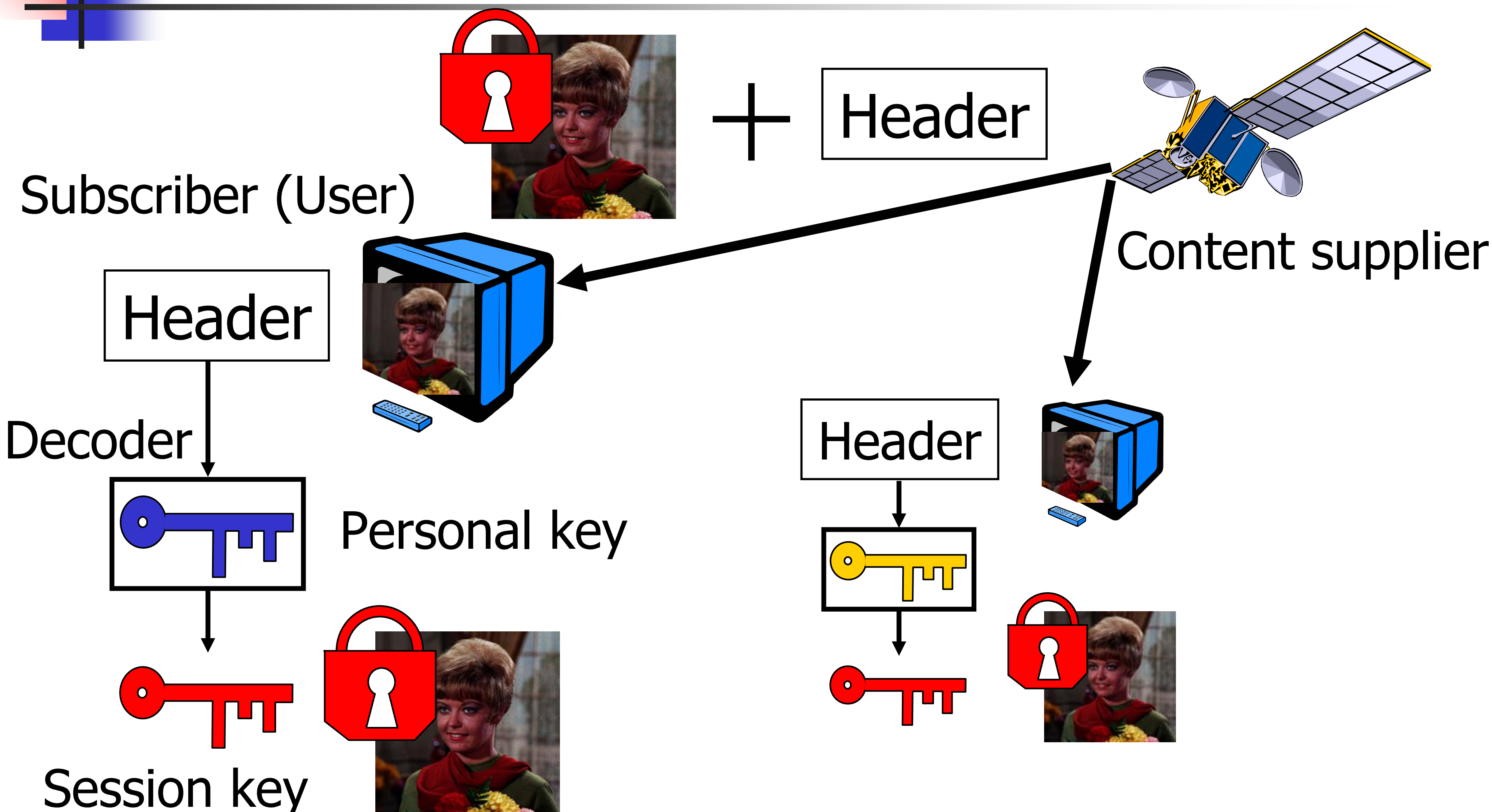
A Public-Key Black-Box Traitor Tracing Scheme with Sublinear Ciphertext Size against Self-Defensive Pirates

T. Matsushita[1,2] and H. Imai[2]

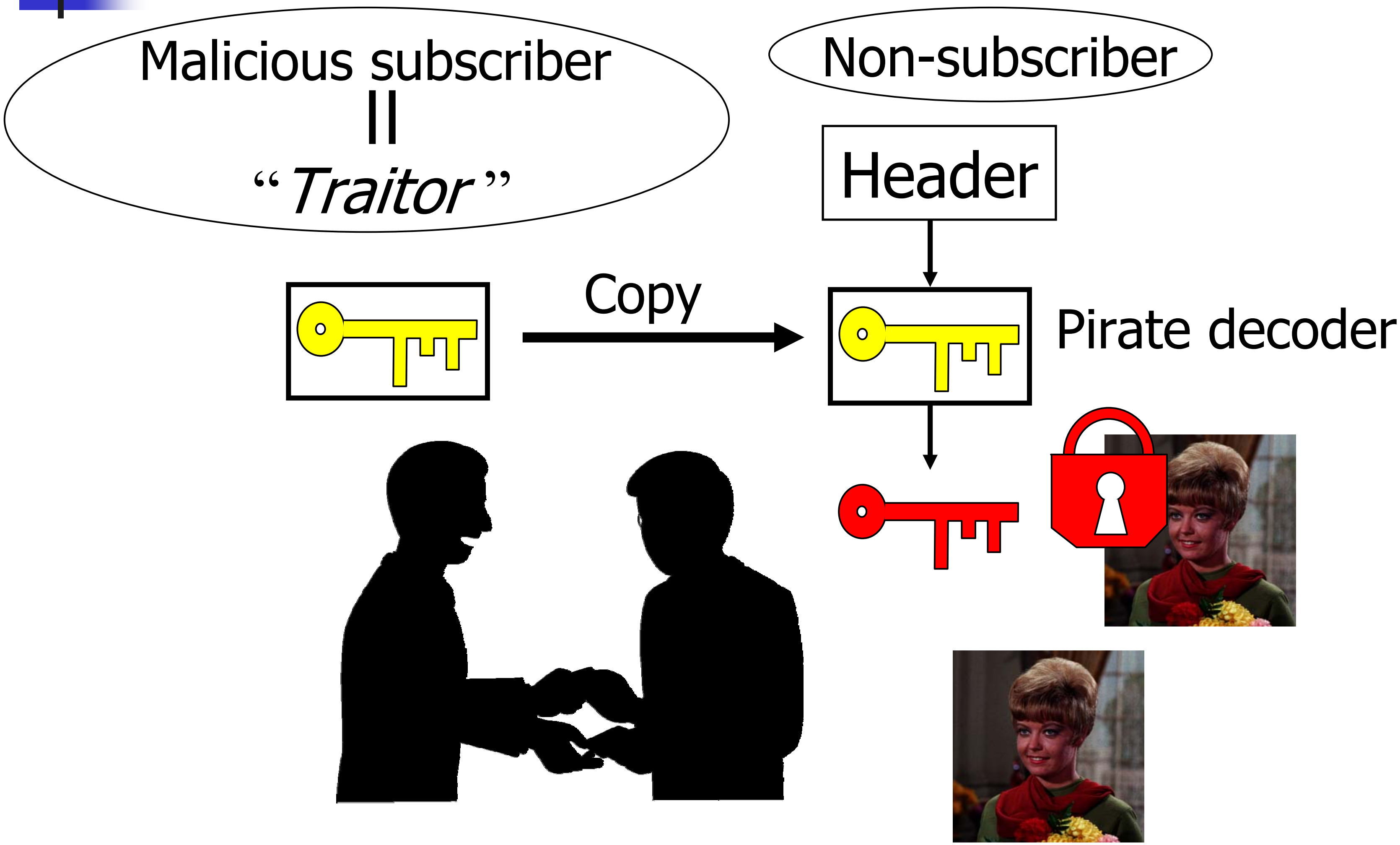
[1]TOSHIBA Corporation

[2]University of Tokyo

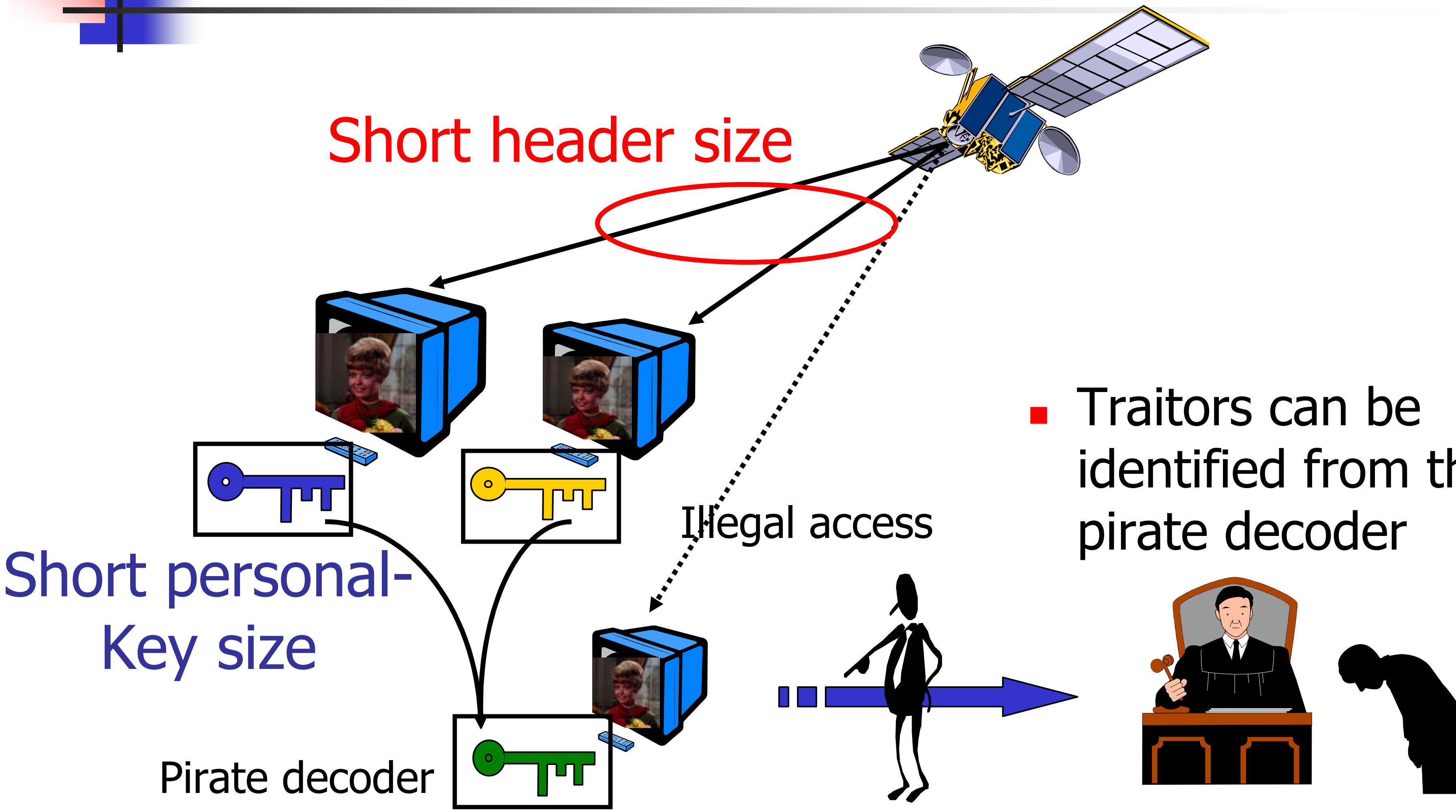
Content distribution system



Piracy

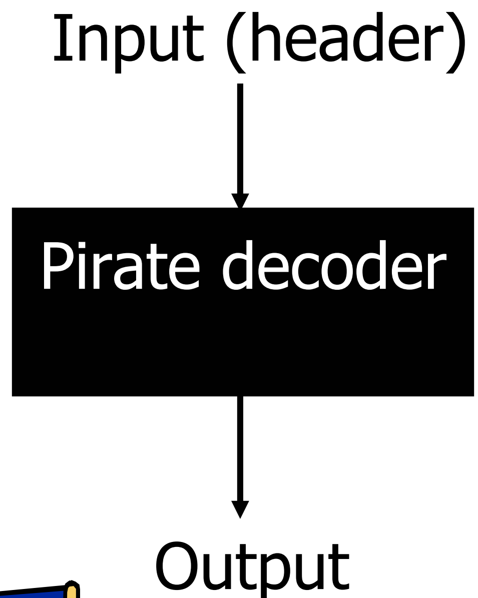

Malicious subscriber
||
"Traitor"
Non-subscriber
Header
Copy
Pirate decoder

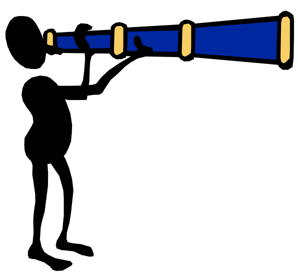
A deterrent to the piracy: Traitor tracing



- Traitors can be identified from the pirate decoder

Black-box tracing





- Traitors can be identified from the pirate decoder used as a black box
- The tracer chooses a set of suspects and inputs the header which can (or cannot) be decrypted by the selected suspects
- A scheme in which header size is linear in the total number of users is trivial

Assumptions on the pirate decoder

- Assumption 1
  - The pirate decoder can take measures that might escape from tracing if it detects tracing
  - E.g., it will take self-defensive reactions:
    - erasing all of the internal keys and shutting down
- Assumption 2
  - The tracer can reset the pirate decoder to its initial state each time the tracer gives the input to it
    - We do not consider the pirate decoder that records the previous inputs

k: max. coalition size

Previous public-key schemes (1/2)

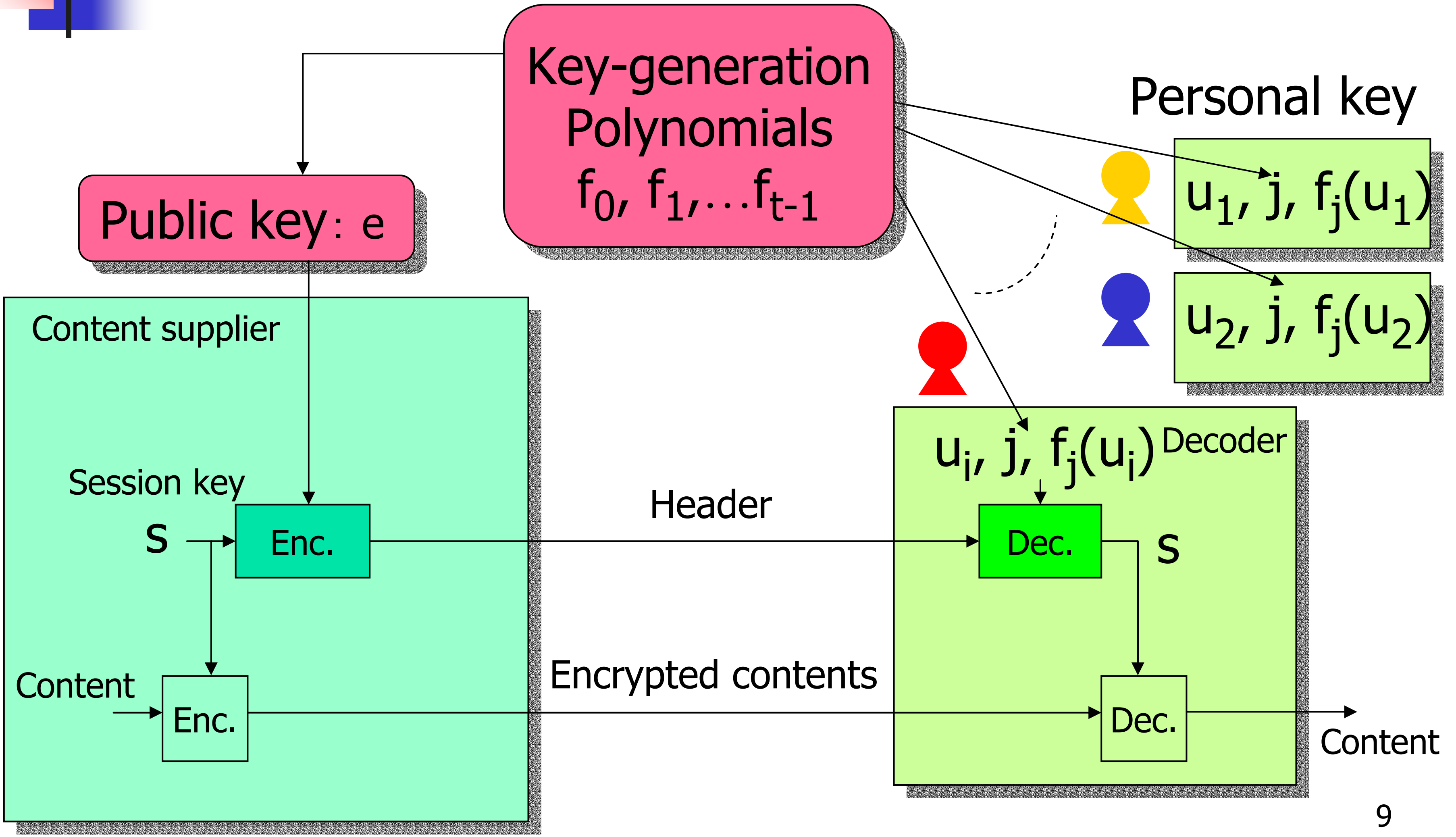
- [BF99], [Kurosawa-Yoshida02]
  - Only black-box confirmation is supported, i.e., it is assumed that suspects can be narrowed down to k users in advance
- [Kiayias-Yung01]
  - The scheme supports black-box list-tracing in which the tracing algorithm outputs a suspect list
  - There is a trade-off between header size and detection probability
- Proposed scheme
  - The above assumption is unnecessary
  - The tracing algorithm can identify at least one traitor with overwhelming probability

Previous public-key schemes (2/2)

	Personal-key size	Header size	Type of tracing	Detection probability
[BF99], [Kurosawa-Yoshida02]	O(1)	O(k)	Black-box confirmation	Overwhelm-ing
[Kiayias-Yung01]	O(1)	$O(\sqrt{n})$	Black-box list-tracing	Trade-off with header size
Ours	O(1)	$O(\sqrt{n})$	Black-box tracing	Overwhelm-ing

k: max. coalition size, n: total # of users

Overview of the proposed scheme



p,q: primes s.t. q|p-1, q≧n+2k-1
g: q-th root of unity over Zp*

k: max. coalition size
n: total # of users
U: a set of users

Proposed scheme (key generation)

- The method of [Mat02]: Split U into t disjoint subsets and assign a distinct key-generation polynomial to each subset

U

$$U_0 : f_0(x) = b_0 + a_1 x + a_2 x^2 + \cdots + a_{2k-1} x^{2k-1} \bmod q$$

$$U_1 : f_1(x) = a_0 + b_1 x + a_2 x^2 + \cdots + a_{2k-1} x^{2k-1} \bmod q$$

$$\vdots \qquad \vdots$$

$$U_i : f_i(x) = a_0 + a_1 x + \cdots + b_i x^i + \cdots + a_{2k-1} x^{2k-1} \bmod q$$

$$\vdots \qquad \vdots$$

Personal key for user i $(i, j, f_j(i)) \quad (i \in U_j)$

Public key $(g, g^{a_0}, \ldots, g^{a_{2k-1}}, g^{b_0}, \ldots, g^{b_{t-1}})$

p,q: primes s.t. $q|p-1$, $q \geqq n+2k-1$
g: q-th root of unity over Zp*
s: session key
R_0,R_1: random numbers

Proposed scheme (encryption)

- Based on [Kurosawa-Yoshida02]
- Choose r_j from $\{R_0,R_1\}$ and compute H_j for subgroup U_j

$$H_j = (h_j, h_{j,0}, h_{j,1}, \ldots, h_{j,j}, \ldots, h_{j,2k-1})$$

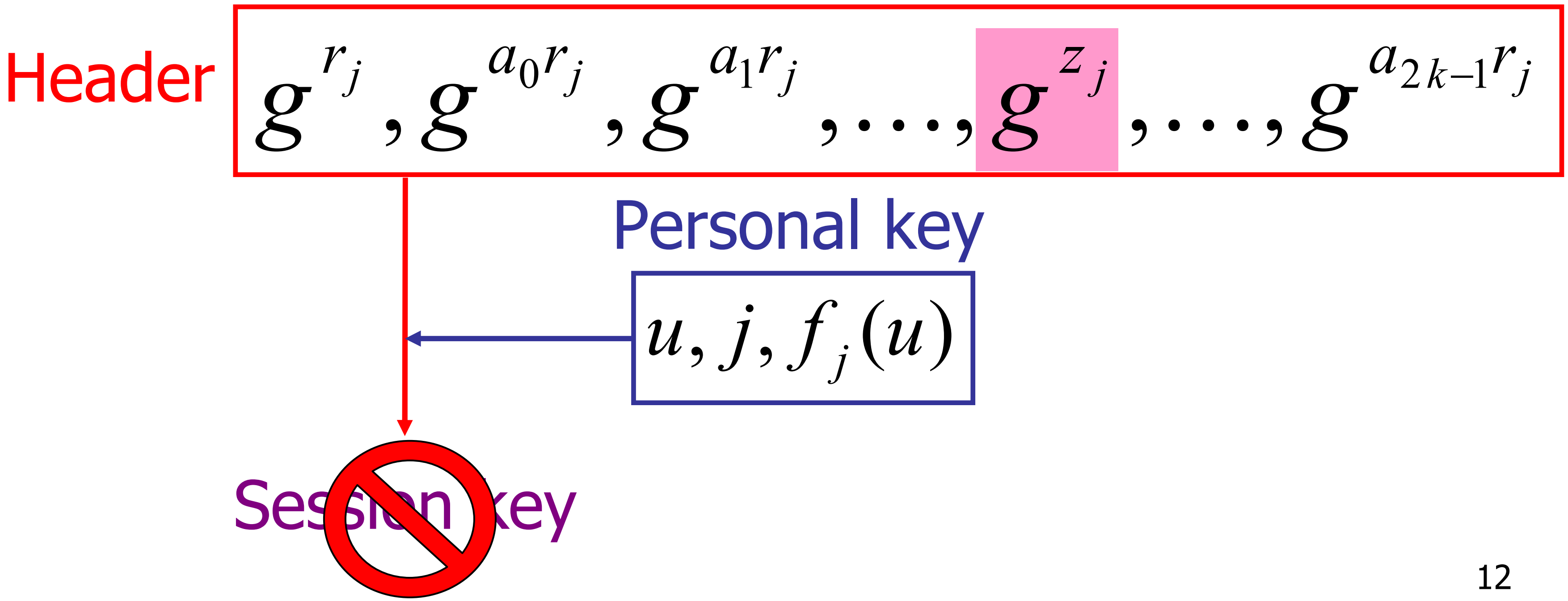
$$= (g^{r_j}, g^{a_0 r_j}, g^{a_1 r_j}, \ldots, sg^{b_j r_j}, \ldots, g^{a_{2k-1} r_j})$$

Element used only by the users in U_j

- Header: $H=\{H_0,\ldots,H_{t-1}\}$

Bulk revocation

- All of the users in U_j can be revoked by substituting a random element for the element used only by them
- This helps to extend black-box confirmation in [Kurosawa-Yoshida02] to black-box tracing with sublinear header size



Individual revocation

- Users in U_j can be revoked when $\sum_{i=0}^{2k-1} c_i u_\alpha^i \neq 0 \bmod q$

Header

$$g^{r_j}, g^{c_0} g^{a_0 r_j}, g^{c_1} g^{a_1 r_j}, \ldots, s g^{c_j} g^{b_j r_j}, \ldots, g^{c_{2k-1}} g^{a_{2k-1} r_j}$$

Personal key

$$u_\alpha, j, f_j(u_\alpha)$$

Session key

Proposed scheme (decryption)

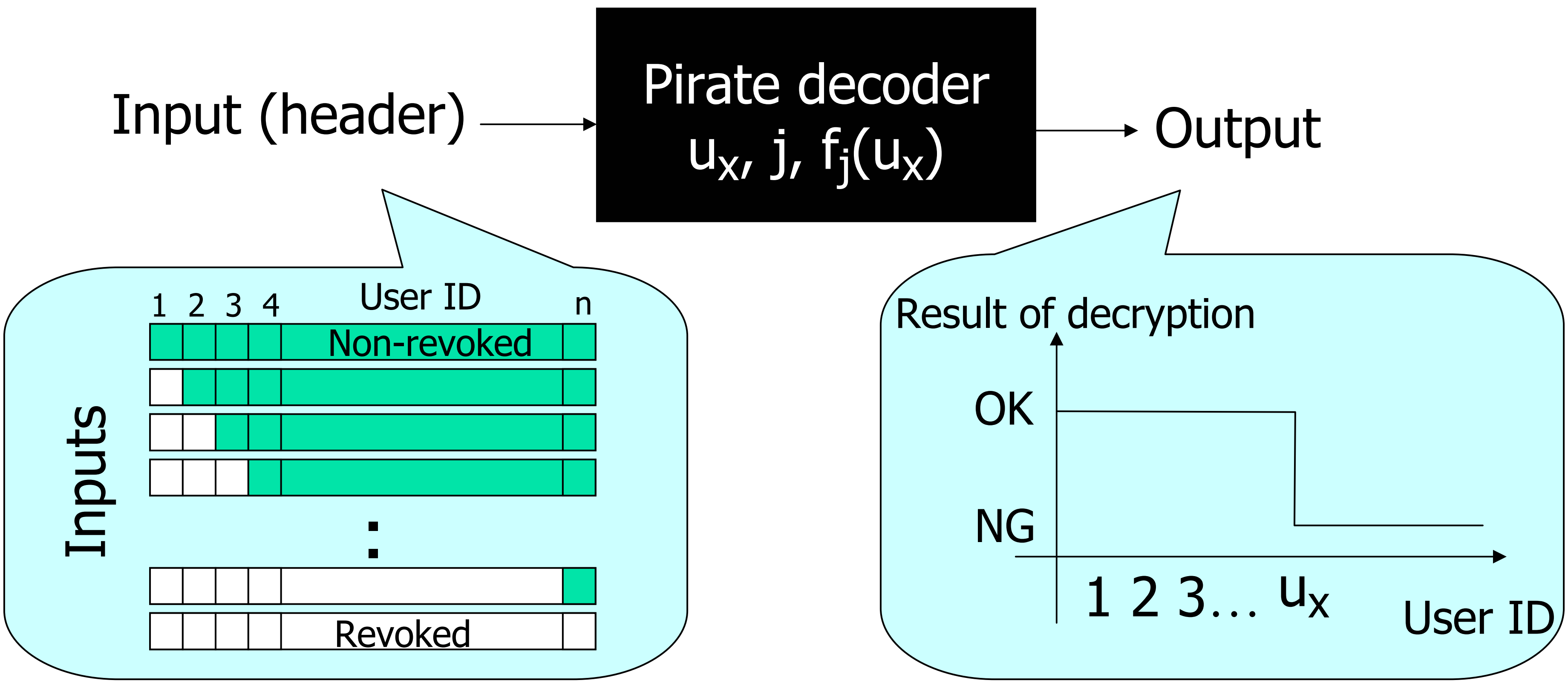
- User u ($u \in U_j$) computes the session key s from H_j

$$H_j = (h_j, h_{j,0}, h_{j,1}, \ldots, h_{j,j}, \ldots, h_{j,2k-1})$$

$$s = \left(\frac{h_{j,0} \times h_{j,1}^{u} \times \cdots \times h_{j,2k-1}^{u^{2k-1}}}{h_j^{f_j(u)}} \right)^{1/u^j}$$

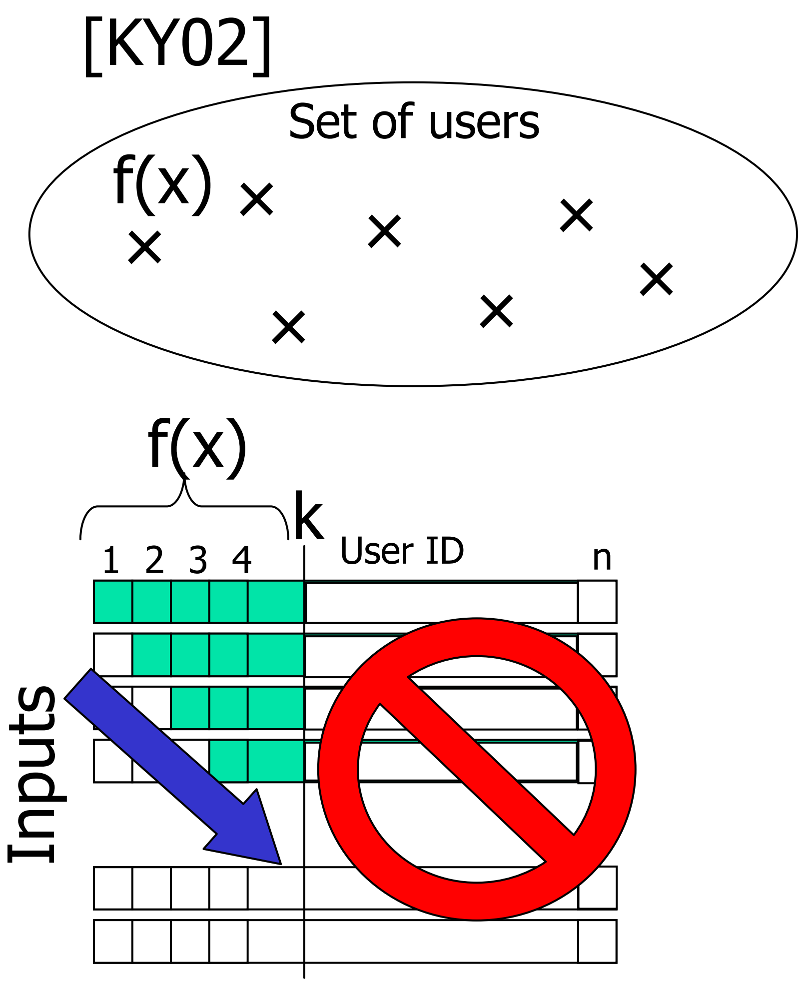
Proposed scheme (tracing)

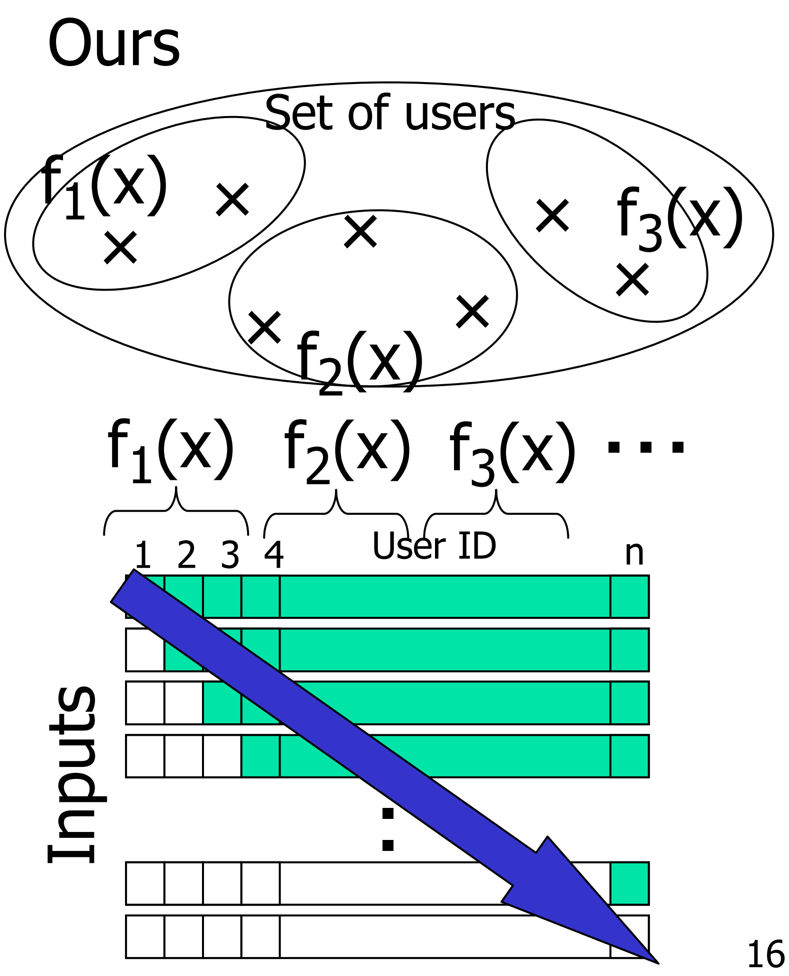
- The users are examined one-by-one in each input



k: max. coalition size, n: total # of users

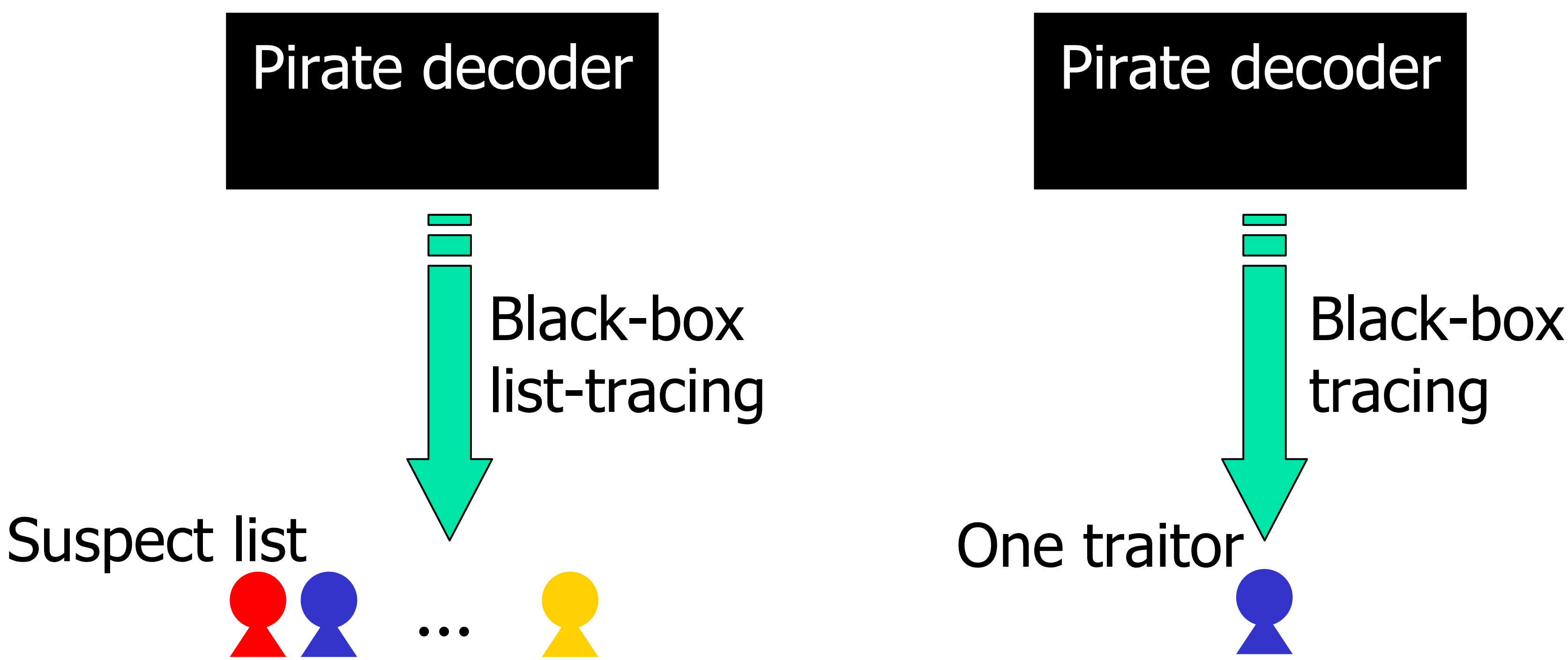
Difference between [Kurosawa-Yoshida02] and ours





Difference between [Kiayias-Yung01] and ours

[KY01] | Ours



The probability that the tracer detects a traitor correctly is in inverse proportion to the size of the suspect list

Security

- Based on the difficulty of DDH problem
- Secrecy of the session key against eavesdroppers
- Black-box traceability
  - From the pirate decoder constructed by a coalition of at most k traitors, the tracing algorithm in our scheme can identify at least one of them with overwhelming probability
    - Indistinguishability of an input
    - Secrecy of a session key in an invalid input
    - Indistinguishability of a suspect

n: total # of users, t: # of subsets of users, k: max. coalition size, c: system parameter ($0<c<1$), ε : negligible probability, P,S,H: sets of possible personal keys/session keys/headers

Efficiency

	Personal-key size (log|P|/log|S|)	Header size (log|H|/log|S|)	# of sets of suspects for testing	Detec-tion prob.	# of exp. for decryption
[Kurosawa-Yoshida02]*	1	2k+1	k	$1-\varepsilon$	O(k)
[Kiayias-Yung01]**	$(1-c)^{-1}$	$2(1-c)^{-1}n^{1-c}$	n^{1-c}	n^{-c}	$O((1-c)^{-1})$
Ours (t= n/2k)	1	4k+n/2k+2	n	$1-\varepsilon$	O(k)

*It is assumed that suspects can be narrowed down to k users in advance

**ElGamal cryptosystem is straightforwardly applied

Efficiency - an example -

	Personal-key size (log|P|/log|S|)	Header size (log|H|/log|S|)	# of sets of suspects for testing	Detec-tion prob.	# of exp. for decryption
[Kiayias-Yung01] (c=1/2)	2	$4\sqrt{n}$	$\sqrt{n}$	$1/\sqrt{n}$	O(1)
Ours (k=(n/8)$^{1/2}$)	1	$2\sqrt{2n}+2$	n	1- ε	$O(\sqrt{n})$

n: total # of users, k: max. coalition size, c: system parameter (0<c<1)
ε : negligible prob., P,S,H: sets of possible personal keys/session keys/headers

Conclusions

- We have proposed a public-key black-box tracing scheme against self-defensive pirate decoders
  - Black-box tracing
    - Against self-defensive pirate decoders
    - With overwhelming detection probability
  - Sublinear ciphertext size
- Future research:
  - Reduction of computational cost for decryption
  - Further reduction of header size

References

[BF99] D. Boneh and M. Franklin, "An Efficient Public Key Traitor Tracing Scheme," CRYPTO '99

[KD98] K. Kurosawa and Y. Desmedt, "Optimum Traitor Tracing and Asymmetric Schemes," EUROCRYPT '98

[Kiayias-Yung01] A. Kiayias and M. Yung, "On Crafty Pirates and Foxy Tracers," SPDRM '01

[Kurosawa-Yoshida02] K. Kurosawa and T. Yoshida, "Linear Code Implies Public-Key Traitor Tracing," PKC '02

[Mat02] T. Matsushita, "A Flexibly Revocable Key-Distribution Scheme for Efficient Black-Box Tracing," ICICS '02