

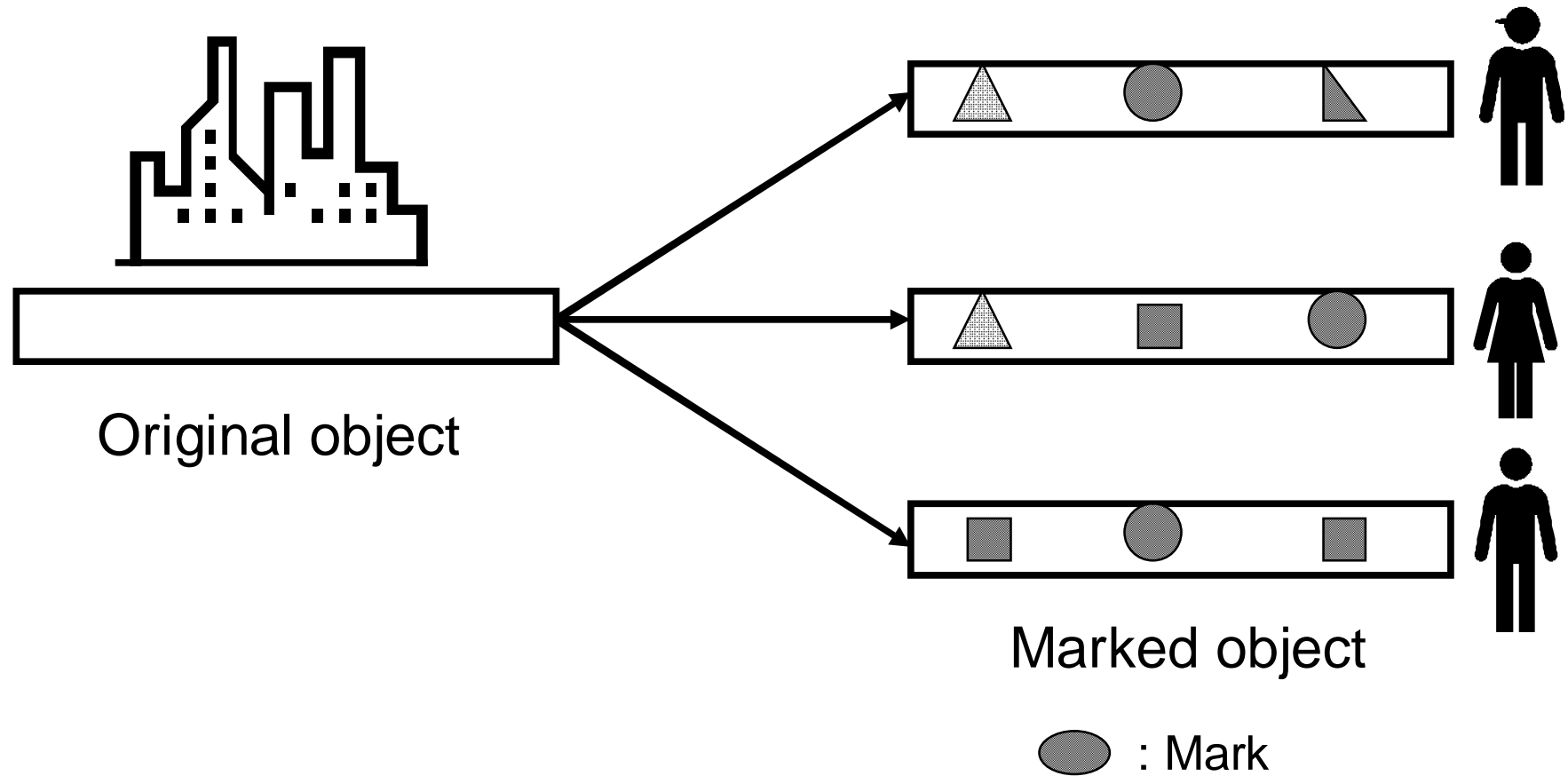
Systematic Treatment of Collusion Secure Codes: Security Definitions and Their Relations

Katsunari Yoshioka, Junji Shikata, and Tsutomu Matsumoto
Yokohama National University, Japan

3rd October, 2003

6th Information Security Conference, Bristol, UK

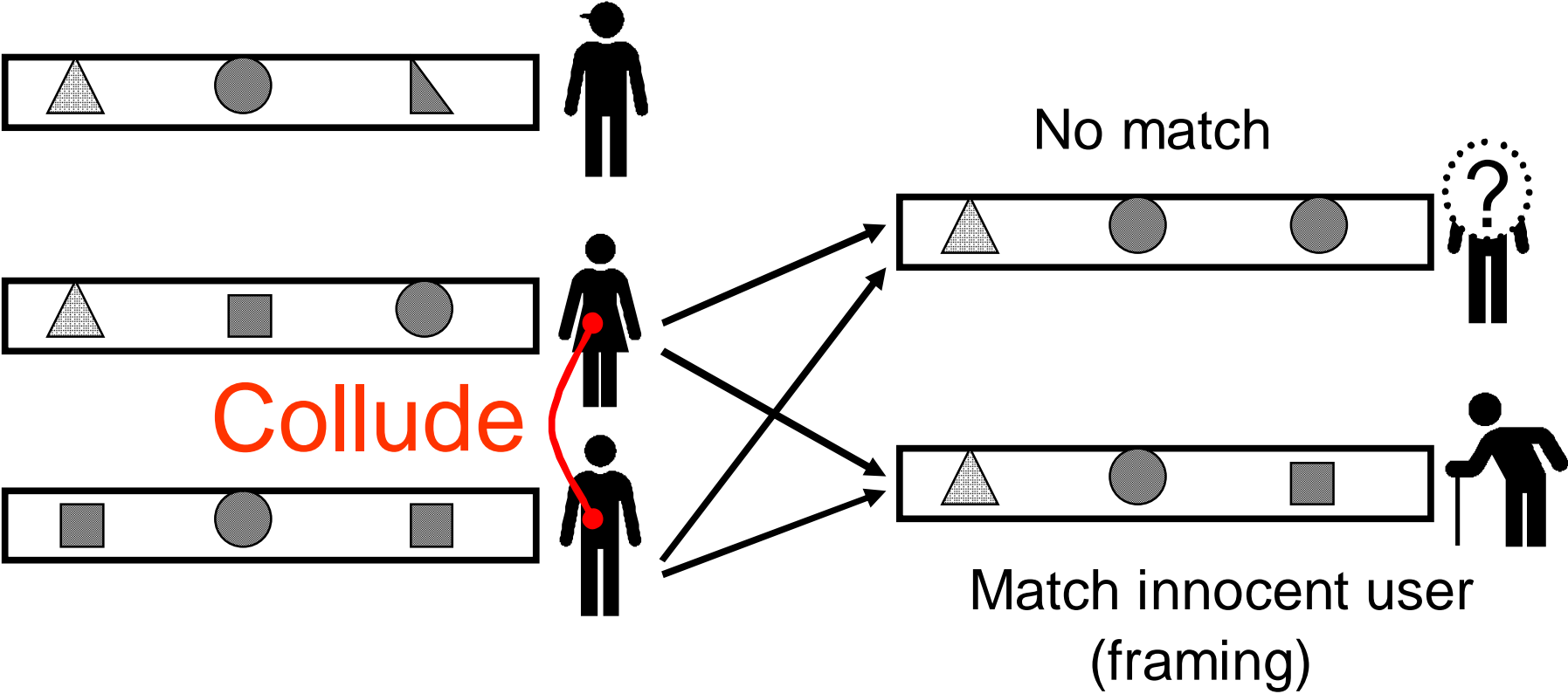
What is fingerprinting?



Examples of object: image, movie, audio, text, program, etc.

Collusion attack

Two or more users collude and then generate an object with other marks.



Related works

- c -frameproof code [Boneh, Shaw 98]
- c -secure frameproof code [Stinson, van Trung, Wei 00]
- c -identifiable parent property code
[Hollmann, Lint, Linnartz, Tolhuizen 98]
- c -traceability code [Char, Fiat, Naor 94]
[Staddon, Stinson, Wei 01]
- totally c -secure code [Boneh, Shaw 98]
- $(c, g/s)$ -secure code [Orihara, Mizuki, Nishizeki 03]

Motivation

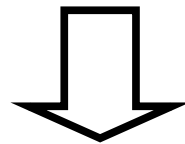
Definitions of attack against the collusion secure codes are not consistent in previous works.



Introduction of more general definitions of collusion secure codes

Our results

- Define various types of attacks (marking assumption) including the ones in the previous works.
- Reveal relationships among codes under the various types of attack.
- Reveal relationships among codes with different collusion secure properties.



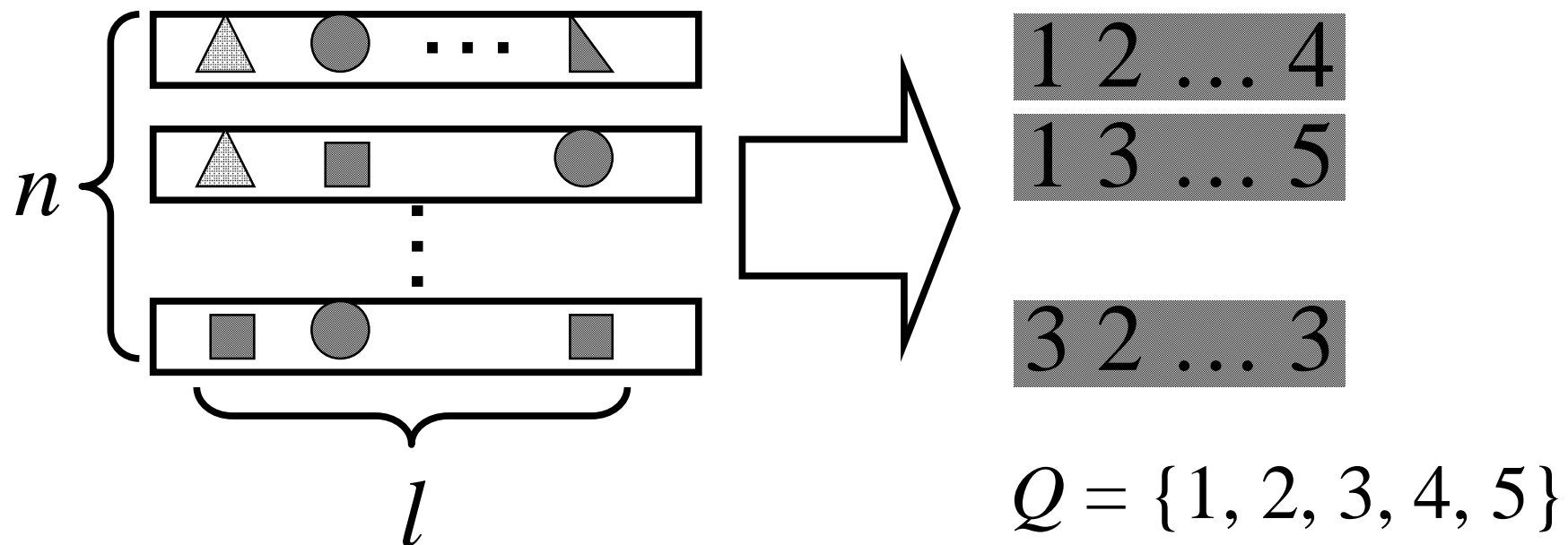
We show new relationships among combined notions of collusion secure properties and marking assumptions.

Overview

- Introduction
- Preliminaries
- Types of attack and codes
- Relationships
- Conclusion

Preliminaries(1/2)

- Let Q be an alphabet of size q .
- The q possible states of a mark correspond to symbols in Q .
- Let fingerprint be a l -word over Q .
- Let n be the number of users.



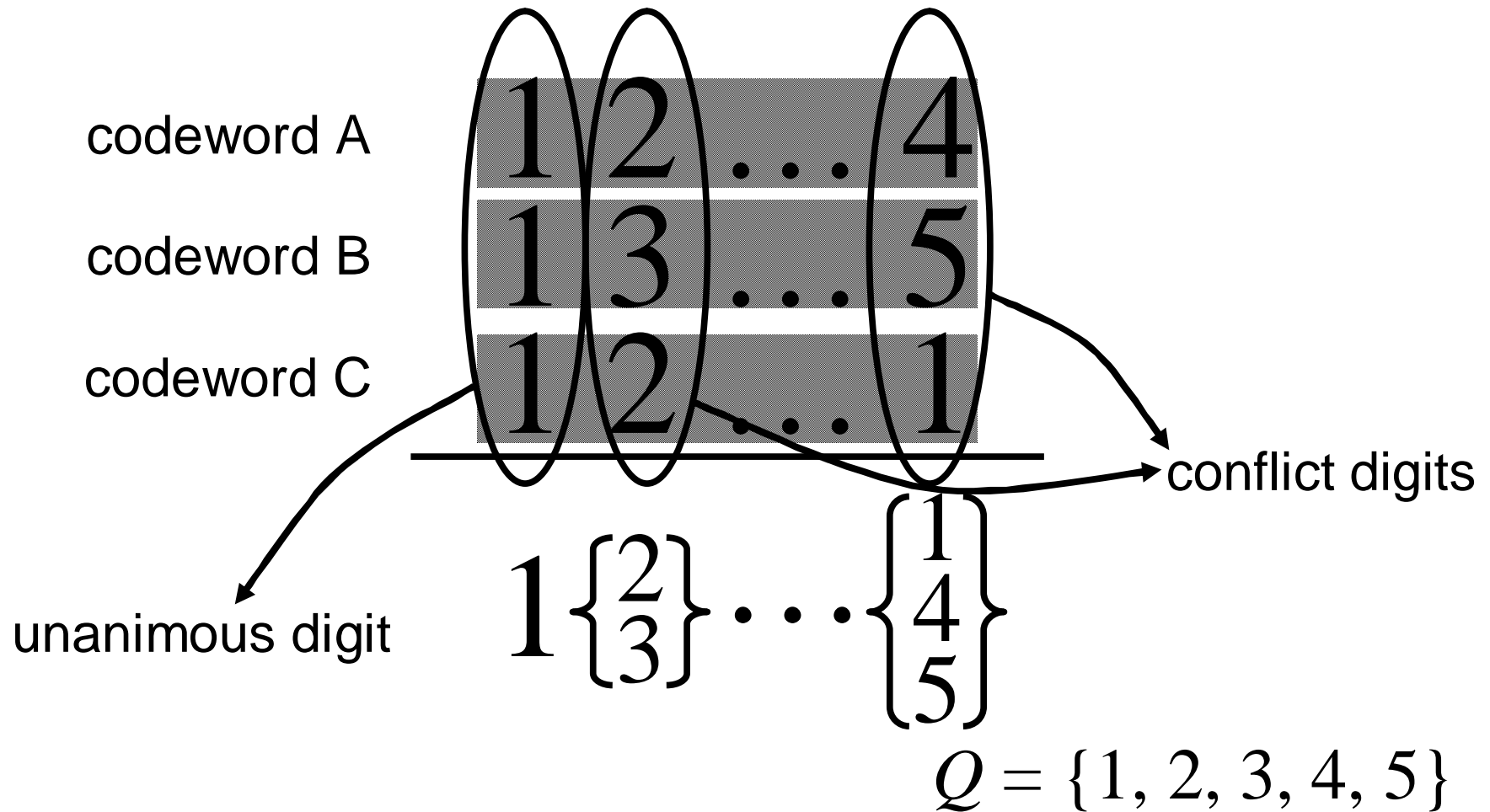
Preliminaries(2/2)

- A set of n distinct fingerprints is called (l, n, q) code.
- Two cases are considered.
 - Case 0: attackers can only generate symbols in Q .
 - Case 1: attackers are able to transfer a mark into unreadable state.

We use symbol • to indicate an unreadable state.

Attacks(1/4)[Chor, Fiat, Naor 94]

Feasible set of a coalition is the set of all the possible l -words which could be generated by the coalition.



Attacks(2/4)[Boneh, Shaw 98]

codeword A 1 2 ... 4

codeword B 1 3 ... 5

codeword C 1 2 ... 1

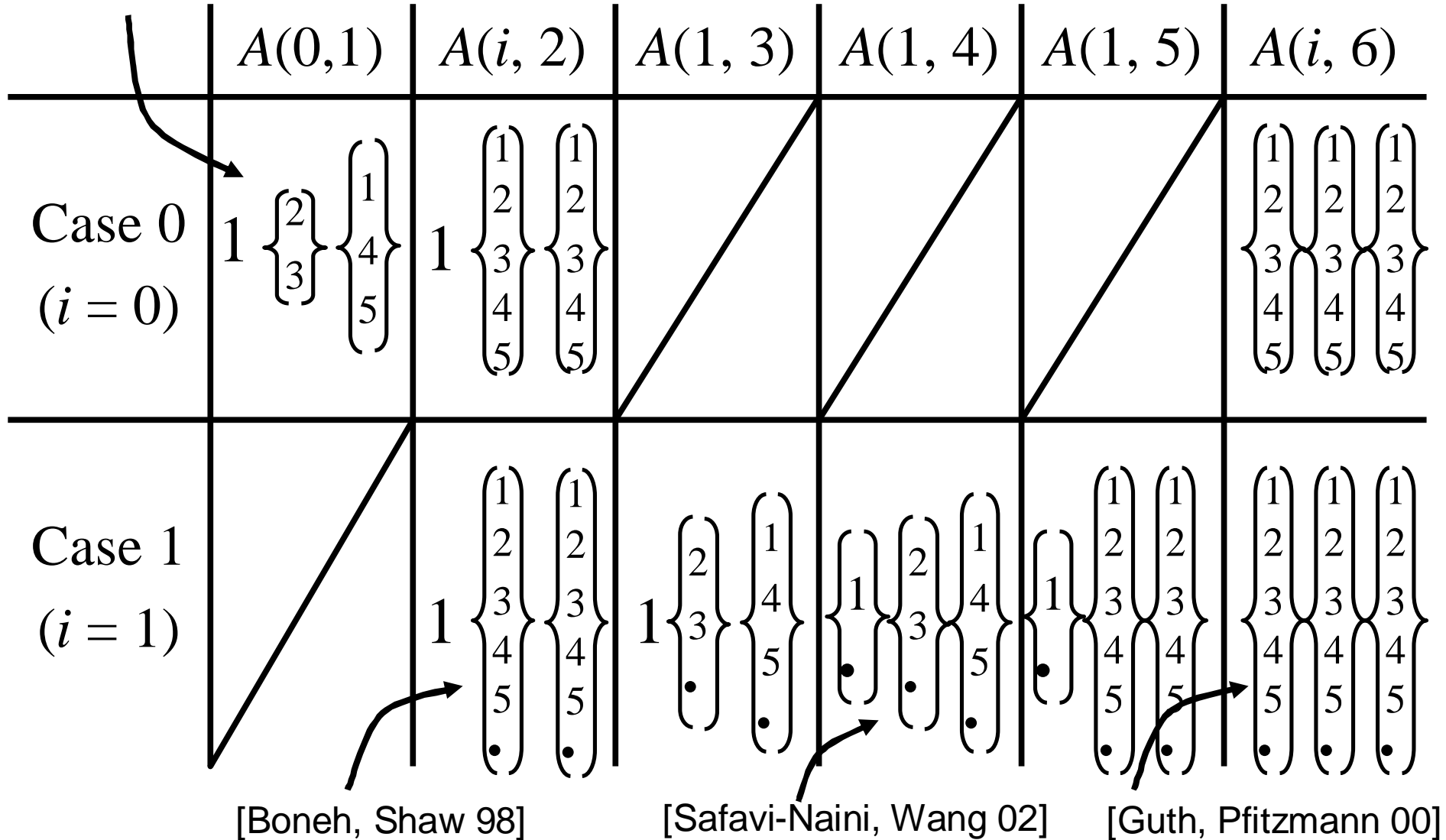
$$1 \left\{ \begin{array}{c} 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ \cdot \end{array} \right\} \dots \left\{ \begin{array}{c} 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ \cdot \end{array} \right\}$$

$$Q = \{1, 2, 3, 4, 5\}$$

[Chor, Fiat, Naor 94]

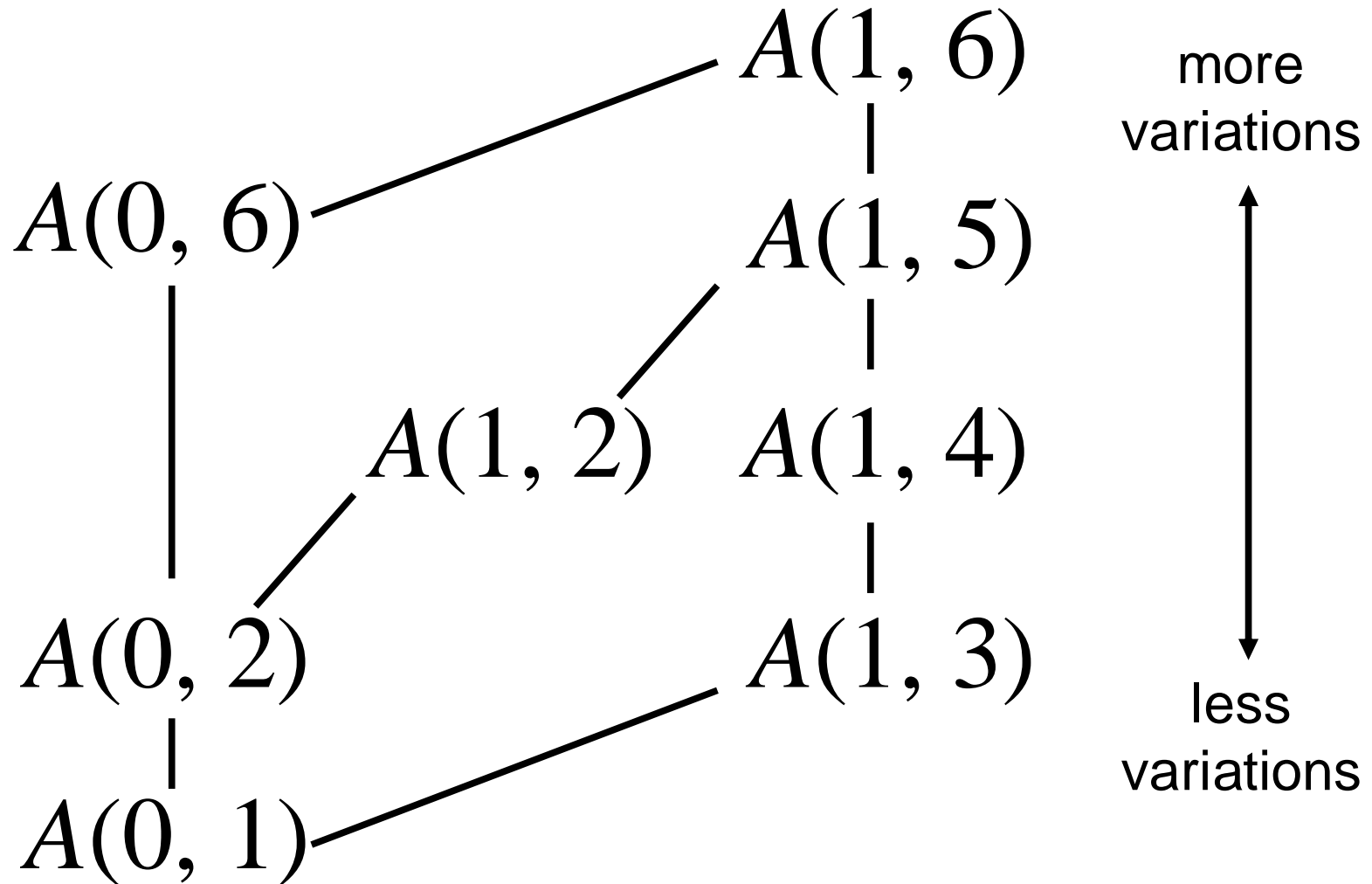
[Staddon, Stinson, Wei01]

Attacks(3/4)



Coalition $\{124, 135, 121\}$, $Q = \{1, 2, 3, 4, 5\}$, $l = 3$

Attacks(4/4)



Collusion secure codes

$FP(A(i, j); c)$: c -frameproof code under $A(i, j)$

$SFP(A(i, j); c)$: c -secure frameproof code under $A(i, j)$

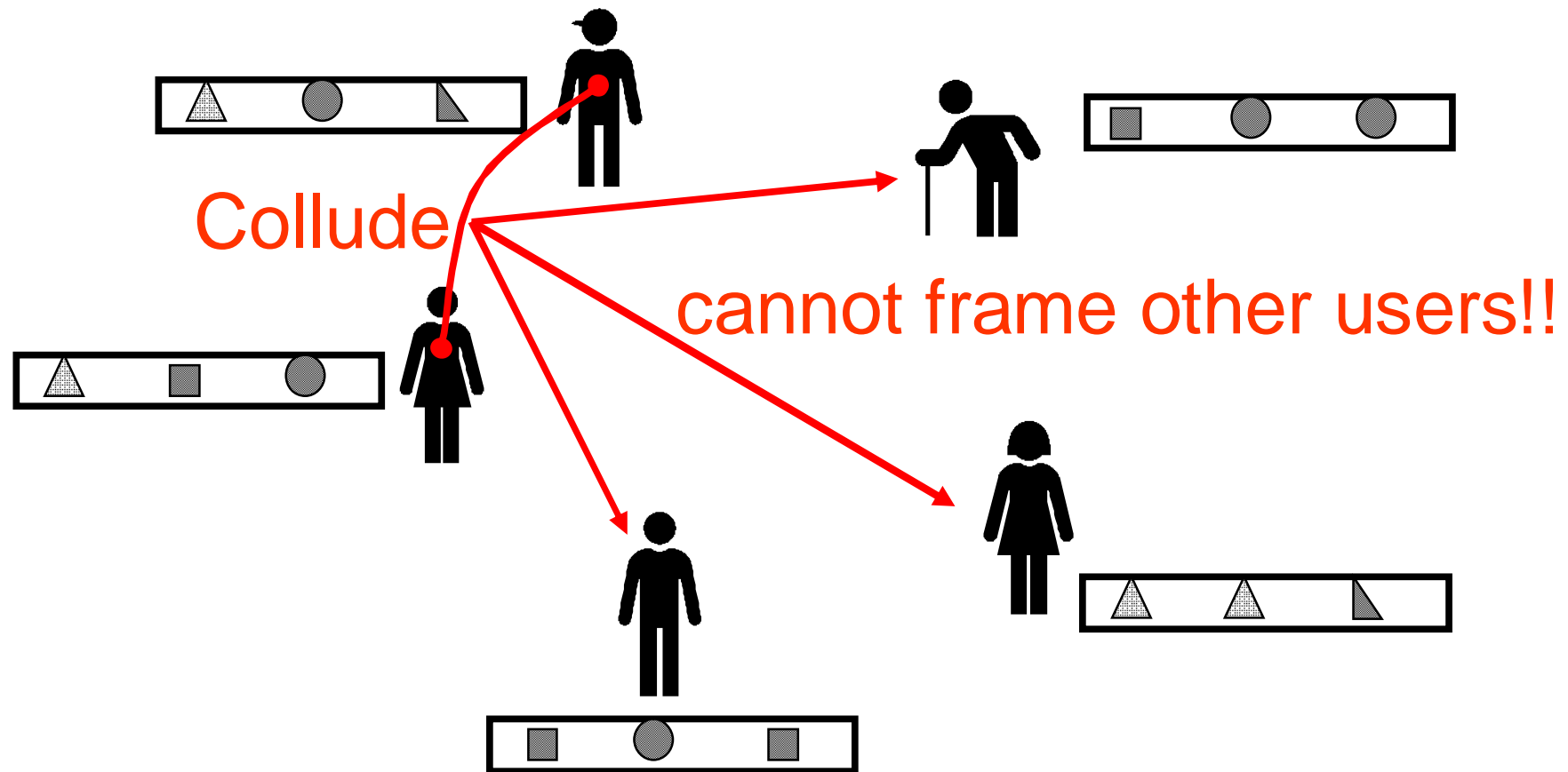
$IPP(A(i, j); c)$: c -identifiable parent property code under $A(i, j)$

$TA(A(i, j); c)$: c -traceability code under $A(i, j)$

$TS(A(i, j); c)$: totally c -secure code under $A(i, j)$

$SS(A(i, j); c)$: $(c, g/s)$ -secure code under $A(i, j)$

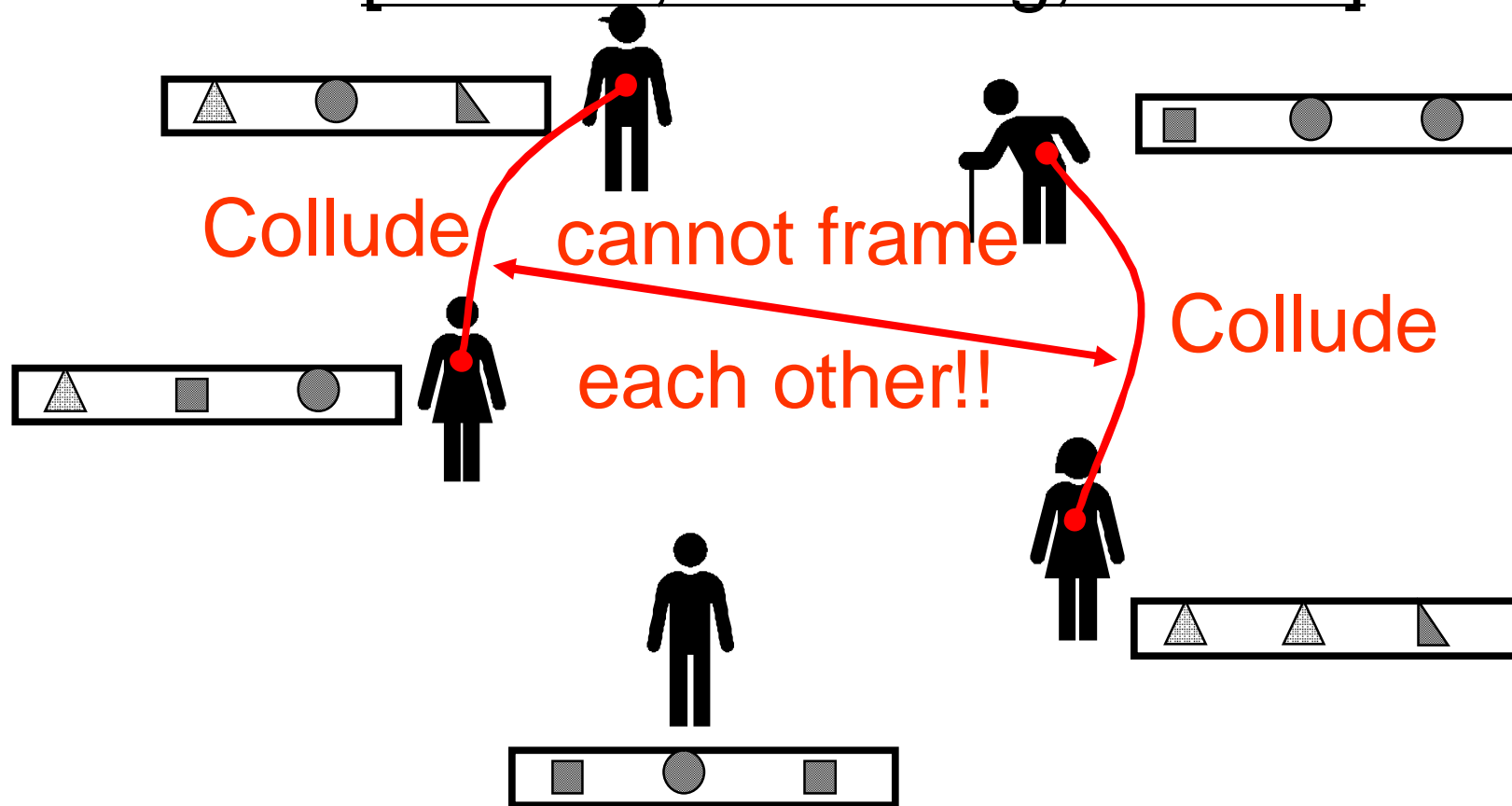
c -frameproof codes [Boneh, Shaw 98]



No coalition of at most c users can frame innocent user.

c -secure frameproof codes

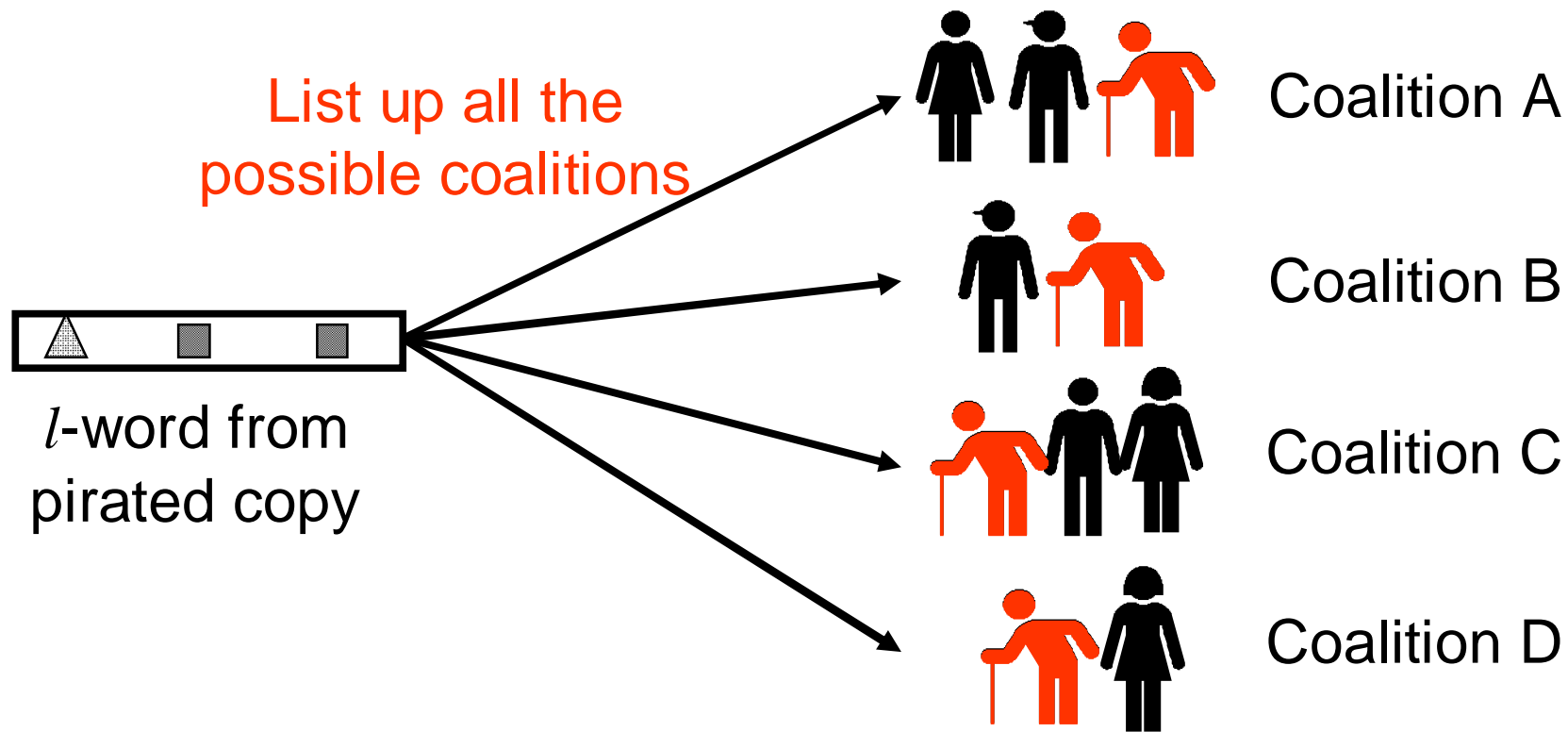
[Stinson, van Trung, Wei 00]



No two disjoint coalition of at most c users can generate the same l -word.

c -identifiable parent property codes

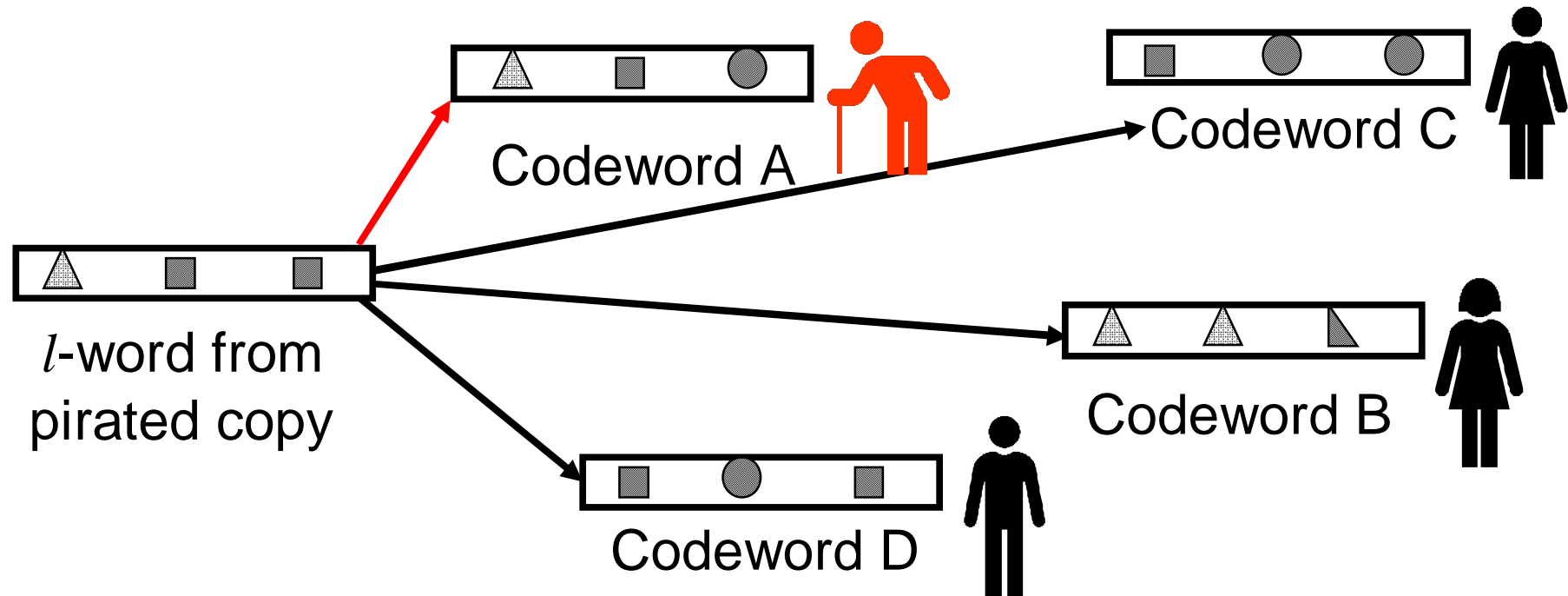
[Hollmann, Lint, Linnartz, Tolhuizen 00]



No coalition of at most c users can generate a l -word which has two disjoint parents (coalitions who can make the l -word).

c -traceability codes

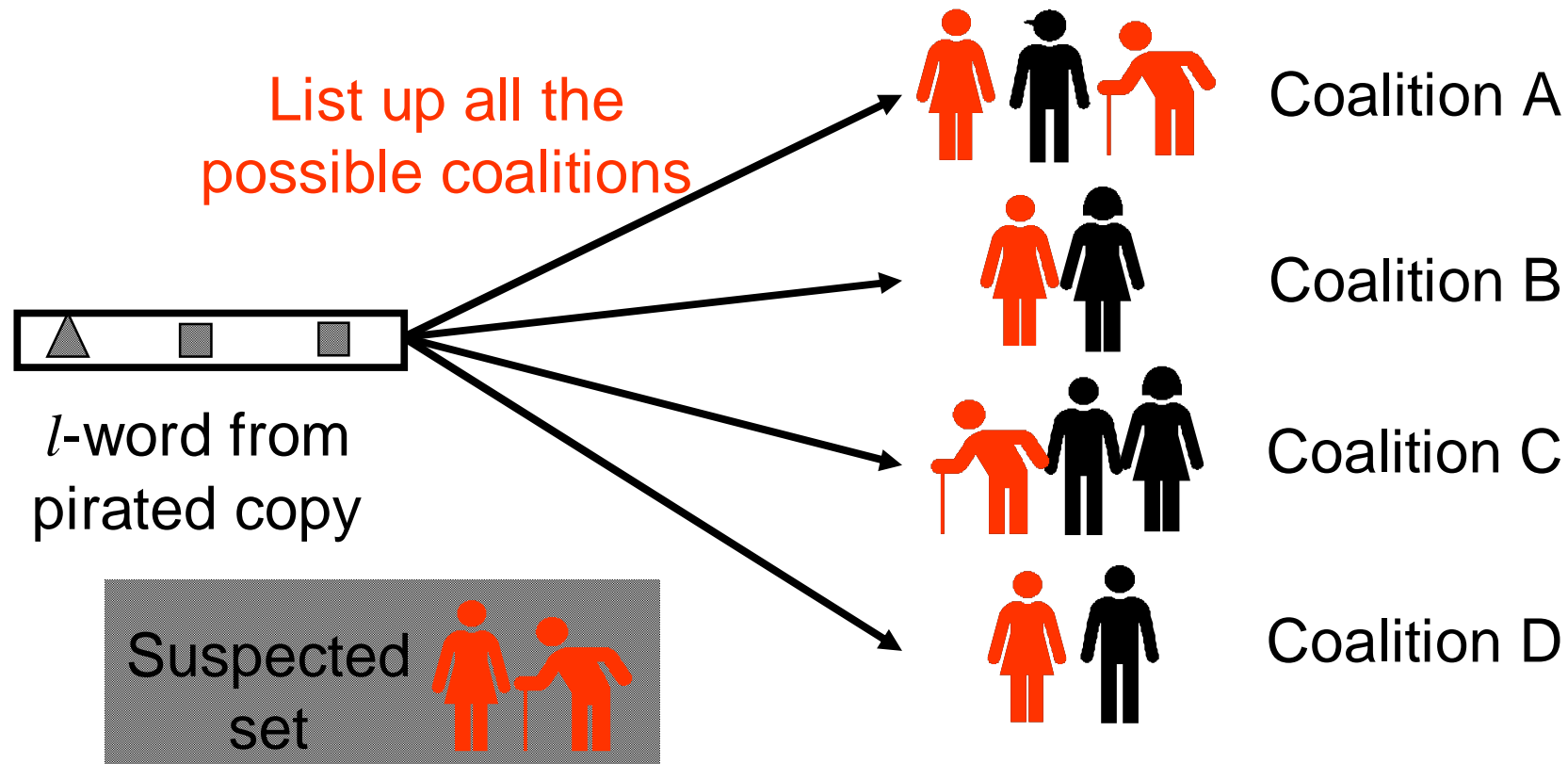
[Chor, Fiat, Naor 94] [Staddon, Stinson, Wei 01]



No coalition of at most c users can generate a l -word whose closest codeword is not in the coalition.

$(c, g / s)$ -secure codes

[Orihara, Mizuki, Nishizeki 03]

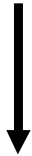


Coalition of at most c users can only generate a l -word which has a suspected set of size s containing g real traitors.

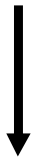
Relationships among codes

[Staddon, Stinson, Wei01]

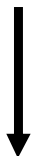
$TA(A(0, 1); c)$



$IPP(A(0, 1); c)$

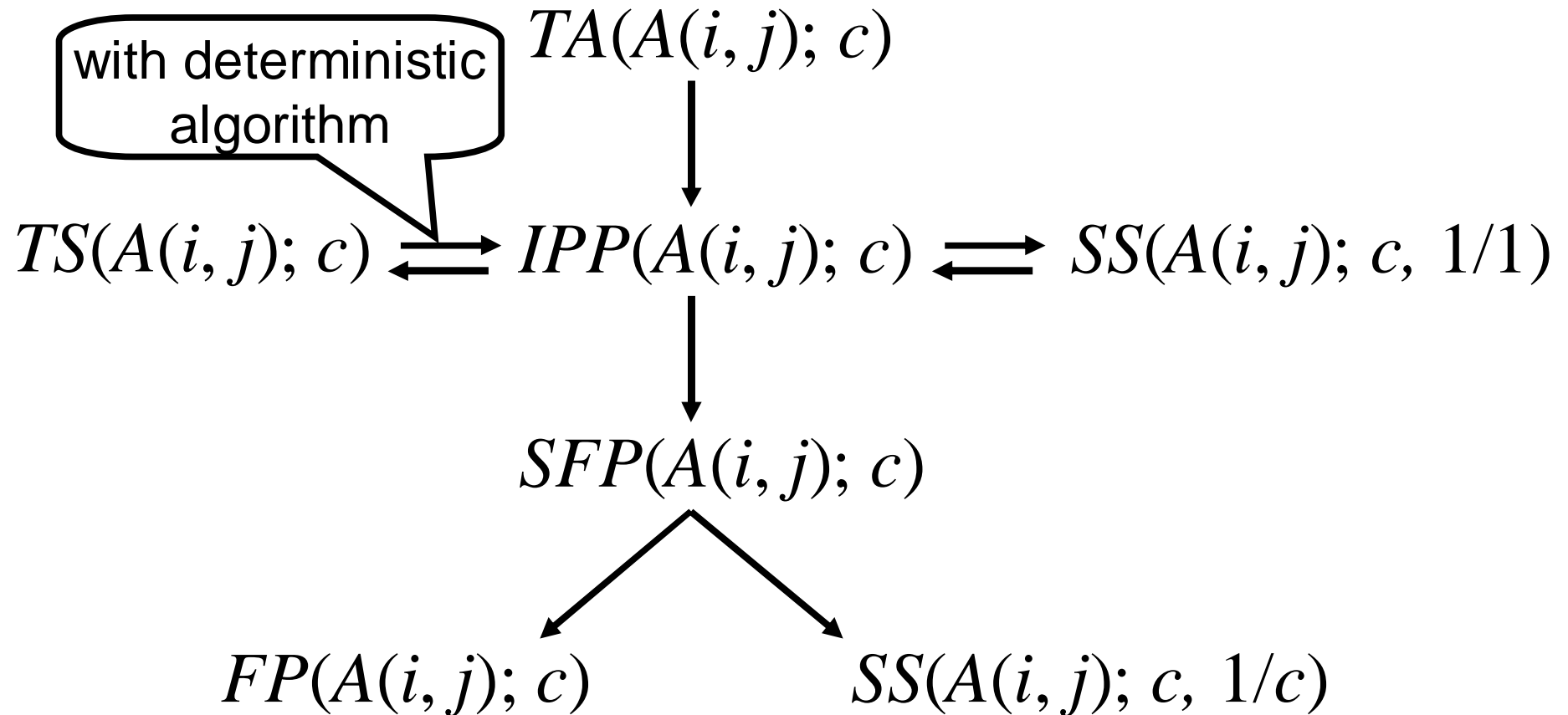


$SFP(A(0, 1); c)$



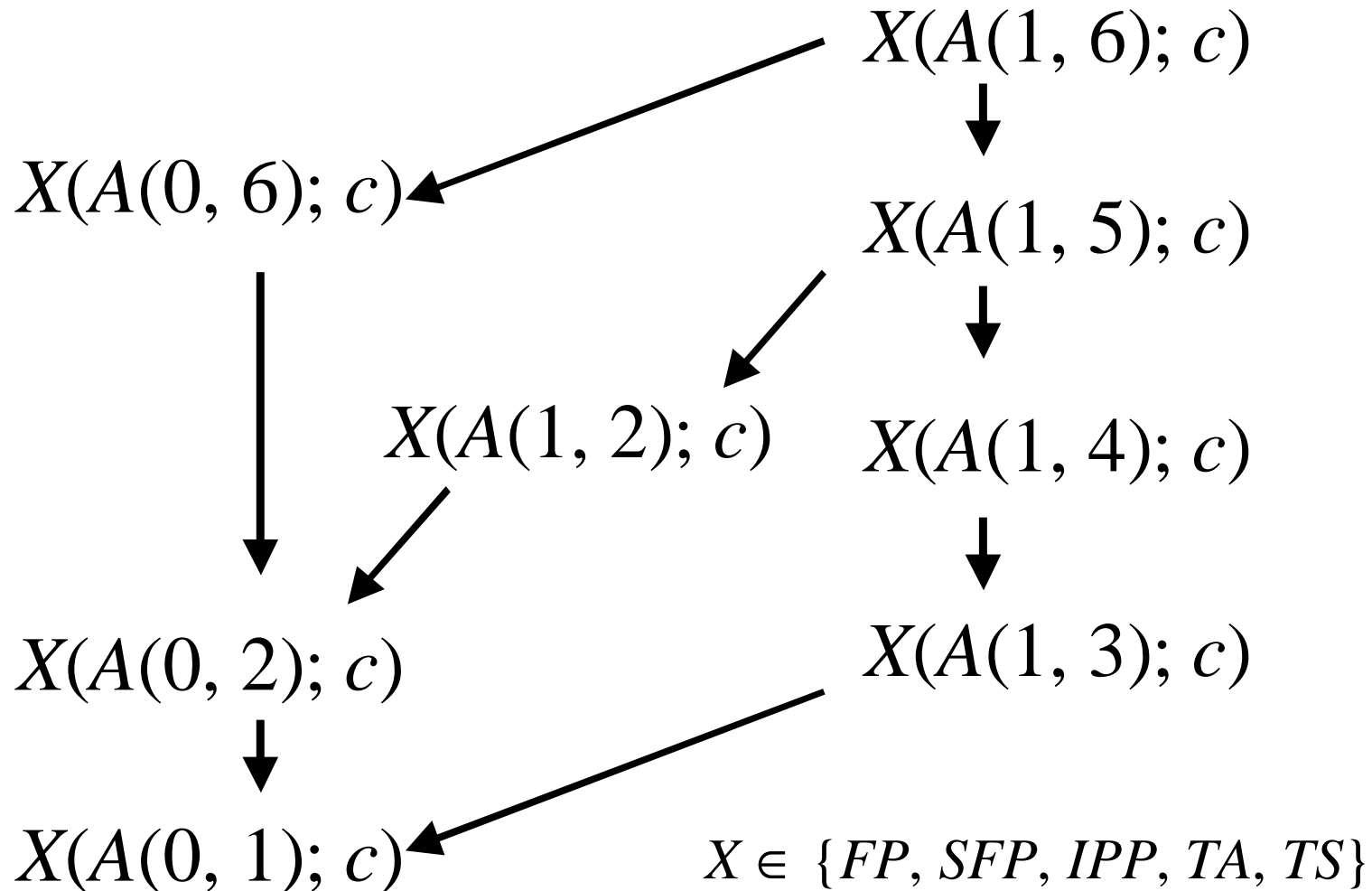
$FP(A(0, 1); c)$

New relationships among codes

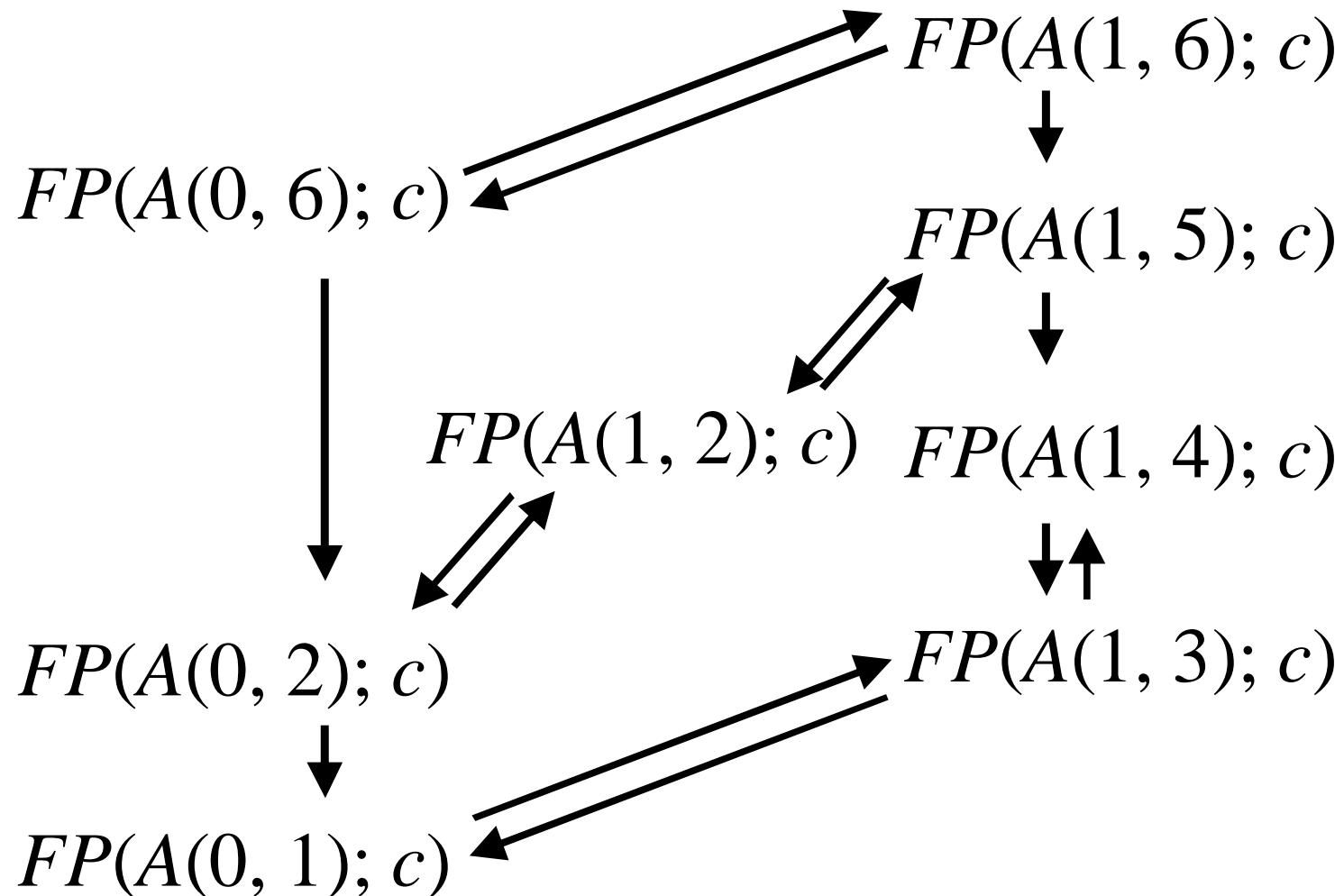


$(i, j) \in \{(0, 1), (0, 2), (0, 6), (1, 2), (1, 3), (1, 4), (1, 5), (1, 6)\}$

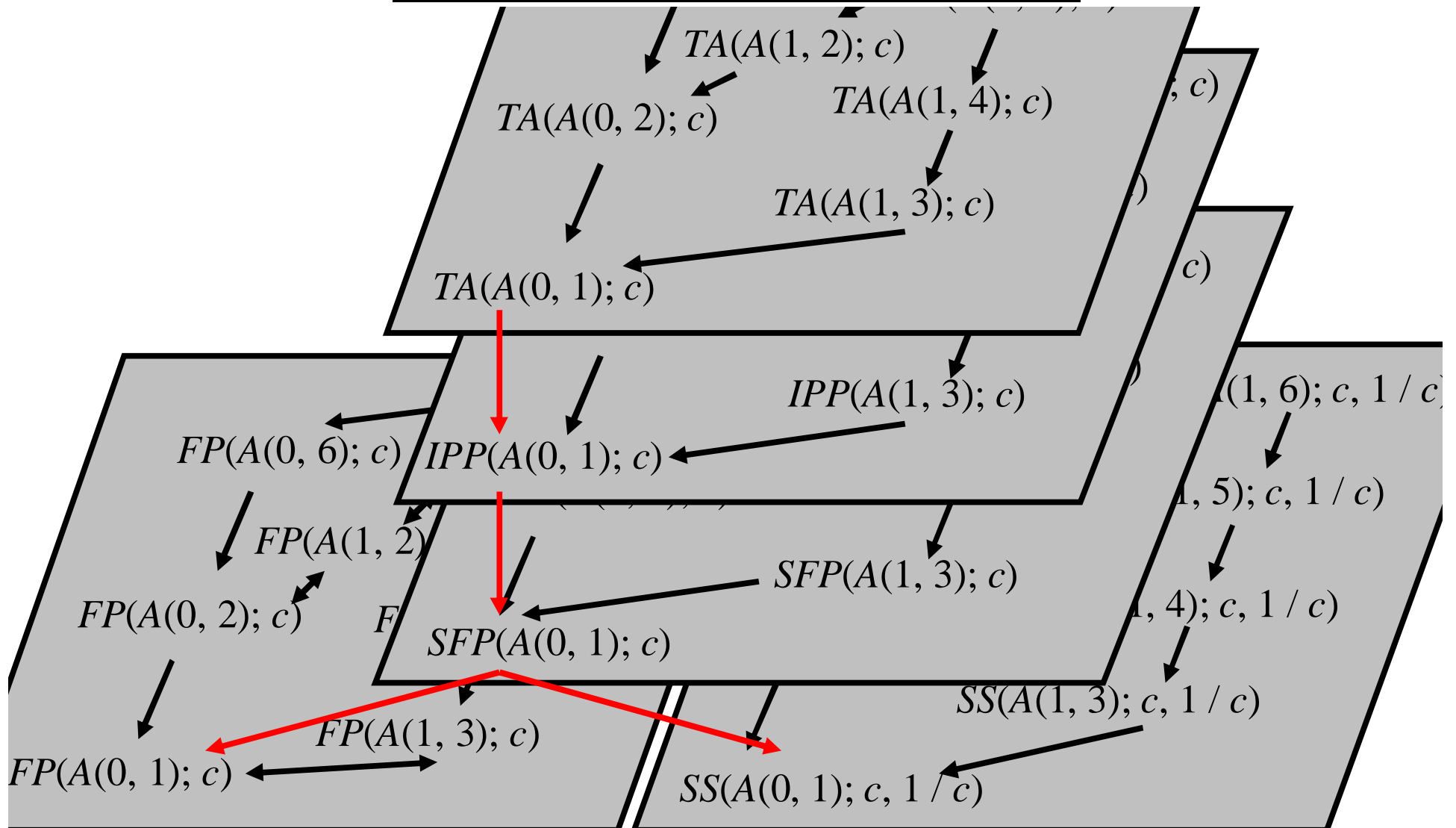
New relationships among codes under different attacks (1/2)



New relationships among codes under different attacks (2/2)



New relationships among combined notions



Conclusion

- Defined various types of attack (marking assumption) including the ones in previous works.
- Revealed new relationships among codes under different types of attack.
- Revealed new relationships among codes with different collusion secure properties.

Thank you!

Q & A