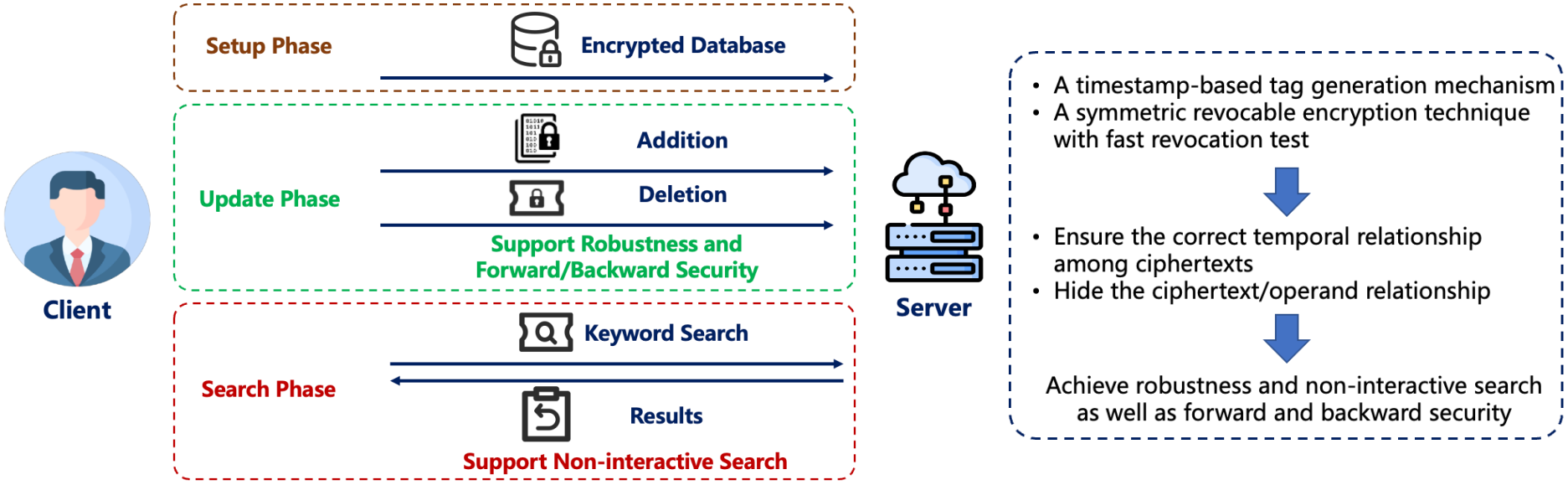
ROSA: Robust Non-Interactive Search in Dynamic Searchable Encryption

Yubo ZHENG, Wei WANG, Peng XU, Runze XU

Frontiers of Computer Science, DOI: 10.1007/s11704-025-51418-5

Problems & Ideas

- Problems of Dynamic Searchable Symmetric Encryption (DSSE):
  - Irrational update issues compromise correctness and forward and backward security in most DSSE schemes, necessitating robustness.
  - The demand for non-interactive search is urgent in real-life scenarios involving queries over large-scale databases in network environments.
- Ideas: Further consideration of non-interactive search scheme that satisfies robustness and forward and backward security.



Robust, Non-interactive Search, and Forward and Backward Secure Scheme

Main Contributions

- Contributions:
  - A universal Type II backward security definition in robust DSSE
    - Extend the Type II backward security definition to the robustness context
  - A DSSE scheme that simultaneously achieves robustness, no-interactive search, and forward and Type II backward security
    - Sub-linear search complexity
    - Employ a timestamp-based tag generation mechanism and a symmetric revocable encryption technique with fast revocation test property to address the robustness challenge
    - Better empirical search performance, particularly under poor network environments

Scheme	Robust	Computation		Communication			Client Storage	BS
		Search	Update	Search	Search Round Trip	Update		
Fides	✓	$O(a_w)$	$O(1)$	$O(a_w)$	2	$O(1)$	$O(W\log F)$	II
MITRA	×	$O(a_w)$	$O(1)$	$O(a_w)$	2	$O(1)$	$O(W\log F)$	II
SD_a	×	$O(a_w + \log N)$	$O(\log N)$	$O(a_w + \log N)$	2	$O(\log N)$	$O(1)$	II
SD_d	×	$O(a_w + \log N)$	$O(\log^3 N)$	$O(a_w + \log N)$	2	$O(\log^3 N)$	$O(1)$	II
Aura	×	$O(a_w - d_w)$	$O(1)$	$O(n_w)$	1	$O(1)$	$O(W \cdot d_{\max})$	II
Janus	×	$O(n_w \cdot d_w)$	$O(1)$	$O(n_w)$	1	$O(1)$	$O(W\log F)$	III
Janus++	×	$O(n_w \cdot d_{\max})$	$O(d_{\max})$	$O(n_w)$	1	$O(1)$	$O(W\log F)$	III
ROSA (Ours)	✓	$O(a_w - d_w)$	$O(\log^2 N)$	$O(n_w)$	1	$O(\log^2 N)$	$O(W \cdot d_{\max} + \log N)$	II

Comparisons with prior DSSE schemes