A proactive secret sharing scheme based on Chinese remainder theorem

Keju MENG, Fuyou MIAO, Yu NING,
Wenchao HUANG, Yan XIONG, Chin-Chen CHANG

Frontiers of Computer Science, DOI: 10.1007/s11704-019-9123-z

Problems

- No proactive secret sharing (PSS) scheme based on Chinese Remainder Theorem (CRT) was proposed.
- Traditional CRT-based SS schemes are over integer ring and they are unsuitable to design PSS scheme.

Main Contributions

- A PSS scheme based on Asmuth-Bloom (t,n) threshold SS which utilizes CRT for integer ring is given
- This paper proposes another PSS scheme based on Ning et al. (t,n) threshold SS which uses CRT for polynomial ring. The scheme is ideal and supports shares refreshing any times.
- We analyze the reason why the PSS scheme over integer ring cannot work effectively when shares are refreshed too many times by comparing it with the second PSS scheme over polynomial ring.