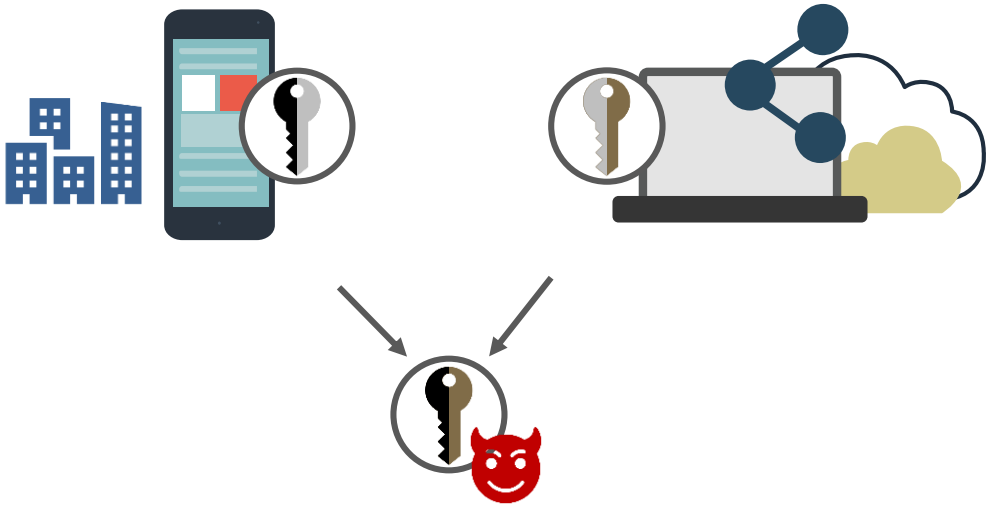
A Survey on Threshold Digital Signature Schemes

Yu PENG, Qi FENG, Debiao HE, Min LUO

Frontiers of Computer Science, DOI: 10.1007/s11704-025-41297-1

Problems & Ideas

- Problems of conventional digital signature schemes:
  - Single point of device failure or key leakage create system fault.
  - Single-party signing authority enables privilege abuse risks (malicious signer) and lacks transparent oversight mechanisms.
- Ideas: Threshold signature schemes achieve dual optimization of private key security preservation and system robustness through distributed validation mechanisms.



Threshold signature schemes can execute secure distribution of key shares among multiple parties, which collectively generate valid signatures through coordinated interactions upon satisfying predefined threshold criteria

Main Contributions

- Contributions:
  - We systematically categorizes threshold signature schemes according to their cryptographic structures and threshold implementation challenges, followed by a comprehensive comparative analysis of their scalability metrics, performance, security guarantees, and functional capabilities;
  - We compile current applications of threshold signatures and difficulties encountered in thresholding digital signatures, and propose thoughts for future directions.

Table 4 Summary of Threshold ECDSA Protocols for evaluation

Scheme	Round	Communication	Computation
GGN16 [76]	6	$O(n)$	$O(n)$
BGG17 [77]	4	$O(n)$	$O(n)$
LNR18 [84]	7	$O(n^2)$	$O(n^2)$
GG18 [81]	8	$O(n^2)$	$O(n^2)$
DKL18 [87]	$\lceil \log t \rceil + 6$	$O(n^2)$	$O(n^2)$
CGG20 [86]	4 or 7	$O(n^3)/O(n^2)$	$O(n^3)/O(n^2)$
GG20 [83]	7	$O(n^2)$	$O(n^2)$
CCL20 [85]	8	$O(n^2)$	$O(n^2)$
ANO22 [91]	2	$O(n^2)$	$O(n^2)$
DKL23 [89]	3	$O(n^2)$	$O(n^2)$
WMY23 [96]	5	$O(n^2)$	$O(n)$

Table 5 Summary of Threshold ECDSA Protocols in functionality

Scheme	Adaptive	UC	IA	Assumptions
GGN16 [76]	Static	✗	✗	Strong RSA,DCR
BGG17 [77]	Static	✗	✗	Strong RSA
LNR18 [84]	Static	✗	✗	DDH, DCR
GG18 [81]	Static	✗	✗	DDH, DCR ,Strong RSA
DKL18 [87]	Static	✓	✗	DH
CGG20 [86]	Adaptive	✓	✓	DDH, DCR, Strong RSA
GG20 [83]	Static	✗	✓	DDH, Strong RSA
CCL20 [85]	Static	✗	✗	DDH, CL
ANO22 [91]	Static	✗	✗	Ring-LPN
DKL23 [89]	Static	✓	✗	DH
WMY23 [96]	Static	✗	✓	DDH, CL

Comparison of threshold ECDSA protocols. Left: the evaluation of threshold ECDSA schemes; Right: the functionality and security of threshold ECDSA schemes.