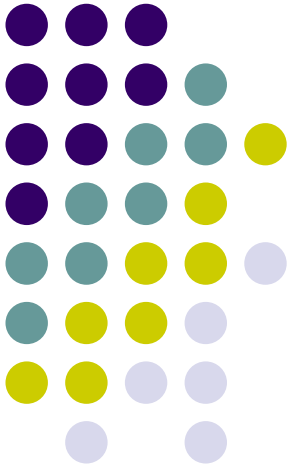
Tracing Traitors

Benny Chor, Amos Fiat, Moni Naor, Benny Pinkas



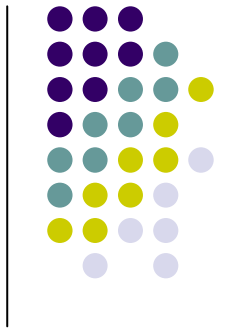
Presented by Jesse Wu

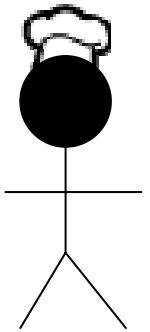
B. Chor, A. Fiat, M. Noar, B. Pinkas, “Tracing Traitors”, *IEEE Trans. Inform. Theory*,vol. 46, NO. 3,pp. 893-910, May 2000,

Next Day's News

CEO eats paper for a diet!

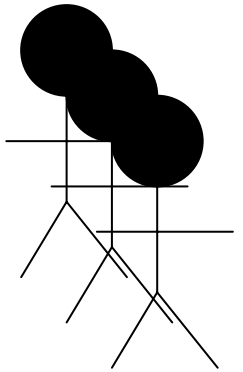
~~~~~ ~~~~~ ~~~~~~~~~~~~~ ~~~~~~~~ ~~~~~~~
~~~~~~
~~~~~~ ~~~~~~~ ~~~~~~~~ ~~~~~ ~~~~~~
~~~~~~~~~ ~~~~~~~~~~~~ ~~~~~~~~~~~~~~
~~~~~~~ ~~~~~~~~ ~~~~~~~ ~~~~~~~~
~~~~~~~~~ ~~~~~~~ ~~~~~~~~~~~~
~~~~~ ~~~~ ~~~ ~~~~~~ ~~~~~ ~~~~~~~~~~~
~~~~~~~~ ~~~~~ ~~~~~~~~~~~~~~~ ~~~~~
~~~~~~~~~ ~~~~~~ ~~~~~~ ~~~~~~~~~
~~~~~~ ~~~~~ ~~~~~~~~~~
~~~~~ ~~~~~~~~~~~~ ~~~~~~~ ~~~~~~~
~~~~~~~ ~~~~~~~~~~ ~~~~~~~~~
~~~
~~~ ~~~~~~~ ~~~~~~~~~ ~~~~~ ~~~~~~ ~~~~~
~~ ~~~~~~ ~~~~~~~~~~ ~~~~~ ~~~~~~ ~~~
~~~~~~ ~~~~~~~~~ ~~~~~~~ ~~~~~ ~~~~~
~~~~~~~~~~~~~~~~~ ~~~~~~~ ~~~~~
~~~~~~~~~ ~~~~~ ~~~~~~~~~ ~~~~~~~ ~~~~~~
~~~~~~ ~~~ ~~~~~~~ ~~~~~~ ~~~~~~
~~~~ ~~~~~ ~~~ ~~~~ ~~~~~~
~~~~~ ~~~~~ ~~~~ ~~~~~~~~ ~~~~~
~~~~~~~ ~~~~~~ ~~~~~~ ~~~~~~~~~~




~~~~~~~

Next Day's News

CEO wear's pink hats!



Introduction

The Data Supplier

Authorized Users

Encrypted data

keys

Cleartext being sent

Pirate users

Introduction

TRAITOR!!!

The Data Supplier

Encrypted data

keys

Keys being sent

Pirate users

A traitor tracing scheme includes ...

- User Initialization scheme

  used by the data supplier to add new users and give them keys. A hash function is used assign the keys to guarantee that any combination of keys is different to anyone else.

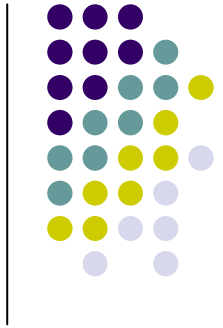
- Encryption/Decryption scheme

  How data gets encrypted/decrypted.

- Traitor tracing algorithm

  used when a pirate decoder is found to determine the keys that have been used.

Critical Comment



- The paper does not emphasize much on the probability of a traitor's innocence. (false positives)

  The paper only mentions one case:
  For **1 million users** and
  At most **500 traitors**
  Then the probability of a false identification is **2^-10** (1 in 5 billion)

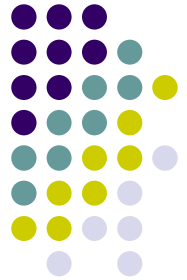
Things that could go wrong when transferring keys

The Data Supplier **Authorized Users**

keys

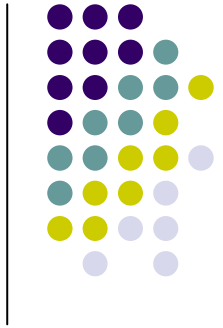
Keys could have been intercepted,
user's computer might get stolen,
data supplier may be corrupt etc…

Critical Comment 2



- The paper goes into too much detail analyzing the algorithms of different traitor tracing schemes, and not enough real world applications

Appreciative Comment



The idea of keys being able to be traced is good because:

- **It could reduce piracy**

  Deters users from co-operating with pirates just by knowing that keys could be traced.

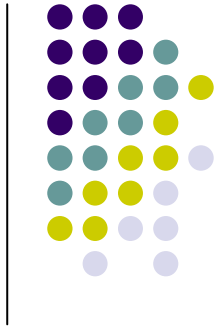
- **It could be used in many real world applications**

  Pay-Television

  Games

  DVD’s

Question



Could an authorized user labeled as a traitor by the data supplier in actual fact be innocent?