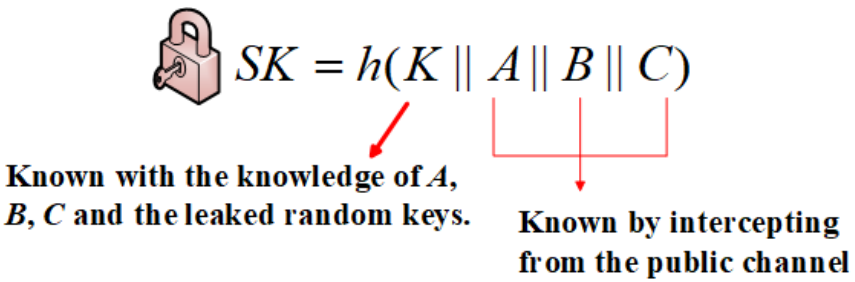
An efficient and authenticated key establishment scheme based on fog computing for healthcare system

Xinghua LI, Ting CHEN, Qingfeng CHENG, Jianfeng MA

Frontiers of Computer Science, DOI: 10.1007/s11704-021-0537-z

Problems & Ideas

- Potential problems of Jia et al.'s scheme and Ma et al.'s scheme
  - Ephemeral key disclosure attack



Potential risk of ephemeral key disclosure attack

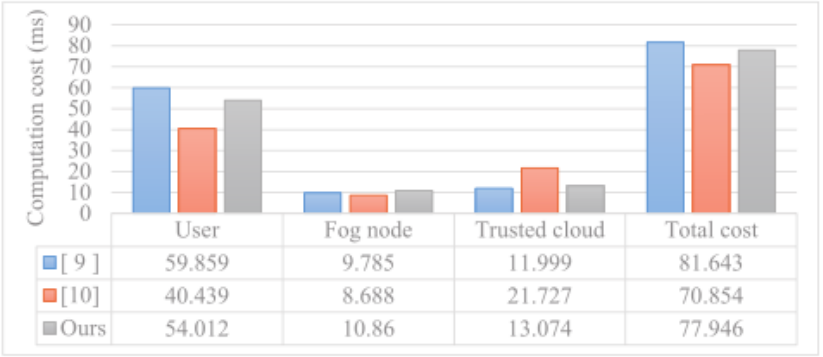
- Ideas: Designing an authenticated key agreement scheme based on fog computing.
  - The user is authenticated by the trusted cloud server through the fog node.
  - The user, the fog node and the trusted cloud agree on a session key.

Main Contributions

- **The improved scheme is securer and resists ephemeral key disclosure attack.**

```
RESULT not attacker (sk_c[]) is true
RESULT not attacker (sk_f[]) is true
RESULT not attacker (sk_u[]) is true
RESULT inj-event(end_Ui(ID_j)) ==> (inj-event(end_TC_2(ID_j)) ==>
(inj-event(begin_TC(ID_i, ID_j)) ==> inj-event(begin_FNj(ID_j)))) is true
RESULT inj-event(end_FNj(ID_i)) ==> (inj-event(end_TC_1(ID_i)) ==>
(inj-event(begin_TC(ID_i, ID_j)) ==> inj-event(begin_Ui(ID_i)))) is true
```

- **The improved scheme costs lower computation overhead.**



	User	Fog node	Trusted cloud	Total cost
[9]	59.859	9.785	11.999	81.643
[10]	40.439	8.688	21.727	70.854
Ours	54.012	10.86	13.074	77.946