Review on Keyword Searchable Public Key Cipher Text with Hidden Structure

Yadav Ashwini, Pondkule Priyanka, Nale Supriya, Khomane Sharmila, Asst. Prof. P. R. Kadam
Department of Computer Engineering, S B Patil College of Engineering,
Indapur Dist.– Pune, Maharashtra, India

Abstract— Now a days a security over internet problem is increases day by day .Existing system get search time large with the whole no of cipher texts. That makes recovery from comprehensive database unreasonable. To improve this problem, this paper propose searchable public key cipher texts with unseen structure for keyword explore as fast as feasible lacking sacrificing semantic security of the encrypted keywords. In SPCHS, every one keyword searchable cipher text are planned by unseen relative, and with the search trapdoor subsequent to a keyword, the smallest amount in sequence of the relations is relate to a look for algorithm as the supervision to discover all corresponding cipher text capably. We build a SPCHS idea from scrape in which the cipher text contains a concealed star like structure. We demonstrate our system to be semantically secure in the Random Oracle (RO) model. The search complexity of the proposed scheme depended upon the actual no of cipher text rather than the no of all cipher text. Lastly we present a generic SPCHS construction from unidentified identity based encryption and clash free full identity malleable identity based key encapsulation mechanism with anonymity.

Keywords—Public-key Searchable encapsulation, Schematic exposure, identify-based key encapsulation mechanism, identity based encapsulation.

I. INTRODUCTION

Public-Key encryption with keyword search(PEKS),are describe by Boneh et al. in [1],the benefit of PEKS is that the anybody can knows the public key of receiver and it can upload a searchable cipher texts to the server. The receiver can hand over the searchable keyword to the server. Generally, every sender individually encrypts a file and its extracted keywords and send the consequential cipher texts to a server; When the receiver requests to regain the files containing exact keyword, he delegates a keyword look for trapdoor to the server. After that server finds the encrypted files containing the queried keyword without knowing the original files or the keyword itself, and returns the corresponding encrypted files to the receiver. Finally, the receiver decrypts these encrypted files.

　　　The authors of PEKS also introduced semantic security against chosen keyword attacks (SSCKA)in the sense that the server cannot distinguish the ciphertexts of the keywords of its pick before observe the equivalent keyword search trapdoors. It seems an suitable security concept, particularly if the keyword space has no high min-entropy. Existing system semantically secure PEKS scheme take search time least with the total number of all cipher texts. This makes salvage from large-scale databases excessive. Therefore, more efficient search performance is important for basically deploying PEKS schemes.

　　　One of important work of system is to speed up search over encrypted keywords in public key setting deterministic encryption introduced by the Bellare et al. [2]. An encryption system is the deterministic if encryption algorithm is deterministic. Bellare et al.[2] focus on the enabling search over encrypted keyword to the efficient as search for the unencrypted keyword, such a cipher text containing given keyword can retrieved in the time complexity logarithmic in total number of cipher texts. The reasonable because encrypted keywords from tree like structure according to the binary values stored. Deterministic encryption has the two inherent limitations. First, keyword privacy can guarantee for keyword are a priori hard to guess by the adversary. Second, certain information of the message leaks inevitably via cipher text of the keywords since encryption is deterministic . Hence deterministic encryption is applicable in special scenarios.

A. Our Motivation and Basic Ideas

We are concerned to provide that highly well-organized search routine with no sacrificing semantic safety in PEKS. We use unseen star-like arrangement produced by keyword searchable cipher texts. a keyword space is typically of no high min entropy in many scenario. Semantic security is important to agreement of keyword privacy in such applications. Thus the linear search complication of existing scheme is the most important difficulty to their acceptance. Regrettably, the linear complication seems to be to be expected because the server has to search and check each cipher text, due to the information that these cipher texts are indistinguishable to the server. A earlier look shows that there is at rest space to develop explore presentation in PEKS with no sacrifice semantic safety if one can categorize the cipher texts with gracefully planned but unknown associations.

Intuitively, if the keyword searchable ciphers texts have a unknown star-like arrangement. Then search over cipher texts containing particular keywords may be accelerated. Exclusively, assume all cipher texts of the similar keyword form a chain by the connected unknown relations, and also a unknown relation exists from a public top to the first cipher text of every chain. With a keyword look for trapdoor and the top, the server seeks out the first corresponding cipher text via the equivalent relation from the top. Then a different relation can be disclosed via the establish cipher text and guides the forager to search for out the next corresponding cipher text. By moving on in this way, all identical cipher texts can be established. Clearly, the search time depends on the definite quantity of the cipher texts contain the query keyword, relatively than on the total number of all cipher texts.

To assurance suitable safety, the secreted star-like structure should protect the semantic security of keywords, which indicate that limited relations are disclose only when the equivalent keyword search trapdoor is recognized. Each sender should be able to produce the keyword -searchable cipher text with the unseen star-like arrangement by the receiver's public-key; the server have a keyword seek out trapdoor should be able to release partial relations, which is interrelated to all similar cipher texts.

II. RELATED WORK

In the earlier year discover on encrypted data has been widely investigated. Since a cryptographic viewpoint, the obtainable work is divide into two category. first is Symmetric searchable encryption and second is Public-key searchable encryption. The search presentation mainly depends on the total number of the cipher texts containing the queried keyword. For safety, the system is verified semantically protected based on the Decisional Bilinear Diffie-Hellman (DBDH) assumption [3] in the RO model. The resultant SPCHS can produce keyword-searchable cipher texts with an unseen star-like arrangement. In addition, if both the necessary IBKEM and IBE have semantic safety and ambiguity, the resultant SPCHS is semantically safe. As present are identified IBE schemes [4], [5], [6], [7] in both the RO model and the usual model, an SPCHS structure is concentrated to collision-free full-identity malleable IBKEM among ambiguity.

In 2013, Abdalla et al. projected quite a few IBKEM scheme to assemble Verifiable Random Functions2 (VRF) [8]. We prove that one of these IBKEM scheme is unsigned and collision-free full identity supple in the RO model. In [9], Freire et al. utilize the "approximation" of multilinear maps [10] to create a standard-model description of Boneh-and-Franklin (BF) IBE scheme [11].We change this IBE method into a collision-free full-identity flexible IBKEM method with semantic protection and ambiguity in the typical replica. Anonymous identity-based broadcast encryption is somewhat more complex function is unidentified identity-based broadcast encryption with efficient decryption. An corresponding application was anticipated correspondingly by Barth et al. [12] and Libert et al. [13] in the established public-key location.

Curtmola R., Garay J.,[14] describe a method is "Searchable Symmetric Encryption". Symmetric searchable encryption is also described as a Symmetric key encryption with keyword search. This primal was introduced by Song D. X., Wagner D[15].This scheme required linear search time among the range of the database. Goh E-J., Bellovin S., Agrawal R., Chang Y-C. ,Boldyreva A.[16][17][18][19][20] they are also follow this follow a line of investigation and filter Song etal.'s original work. The SEKS scheme has been verified to be semantically secure next to an adaptive opponent. It allows the search to be process in logarithmic time, even though the keyword searching requires length linear with the size of the database. According to above efforts dedicated to either verifiable security or better search performance.

The work in the above system is extended SEKS to the multi-sender state. Wang Q. [22] proposed by "Fuzzy keyword look for over encrypted information in cloud computing". As make unclear Computing become widespread, extra and extra receptive information are creature national into the shade. even though usual searchable encryption scheme permit a user to securely search greater than encrypted data all the way through keywords and selectively repossess files of interest, these techniques support only accurate keyword search. In this paper, meant for the first time we make official and explain the problem of helpful fuzzy keyword search larger than encrypted shade data whereas maintaining keyword isolation. Fuzzy keyword investigate seriously enhance collection usability by frequent the identical files whilst users' searching inputs exactly counterpart the predefined keywords or the closest promising similar files based on keyword correspondence semantics, as soon as exact match fails.

The Waters .B.R.[23] present the practical applications of SEKS and employs it to understand secure and searchable audit logs.Chase M.[24] proposed to a encrypt prepared data and a secure method to search that data. In on top of PEKS schemes, the search complication takes time linear with the numeral of all cipher text. during , an unconscious production of keyword search trapdoor is to preserve the isolation of the keyword adjacent to a inquiring trapdoor production. Kamara S.[25] proposed to support the dynamic update of the encrypted data and dynamic searchable symmetric encryption.

Searchable symmetric encryption (SSE) allow a client to encrypt its data in such a technique that this statistics can unmoving be searched. The a large amount instantaneous submission of SSE is to shade storage, someplace it enable a client to securely farm out its data to an untrusted shade bringer exclusive of sacrifice the ability to search over it. SSE have been the focal point of on the go examine and a huge amount of schemes that accomplish a mixture of levels of safety measures and efficiency have be projected. Any useful SSE arrangement, on the other hand, should satisfy the subsequent property: sub linear search time, protection alongside adaptive preferred keyword attacks, compact guide and the capacity to add and delete files resourcefully.

Additional improved extra security in [26] at the cost of the large index. Cash D. planned by Dynamic searchable encryption in extremely huge database. This scheme simultaneously achieves strong security and high efficiency. Dynamic Searchable Symmetric Encryption (DSSE) enables a consumer to achieve keyword query and keep informed operation on the encrypted organizer collections. DSSE has more than a few important applications such as privacy-preserving data outsourcing for computing clouds. In this document, we residential a new DSSE format that achieve the maximum time alone in the middle of all compared alternative with little in sequence escape, non-interactive and professional updates, compressed client storage space, low attendant storage space for huge file-keyword pair with an trouble-free intend and accomplishment. Our method achieve these advantageous properties with a extremely effortless figures arrangement (i.e., a bit matrix supported with two static hash tables) that enables resourceful yet secure explore/inform operation on it. We establish that our method is protected and established that it is realistic with huge number of file-keyword pair smooth with an accomplishment on trouble-free hardware configurations.

The similar work on PEKS, Abdalla et al. [28] file some gaps write reliability for PEKS and deals with the conversion among premitives related to PEKS .some labors have also been dedicated to make PEKS flexible. The work of this type include conjunctive search [29], [30], [31], [32], [33], [34], variety search [35], [36], [37], compartment search , time-scope search [38], parallel search [39], allowed search [49], [50], impartiality test between mixed cipher texts [51], and fuzzy keyword search [52]. Searchable encryption is worn to prop up search over encrypted data store on shade servers. established searchable encryption no more than chains accurate keyword search as a substitute of supplementary bendable fuzzy keyword search.

To explain this dilemma, a topical promising archetype, name fuzzy keyword searchable encryption, has be projected. in attendance have been some proposal considered for fuzzy keyword explore in the symmetric key situation, but not a bit efficient scheme in the public key setting. In this paper, we proposition a new primal of interactive public type encryption among unclear keyword explore (IPEFKS), which chains proficient fuzzy keyword search greater than encrypted figures in the public key background. We construct and spend a homomorphic encryption base IPEFKS system. In adding together, Arriaga et al. [53] projected a PEKS scheme to maintain the isolation of keyword search trapdoors.

A chain-like construction is describe to velocity awake the search on encrypted keywords. One can message that the sequence in [40] cannot be completely unseen to the server and drip the reliability of the keywords . To recognize an resourceful keyword search, Bellare et al. [2] introduce deterministic public key encryption (PKE) and dignified a ratinalization examination "the connected when the equivalent generation as heavy while expected". A deterministic searchable encryption system allow capable keyword search as condition the keywords be not encrypted.

Bellare et al. [2] showed a well obtainable a deterministic PKE system and a general revolution starting a randomized PKE toward a deterministic PKE in the random oracle model. Afterward, deterministic PKE scheme protected in the usual model be in parallel projected next to Bellare et al. [41] and Boldyreva et al. [42]. Particularly we think about seven thinking of isolation for deterministic encryption, together with six forms of semantic protection and an in distinguish ability view, and show them all corresponding.

We then current a deterministic method for the protected encryption of consistently and independently spread letters based exclusively on the subsistence of trapdoor in one direction permutation. The earlier uses common convolution assumption and the structure is common, while the final exploit substantial complexity guess and have enhanced efficiency. Brakerski et al. [43] projected the deterministic PKE scheme by way of enhanced security, even though these schemes are at a halt not semantically secure. So far, deterministic PEKS schemes can agreement semantic security simply condition the keyword freedom has a soaring min-entropy. If not, an opposition can extort the encrypted keyword as a result of a straightforward encrypt-and-test bother. Therefore, deterministic PEKS schemes be relevant to application somewhere the keyword space is of a high min-entropy

III. IMPLICATIONS OF THIS SURVEY
A. *Proposed System as a Solution for Existing System*
In our proposed system we provide more security as well as we search keyword in a specified file not overall database that make a minimization of time and search keyword as fast as possible without sacrificing semantic security. Build a generic SPCHS construction with Identity-Based Encryption (IBE) and collision-free full-identity malleable IBKEM.

B. *Our Work*
We initiate by officially defining the idea of Searchable Public-key Cipher texts with secret Structures and its semantic security. In this new conception, keyword searchable cipher texts with their unknown structures can be generated in the public key location; with a keyword look for trapdoor, incomplete associations can be disclosed to show the innovation of all corresponding cipher texts. Semantic security is definite for both the keywords and the unknown structures. It is worth noting that this new perception and its semantic safety are appropriate for keyword-searchable cipher texts with any kind of unknown structures. In difference, the idea of conventional PEKS does not include any unseen structure between the PEKS cipher texts; likewise, its semantic safety is only defined for the keywords.

We build a straightforward SPCHS from scrape in the random oracle (RO) model. The system generates keyword-searchable cipher texts with a secret star-like structure. The search presentation mostly depends on the real number of the cipher texts contain the query keyword. For safety, the system is established semantically safe based on the Decisional Bilinear Diffie- Hellman (DBDH) hypothesis in the RO model. We are also paying attention in provided that a standard SPCHS building to produce keyword-searchable cipher texts with a secret star-like construction. Our standard SPCHS is stimulated by several exciting explanation on Identity-Based Key Encapsulation Mechanism (IBKEM).

In IBKEM, a sender encapsulates a key K to an intentional receiver ID. Of course, receiver ID can de capsulate and achieve K, and the sender know that receiver ID will achieve K. conversely, a non-intended receiver ID0 may also try to de capsulate and achieve K0. We examine that, (1) it is typically the case that K and K0 are self-determining of every other from the view of the receivers, and (2) in some IBKEM the sender may also know K0 obtained by receiver ID0. We refer to the former goods as conflict freeness and to the final since full-identity flexibility. An IBKEM scheme is said to be collision-free full-identity impressionable if it possesses together property. We build a basic SPCHS creation with Identity-Based Encryption and collision-free full-identity malleable IBKEM.

IV. COMPARATIVE STUDY

In the existing system there are some limitations such as Deterministic encryption is only applicable in special context. It means that deterministic encryption having to limitations. First is that keyword privacy in this keyword identification process is very complicated. It identify the keyword is very difficult task to another person. Second is file leakage. When we send a file from location one to another at that time some information is lost so encryption is applicable for special scenario.

In the existing system it give linear search time with total no of keywords so according to this limitation it is difficult to get the large no of data from the database .In recently scheme security is only provided for keyword and use chain like structure so the problem of data loss, less frequency is occurred. In previous system size of contents is large so it contains huge database .According to study of previous paper the efficiency is very less. In previous generation privacy is maintain according to keyword search. In system keyword is check by all over database not for particular file due to this search time complexity is increase. For comparing keywords takes more time.

V. CONCLUSIONS

In the existing system there are some limitations such as Deterministic encryption is only applicable in special context. It means that deterministic encryption having to limitations. First is that keyword privacy in this keyword identification process is very complicated. It identify the keyword is very difficult task to another person. Second is file leackage. When we send a file from location one to another at that time some information is lost so encryption is applicable for special scenario.

In the existing system it give linear search time with total no of keywords so according to this limitation it is difficult to get the large no of data from the database .In recently scheme security is only provided for keyword and use chain like structure so the problem of data loss, less frequency is occurred. In previous system size of contents is large so it contain huge database .According to study of previous paper the efficiency is very less. In previous generation privacy is maintain according to keyword search. In system keyword is check by all over database not for particular file due to this search time complexity is increase. For comparing keywords takes more time.file. Obtain public key searchable encryption allowing content a search.

REFERENCES

[1]   Ateniese G., Gasti P.: Universally Anonymous IBE Based on [1] Boneh 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) the Quadratic Residuosity Assumption. In: Fischlin M. (ed.) CT-RSA 2009. LNCS, vol. 5473, pp. 32-47. Springer, Heidelberg (2009)

[6]   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)

[7]   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)

[8]   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)

[9]   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)

[10]   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)

[11]   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)

[12]   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)

[13]   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)

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

[15]   Goh E.-J.: Secure Indexes. Cryptography ePrint Archive, Report 2003/216 (2003)

[16]   Bellovin S. M., Cheswick W.R.: Privacy-Enhanced Searches Using Encrypted Bloom Filters. Cryptography ePrint Archive, Report 2004/022 (2004)

[17]   Agrawal R., Kiernan J., Srikant R., Xu Y.: Order Preserving Encryption for Numeric Data. In: Proceedings of the 2004 ACM SIGMOD international conference on Management of data, pp. 563-574. ACM (2004)

[18]   Chang Y.-C., Mitzenmacher M.: Privacy Preserving Keyword Searches on Remote Encrypted Data. In: Ioannidis J., Keromytis A. and Yung M. (eds.) ACNS 2005. LNCS, vol. 3531, pp. 442-455. Springer, Heidelberg (2005)

[19]   Boldyreva A., Chenette N., Lee Y., O'Neill A. : Order-Preserving Symmetric Encryption. In: Joux A. (ed.) EUROCRYPT 2009. LNCS, vol. 5479, pp. 224-241. Springer, Heidelberg (2009)

[20]   Bao F., Deng R. H., Ding X., Yang Y.: Private Query on Encrypted Data in Multi-User Settings. In: Chen L., Mu Y., Susilo W. (eds.) ISPEC 2008. LNCS, vol. 4991, pp. 71-85. Springer, Heidelberg (2008)

[21]   Li J., Wang Q., Wang C., Cao N., Ren K., Lou W.: Fuzzy Keyword Search over Encrypted Data in Cloud Computing. In: IEEE INFOCOM 2010, pp. 1-5. (2010)

[22]   Waters B. R., Balfanz D., Durfee G., Smetters D. K.: Building an Encrypted and Searchable Audit Log. In: NDSS 2004 (2004)

[23]   Chase M., Kamara S.: Structured Encryption and Controlled Disclosure. In: M. Abe (ed.) Advances in Cryptology - ASIACRYPT 2010. LNCS, vol. 6477, pp. 577-594. Springer, Heidelberg (2010)

[24]   Kamara S., Papamanthou C., Roeder T.: Dynamic searchable symmetric encryption. In ACM Conference on Computer and Communications Security, pp. 965976 (2012)

[25]   Kamara S., Papamanthou C.: Parallel and Dynamic Searchable Symmetric Encryption. In: Sadeghi A.-R. (ed.) FC 2013. LNCS, vol.7859, pp. 258-274. Springer, Heidelberg (2013)

[26]   Cash D., Jaeger J., Jarecki S., Jutla C., Krawczyk H., Ros M.-C., Steiner M.: Dynamic Searchable Encryption in Very Large Databases: Data Structures and Implementation. In: NDSS 2014.

[27]   Abdalla M., Bellare M., Catalano D., Kiltz E., Kohno T., Lange T., Malone-Lee J., Neven G., Paillier P., Shi H.: Searchable Encryption Revisited: Consistency Properties, Relation to Anonymous IBE, and Extensions. In: Shoup V. (ed.) CRYPTO 2005. LNCS, vol. 3621, pp. 205-222. Springer, Heidelberg (2005)

[28]   Park D. J., Kim K., Lee P. J.: Public Key Encryption with Conjunctive Field Keyword Search. In: Lim C. H. and Yung M. (eds.) WISA 2004. LNCS, vol. 3325, pp. 73-86. Springer, Heidelberg (2004)

[29]   Golle P., Staddon J., Waters B. R.: Secure Conjunctive Keyword Search over Encrypted Data. In: Jakobsson M., Yung M., Zhou J. (eds.) ACNS 2004. LNCS, vol. 3089, pp. 31-45. Springer, Heidelberg (2004)

[30]   Ballard L., Kamara S., Monrose F.: Achieving Efficient Conjunctive Keyword Searches over Encrypted Data. In: Qing S. et al. (eds.) ICICS 2005. LNCS, vol. 3783, pp. 414-426. Springer, Heidelberg (2005)

[31]   Hwang Y. H., Lee P. J.: Public Key Encryption with Conjunctive Keyword Search and Its Extension to a Multi-user System. In: Takagi T., Okamoto T., Okamoto E. and Okamoto T. (eds.) Pairing 2007. LNCS, vol. 4575, pp. 2-22. Springer, Heidelberg (2007)

[32]   Ryu E.K., Takagi T.: Efficient Conjunctive Keyword-Searchable Encryption. In: 21st International Conference on Advanced Information Networking and Applications Workshops, pp. 409-414. IEEE (2007)

[33]   Baek J., Safavi-Naini R., Susilo W.: Public Key Encryption with Keyword Search Revisited. In: Gervasi O. (ed.) ICCSA 2008. LNCS, vol. 5072, pp. 1249-1259. Springer, Heidelberg (2008)

[34]   Bethencourt J., Chan T.-H. H., Perrig A., Shi E., Song D.: Anonymous Multi-Attribute Encryption with Range Query and Conditional Decryption. Technical Report CMU-CS-06-135 (2006)

[35]   Shi E., Bethencourt J., Chan T.-H. H., Song D., Perrig A.: Multi- Dimensional Range Query over Encrypted Data. In: IEEE S&P 2007, pp. 350-364. IEEE (2007)

[36]   Boneh D., Waters B. R.: Conjunctive, Subset, and Range Queries on Encrypted Data. In: Vadhan S. P. (ed.) TCC 2007. LNCS, vol. 4392, pp. 535-554. Springer, Heidelberg (2007)

[37]   Davis D., Monrose F., Reiter M. K.: Time-Scoped Searching of Encrypted Audit Logs. In: Lopez J., Qing S., Okamoto E. (eds.) ICICS 2004. LNCS, vol. 3269, pp. 532-545. Springer, Heidelberg (2004)

[38]   Cheung D. W., Mamoulis N., Wong W. K., Yiu S. M., Zhang Y.: Anonymous Fuzzy Identity-based Encryption for Similarity Search. In: Cheong O., Chwa K.-Y and Park K. (eds.) ISAAC 2010. LNCS, vol. 6505, pp. 61-72. Springer, Heidelberg (2010)

[39]   Camenisch J., Kohlweiss M., Rial A., Sheedy C.: Blind and Anonymous Identity-Based Encryption and Authorised Private Searches on Public Key Encrypted Data. In: Jarecki S. and Tsudik G. (eds.) PKC 2009. LNCS, vol. 5443, pp. 196-214. Springer, Heidelberg (2009)

[40]   Bellare M., Fischlin M., O'Neill A., Ristenpart T.: Deterministic Encryption: Definitional Equivalences and Constructions without Random Oracles. In: Wagner D. (ed.) CRYPTO 2008. LNCS, vol. 5157, pp. 360-378. Springer, Heidelberg (2008)

[41]   Boldyreva A., Fehr S., O'Neill A. : On Notions of Security for Deterministic Encryption, and Efficient Constructions without Random Oracles. In: Wagner D. (ed.) CRYPTO 2008. LNCS, vol. 5157, pp. 335-359.

Springer, Heidelberg (2008)

[42] Brakerski Z., Segev G.: Better Security for Deterministic Public- Key Encryption: The Auxiliary-Input Setting. In: Rogaway P. (ed.) CRYPTO 2011. LNCS, vol. 6841, pp. 543-560. Springer, Heidelberg (2011)

[43] Menezes A. J., Okamoto T., Vanstone S. A.: Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field. IEEE Transactions on Information Theory, 39(5), pp. 1639-1646 (1993)

[44] Frey G., Muller M., Ruck H.-G.: The Tate Pairing and the Discrete Logarithm Applied to Elliptic Curve Cryptosystems. IEEE Transactions on Information Theory, vol. 45, no. 5, pp. 1717-1719 (1999)

[45] Abdalla M., Bellare M., Neven G.: Robust encryption. In: Micciancio G. (ed.) TCC 2010. LNCS, vol. 5978, pp. 480497. Springer, Heidelberg (2010)

[46] Izabach_ene M., Pointcheval D.: New Anonymity Notions for Identity-Based Encryption. In: Ostrovsky R., De Prisco R. and Visconti I. (eds.) SCN 2008. LNCE, vol. 5229, pp. 375-391. Springer, Heidelberg (2008)

[47] Waters B.: Efficient Identity-Based Encryption Without Random Oracles. In: Cramer R. (ed.), Advances in Cryptology – EUROCRYPT 2005. LNCS, vol. 3494, pp. 1-17. Springer, Heidelberg (2005)

[48] Tang Q., Chen X.: Towards asymmetric searchable encryption with message recovery and flexible search authorization. ASIACCS 2013, pp. 253-264 (2013)

[49] Ibraimi L., Nikova S., Hartel P. H., Jonker W.: Public-Key Encryption with Delegated Search. In: Lopez J. and Tsudik G. (eds.) ACNS 2011. LNCS, vol. 6715, pp. 532-549. Springer, Heidelberg (2011)

[50] Yang G., Tan C. H., Huang Q., Wong D. S.: Probabilistic Public Key Encryption with Equality Test. In: Pieprzyk J. (ed.) CT-RSA 2010. LNCS, vol. 5985, pp. 119-131. Springer, Heidelberg (2010)

[51] Xu P., Jin H., Wu Q., Wang W.: Public-Key Encryption with Fuzzy Keyword Search: A Provably Secure Scheme under Keyword Guessing Attack. IEEE Transactions on Computers, 62(11), pp. 2266-2277 (2013)

[52] Arriaga A., Tang Q., Ryan P.: Trapdoor Privacy in Asymmetric Searchable Encryption Schemes. In: Pointcheval D. and Vergnaud D. (eds.) AFRICACRYPT 2014. LNCS, vol. 8469, pp. 31-50. Springer, Heidelberg (2014)