Team Members:

Uday Kumar Vatti

Naga Navya Mingu

Preethi Kondaprithviraj

Title:

Alice's Jewelry store -Educational multi-media presentation on Fully Homomorphic Encryption

Introduction:

The growth of communication networks and their capabilities has led to the demand for privacy of digital data which is vulnerable to security attacks such as theft of highly sensitive information. Over the years, many algorithms and methods have been devised to provide guaranteed privacy for storing and accessing data, but it was not possible to make changes to the data without affecting their privacy. This problem can be solved by the use of Homomorphic cryptosystems which allow the computation of encrypted data while still protecting its privacy. The initial Homomorphic schemes could perform only one type of operation on a ciphertext, but with the introduction to fully homomorphic encryption in 2009, arbitrary calculations on the ciphertext became possible. The data will not be decrypted anywhere during the intermediate stages, the computations will be done on the encrypted data without the knowledge of its actual content and only the authenticated receiver will decrypt the message. The practical implementation of fully homomorphic cryptosystems finds its use when an entity outsources computational tasks to another entity e.g., Cloud computing and verifiable computing.

Motivation:

The idea of processing data without having access to it seems logically impossible. So, considering an analogous problem in (the fictional version of) the "physical world" gives some intuition about the solution.

Alice's jewelry store provides such physical analogy of how homomorphic encryption is done, provides a better understanding and simple explanation for the slightly complicated topic.

Physical analogy: a jewelry store owner, Alice, who wants her workers to process raw precious materials into intricately designed rings and necklaces, but is afraid to give her workers complete access to the materials for fear of theft.

Since the concept of fully homomorphic encryption is still new not many learning means are available to understand this physical analogy. It motivates us to explain this analogy in multi-media presentation which in turn helps the understanding of homomorphic encryption.

Detailed description of problems/hypotheses we are planning to investigate:

- We are going to develop an educational video and slides based on the Physical analogy used to understand Homomorphic Encryption as mentioned in the research highlights of "Computing Arbitrary Functions of Encrypted Data", by Craig Gentry.
- Simultaneously compare the physical analogy with the Mathematical model.
- Discuss the encryption schemes and the security aspects.
- We would try to improve the glove box analogy where it was unsatisfactory earlier or wherever required.

Tentative Table Of Contents

- Introduction to Homomorphic Encryption
- Introduction to Physical Analogy
- Security Aspects of FHE
- Somewhat Encryption Scheme
- Bootstrappable Encryption Scheme
- Future Scope and Improvement
- Conclusion
- References

Procedure/experiments used for verifying the results of your investigation.

- Reading and thoroughly understanding Homomorphic Encryption and its physical analogy from various educational videos, research and scholarly papers etc.

Time schedule:

- **Oct. 26-27**: Analyzing Homomorphic Encryption and searching for new ways or tools that can be used to prepare interactive and interesting slides.
- **Nov. 9-10**: With the knowledge attained from the analysis and about the presentation tools, we would start making the video and slides.
- **Nov. 23-24**: Will start drafting the report and also try to implement further extensions.
- **Dec. 7-8**: Preparing a final draft of report and slides with video.

A list of possible areas, where the specification can change depending on the progress of the project:

- Try and use the analogy for understanding Leveled Fully Homomorphic Encryption, which is based on learning with errors assumption.
- As we progress with the project we might be able to come up with some other analogy which is more apt in all cases.

Reference Links:

[1] Homomorphic encryption (n.d.). Wikipedia. Available: https://en.wikipedia.org/wiki/Homomorphic_encryption. Accessed Sep. 18, 2015.

[2] E. Naone. (2011, Jun). Homomorphic Encryption [Online]. Available: http://www2.technologyreview.com/article/423683/homomorphic-encryption/

[3] B. Hayes. (2012, Sep). Alice and Bob in Cipherspace [Online]. Available: http://www.americanscientist.org/issues/pub/2012/5/alice-and-bob-in-cipherspace

[4] Grecs. (2013, Dec. 11). What Is Homomorphic Encryption? [Online]. Available: https://www.novainfosec.com/2013/12/11/what-is-homomorphic-encryption/

[5] Cryptography Research (n.d.). IBM Research. [Online]. Available: http://researcher.watson.ibm.com/researcher/view_group_subpage.php?id=2661 . Accessed Sep. 21, 2015.

[6] Mikeazo. (2013, Jun. 24). What are some disadvantages of homomorphic encryption schemes? [Online]. Available: http://crypto.stackexchange.com/questions/8822/what-are-some-disadvantages-of-homomorphic-encryption-schemes

[7] C. Stunts. (2010, Mar. 18). What is Homomorphic Encryption, and Why Should I Care? [Online]. Available: http://blogs.teamb.com/craigstuntz/2010/03/18/38566/

[8] M. Kassner. (2011, May. 09). Homomorphic encryption: Can it save cloud computing? [Online]. Available: http://www.techrepublic.com/blog/it-security/homomorphic-encryption-can-it-save-cloud-computing/

[9] A. Greenberg. (2011, Mar. 14). Hacker Lexicon: What Is Homomorphic Encryption? [Online]. Available: http://www.wired.com/2014/11/hacker-lexicon-homomorphic-encryption/

[10] Homomorphic encryption (n.d.). Wikia. [Online]. Available: http://cryptography.wikia.com/wiki/Homomorphic_encryption . Accessed Sep. 21, 2015.