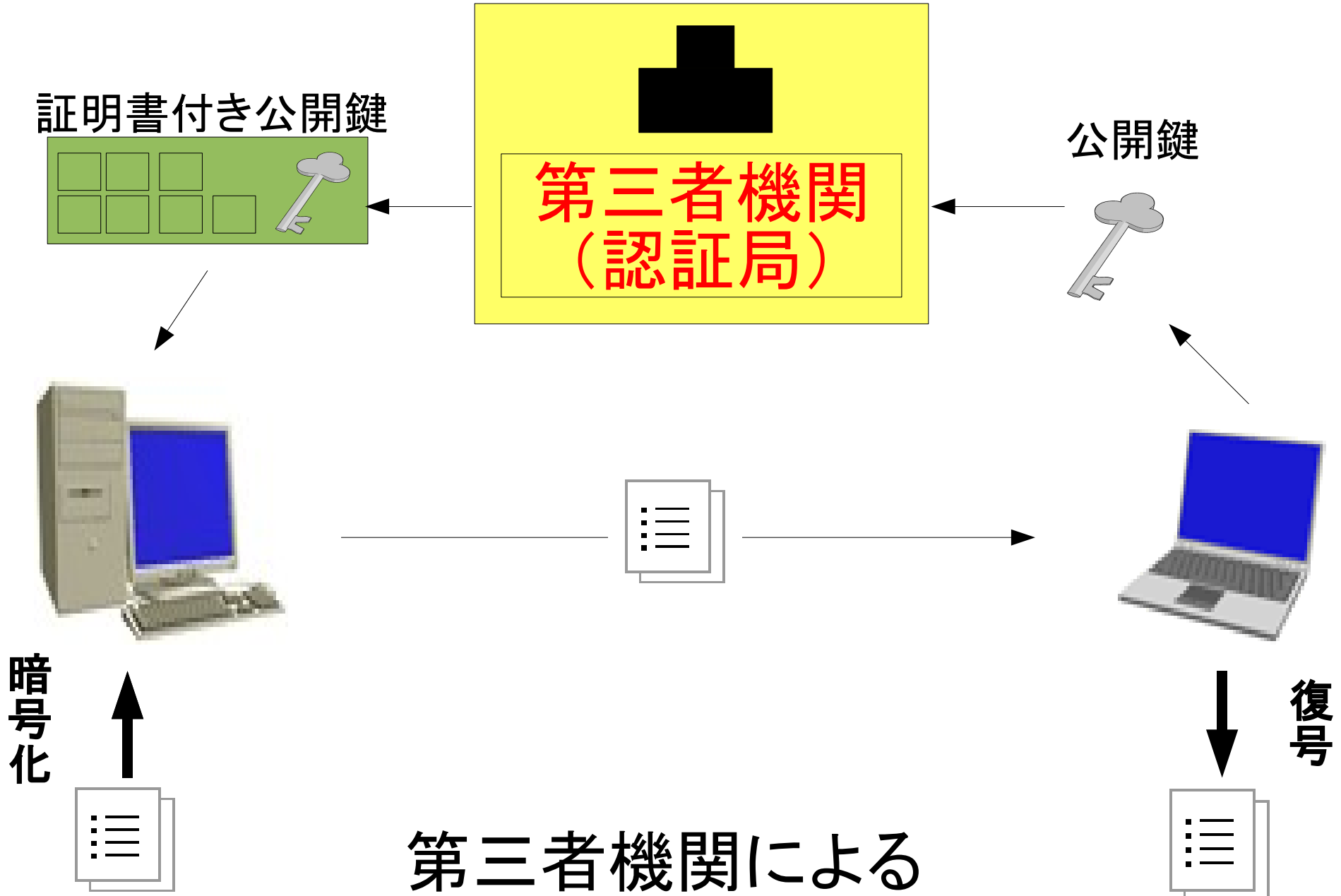
# nチャネルメッセージ伝送方式による暗号化通信

木下研究室　200402931　渡邉優司

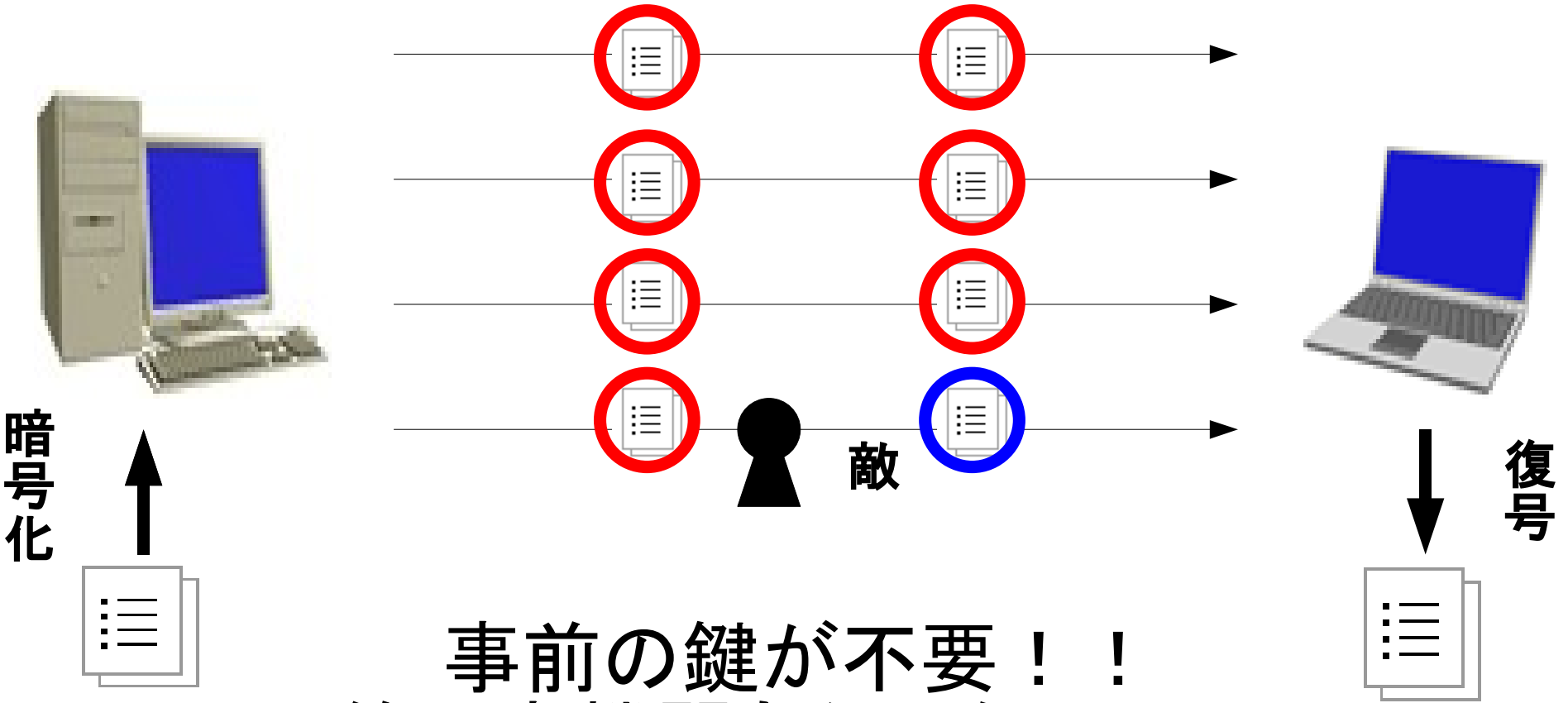
# 従来の暗号方式～公開鍵暗号～




第三者機関による
公開鍵の正当性証明が必要

# nチャネルメッセージ伝送

## n本の通信路を使用する伝送方式




事前の鍵が不要！！
第三者機関も必要ない！！

# 安全性の定義
# PSMT：Perfectly Secure Message Transmission

盗聴や改ざんする敵がn本の通信路の内t本に潜んでいるとき・・・・

1. **盗聴耐性**
   敵は送信メッセージに関する情報を何も得られない。

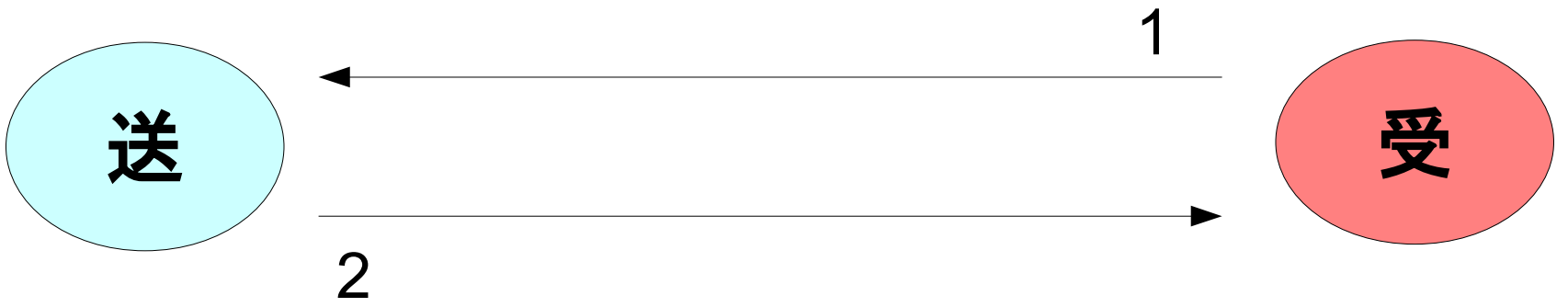
2. **改ざん耐性**
   受信者がメッセージを正しく受信できる確率が100％である。

# PSMTの歴史

| | PSMT | |
|---|---|---|
| | 2-round | 1-round |
| Dolev 1993 | n≧ 2t+1が必要十分条件<br>通信量:$O(2^n)$ | n≧ 3t+1が必要十分条件<br>通信量:O(n)<br>計算量:多項式時間 |
| Sayeed 1996 | 通信量:$O(n^3)$ | |
| Agarwal 2006 | 通信量:O(n)<br>ただし大量のSを送る<br>ことが前提<br>計算量:指数的 | |
| Kurosawa 2008 | 通信量:O(n)<br>計算量:$O(n^3)$ | |

# 1-round


# 2-round



# PSMTの歴史

| | PSMT | |
|---|---|---|
| | 2-round | 1-round |
| Dolev 1993 | n≧ 2t+1が必要十分条件<br>通信量:$O(2^n)$ | n≧ 3t+1が必要十分条件<br>通信量:O(n)<br>計算量:多項式時間 |
| Sayeed 1996 | 通信量:$O(n^3)$ | |
| Agarwal 2006 | 通信量:O(n)<br>ただし大量のSを送る<br>ことが前提<br>計算量:指数的 | |
| Kurosawa 2008 | 通信量:O(n)<br>計算量:$O(n^3)$ | |

# 安全性の定義
# ASMT：Almost Secure Message Transmission

1. **盗聴耐性**
   敵は送信メッセージに関する情報を何も得られない。

2. **改ざん耐性**
   受信者がメッセージを正しく受信できる確率が1-δ以上である。

3. **失敗検知能力**
   受信者が正しく受信できない確率がδ以下であり、そのとき受信者はfailureを出力できる。

4. **遮断耐性**
   敵がt本の通信路を遮断しても受信者は残りの通信路で得た情報だけからメッセージを受信できる。

# ASMTの歴史

2004　Srinathanらがプロトコル提案　→　間違いがあった。

2007　KurosawaらがASMTを厳密に定義。プロトコル提案。

**定理（Kurosawa, et al.)**

n=2t+1のとき通信効率の限界は

$|X_i| \geqq (|S|-1)/\delta+1$

$X_i$：channel(i)を流れる情報の集合

S：秘密情報の集合

δ：失敗確率

# Kurosawaらのプロトコルの通信効率

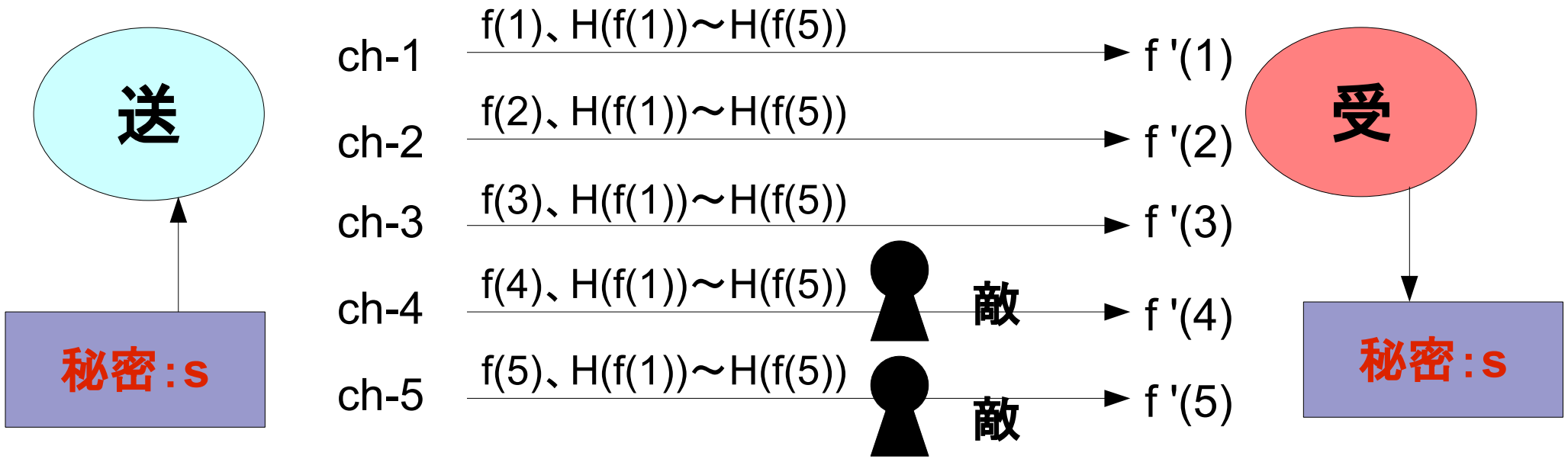
失敗確率をεとすると、通信量|Xi|は

$$|X_i| = \frac{|S|-1}{\delta} + 1 > \frac{|S|-1}{\varepsilon} + 1$$

ただし $$\varepsilon = \left\{ \binom{n}{t+1} - \binom{n-t}{t+1} \right\} \delta$$

通信効率は限界値に近いが、
計算量が指数関数的である。

# 提案するASMT（Basic プロトコル）




n=2t+1（n：通信路の数　t：敵の数）

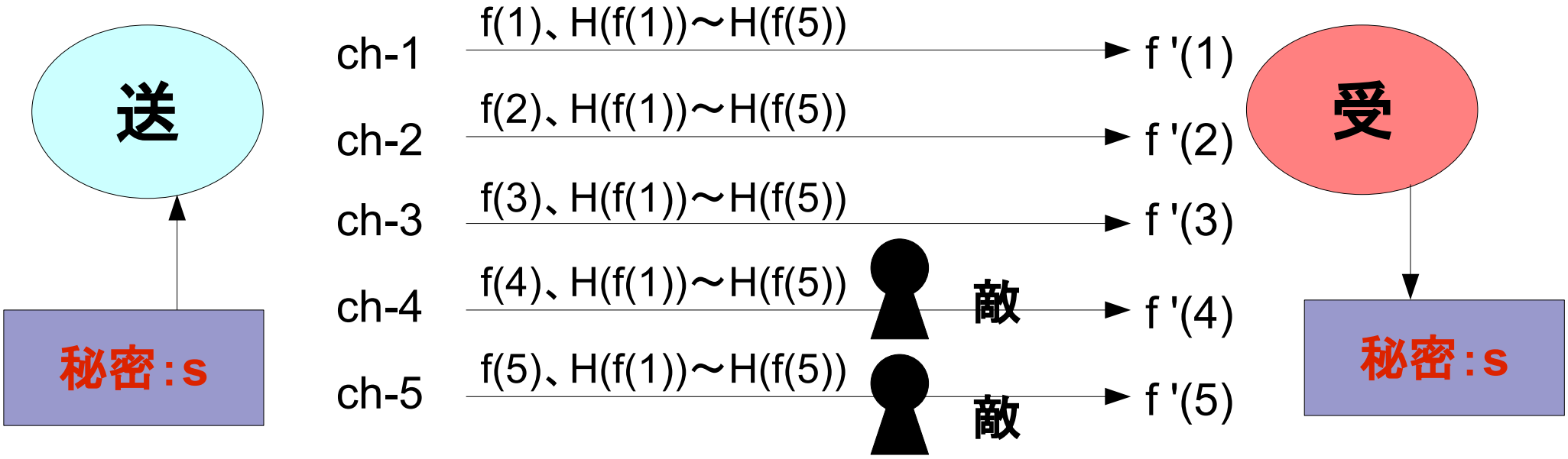
**送信者**

・$f(x)=s+a_1x+a_2x^2+\cdots+a_tx^t$ modP をランダムに作る。

・ハッシュ値H(f(1))～H(f(n))を計算する。

・各ch-iにf(i)、H(f(1))～H(f(n))を送る。

# 提案するASMT（Basic プロトコル）



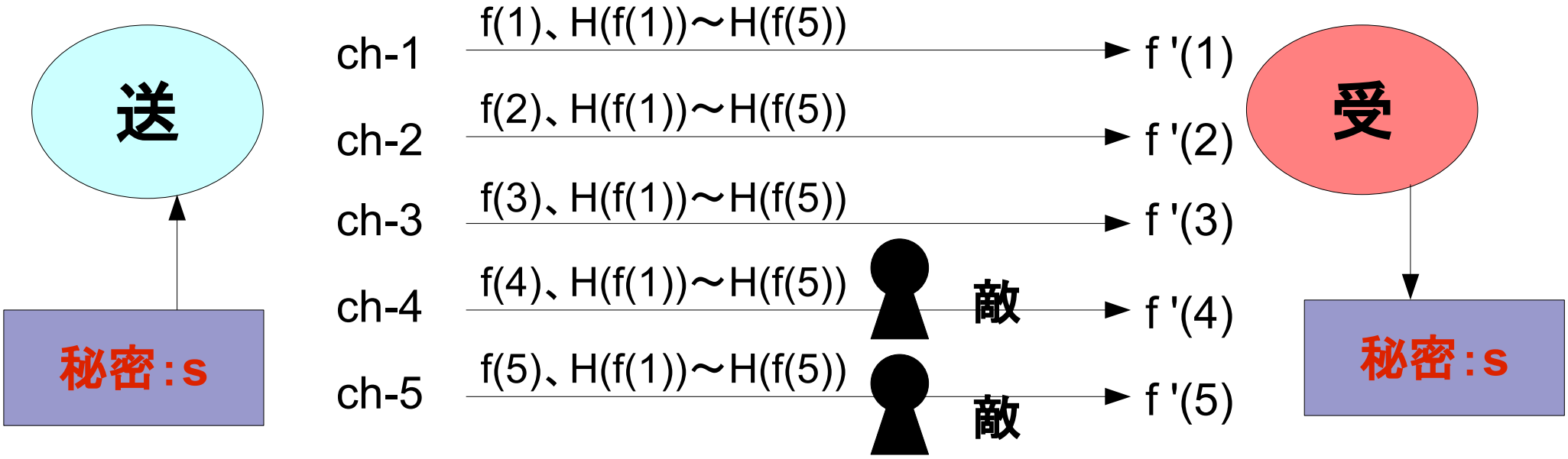

n=2t+1（n：通信路の数　t：敵の数）

**敵**

- f(1)～f(n)のうち、t個しか知らない。
  →f(x)はt次関数なのでt点からはsについて何も分からない。（Privacy）

- ここでハッシュ関数Hは一方向性があると仮定するのでH(f(x))からf(x)を逆算できない。
  →ハッシュ値からはsについて何も分からない。

# 提案するASMT（Basic プロトコル）




n=2t+1（n：通信路の数　t：敵の数）

**受信者**

・f '(1)～f '(n)を得る。

・多数決で正しいH(f(1))～H(f(n))を得る。

・H(f '(1))～H(f '(n))を計算し、H(f(1))～H(f(n))と等しいか調べる。

・H(f(i))=H(f '(i))となるf(i)はt+1個以上ある。
　→f(x)を復元し、sを得られる。

# Basicプロトコルの計算量・通信量

・計算量は多項式時間である。

・通信量

s、f(i)のビット数をq、ハッシュ関数のビット数をhとすると

$$q+\underline{hn}=\log_2|X_i|\geqq\underline{h}+q-\log_2 t$$

差が大きい

⇒ まだ通信効率の限界に近いとは言えない。

# 改良プロトコル

## 特徴

・1度にm個の秘密$s_i$を送信する。

## 送信者

・$f_1(x)$～$f_m(x)$をランダムに作る。

（$f_i(x)=s_i+a_{i1}x+a_{i2}x^2+\cdots+a_{it}x^t$）

・$\mathbf{F}_1=f_1(1)||f_2(1)||f_3(1)||\cdots||f_m(1)$

$\mathbf{F}_2=f_1(2)||f_2(2)||f_3(2)||\cdots||f_m(2)$

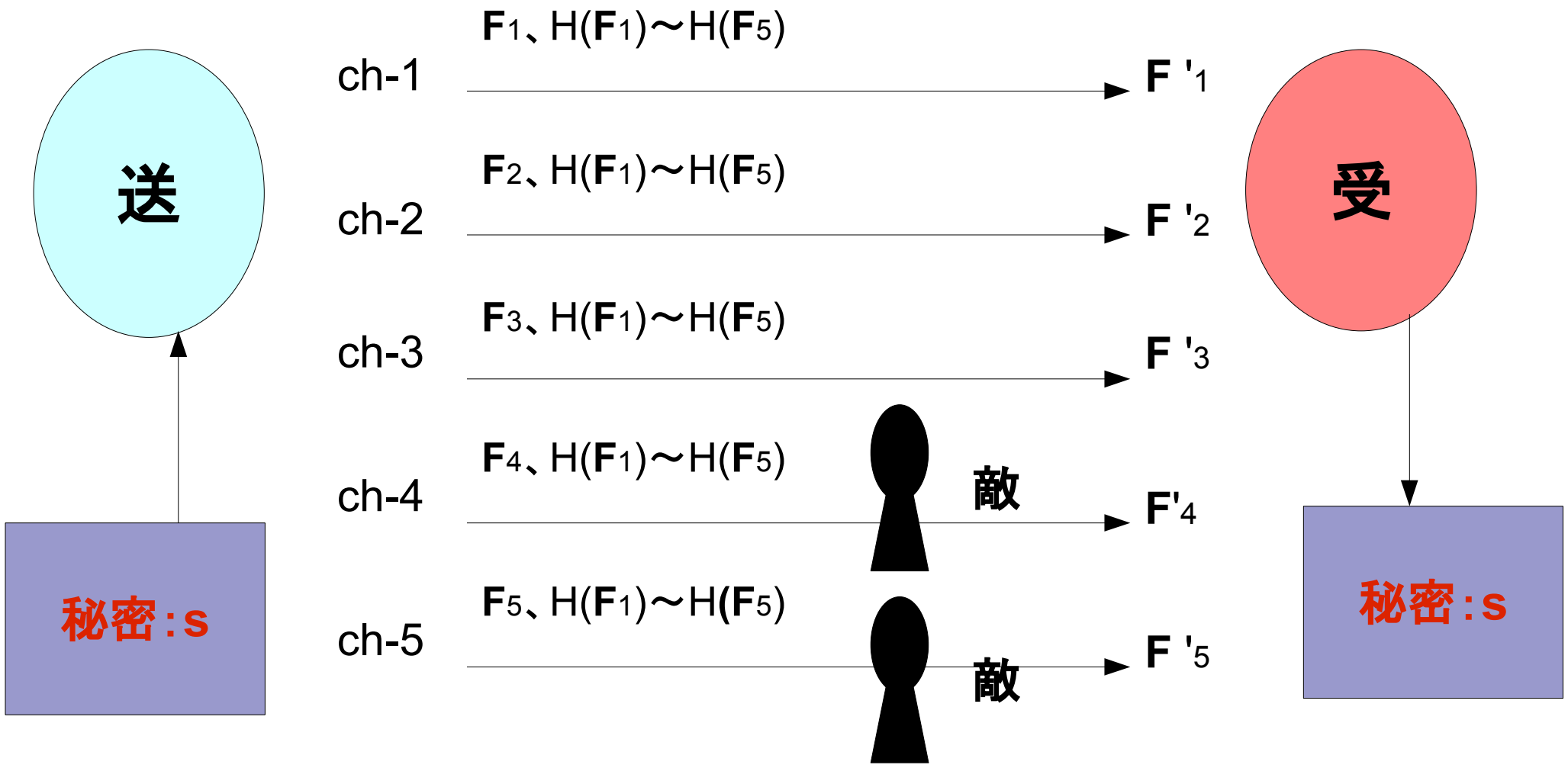
:

$\mathbf{F}_n=f_1(n)||f_2(n)||f_3(n)||\cdots||f_m(n)$　とおく。

・ハッシュ値$H(\mathbf{F}_1)$～$H(\mathbf{F}_n)$を計算する。

・各チャンネルch-iに$\mathbf{F}_i$、$H(\mathbf{F}_1)$～$H(\mathbf{F}_n)$を送る。

# 改良プロトコル




n=2t+1（n:通信路の数　t:敵の数）

# 改良プロトコル

**敵**

- $\mathbf{F}_1$～$\mathbf{F}_n$のうち、t個しか知らない。
  →$\mathbf{F}_i$中の$f_i(x)$はt次関数なのでt点からは$s_i$について何も分からない。
- ここでハッシュ関数Hは一方向性があると仮定するので
  $H(\mathbf{F}_i)$から$\mathbf{F}_i$を逆算できない。
  →ハッシュ値からは$s_i$について何も分からない。

**受信者**

- $\mathbf{F}'_1$～$\mathbf{F}'_n$を得る。
- 多数決で正しい$H(\mathbf{F}_1)$～$H(\mathbf{F}_n)$を得る。
- $H(\mathbf{F}'_1)$～$H(\mathbf{F}'_n)$を計算し、$H(\mathbf{F}_1)$～$H(\mathbf{F}_n)$と等しいか調べる。
- $H(\mathbf{F}_i)=H(\mathbf{F}'_i)$となる$\mathbf{F}_i$はt+1個以上である。
  →$f_i(x)$を復元し、$s_i$を得られる。

# 改良プロトコルの計算量・通信量

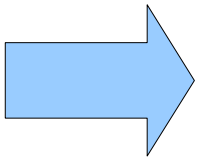
・計算量は多項式時間である。

・通信量

1度にm個の秘密$s_i$を送るので、秘密全体のビット数と、$\mathbf{F}_i(i)$のビット数はqmとなる。ハッシュ関数のビット数はhのままである。

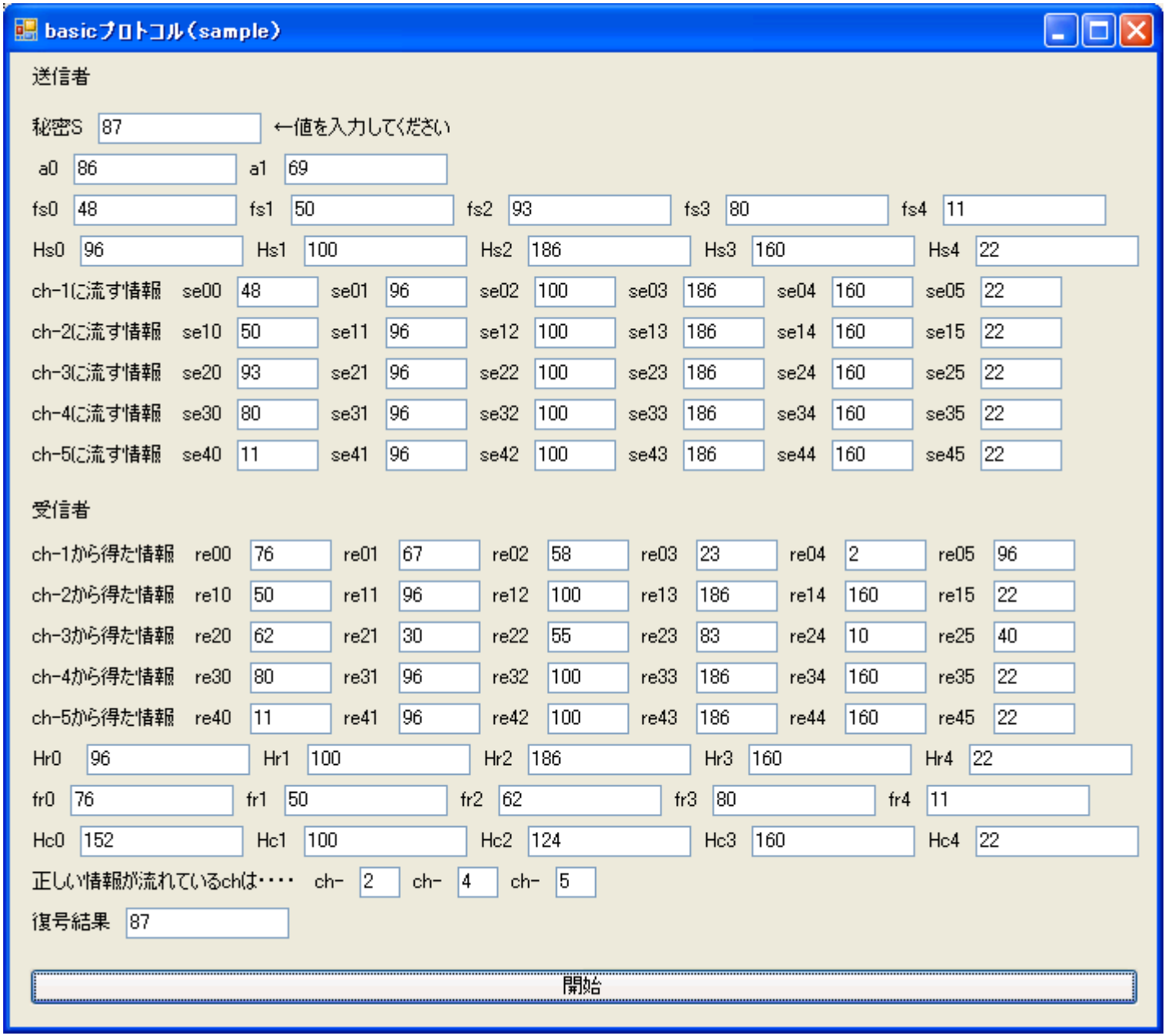
ここでq=h、m=n、nを十分に大きい値とすると、

$$O(hn)=O(\log_2|X_i|)\geqq\Omega(hn)$$



通信効率の限界に近い。

# Basicプロトコルのプログラム実装



# 結論

- Basicプロトコルを用いることによって計算量を多項式時間にすることができたが、通信量があまりよくない。
- Basicプロトコルを改良することで通信効率の限界に近い通信量に改善できた。
- Basicプロトコルをプログラム実装した結果、正しく動作することが検証できた。