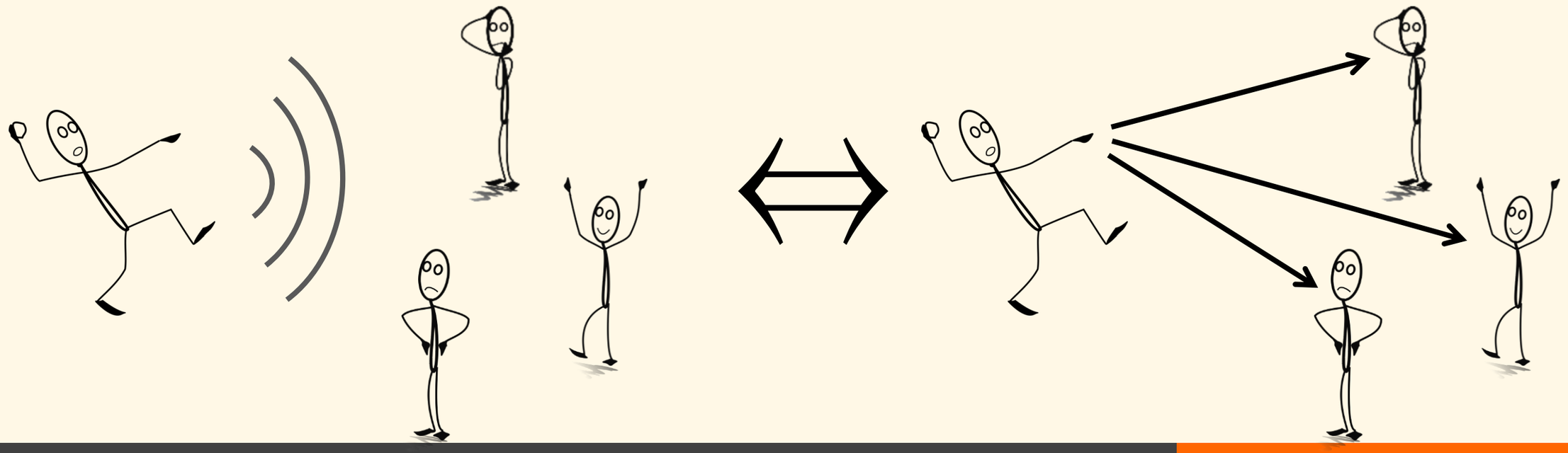
通信路に関するその他の仮定

- ☑ 攻撃者は以下の攻撃を行わないものとする
  - 通信路の切断
  - 受信を遅延させる攻撃
  - 受信者に届かないようにする攻撃

- ☑「放送する」

  ⇔「他の全てのエンティティにAuthenticated Channelを通じて送信する」

  - 放送された情報は全員に**同時に**届くものとする



現代暗号理論分野と本発表の位置づけ

計算量的安全性
Computational Security

情報理論的安全性
Information-Theoretic Security

基礎

計算量仮定の解析　　種々の安全性間の関係性

暗号プロトコルの提案･効率化

SSL/TLSの理論的解析　　物理層セキュリティ

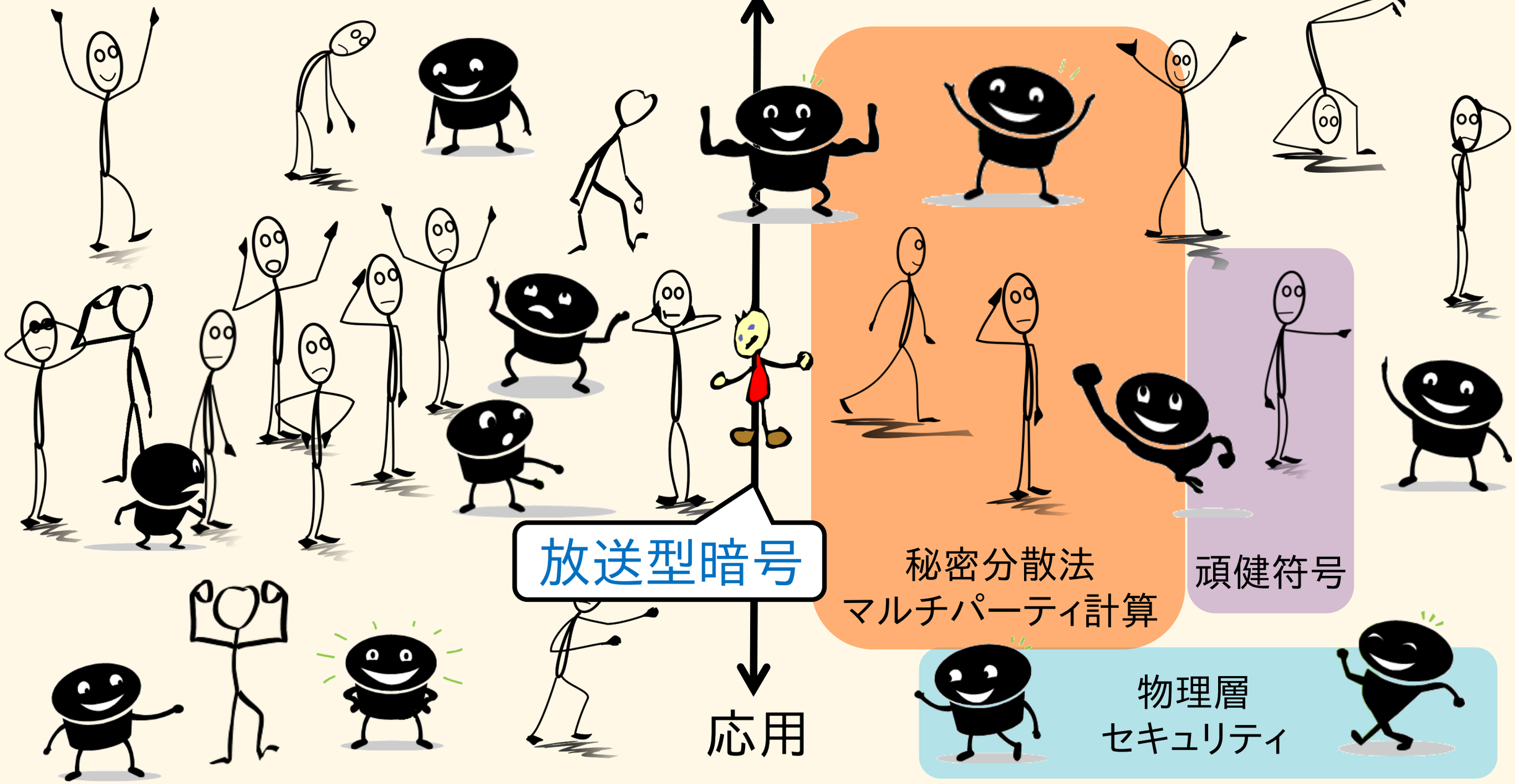
応用

現代暗号理論分野と本発表の位置づけ

計算量的安全性
Computational Security

情報理論的安全性
Information-Theoretic Security

基礎



放送型暗号

応用

秘密分散法
マルチパーティ計算

頑健符号

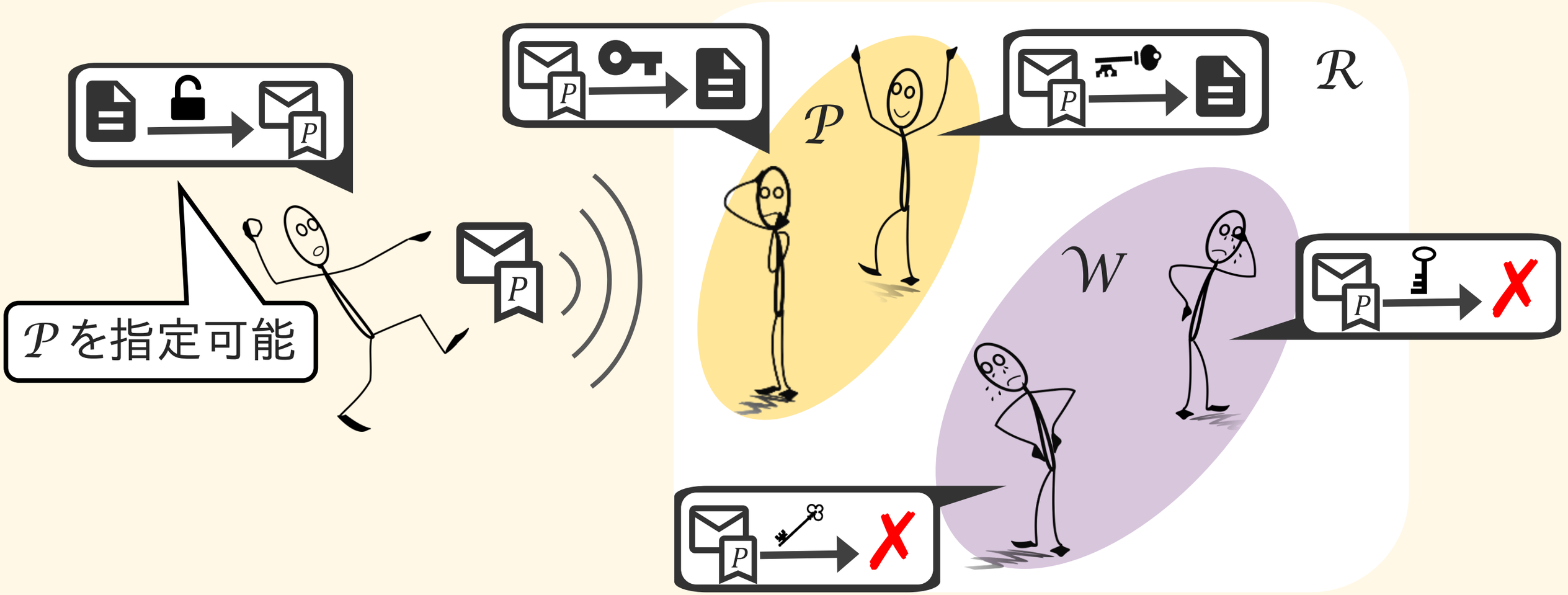
物理層
セキュリティ

OUTLINE

- ☑ 準備と本発表の位置づけ
- ☑ 放送型暗号 (Broadcast Encryption: BE)
  - ☐ $(t, \leq \omega)$-secure BEと$(\leq n, \leq \omega)$-secure BE
- ☑ Key Predistribution System (KPS) との関係
- ☑ 暗号文長と秘密鍵長のトレードオフ
  - ☐ $(t, \leq \omega)$-secure BEにおける鍵長の下界と構成法
  - ☐ $(\leq n, \leq \omega)$-secure BEにおける鍵長の下界と構成法
- ☑ 放送型暗号の拡張
  - ☐ BE for Cloud Environments
  - ☐ BE with Specific Broadcast Channels
  - ☐ BE with Relaxed Security Definitions

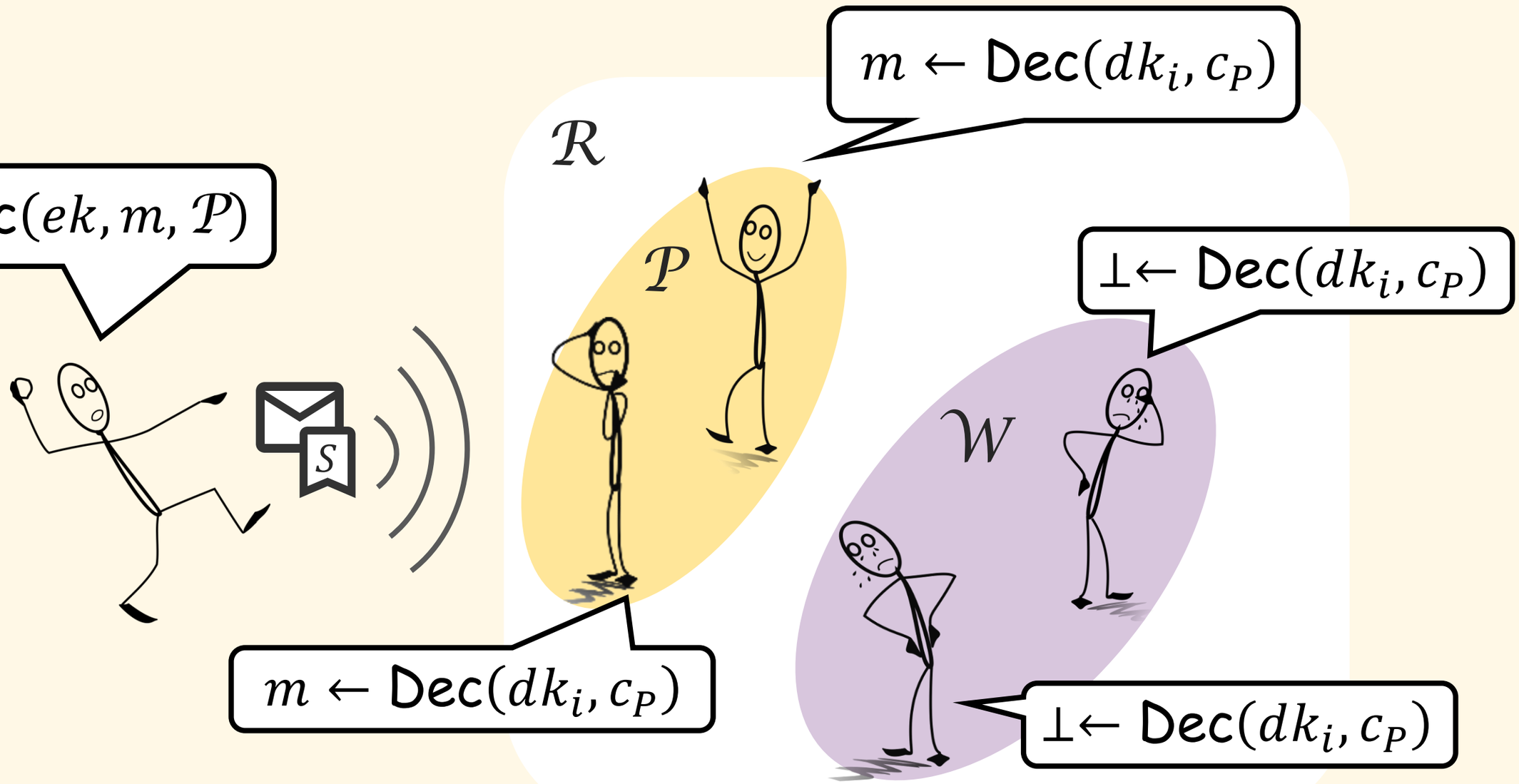
放送型暗号 (BROADCAST ENCRYPTION: BE)

- Goal: 暗号学的アクセス制御
  - ✓ $\mathcal{R}$: n人の受信者全体の集合
  - ✓ 復号を許す受信者 (受信者集合) $\mathcal{P} \subset \mathcal{U}$ を指定可能
  - ✓ 結託集合 $\mathcal{W} \subset \mathcal{R} \setminus \mathcal{P}$ ($|\mathcal{W}| \leq \omega$) に対して 📄 の情報が漏れない



BE: MORE FORMALLY

$(ek, dk_1, dk_2, \ldots, dk_n) \leftarrow \mathsf{Setup}(n, P_{EK,DK_1,\ldots,DK_n})$



$\mathcal{P}$ の範囲によって2種類のBEにクラス分けされる

$(t, \leq \omega)$-SECURE BE & $(\leq n, \leq \omega)$-SECURE BE

安全性の直感

$\mathcal{P} \subset \mathcal{R}$に含まれない高々$\omega$人 $(\mathcal{W} \subset \mathcal{R} \setminus \mathcal{P})$ が結託したとしても平文の情報を得ることができない

- ☑ $\mathcal{P} \subset \mathcal{U}$ s.t. $|\mathcal{P}| = t$ → $(t, \leq \omega)$-secure BE $(\omega \coloneqq n - t)$
- ☑ 任意の$\mathcal{P} \subset \mathcal{U}$ → $(\leq n, \leq \omega)$-secure BE $(0 \leq \omega < n)$

完全秘匿性 (Perfect Secrecy)

BEは, 任意の $\begin{Bmatrix} \mathcal{P} \in \mathcal{P}(t) \\ \mathcal{P} \subset \mathcal{R} \end{Bmatrix}$, 任意の $\mathcal{W} \in \mathcal{W}(\mathcal{P}, \omega)$に対して

$H(M \mid C_P, DK_W) = H(M)$ を満たすとき, $\begin{Bmatrix} (t, \leq \omega) \\ (\leq n, \leq \omega) \end{Bmatrix}$-secure BEという

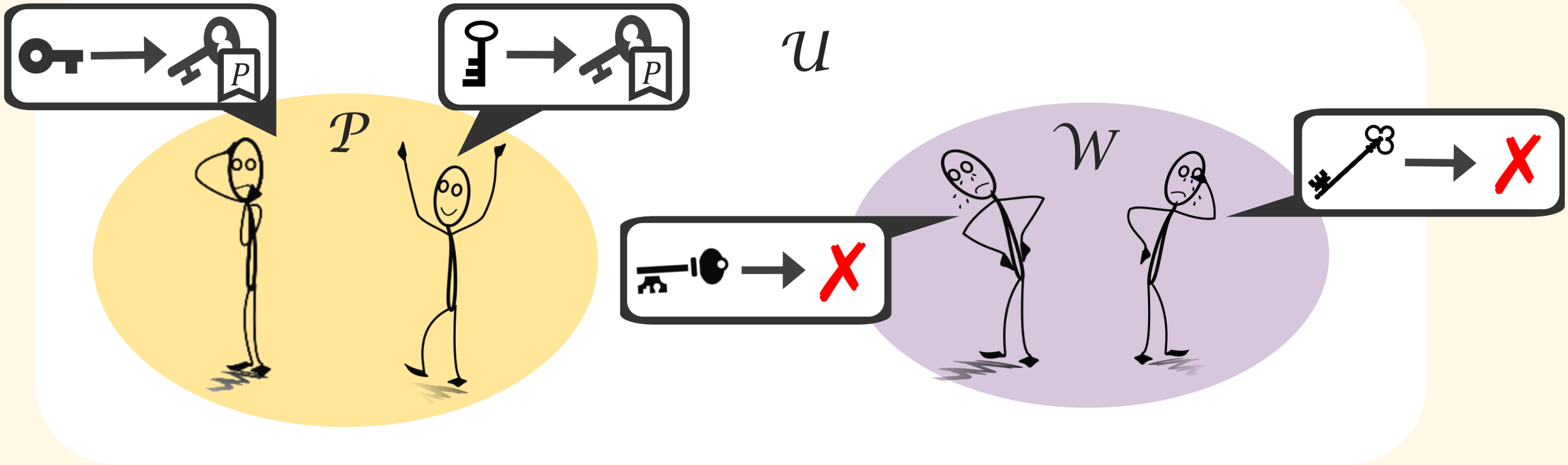
記法: $\mathcal{P}(t) \coloneqq \{\mathcal{P} \in \mathcal{R} \mid |\mathcal{P}| = t\}$, $\mathcal{W}(\mathcal{P}, \omega) \coloneqq \{\mathcal{W} \in \mathcal{R} \setminus \mathcal{P} \mid |\mathcal{W}| \leq \omega\}$

OUTLINE

- ☑ 準備と本発表の位置づけ
- ☑ 放送型暗号 (Broadcast Encryption: BE)
  - ☐ $(t, \leq \omega)$-secure BEと$(\leq n, \leq \omega)$-secure BE
- ☑ Key Predistribution System (KPS) との関係
- ☑ 暗号文長と秘密鍵長のトレードオフ
  - ☐ $(t, \leq \omega)$-secure BEにおける鍵長の下界と構成法
  - ☐ $(\leq n, \leq \omega)$-secure BEにおける鍵長の下界と構成法
- ☑ 放送型暗号の拡張
  - ☐ BE for Cloud Environments
  - ☐ BE with Specific Broadcast Channels
  - ☐ BE with Relaxed Security Definitions

KPS (KEY PREDISTRIBUTION SYSTEM) [Matsumoto-Imai88, Blom85]

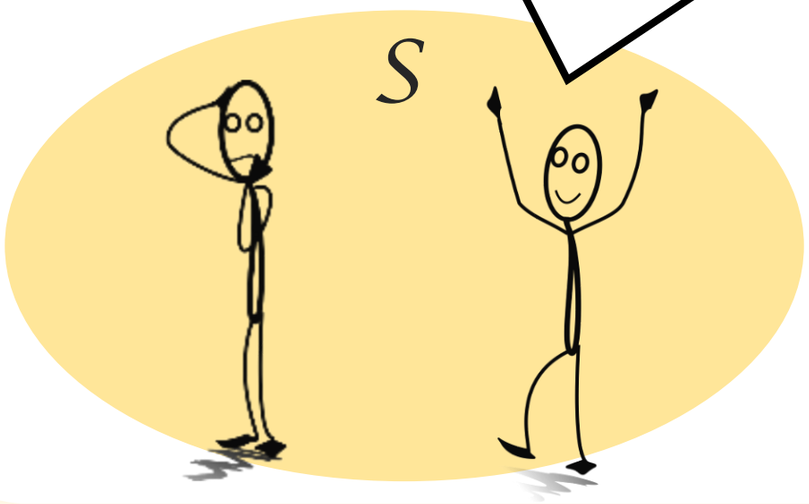
- 初期鍵を用いた非対話グループ鍵共有方式
  - ✓ $\mathcal{U}$: n人のユーザ集合
  - ✓ 任意のグループ $\mathcal{P} \subset \mathcal{U}$ 間で鍵  を (非対話で) 共有する
  - ✓ 結託集合 $\mathcal{W} \subset \mathcal{U} \setminus \mathcal{P}$ ($|\mathcal{W}| \leq \omega$) に対して  の情報が漏れない



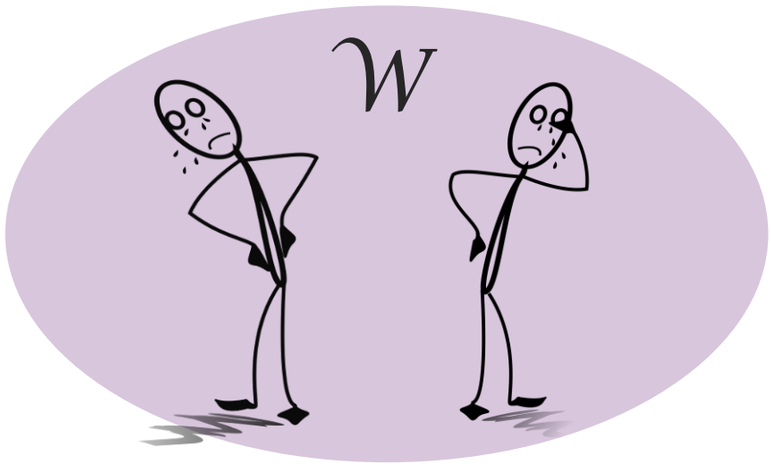
KPS: MORE FORMALLY…

$(uk_1, uk_2, \ldots, uk_n) \leftarrow \mathsf{Init}(n, P_{UK_1,\ldots,UK_n})$

$ck_P \leftarrow \mathsf{KeyDer}(uk_i, \mathcal{P})$



$\mathcal{U}$



KPSは，任意の $\begin{Bmatrix} \mathcal{P} \in \mathcal{P}(t) \\ \mathcal{P} \subset \mathcal{R} \end{Bmatrix}$，任意の $\mathcal{W} \in \mathcal{W}(\mathcal{P}, \omega)$に対して

$H(CK_P \mid UK_W) = H(CK_P)$ を満たすとき，$\begin{Bmatrix} (t, \leq \omega) \\ (\leq n, \leq \omega) \end{Bmatrix}$-KPSという

BEとKPSの同値性: BE FROM KPS

KPS → BE [Kurosawa-Yoshida-Desmedt-Burmester98]

$\begin{Bmatrix} (t, \leq \omega) \\ (\leq n, \leq \omega) \end{Bmatrix}$-KPSが存在する時, 全ての$\begin{Bmatrix} \mathcal{P} \in \mathcal{P}(t) \\ \mathcal{P} \subset \mathcal{R} \end{Bmatrix}$に対して

$|C_P| = |\mathcal{M}| = |\mathcal{CK}_P|$であるような$\begin{Bmatrix} (t, \leq \omega) \\ (\leq n, \leq \omega) \end{Bmatrix}$-secure BEが存在する

Idea: KPSで共有した鍵ck_Pで平文をワンタイムパッドする

- ☑ $(ek, dk_1, dk_2, \ldots, dk_n) \leftarrow \mathsf{Setup}(n, P_{EK,DK_1,\ldots,DK_n})$
  - ✓ Set $ek := (uk_1, uk_2, \ldots, uk_n) \leftarrow \mathsf{Init}(n, P_{UK_1,\ldots,UK_n})$ and $dk_i := uk_i$
- ☑ $c_P \leftarrow \mathsf{Enc}(ek, m, \mathcal{P})$
  - ✓ Output $c_P := m \oplus ck_P$, where $ck_P \leftarrow \mathsf{KeyDer}(uk_i, \mathcal{P})$
- ☑ $m \leftarrow \mathsf{Dec}(dk_i, c_P)$
  - ✓ Output $m = c_P \oplus ck_P$ if $R_i \in P$, otherwise output $\perp$.

BEとKPSの同値性: KPS FROM BE

BE → KPS [Kurosawa-Yoshida-Desmedt-Burmester98]

全ての$\begin{Bmatrix}\mathcal{P} \in \mathcal{P}(t) \\ \mathcal{P} \subset \mathcal{R}\end{Bmatrix}$に対して$|C_P| = |\mathcal{M}|$であるような$\begin{Bmatrix}(t, \leq \omega) \\ (\leq n, \leq \omega)\end{Bmatrix}$-secure BEが存在する時, 全ての$\begin{Bmatrix}\mathcal{P} \in \mathcal{P}(t) \\ \mathcal{P} \subset \mathcal{R}\end{Bmatrix}$に対して$|\mathcal{M}| = |\mathcal{CK}_P|$かつ$H(M) = H(CK_P)$であるような$\begin{Bmatrix}(t, \leq \omega) \\ (\leq n, \leq \omega)\end{Bmatrix}$-KPSが存在する

Idea: 平文を共有鍵として考える

- $(uk_1, uk_2, \ldots, uk_n) \leftarrow \mathsf{Init}(n, P_{UK_1,\ldots,UK_n})$
  - For every $\mathcal{P} \in \mathcal{P}(t)$ (or $\mathcal{P} \subset \mathcal{R}$), arbitrarily fix $c_P \in C_P$
  - Set $\mathrm{uk_i} := dk_i$, where $(ek, dk_1, dk_2, \ldots, dk_n) \leftarrow \mathsf{Setup}(n, P_{EK,DK_1,\ldots,DK_n})$
- $ck_P \leftarrow \mathsf{KeyDer}(uk_i, \mathcal{P})$
  - Output $ck_P := m \leftarrow \mathsf{Dec}(dk_i, c_P)$

OUTLINE

- ☑ 準備と本発表の位置づけ
- ☑ 放送型暗号 (Broadcast Encryption: BE)
  - ☐ $(t, \leq \omega)$-secure BEと$(\leq n, \leq \omega)$-secure BE
- ☑ Key Predistribution System (KPS) との関係
- ☑ 暗号文長と秘密鍵長のトレードオフ
  - ☐ $(t, \leq \omega)$-secure BEにおける鍵長の下界と構成法
  - ☐ $(\leq n, \leq \omega)$-secure BEにおける鍵長の下界と構成法
- ☑ 放送型暗号の拡張
  - ☐ BE for Cloud Environments
  - ☐ BE with Specific Broadcast Channels
  - ☐ BE with Relaxed Security Definitions

TRADE-OFF: 暗号文長 VS. 秘密鍵長

- ☑ BEには暗号文長と秘密鍵長にトレードオフが存在する

$\left\{\begin{matrix}(t, \leq \omega) \\ (\leq n, \leq \omega)\end{matrix}\right\}$-secure BEにおいて, $\delta := \dfrac{\max_P |C_P|}{\log |\mathcal{M}|}$と定義する.

このとき, $\left\{\begin{matrix}(t, \leq \omega; \delta) \\ (\leq n, \leq \omega; \delta)\end{matrix}\right\}$-secure BEという.

- ☑ 鍵長の下界に関する研究
  - [Blundo-Cresti94], [Blundo-Mattos-Stinson96], [Kurosawa-Yoshida-Desmedt-Burmester98], [Padro-Gracia-Martin04], [**W**-Hanaoka-Shikata16]
- ☑ 構成法 (上界の導出) に関する研究
  - [Blundo et al.92], [Fiat-Naor93], [Blundo-Mattos-Stinson96], [Padro-Gracia-Martin04], [**W**-Shikata15], [**W**-Hanaoka-Shikata16]

暗号文長の下界

$\begin{Bmatrix} (t, \leq \omega) \\ (\leq n, \leq \omega) \end{Bmatrix}$-secure BEにおいて, 任意の$\begin{Bmatrix} \mathcal{P} \in \mathcal{P}(t) \\ \mathcal{P} \subset \mathcal{R} \end{Bmatrix}$に対して,

$$H(C_P) \geq H(M)$$

が成り立つ.

証明. 任意の $\begin{Bmatrix} \mathcal{P} \in \mathcal{P}(t) \\ \mathcal{P} \subset \mathcal{R} \end{Bmatrix}$, 及び$R_i \in \mathcal{P}$ に対して,

$$\begin{aligned} H(C_P) &\geq H(C_P \mid DK_i) \\ &\geq I(C_p; M \mid DK_i) \\ &= \underline{H(M \mid DK_i)} - \underline{H(M \mid C_P, DK_i)} \\ &= H(M). \end{aligned}$$

MとDK_iの独立性

Dec の正当性

TRADE-OFF IN $(t, \leq \omega)$-SECURE BE: 鍵長の下界

KPS	$\mathcal{UK} := \bigcup_{i=1}^{n} \mathcal{UK}_i$	初期秘密鍵 $\mathcal{UK}_i$	
	$H(UK) \geq \binom{t+\omega}{\omega} H(CK)$	$H(UK_i) \geq \binom{t+\omega-1}{\omega} H(CK)$	[Blundo-Cresti94]
BE			
暗号文長	暗号化鍵 $\mathcal{EK}$	復号鍵 $\mathcal{DK}_i$	
$\delta = 1$	—	$\log \lvert\mathcal{DK}_i\rvert \geq \binom{t+\omega-1}{\omega} H(M)$	[Kurosawa-Yoshida-Desmedt-Bermester98]
	$H(EK) \geq \binom{t+\omega}{\omega} H(M)$	$H(DK_i) \geq \binom{t+\omega-1}{\omega} H(M)$	[W-Hanaoka-Shikata16]
$\delta \in [1, t]$	—	When $t \geq \omega + 1$, $H(C_P) + \sum_{R_j \in P} H(DK_j) \geq (2\omega+1)H(M)$	[Blundo-Mattos-Stinson96]

TRADE-OFF IN $(t, \leq \omega)$-SECURE BE: 構成法

KPS	$\mathcal{UK} := \bigcup_{i=1}^{n} \mathcal{UK}_i$	初期秘密鍵長	暗号文長	Optimal?
[Blundo et al.92]	$\binom{t+\omega}{\omega} \log \lvert C\mathcal{K} \rvert$	$\binom{t+\omega-1}{\omega} \log \lvert C\mathcal{K} \rvert$	—	✓

BE	暗号化鍵長	復号鍵長	暗号文長	Optimal?
[Blundo et al.92] + OTP	$\binom{t+\omega}{\omega} \log \lvert \mathcal{M} \rvert$	$\binom{t+\omega-1}{\omega} \log \lvert \mathcal{M} \rvert$	$\delta = 1$	✓
[Blundo-Mattos-Stinson96]	$\frac{\binom{t+\omega}{\ell}}{\binom{t-1}{\ell-1}} \log \lvert \mathcal{M} \rvert$	$\frac{\binom{t+\omega-1}{\ell-1}}{\binom{t-1}{\ell-1}} \log \lvert \mathcal{M} \rvert$	$\delta = \frac{t}{\ell}$, $(\ell \in \{1, \dots, t\})$	—
[Padro-Gracia-Martin04] (平文分布は一様と仮定)	$\frac{\binom{t+\omega}{\lfloor t/\delta \rfloor} + \binom{t+\omega}{\lfloor t/\delta \rfloor + 1}}{\binom{t-1}{\lfloor t/\delta \rfloor - 1} + \binom{t-1}{\lfloor t/\delta \rfloor}} \log \lvert \mathcal{M} \rvert$	$\frac{\binom{t+\omega-1}{\lfloor t/\delta \rfloor - 1} + \binom{t+\omega-1}{\lfloor t/\delta \rfloor}}{\binom{t-1}{\lfloor t/\delta \rfloor - 1} + \binom{t-1}{\lfloor t/\delta \rfloor}} \log \lvert \mathcal{M} \rvert$	$\delta \in [1, t]$	—

TRADE-OFF IN $(\leq n, \leq \omega)$-SECURE BE: 鍵長の下界

KPS	$\mathcal{UK} := \bigcup_{i=1}^{n} \mathcal{UK}_i$	初期秘密鍵 $\mathcal{UK}_i$	
	$H(UK) \geq \sum_{j=0}^{\omega} \binom{n}{j} H(CK)$	$H(UK_i) \geq \sum_{j=0}^{\omega} \binom{n-1}{j} H(CK)$	[Blundo-Cresti94]

BE			
暗号文長	暗号化鍵 $\mathcal{EK}$	復号鍵 $\mathcal{DK}_i$	
$\delta = 1$	—	$\log \lvert\mathcal{DK}_i\rvert \geq \sum_{j=0}^{\omega} \binom{n-1}{j} H(M)$	[Kurosawa-Yoshida-Desmedt-Bermester98]
	$H(EK) \geq \sum_{j=0}^{\omega} \binom{n}{j} H(M)$	$H(DK_i) \geq \sum_{j=0}^{\omega} \binom{n-1}{j} H(M)$	[W-Hanaoka-Shikata16]
$\delta \in [1, t]$	—	—	—

$(\leq n, \leq \omega)$-SECURE BE: 鍵長の下界 [W-Hanaoka-Shikata16]

$\delta = 1$

$(\leq n, \leq \omega)$-secure BEにおいて,
任意の$\mathcal{P} \subset \mathcal{R}$に対して$H(C_P) = H(M)$であるとき, 次が成り立つ:

$$\text{(i) } H(EK) \geq \sum_{j=0}^{\omega} \binom{n}{j} H(M),$$

$$\text{(ii) } H(DK_i) \geq \sum_{j=0}^{\omega} \binom{n-1}{j} H(M) \text{ for any } i \in \{1, \dots, n\}.$$

$\mathcal{W}(\omega) \coloneqq \{\mathcal{W}_1, \dots, \mathcal{W}_t\}$ に対して, $\mathcal{P}_i \coloneqq \mathcal{R} \setminus \mathcal{W}_i$ とする $(|\mathcal{W}_1| \leq \cdots \leq |\mathcal{W}_t|)$

$$\begin{aligned} H(EK) &= H(EK \mid M) \geq I(EK; C_{P_1}, \dots, C_{P_t} \mid M) \\ &= H(C_{P_1}, \dots, C_{P_t} \mid M) - H(C_{P_1}, \dots, C_{P_t} \mid M, EK) \\ &= \textstyle\sum_{i=1}^{t} H(C_{P_i} \mid M, C_{P_1}, \dots, C_{P_t}) \\ &\geq \textstyle\sum_{i=1}^{t} H(C_{P_i} \mid M, C_{P_1}, \dots, C_{P_t}, DK_{W_i}) \geq \sum_{j=0}^{\omega} \binom{n}{j} H(M) \end{aligned}$$

Encの正当性

$H(C_P) = H(M)$の仮定の下で成り立つ

TRADE-OFF IN $(\leq n, \leq \omega)$-SECURE BE: 構成法

KPS	$\mathcal{UK} := \bigcup_{i=1}^{n} \mathcal{UK}_i$	初期秘密鍵長	暗号文長	Optimal?
[Fiat-Naor93] – OTP	$\sum_{j=0}^{\omega} \binom{n}{j} \log \lvert C\mathcal{K} \rvert$	$\sum_{j=0}^{\omega} \binom{n-1}{j} \log \lvert C\mathcal{K} \rvert$	—	✓

BE	暗号化鍵長	復号鍵長	暗号文長	Optimal?
[Fiat-Naor93]	$\sum_{j=0}^{\omega} \binom{n}{j} \log \lvert \mathcal{M} \rvert$	$\sum_{j=0}^{\omega} \binom{n-1}{j} \log \lvert \mathcal{M} \rvert$	$\delta = 1$	✓
[W-Shikata15]	$\left(\delta_1 \sum_{j=0}^{\omega_1} \binom{\lfloor n/\delta \rfloor + 1}{j} + \delta_2 \sum_{j=0}^{\omega_2} \binom{\lfloor n/\delta \rfloor}{j} \right) \log \lvert M \rvert$	$\sum_{j=0}^{\omega_1} \binom{\lfloor n/\delta \rfloor}{j} \log \lvert M \rvert$ or $\sum_{j=0}^{\omega_2} \binom{\lfloor n/\delta \rfloor - 1}{j} \log \lvert M \rvert$	$\delta \in \{1, \ldots, n\}$	—
—	—	—	$\delta \in [1, n]$	—

$\delta_1 := n \bmod \delta, \quad \delta_2 := \delta - \delta_1, \quad \omega_1 := \min\{n/\delta, \omega\}, \quad \omega_2 := \min\{n/\delta - 1, \omega\}$

FIAT-NAOR CONSTRUCTION [Fiat-Naor93]

$$\mathcal{W}(\omega) \coloneqq \{\mathcal{W} \subset \mathcal{R} \mid |\mathcal{W}| \leq \omega\}$$
$$\mathcal{W}^{(i)}(\omega) \coloneqq \{\mathcal{W} \subset \mathcal{R} \setminus \{R_i\} \mid |\mathcal{W}| \leq \omega\}$$
$$(\ \mathcal{W}(\mathcal{P}, \omega) \coloneqq \{\mathcal{W} \subset \mathcal{R} \setminus \mathcal{P} \mid |\mathcal{W}| \leq \omega\}\ )$$
$$\widehat{\mathcal{W}}(\mathcal{P}, \omega) \coloneqq \{\mathcal{W} \subset \mathcal{R} \setminus \mathcal{P} \mid |\mathcal{W}| = \min\{\omega, n - |\mathcal{P}|\}\}$$

- ☑ $(ek, dk_1, dk_2, \ldots, dk_n) \leftarrow \mathsf{Setup}(n, P_{EK,DK_1,\ldots,DK_n})$:
  - ☐ Choose $r_W \leftarrow \mathbb{F}_q$ for every $\mathcal{W} \in \mathcal{W}(\omega)$.
  - ☐ Set $ek \coloneqq \{r_W \mid \mathcal{W} \in \mathcal{W}(\omega)\}$ and $dk_i \coloneqq \{r_W \mid \mathcal{W} \in \mathcal{W}^{(i)}(\omega)\}$.
- ☑ $c_P \leftarrow \mathsf{Enc}(ek, m, P)$:
  - ☐ Output $c_P \coloneqq m + \sum_{W \in \widehat{\mathcal{W}}(P,\omega)} r_W$.
- ☑ $m \leftarrow \mathsf{Dec}(dk_i, c_P)$:
  - ☐ Output $m = c_P - \sum_{W \in \widehat{\mathcal{W}}(P,\omega)} r_W$ if $R_i \in \mathcal{P}$. Otherwise, output $\perp$.

$(\leq n, \leq \omega; \delta)$-SECURE BE: 構成法の直感 [W-Shikata15]

- Idea: 平文mの暗号文をδ個用意する

$\mathcal{R}$

$|\mathcal{R}| = n$

δ個に分割

$\mathrm{P}_i := \mathcal{P} \cap \mathcal{R}_i$ 向けの共有鍵 ck_{P_i} を作り $c_{P_i} := m \oplus ck_{P_i}$ を計算

$\mathcal{R}_1$	$\mathcal{R}_2$	.....	$\mathcal{R}_\delta$
$\lvert\mathcal{R}_1\rvert = \ell_1$	$\lvert\mathcal{R}_2\rvert = \ell_2$		$\lvert\mathcal{R}_\delta\rvert = \ell_\delta$
$(\leq \ell_1, \leq \omega_1)$-**KPS Φ_1**	$(\leq \ell_2, \leq \omega_2)$-**KPS Φ_2**	.....	$(\leq \ell_\delta, \leq \omega_\delta)$-**KPS Φ_δ**
$\omega_1 := \min\{\omega, \ell_1 - 1\}$	$\omega_2 := \min\{\omega, \ell_2 - 1\}$	.....	$\omega_\delta := \min\{\omega, \ell_\delta - 1\}$

最適な $L := (\ell_1, \ell_2, \ldots, \ell_\delta)$?

$\mathcal{R}_1$
$|\mathcal{R}_1| = \ell_1$

$(\leq \ell_1, \leq \omega_1)$-**KPS Φ_1**
$\omega_1 := \min\{\omega, \ell_1 - 1\}$

$\mathcal{R}_2$
$|\mathcal{R}_2| = \ell_2$

$(\leq \ell_2, \leq \omega_2)$-**KPS Φ_2**
$\omega_2 := \min\{\omega, \ell_2 - 1\}$

.....

.....

$\mathcal{R}_\delta$
$|\mathcal{R}_\delta| = \ell_\delta$

$(\leq \ell_\delta, \leq \omega_\delta)$-**KPS Φ_δ**
$\omega_\delta := \min\{\omega, \ell_\delta - 1\}$

総和がnとなるδ個の自然数の組み合わせの集合:

$$\mathcal{L}(n, \delta) := \left\{ \boldsymbol{L := (\ell_1, \ell_2, \ldots, \ell_\delta) \in N^\delta} \mid (\ell_1 \geq \cdots \geq \ell_\delta) \wedge \sum_{i=1}^{\delta} \ell_i = n \right\}$$

秘密鍵長を最小化する$L \in \mathcal{L}(n, \delta)$の条件を見つけたい

鍵長を最小化する最適な $\boldsymbol{L} \in \mathcal{L}(n, \delta)$

$(\leq \ell_i, \leq \omega_i)$-Fiat-Naor KPS [Fiat-Naor93] を適用した上記構成法による
$(\leq n, \leq \omega)$-secure BEの構成法の秘密鍵長は以下の通り:

$$\textbf{(i)}\ \log|\mathcal{EK}| = \sum_{i=1}^{\delta}\sum_{j=0}^{\omega_i}\binom{\ell_i}{j}\log|\mathcal{M}|,$$

$$\textbf{(ii)}\ \sum_{i=1}^{n}\log|\mathcal{DK}_i| = \sum_{i=1}^{\delta}\left(\ell_i\sum_{j=0}^{\omega_i}\binom{\ell_i-1}{j}\right)\log|\mathcal{M}|.$$

この時, 暗号化鍵長は $\boldsymbol{L} \in \mathcal{L}(n, \delta)$ が以下の条件を満たすとき最小化される :

$$\begin{cases} \forall \boldsymbol{L} & \text{if } \boldsymbol{\omega = 0}, \\ \boldsymbol{L = (n-(\delta-1), 1, \ldots, 1)} & \text{if } \boldsymbol{\omega = 1}, \\ \boldsymbol{\ell_1 - \ell_\delta = 0} & \text{if } \boldsymbol{\omega \geq 2 \wedge n/\delta \in \mathbf{N}}, \\ \boldsymbol{\ell_1 - \ell_\delta = 1} & \textbf{otherwise.} \end{cases}$$

復号鍵長 (の総和) は $\boldsymbol{L} \in \mathcal{L}(n, \delta)$が以下の条件を満たすとき最小化される :

$$\begin{cases} \forall \boldsymbol{L} & \text{if } \boldsymbol{\omega = 0}, \\ \boldsymbol{\ell_1 - \ell_\delta = 0} & \text{if } \boldsymbol{\omega \geq 1 \wedge n/\delta \in \mathbf{N}}, \\ \boldsymbol{\ell_1 - \ell_\delta = 1} & \text{otherwise.} \end{cases}$$

証明のアイディア

$$\sum_{i=1}^{\delta}\sum_{j=0}^{\omega_i}\binom{\ell_i}{j} = \underbrace{\begin{matrix}\overbrace{\binom{\ell_1}{0}}^{\delta\text{ terms}} & + & \overbrace{\binom{\ell_1}{1}}^{k_1(=\delta)\text{ terms}} & + \cdots + & \overbrace{\binom{\ell_1}{\omega-1}}^{k_{\omega-1}\text{ terms}} & + & \overbrace{\binom{\ell_1}{\omega\,(=\omega_1)}}^{k_\omega\text{ terms}} \\ + \binom{\ell_2}{0} & + & \binom{\ell_2}{1} & + \cdots + & \binom{\ell_2}{\omega-1} & + & \binom{\ell_2}{\omega(=\omega_2)} \\ + \binom{\ell_3}{0} & + & \binom{\ell_3}{1} & + \cdots + & \binom{\ell_3}{\omega-1(=\omega_3)} & & \\ + \cdots\cdots & & \cdots\cdots & & & & \\ + \binom{\ell_\delta}{0} & + & \binom{\ell_\delta}{1(=\omega_\delta)} & & & & \end{matrix}}_{\delta} \Bigg\} k_\omega$$

$$= \sum_{j=1}^{\delta}\binom{\ell_j}{0} + \sum_{j=1}^{k_1}\binom{\ell_j}{1} + \cdots + \sum_{j=1}^{k_{\omega-1}}\binom{\ell_j}{\omega-1} + \sum_{j=1}^{k_\omega}\binom{\ell_j}{\omega}$$

証明のアイディア

$$\delta\sum_{j=0}^{\widetilde{\omega}}\binom{\left\lfloor\frac{n}{\delta}\right\rfloor}{j}=\delta\binom{\left\lfloor\frac{n}{\delta}\right\rfloor}{0}+\delta\binom{\left\lfloor\frac{n}{\delta}\right\rfloor}{1}+\cdots+\delta\binom{\left\lfloor\frac{n}{\delta}\right\rfloor}{\widetilde{\omega}-1}+\delta\binom{\left\lfloor\frac{n}{\delta}\right\rfloor}{\widetilde{\omega}}$$

$$\sum_{\boldsymbol{i=1}}^{\boldsymbol{\delta}}\sum_{\boldsymbol{j=0}}^{\boldsymbol{\omega_i}}\binom{\ell_{\boldsymbol{i}}}{\boldsymbol{j}}=\sum_{\boldsymbol{j=1}}^{\delta}\binom{\ell_j}{0}+\sum_{\boldsymbol{j=1}}^{k_1}\binom{\ell_j}{1}+\cdots+\sum_{\boldsymbol{j=1}}^{k_{\omega-1}}\binom{\ell_j}{\omega-1}+\sum_{\boldsymbol{j=1}}^{k_\omega}\binom{\ell_j}{\omega}$$

任意の $a, j \in \mathbb{N}$, 任意の $r \in \{1, \ldots, a]$ に対して, $b_1 \geq \cdots \geq b_j \geq -(a-r)$ かつ $\sum_{i=1}^{j} b_i = 0$ となるような任意の $b_i \in \mathbb{Z}\ (1 \leq i \leq j)$ を選ぶ. この時,

$$j\binom{a}{r} \leq \binom{a+b_1}{r}+\binom{a+b_2}{r}+\cdots+\binom{a+b_j}{r}.$$

等号は$r = 1$の時成り立つ.

任意の $a, j \in \mathbb{N}$, 任意の $r \in \{2, \ldots, a]$ に対して, $b_1 \geq \cdots \geq b_k \geq -(a-r) \geq b_{k+1} \geq \cdots \geq b_j > -a$ かつ $\sum_{i=1}^{j} b_i = 0$ となるような任意の $b_i \in \mathbb{Z}\ (1 \leq i \leq j)$ を選ぶ. この時,

$$j\binom{a}{r} < \binom{a+b_1}{r}+\binom{a+b_2}{r}+\cdots+\binom{a+b_k}{r}.$$

補題

任意の $a, j \in \mathbb{N}$, 任意の $r \in \{1, \ldots, a]$ に対して, $b_1 \geq \cdots \geq b_j \geq -(a-r)$ かつ $\sum_{i=1}^{j} b_i = 0$ となるような任意の $b_i \in \mathbb{Z}\ (1 \leq i \leq j)$ を選ぶ. この時,

$$j\binom{a}{r} \leq \binom{a+b_1}{r} + \binom{a+b_2}{r} + \cdots + \binom{a+b_j}{r}.$$

等号は$r = 1$の時成り立つ.

証明: $b_1 \geq \cdots \geq b_k \geq 0 > b_{k+1} \geq \cdots \geq b_j$ とする.

各$b_i\ (1 \leq i \leq k)$ に対して,

$$\binom{a+b_i}{r} = \binom{a}{r} + \sum_{m=0}^{b_i-1} \binom{a+m}{r-1}.$$

各$b_i\ (k+1 \leq i \leq j)$ に対して,

$$\binom{a+b_i}{r} = \binom{a}{r} - \sum_{m=1}^{-b_i} \binom{a-m}{r-1}.$$

補題

任意の $a, j \in \mathbb{N}$, 任意の $r \in \{1, \dots, a]$ に対して, $b_1 \geq \cdots \geq b_j \geq -(a-r)$ かつ $\sum_{i=1}^{j} b_i = 0$ となるような任意の $b_i \in \mathbb{Z}\ (1 \leq i \leq j)$ を選ぶ. この時,

$$j\binom{a}{r} \leq \binom{a+b_1}{r} + \binom{a+b_2}{r} + \cdots + \binom{a+b_j}{r}.$$

等号は$r = 1$の時成り立つ.

証明:

$$\sum_{i=1}^{j}\binom{a+b_i}{r} = j\binom{a}{r} + \underbrace{\sum_{i=1}^{k}\sum_{m=0}^{b_i-1}\binom{a+m}{r-1}}_{\tau \text{ terms} \coloneqq \sum_{i=1}^{k} b_i \text{ terms}} - \underbrace{\sum_{i=k+1}^{j}\sum_{m=0}^{-b_i}\binom{a-m}{r-1}}_{= \sum_{i=k+1}^{j} b_i \text{ terms}}$$

$$= j\binom{a}{r} + \sum_{m=1}^{\tau}\underbrace{\left(\binom{a+\beta_m}{r-1} - \binom{a-\gamma_m}{r-1}\right)}_{\geq 0} \quad (\beta_m, \gamma_m \in \mathbb{N})$$

BEにおけるトレードオフ:まとめ

- ☑ $\delta = 1$の場合: 解決済み
- ☑ $\delta > 1$の場合: 今後の課題
  - □ $(\leq n, \leq \omega; \delta)$-secure BEの構成法を提案 [W-Shikata15]
  - □ 以下$(\leq 100, \leq \omega; \delta)$-secure BEの復号鍵長の表

[Fiat-Naor93]　　[W-Shikata15]　　OTP×n個

	$\delta = 1$	…	$\delta = 10$	…	$\delta = 100$
$\omega = 3$	$161{,}800 \log\lvert\mathcal{M}\rvert$	…	$130 \log\lvert\mathcal{M}\rvert$	…	$\log\lvert\mathcal{M}\rvert$
$\omega = 4$	$3{,}926{,}176 \log\lvert\mathcal{M}\rvert$	…	$256 \log\lvert\mathcal{M}\rvert$	…	$\log\lvert\mathcal{M}\rvert$
$\omega = 5$	$75{,}449{,}320 \log\lvert\mathcal{M}\rvert$	…	$382 \log\lvert\mathcal{M}\rvert$	…	$\log\lvert\mathcal{M}\rvert$

OUTLINE

- ☑ 準備と本発表の位置づけ
- ☑ 放送型暗号 (Broadcast Encryption: BE)
  - ☐ $(t, \leq \omega)$-secure BEと$(\leq n, \leq \omega)$-secure BE
- ☑ Key Predistribution System (KPS) との関係
- ☑ 暗号文長と秘密鍵長のトレードオフ
  - ☐ $(t, \leq \omega)$-secure BEにおける鍵長の下界と構成法
  - ☐ $(\leq n, \leq \omega)$-secure BEにおける鍵長の下界と構成法
- ☑ 放送型暗号の拡張
  - ☐ BE for Cloud Environments
  - ☐ BE with Specific Broadcast Channels
  - ☐ BE with Relaxed Security Definitions

暗号技術の拡張

- クラウド技術に対応
- 他暗号技術への応用
- 数学的技法の発展

機能・性質の追加

- より実用的な方式
- 数学的技法の発展

方式の再考
他方式への拡張

暗号技術

安全性定義の再考

- 効率化
- より実用的な定義
- よりシンプルな定義

暗号技術の拡張: 秘密分散法の場合

- Robust Secret Sharing
- Verifiable Secret Sharing

機能・性質の追加

- Proactive Secret Sharing
- Threshold Changeable Secret Sharing

方式の再考
他方式への拡張

秘密分散法

- Ramp Secret Sharing
- Rational Secret Sharing

安全性定義の再考

放送型暗号の拡張

Revocable-Storage BE
- クラウド環境を考慮
- ゲノム情報への安全性

動的アクセス制御
機能の追加

BE w/ Guessing Secrecy
- 効率化
- より実用的な定義

BE w/ Network Coding
- 実利用シーンを考慮
- 効率化

放送型暗号

放送通信路
の再考

非一様乱数を
扱える
安全性の定義

OUTLINE

- ☑ 準備と本発表の位置づけ
- ☑ 放送型暗号 (Broadcast Encryption: BE)
  - ☐ $(t, \leq \omega)$-secure BEと$(\leq n, \leq \omega)$-secure BE
- ☑ Key Predistribution System (KPS) との関係
- ☑ 暗号文長と秘密鍵長のトレードオフ
  - ☐ $(t, \leq \omega)$-secure BEにおける鍵長の下界と構成法
  - ☐ $(\leq n, \leq \omega)$-secure BEにおける鍵長の下界と構成法
- ☑ 放送型暗号の拡張
  - ☐ BE for Cloud Environments
  - ☐ BE with Specific Broadcast Channels
  - ☐ BE with Relaxed Security Definitions

クラウドコンピューティングの普及

<u>クラウド登場の影響: アクセス制御可能な暗号技術がより重要に</u>

➡ これまで考えられていなかった状況が有り得る

- ☑ クラウドストレージに保存された暗号文の復号権限制御 (本拡張)

  Revocable-Storage Attribute-Based Encryption [Sahai-Seyalioglu-Waters12]

  ※計算量的安全性

  Revocable-Storage BE (RS-BE) [W-Hanaoka-Shikata16]

クラウドにおける長期的安全性の必要性

- クラウド技術の発展は目覚ましい

- ☑ 様々な情報がクラウド上で使われている (期待されている)
  - ✓ “マイナンバー”, ゲノム情報などの情報も含む
  - ✓ 遺伝情報は子孫に遺伝し続けていく

➡ ゲノム情報には長期的安全性が必要不可欠!

- ☑ クラウドでの利用が期待されているゲノム技術
  - ✓ 全ゲノム配列決定

全ゲノム配列決定の抱える諸問題

ゲノム情報をどう扱うか？
誰がどこにゲノム情報を保存するのか？

- ☑ 生命倫理問題に関するアメリカ大統領諮問委員会,
  “Privacy and Progress in Whole Genome Sequencing,” 2012.
  - ➢ 全ゲノム配列決定がもたらす臨床診療の進歩と公益の実現には,
    個人のプライバシーの尊重と,その安全性の保障が不可欠

- ☑ E. Ayday et al., “Whole Genome Sequencing: Revolutionary Medicine or Privacy Nightmare?,” IEEE Computer, 2015.

1. **長期的安全性を達成するためにはどうすべきか？**
   - ✓ 計算量的に安全な暗号の鍵長を伸ばすだけでは不十分
   - ✓ 定期的に再暗号化する？ (誰が?)
2. **ゲノムストレージはどう管理する?クラウドに委託可能か？**
   - ✓ 日本における2013年の総情報漏洩被害人数は925万人
   - ✓ その原因の大部分が管理ミス等のヒューマンエラー

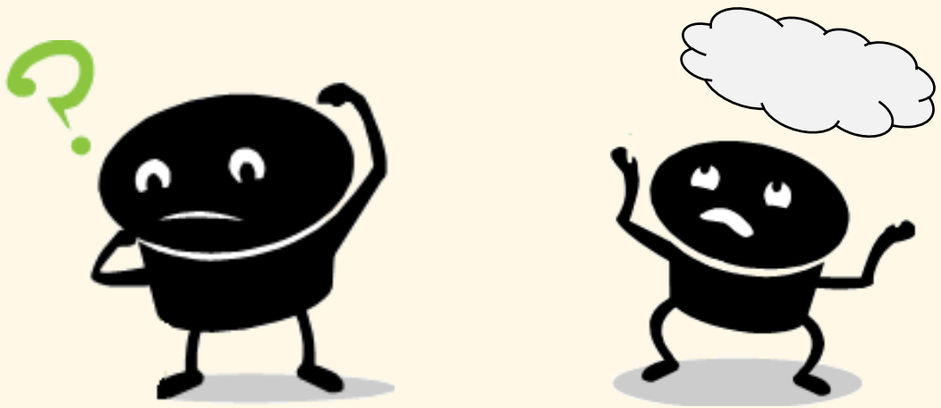
(暗号学的) 解決アプローチ

- ☑ 計算量的に安全な暗号は長期的安全性を保証できない
  - ✓ 鍵長を伸ばすだけでは不十分
  - ✓ 2,048-bit RSA暗号でも2030年以降の安全性は不透明 [NIST12]

➡ 情報理論的安全性が必要

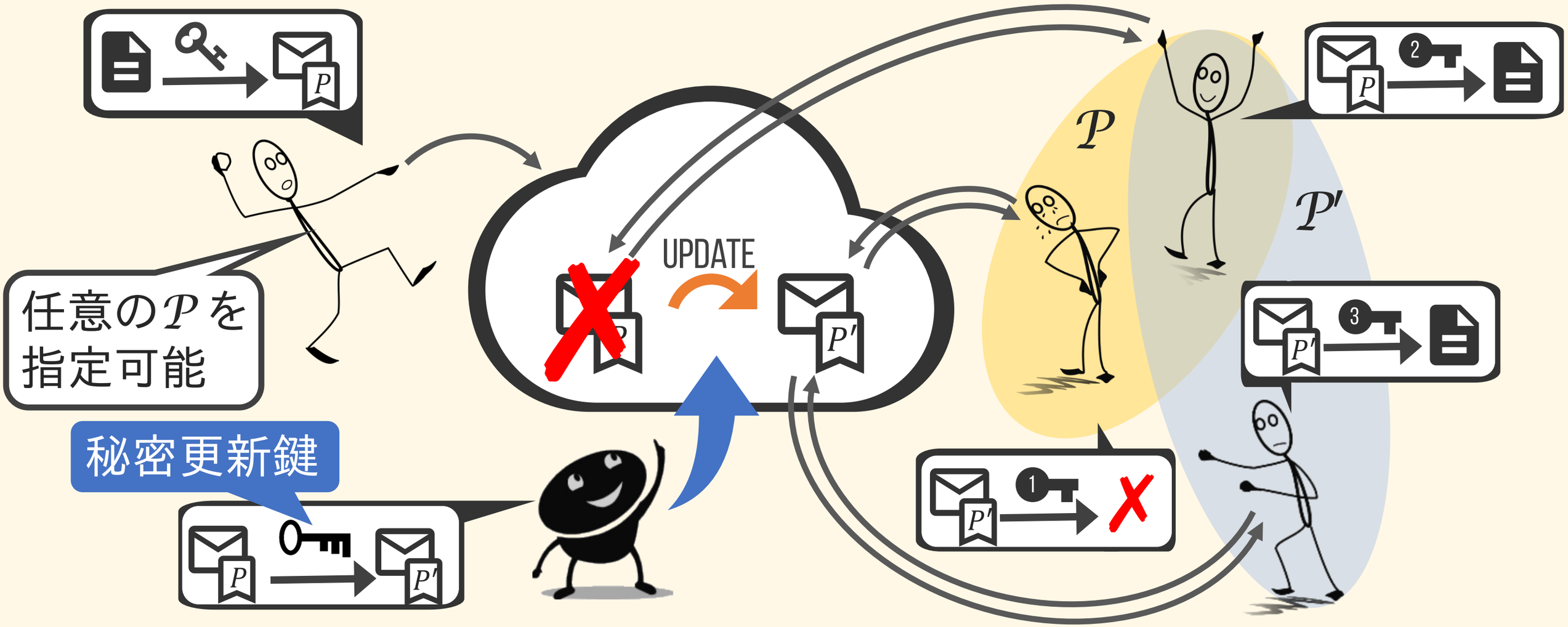
- ☑ クラウドストレージ上に暗号文が保存されるという意味
  - ✓ 誰でもアクセス可能 → アクセス制御が必要
  - ✓ アクセス権限を持つユーザは変わり得る → 動的アクセス制御が必要

➡ 動的アクセス制御を持つBEを考える



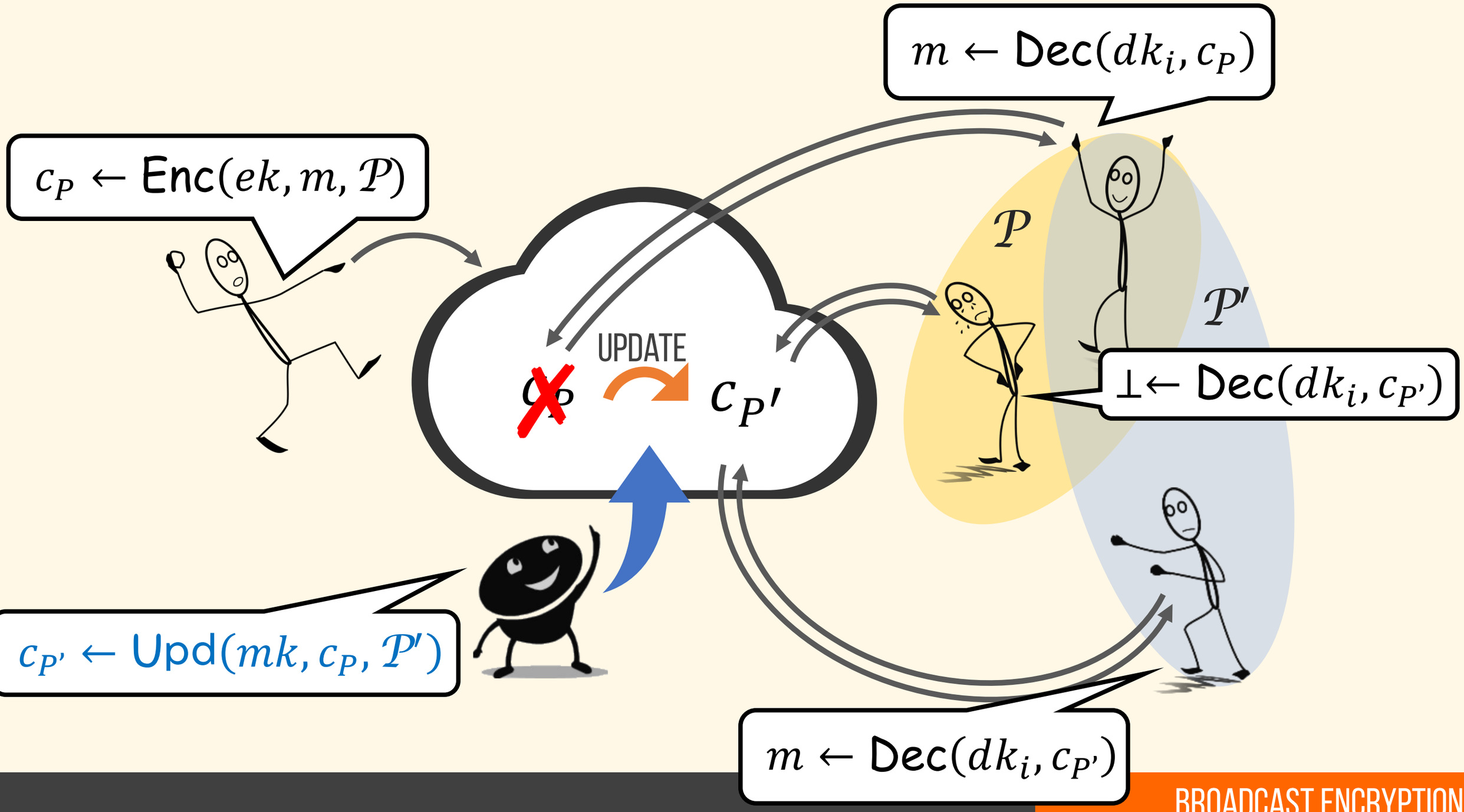
REVOCABLE-STORAGE BE (RS-BE) [W-hanaoka-Shikata16]

- ☑ 暗号文の受信者集合を$\mathcal{P}$を任意の$\mathcal{P}'$に変更可能
  - 秘密更新鍵🔑を用いて復号することなく更新（受信者追加も可能）
  - 受信者結託に対してだけでなく，更新者に対しても平文の情報が漏れない



RS-BE: MORE FORMALLY…

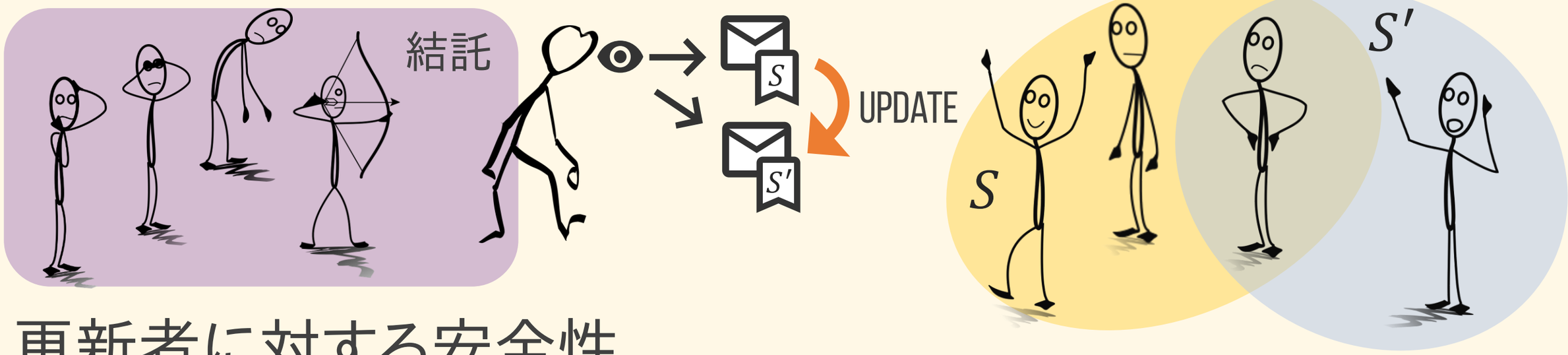
$(ek, dk_1, dk_2, \ldots, dk_n, mk) \leftarrow \mathsf{Setup}(n, P_{EK,DK_1,\ldots,DK_n,MK})$



RS-BE: 安全性要件

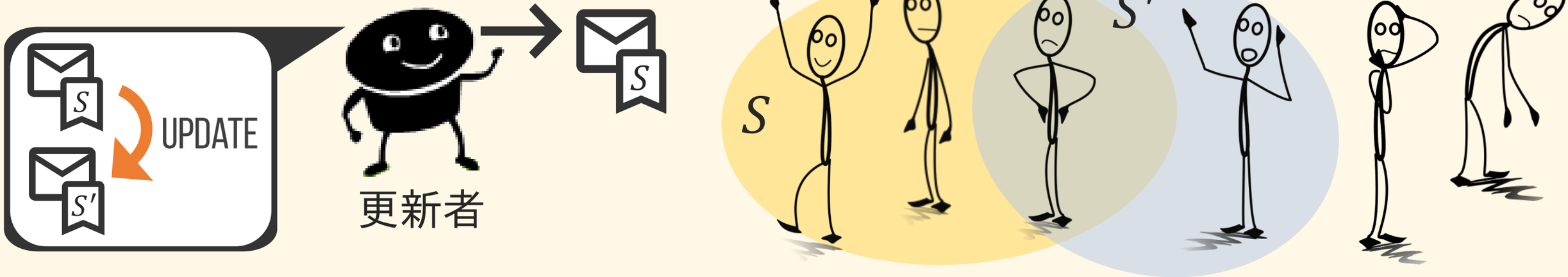
- ☑ 受信者の結託に対する安全性

  結託者以外の受信者宛の暗号文から平文の情報が漏れない



- ☑ 更新者に対する安全性

  ✓ 更新鍵を持つ更新者に対しても, 暗号文から平文の情報が漏れない



RS-BEの完全秘匿性 (Perfect Secrecy)

BEは, 次を満たすとき, $\begin{Bmatrix} (t, \leq \omega) \\ (\leq n, \leq \omega) \end{Bmatrix}$-secure RS-BEという:

(1) 任意の $\begin{Bmatrix} \mathcal{P}_1, \dots, \mathcal{P}_k \in \mathcal{P}(t) \\ \mathcal{P}_1, \dots, \mathcal{P}_k \subset \mathcal{R} \end{Bmatrix}$, 任意の $\mathcal{W} \in \mathcal{W}\left(\mathsf{U}_{i=1}^{k} \mathcal{P}_i, \omega\right)$に対して

$$H\left(M \mid C_{P_1}, \dots, C_{P_k}, DK_W\right) = H(M).$$

(2) 任意の$\begin{Bmatrix} \mathcal{P} \in \mathcal{P}(t) \\ \mathcal{P} \subset \mathcal{R} \end{Bmatrix}$に対して

$$H(\, M \mid C_P, MK\,) = H(M).$$

RS-BE: 鍵長の下界

$(\leq n, \leq \omega)$-secure RS-BEにおいて,
任意の$\mathcal{P} \subset \mathcal{R}$に対して$H(C_P) = H(M)$であるとき, 次が成り立つ:

$$\text{(i) } H(EK) \geq \sum_{j=0}^{\omega} \binom{n}{j} H(M),$$

$$\text{(ii) } H(DK_i) \geq \sum_{j=0}^{\omega} \binom{n-1}{j} H(M) \text{ for any } i \in \{1, \ldots, n\},$$

$$\text{(iii) } H(MK) \geq \left(\sum_{j=0}^{\omega} \binom{n}{j} - 1 \right) H(M).$$

RS-BE: 構成法

基本的にはFiat-Naor construction (任意の$\delta \in \{1, \ldots, n\}$に拡張可)

- ☑ $(ek, dk_1, dk_2, \ldots, dk_n) \leftarrow \mathsf{Setup}(n, P_{EK,DK_1,\ldots,DK_n})$:
  - Choose $r_W \leftarrow \mathbb{F}_q$ for every $\mathcal{W} \in \mathcal{W}(\omega)$.
  - Set $ek := \{r_W \mid \mathcal{W} \in \mathcal{W}(\omega)\}$ and $dk_i := \{r_W \mid \mathcal{W} \in \mathcal{W}^{(i)}(\omega)\}$.
  - Set $mk := \{r_W \mid \mathcal{W} \in \mathcal{W}(\omega) \setminus \{\emptyset\}\}$
- ☑ $c_P \leftarrow \mathsf{Enc}(ek, m, P)$:
  - Output $c_P := m + \sum_{W \in \widehat{\mathcal{W}}(P,\omega)} r_W + r_\emptyset$.
- ☑ $m \leftarrow \mathsf{Dec}(dk_i, c_P)$:
  - Output $m = c_P - \sum_{W \in \widehat{\mathcal{W}}(P,\omega)} r_W - r_\emptyset$ if $R_i \in \mathcal{P}$. Otherwise, output $\perp$.
- ☑ $c_{P'} \leftarrow \mathsf{Upd}(mk, c_P, P')$:
  - Output $c_{P'} = c_P - \sum_{W \in \widehat{\mathcal{W}}(P,\omega)} r_W + \sum_{W \in \widehat{\mathcal{W}}(P',\omega)} r_W$.

RS-BE: その他の結果と今後の課題

その他の結果

- ☑ 能動的な攻撃 (改ざん攻撃) に耐性のある方式の提案
  - 暗号文長の下界: $|C_P| \geq \frac{|M|-1}{|\gamma^2|} + 1$ (γ は改ざん攻撃成功確率)
  - 構成: Algebraic Modification Detection (AMD) code を利用
  - $\mathcal{M} := \mathbb{F}_q$ である $\mathbb{F}_q$ 上での方式を構成するためには，
    暗号文は $\mathbb{F}_q$ の要素が最低3つ必要

今後の課題

- 通常のBEと同じ
- 計算量的に安全な方式の提案
  - 投稿予定

OUTLINE

- ☑ 準備と本発表の位置づけ
- ☑ 放送型暗号 (Broadcast Encryption: BE)
  - ☐ $(t, \leq \omega)$-secure BEと$(\leq n, \leq \omega)$-secure BE
- ☑ Key Predistribution System (KPS) との関係
- ☑ 暗号文長と秘密鍵長のトレードオフ
  - ☐ $(t, \leq \omega)$-secure BEにおける鍵長の下界と構成法
  - ☐ $(\leq n, \leq \omega)$-secure BEにおける鍵長の下界と構成法
- ☑ 放送型暗号の拡張
  - ☐ BE for Cloud Environments
  - ☐ BE with Specific Broadcast Channels
  - ☐ BE with Relaxed Security Definitions

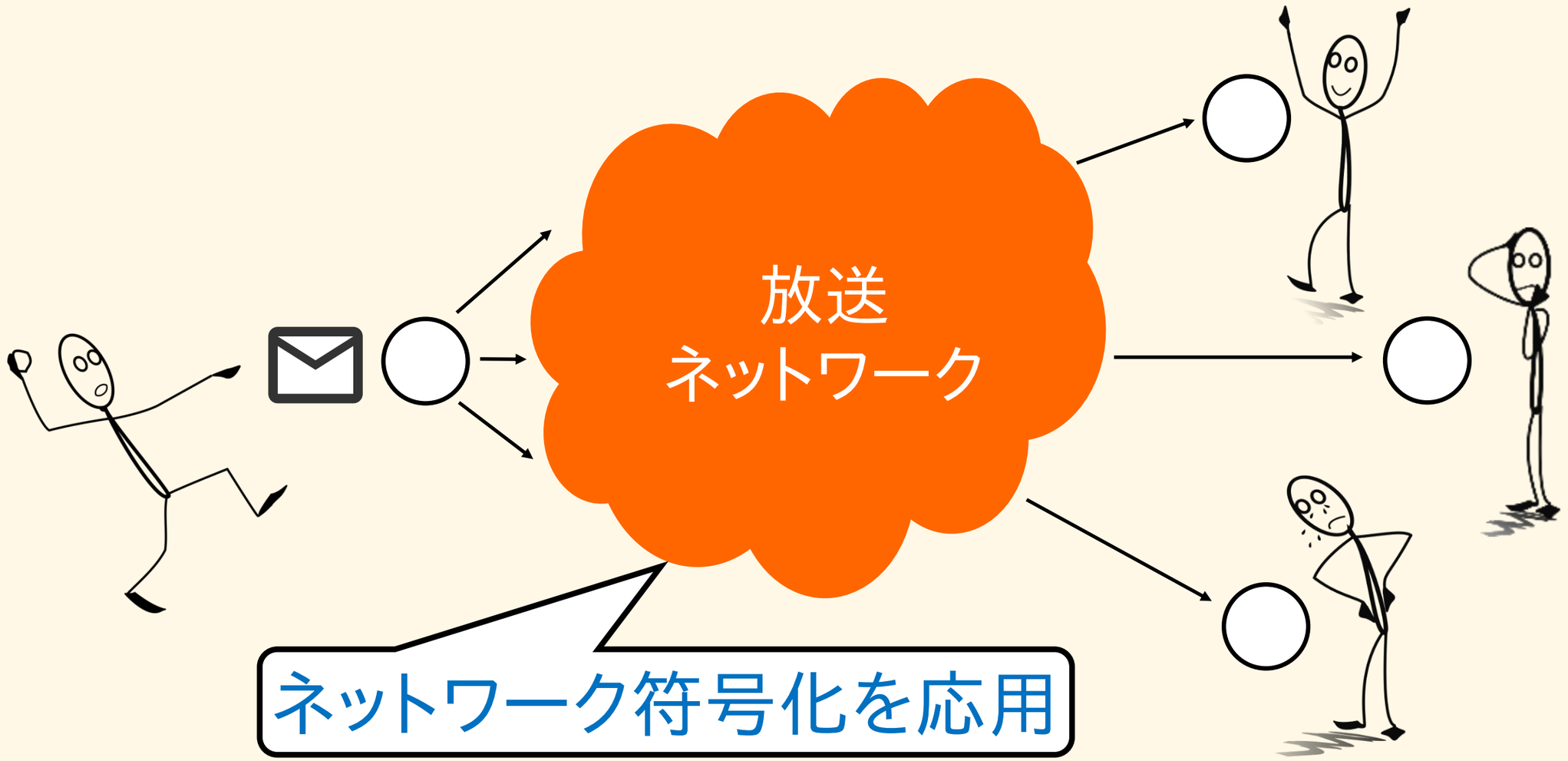
BE WITH NETWORK CODING [岩本-渡邉17]: 概要

Focus: 放送型暗号における通信ネットワークを意識

本研究: Combination Network

Goal: 必要な秘密鍵長を削減

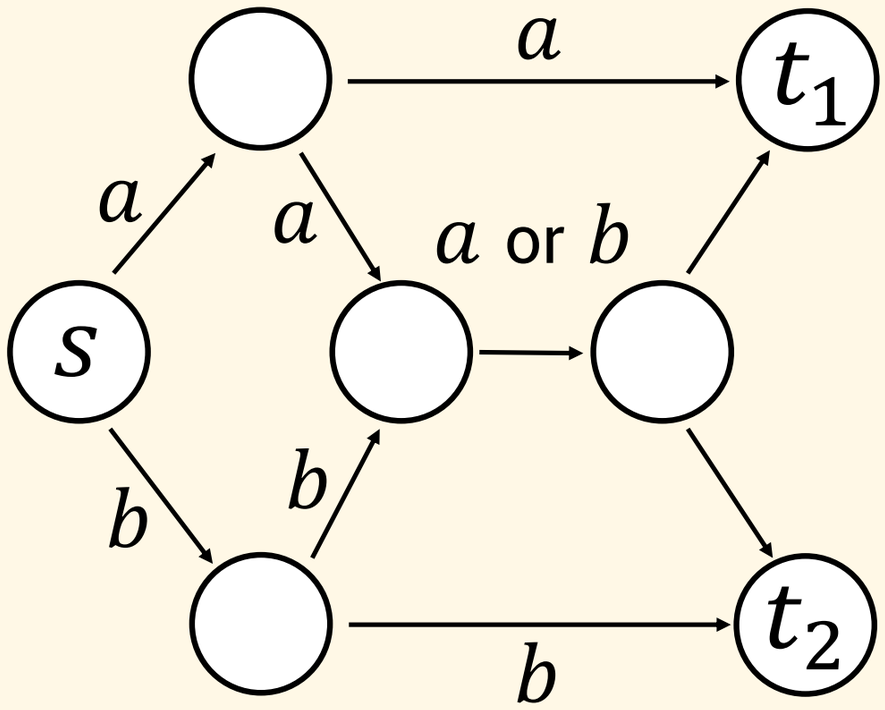
Result: 非現実的なサイズ → 現実的なサイズ



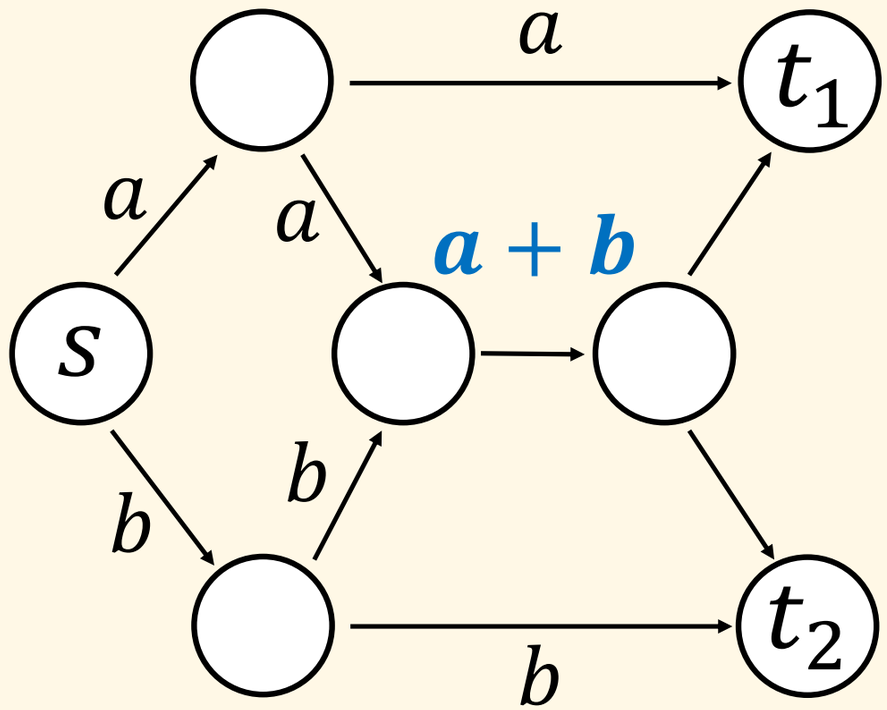
ネットワーク符号化 (NETWORK CODING: NC)

- ☑ネットワークの中間ノード上でデータを符号化・転送
  - 😀データ伝送速度の向上
    - ✓最大伝送速度 N: ソースから各 t_i に至る最大流の最小値

蓄積転送



NC

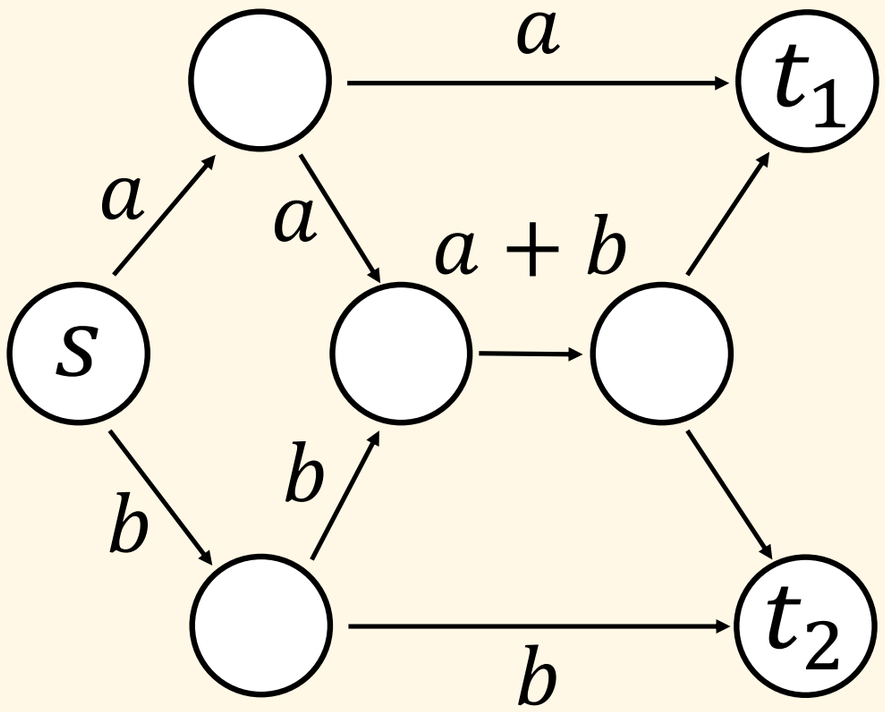


効率的なデータ伝送が可能!

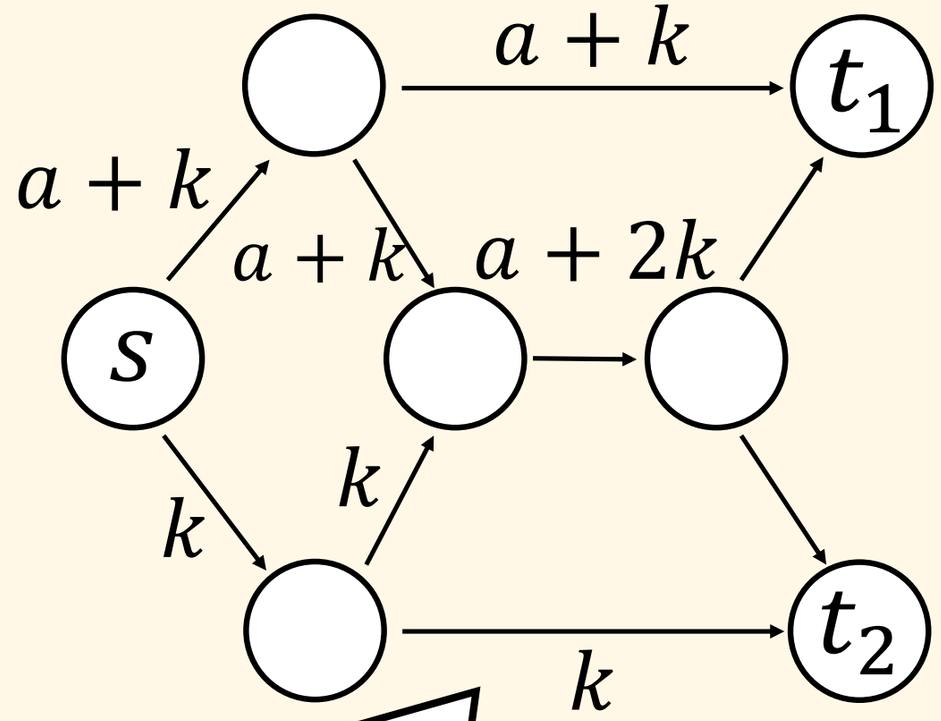
セキュアネットワーク符号化 (SECURE NC: SNC)

- ネットワーク符号化 (NC) + 秘匿性
  - 通信路を高々 h 本盗聴したとしてもシンボルの情報が漏れない
  - 送信できるシンボル数が減る

NC



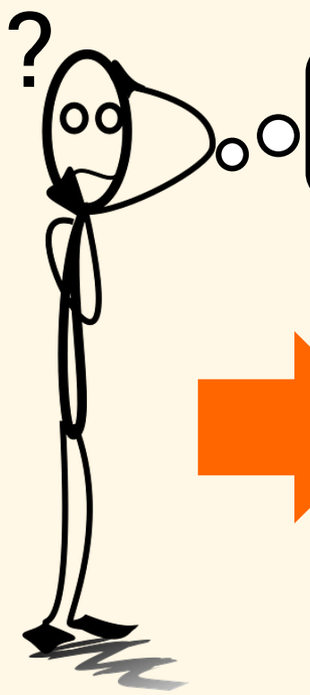
SNC



任意の通信路を1本盗聴されても
a に関する情報が漏れない

本研究の目的

- ☑ **セキュアネットワーク符号化**
  - 😀 秘密鍵が不要
  - ☹ 受信者集合を指定不可能
- ☑ **放送型暗号**
  - ☹ (非常に大きい) 秘密鍵の共有が必要
  - 😀 任意の受信者集合を指定可能



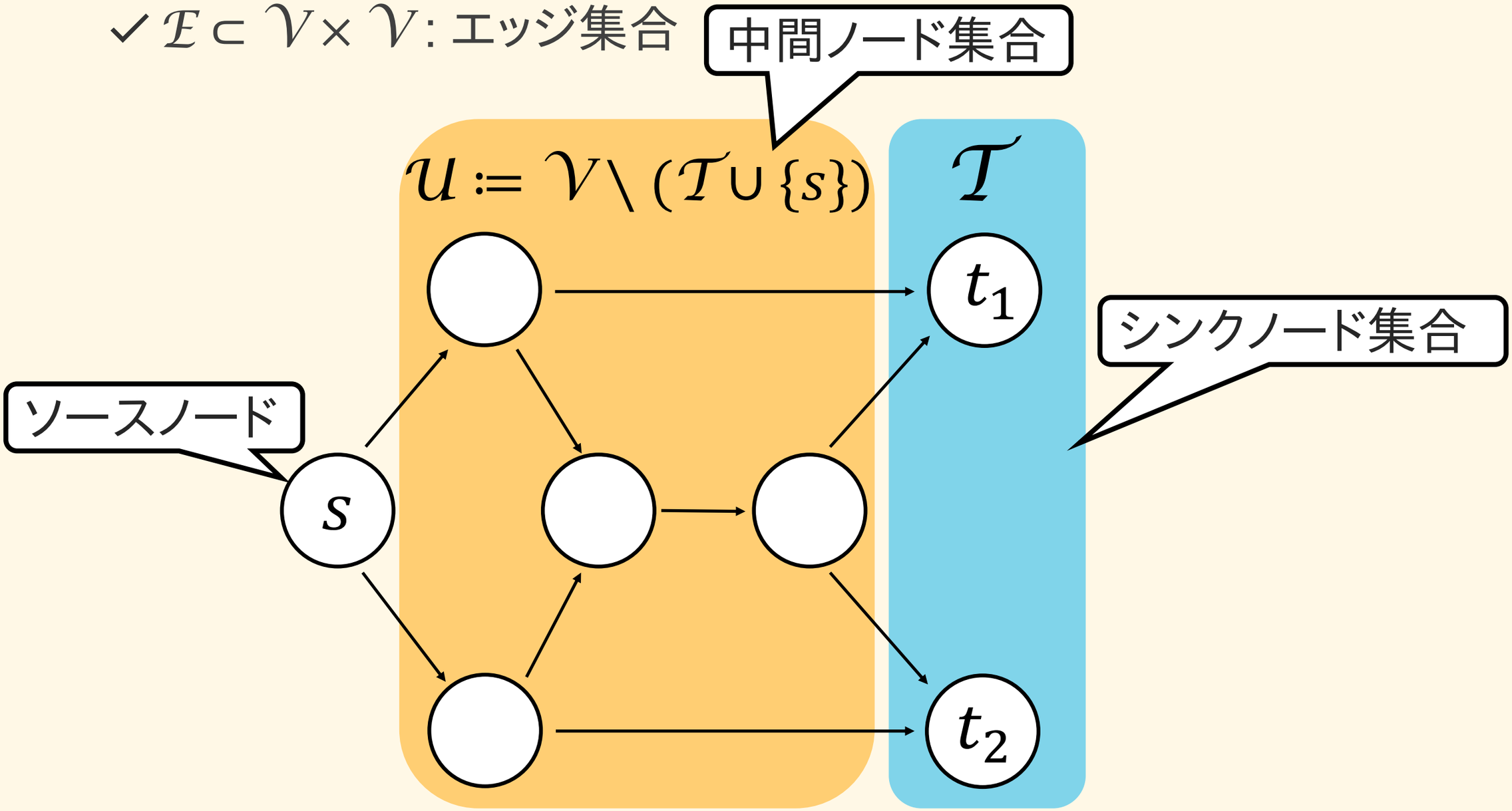
両者の良いとこ取りができないか？

Broadcast Encryption meets Network Coding!

鍵長の短い放送型暗号を実現する!

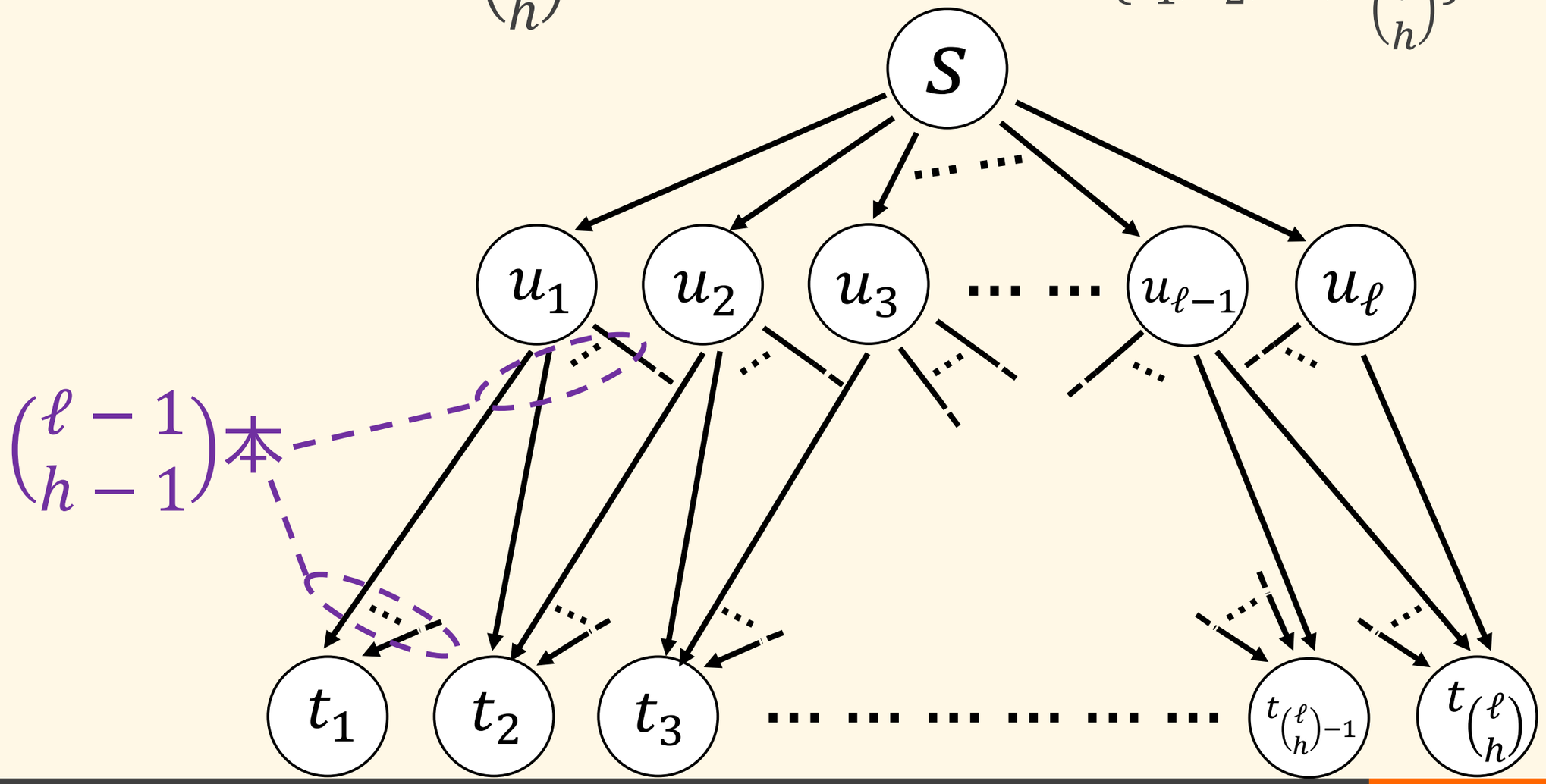
ネットワーク

- ☑ 有向非巡回グラフ$\mathcal{G} = (\mathcal{V}, \mathcal{E})$
  - ✓ $\mathcal{V}$: ノード集合
  - ✓ $\mathcal{E} \subset \mathcal{V} \times \mathcal{V}$: エッジ集合



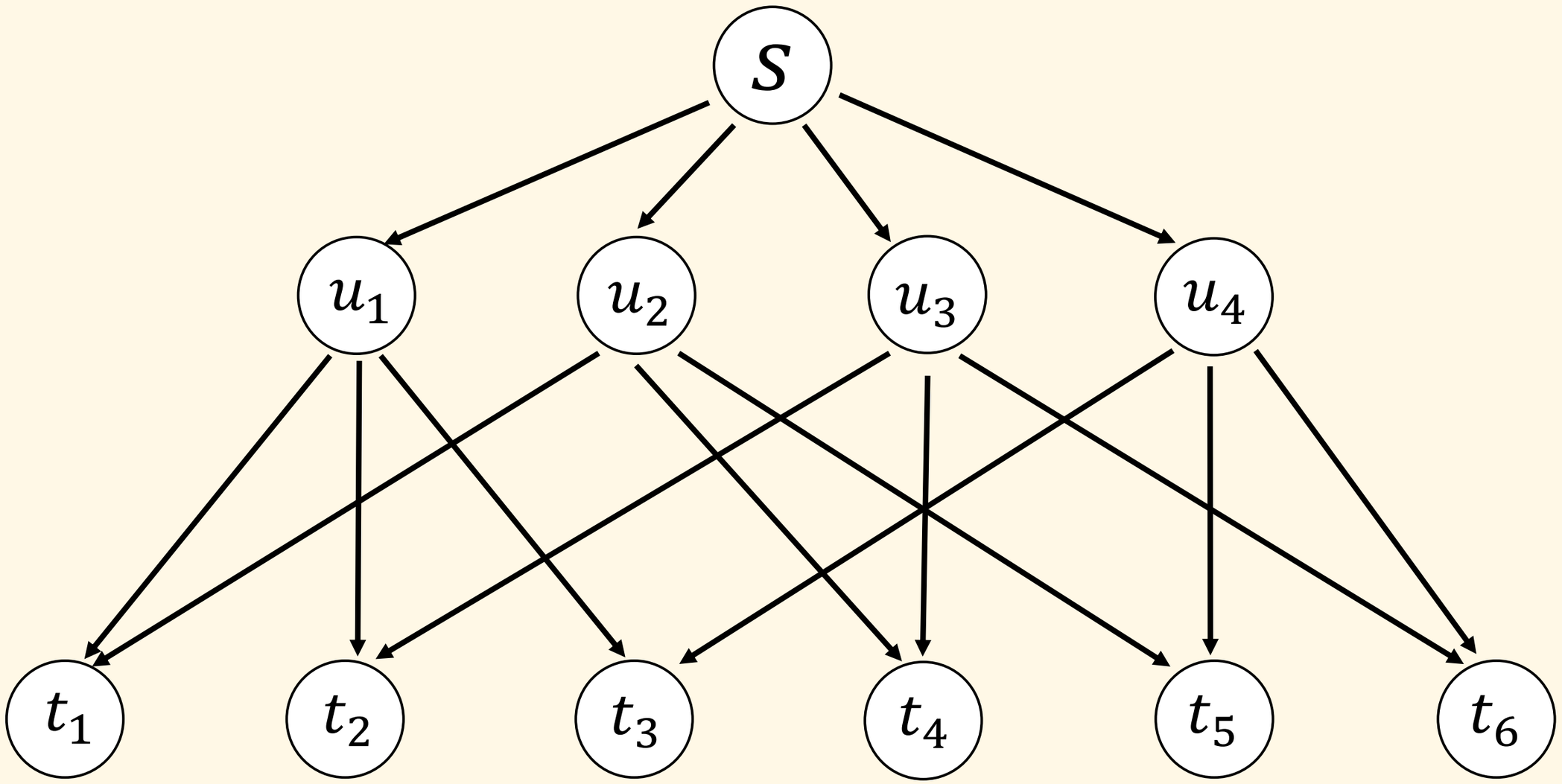
COMBINATION NETWORK

- ☑ (ℓ, h)-Combination Network $\mathcal{G}_{\ell,h} = (\mathcal{V}, \mathcal{E})$
  - ✓ 第一層: ソースノード s
  - ✓ 第二層: ℓ個の中間ノード $\mathcal{U} := \{u_1, u_2, \ldots, u_\ell\}$ から成る
  - ✓ 第三層: $\binom{\ell}{h}$個のシンクノード $\mathcal{T} := \{t_1, t_2, \ldots, t_{\binom{\ell}{h}}\}$ から成る



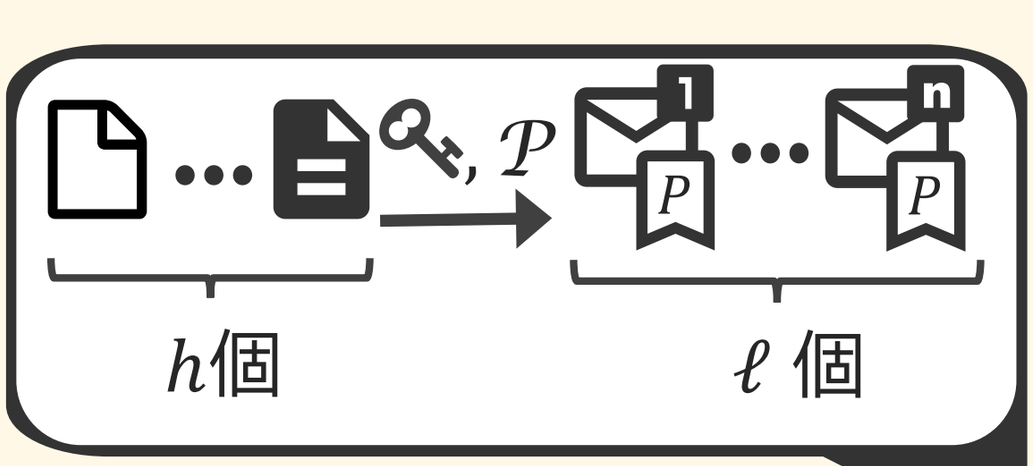
COMBINATION NETWORK: 例

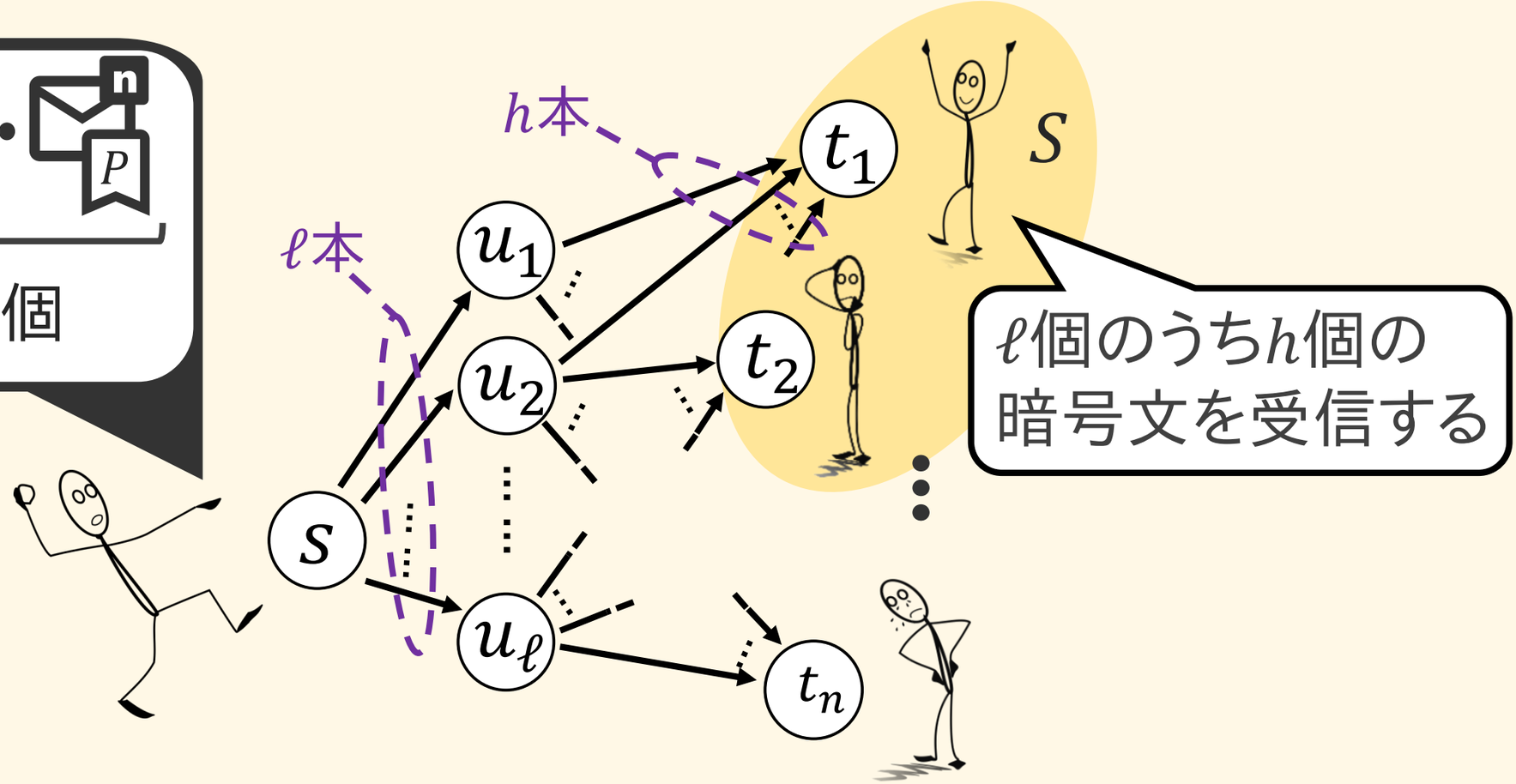
- ☑ $(4,2)$-Combination Network $\mathcal{G}_{4,2} = (\mathcal{V}, \mathcal{E})$



BE WITH COMBINATION NETWORK: モデル

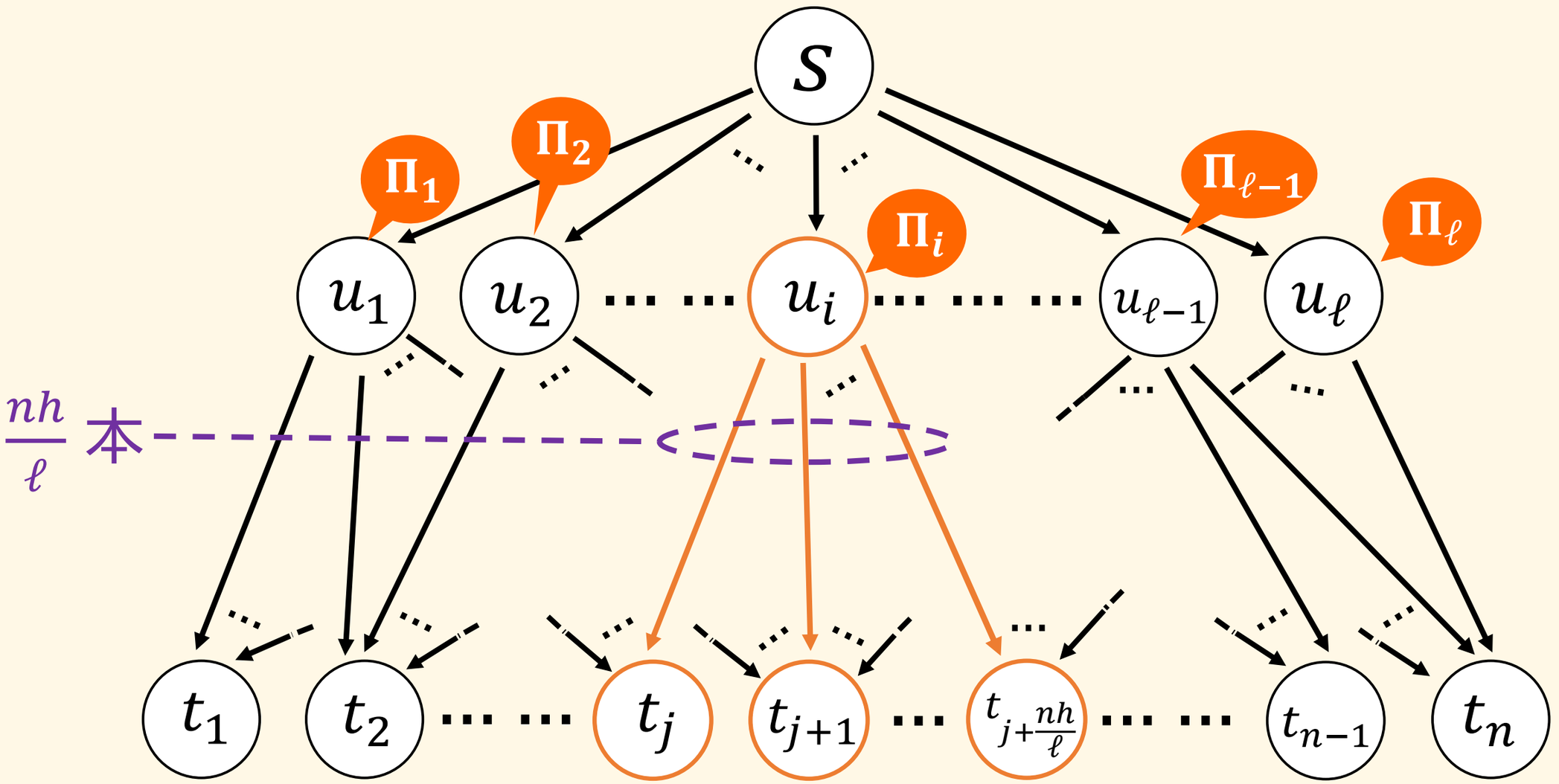
- ☑ $(\leq n, \leq \omega)$-secure BE with $\mathcal{G}_{\ell,h}$ such that $\mathrm{n} = \binom{\ell}{h}$
  - ✓ 任意の $\mathcal{P} \subset \mathcal{R}$ を指定して h 個の平文を暗号化
    - ✓ $\mathcal{G}_{\ell,h}$ の最大伝送速度 $N = h$ であるため
  - 🛡 結託集合 $\mathcal{W} \in \mathcal{W}(\mathcal{P}, \omega)$ に対する安全性
    - ✓ 暗号文を全て手に入れても平文に関する情報が漏れない





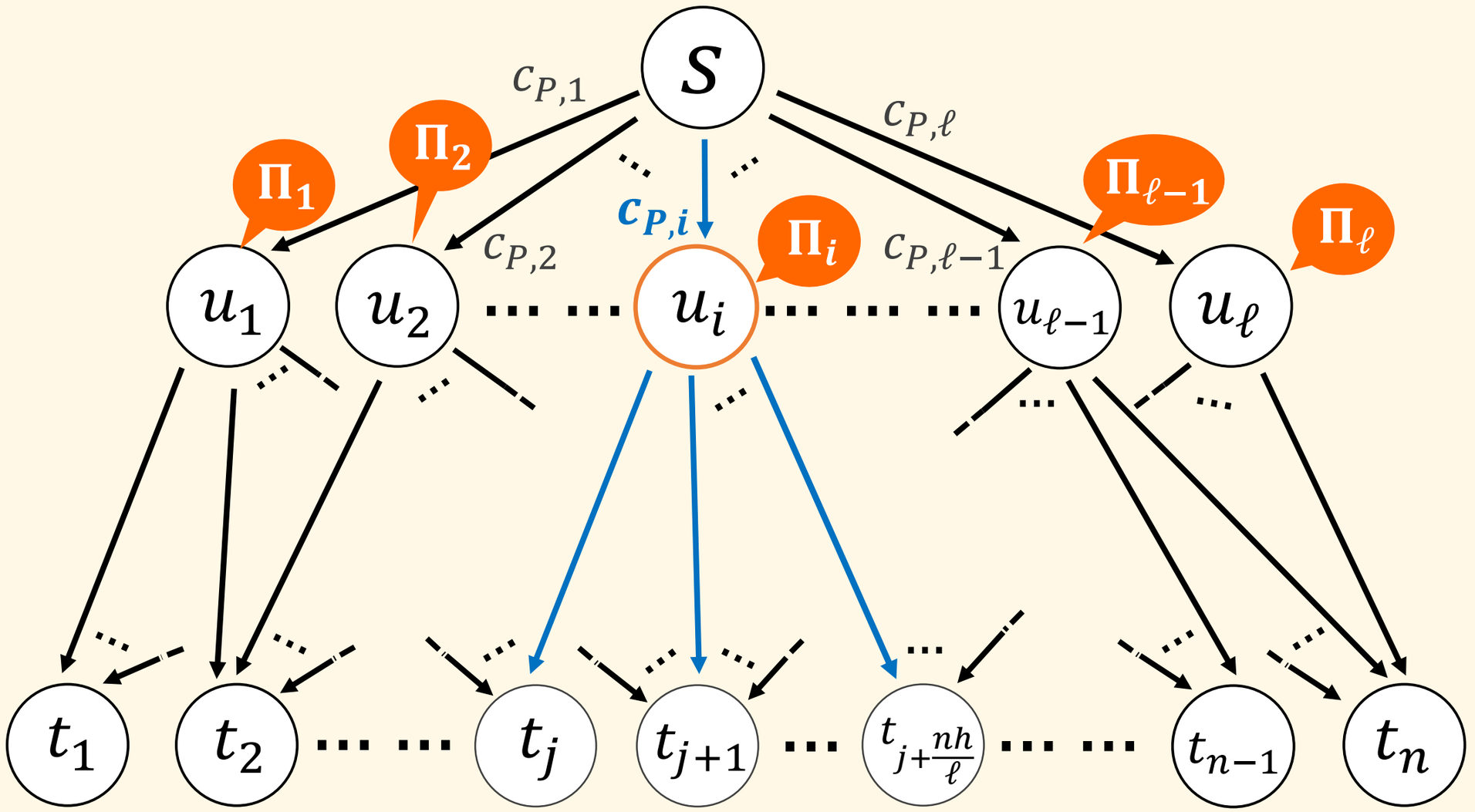
構成のアイディア

- ☑ 各中間ノードに$\left(\leq \frac{nh}{\ell}, \leq \tilde{\omega}\right)$-one-time secure BEを適用
  - ✓ $\tilde{\omega} := \min\left\{\frac{nh}{\ell} - 1, \omega\right\}$
  - ✓ 各ユーザは h 種類の復号鍵をもつ



構成のアイディア

- ☑ $\mathcal{P} \subset \mathcal{R}$ に h 個のシンボル全てが届くように符号化する
  - ✓ Linear Information Flow (LIF) [Jaggi et al.05] アルゴリズムを用いる
- ☑ 各符号語 cw_i をそれぞれ Π_i で暗号化し，暗号文 $c_{P,i}$ を u_i に送る



鍵長の比較

- ☑ Fiat-Naor Construction [FN93] × h回 vs.提案構成法
  - ✓ 大幅な効率化に成功 (ただし[**W**-Shikata15]と同程度)

$(\leq n, \leq \omega)$-secure BE × h 回

$$\log|\mathcal{EK}| = h\sum_{j=0}^{\omega}\binom{n}{j}\log|\mathcal{M}|$$

$$\log|\mathcal{DK}_i| = h\sum_{j=0}^{\omega}\binom{n-1}{j}\log|\mathcal{M}|$$

$(\leq n, \leq \omega)$-secure BE with $\mathcal{G}_{\ell,h}$

$$\log|\mathcal{EK}| = \ell\sum_{j=0}^{\tilde{\omega}}\binom{\frac{nh}{\ell}}{j}\log|\mathcal{M}|$$

$$\log|\mathcal{DK}_i| = h\sum_{j=0}^{\tilde{\omega}}\binom{\frac{nh}{\ell}-1}{j}\log|\mathcal{M}|$$

BE WITH NETWORK CODING:今後の課題

- 安全性の拡張
  - セキュアネットワーク符号化ライクな安全性にできるか
  - 現在の定義は最も強いもの (=暗号文が全て手に入る状況)
- 他の特定のネットワークではどうなるか
  - Combination Networkでは [W-Shikata15] と同程度の効率化
- 任意のネットワークに関して構成できるか
- .....

OUTLINE

- ☑ 準備と本発表の位置づけ
- ☑ 放送型暗号 (Broadcast Encryption: BE)
  - ☐ $(t, \leq \omega)$-secure BEと$(\leq n, \leq \omega)$-secure BE
- ☑ Key Predistribution System (KPS) との関係
- ☑ 暗号文長と秘密鍵長のトレードオフ
  - ☐ $(t, \leq \omega)$-secure BEにおける鍵長の下界と構成法
  - ☐ $(\leq n, \leq \omega)$-secure BEにおける鍵長の下界と構成法
- ☑ 放送型暗号の拡張
  - ☐ BE for Cloud Environments
  - ☐ BE with Specific Broadcast Channels
  - ☐ BE with Relaxed Security Definitions

非一様乱数を用いた共通鍵暗号(SKE)

- ☑ 完全秘匿性を有する最適なSKEは必ず鍵が一様ランダムに選ばれることを要求する

$|\mathcal{M}| = |C| = |\mathcal{K}|$であるSKEは
以下の条件を満たすときかつその時に限り完全秘匿性を満たす:

1. 鍵の確率分布 P_K が一様である
2. 各$m \in \mathcal{M}$, 各$c \in C$に対して, $c \leftarrow \mathsf{E}(k, m)$となる単一の$k \in \mathcal{K}$が存在する

非一様な鍵を用いた情報理論的に安全な方式は作れない？

GUESSING SECRECY [Alimomeni-Safavi-Naini12, Iwamoto-Shikata15]

Goal: minエントロピーでもって安全性を保証する

SKEは次を満たすときAverage Guessing Secrecy (A-GS) を満たすという:

$$\sum_{c\in C} P_C(c) \max_{m\in M} P_{M|C}(m \mid c) = \max_{m\in M} P_M(m).$$

SKEは次を満たすときOptimal Guessing Secrecy (O-GS) を満たすという:

$$\max_{c\in C} \max_{m\in M} P_{M|C}(m \mid c) = \max_{m\in M} P_M(m).$$

鍵長の下界 [Iwamoto-Shikata15]

$$|\mathcal{K}| \geq |C| \geq |\mathcal{M}|$$

OTP over $\{0,1\}$ [Iwamoto-Shikata15]

OTP meets A-GS iff $\max_{k\in K} P_K(k) \leq \max_{m\in M} P_M(m)$

➡ 非一様乱数 (鍵) を用いたSKEを実現可能

BE WITH GUESSING SECRECY [W17]

Goal: Guessing Secrecyの枠組みをBEに拡張する

BEは次を満たすときAverage Guessing Secrecy (A-GS) を満たすという:

$$\sum_{dk_W \in DK_W} P_{DK_W}(dk_W) \sum_{c \in C} P_C(c) \max_{m \in M} P_{M|C\ DK_W}(m \mid c, dk_W) = \max_{m \in M} P_M(m).$$

SKEは次を満たすときOptimal Guessing Secrecy (O-GS) を満たすという:

$$\max_{dk_W \in DK_W} \max_{c \in C} \max_{m \in M} P_{M|C\ DK_W}(m \mid c, dk_W) = \max_{m \in M} P_M(m).$$

鍵長の下界

$$|\mathcal{EK}| \geq \sum_{j=0}^{\omega} \binom{n}{j} |\mathcal{M}|,$$

$$|\mathcal{DK}_i| \geq \sum_{j=0}^{\omega} \binom{n-1}{j} |\mathcal{M}|.$$

Fiat-Naor Construction over $\{0,1\}$

It meets A-GS iff $\max_{r \in \{0,1\}} P_R(r) \leq \max_{m \in M} P_M(m)$

全体のまとめ

- ☑ 情報理論的に安全な放送型暗号
  - $(t, \leq \omega)$-secure BE と $(\leq n, \leq \omega)$-secure BE
  - 暗号文長と秘密鍵長のトレードオフ
  - 各種拡張方式
- 🔍 未解決問題は残っている
  - トレードオフ周り