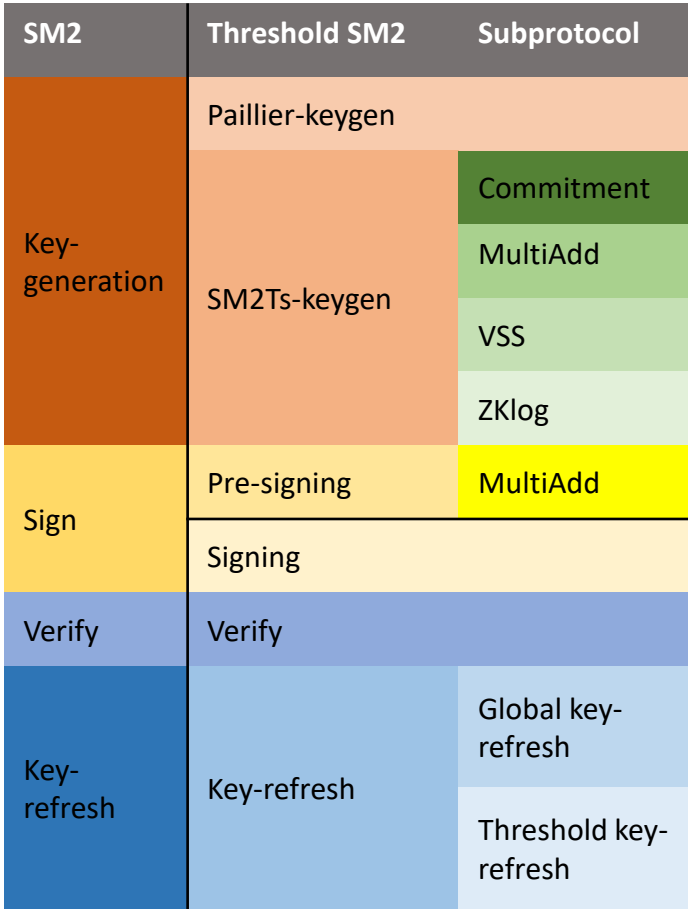
Non-interactive SM2 Threshold Signature Scheme with Identifiable Abort

Huiqiang LIANG, Jianhua CHEN

Frontiers of Computer Science, DOI: 10.1007/s11704-022-2288-x

Problems & Ideas

- Problems:
  - What technologies are required for SM2 threshold signature and what functions does it achieve?
  - How to security implement the SM2 threshold signature and what security goals are achieved.
- Ideas:
  - Implementing SM2 threshold signature using Paillier encryption. Then use verifiable secret sharing to achieve a flexible access structure.
  - Ensuring the protocol is UC-secure using commitments and zero-knowledge proof.



Threshold SM2 signature scheme

Main Contributions

- Contributions:
  - A novel joint virtual view synthesis and disparity refinement model that outputs not only refined disparity maps but also a synthesized middle view with high visual coherency;
  - The amount of computation and communication of ours scheme is 1/3 of the previous threshold ECDSA scheme.

Computational and communication costs of the protocol

Step	Round	Computation	Communication
Paillier	1	$422N$	$n(2k + 334\mu)$
SM2ts	6	$8N + (14 + t)G + 4N^2 + n(17N + 8G + 14N^2)$	$9k + 7\mu + n(18k + 13\mu)$
Pre-signing	2	$8N + 4G + 4N^2 + n(17N + 4G + 12N^2)$	$9k + 7\mu + t(17k + 12\mu)$
Signing	1	0	nk

Computational and communication costs of Canetti's protocol

Pre-signing step	Round	Computation	Communication
Three rounds	3	$n(56N + 12G + 33N^2)$	$n(57k + 54\mu)$
Six rounds	6	$n(49N + 29G + 33N^2)$	$n(67k + 30\mu)$
Lightweight	7	$n(38N + 26G + 19N^2)$	$n(67k + 30\mu)$
Ours	2	$8N + 4G + 4N^2 + n(17N + 4G + 12N^2)$	$9k + 7\mu + t(17k + 12\mu)$