A privacy-preserving group encryption scheme with identity exposure

Chuan-Kun WU

Frontiers of Computer Science, DOI: 10.1007/s11704-022-1555-1

Problems & Ideas

- Medical practitioners may need to report special medical cases. However, “whistleblowers” may worry about their over-responsibility.
  - Allow report anonymously? Not a good solution. What about hoaxes?
  - Privacy-preserving solution? No solution meets the requirement.
- Ideas: Reporter makes himself certain level of anonymity.
  - Choose a logical group (including himself) with certain level of trust.
  - Ask the authority AUT to encrypt a session key (a random number) using each of the public keys of the group members, respectively, and send the whole encryption to the reporter;
  - The reporter is able to decrypt the session key, and hence can establish a secure communication channel with the authority AUT.
  - The reporter encrypt the message to report to the AUT together with some other additional messages.

Main Contributions

- Contributions: The proposed privacy-preserving encryption has a number of good properties preferable for whistleblowers, including
  - Easy to use. To start the protocol, one choses a logical group of registered members;
  - The group members should have certain level of trust, so that the reported message can be trusted, i.e., the chances of hoaxes are small.
  - The identity of the message sender is anonymous. The AUT only knows that the message sender belongs to the logical group.
  - If the reported message is latter on proved to be valuable and the reporter deserves reward, the message sender is able to prove his identity.