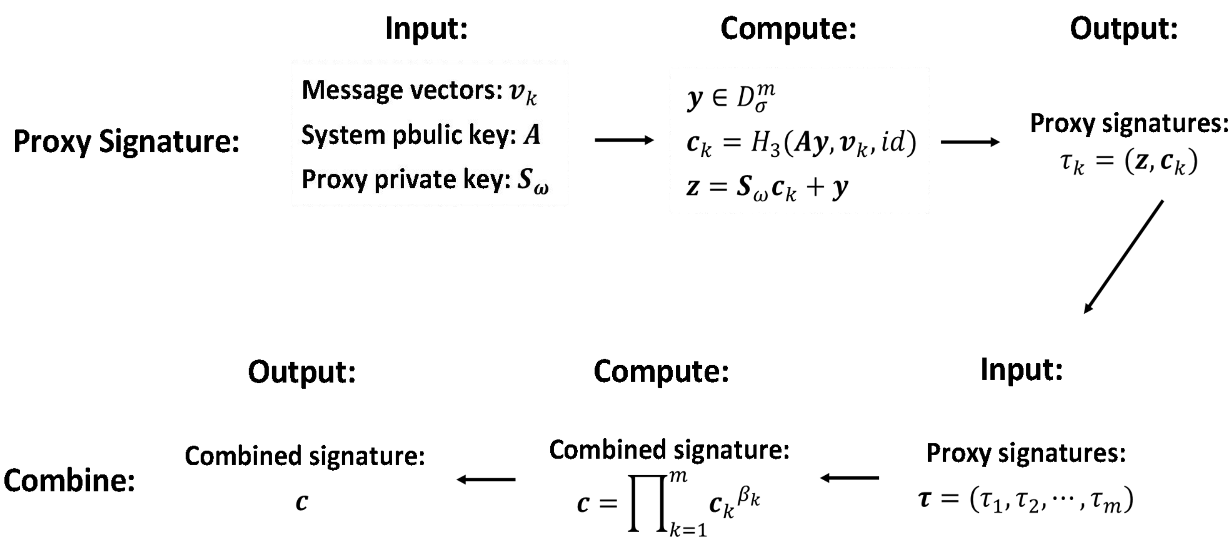
Certificateless Network Coding Proxy Signatures from Lattice

Huifang YU, Ning WANG

Frontiers of Computer Science, DOI: 10.1007/s11704-022-2128-z

Problems & Ideas

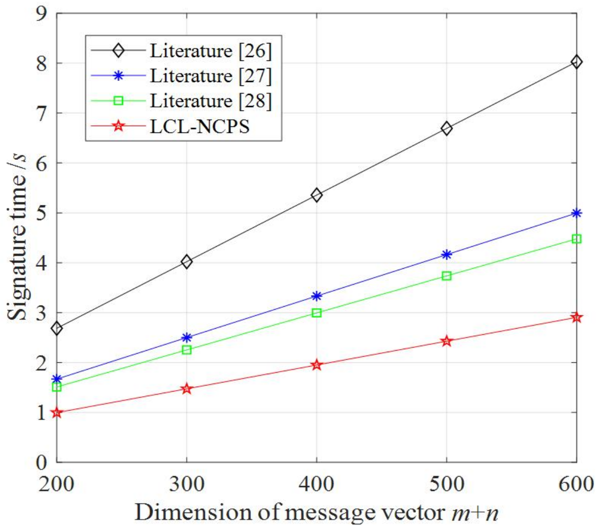
- Problems of conventional certificateless proxy signature approaches:
  - Not having the ability against the quantum computing attacks.
  - Not suitable for applying in network coding environment.
- Ideas: A integration of certificateless network coding proxy signatures from lattice that integrates certificateless proxy signature and network coding.



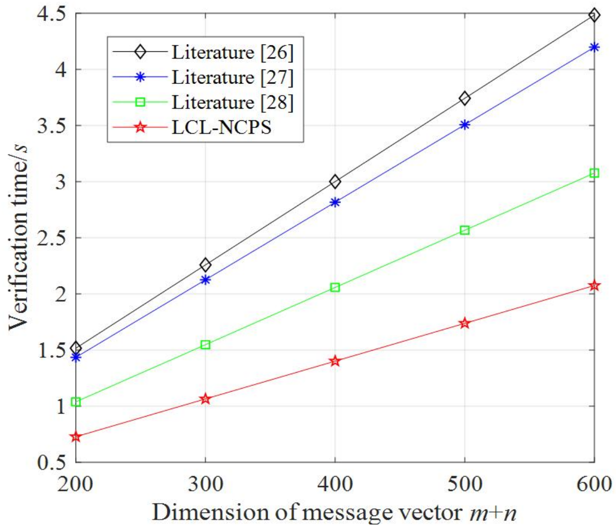
Flowchart about proxy signature and combination

Main Contributions

- Contributions:
  - A construction of certificateless proxy signature and multi-source network coding technology;
  - Multi-source proxy signatures from lattice can resist the quantum computing attacks and are very suitable for applying to network coding scenario.



Signature time comparison



Verification time comparison