

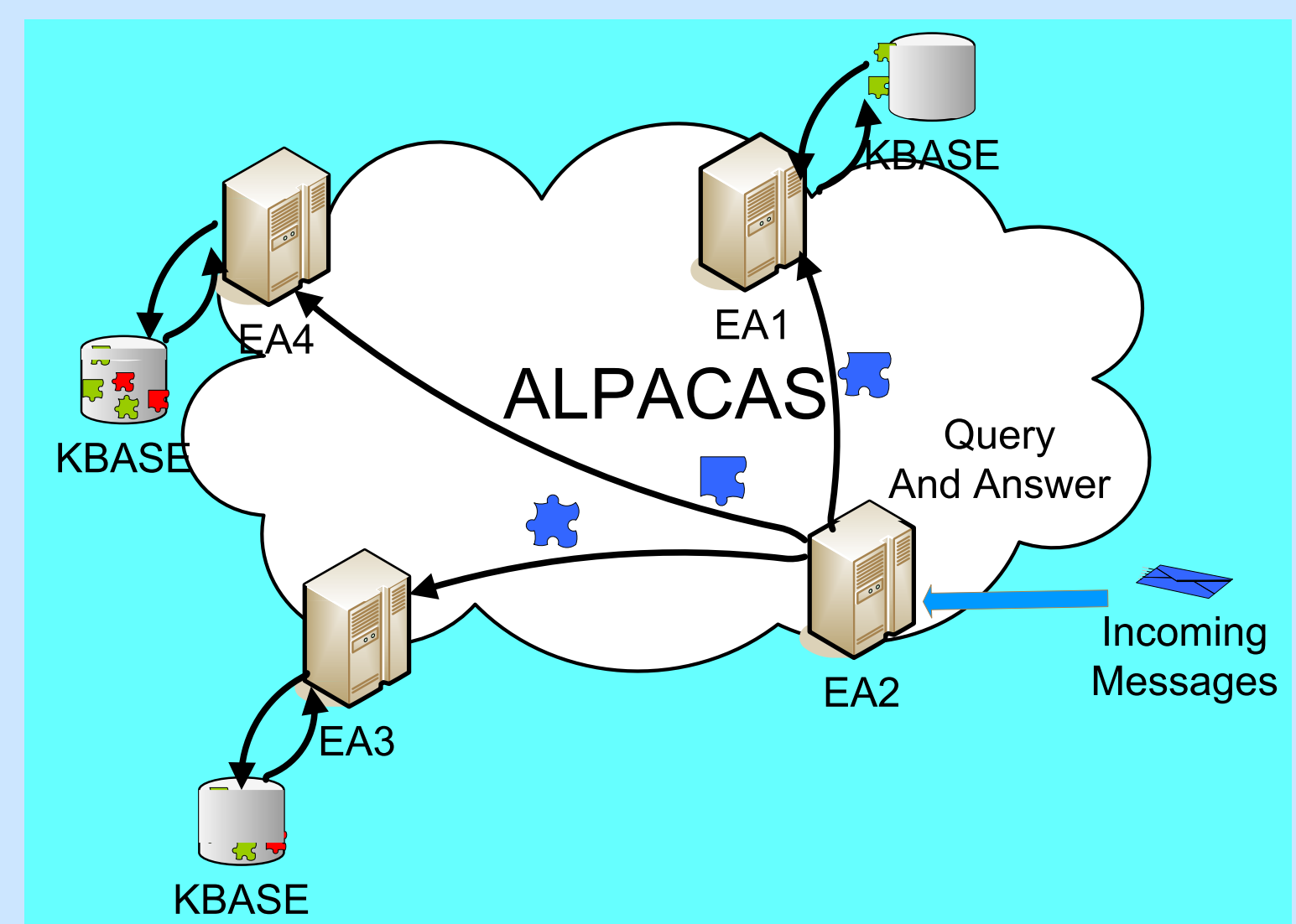


Privacy-Aware Collaborative Spam Filtering

Collaboration is a natural defense against spam attacks. However, any large-scale collaborative anti-spam approach is faced with a fundamental challenge, *ensuring the privacy of the messages among collaborative but untrusted users.*

Our Approach

- Design a cryptographic transformation that satisfies two competing requirements:
 - hide the actual content for privacy protection.
 - retain important features of the message so that effective similarity comparison can still be performed on the encrypted messages.
- Design a novel query-response protocol to avoid privacy breaches by minimizing the information revealed during the collaboration.



ALPACAS Collaborative System Overview

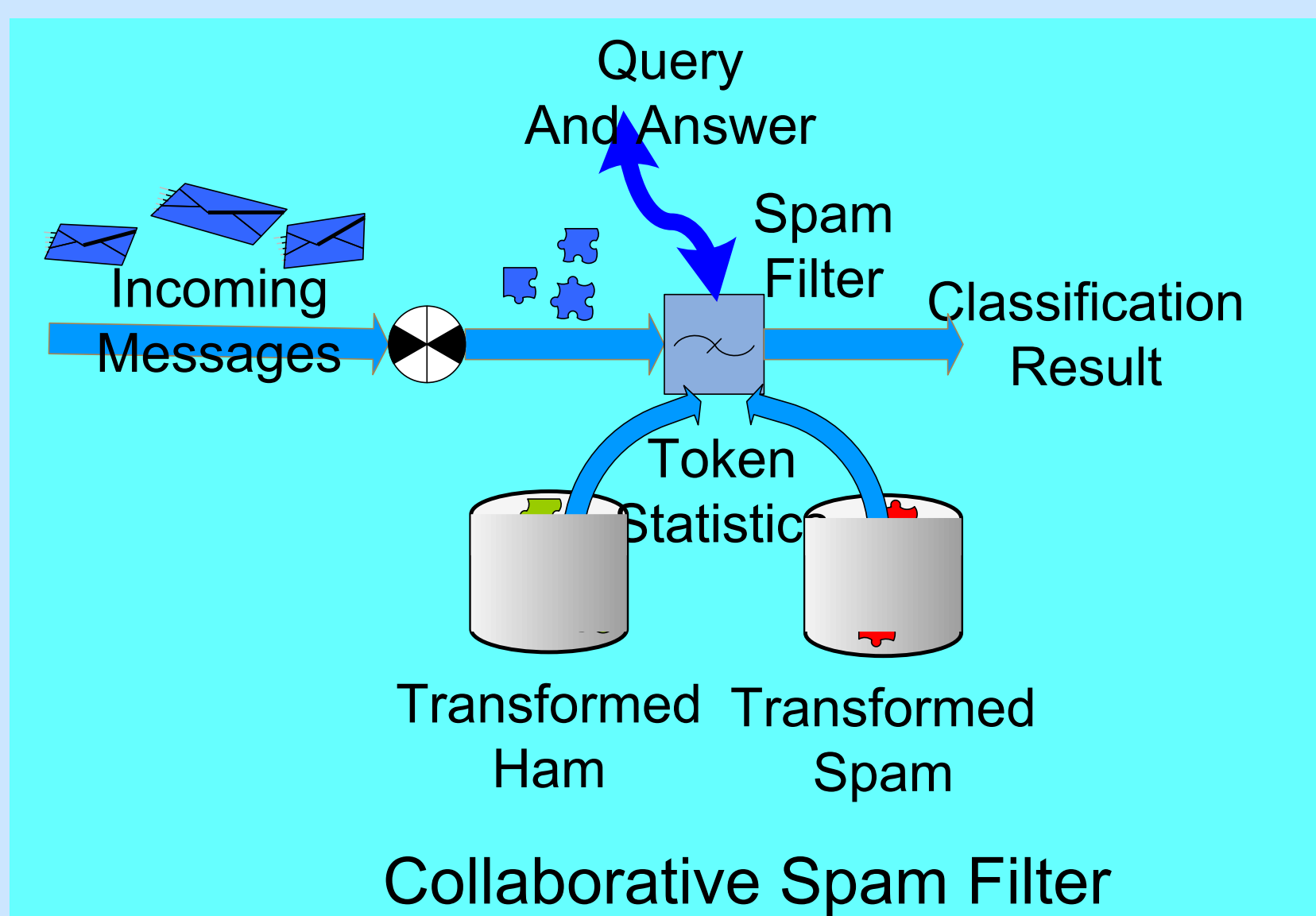
Approach and Impact

New approach

- Classification with shingle-based message digests
- Privacy-aware distributed query protocols

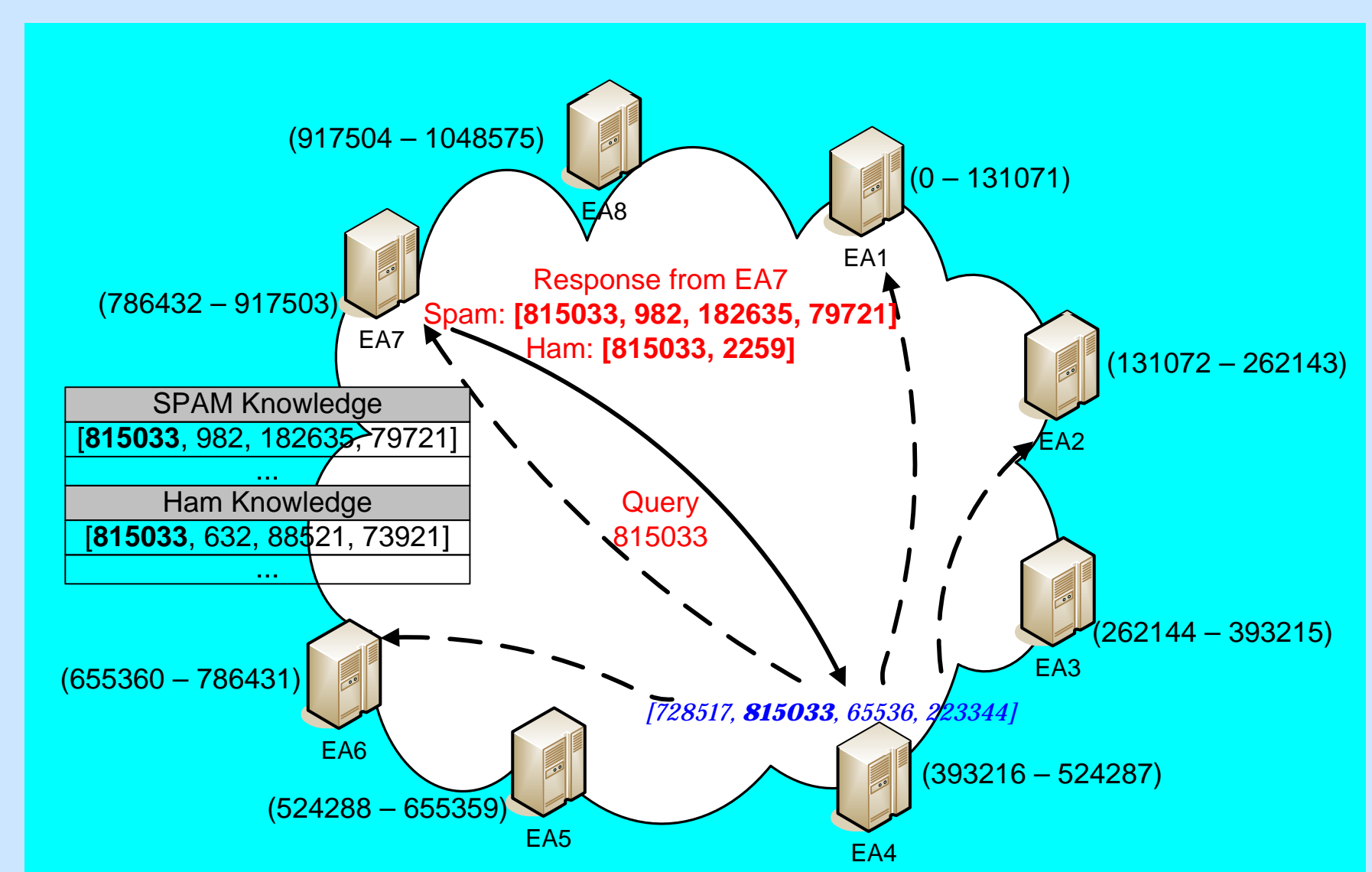
Research Impact

- Robust defense against camouflage attacks
- Metrics for privacy breach measurement in collaboration



Feature-preserving Transformation

- Shingle based message digests
 - Robust similarity detection even under camouflage attacks
- Message shuffle to prevent term-level privacy breaches



Privacy-aware Query Protocols

- Approximate Query
 - Partial digests and digest ranges
- Asymmetric Response
 - Spam/ham dichotomy: return entire spam digests but partial ham digests