A Simple Construction of CRT-based Ideal Secret Sharing Scheme and Its Security Extension Based on Common Factor

Lei WU, Fuyou MIAO, Keju MENG, Xu WANG

Frontiers of Computer Science, DOI: 10.1007/s11704-021-0483-9

Problems & Ideas

- Problems:
  - SS schemes based on the Chinese Remainder Theorem (CRT) are either low in the information rate or complicated in construction.
  - Most of the existing SS schemes face two types of attacks, message modification attack, and eavesdropping attack.
- Ideas:
  - A simple construction of an ideal (t,n)-SS scheme is proposed based on CRT for a polynomial ring.
  - We proposed a SS scheme which is resistant to eavesdropping and modification attacks by outside adversaries based on common polynomial factor.

Main Contributions

- An ideal (t,n)-SS scheme based on CRT for polynomial ring with an easy construction phase is given.
- This paper proposed another (t,n)-SS scheme which can not only prevent message modification attack in the distribution phase and reconstruction phase but also thwart eavesdropping attack in the reconstruction phase.