© 2015 IJSRSET | Volume 1 | Issue 2 | Print ISSN : 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

Encryption scheme with Ordered Bucketization

Raghunathan M, Ramakrishna V, Rathana kumar M, Murugesan M
Computer Science and Engineering, Dhanalakshmi College of Engineering, Chennai, Tamilnadu, India

ABSTRACT

Requested bucketization (OB), a primitive for permitting productive reach inquiries on encoded information. Initially, we address the open issue of portraying what encryption by means of an irregular request saving capacity spills about hidden information. Specifically, we demonstrate that, for a database of haphazardly circulated plaintexts and fitting decision of parameters, Random Order Preserving Function (ROPF) encryption releases neither the exact estimation of any plaintext nor the exact separation between any two of them. Then again, we likewise demonstrate that ROPF encryption does release both the estimation of any plaintext and additionally the separation between any two plaintexts to inside a scope of conceivable outcomes generally the square base of the space size. We then study an encryption plan with OB (EOB) and recommend another security model for EOB, IND-OCPA-P, which expect a foe has sensible force. The IND-OCPA-P model to dissect the security of the proposed EOB and the encryption plans supporting an effective reach question over encoded information. Since this model permits an enemy to question an encryption of a picked message, it is stronger than the security demonstrate on which the Order-saving Encryption Revisited was demonstrated secure.

Keywords: OCPA-P, ROPF, Requested bucketization , Order-saving Encryption, plaintext, semantic security, Order Preserving Encryption

I. INTRODUCTION

Semantic-security of individual bits under a ciphertext is principal idea in current cryptography. In this work we show the first results about this principal issue for Order Preserving Encryption (OPE): "what plaintext data can be semantically covered up by OPE encryptions?" While OPE has increased much consideration as of late because of its convenience in secure databases, any halfway plaintext indistinctness (semantic security) result for it was open. Here, we propose another indistinctness based security idea for OPE, which can guarantee mystery of lower bits of a plaintext (under basically an arbitrary ciphertext examining setting). We then propose another plan fulfilling this security thought (while prior plans don't fulfil it!). We take note of that the known security ideas let us know nothing about the above halfway plaintext lack of definition in light of the fact that they are constrained to being restricted based. Furthermore, we demonstrate that our security idea with particular parameters infers the known security thought called WOW, and further, our plan attains to WOW with preferable parameters over prior plans.

Encryption is an entrenched innovation for securing delicate information. Then again, once encoded, information can never again be effortlessly questioned beside accurate matches. We exhibit a request saving encryption plan for numeric information that permits any examination operation to be specifically connected on encoded information. Inquiry results delivered are sound (no false hits) and complete (no false drops). Our plan handles overhauls smoothly and new values can be included without obliging changes in the encryption of different qualities. It permits standard database lists to be assembled over encoded tables and can without much of a stretch be coordinated with existing database frameworks. The proposed plan has been intended to be sent in application situations in which the gate crasher can become acquainted with the encoded database, however does not have earlier space data, for example, the dissemination of qualities and can't encode or unscramble self-assertive estimations of his decision.

The encryption is strong against estimation of the genuine esteem in such situations.

Objective

This paper proposes the IND-OCPA-P model to analyse the security of the proposed EOB nd the encryption schemes supporting an efficient range query over encrypted data. Because this model allows an adversary to query an encryption of a chosen message, it is stronger than the security model on which the Order-Preserving Encryption Revisited was proven secure. Encryption with Ordered Bucketization, where a range query can be supported efficiently while preserving high-level security compared to existing methods.

II. METHODS AND MATERIAL

OB and introduces Encryption with Ordered Bucketization (EOB) that can be constructed from an implementation of OB. After that, the security model, IND-OCPA-P, is proposed at the next section. Finally, the proposed OB construction is provided.

Definition of the Ordered Bucketization and the Encryption with the Ordered Bucketization

An OB scheme is composed of two algorithms OBp; M (KOB ; T OB), which are defined as follows:

K_{OB} : is a randomized key generation algorithm.

$K_{OB} \leftarrow^{\$} K_{OB}(p)$ (K_{OB} : N → Keys).

T_{OB} : is a deterministic bucketing algorithm. bucketnumber ← $T_{OB}(K_{OB}$; m) (T_{OB} : Keys M → [0; p1].) T_{OB} works on the following condi-tion: suppose K_{OB} $ K_{OB}(M, p) and m_0 , $m_1 \leftarrow_{\$}$ M,then T_{OB} (K_{OB} , m_0)≥T_{OB}(K_{OB} , m_1) if and only if $m_0 \geq m_1$.

With the above OB and a symmetric encryption schemeSE(K,E,D),thesymmetricencryption with ordered bucketi-zation EOB ($OB_{M;p}$, SE (K_{EOB}, E_{EOB} , D_{EOB}), is defined as follows:

K_{EOB}(p): key generation algorithm, where p is thenumber of buckets.

1) K ←$^{\$}$ K

2) $K_{OB} \leftarrow^{\$} K_{OB}(p)$

3) return K_{EOB} =(K, K_{OB}).

$\mathcal{E}_{EOB}$ (K_{EOB} , m) (m Ɛ M):encryption algorithm.

1) (K, K_{OB}) K_{EOB}

2) bucket# T_{OB} (K_{OB} ,m)

3) c ←$^{\$}$ EðK; mÞ

4) return c_{EOB} = bucket#||c.

D_{EOB} (K_{EOB} ,c_{EOB}): decryption algorithm.

1) (K, K_{OB}) K_{EOB}

2) n||c c_{EOB}

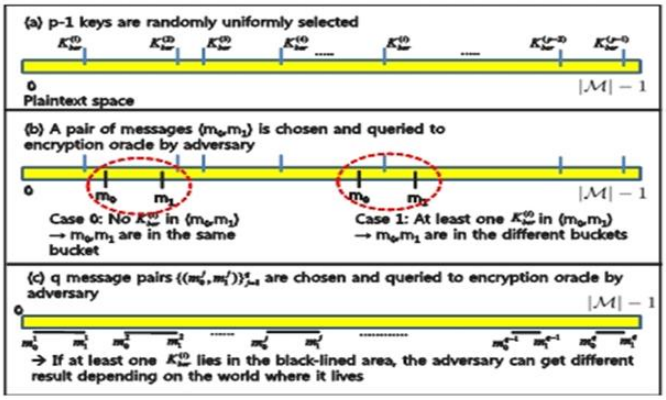
3) m ←D(K,c)

4) return m.

III. RESULTS AND DISCUSSION

A. Security Analysis

Security on IND-OCPA model. Unless there is only a single bucket in M, the adversary trivially wins in this model. The bucket number for the plaintext 0 and the bucket number for the plaintext jMj1 are different from each other. There-fore, an adversary can be constructed easily requiring only a single query to obtain a non-negligible advantage



B. Efficiency Analysis

This segment investigates the proficiency of a reach question over the information that is encoded by EOB where the proposed OB is utilized. The fundamental center was to investigate the seeking effectiveness regarding the false positive rate. To do this, the likelihood conveyance of the rate of the width of a can to the extent of the plaintext space was initially

examined to demonstrate that the width of a can is not skewed to be amazingly vast or little. This even-pail width property gives the proposed plan a decent questioning execution by and large. Next, the false positive rate between the proposed plan and existing plan (QOB) werecompared. Both plans were actualized and the false positive rates were measured in a comparable test environment.

IV. CONCLUSION

This paper presented another encryption plan Encryption with Ordered Bucketization, where an extent inquiry can be upheld productively while saving abnormal state security contrasted with existing routines. To examine the security, this paper proposed a security model called IND-OCPA-P (INDistinguishability under requested Chosen Plaintext Adversary with Polynomial questioning separation) where no current OPE and encryption with bucketization plans have ended up being secure as such. A protected OB (Ordered Bucketization) was built with which any EOB that chips away at top of any IND-CPA-secure symmetric encryption plan is secure on the IND-OCPA-P model. By examining the likelihood dissemination of the width of a pail in the proposed OB and checking the investigation come about through examinations after execution, the proposed plan gave a sensible extent questioning proficiency.

V. REFERENCES

[1] Difference of Order Statistics in a Sample of Uniform Random Variables[Online].Available: http://math.stackexchange.com/questions/68749/difference-of-order-statistics-in-a-sample-of-uniform-random-variables, 2011.

[2] OPEN SSL: Cryptography and SSL/TLS Toolkit,"[Online].Available:http://www.openssl.org, 1999.

[3] R. Agrawal, J. Kiernan, R. Srikant, and Y.Xu,"Order preserving encryption for numeric data," in Proc. ACM SIGMOD Int. Conf.Manage. Data, 2004, pp. 563-574.

[4] M. Bellare and P. Rogaway, "Course Notes on Introduction to Modern Cryptography," [Online]. Available: http://cseweb.ucsd.edu/~mihir/cse207/index.html, 2005.

[5] A. Boldyreva, N. Chenette, Y. Lee, and A. O'Neill, "Order-pre-serving symmetric encryption," in Proc. 31st Annu. Int. Conf. Adv.Cryptology, 2009, vol. 5479, pp. 224-241.

[6] A. Boldyreva, N. Chenette, and A. O'Neill, "Order-preserving encryption revisited: Improved security analysis and alternative solutions," in Proc. 31st Annu. Conf. Adv. Cryptology, 2011,vol. 6841, pp. 578-595.

[7] D. Boneh and B. Waters, "Conjunctive, subset, and range queries on encrypted data," in Proc. 4th Conf. Theory Cryptography, 2007, pp. 535-554.