HOMOMORPHIC CRYTOGRAPHY DEVELOPMENT USING SCHEMES

Priyanka[1], Dinesh[2]

[1,2] *Computer Science & Engineering Department, M.D.U, (India)*

ABSTRACT

This paper presents the study of homomorphic cryptography. . In this paper a study of various papers and articles is done, and in this paper we explain the schemes of homomorphic cryptography.The main part of this paper covers the privacy or security of data communication by using schemes

Keywords: Homomorphic, RSA,Pailler, Gentry, Complexity Cipher

I. INTRODUCTION

From earlier study ,we know that public key cryptography is discovered by diffie and Hellman in [12]in 1976.Privacy of digital data has become necessary especially when internet has become an indispensable part of private and work lives .To achieve confidentiality application such as online banking, electronic voting, virtual network etc. are homomorphic and homomorphic schemes.

Homomorphic cryptosystem were introduced by Rivest ,Adleman,Detrouzons in 1978[31].

Fully homomorphic cryptosystems or privacy homomorphisms were introduced by Rivest, Adleman, and Dertouzous in 1978 [37]. In their paper they asked for a way to allow a third, untrusted party to carry out extensive computation on encrypted data, without having to decrypt first. Unfortunately, shortly after its publication, major security flaws were found in the original proposed schemes of Rivest et al.The search for fully homomorphic cryptosystems began.

Over the years a lot of either additively (Paillier [35] 1999, Goldwasser-Micali [23]1984, Naccache-Stern [34] 1998) or multiplicatively (El Gamal [14] 1984, RSA [37]1978) homomorphic schemes have been introduced to the world. The demand for a fully homomorphic cryptosystem rose again in 1991 when Feigenbaum et al. [15]asked: "Is there an encryption function Enc() such that both Enc(x+y) and Enc(x_y)are easy to compute from Enc(x) and Enc(y)?" and was answered in 2009. Craig Gentry published his fully homomorphic cryptosystem [19] in the summer of 2009.

Although not yet useful for practical applications, it ended the long search for the in 1978 emerged question about the existence of privacy homomorphism

II. OBJECTIVE

The main objective of homomorphic cryptography is to ensure privacy of data in communication and storage processes, such as the ability to delegate computations to untrusted parties. If a user could take a problem explained in one algebraic system and encode it into a problem in a various algebraic system in a way that decoding back to the original algebraic system is hard, then the user could encode expensive computations and

send them to the untrusted party. This untrusted party then performs the corresponding computation in the second algebraic system, returning the result to the
user. Upon receiving the result, the user can decode it into a solution in the original algebraic system, while the untrusted party learns nothing of which computation was actually performed

III BRIEF OF HOMOMORPHIC ENCRYPTION

The security requirements for data and algorithms has become very necessary in the last few years. Due to the excessive growth of technology, a great variety of attacks on digital goods and technical devices has increased or increasing day by day.Some possibilities exists for storing and reading data securely i.e Secure data encryption. The problem becomes more complex when asking for the possibility to compute (publicly) with encrypted data or to modify functions in such a way that they are still executable while our privacy is ensured. That is where homomorphic cryptosystems can be used. Even in 1978 this was a highly important matter, it is even more important nowadays. However the patial homomorphic properties of schemes like RSA, Paillier, ElGamal, etc. have been acknowledged ever since, it was not before 2009 when a young IBM researcher published the first working fully homomorphic cryptosystem, based on lattices

IV. SCHEMES OF HOMOMORPHIC CRYTOGRAPHY

The development of homomorphic cryptography is based on three schemes. They are as follows-
RSA-i.e Multiplicatively homomorphic schemes
Paillier-i. e Additively homomorphic schemes
Gentry-i.e Algebrically homomorphic schemes

4.1 RSA

It is based on multiplicative. It is also called multiplicatively Schemes In 1978, Rivest, Shamir, and Adleman published their public-key cryptosystem, which only uses elementary ideas from number theory, in their paper "A Method for Obtaining Digital signatures and Public-Key Cryptosystems" [37]. It was one of the first homomorphic cryptosystem. The RSA cryptosystem is the most widely used public-key cryptosystem. It may be used to provide both secrecy and digital signatures and its security is based on the intractability of the integer factorization

4.2 Paillier

It is based on the Additive.It is also called Additively Schemes.As we observe from earlier study that RSA scheme has a multiplicative homomorphic property. This means it is possible to perform multiplications with the encryptions of messageswithout losing or tampering with their underlying information. This is possible since the operation "multiplication" in the ciphertext space (Zn; _) can be compared with the operation "multiplication" in the plaintext space (Zn; _).
The Paillier scheme is known to be additively homomorphic. What might seem confusing at first is the fact that the two group operations are different, namely the product of two ciphertexts will decrypt to the sum of their plaintexts.In comparison to that, the product of two RSA ciphertexts decrypt to the productof their plaintexts. Hence the Paillier scheme is additivly homomorphic and RSA multiplicatively.

4.3 Gentry

It is based on the Algebric equations.It is also called Algebrically homomorphic enPascal Paillier introduced his cryptosystem in the 1999 published paper "Public-Key
Cryptosystems Based on Composite Degree Residuosity Classes" [35]. The proposed technique is based on composite residuosity classes, whose computation is believed to be computationally difficult. It is a probabilistic asymmetric algorithm for public key cryptography and inherits additive homomorphic properties. In the decades before Gentry discovered his novel method to gain homomorphic encryption, many researchers worldwide tried to find more powerful and therefore more complex schemes to achieve the fully homomorphic property. Gentry uses a method which no other researcher tried before. Instead of directly creating a superior scheme, he would build one from a "somewhat" homomorphic scheme, if its decryption circuit is sufficiently simple. He realized that he could build a fully homomorphic scheme from any scheme that is boot strappable, i.e., could homomorphically compute a slightly augmented version of its own decryption circuit

V. DECRYPTION COMPLEXITY

The aim of this initial construction of a somewhat homomorphic encryption scheme was to obtain a scheme that is bootstrappable. Up to now we do not know what bootstrappability even means and why it is a necessary prerequisite. Informally speaking a scheme is bootstrappable if it can homomorphically evaluate its own decryption circuit. Unfortunately this is not the case in this initial scheme [20]. In order to obtain a scheme that can be transformed into a fully homomorphic encryption scheme it is crucial to lower the complexity of the decryption circuit

VI. CONCLUSION

From the above study we conclude that homomorphic encryption works on the privacy of data communication.we make our communication secure by applying schemes.we can make our data encrypt by algebriically,additively and multiplicatively.It make our online processes confidential

VII. ACKNOWLEDGMENT

I show my thanks to all the departments' personals and sponsors who give us an opportunity to present and express my paper on this level

REFERENCES

[1] ISO/IEC 8859. URL http://www.iso.org.

[2] L. Babai. On Lovsz' lattice reduction and the nearest lattice point problem. Combinatorica, 6:1{13, 1986.

[3] M. Bellare, A. Boldyreva, and A. O'Neill. Deterministic and efficiently searchable encryption. In Proceedings of 28th Annual International Cryptology Conference - CRYPTO 2008, volume 4622/2007 of LNCS, pages 535{552. Springer Berlin / Heidelberg, 2007.

[4] M. Bellare, M. Fischlin, A. O'Neill, and T. Ristenpart. Deterministic encryption: Definitional equivalences and constructions without random oracles. In Proceedings of 28th Annual International Cryptology Conference – CRYPTO 2008, volume 5157/2008 of LNCS, pages 360{378. Springer Berlin / Heidelberg, 2008.

[5] D. J. Bernstein, J. Buchmann, and E. Dahmen. Post-Quantum Cryptography. Springer Berlin / Heidelberg, 2009.

[6] J. Black, P. Rogaway, and T. Shrimpton. Encryption-scheme security in the presence of key-dependent messages. In Selected Areas in Cryptography, volume 2595 of Lecture Notes in Computer Science, pages 62{75. Springer Berlin / Heidelberg, 2003.

[7] D. Boneh, E. Goh, and K. Nissim. Evaluating 2-dnf formulas on ciphertexts. In Proceedings of theory of Cryptography (TCC) '05, LNCS 3378, pages 325{341,2005.

[8] D. M. Bressoud. Factorization and Primality Testing. Springer-Verlag GmbH, Heidelberg, 1989.

[9] D. M. Burton. Elementary Number Theory. McGraw-Hill, 6 edition, 2007.

[10] R. D. Carmichael. On composite numbers p which satisfy the fermat congruenceaP□1 _ 1 mod p. The American Mathematical Monthly, 19(2):22{27, 1912.

[11] T. H. Cormen, C. E. Leiserson, and R. L. Rivest. Introduction to Algorithms.MIT Press, 2nd edition edition, 2001

12] W. Di _e and M. Hellman. New directions in cryptography. IEEE Transactions on Information Theory, 22(6):644{654, 1976.

[13] M. Drmota. Lecture Notes on Lineare Algebra 1. Technische Universit at Wien, 2005.

[14] T. El Gamal. A public key cryptosystem and a signature scheme based on discrete logarithms. In Proceedings of CRYPTO 84 on Advances in cryptology, pages 10{18. Springer-Verlag New York, 1984.

[15] J. Feigenbaum and M. Merritt. DIMACS Series in Discrete Mathematics and Theoretical Computer Science, volume 2, chapter Open Questions, Talk Abstracts, and Summary of Discussions, pages 1{45. ACM, 1991.

[16] N. Gama and P. Q. Nguyen. Predicting lattice reduction. In Proceedings of the theory and applications of cryptographic techniques 27th annual international conference on Advances in cryptology, EUROCRYPT'08, pages 31{51, Berlin, Heidelberg, 2008. Springer- Verlag.

[17] P. B. Garrett. Abstract Algebra. Chapman & Hall/CRC, 2008.

[18] C. F. Gau_. Disquisitiones Arithmeticae. Gerhard Fleischer, Lipsiae, 1801.

[19] C. Gentry. Fully homomorphic encryption using ideal lattices. In Proceedings of the 41st annual ACM symposium on Theory of computing, pages 169{178. ACM, 2009.

[20] C. Gentry. A fully homomorphic encryption scheme. PhD thesis, Department of Computer Science - Stanford University, 2009.

[21] O. Goldreich, S . Goldwasser, and S. Halevi. Public-key cryptosystems from lattice reduction problems. In Proceedings of the 17th Annual International Cryptology Conference on Advances in Cryptology, pages 112{131. Springer- Verlag, 1997.

[22] S. Goldwasser and M. Bellare. Lecture Notes on Cryptography. Massachusetts Institute of Technology, 2008. URL http:// cseweb.ucsd.edu/ ~mihir/papers/gb.html.

[23] S. Goldwasser and S. Micali. Probabilistic encryption. Journal of Computer and System Sciences, 28:270{297, 1984.

[24] J. Katz and Y. Lindell. Introduction to Modern Cryptography. Chapman & Hall/CRC Press, 2008.

[25] R. W. Keener and R. W. Keener. Probability and measure. In Theoretical Statistics, Springer Texts in Statistics, pages 1{24. Springer New York, 2010.

[26] A. Kerckho_s. La cryptographie militaire. Journal des sciences militaires, IX: 5{83, 1883.

[27] T. Kleinjung, K. Aoki, J. Franke, A. Lenstra, E. Thom, J. Bos, P. Gaudry, A. Kruppa, P. Montgomery, D. A. Osvik, H. t. Riele, A. Timofeev, and P. Zimmermann. Factorization of a 768-bit rsa modulus. Cryptology ePrint Archive, Report, 2010/006:1, 2010.

[28] A. K. Lenstra, H. W. Lenstra, and L. Lovsz. Factoring polynomials with rational coe_cients. Mathematische Annalen, 261:515{534, 1982.

[29] Y.-K. Liu, V. Lyubashevsky, and D. Micciancio. On bounded distance decoding for general lattices. In Approximation, Randomization, and Combinato- rial Optimization. Algorithms and Techniques, volume 4110 of Lecture Notes in Computer Science, pages 450{461. Springer Berlin / Heidelberg, 2006.

[30] A. J. Menezes, S. A. Vanstone, and P. C. Van Oorschot. Handbook of Applied Cryptography. Discrete Mathematics and Its Applications. CRC Press, Inc., 1996.

[31] D. Micciancio. The shortest vector problem is NP-hard to approximate to within some constant. SIAM Journal on Computing, 30(6):2008{2035, March 2001.

[32] D. Micciancio and S. Goldwasser. Complexity of Lattice Problems: a crypto- graphic perspective, volume 671 of The Kluwer International Series in Engi- neering and Computer Science. Kluwer Academic Publishers, Boston, Massachusetts, Mar. 2002.

[33] H. Minkowski. Geometrie der Zahlen. Teubner, 1910.

[34] D. Naccache and J. Stern. A new public key cryptosystem based on higher residues. In ACM Conference on Computer and Communications Security, pages 59 { 66, 1998.

[35] P. Paillier. Public-key cryptosystems based on composite degree residuosity classes. Advances in Cryptology Eurocrypt, 1592:223{238, 1999.