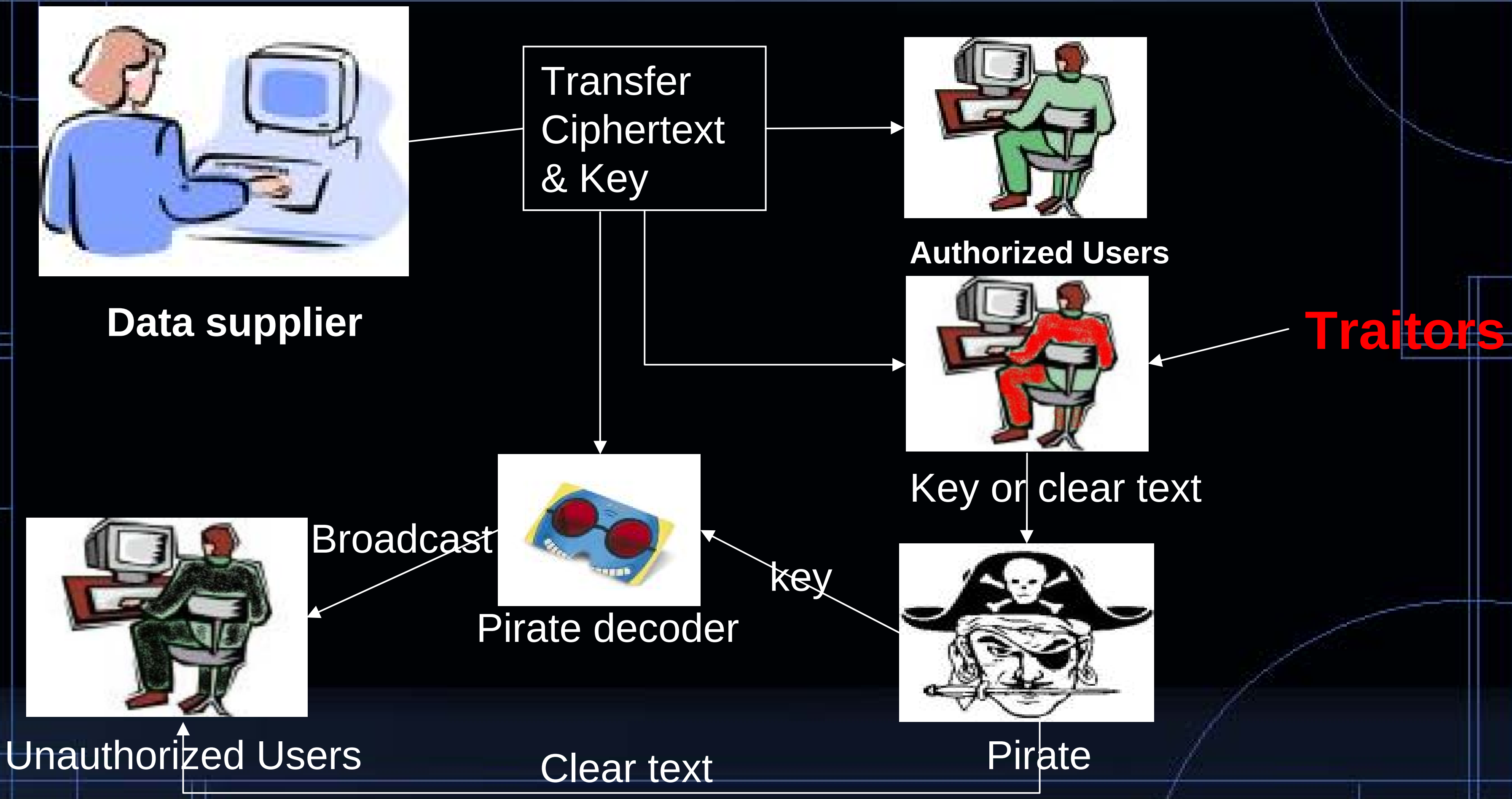
Tracing Traitors

B. Chor, A. Fiat, M. Naor, & B. Pinkas, Information Theory, IEEE Transactions on Volume 46, Issue 3, May 2000 Page(s):893 - 910
Digital Object Identifier 10.1109/18.841169

Presented by Chang Chen

Who is traitor?



"The traitor or traitors is the (set of) authorized user(s) who allow other, non-authorized parties, to obtain the data."

- There are at least four possible ways for a pirate to obtain keys:

-spy transmission, and break encryption of keys

-steal some honest users' keys

-conspire with traitors

-conspire with insiders within data supplier

- The tracing traitor scheme in this paper focus on preventing traitors from distributing their keys to pirate. This paper assumes that encryption/decryption transmission is secure.

Tracing Traitor Scheme

Basic idea of scheme:

- In initialization, data supplier distributes different keys (personal keys) to each user for decrypting ciphertext.
- If data supplier captures a pirate decoder, test it as a black box, which means just using ciphertext encrypted by different users' personal keys to input into pirate decoder and see the output of pirate decoder.
- If detect a key for particular user in pirate decoder, the user is a traitor.

Tracing traitor Scheme

Ways to apply schemes

- Combine with broadcast encryption scheme.

  Trace one, delete one until pirate decoder useless.

- “The data provider itself can use this evidence to identify the pirates and then try to obtain other types of legal proofs about their activities.”

Appreciative Comment

- The schemes are inexpensive to be implemented.

  --no any secure hardware requirement.

  --treat pirate decoder as a blackbox.

Critical Comment

- The schemes cannot prevent fabrication by data supplier. Therefore, honest users could be in the risk of being framed.

- The schemes in the paper only can trace the traitors who leak keys. What the schemes can do does not conform with the definition of traitors.

Critical Comment

- The personal keys distributed to users store in users' devices, which increases the risk of device being hacked. But, the paper ignores this probability.

Question

Just depending on a key detected from pirate decoder, can the user be regarded as a traitor?