Efficient Confidentiality - Preserving Data Analytics over Symmetrically Encrypted Datasets

Authors: Savvas Savvides, Darshika Khandelwal, Patrick Eugster

Presenter: Antonis Louca

Πανεπιστήμιο Κύπρου

01
Introduction

Πανεπιστήμιο Κύπρου

Motivation - Cloud computing

Economical and practical for computations

Used by corporations and governments

Computations can contain sensitive data that are moved to the cloud

Trust in the third-party cloud provider

Confidentiality concerns

Homomorphic encryption is used to mitigate concerns

Πανεπιστήμιο Κύπρου

Motivation - Homomorphic encryption

Form of encryption to **allow computation on encrypted data without decryption**

Fully homomorphic encryption (FHE). Offers arbitrary operations but with high performance overhead

Partially Homomorphic encryption (PHE). Individual operations like addition, subtraction

PHE uses asymmetric and symmetric approaches that sacrifice expressiveness

Property preserving Encryption (PPE)
Create ciphertexts that preserve a property of the plaintext

Symmetria is suggested to solve problems of previous approaches, and performance overhead

Πανεπιστήμιο Κύπρου

Contributions

- Design and evaluate a system that employs the proposed schemes
    - Propose symmetric additive homomorphic encryption (**SAHE**)
        - method for additions and other operations in encrypted data
    - Propose symmetric multiplicative homomorphic encryption (**SMHE**)
        - method for multiplications and other operations over encrypted data
- Introduce compaction techniques

Πανεπιστήμιο Κύπρου

02
Background

Πανεπιστήμιο
Κύπρου

Background - Homomorphic encryption

- When Ciphertexts are altered → plaintexts are altered in predictable way
- The **decryption of the result** when the operation is performed **with encrypted data yields** the **same result** as **with** the **plaintext** data
  - dec(enc(m1) + enc(m2)) = m1 + m2
  - dec(enc(m1) χ enc(m2)) = m1 × m2
- <u>Paillier</u> uses AHE which takes an <u>asymmetric</u> approach
- <u>ASHE</u> is a <u>symmetric</u> approach for <u>addition</u> operations <u>only</u>

Πανεπιστήμιο Κύπρου

Background - PPE

- Schemes that preserve properties of the plaintext.
  - Allow certain operations (equality, order)
- Deterministic Encryption (DE):
  - Supports **equality comparisons** – same plaintext always yields same ciphertext
- Order preserving encryption (**OPE**):
  - **Order comparison** on encrypted data

Πανεπιστήμιο Κύπρου

Background - SAHE

- Symmetric additive homomorphic encryption (**SAHE**)
  - Consider message **m** and the abelian additive group Z_N
  - **Ciphertext** format is a **triplet of <v, lp, ln >**
    - v is the obfuscated value
    - lp: list of ids that generate random element in the group that is **added to m**
    - ln: list of ids that generate random element in the group that is **subtracted from m**

Πανεπιστήμιο Κύπρου

Background - SMHE

- Symmetric multiplicative homomorphic encryption (**SMHE**)
  - Consider message **m**, the abelian multiplicative group Z^*_N
  - **g** a generator element of the group
  - **Ciphertext** format is a **triplet of <v, lp, ln >**
    - v is the obfuscated value
    - lp: list of ids that generate random element in the group that is **raised to the power of g and multiplied by m**
    - ln: list of ids that generate random element in the group that is **raised to the power of g, then it is inverted and multiplied by m**

Πανεπιστήμιο Κύπρου

Background - Compaction Techniques

Lp and Ln list size grows and reduces performance

List aggregation

lp = [r1 , r2 , r3], ln = [r1 , r4] ⇒
lp = [r2 , r3], ln = [r4]

Id grouping

[r1 , r1 , r1 , r2] ⇒ [3 : r1 , r2]

Range folding

[2, 3, 4, 5, 8] ⇒ [2 − 5, 8]

Telescoping

Change encryption functions to use 2 PRNs that when added to lp and ln will cancel each other out

Integer list compression

Integer array compression, ids are stored in non-decreasing order. And chosen incrementally

Πανεπιστήμιο Κύπρου

03

Symmetria Design

Πανεπιστήμιο Κύπρου

Symmetria Design - Threat Model

- Preserve **confidentiality** in semi-honest / **honest-but-curious environment**
- The adversary has **access** to all cloud nodes, and can observe data and queries
- **Adversary does not**
  - **Change** queries or data stored in the cloud
  - **Interfere** with the results
- Attacks that target integrity or availability of the system are out of scope
  - Like side-channel attacks

Πανεπιστήμιο Κύπρου

Symmetria Design - Operations

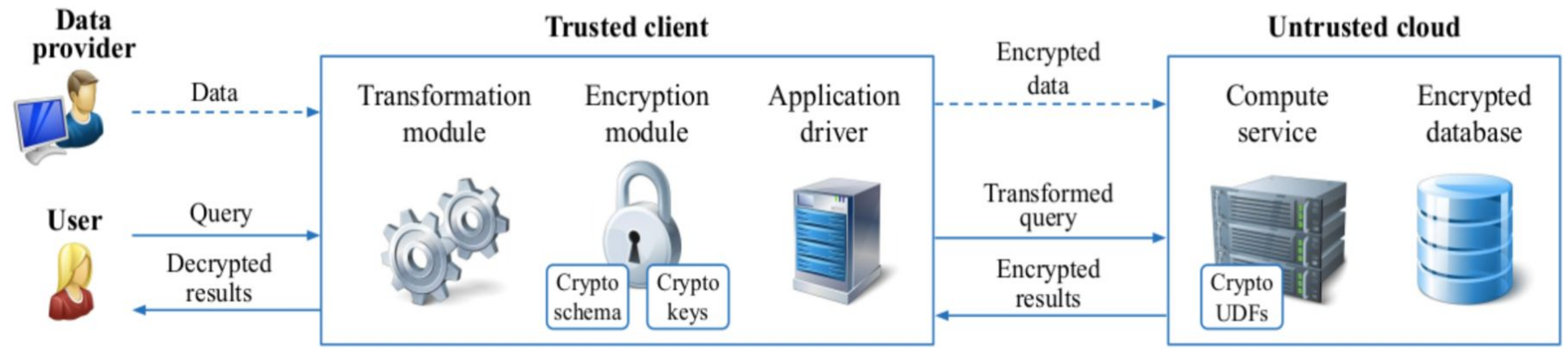


Figure 1: Symmetria system architecture. Dashed arrows indicate setup phase. Solid arrows indicate query execution phase.

Πανεπιστήμιο Κύπρου

Symmetria Design - Implementation

- Java
- AES as PRF
- **AES** Symmetric encryption (ECB mode)
- **Extending Apache spark** classes on the trusted node to create the transformation module
- **Unmodified Apache spark** service on the cloud

Πανεπιστήμιο Κύπρου

04
Evaluation

Πανεπιστήμιο Κύπρου

Evaluation - Setup

- 3 system setups
  - **Plaintext**:
    - Setup without encryption and confidentiality guarantees
  - **Symmetria**:
    - SAHE and SMHE schemes for arithmetic operations
  - **Asym**:
    - Setup with asymmetric schemes (Paillier, ElGamal) for operations
- Benchmarks:
  - **TPC-H**: decision support benchmark (22 queries)
  - **TPC-DS**: big data decision solutions (100 queries)

Πανεπιστήμιο Κύπρου

Evaluation - Expressiveness comparison

Table 4: Expressiveness comparison. *Type* indicates whether a scheme is symmetric (sym) or asymmetric (asym).

(a) AHE

	Paillier	ASHE	SAHE
Type	asym	sym	sym
add	✓	✓	✓
adp	✓	✗	✓
mlp	✓	✗	✓
neg	✓	✗	✓
sub	✓	✗	✓

(b) MHE

	ElGamal	SMHE
Type	asym	sym
mul	✓	✓
mlp	✓	✓
pow	✓	✓
inv	✓	✓
div	✓	✓

Πανεπιστήμιο Κύπρου

Evaluation - Execution times

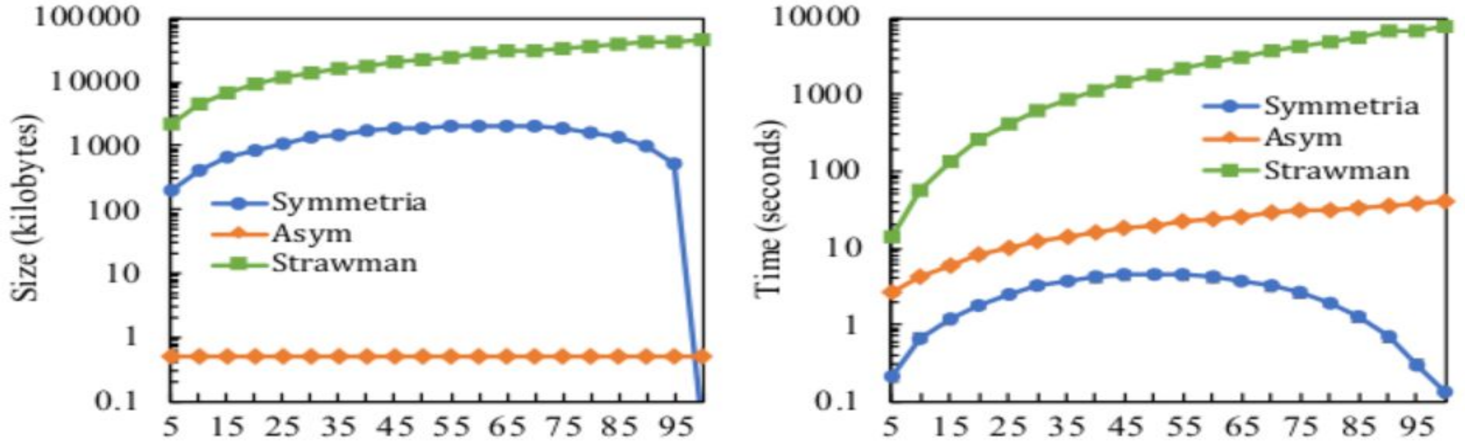
Table 5: Operation execution times of SAHE and SMHE compared to asymmetric schemes. All reported times are given in *nanoseconds* followed by the *relative standard error*. Values in parentheses indicate pre-computation.

	Paillier	Packed Paillier	SAHE
enc	17285376 ± 0.13%	880921 ± 0.11%	1321 (63) ± 1.43%
dec	16390295 ± 0.01%	781727 ± 0.01%	1202 (153) ± 4.18%
add	34807 ± 1.37%	1666 ± 1.21%	457 ± 3.10%
adp	917141 ± 2.38%	104775 ± 0.95%	71 ± 0.37%
mlp	857943 ± 2.54%	–	406 ± 0.18%
neg	1370859 ± 0.07%	–	397 ± 0.11%
sub	1408870 ± 0.08%	–	819 ± 3.88%

	ElGamal	SMHE
enc	8700278 ± 0.04%	2974 (752) ± 0.29%
dec	4768193 ± 0.02%	3090 (1420) ± 0.23%
mul	25803 ± 0.16%	419 ± 0.92%
mlp	678 ± 1.17%	371 ± 0.11%
pow	505675 ± 2.53%	2856 ± 0.37%
inv	809711 ± 0.09%	3529 ± 0.24%
div	841260 ± 0.14%	4172 ± 0.25%

Πανεπιστήμιο Κύπρου

Evaluation - Effect of non-compactness



(a) Ciphertext size **(b)** Execution time

Figure 2: Summation of 1 million rows as sampling size (x-axes) changes from 5% to 100%, with y-axes in log scale.

Πανεπιστήμιο Κύπρου

Evaluation - Encryption Overhead

Table 6: Encryption overheads. `Plaintext` (text) indicates uncompressed data. All other setups use Parquet to store compressed data. Time column refers to compression time for `Plaintext`, and adds encryption time for other setups.

Benchmark	System setup	Size	Time
TPC-H	Plaintext (text)	106.8 GB	–
	Plaintext	34.0 GB	2.4 min
	Asym	363.7 GB	84 min
	Symmetria	67.8 GB	14 min
TPC-DS	Plaintext (text)	38.6 GB	–
	Plaintext	15.1 GB	1.5 min
	Asym	482.4 GB	228 min
	Symmetria	39.7 GB	4 min

Πανεπιστήμιο Κύπρου

Evaluation - End-to-end Slowdown Factor

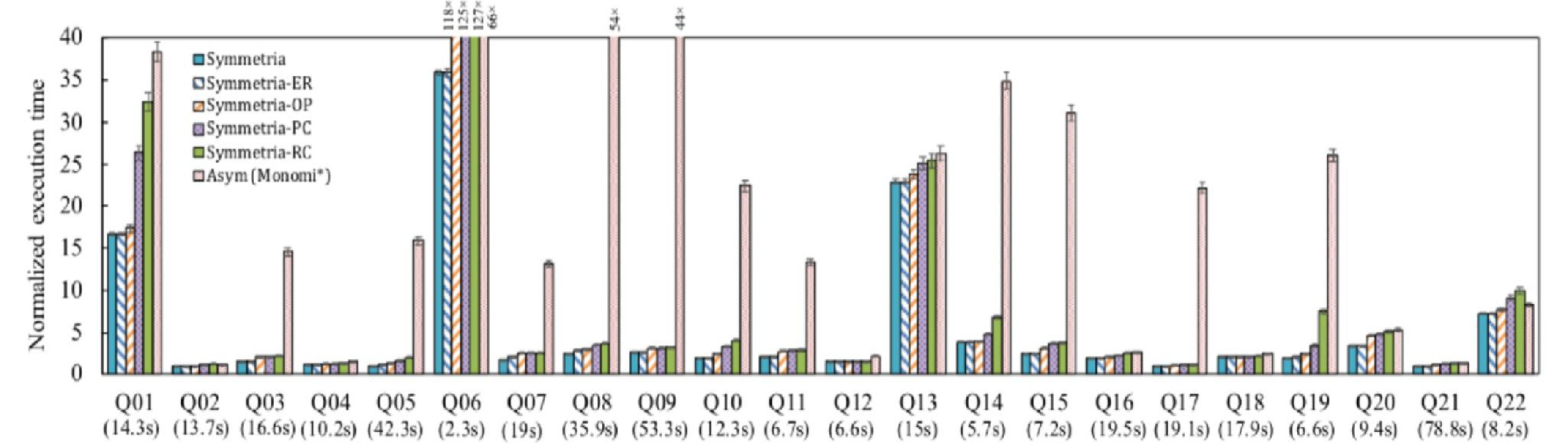


Figure 3: TPC-H end-to-end execution times normalized to `Plaintext` execution (slowdown factor)

Πανεπιστήμιο Κύπρου

Evaluation - End-to-end Slowdown Factor

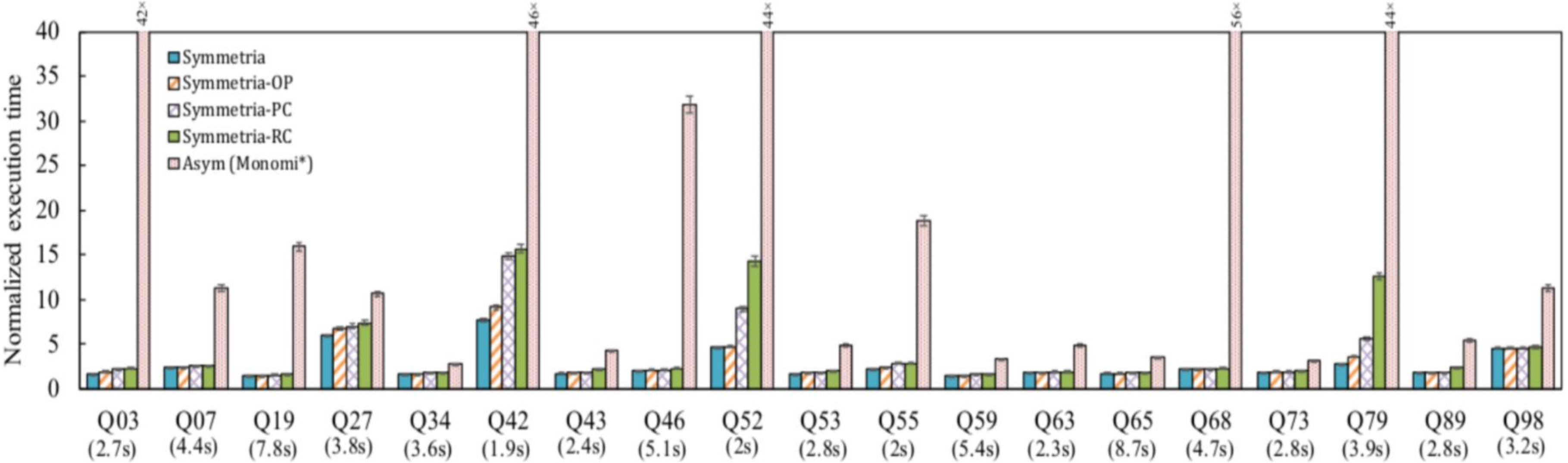


Figure 4: TPC-DS (subset) end-to-end execution times normalized to `Plaintext` execution (slowdown factor)

Πανεπιστήμιο
Κύπρου

Conclusions

- **Symmetria**
  - with <u>all compaction techniques</u> and <u>query optimizations enabled</u> is
    - **3.8× faster** on **TPC-H** queries
    - **7× faster** on **TPC-DS** queries
  - **than** the **state-of-the-art asymmetric PHE-based systems**
- Authors Symmetria improvements:
  - Adopting more recent PPE schemes
  - Stronger security models
  - Combining proposed schemes with techniques like **ORAM**
    - To prevent active attacks

Πανεπιστήμιο Κύπρου

Thank you for your attention

Any Questions?

Πανεπιστήμιο
Κύπρου