RGC Ref. No.:
UGC/FDS14/E03/17
(please insert ref. above)

RESEARCH GRANTS COUNCIL
COMPETITIVE RESEARCH FUNDING SCHEMES FOR THE LOCAL SELF-FINANCING DEGREE SECTOR

FACULTY DEVELOPMENT SCHEME (FDS)

Completion Report
(for completed projects only)

Submission Deadlines:
1. *Auditor's report with unspent balance, if any: within **six** months of the approved project completion date.*
2. *Completion report: within **12** months of the approved project completion date.*

Part A: The Project and Investigator(s)

1. Project Title

Optimizing Analytics Processing in Encrypted Database Systems

2. Investigator(s) and Academic Department(s) / Unit(s) Involved

Research Team	**Name / Post**	**Unit / Department / Institution**
Principal Investigator	Dr. Wong Wai Kit, Assistant Professor	Department of Computing, The Hang Seng University of Hong Kong
Co-Investigator(s)	Dr. Chris Ma Yu Tak, Assistant Professor	Department of Computing, The Hang Seng University of Hong Kong
Others		

3. Project Duration

	Original	**Revised**	**Date of RGC / Institution Approval** *(must be quoted)*
Project Start Date	1 Jan 2018		
Project Completion Date	31 Dec 2020		
Duration *(in month)*	36		
Deadline for Submission of Completion Report	31 Dec 2021		

Part B: The Final Report

5. Project Objectives

5.1 Objectives as per original application

- Integrate progressive query processing into EDBMS for answering analytical queries.
- Develop indexing structure to support efficient computation of analytical queries, including aggregate queries (e.g., COUNT, SUM, MEDIAN), top-k queries.
- Develop encryption method to support efficient computation of approximate aggregate result.
- Extend the developed methods to support efficient interactive online analytical processing (OLAP).
- Prove the security of developed algorithms.
- Perform theoretical and empirical analysis on the performance of the developed methods.

5.2 Revised objectives

Date of approval from the RGC: ________________________________

Reasons for the change: ________________________________

____

N/A

5.3 Realisation of the objectives

(Maximum 1 page; please state how and to what extent the project objectives have been achieved; give reasons for under-achievements and outline attempts to overcome problems, if any)

The methods stated in objectives #1, 2, 3, 4 were developed. Security analysis of the methods (Objective #5) was completed. Experiments were designed and conducted (Objective #6). The results were documented.

We prepared a paper about our results for publishing in a respected journal/conference. We were not successful so far. The PI has now left academia. The publication work is ceased.

The latest draft of the paper that were being worked on is attached (Annex I) for reference.

5.4 Summary of objectives addressed to date

Objectives *(as per 5.1/5.2 above)*	**Addressed** *(please tick)*	**Percentage Achieved** *(please estimate)*
Integrate progressive query processing into EDBMS for answering analytical queries.	√	100%
Develop indexing structure to support efficient computation of analytical queries, including aggregate queries (e.g., COUNT, SUM, MEDIAN), top-k queries.	√	100%
Develop encryption method to support efficient computation of approximate aggregate result.	√	100%
Extend the developed methods to support efficient interactive online analytical processing (OLAP).	√	100%
Prove the security of developed algorithms	√	100%
Perform theoretical and empirical analysis on the performance of the developed methods.	√	100%

6. Research Outcome

6.1 Major findings and research outcome
(Maximum 1 page; please make reference to Part C where necessary)

We developed the algorithms as planned.

6.2 Potential for further development of the research and the proposed course of action *(Maximum half a page)*

There was new development in the community on secure database system, e.g., in-memory database systems. More research work is needed to integrate secure database system with these state-of-the-art techniques.

As the PI has left academia, there is no proposed course of action for the team.

7. Layman's Summary

(Describe in layman's language the nature, significance and value of the research project, in no more than 200 words)

Data confidentiality is an important concern in database-as-a-service (DBaaS) model. The cloud server should not see users' plain data. Data should be encrypted before they are stored in cloud database. Query computation over encrypted data is then not straight-forward. Secure algorithms were developed in Encrypted Database Systems (EDBMS) to allow the server to observe the selection result without knowing information about plain data, i.e., achieving data confidentiality. As a trade-off for security, these algorithms are significantly slower. To reduce the cost and make EDBMS more practical, our idea is to make use of what the server has already seen during the usual of EDBMS. We have developed two optimization techniques. The first one is Past Result Knowledge Base (PRKB), where the server extracts information from past selection results and use the information to optimize the processing of selection queries. The second one is progressive query processing technique for post-selection aggregation on encrypted data. Security of our techniques are ensured as they operate solely on the server. Experiment results show that our techniques can save processing cost by orders of magnitudes.

Part C: Research Output

8. Peer-Reviewed Journal Publication(s) Arising Directly From This Research Project

(Please attach a copy of the publication and/or the letter of acceptance if not yet submitted in the previous progress report(s). All listed publications must acknowledge RGC's funding support by quoting the specific grant reference.)

The Latest Status of Publications				Author(s) *(denote the corresponding author with an asterisk*)*	Title and Journal / Book *(with the volume, pages and other necessary publishing details specified)*	Submitted to RGC *(indicate the year ending of the relevant progress report)*	Attached to this Report *(Yes or No)*	Acknowledged the Support of RGC *(Yes or No)*	Accessible from the Institutional Repository *(Yes or No)*
Year of Publication	Year of Acceptance *(For paper accepted but not yet published)*	Under Review	Under Preparation *(optional)*						
	N/A								

9. Recognized International Conference(s) In Which Paper(s) Related To This Research Project Was / Were Delivered

(Please attach a copy of each conference abstract)

Month / Year / Place	Title	Conference Name	Submitted to RGC *(indicate the year ending of the relevant progress report)*	Attached to this Report *(Yes or No)*	Acknowledged the Support of RGC *(Yes or No)*	Accessible from the Institutional Repository *(Yes or No)*
	N/A					

10. Whether Research Experience And New Knowledge Has Been Transferred / Has Contributed To Teaching And Learning

(Please elaborate)

N/A

11. Student(s) Trained

(Please attach a copy of the title page of the thesis)

Name	Degree Registered for	Date of Registration	Date of Thesis Submission / Graduation
N/A			

12. Other Impact

(e.g. award of patents or prizes, collaboration with other research institutions, technology transfer, teaching enhancement, etc.)

N/A

13. Statistics on Research Outputs

	Peer-reviewed Journal Publications	Conference Papers	Scholarly Books, Monographs and Chapters	Patents Awarded	Other Research Outputs (please specify)	
No. of outputs arising directly from this research project	0	0	0	0	Type	No.
					0	0

14. Public Access Of Completion Report

(Please specify the information, if any, that cannot be provided for public access and give the reasons.)

Information that Cannot Be Provided for Public Access	**Reasons**
Nil	