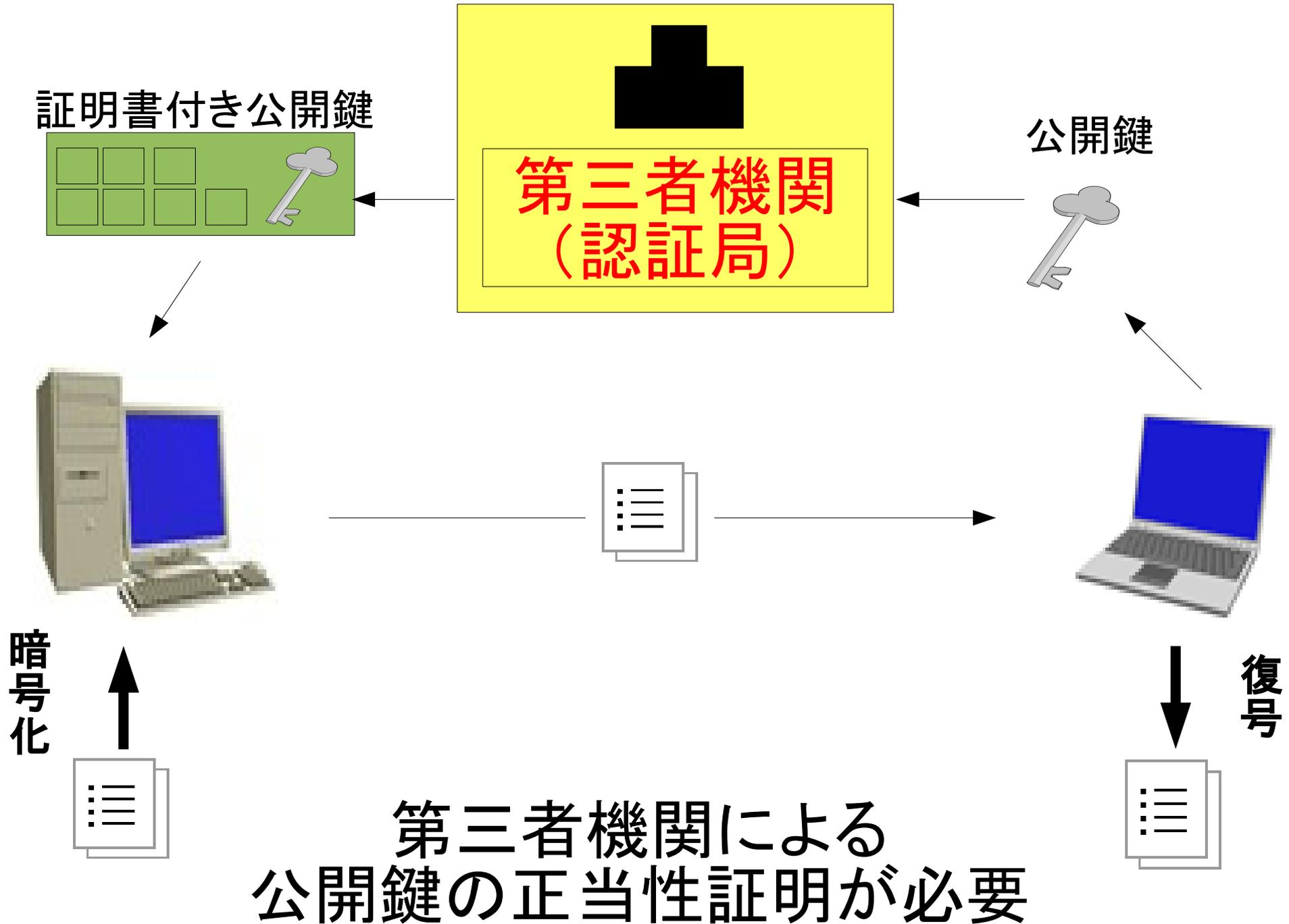


nチャンネルメッセージ伝送方式 による暗号化通信

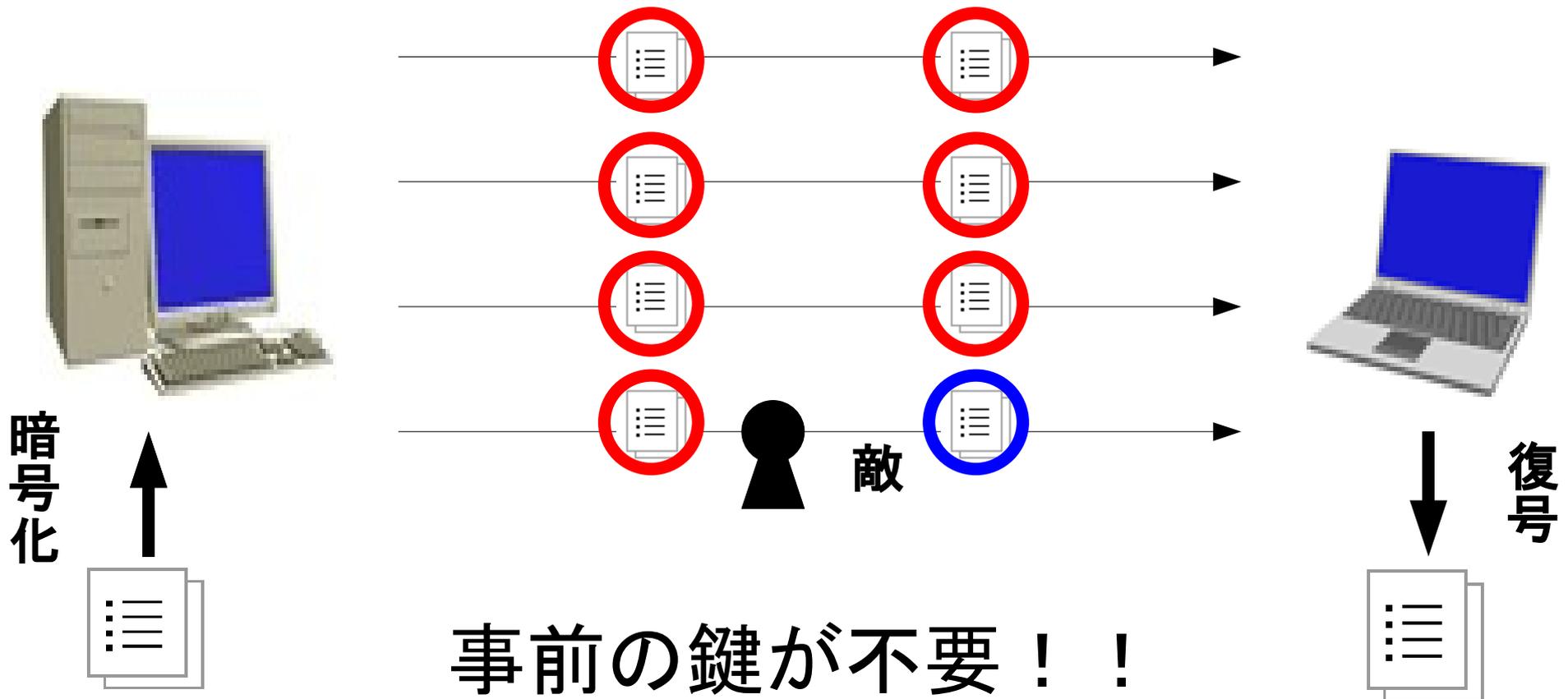
木下研究室 200402931 渡邊優司

従来の暗号方式～公開鍵暗号～



nチャン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。

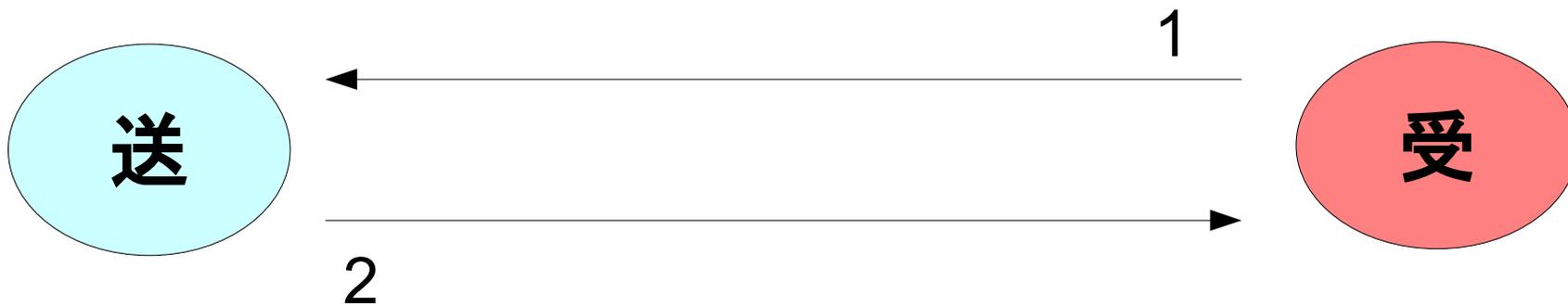
PSMTの歴史

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

1-round



2-round



PSMTの歴史

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

敵が本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

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

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 $|X_i|$ は

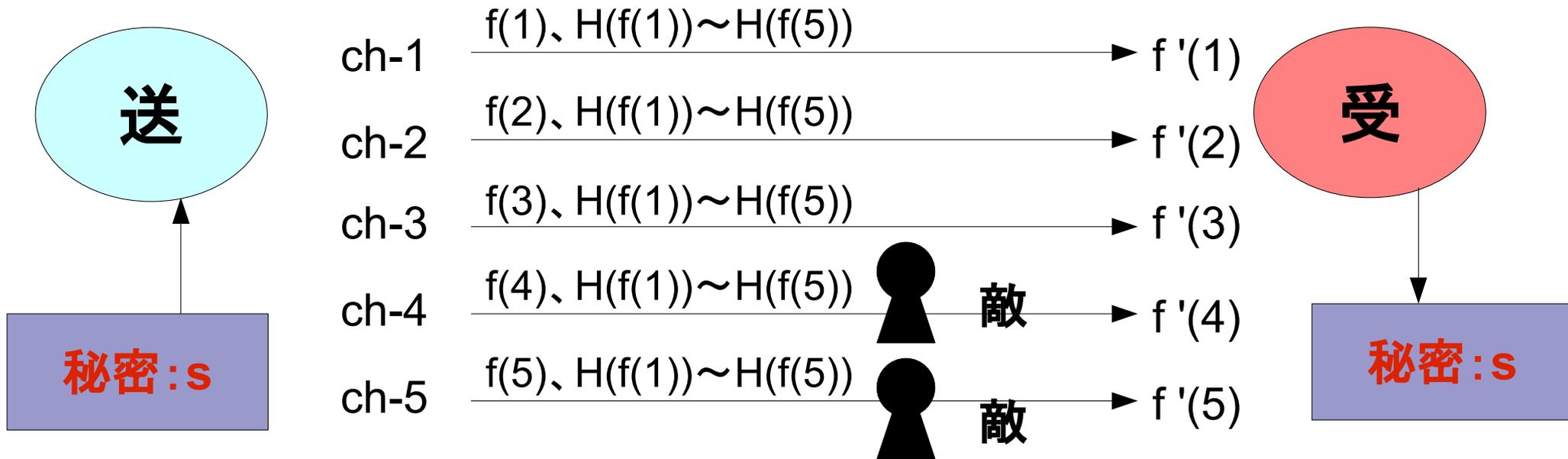
$$|X_i| = \frac{|S|-1}{\delta} + 1 > \frac{|S|-1}{\varepsilon} + 1$$

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)

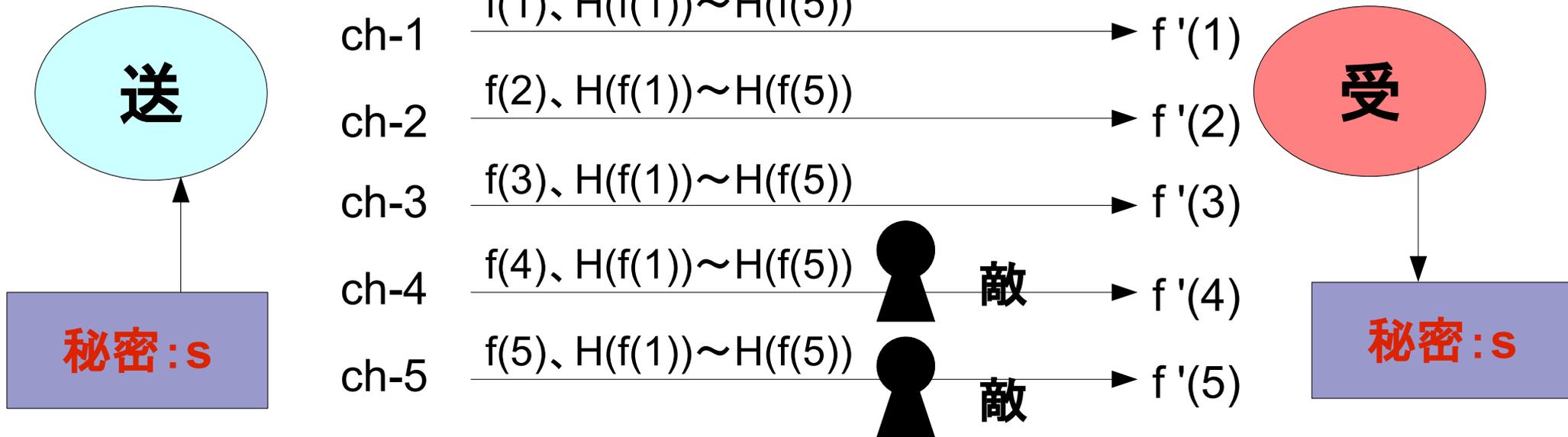


$$n=2t+1 \text{ (} n: \text{通信路の数 } t: \text{敵の数)}$$

送信者

- $f(x) = s + a_1x + a_2x^2 + \dots + a_tx^t \pmod{P}$ をランダムに作る。
- ハッシュ値 $H(f(1)) \sim H(f(n))$ を計算する。
- 各 ch- i に $f(i)$ 、 $H(f(1)) \sim H(f(n))$ を送る。

提案するASMT (Basic プロトコル)

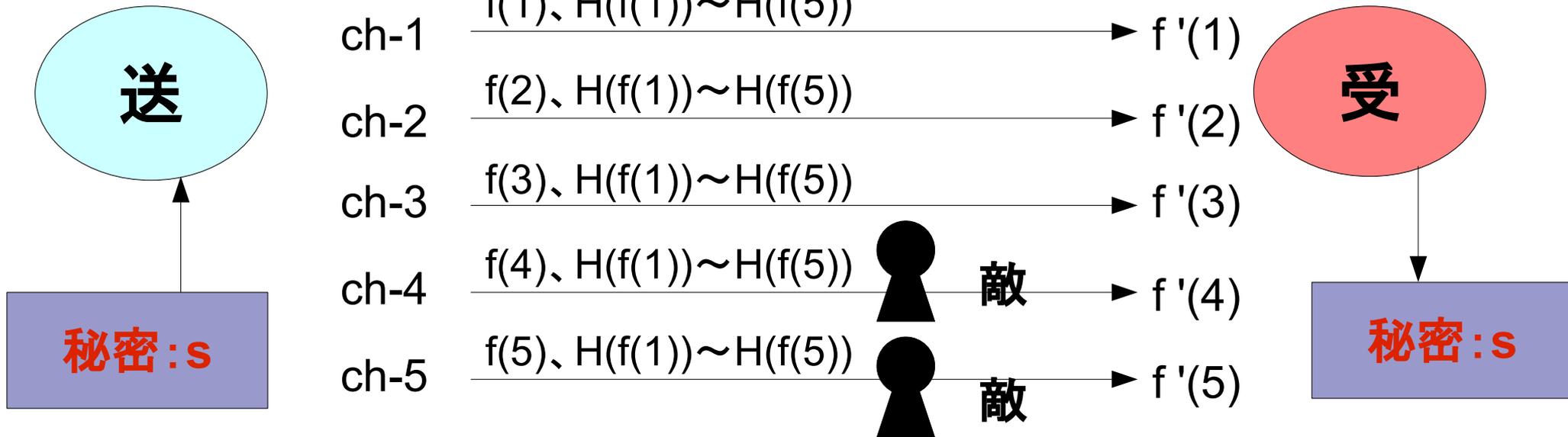


$$n=2t+1 \text{ (} n: \text{通信路の数 } t: \text{敵の数)}$$

敵

- ・ $f(1) \sim f(n)$ 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)



$$n=2t+1 \text{ (} n: \text{通信路の数 } t: \text{敵の数)}$$

受信者

- ・ $f'(1) \sim f'(n)$ を得る。
- ・ 多数決で正しい $H(f(1)) \sim H(f(n))$ を得る。
- ・ $H(f'(1)) \sim H(f'(n))$ を計算し、 $H(f(1)) \sim H(f(n))$ 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

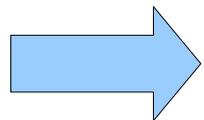
- ・計算量は多項式時間である。

- ・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

$$q + \frac{hn}{t} = \log_2 |X_i| \geq \frac{h}{t} + q - \log_2 t$$

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

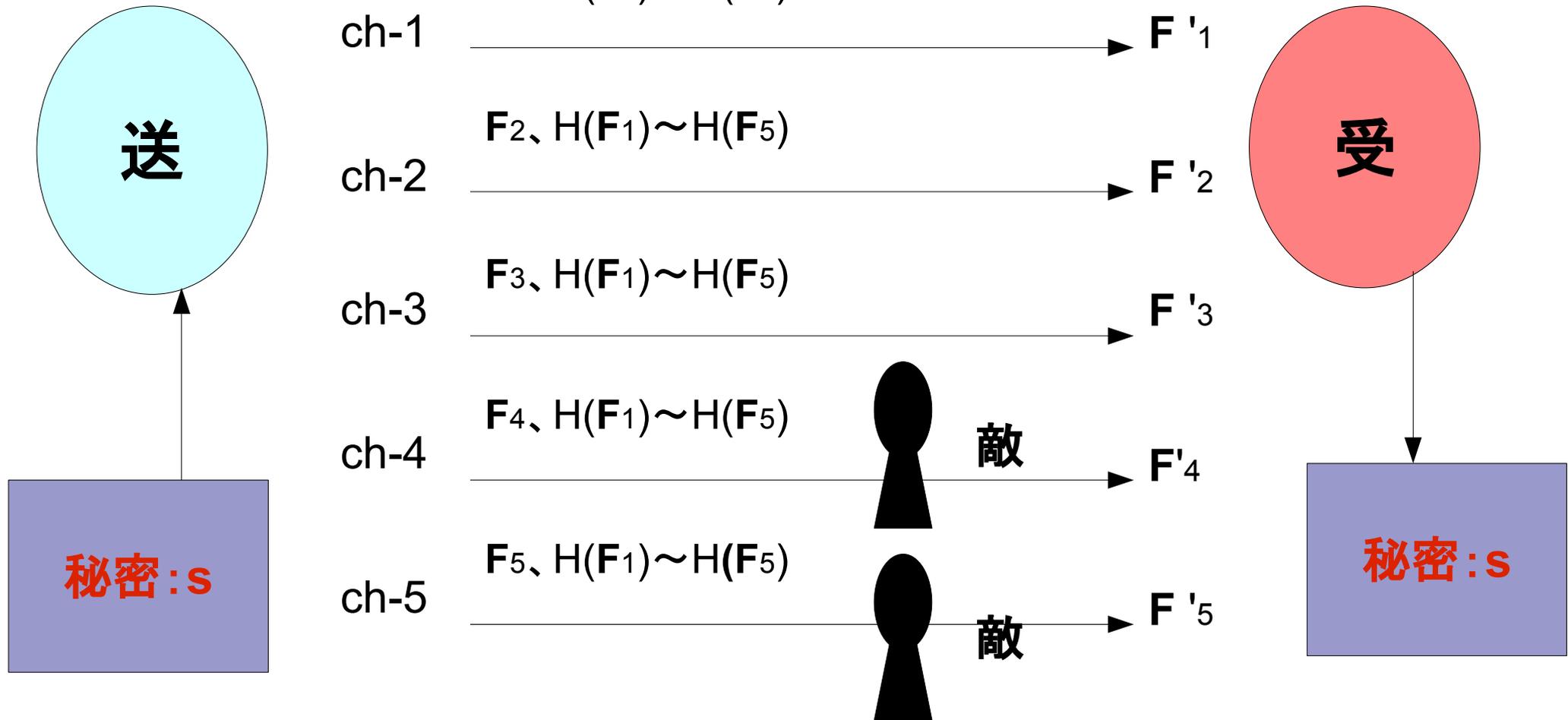
特徴

- ・1度にm個の秘密 s_i を送信する。

送信者

- ・ $f_1(x) \sim f_m(x)$ をランダムに作る。
($f_i(x) = s_i + a_{i1}x + a_{i2}x^2 + \dots + a_{it}x^t$)
- ・ $\mathbf{F}_1 = f_1(1) || f_2(1) || f_3(1) || \dots || f_m(1)$
 $\mathbf{F}_2 = f_1(2) || f_2(2) || f_3(2) || \dots || f_m(2)$
:
 $\mathbf{F}_n = f_1(n) || f_2(n) || f_3(n) || \dots || f_m(n)$ とおく。
- ・ハッシュ値 $H(\mathbf{F}_1) \sim H(\mathbf{F}_n)$ を計算する。
- ・各チャンネルch-iに \mathbf{F}_i 、 $H(\mathbf{F}_1) \sim H(\mathbf{F}_n)$ を送る。

改良プロトコル



$$n=2t+1 \text{ (} n: \text{通信路の数 } t: \text{敵の数)}$$

改良プロトコル

敵

- ・ $F_1 \sim F_n$ のうち、 t 個しか知らない。
 - 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 $H(F_i)$ から 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

- ・ $F'_1 \sim F'_n$ を得る。
- ・多数決で正しい $H(F_1) \sim H(F_n)$ を得る。
- ・ $H(F'_1) \sim H(F'_n)$ を計算し、 $H(F_1) \sim H(F_n)$ 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

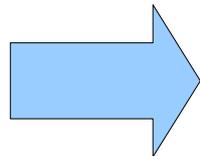
- ・計算量は多項式時間である。

- ・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、 $F_i(i)$ 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、

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



通信効率の限界に近い。

Basicプロトコルのプログラム実装

basicプロトコル(sample)

送信者

秘密S ←値を入力してください

a0 a1

fs0 fs1 fs2 fs3 fs4

Hs0 Hs1 Hs2 Hs3 Hs4

ch-1に流す情報 se00 se01 se02 se03 se04 se05

ch-2に流す情報 se10 se11 se12 se13 se14 se15

ch-3に流す情報 se20 se21 se22 se23 se24 se25

ch-4に流す情報 se30 se31 se32 se33 se34 se35

ch-5に流す情報 se40 se41 se42 se43 se44 se45

受信者

ch-1から得た情報 re00 re01 re02 re03 re04 re05

ch-2から得た情報 re10 re11 re12 re13 re14 re15

ch-3から得た情報 re20 re21 re22 re23 re24 re25

ch-4から得た情報 re30 re31 re32 re33 re34 re35

ch-5から得た情報 re40 re41 re42 re43 re44 re45

Hr0 Hr1 Hr2 Hr3 Hr4

fr0 fr1 fr2 fr3 fr4

Hc0 Hc1 Hc2 Hc3 Hc4

正しい情報が流れているchは…… ch- ch- ch-

復号結果

開始

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。