Docket #: S10-404

Fully Homomorphic Encryption Method, Program, and Apparatus

Stanford has patented a fully homomorphic encryption (FHE) method, computer program, and apparatus that grant the ability to outsource data processing without giving away access to the data. FHE keeps data private, but allows a worker that does not have the secret decryption key to compute (still encrypted) result of the data, even when the function of the data is very complex. In short, a third party can perform complicated processing of data without being able to see the data, making cloud computing compatible with privacy.

Applications

- Data encryption, processing, and cloud computing

Advantages

- Keeps data private while outsourcing the data processing
- Makes cloud computing compatible with privacy

Publications

- Gentry, Craig. "Computing arbitrary functions of encrypted data." *Communications of the ACM* 53.3 (2010): 97-105. https://crypto.stanford.edu/craig/easy-fhe.pdf
- Gentry, Craig. *A Fully Homomorphic Encryption Scheme*. 2009. Stanford University PhD Dissertation. https://crypto.stanford.edu/craig/craig-thesis.pdf
- Van Dijk, Marten, Craig Gentry, Shai Halevi, and Vinod Vaikuntanathan. "Fully homomorphic encryption over the integers." In Annual International Conference

on the Theory and Applications of Cryptographic Techniques, pp. 24-43. Springer, Berlin, Heidelberg, 2010. https://link.springer.com/content/pdf/10.1007/978-3-642-13190-5_2.pdf
- "Craig Gentry wins dissertation award -Encryption that allows privacy and access to co-exist earns top dissertation award." Stanford Engineering News. 1 August 2010. https://engineering.stanford.edu/news/craig-gentry-wins-dissertation-award
- Gentry, Craig B. "Bootstrappable homomorphic encryption method, computer program and apparatus." U.S. Patent No. 8,515,058. 20 Aug. 2013. https://patents.google.com/patent/US8515058B1/en

Innovators

- Craig Gentry

Licensing Contact

Michael Spaid

Technology Licensing Associate 2

Email