Fully Homomorphic Encryption Scheme that Secures Clouds and Blockchains

(2018-004)

Fully Homomorphic Encryption method that allows for data stored in the cloud to remain encrypted and secure during research.

Market Overview

This fully homomorphic encryption method allows for users of cloud storage platforms to retrieve encrypted information or data without having first to decrypt the data, reducing the risk of exposing sensitive data. Hackers have broken into preexisting encrypted clouds, accessing the personal data of millions of people worldwide. In 2021, data breach costs reached $4.35 million, hitting a record high, and are continually increasing. With preexisting encryption technologies, data cannot be searched without decrypting it first, which puts it at a higher risk of being accessed by malicious parties. Fully homomorphic encryption schemes solve this issue by eliminating the need to decrypt data to search it, and currently, there are no practical FHE schemes. According to market analysis, the fully homomorphic encryption market expects to grow at a rate of 7.50% from 2021 to 2028 to reach 437.30 million USD. A Clemson University researcher has developed a fully homomorphic encryption (FHE) method that allows data to be searched while remaining encrypted, reducing the risk of access for unauthorized parties.

Technical Summary

As distributed computing becomes increasingly popular, there is an urgent need to protect the privacy of massive sensitive data stored in clouds and blockchains. The traditional encryption schemes can only allow searching on encrypted data with decryption first. The fully homomorphic encryption method is a practical encryption scheme that protects the privacy of massive amounts of sensitive data stored in clouds, blockchains, and company databases. In addition, the FHE scheme allows for all possible searched to be performed in encrypted form and decrypted only by the data owner.

Application

The disclosure is a fully homomorphic encryption scheme that protects the privacy of sensitive data stored in untrusted storage (e.g. clouds, blockchains, company data bases), but still allows searching directly on encrypted data without decryption.

Development Stage

TRL 6: Fully functional prototype

Advantages

- Data is encrypted with a private key, eliminating access for users without the private key
- Data encryption has a much smaller ciphertext expansion, reducing the total file size
- All search functions can be performed with this method, allowing information to be found in encrypted form

App Type	Country	Serial No.	Patent No.	CURF Ref. No.	Inventors
Utility	United States	62/687,681	11,374,736	2018-004	Dr. Shuhong Gao

About the Inventors

Dr. Shuhong Gao

Professor in the Department of Mathematical Sciences at Clemson University

Dr. Shuhong Gao is a Rodger Adger Bowen Professor in the Clemson University Department of Chemistry. He earned his Ph.D. in Combinatorics and Optimization from the University of Waterloo in Ontario, Canada. From 1993-1995, Dr. Gao was a postdoctoral fellow in computer science at the University of Toronto. Dr.Gao currently serves on the Editorial Board of the international journal Finite Fields and Their Applications. He has authored and co-authored over 50 scholarly articles and two books on cryptology. Dr. Gao's research focuses on cryptography, finite fields, symbolic computational, and quantum computation.

For more information on this technology contact:

curf@clemson.edu

Please put technology ID in subject line of email.