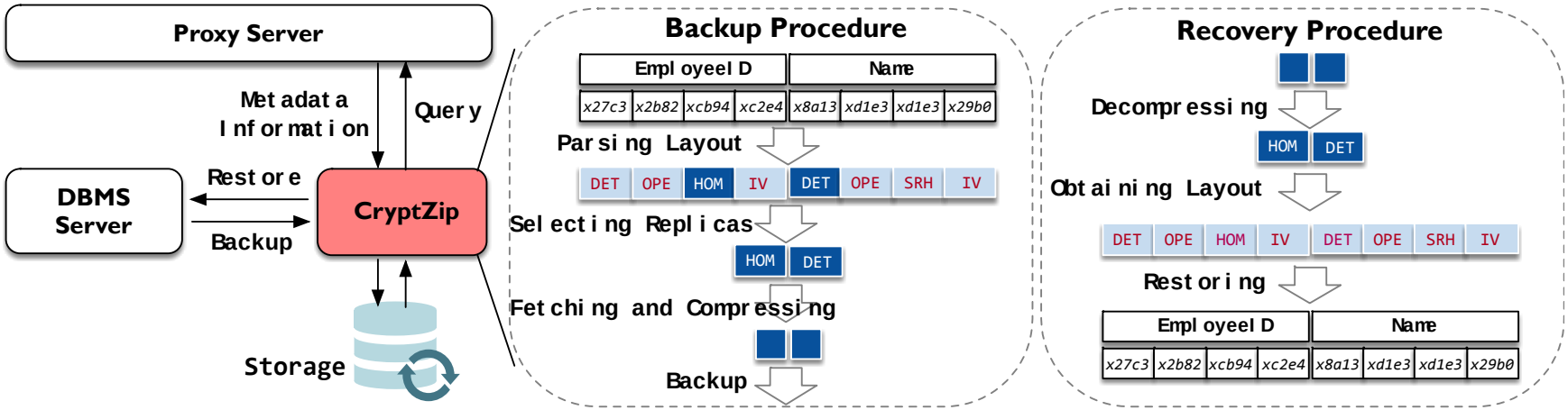
Practices of backuping homomorphically encrypted databases

Sa WANG, Yiwen SHAO, Yungang BAO

Frontiers of Computer Science, DOI: 10.1007/s11704-019-8394-8

Problems & Ideas

- Homomorphically encrypted databases **introduce great storage overhead when making backups**.
  - MySQLDump produces 21.3x storage cost on CryptDB.
- Ideas: Metadata-aware deduplication
  - Columns in CryptDB are replicated and encrypted for supporting varies SQL queries.
  - Insight: Leveraging the metadata information to deduplicate columns.



The backup and restore procedure of CryptZip

Main Contributions

Backup Strategy	Schemes		Storage Cost	Storage Ratio	Recovery Time	Time Ratio
	String	Integer				
MySQLDump	-	-	1680MB	-	244s	-
Space-Optimal Strategy	[DET]	[DET]	160MB	9.5%	26215s	107.4x
Time-Optimal Strategy	[DET,OPE, SRH]	[DET,HOM,OPE]	1368MB	81.4%	246s	1.008x
Balanced Strategy	[DET,OPE]	[DET,HOM]	1205MB	71.7%	1031s	4.23x

- The space-optimal strategy saves huge storage, but incurs significant recovery time.
- The time-optimal strategy only reduce 18.6% storage.
- The balanced strategy is not *that* balanced.