IJRRECS/October 2013/Volume-1/Issue-6/1070-1074 **ISSN 2321-5461**

INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE

CONFIDENTIAL DATA RECOVERY FOR A SINGLE DATABASE THROUGH INVARIABLE COMMUNICATION RATE

Sitarami Reddy Polimera[1], D.Deepika[2]

[1]M.Tech Student, Dept of CSE, Mahatma Gandhi Institute of Technology, Hyderabad, A.P,India

[2]Assistant Professor, Dept of CSE, Mahatma Gandhi Institute of Technology, Hyderabad, A.P,India

ABSTRACT:

Private information retrieval was commenced in the setting where there are numerous copies of the identical database and not any of the replicas are authorized to correspond with each other. These single-database Private information retrieval protocols make available approximately most favourable communication outlay, excluding requires the database to make use of a vast quantity of computational power. It allows the user to get back data from an unlimited database by means of smaller communication then just downloading the complete database. Building of a single-database Private information retrieval from a homomorphic encryption system permits homomorphic calculation of only one function moreover addition or multiplication taking place on plaintexts. The normal and added realistic expansion of private information retrieval is the Private Block Retrieval in which, the user get backs a block of bits from the database as a substitute of regaining only a single bit. The general single-database private information retrieval is semantically protected if the fundamental fully homomorphic encryption scheme is semantically locked has been shown by the security examination.

Keywords: single-database Private information retrieval, Homomorphic encryption, Private block retrieval.

1. INTRODUCTION:

In the Private Information Retrieval scheme connecting a user and a database, holds some public data. The user desires to recover some entry from the database exclusive of revealing to the database which item was queried [1]. An advanced private data retrieval procedure is probable to have distinctly lower communication obstacle. Private Information Retrieval protocols allow the user to get back data from an unlimited database by means of smaller communication then just downloading the complete database [2]. Private information retrieval was commenced in the setting where there are numerous copies of the identical database and not any of the replicas are authorized to correspond with each other. These single-database Private information retrieval protocols make available approximately most favourable communication outlay, excluding requires the database to make use of a vast quantity of computational power [8] [11]. Casually, a single-database Private Information Retrieval procedure is a two-party procedure, where a user get backs the p-th bit from an q-bit database BS = s_1, s_2 …..s_q, devoid of instructing to the database server about the value of p. Properly, a single-database Private Information Retrieval protocol comprises of three algorithms such as Query Generation: which takes as input a protection parameter, the dimension of the database, and the index of a bit in the database, and yields a query and a secret [3]. Response Generation: It takes as input the protection parameter, the query and the database, and yields a response. Response Retrieval: Takes as input the defenses parameter, the response, the index of the bit, the size of the database, the query, and the secret, and output a bit [5] [7]. Private Block Retrieval is a normal and added realistic expansion of private information retrieval in which, as a substitute of regaining only a single bit, the user get backs a block of bits from the database. The servers should be trusted not to join together on the way to make assured about the user confidentiality in the multi-server setting [4]. Single-database Private information retrieval has a secure association to the conception of Oblivious Transfer which is a two-party procedure, where a sender and a receiver interrelate. It is dissimilar from Private information retrieval in that there is no message difficulty obligation other than; on the other hand, confidentiality is necessary for both players, whereas for Private

information retrieval it is necessary only for the user [6] [10].

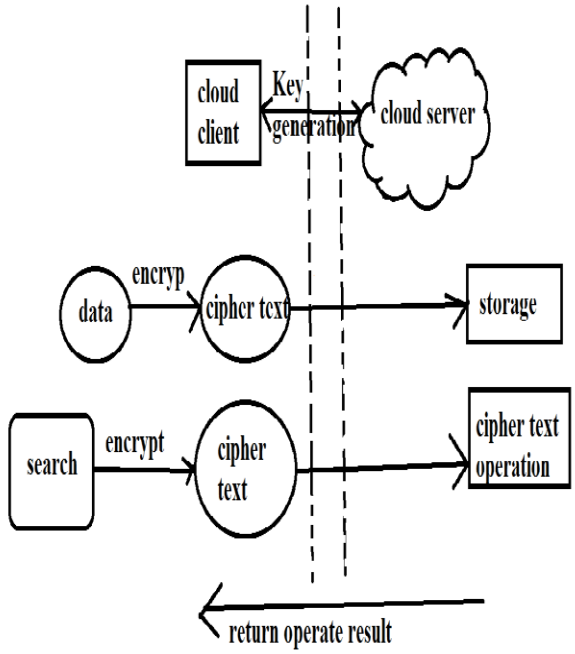

Fig1: An overview of homomorphic encryption enhancing data security.

2. METHODOLOGY:

A general means to build a single-database Private information retrieval from a homomorphic encryption system shown in fig1 was proposed which permits homomorphic calculation of only one function moreover addition or multiplication taking place on plaintexts. In the homomorphic encryption system by lattice-based cryptography permits homomorphic calculation of two functions both addition and multiplication of plaintexts [9] [13]. Soon after various other encryption system was proposed, by making usage of several tools of the initial encryption method, and the later method differ from the initial one by not entailing ideal lattices. A Fully Homomorphic Encryption system consists of five algorithms such as Key Generation: Here the algorithm obtains as an input a defence parameter and outputs a public and private key pair. Encryption: The algorithm obtains as input a plaintext and the public key and output a cipher text. Decryption: The algorithm acquires as input a ciphertext and the private key and outputs a plaintext [12]. Homomorphic Addition: The algorithm takes as input two ciphertexts and the public key, and outputs a ciphertext. Homomorphic Multiplication: The algorithm takes as input two ciphertexts and the public key, and outputs a ciphertext [15]. While the single-database private block retrieval protocol is a grouping of the single-database private information retrieval protocol and the realistic private block retrieval protocol from fully homomorphic encryption is an unusual case of the general private block retrieval from fully homomorphic encryption, we only have to analyze the protection of the generic private

information retrieval protocol from fully homomorphic encryption [14]. Private information retrieval and Private Block Retrieval protocols from Fully Homomorphic Encryption make available confidentiality of the user as long as the essential Fully Homomorphic Encryption scheme is semantically protected. The additively homomorphic encryption system by means of d-operand multiplications can be capable to assess the multivariate polynomials for encrypted information in the Private Block Retrieval protocol which requests two chainable encryptions to amalgam two cipher texts to single cipher text and a succession of chainable decryptions to decrypt a complex cipher text.

3. RESULTS:

Single-database Private Block Retrieval from fully homomorphic encryption, Assuming that the database has j bits, which are equally divided into k blocks, the user needs to encrypt log k bits and decrypt j/k ciphertexts, whereas the database server desires to carry out about k log k Mult operations and about j/2 Add operations. The degree of the boolean utility corresponding to the response generation circuit assessed by means of the database server is in relation to log k only. Consequently, it is probable for the Private Block Retrieval procedure to assemble on a somewhat homomorphic encryption system in appropriate setting. In the realistic single-database Private Block Retrieval protocol, the public key has the similar size as a cipher-text, and the Add and Mult Operations are modular addition and multiplication.

4. CONCLUSION:

Private Information Retrieval protocols allow the user to get back data from an unlimited database by means of smaller communication then just downloading the complete database. Private information retrieval was commenced in the setting where there are numerous copies of the identical database and not any of the replicas are authorized to correspond with each other. A superior private information retrieval protocol is likely to have noticeably lower communication complication. Homomorphic encryption methods are frequently extremely accepted ways to build a selection of privacy-preserving procedures. A general means to build a single-database Private information retrieval

from a homomorphic encryption system was proposed which permits homomorphic calculation of only one function moreover addition or multiplication taking place on plaintexts The general single-database private information retrieval is semantically protected if the fundamental fully homomorphic encryption scheme is semantically locked has been shown by the security examination. Realistic private block retrieval procedure has lower calculation difficulty but superior communication intricacy than active private block retrieval protocols.

REFERENCES:

[1] C. Aguilar-Melchor and P. Gaborit. A lattice-based computationally-efficient private information retrieval protocol. In Proc. WEWORC'07, 2007.

[2] C. Aguilar-Melchor and P. Gaborit. A fast private infor- mation retrieval protocol. In Proc. ISIT'08, 2008.

[3] C. Aguilar-Melchor, P. Gaborit and J. Herranz. Additively homomorphic encryption with d-operand multiplications. http://eprint.iacr.org/2008/378.

[4] Z. Brakerski, C. Gentry and V. Vaikuntanathan. Fully homomorphic encryption without bootstrapping. http://eprint.iacr.org/2011/277.

[5] Z. Brakerski and V. Vaikuntanathan. Efficient fully homomorphic encryption from (standard) LWE. http://eprint.iacr.org/2011/344.

[6] G. Brassard, C. Crepeau and J.M. Robert. All-or-nothing disclosure of secrets. In Proc. CRYPTO'86, pages 234-238, 1986.

[7] C. Cachin, S. Micali, and M. Stadler. Computationally pri- vate information retrieval with polylogarithmic commu- nication. In Proc. EUROCRYPT'99, pages 402-414, 1999.

[8] Y. C. Chang. Single Database Private Information Retrieval with Logarithmic Communication. In Proc. ACISP'04, pages 50-61, 2004

[9] B. Chor, O. Goldreich, E. Kushilevitz, and M. Sudan. Private information retrieval. In Proc. 36th Annual IEEE Conference on Foundations of Computer Science, pages 41-50, 1998.

[10] G. Di Crescenzo, T. Malkin, and R. Ostrovsky. Single-database private information retrieval implies oblivious transfer. In Proc. EUROCRYPT'00, pages 122-138, 2000.

[11] I. Damgard and M. Jurik. A Generalisation, a simplifi- cation and some applications of Paillier's probabilistic public-key system. In Proc. PKC'01, pages 119-136, 2001.

[12] M. Dijk, C. Gentry, S. Halevi and V. Vaikuntanathan. Fully homomorphic encryption over the integers. In Proc. EUROCRYPT'10, pages 24-43, 2010.

[13] S. Even, O. Goldreich and A. Lempel. A randomized protocol for signing contracts. Communications of the ACM, 28(6): 637-647, 1985.

[14] C. Gentry and Z. Ramzan. Single database private in- formation retrieval with constant communication rate. In Proc. ICALP'05, pages 803-815, 2005.

[15] C. Gentry. Fully Homomorphic Encryption Scheme. PhD thesis, Stanford University, 2009. Manuscript available at http://crypto.stanford.edu/craig.