VLDB: Privacy and Security

A Comparative Evaluation of Order-Revealing Encryption Schemes and Secure Range-Query Protocols

by **Dmytro Bogatov**, George Kollios and Leonid Reyzin

[BKR19] (PVLDB 2019)

Dmytro Bogatov
dmytro@dbogatov.org

Built from *71921593* on June 6, 2020

Boston University

Secure Range Queries

The problem

- Many different solutions
- Understanding performance / security tradeoff
- Heterogeneous security definitions and leakage profiles
- **Performance not well-understood**
  - Some constructions were not even implemented
  - Most constructions have at most prototype implementation
  - Most of them were not benchmarked against one another
  - Constructions use different primitive implementations

Secure Range Queries

The solution

- Analysed security and leakages of the constructions under a common framework
- Analysed theoretically performance of the constructions
- **Implemented and run experiments**
    - Implemented 5 OPE / ORE schemes and 5 range query protocols
    - Used same language, framework and primitive implementations
    - Benchmarked primitives execution times
    - Simulated insertion and query stages of all protocols
        - OPE / ORE schemes use our implementation of B^+ tree
    - Used different data sizes and distributions, query loads, cache policies and parameters of the constructions

OPE / ORE schemes

Scheme
BCLO [Bol+09]
CLWW [Che+16]
Lewi-Wu [LW16]
CLOZ [Cas+18]
FH-OPE [Ker15]

OPE / ORE schemes

Scheme	Primitive usage		Ciphertext size,	Leakage
	Encryption	Comparison	or state size	(In addition to inherent total order)
BCLO [Bol+09]				
CLWW [Che+16]				
Lewi-Wu [LW16]				
CLOZ [Cas+18]				
FH-OPE [Ker15]				

OPE / ORE schemes

Scheme	Primitive usage		Ciphertext size,	Leakage
	Encryption	Comparison	or state size	(In addition to inherent total order)
BCLO [Bol+09]	**n HG**	none	$2n$	**$\approx$ Top half of the bits**
CLWW [Che+16]	n PRF	none	$2n$	**Most-significant differing bit**
Lewi-Wu [LW16]	**${}^{2n}/_{d}$ PRP** $2\frac{n}{d}\left(2^d+1\right)$ PRF $\frac{n}{d}2^d$ Hash	$\frac{n}{2d}$ Hash	$\frac{n}{d}\left(\lambda+n+2^{d+1}\right)+\lambda$	Most-significant differing block
CLOZ [Cas+18]	n PRF n PPH 1 PRP	**n^2 PPH**	$n \cdot h$	Equality pattern of most-significant differing bit
FH-OPE [Ker15]	1 Traversal	3 Traversals	$\mathbf{3 \cdot n \cdot N}$	Insertion order

Range query protocols

Protocol
B^+ tree with ORE
Kerschbaum [KT17]
POPE [Roc+16] warm
POPE [Roc+16] cold
Logarithmic-BRC [Dem+16]
ORAM

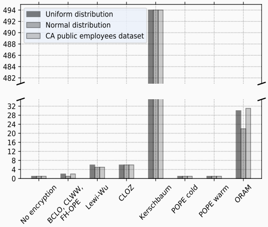
Range query protocols

Protocol	I/O requests		Leakage	Communication (result excluded)	
	Construction	Query		Construction	Query
B+ tree with ORE					
Kerschbaum [KT17]					
POPE [Roc+16] warm					
POPE [Roc+16] cold					
Logarithmic-BRC [Dem+16]					
ORAM					

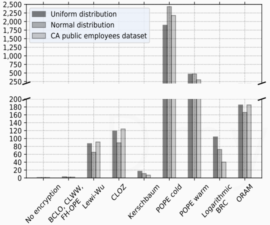
Range query protocols

Protocol	I/O requests		Leakage	Communication (result excluded)	
	Construction	Query		Construction	Query
B⁺ tree with ORE	$\log_B \frac{N}{B}$	$\log_B \frac{N}{B} + \frac{r}{B}$	**Same as ORE**	1	1
Kerschbaum [KT17]	$\mathbf{\frac{N}{B}}$	$\log_2 \frac{N}{B} + \frac{r}{B}$	**Total order**	$\log_2 N$	$\log_2 N$
POPE [Roc+16] warm	1	$\log_L \frac{N}{B} + \frac{r}{B}$	**Partial order**	1	$\log_L N$
POPE [Roc+16] cold		$\mathbf{N/B}$	Fully hiding		$\mathbf{N}$
Logarithmic-BRC [Dem+16]	—	$\mathbf{r}$	Same as SSE	—	$\log_2 N$
ORAM	$\mathbf{\log^2 \frac{N}{B}}$	$\mathbf{\log_2 \frac{N}{B} \left(\log_B \frac{N}{B} + \frac{r}{B}\right)}$	Fully hiding (access pattern)	$\mathbf{\log^2 \frac{N}{B}}$	$\mathbf{\log^2 \frac{N}{B}}$

Simulation results

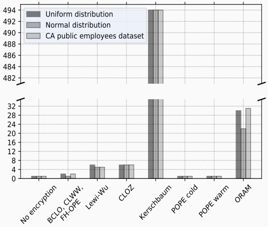


Construction stage number of I/O requests

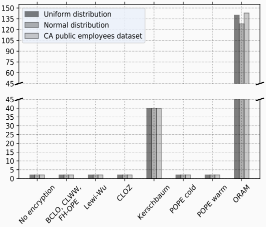


Queries stage number of I/O requests

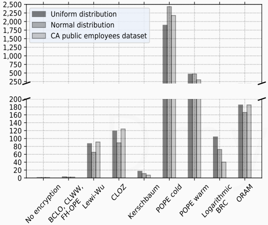
Simulation results



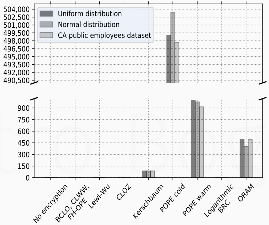
Construction stage number of I/O requests



Construction stage communication volume (number of messages)

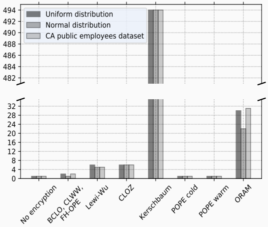


Queries stage number of I/O requests

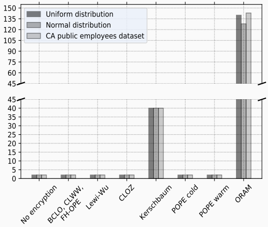


Queries stage communication volume (number of messages)

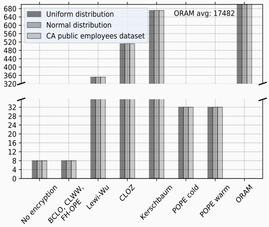
Simulation results



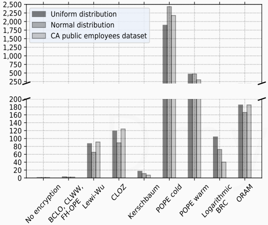
Construction stage number of I/O requests



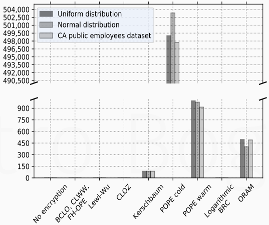
Construction stage communication volume (number of messages)



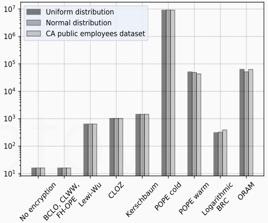
Construction stage communication size (bytes transferred)



Queries stage number of I/O requests



Queries stage communication volume (number of messages)



Queries stage communication size (bytes transferred, log scale)

Conclusions

- Strengths, weaknesses and use cases for each construction
- Ranked by security and performance
- Bugs in algorithms
- Security vulnerabilities in implementations
- Positive performance results for ORAM with B^+ tree, and Logarithmic-BRC

VLDB: Privacy and Security

A Comparative Evaluation of Order-Revealing Encryption Schemes and Secure Range-Query Protocols

by **Dmytro Bogatov**, George Kollios and Leonid Reyzin

[BKR19] (PVLDB 2019)

Dmytro Bogatov
dmytro@dbogatov.org

Built from *71921593* on June 6, 2020

Boston University

References i

- Alexandra Boldyreva *et al.* “Order-Preserving Symmetric Encryption”. In: *Advances in Cryptology - EUROCRYPT 2009*. Springer Berlin Heidelberg, 2009, pp. 224–241.

- Florian Kerschbaum. “Frequency-Hiding Order-Preserving Encryption”. In: *Proceedings of the 22Nd ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2015, pp. 656–667.

- Nathan Chenette *et al.* “Practical Order-Revealing Encryption with Limited Leakage”. In: *Fast Software Encryption*. Springer Berlin Heidelberg, 2016, pp. 474–493.

- Ioannis Demertzis *et al.* “Practical Private Range Search Revisited”. In: ACM, 2016, pp. 185–198.

- Kevin Lewi and David J. Wu. “Order-Revealing Encryption: New Constructions, Applications, and Lower Bounds”. In: ACM, 2016, pp. 1167–1178.

References ii

- Daniel S. Roche *et al.* “POPE: Partial Order Preserving Encoding”. In: *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2016, pp. 1131–1142.

- Florian Kerschbaum and Anselme Tueno. “An Efficiently Searchable Encrypted Data Structure for Range Queries”. In: *arXiv preprint arXiv:1709.09314* (2017).

- David Cash *et al.* “Parameter-Hiding Order Revealing Encryption”. In: *Advances in Cryptology – ASIACRYPT 2018*. Springer International Publishing, 2018, pp. 181–210.

- Dmytro Bogatov, George Kollios, and Leonid Reyzin. “A Comparative Evaluation of Order-Revealing Encryption Schemes and Secure Range-Query Protocols”. In: *PVLDB* 12.8 (2019), pp. 933–947.