第6回誤り訂正符号のワークショップ
セントコア山口（山口市湯田温泉）

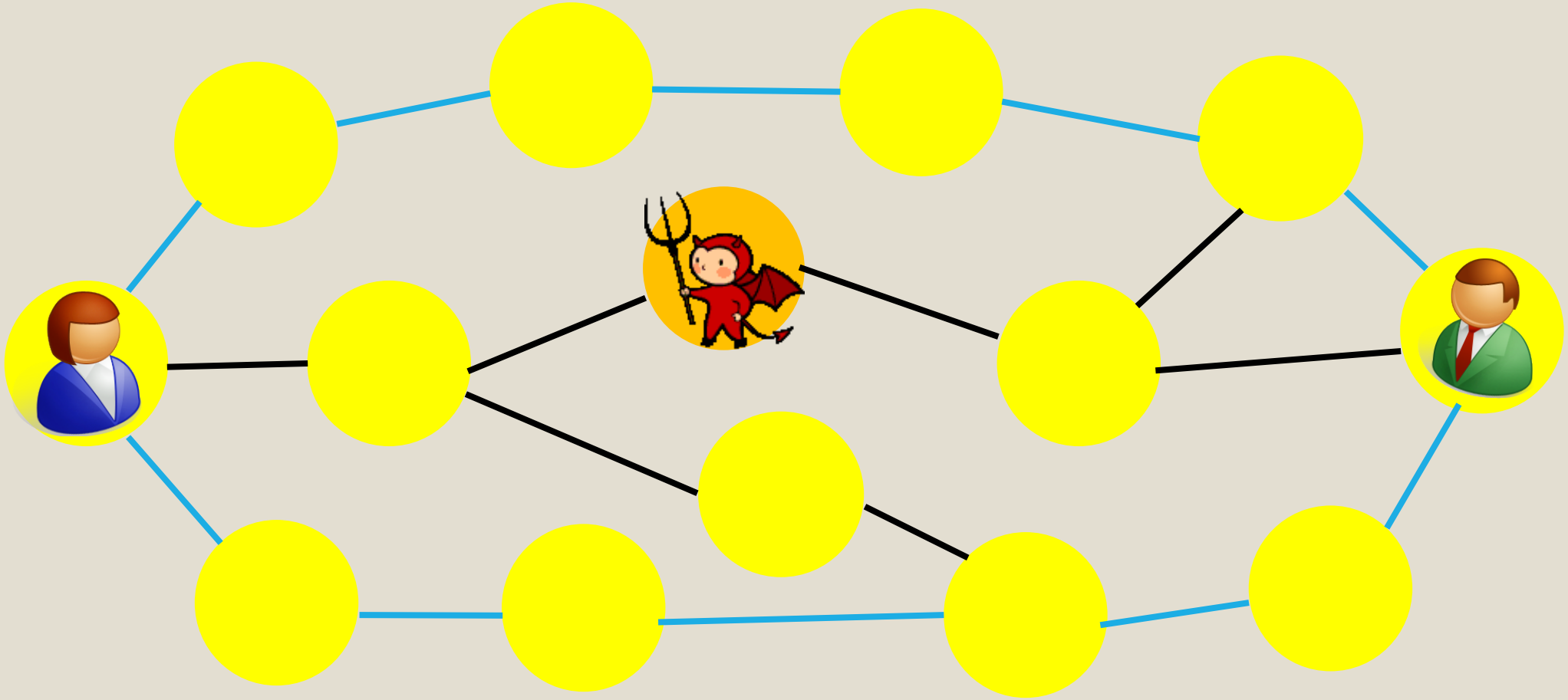
SECURE MESSAGE TRANSMISSION

可能性と限界

WASEDA University

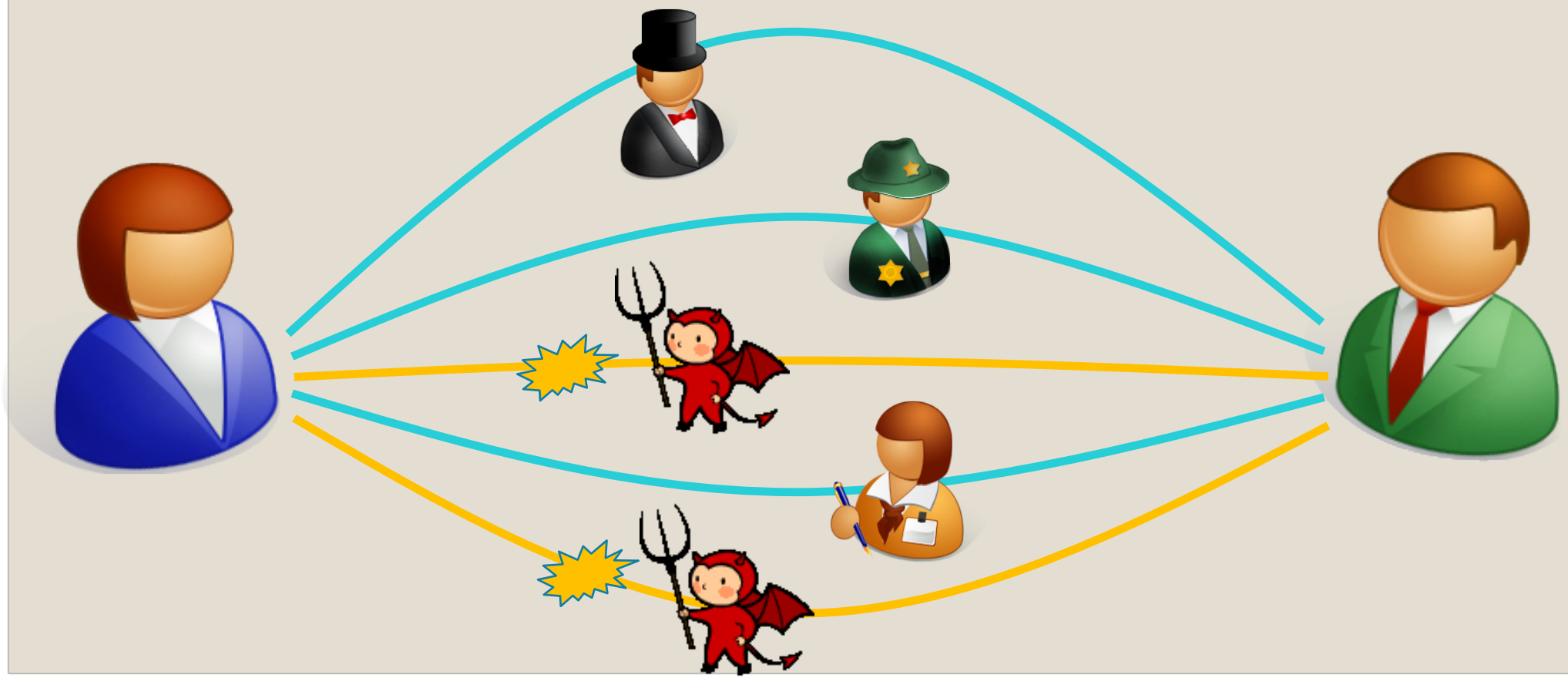
小柴健史（早稲田大学）

セキュアメッセージ転送



セキュアメッセージ転送 (Secure Message Transmission)

- Dolev, Dwork, Waarts & Yung (FOCS 1990 & JACM 1993)



基本設定と目的

基本設定

- アリスとボブの間に複数のチャネルが利用可能
  - チャネルを通じて同期的にメッセージを送信することが可能
- その複数のチャネルのうちいくつかは敵対者イブによって支配制御される
  - イブは支配チャネル下で送信中のメッセージを盗聴・改竄できる
  - イブはノード内に存在して支配するというより，外部からノードを支配する存在で支配かのチャネル情報はすべて把握できる

目的

- アリスが持つメッセージ m をボブに伝達すること
  - **信頼性**(Reliability): ボブが受信したメッセージm'は m と同一
  - **秘匿性**(Privacy): イブは m に関する情報を一切得られない

なぜ，セキュアメッセージ転送？

なぜ，セキュアメッセージ転送を考えるのか？

- 多者間秘匿計算(Multi-party Secure Computation)では，
  - 各プレーヤは完全グラフのノードに対応
  - 任意の2人のプレーヤの間には直接辺が存在し安全なチャネルと考える

- 不完全なグラフ（ネットワーク）にて，
  - グラフ上の2ノードに対応するアリスとボブはメッセージを交換したい
  - もしアリスとボブがSMTを実行できるならば, 直接辺に相当する安全なチャネルが存在すると仮想的に考えられる

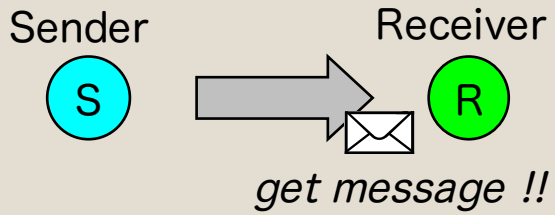
いろいろなSMT

安全性	Perfect	or	Probabilistic
通信回数	1-way (1-round)	or	2-way (2 or more rounds)
ネットワーク	有向グラフ	or	無向グラフ
敵のモデル	Threshold Adv	or	Generalized Adv
公開チャンネル	使用する	or	使用しない

1-way or 2-way (ラウンド数)

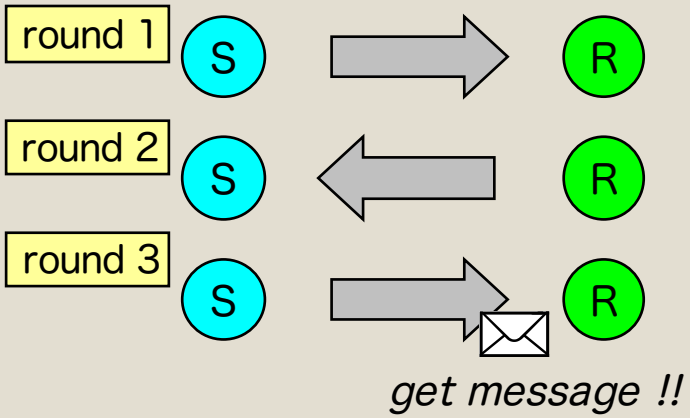
1-way Rは受信するだけ

= 1-round SMT protocol

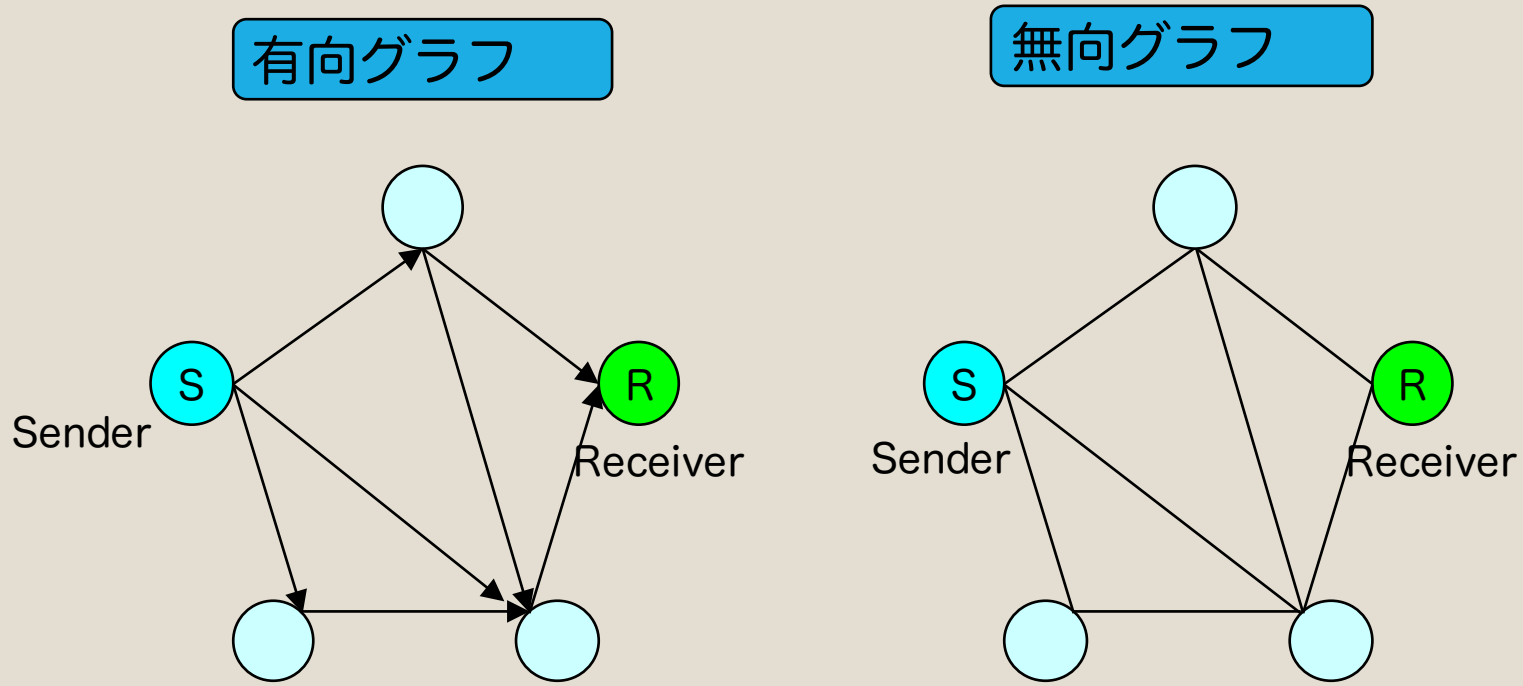


2-way SとRは情報のやり取りをする

= 2 or more rounds SMT protocol

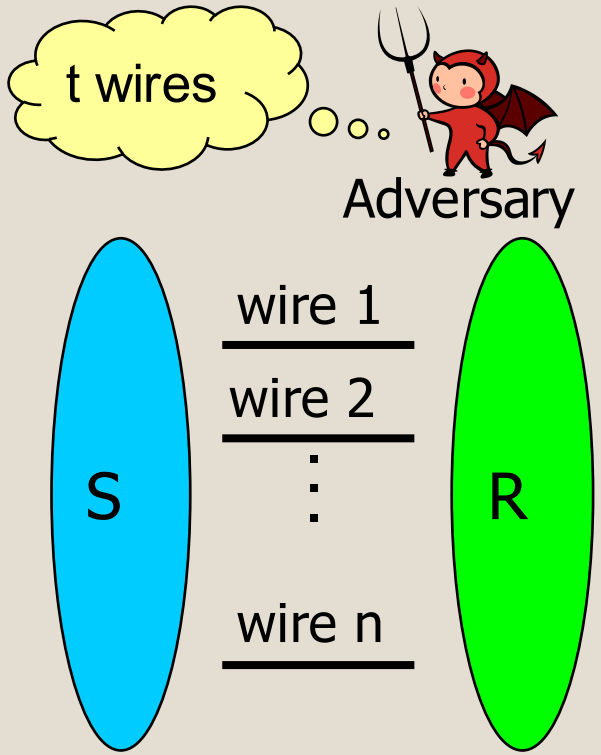


ネットワーク



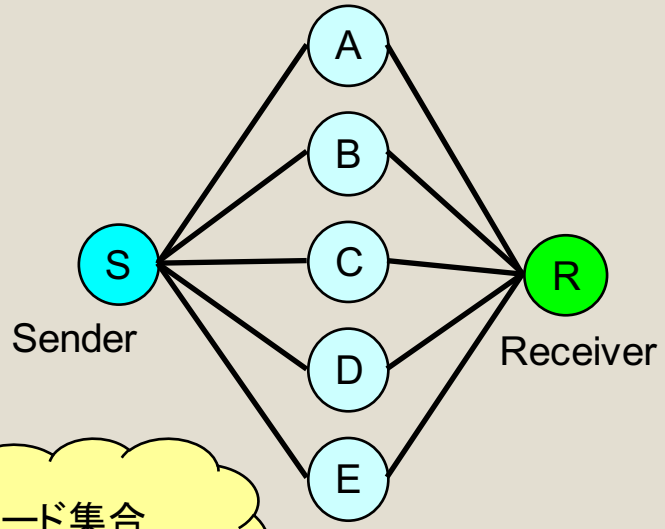
Threshold Adversary

- SとRの間には*n*本のwireがあると抽象化
- 敵は *n*本の内 *t* 本を任意に選び、支配できる (しきい値:*t*)
- 敵は 支配したwire上の情報を盗聴、改ざんできる



Generalized Adversary [Kumar et al. 2002]

- 抽象化せず、グラフで考える
- Adversary structure A_{adv} により支配するノードを決める



どのノード集合を支配しようか

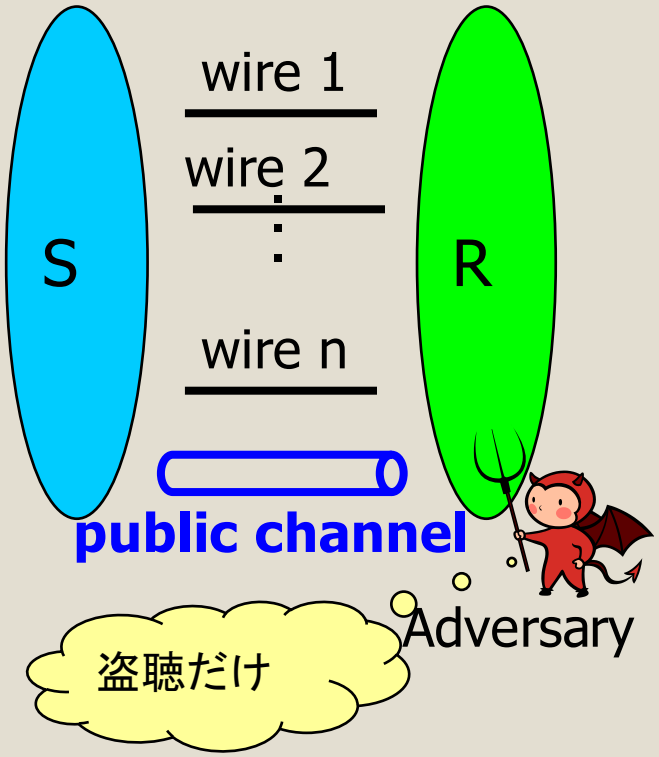
Adversary

Adversary structure の例

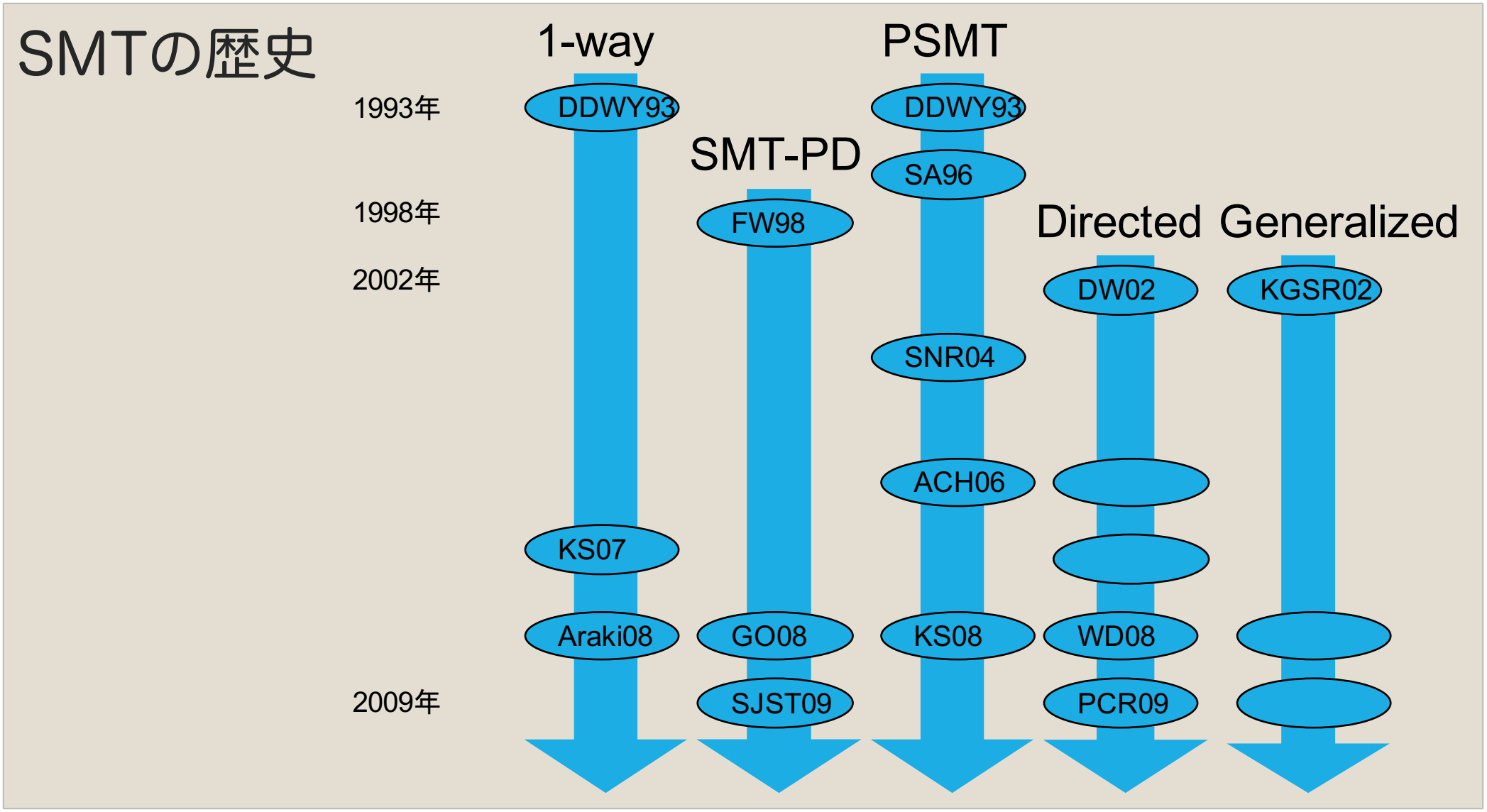
A_{adv}= { {A,B,C}, {A,B,D}, {A,E}, {B,D}, {C,D}, {BE} }

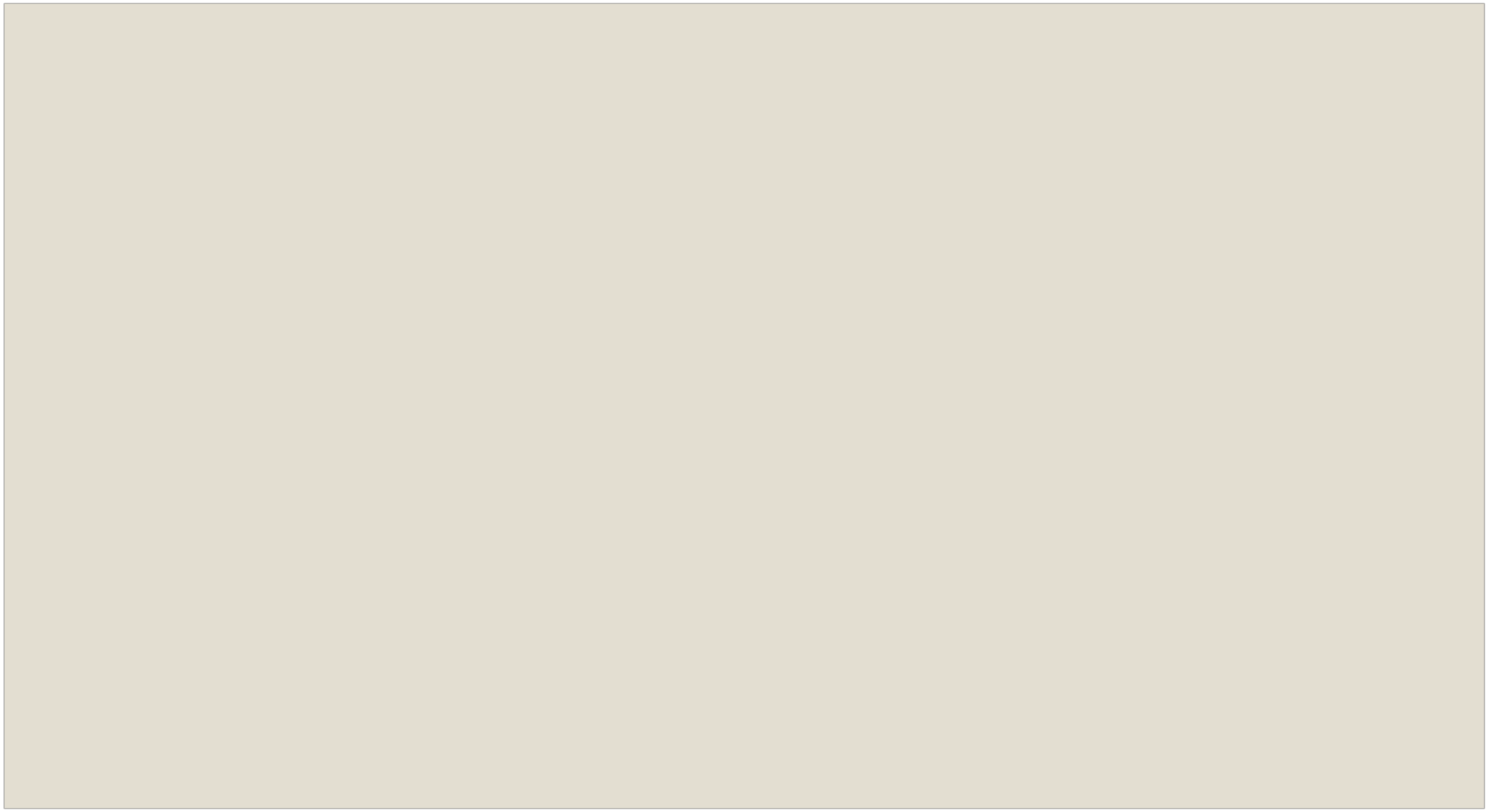
公開チャンネルモデル(SMT-PD)

- n本のwireに加え、公開チャンネルを使う
- 敵は公開チャンネル上の情報を見られるが、改ざんはできない
- 敵は n本の内 t 本の wire を支配し、 盗聴、改ざんできる



SMTの歴史


1-way
PSMT
SMT-PD
Directed
Generalized
1993年
1998年
2002年
2009年
DDWY93
DDWY93
SA96
FW98
DW02
KGSR02
SNR04
ACH06
KS07
Araki08
GO08
KS08
WD08
SJST09
PCR09



セキュアメッセージ転送：詳細

アリスとボブの間の n 本のチャネルを利用した通信プロトコル

- アリスは事前にメッセージ m を持つ。確率変数 M_A を想定して，m は M_A が取る値と考える。
- アリスとボブは確率的アルゴリズム。アリスは乱数 r_A をボブは乱数 r_B を利用する。
- アリスとボブは交互に n 本のチャネルを通じて情報を送信
- 1回のラウンドは，送信者（アリスあるいはボブ）から n 個の情報を各チャネルに流すことで開始。受信者（ボブあるいはアリス）は n 個の情報を各チャネルから受け取り，ラウンド終了。
- イブ支配化のチャネルは盗聴・改竄されているかもしれない。イブがチャネルに流れる情報を遮断した場合は，受信者は何も送られてこなかったことを認識できる。
- アリスが i ラウンド目に送る情報は，m と r_A と i -1 ラウンド目までに得た情報から決定的に計算できる
- ボブが i ラウンド目に送る情報は r_B と i -1 ラウンド目までに得た情報から決定的に計算できる。最終的にボブはアリスから M_B を受け取ったと認識。

ビュー (View)

アリスのビュー（確率変数 V_A）：アリスが見ることのできるすべて

- i ラウンド目のビュー
  - メッセージ m
  - アリスの乱数 r_A
  - i ラウンド目までにアリスがボブから受け取った情報（ボブの乱数 r_B，イブの乱数 r_E に依存）

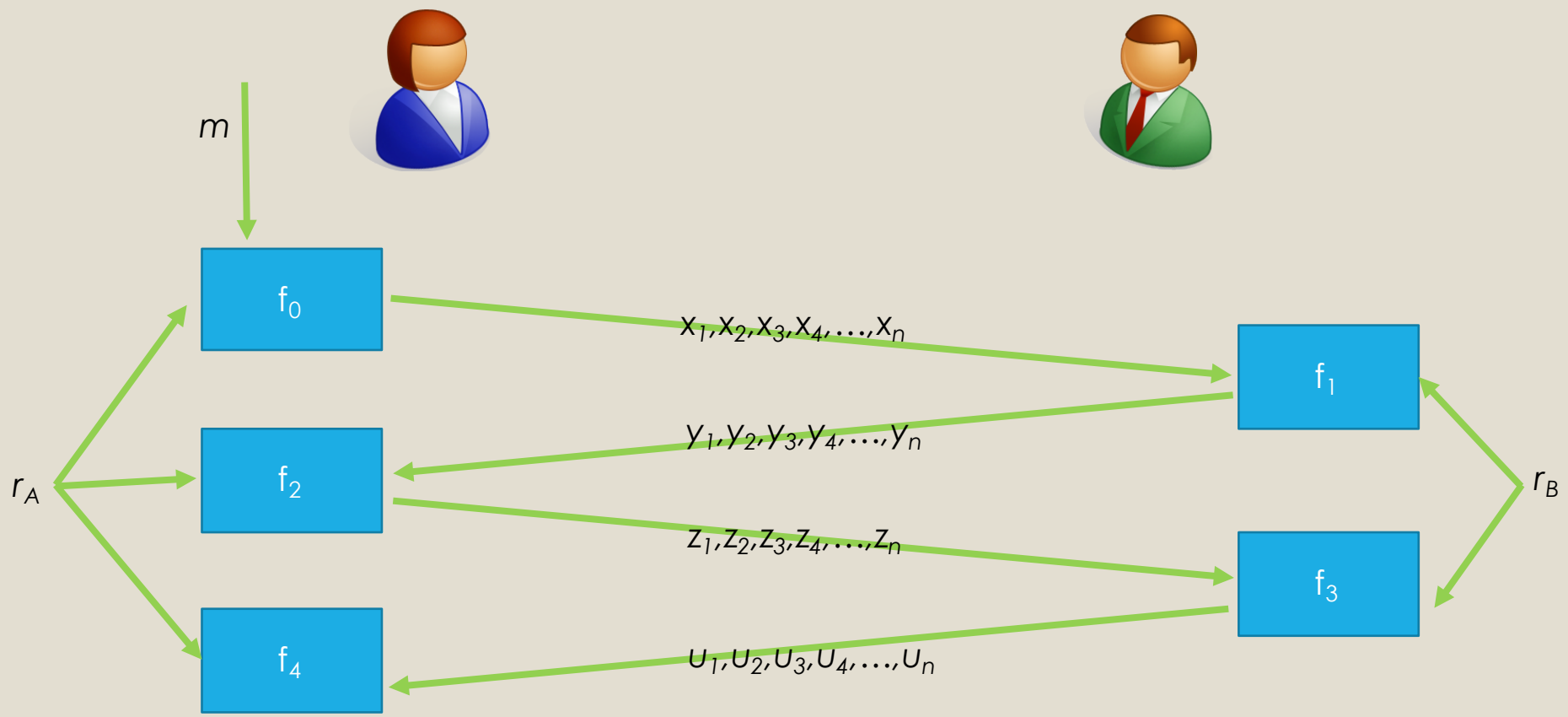
ボブのビュー（確率変数 V_B）：ボブが見ることのできるすべて

- i ラウンド目のビュー
  - ボブの乱数 r_B
  - i ラウンド目までにボブがアリスから受け取った情報（アリスの乱数 r_A，イブの乱数 r_E に依存）

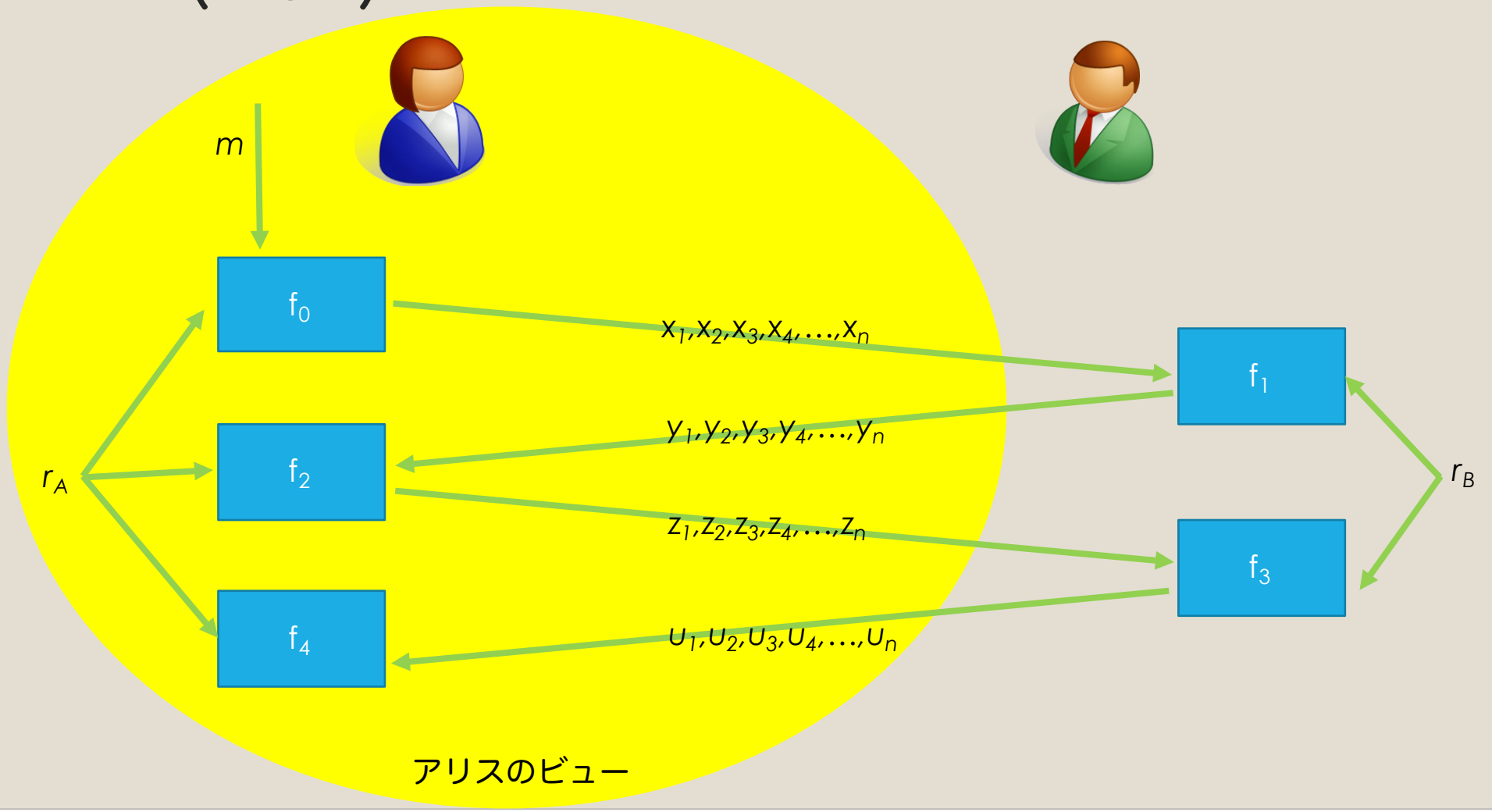
イブのビュー（確率変数 V_E）：イブがみ見ることのできるすべて

- イブの乱数 r_E
- i ラウンドまでに支配チャネルに流れた情報（アリスの乱数 r_A，ボブの乱数 r_B）に依存

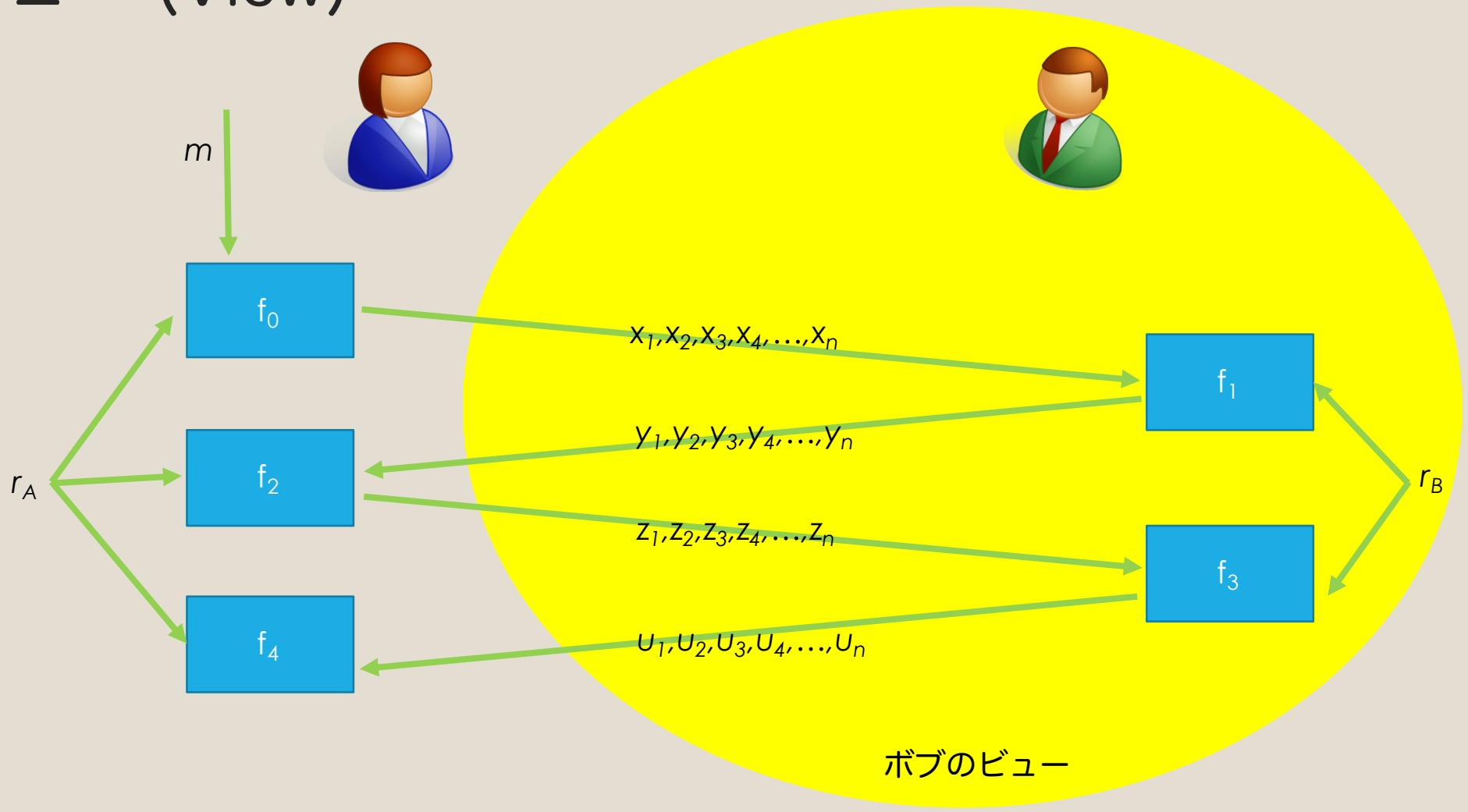
ビュー (View)


m
f0
f1
f2
f3
f4
rA
rB
x1,x2,x3,x4,...,xn
y1,y2,y3,y4,...,yn
z1,z2,z3,z4,...,zn
u1,u2,u3,u4,...,un

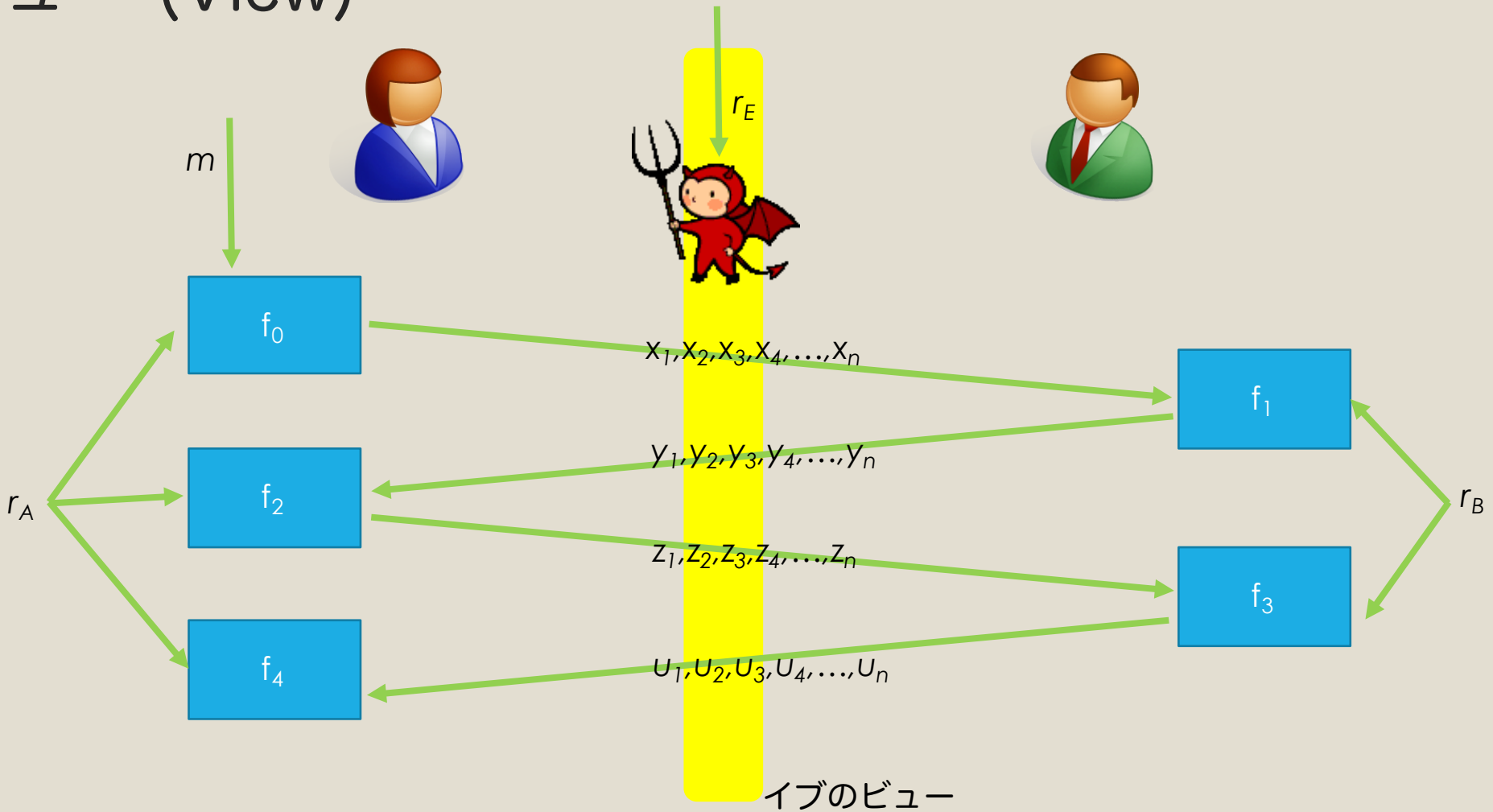
ビュー (View)


m
f0
f1
f2
f3
f4
rA
rB
x1,x2,x3,x4,…,xn
y1,y2,y3,y4,…,yn
z1,z2,z3,z4,…,zn
u1,u2,u3,u4,…,un
アリスのビュー

ビュー (View)


m
f0
f1
f2
f3
f4
rA
rB
x1,x2,x3,x4,…,xn
y1,y2,y3,y4,…,yn
z1,z2,z3,z4,…,zn
u1,u2,u3,u4,…,un
ボブのビュー

ビュー (View)


m
r_E
f_0
f_1
f_2
f_3
f_4
r_A
r_B
$x_1,x_2,x_3,x_4,\ldots,x_n$
$y_1,y_2,y_3,y_4,\ldots,y_n$
$z_1,z_2,z_3,z_4,\ldots,z_n$
$u_1,u_2,u_3,u_4,\ldots,u_n$
イブのビュー

基本性質の定義

δ 信頼性

$\Pr(M_A \neq M_B) \leqq \delta$

ε 秘匿性

任意の m, m' および任意の r_E において

$\Delta((V_E \mid M_A = m, R_E = r_E), (V_E \mid M_A = m', R_E = r_E)) \leqq \varepsilon$

Δは変動距離

$\Delta(X,Y) = (1/2) \Sigma_\alpha \mid \Pr(X = \alpha) - \Pr(Y = \alpha) \mid$

(ε, δ)-SMT：秘匿性ε，信頼性δのセキュアメッセージ転送プロトコル

(0, 0)-SMT：完全セキュアメッセージ転送 (Perfect SMT, PSMT)

セキュアメッセージ転送：上限と下限

イブは，n本のチャネルの内，t本までを支配できる（と想定）

◦ 信頼性・秘匿性ともに完全な場合(Perfect SMT (PSMT))

$n > 2t$: efficient PSMT protocol

e.g., Kurosawa & Suzuki (EuroCrypt 2008 & IEEEIT 2009)

$n \leq 2t$: impossible (Dolev, Dwork, Waarts & Yung 1993)

◦ Almost Reliable Case (Bob receives a wrong message with small prob.)

$n \leq 2t$: still impossible (Franklin & Wright, EuroCrypt 1998 & JoC 2000)

下限の例

$n \leqq 2t$ とする。

$\varepsilon+\delta < 1 - 1/|M|$ を満たす (ε, δ)-SMT は存在しない

下限の証明概略 1

（簡単のため）$n = 2t$ とする

- つまり，半分はイブに支配されていて，残り半分は支配されていない。
- X_j : j 番目のラウンドで前半のチャネルに流れる情報
- Y_j : j 番目のラウンドで後半のチャネルに流れる情報

- 以下のような特殊なイブを想定し，秘匿性と信頼性を同時に満たせないことを示す。
  - r_E の1ビット目が0のときは前半を支配，1の時は後半を支配。r_E の1ビット目を r_{E1} とし，残りを r_{E2} と記す

以下，$r_{E1} = 1$ の場合

- アリスからボブへの通信はすべて遮断，つまり，アリスが X_jY_j を流しても X_j だけボブに伝わる
- ボブからアリスへの通信は改ざん，つまり，ボブが X_jY_j を流した時，$X_j'Y_j' = f_j(V_E^{j-1}, r_{E2})$ を計算し，後半をすり替える。つまり，アリスには X_jY_j' が伝わる。
- 最終的にイブは $M_E = g(V_E^k, r_{E2})$ を m の予想として出力

下限の証明概略２

プロトコルすべてを眺めることができる（神様の）ビュー V を考える

- V は M_A，r_A，r_B，r_E によって決まる
- 神様ビュー上の二項関係 W を導入（反転ビュー関係）

(V, V') in W ⇔

(1) M, r_Aパートは同一

(2) r_{E1}パートは反転

(3) $r_{E2} = r_B'$ かつ $r_{E2}' = r_B$

補題：(V, V') in W とする。このとき，以下が成立

(a) $V_A = V_A'$

(b) $V_E' = V_B$，つまり，$M_B = M_E$

下限の証明概略３

成功ビュー：$M_A = M_B$ となるビュー

◦ $p = \Pr[M_A = M_B]$ は，ビューが成功ビューとなる確率の総和で計算される

◦ Vが成功ビューなら，反転ビューV' においても $\Pr[M_A = M_E] = p$ となる

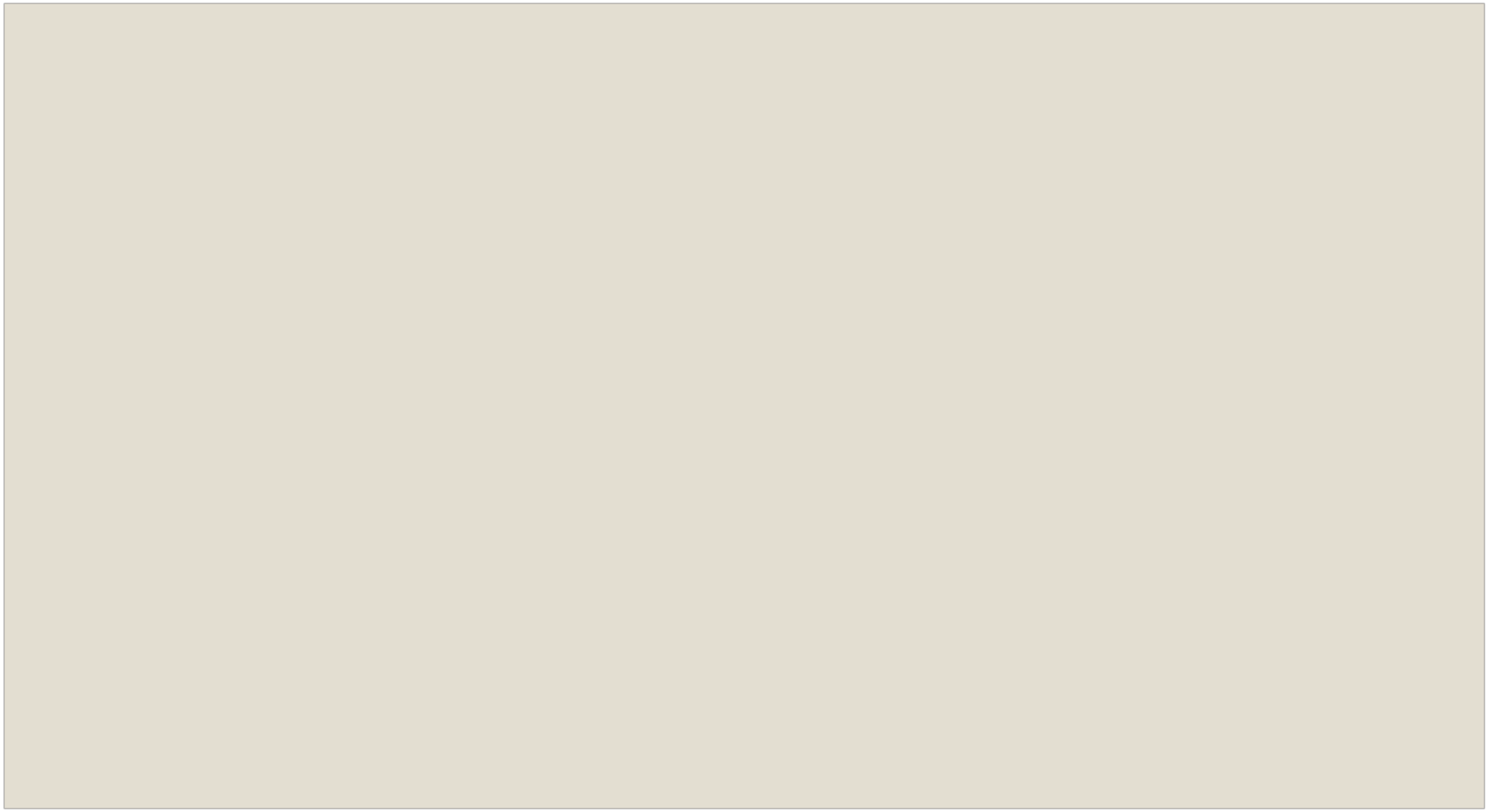
補題：(ε, δ)-SMT において

$$\Pr[M_E = M_A] \leqq \varepsilon + 1/|M|$$

つまり，

$$1 - \delta \leqq \Pr[M_A = M_B] = \Pr[M_A = M_E] \leqq \varepsilon + 1/|M|$$

となり矛盾！



完全セキュアメッセージ転送(PSMT)

以下の接続数を持つときに限り、(0,0)-SMTプロトコルは存在する。 [Dolev et al. 1993]

1-way $n \geqq 3t+1$

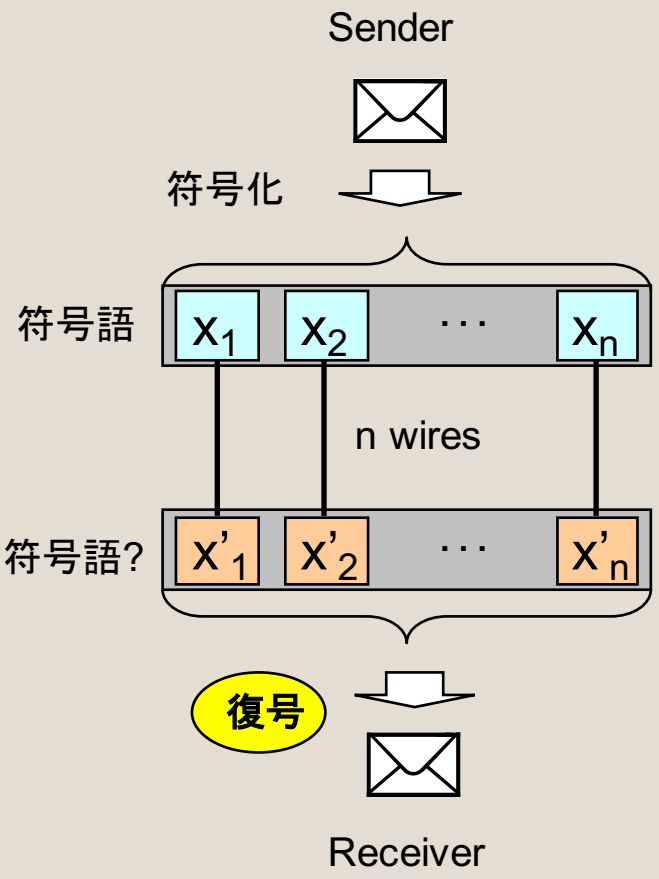
⇨ 全てのwireの1/3未満なら、敵に支配されてもよい

2-way $n \geqq 2t+1$

⇨ 全てのwireの1/2未満なら、敵に支配されてもよい

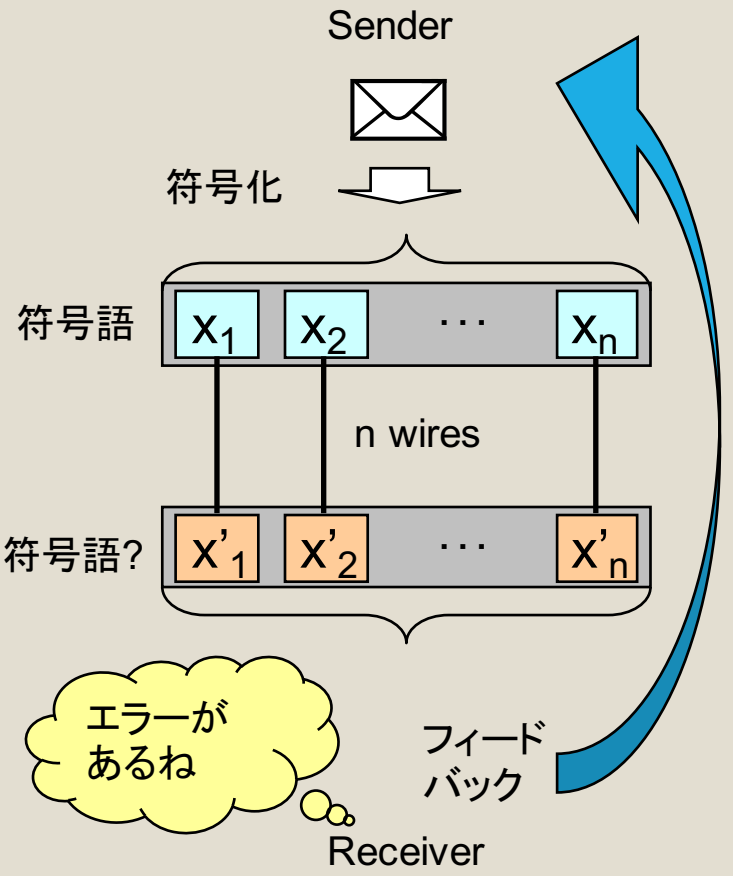
1-way PSMTと符号理論

- SはRから何のフィードバックも得られない
- $(x'_1, x'_2, \ldots, x'_n)$からメッセージを復元するしかない
- t エラー訂正可能な誤り訂正符号を解くことと同じ
- t 個以下の情報からメッセージは復元できてはならない



2-way PSMTと符号理論

- SはRからフィードバックを得ることができる
- $(x'_1, x'_2, \ldots, x'_n)$が符号語かどうか判断できる必要あり
- t エラー検出可能な誤り検出符号を使う
- t 個以下の情報からメッセージは復元できてはならない



PSMTと符号理論

(n,k,d)符号

- **長さ:** n
- **情報記号数(次元):** k
- **最小ハミング距離:** d　である線形符号

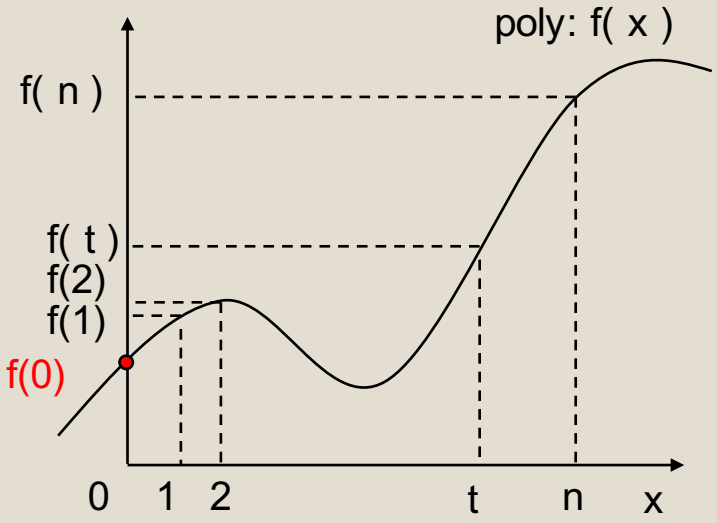
検出能力: d-1

訂正能力: (d-1)/2

敵は t wiresを支配できるので、$k \geqq t+1$ の符号を考える。

また、符号長を短くするにはd=n-k+1 を満たす必要がある。

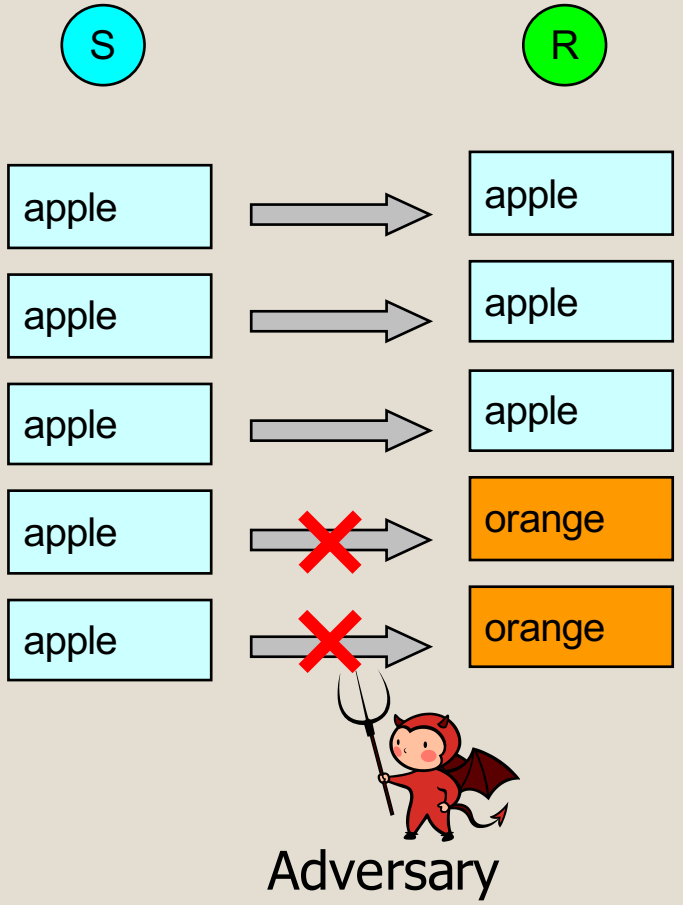
t 次多項式 f(x)



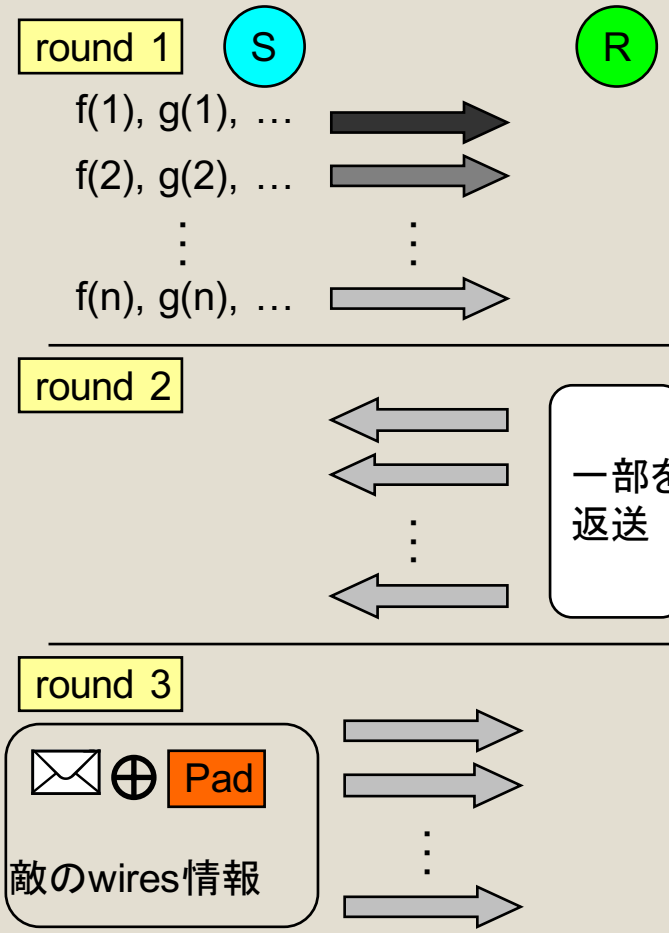
- f(0) を秘密の値とする
- t+1 個の座標がわかるとき、多項式を一意に特定し、f(0)を復元できる
- ただし、t 個の座標では f(0) について何の情報も得られない

ブロードキャスト

- 全てのwire に対して同じ情報を送ること
- n≧2t+1 ならば、相手に正確な情報が伝えられる
- 受信側は多数決をとるだけでよい



2-way PSMTの基本的なアイディア



Sは t次多項式をいくつも生成する

代入値 f(i), g(i),… をwire i で送る

Rは改ざんされた多項式を検出できる

Rはいくつかの多項式の代入値をブロードキャストして送り返す

Sは返送された値を元に敵のwires を特定

Sはブロードキャストされなかった多項式からワンタイムパッドを生成

暗号文と敵のwires情報をブロードキャスト

Rは敵のwires情報を使って暗号文解読

2-way PSMT プロトコルの効率

	伝送率	通信複雑性	計算コスト
DDWY93	$O(n^5)$	exp	exp
SA96	$O(n^3)$	exp	exp
ACH06	O(n)	exp	exp
KS08	O(n)	$O(n^3)$	poly

伝送率 = 全ビット数 / メッセージのビット数

伝送率の下限がn であることを示した [SNR04]

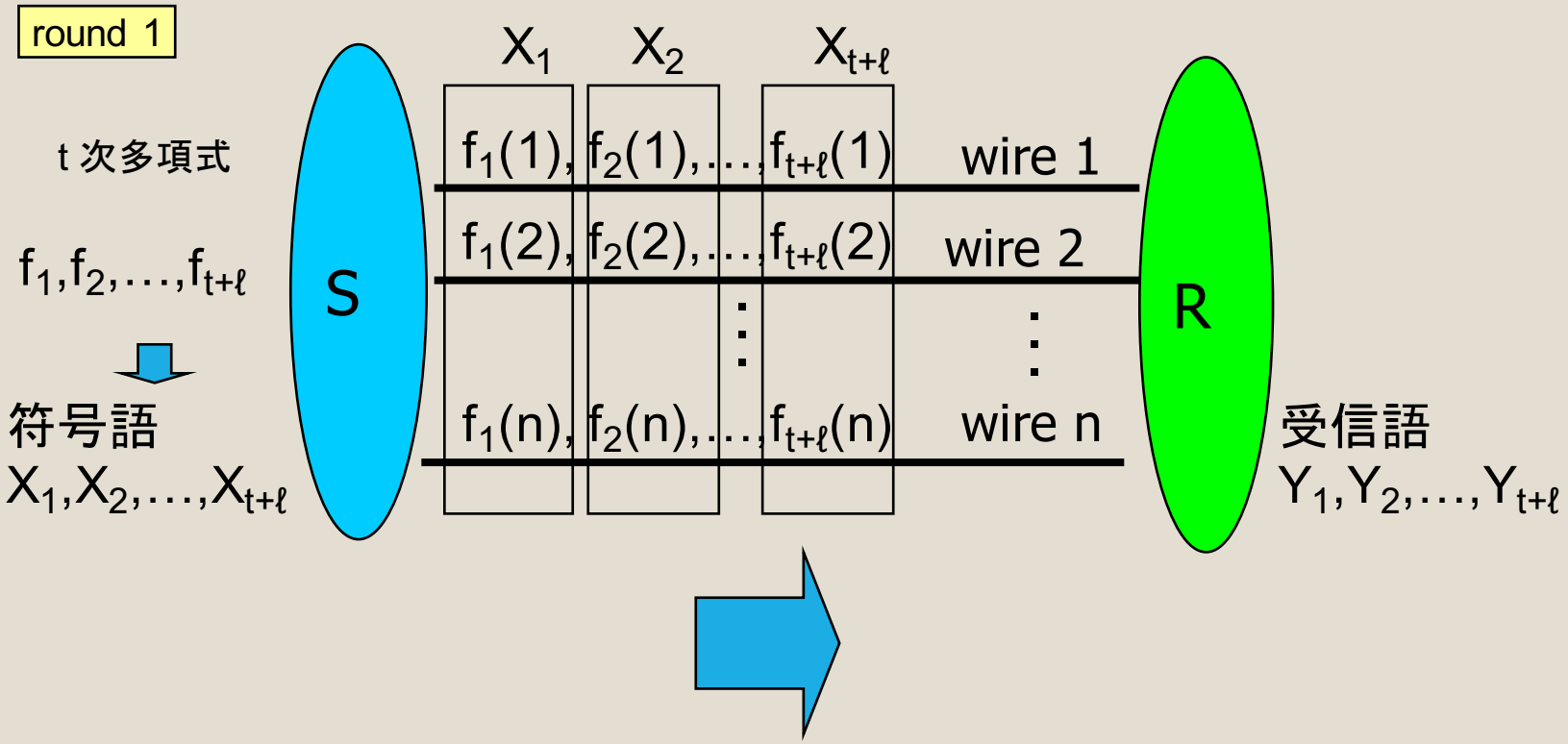
DDWY93 のPSMTプロトコル

- Slow protocol (many rounds)
  - 各round で多項式を1つだけ送る
  - 各round で少しずつ支配wire を除外していく
- Fast protocol (3-rounds)
  - 1st round で大量に多項式を送る
  - 一部の多項式を送り返す(鳩の巣原理を利用)
  - 使用していない多項式によりメッセージをマスク

KS08 3-round PSMTプロトコル

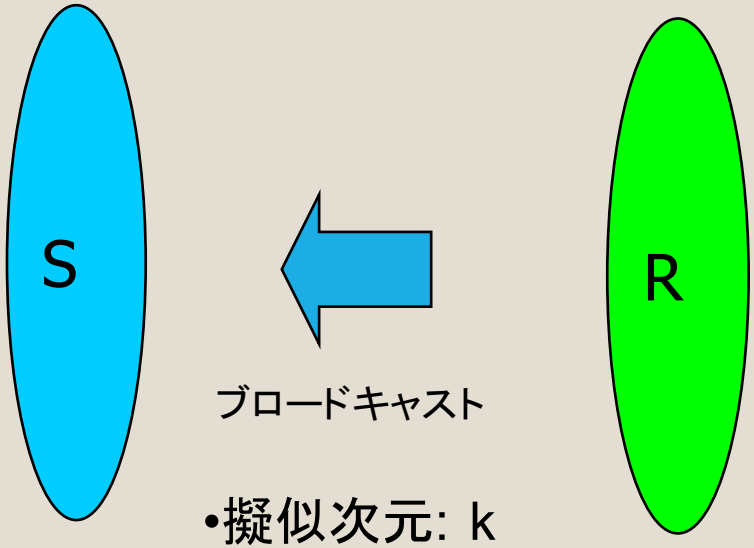
- $t+\ell$ 個の多項式を送る
- 符号理論に擬似基底を取り入れて、効率良く敵の検出をしている
- 同時にメッセージをℓ 個送信することで、伝送率を向上させている

KS08 3-round PSMTプロトコル



KS08 3-round PSMTプロトコル

round 2



Corrupted wires
を特定できる

ブロードキャスト

- 擬似次元: k
- 擬似基底: B
- 基底の添字集合

受信語
$Y_1, Y_2, \ldots, Y_{t+\ell}$

擬似基底
$B=\{Y_{j1}, Y_{j2}, \ldots, Y_{jk}\}$
を見つけ出す

KS08 3-round PSMTプロトコル

round 3

未公開の多項式
$f_{i1}, f_{i2}, \ldots, f_{i\ell}$

$f_{i1}(0), f_{i2}(0), \ldots, f_{i\ell}(0)$
を使ってℓ個のメッセージをマスク

S

ブロードキャスト

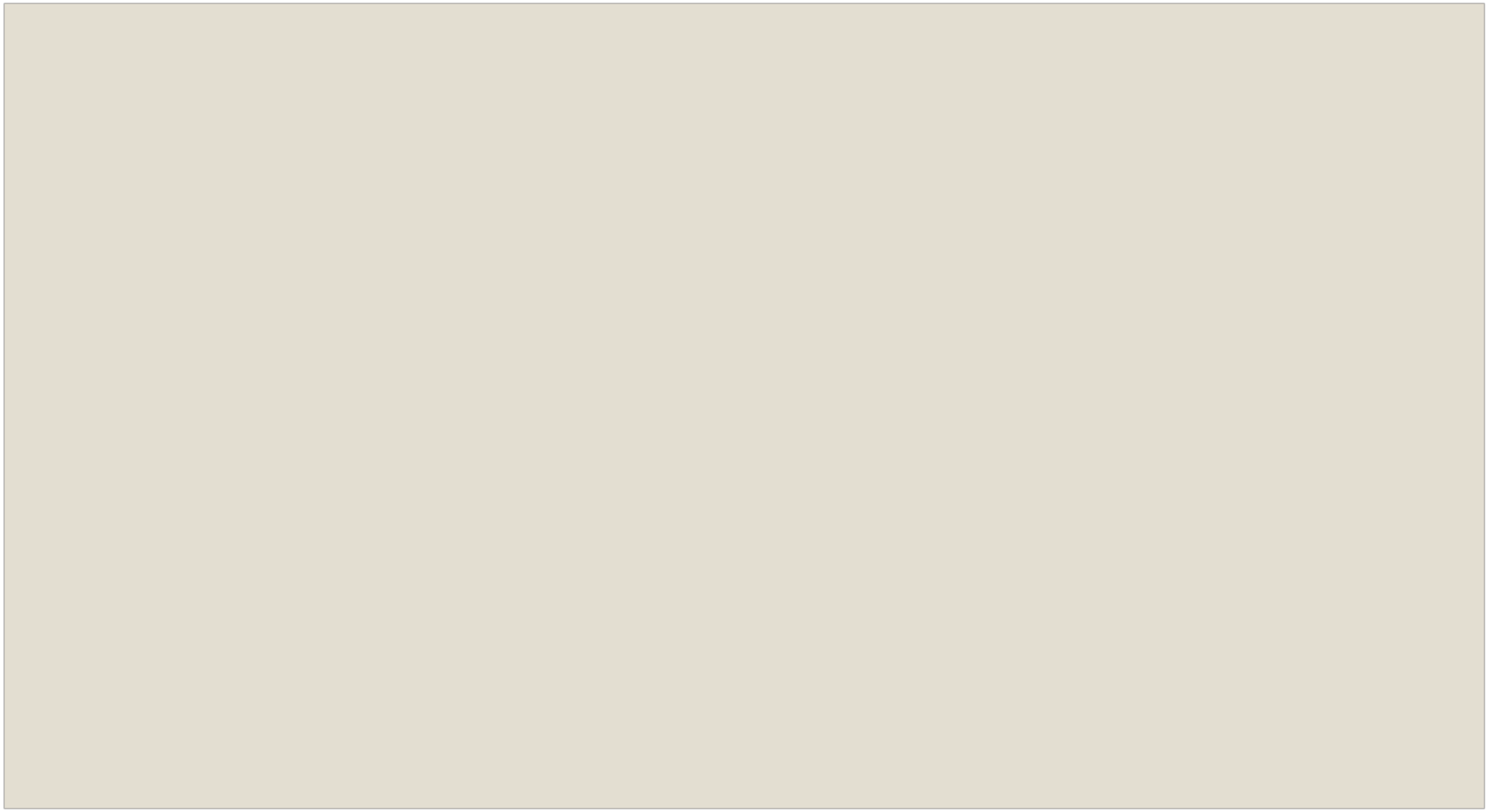
- Corrupted wires
- マスクした暗号文

R

受信語
$Y_1, Y_2, \ldots, Y_{t+\ell}$

未公開の受信語から
正確な成分を抽出
(corrupted wires 参照)

$f_{i1}(0), f_{i2}(0), \ldots, f_{i\ell}(0)$
を復元して暗号文を復号

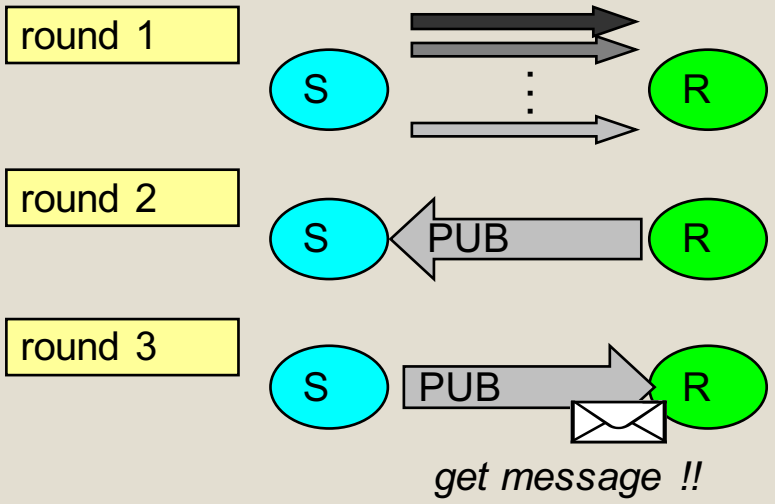


SMT-PD [Franklin & Wright 1998]

- multicast model は wires + broadcast と等価であることを示した
- $n \leqq 2t$ wires だけのとき、reliability δの値を1/2以下にできない
- $n \leqq 2t$ wires + broadcast なら、$(0,\delta)$-SMT プロトコルが構成できる

SMT-PD プロトコル

	rounds	Forward PUB	Backward PUB
GO08	4	2rounds	1round
SJST09	3	1round	1round



SMT-PD プロトコルのアイディア

- 1st round に いくつか乱数を共有する(wiresを使って)
- (ハッシュ)関数を使い、確率的にreliability を保証する
- 少なくとも1 wire は支配されないので、敵はそこを通る情報を知らない(0-privacy)

Almost Strongly Universal$_2$ Hash

$m > \ell$

$\mathcal{H} = \{ h : \{0,1\}^m \rightarrow \{0,1\}^\ell \}$ が γ-almost strongly universal$_2$

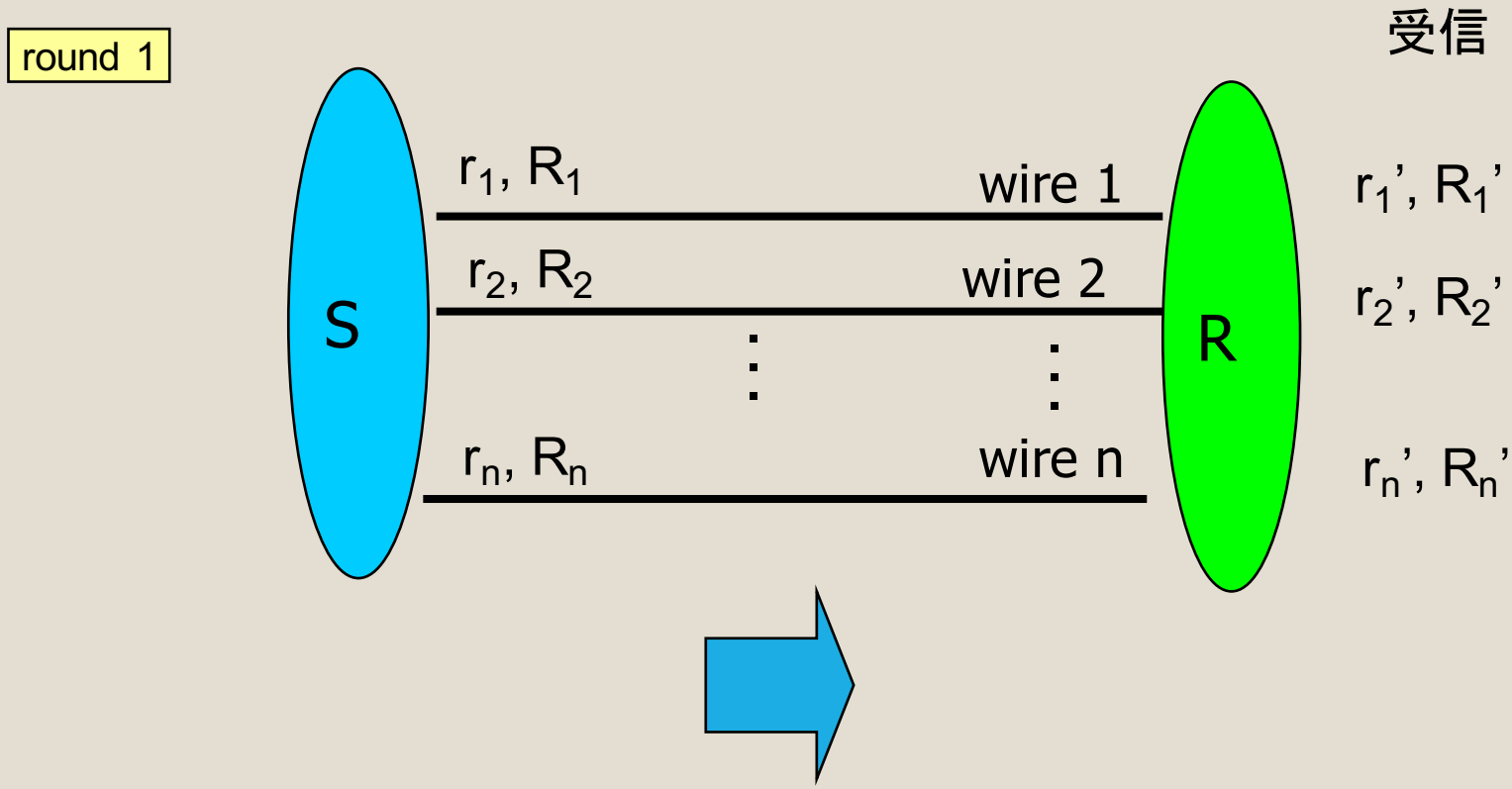
$\Leftrightarrow$

任意の $a_1 \neq a_2$ in $\{0,1\}^m$ と b_1, b_2 in $\{0,1\}^\ell$ で

$\Pr_{h \leftarrow \mathcal{H}} [h(a_1) = b_1 \ \& \ h(a_2) = b_2] \leqq \gamma$

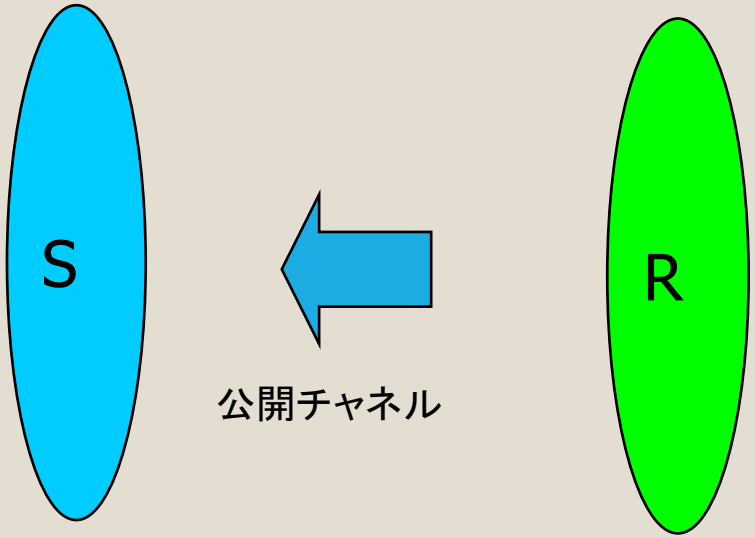
[Wegman & Carter (1981)]

SJST09 3-round SMT-PDプロトコル



SJST09 3-round SMT-PDプロトコル

round 2



公開チャネル

各ワイヤで $h_i \leftarrow \mathcal{H}$

$T_i' = r_i' \oplus h_i(R_i')$を計算,
計算できたときは$b_i=0$
できないときは$b_i=1$

$(T_1', h_1, b_1), \ldots, (T_n', h_n, b_n)$

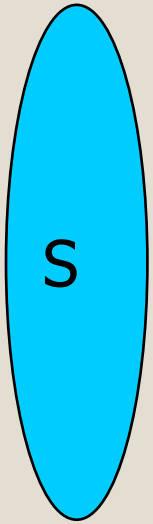
SJST09 3-round SMT-PDプロトコル

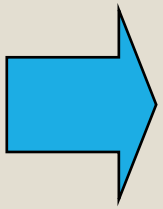
round 3

b_i=1のときi番目要素は無視

$T_i = r_i \oplus h_i(R_i)$を計算し
$T_i = T_i'$ かどうかチェック
等しいときv_i=0，それ以外v_i=1

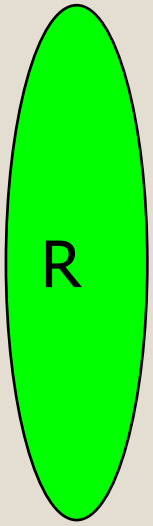
$C = m \oplus (\oplus_{j:v_j=0} R_j)$を計算





公開チャネル

C, v_1v_2…

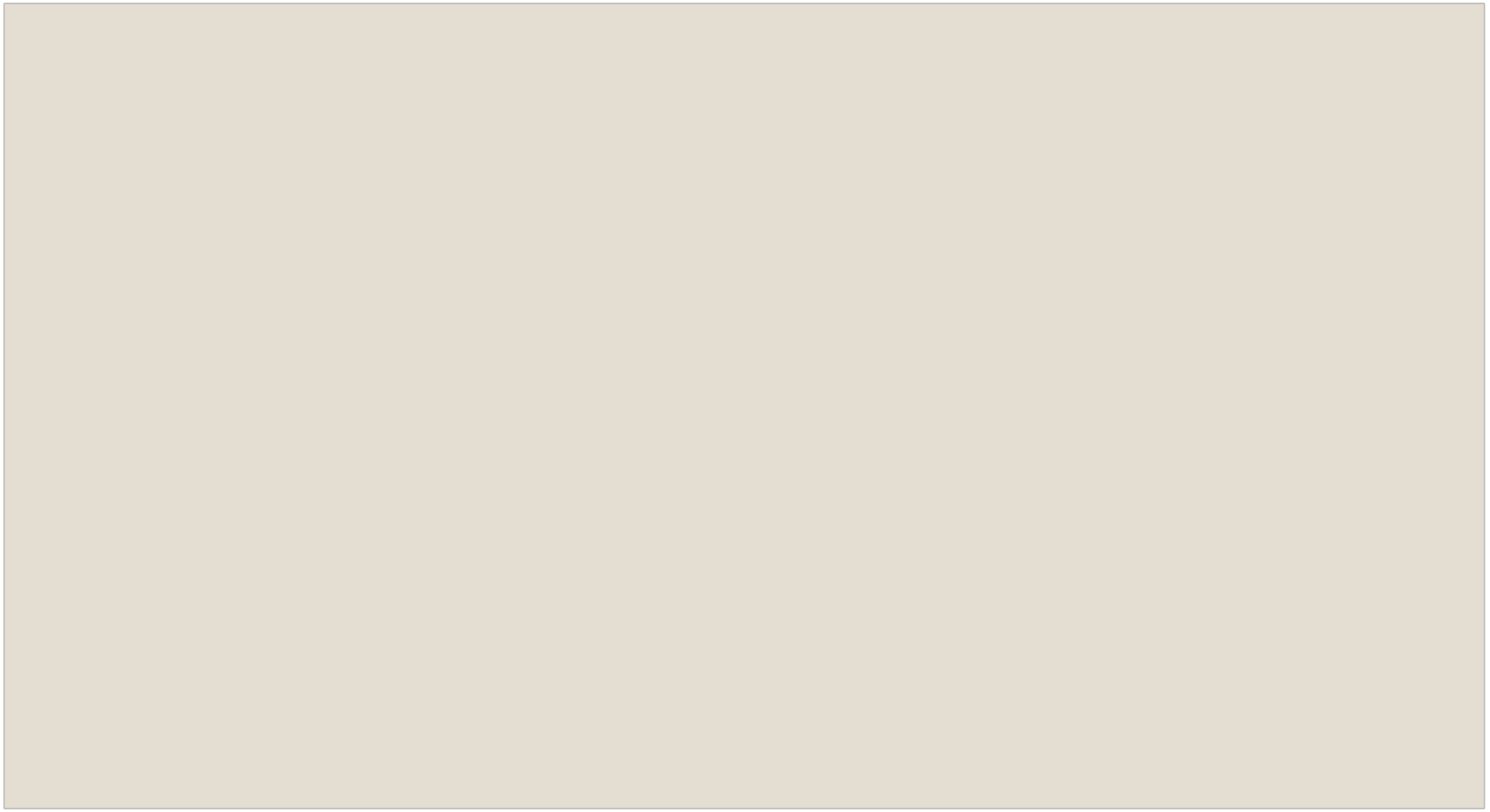


$m' = C \oplus (\oplus_{j:v_j=0} R_j')$を計算&出力

SJST09 3-round SMT-PDプロトコル

SJST09 SMT-PDプロトコルは以下を達成

- 0-秘匿性
- $(n-1)2^{1-\ell}$ 信頼性



$n=2t$ のバリア

- PSMT は $n \geqq 2t+1$が必要
  - δ-信頼性($\delta \neq 0$)への緩和はバリアを超えない
  - 公開チャネルが利用できると$n \geqq t+1$まで可能
    - $n \geqq t+1$で (0,0)-PSMT-PD は可能？
  - 敵対者モデルの緩和
    - 合理的な敵対者の導入 → いくつかの条件のもと，$n \geqq t+1$でも PSMT が達成

まとめ

- セキュアメッセージ転送とは？
- 様々なSMTモデル
- SMTの敵対者支配数の下限
- PSMTプロトコル
- SMT-PDプロトコル