Daunting Mathematical Puzzle Solved, Enables Unlimited Analysis of Encrypted Data

IBM

ARMONK, NY — IBM inventors have received a patent for a breakthrough data encryption technique that is expected to further data privacy and strengthen cloud computing [1] security.

The patented breakthrough, called "fully homomorphic encryption," could enable deep and unrestricted analysis of encrypted information — intentionally scrambled data — without surrendering confidentiality. IBM's solution has the potential to advance cloud computing privacy and security by enabling vendors to perform computations on client data, such as analyzing sales patterns, without exposing or revealing the original data.

IBM's homomorphic encryption [2] technique solves a daunting mathematical puzzle that confounded scientists since the invention of public-key encryption over 30 years ago.

Invented by IBM cryptography [3] Researcher Craig Gentry, fully homomorphic encryption uses a mathematical object known as an "ideal lattice" that allows people to interact with encrypted data in ways previously considered impossible. The breakthrough facilitates analysis of confidential encrypted data without allowing the user to see the private data, yet it will reveal the same detailed results as if the original data was completely visible.

IBM received U.S. Patent #8,565,435: Efficient implementation of fully homomorphic encryption [4] for the invention, which is expected to help cloud computing clients to make more informed business decisions, without compromising privacy and security.

"Our patented invention has the potential to pave the way for more secure cloud computing services — without having to decrypt or reveal original data," said Craig Gentry, IBM Researcher and co-inventor on the patent. "Fully homomorphic encryption will enable companies to confidently share data and more easily and quickly overcome challenges or take advantage of emerging opportunities."

Following the initial revelation of the homomorphic encryption breakthrough in 2009 Gentry and co-inventor Shai Halevi began testing, refining and pursuing a working implementation of the invention. In 2011, the scientists reported [5] a number of optimizations that advanced their goal of implementing of the scheme. The researchers continue to investigate homomorphic encryption and test its practical applicability.

IBM invests more than $6 billion annually in R&D and consistently explores new

approaches to cloud computing that will deliver a competitive advantage to the company and its clients.

For 20 consecutive years, IBM has topped the list of U.S. patent recipients. The company's invention and patent leadership is illustrated at http://ibm.co/11k6fRn [6].

IBM has a tradition of making major cryptography breakthroughs, such as the design of the Data Encryption Standard (DES); Hash Message Authentication Code (HMAC); the first lattice-based encryption with a rigorous proof-of-security; and numerous other solutions that have helped advance data security.

More information about how IBM inventors are propelling cloud computing [7] innovations is available at http://ibm.co/174A8tS [8].

Links:
[1] http://www.ibm.com/cloud-computing/us/en/
[2] http://researcher.watson.ibm.com/researcher/view_project_subpage.php?id=2661
[3] http://researcher.watson.ibm.com/researcher/view_project.php?id=2659
[4] http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PALL&p=1&u=%2Fnetahtml%2FPTO%2Fsrchnum.htm&r=1&f=G&l=50&s1=8,565,435.PN.&OS=PN/8,565,435&RS=PN/8,565,435
[5] http://eprint.iacr.org/2010/520.pdf
[6] http://ibm.co/11k6fRn
[7] http://www.ibm.com/cloud-computing/us/en/what-is-cloud-computing.html
[8] http://ibm.co/174A8tS