Generating Searchable Public-Key Cipher Texts with Hidden Structures for Fast Keyword Search

Virsha Mishra
PG Scholar, Department of CSE
Godavari Institute of Engineering & Technology (A)
Rajahmundry, Andhra Pradesh, India.

Dr.B.Sujatha
Head of the Department, Department of CSE
Godavari Institute of Engineering & Technology (A)
Rajahmundry, Andhra Pradesh, India

Abstract— ***Present day's definition of protection of public-key finding encryption idea take find time linear with the total number of the cipher texts. This makes renewal from large-scale databases preventing. To eradicate this problem, this paper introduce finding Public-Key Cipher texts with Hidden Structures (SPCHS) for keyword find as quick as possible without losing definition protection of the encrypted keywords. In SPCHS, all keyword-finding cipher texts are efficient by private relations, and with the find trapdoor identical to a keyword, the minimal message of the relations is expose to a find algorithm as the advice to search all identical cipher texts effortlessly. We construct a SPCHS chart from scratch in which the cipher texts have a private star-like structure. We prove our chart to be definition protection in the Random Oracle (RO) model. The find complication of our chart is defenseless t on the actual number of the cipher texts involving the queried keyword, rather than the number of all cipher texts. Finally, we present a generic SPCHS construction from nameless identity-based encryption and collision-free full-identity malleable Identity-Based Key Encapsulation Mechanism (IBKEM) with anonymity. We illuminate two collision-free full-identity malleable IBKEM instances, which are semantically secure and anonymous, respectively, in the RO and standard models. The recent instance enables us to construct an SPCHS chart with semantic protection in the standard model.***

I. INTRODUCTION

Public-Key encryption with keyword find (PEKS), introduced by Boneh et al., has the asset has anyone who knows the receiver's public key can upload keyword-finding cipher texts to a server. The collector can agent the keyword search to the server. when the receiver wants to recover the files involving a specific keyword, he agent a keyword search trapdoor to the server; the server finds the encrypted files involving the queried keyword without expecting the original files

The authors of PEKS also presented definition protection against chosen keyword attacks (SSCKA) in the sense that the server cannot analyze the cipher texts

of the keywords of its select before aware the containing keyword search trapdoors.

II. RELATED WORK

Present definition protection PEKS chart take find time linear with number of cipher texts. This makes improve from large-scale databases excessive. Therefore, more efficient search performance is crucial for practically expand PEKS chart.

One of the outstanding works to advance the find over encrypted keywords in the public-key setting is deterministic encryption introduce by Bellare et al.

III. LITERATURE REVIEW

Bellare et al. focus on permissive find over encrypted keywords to be able as the find for unencrypted keywords, such that a cipher text corresponding a given keyword can be recovered in time involvement logarithmic in the total number of all cipher texts. However, deterministic encryption has two inherent drawbacks. First, keyword privacy can be approved only for keywords that are a priority hard to-guess by the second certain information of a message leaks surely via the cipher text of the keywords.

IV. PROBLEM DEFINITION

One of the outstanding works to advance the find over encrypted keywords in the public-key frame is deterministic encryption introduced by Bellare et al.

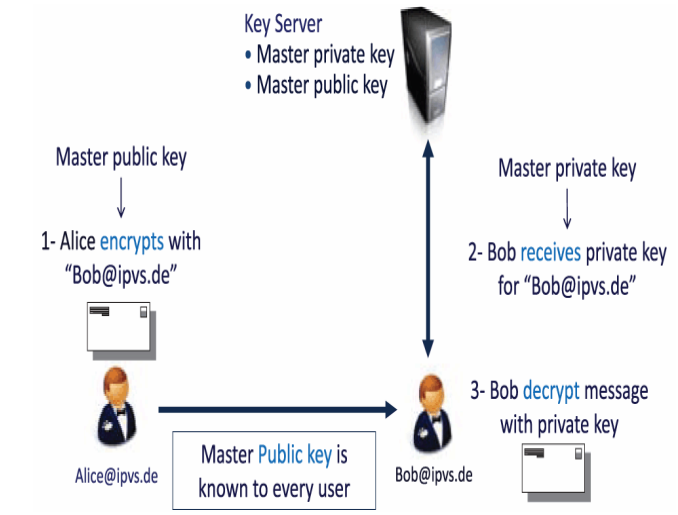
Bellare et al. focus on permissive find over encrypted keywords to be able as the find for unencrypted keywords, such that a cipher text corresponding a given keyword can be recover in time involvement logarithmic in the total number of all cipher texts. from a cryptographic overview, the present works fall into two kind, i.e., symmetric searchable encryption and public-key searchable encryption.

V. PROPOSED APPROCH

Present definition protection PEKS chart take time to all cipher texts. This makes retrieval from large-scale databases excessive. Therefore, more able find performance is crucial for practically deploying PEKS schemes.

Deterministic encryption has two inherent drawbacks. First, keyword protection can be guaranteed only for keywords that are a priori hard to guess by the oppose (i.e., keywords with high min-entropy to the oppose); second, certain report of a information flow necessarily via the cipher text of the keywords since the encryption is deterministic. Hence, deterministic encryption is only applicable in special synopsis.
We are interested in adding highly efficient search performance without losing semantic protection in PEKS.
We start by suitably defining the concept of Searchable Public-key Cipher texts with Hidden Structures (SPCHS) and its definition protection.

VI. SYSTEM ARCHITECTURE



VII. PROPOSED METHODOLOGY

We build a universal SPCHS development with Identity-Based Encryption (IBE) and collision-free full-identity adaptable IBKEM.
The appearing SPCHS can create keyword-finding cipher texts with a hidden star-like structure. Moreover, if both the analytical IBKEM and IBE have semantic protection and anonymity (i.e. the privacy of receivers' identities), the resulting SPCHS is semantically safe.

VIII. IMPLEMENTATION

MODULE:

1. Data owner Module
2. Data User Module
3. Encryption Module
4. Rank Search Module

MODULE DESCRIPTION:

Data owner Module

In SPCHS, all keyword-finding cipher texts are structured by private relations, and with the find side door identical to a keyword, the minimum information of the relations is disclosed to a search algorithm as the control to find all comparable cipher texts efficiently

Data User Module

In this module, we establish the data user module. It start by formally defining the theory of Searchable Public-key Cipher texts with Hidden Structures (SPCHS) and its semantic protection. In this new theory, keyword searchable cipher texts with their private structures can be achieve in the public key framework; with a keyword find side door, partial relations can be disclosed to counselor the analysis of all identical cipher texts.

Encryption Module

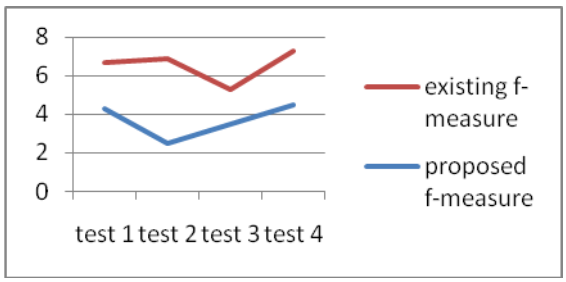
Nameless entity-based transmission encryption. A hardly more entangled application is nameless entity-based transmission encryption with efficient decryption. An equivalent utilization was proposed respectively by Barth et al. and Libert et al. in the traditional public-key frame . With collision-free full entity adaptable IBKEM, a sender achieve an entity based transmission

Cipher text hC1, C2, (K1 1 jjSE(K1 2 ; F1)), :::, (KN 1 jjSE(KN 2 ; FN))i, where C1 and C2 are two IBKEM encapsulations,

Rank Search Module

It grant the find to be handled in logarithmic time, although the keyword find side door has length linear with the size of the database. In addition to the above efforts devoted to either provable protection or better search performance.

IX. RESULT



X. CONCLUSION

This paper inspected as-quick-as-possible find in PEKS with semantic protection. We proposed the theory of SPCHS as a variant of PEKS. The new theory grant keyword-finding cipher texts to be achieve with a private structure. Given a keyword find side door, the find algorithm of SPCHS can disclose part of this private structure for advice on finding out the cipher texts of the inquire keyword. Semantic protection of SPCHS captures the protection of the keywords and the abduction of the private structures. We expected an SPCHS chart from scratch with semantic protection in the RO model. The charts achieve keyword-finding cipher texts with a hidden star-like structure. It has find complication mainly linear with the exact number of the cipher texts consist of the queried

keyword. We illuminated two collision-free full-entity adaptable IBKEM detail, which are correspondingly safe in the RO and standard models.

SPCHS seems a promising tool to solve some challenging problems in public-key finding encryption.

References

[1] Joneh D., Crescenzo G. D., Ostrovsky R., Persiano G.: Public Key Encryption with Keyword Search. In: Cachin C., Camenisch J. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 506-522. Springer, Heidelberg (2004)

[2] Bellare M., Boldyreva A., O'Neill A.: Deterministic and Efficiently Searchable Encryption. In: Menezes A. (ed.) CRYPTO 2007. LNCS, vol. 4622, pp. 535-552. Springer, Heidelberg (2007)

[3] Boneh D., Boyen X.: Efficient Selective-ID Secure Identity-Based Encryption Without Random Oracles. In: Cachin C., Camenisch J. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 223-238. Springer, Heidelberg (2004)

[4] Boyen X., Waters B. R.: Anonymous Hierarchical Identity-Based Encryption (Without Random Oracles). In: Dwork C. (ed.) CRYPTO 2006. LNCS, vol. 4117, pp. 290-307. Springer, Heidelberg (2006)

[5] Gentry C.: Practical Identity-Based Encyrption Without Random Oracles. In: Vaudenay S. (ed.) EUROCRYPT 2006. LNCS, vol. 4004, pp.445-464. Springer, Heidelberg (2006)

[6] Ateniese G., Gasti P.: Universally Anonymous IBE Based on the Quadratic Residuosity Assumption. In: Fischlin M. (ed.) CT-RSA 2009. LNCS, vol. 5473, pp. 32-47. Springer, Heidelberg (2009)

[7] Ducas L.: Anonymity from Asymmetry: New Constructions for Anonymous HIBE. In: Pieprzyk J. (ed.) CT-RSA 2010. LNCS, vol. 5985, pp. 148-164. Springer, Heidelberg (2010)

[8] Abdalla M., Catalano D., Fiore D.: Verifiable Random Functions: Relations to Identity-Based Key Encapsulation and New Constructions. Journal of Cryptology, 27(3), pp. 544-593 (2013)

[9] Freire E.S.V., Hofheinz D., Paterson K.G., Striecks C.: Programmable Hash Functions in the Multilinear Setting. In: Canetti R., Garay J.A. (eds.) Advances in Cryptology - CRYPTO 2013. LNCS, vol. 8042, pp. 513-530. Springer, Heidelberg (2013)

[10] Garg S., Gentry C., Halevi S.: Candidate Multilinear Maps from Ideal Lattices. In: Johansson T., Nguyen P. (eds.) Advances in Cryptology - EUROCRYPT 2013. LNCS, vol. 7881, pp. 1-17. Springer, Heidelberg (2013)

[11] Boneh D., Franklin M.: Identity-Based Encryption from the Weil Pairing. In: Kilian J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 213-239. Springer, Heidelberg (2001)

[12] Barth A., Boneh D., Waters B.: Privacy in Encrypted Content Distribution Using Private Broadcast Encryption. In: Di Crescenzo G., Rubin A.(eds.) FC 2006. LNCS, vol. 4107, pp. 52-64. Springer, Heidelberg (2006)

[13] Libert B., Paterson K. G., Quaglia E. A.: Anonymous Broadcast Encryption: Adaptive Security and Efficient Constructions in the Standard Model. In: Fischlin M., Buchmann J., Manulis M. (eds.) PKC 2012. LNCS, vol. 7293, pp. 206-224. Springer, Heidelberg (2012)

[14] Curtmola R., Garay J., Kamara S., Ostrovsky R.: Searchable Symmetric Encryption: Improved Definitions and Efficient Constructions. In: ACM CCS 2006, pp. 79-88. ACM (2006)

[15] Song D. X., Wagner D., Perrig A.: Practical techniques for searches on encrypted data. In: IEEE S&P 2000, pp. 44-55. IEEE (2000)