Improvement on a Batch Authenticated Key Agreement Scheme

Qingfeng Cheng, Ting Chen, Siqi Ma, Xinghua Li

Frontiers of Computer Science, DOI: 10.1007/s11704-020-0194-7

Problems & Ideas

- Problems of Yao et al.'s scheme (abbreviated as YC-BAKA scheme)
  - Potential risk of master key disclosure.
  - No perfect forward secrecy.

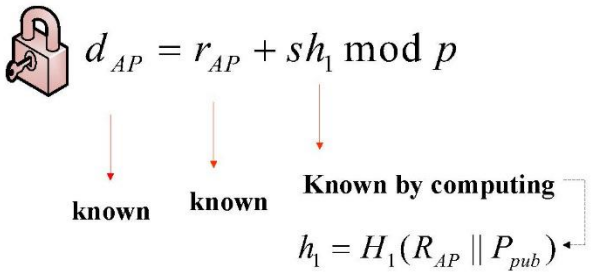

Fig.1 Potential risk of master key disclosure

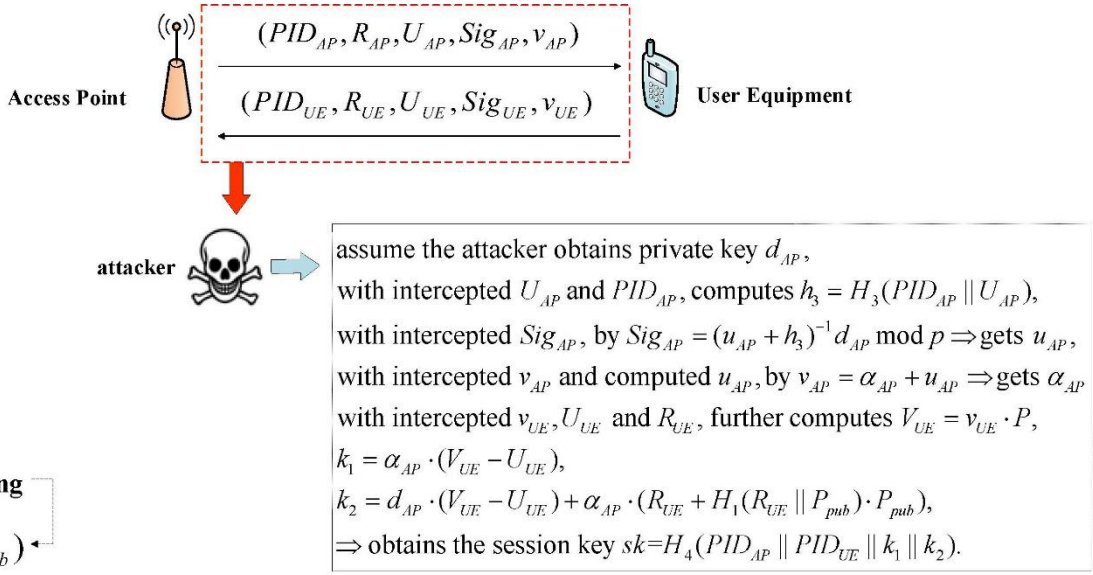

Fig.2 Explanation of no perfect forward secrecy

- Ideas: Designing a batch authenticated key agreement scheme
  - Protocol entities generate signatures and authenticate mutually.
  - After authentication, protocol entities share a session key one-to-one.

Main Contributions

- **Realize perfect forward secrecy**
  - Protect α_{AP} and the session key by adopting some computational hard problems, shown in Fig.3.

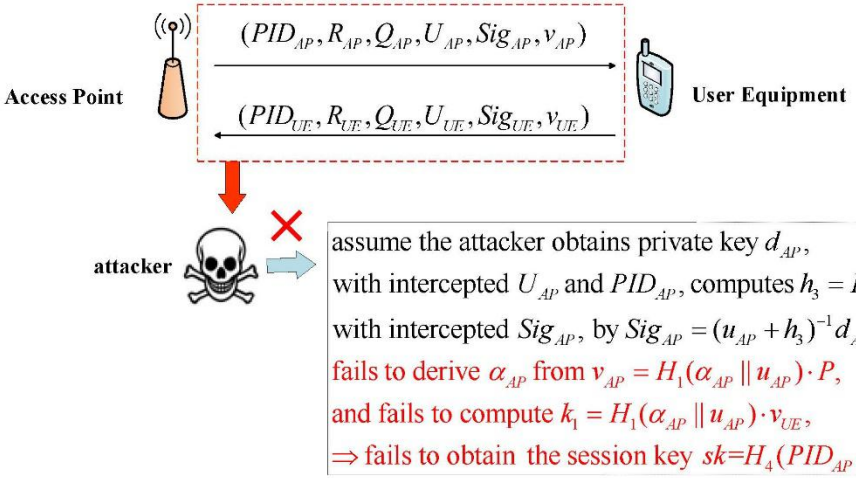

Fig.3 Realizing perfect forward secrecy

- **Fix the potential risk of master key disclosure**
  - Protect the master key by adopting elliptic curve discrete logarithm problem, i.e. do not use the master key directly but use its corresponding public key.