Accelerate the Paillier Cryptosystem in CryptDB by Chinese Remainder Theorem

Liu Yao*, Xue Shuai*

*Shanghai Key Lab of Scalable Computing and System, Shanghai Jiao Tong University, China

liuyao@sjtu.edu.cn, mattxue_sjtu@sjtu.edu.cn

***Abstract*—CryptDB is an encrypted database management system which was proposed by CSAIL Lab of MIT. It can ensure the privacy of private data by executing SQL queries on the encrypted data. However, some encryption algorithms used in CryptDB might be time-consuming. Homomorphic encryption (HOM) is a secure probabilistic encryption scheme, and in CryptDB, the author implemented HOM by Paillier Cryptosystem, which is a probabilistic asymmetric algorithm for public key cryptography. Due to the complex computation, Paillier has become a bottleneck of the system performance. In this paper, we use Chinese Remainder Theorem(CRT) to accelerate the process of encryption. And results show that our method improve the performance of cryptDB under certain condition.**

***Keyword*—Database, Security, Privacy, CryptDB, Encryption, CRT, Paillier Cryptosystem**

Liu Yao received the B.S. degree in software engineering from Southeast University in 2015. She is now studying in the school of computer science and technology in Shanghai Jiao Tong University, Shanghai, China. Her research interests are mainly focused on encrypted databases, cloud computing, hardware acceleration, high availability.

Xue Shuai received the B.S. degree in software engineering from Huazhong University of Science and Technology in 2015. He currently purses the M.S. degree in the school of software engineering in Shanghai Jiao Tong University, Shanghai, China. His research interests are mainly focused on hardware-assisted virtualization, cloud computing, hardware acceleration, Internet of things, and distributed in-memory databases.