International Journal of Pure and Applied Mathematics
Volume 116 No. 9 2017, 243-248
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
Special Issue

ijpam.eu

FAST KEYWORD SEARCH USING SEARCHABLE PUBLIC KEY CIPHERTEXT WITH HIDDEN STRUCTURE

K.P.Kaliyamurthie
Dean, Department of CSE,
Bharth University,Chennai-73.
kpkaliyamurthie@gmail.com

Abstract: Semantically secure PEKS schemes take search time linear with the total number of all cipher texts. The concept of Searchable Public-key Cipher texts with Hidden Structures (SPCHS) and its semantic security will enable the keyword-searchable cipher texts with their hidden structures can be generated in the public key setting. The objective of this project is to implement the concept of SPCHS (searchable public key cipher text with hidden structure) as a variant of PEKS (public key encryption keyword search). The new concept allows keyword-searchable cipher texts to be generated with a hidden structure.

Keywords: Malware, Android, Smartphone, Security.

1. Introduction

A public-key encryption scheme is said to be deterministic if its encryption algorithm is deterministic. Deterministic encryption was introduced by Bellare, Boldyreva, and O'Neill. The motivating application they gave is efficiently searchable encryption. Deterministic encryption permits logarithmic time search on encrypted data, while randomized encryption only allows linear time search, meaning a search requires scanning the whole database. This difference is crucial for large outsourced databases which cannot afford to slow down search. Of course deterministic encryption cannot achieve the classical notions of security of randomized encryption, but formalize a semantic security style notion PRIV that captures the "best possible" privacy achievable when encryption is deterministic, namely that an adversary provided with encryptions of plaintexts drawn from a message-space of high (super-logarithmic) min-entropy should have negligible advantage in computing any public-key independent partial information function of the plaintexts. The authors provide some schemes in the random-oracle (RO) model meeting this definition but leave open the problem of finding standard model schemes. The PRIV definition captures intuition well but is hard to work with. We would like to find simpler, alternative definitions of privacy for deterministic encryption- restricted forms of semantic security as well as an in distinguish ability style definition— that are equivalent to PRIV[4]. We would also like to find schemes not only in the standard model but based on general assumptions. Notions considered. We define seven notions of privacy for deterministic encryption inspired by the work of. These include a notion IND in the in distinguishability style and six notions —A-CSS, B-CSS, BB-CSS, A-SSS, BSSS, BB-SSS— in the semantic-security style[1,5,6]. The IND definition — adapted from, asks that the adversary be unable to distinguish encryptions of plaintexts drawn from two, adversary-specified, high-entropy message spaces, and is simple and easy to use. The semantic security notions are organized along two dimensions. The first dimension is the class of partial information functions considered, and we look at three choices, namely arbitrary (A), boolean (B), or balanced boolean (BB). (A boolean function is balanced if the probabilities that it returns 0 or 1 are nearly the same.) The second dimension is whether the formalization is simulation (S) based or comparison (C) based.1 The PRIV notion of is A-CSS in our taxonomy. Low-end notions — think of BB as the lowest, then B then A and similarly C then S in the other dimension— are simpler and easier to use in applications, while high end ones are more intuitively correct[2,3]. The question is whether the simplifications come at the price of power.

2. Related work

The foundations of public-key encryption, as laid by Goldwasser and Micaliand their successors, involve two central threads. The first is definitional equivalences which aim not only to increase our confidence that we have the "right" notion of privacy but also to give us definitions that are as easy to use in applications as possible. (Easy-to-use indistinguishability is equivalent to the more Intuitive, but also more complex, semantic security. The second

(of the two threads) is to obtain schemes achieving the definitions under assumptions as minimal as possible. In this paper we pursue these same two threads for deterministic encryption, proving definitional equivalences and providing constructions based on general assumptions[7,8,9]. A public-key encryption scheme is said to be deterministic if its encryption algorithm is deterministic. Deterministic encryption was introduced. The motivating application they gave is efficiently searchable encryption. Deterministic encryption permits logarithmic time search on encrypted data, while randomized encryption only allows linear time search, meaning a search requires scanning the whole database.

Anonymous Broadcast Encryption: Adaptive Security and Efficient Constructions in the Standard Model Benoıt Libert, Kenneth. Paterson, and Elizabeth A. Quaglia University's Catholique de Louvain, ICTEAM Institute, Belgium Information Security Group, Royal Holloway, University of London, U.K, 2009 Broadcast Encryption (BE) addresses the issue of confidentially broadcasting a message to an arbitrary subset drawn from a universe of users. We will call the universe of n users U and the target, or privileged, set S, where $S \subseteq U$. Since its introduction in 1993 by Fiat and, various flavors of BE have been introduced: the scheme can be in a symmetric or asymmetric setting; the set of receivers could be static or dynamic; revocation and traitor-tracing algorithms could be integrated into the system, users' keys might or might not be updated and then forward secrecy may be achieved. We refer to some of the relevant work in the area and the references therein. One of the fundamental properties of a BE scheme is collusion resistance in the sense that no coalition of users in $U \setminus S$ should be able to recover the message. In the literature we can find several schemes that resist collusion attacks mounted by coalitions of at most $t < n$ users; only some schemes are fully collusion-resistant, i.e. they can tolerate attacks by coalitions of any size[11].

Fuzzy Keyword Search over Encrypted Data in Cloud Computing Jin Li, Qian Wang, Cong Wang, Ning Cao, KuiRen, and Wenjing Lou†Department of ECE, Illinois Institute of Technology Department of ECE, Worcester Polytechnic Institute Email: jinli, qian, cong, kren@ece.iit.edu, ncao, wjlou@ece.wpi.edu,2010 Privacy-preserving fuzzy search for achieving effective utilization of remotely stored, encrypted data in Cloud Computing. We design an advanced technique (i.e., wildcard-based technique) to construct the storage-efficient fuzzy keyword sets by exploiting a significant observation on the similarity metric of edit distance[10,12]. Based on the constructed fuzzy keyword sets, we further propose an efficient fuzzy keyword search scheme. Through rigorous security analysis, we show that our proposed solution is secure and privacy-preserving, while correctly realizing the goal of fuzzy keyword search. As our ongoing work, we will continue to research on security mechanisms that support: 1) search semantics that takes into consideration conjunction of keywords, sequence of keywords, and even the complex natural language semantics to produce highly relevant search results; and 2) search ranking that sorts the searching results according to the relevance criteria.Public-Key Encryption with Fuzzy Keyword Search: A Provably Secure Scheme under Keyword Guessing Attack PengXu, Hai Jin, Senior Member, IEEE, Qianhong Wu, Member, IEEE, and Wei Wang,2013.

The polynomial size of the keyword space in the real world in this paper investigated the insecurity of PEKS under keyword guessing attack. Motivated by this, we proposed the new primitive of PEFKS to resist KGA and formalized the SS-CKA and the IK-NCK-KGA securities of PEFKS, followed with a universal transformation from anonymous IBE to PEFKS. We proved that the resulting PEFKS is SS-CKA and the IK-NCK-KGA secure if the underlying IBE is an on-ID-CPA secure. Following the generic construction, we instantiated a secure PEFKS scheme based the anonymous IBE scheme in. We further studied how to sort the keywords if they are not uniformly distributed. Finally, it was shown that the outputs of any other fuzzy function do not have min-entropy greater than the outputs of our fuzzy function. This implies that our fuzzy function is optimal and produces the maximum min-entropy to the adversary who knows the fuzzy keyword search trapdoors of all keywords[13,14].

Dynamic Searchable Encryption in Very-Large Databases: Data structures and Implementation David Cash, Joseph Jaeger, Stanislaw Jarecki, CharanjitJutla, Hugo Krawczyk, Marcel-CatalinRosu, and Michael Steiner, Rutgers University, University of California, Irvine IBM Research,2014.

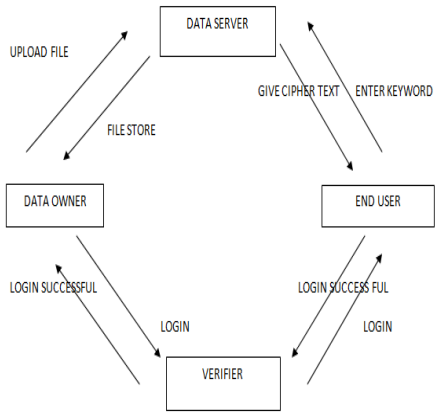
The tension between security and performance requirements for SSE systems pose non-trivial challenges for both the Cryptographic design and the data structures needed to support this design, as well as for their implementation. Leakage Minimization calls for randomization of data locations in the encrypted database, EDB, in order to obscure any relations in the original clear-text database. This results in the need to randomize access to edb elements even when these elements are logically correlated (e.g., the set of documents containing a given keyword). This random-order access is affordable for Ram-resident but becomes prohibitive

for disk-resident ones; on the other hand, restricting an implementation to a RAM-resident means limiting the database sizes one can support. Thus, much of the work reported here, both at the abstract data structure level and the specifics of their implementation are driven by the need to bridge over this Security-performance conundrum, and are intended to find a balance between randomized ordering of data, locality of access and parallel processing. In particular, our two-level scheme seems to achieve a desirable trade-off between these competing requirements.

3. Proposed methodology

Searchable public-key cipher texts with hidden structures (SPCHS) for keyword search as fast as possible without sacrificing semantic security of the encrypted keywords. Two collision free full-identity malleable IBKEM instances, which are semantically secure and anonymous, respectively in the RO and standard models. Algorithm Trapdoor allows the receiver to delegate a keyword search trapdoor to the server.

Proposed Architecture



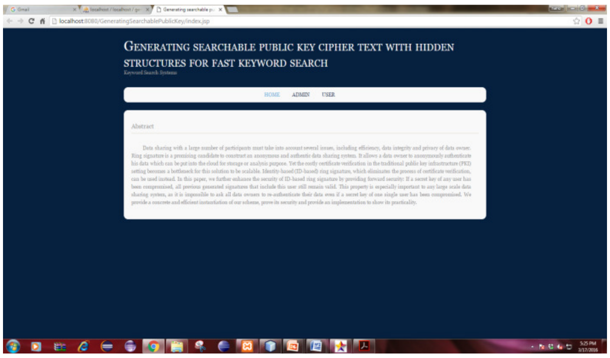
Data Owner firstly login and then it upload a file into the data server. Then that files are successfully stored by the data server. It uploads the files with searchable keyword. Data server is stored server files. Data server also detects the attacker and attacker's entry will be stored by the data server in the database. All transactions record is also stored by the data server. Data server gives the secret key to the end user. It also gives the file to the end user for download. End user firstly login after that it will send the cipher text to the data server. After that data server passes a public key. Then end user will be giving the file name to the data server. If the file name present in the data server with respected keyword then and then only that file are downloaded, otherwise not. It gives file with their ratio and delay. Verifier is to check the entry of both data owner and end user[15,16,17]. If the entry is present in the database then and then only data owner and end user can login successfully, otherwise it will get rejected by the verifier.

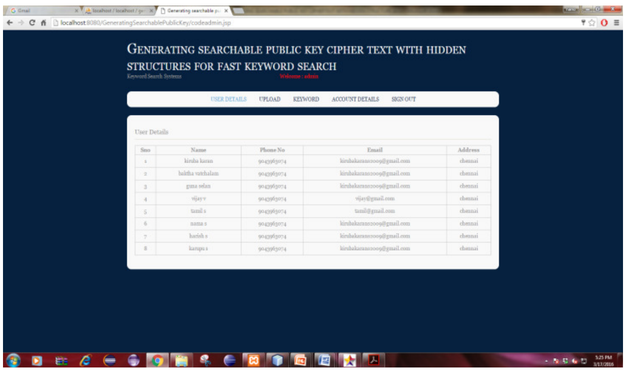
Algorithm

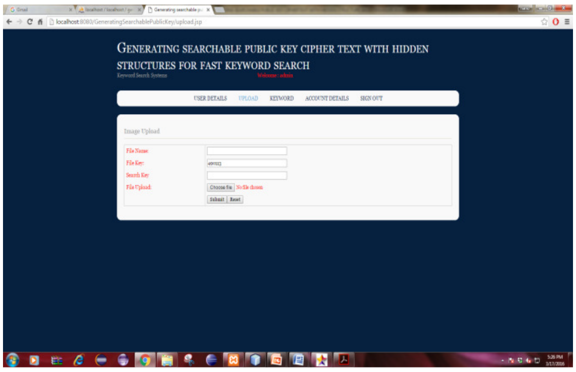
1. Choose two distinct prime numbers p and q.
2. For security purposes, the integer's p and q should be chosen at random, and should be similar in magnitude but 'differ in length by a few digits to make factoring harder. Prime integers can be efficiently found using a primarily[18].
3. Compute n = p q.
4. n is used as the modulus for both the public and private keys. Its length, usually expressed in bits, is the key length.
5. Compute $\varphi(n) = \varphi(p)\varphi(q) = (p-1)(q-1) = n-(p+q-1)$, where φ is Euler's toting function. This value is kept private.
6. Choose an integer e such that $1 < e < \varphi(n)$ and $\gcd(e, \varphi(n)) = 1$; i.e., e and φ(n) are co prime.
7. Determine d as $d \equiv e^{-1} \pmod{\varphi(n)}$; i.e., d is the modular multiplicative inverse of e (modulo φ(n))
8. This is more clearly stated as: solve ford given $d \cdot e \equiv 1 \pmod{\varphi(n)}$
9. e having a short bit-length and small Hamming weight results in more efficient encryption – most commonly $2^{16} + 1 = 65{,}537$. However, much smaller values of e (such as 3) have been shown to be less secure in some settings.
10. e is released as the public key exponent.
11. d is kept as the private key exponent.
12. The public key consists of the modulus n and the public (or encryption) exponent e. The private key consists of the modulus n and the private (or decryption) exponent d, which must be kept secret. p, q, and φ(n) must also be kept secret because they can be used to calculate d.
13. An alternative, used by, is to choose d matching $de \equiv 1 \pmod{\lambda}$ with $\lambda = \text{lcm}(p-1, q-1)$, where lcm is the least common multiple. Using λ instead of φ(n) allows more choices for d. λ can also be defined using the Carmichael function, λ(n).
14. Since any common factors of (p − 1) and (q − 1) are present in the factorization of pq − 1, it is recommended that (p − 1) and (q − 1) have only very small common factors, if any besides the necessary

4. Experimental results

The concept of Searchable Public-key Ciphertext with Hidden Structures (SPCHS) and its semantic security. In this new concept, keyword-searchable ciphertext with their hidden structures can be generated in the public key setting; with a keyword search trapdoor, partial relations can be disclosed to guide the discovery of all matching ciphertext. Semantic security is defined for both the keywords and the hidden structures. It is worth noting that this new concept and its semantic security are suitable for keyword-searchable ciphertext with any kind of hidden structures. In contrast, the concept of traditional PEKS does not contain any hidden structure among the PEKS ciphertext; correspondingly, its semantic security is only defined for the keywords. Following the SPCHS definition, we construct a simple SPCHS from scratch in the random oracle (RO) model. The scheme generates keyword-searchable ciphertexts with a hidden star-like structure[19]. The search performance mainly depends on the actual number of the ciphertexts containing the queried keyword.







5. Conclusion

SPCHS seems a promising tool to solve some challenging problems in public-key searchable encryption. One application may be to achieve retrieval completeness verification which, to the best of our knowledge, has not been achieved in existing PEKS schemes. Specifically, by forming a hidden ring-like structure, i.e., letting the last hidden pointer always point to the head, one can obtain PEKS allowing checking the completeness of the retrieved ciphertexts by checking whether the pointers of the returned ciphertexts form a ring. Another application may be to realize public key encryption with content search, a similar functionality realized by symmetric searchable encryption. Such kind of content-searchable encryption is useful in practice, e.g., to filter the encrypted spasm. Specially, by forming a hidden tree-like structure between the sequentially encrypted words in one file, one can obtain public-key searchable encryption allowing content search (e.g., to find whether there are specific contents in an encrypted file). The search complexity is linear with the size of the queried content.

References

[1]D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano, “Publickey encryption with keyword search,” in Advances in Cryptology—EUROCRYPT (Lecture Notes in Computer Science), vol. 3027,C. Cachin and J. L. Camenisch, Eds. Berlin, Germany: Springer-Verlag,2004, pp. 506–522.

[2] M. Bellare, A. Boldyreva, and A. O’Neill, “Deterministic and efficiently searchable encryption,” in Advances in Cryptology—CRYPTO (Lecture Notes in Computer Science), vol. 4622, A. Menezes, Ed. Berlin,Germany: Springer-Verlag, 2007, pp. 535–552.

[3] D. Boneh and X. Boyen, "Efficient selective-ID secure identity-based encryption without random oracles," in Advances in Cryptology—EUROCRYPT (Lecture Notes in Computer Science), vol. 3027, C. Cachin and J. Camenisch, Eds. Berlin, Germany: Springer-Verlag, 2004, pp. 223–238.
[4]Udayakumar R., Kaliyamurthie K.P., Khanaa, Thooyamani K.P., Data mining a boon: Predictive system for university topper women in academia, World Applied Sciences Journal, v-29, i-14, pp-86-90, 2014.
[5]Kaliyamurthie K.P., Parameswari D., Udayakumar R., QOS aware privacy preserving location monitoring in wireless sensor network, Indian Journal of Science and Technology, v-6, i-SUPPL5, pp-4648-4652, 2013.
[6]Brintha Rajakumari S., Nalini C., An efficient cost model for data storage with horizontal layout in the cloud, Indian Journal of Science and Technology, v-7, i-, pp-45-46, 2014.
[7]Brintha Rajakumari S., Nalini C., An efficient data mining dataset preparation using aggregation in relational database, Indian Journal of Science and Technology, v-7, i-, pp-44-46, 2014.
[8]Khanna V., Mohanta K., Saravanan T., Recovery of link quality degradation in wireless mesh networks, Indian Journal of Science and Technology, v-6, i-SUPPL.6, pp-4837-4843, 2013.
[9]Khanaa V., Thooyamani K.P., Udayakumar R., A secure and efficient authentication system for distributed wireless sensor network, World Applied Sciences Journal, v-29, i-14, pp-304-308, 2014.
[10]Udayakumar R., Khanaa V., Saravanan T., Saritha G., Retinal image analysis using curvelet transform and multistructure elements morphology by reconstruction, Middle - East Journal of Scientific Research, v-16, i-12, pp-1781-1785, 2013.
[11]Khanaa V., Mohanta K., Saravanan. T., Performance analysis of FTTH using GEPON in direct and external modulation, Indian Journal of Science and Technology, v-6, i-SUPPL.6, pp-4848-4852, 2013.
[12]Kaliyamurthie K.P., Udayakumar R., Parameswari D., Mugunthan S.N., Highly secured online voting system over network, Indian Journal of Science and Technology, v-6, i-SUPPL.6, pp-4831-4836, 2013.
[13]Thooyamani K.P., Khanaa V., Udayakumar R., Efficiently measuring denial of service attacks using appropriate metrics, Middle - East Journal of Scientific Research, v-20, i-12, pp-2464-2470, 2014.
[14]R.Kalaiprasath, R.Elankavi, Dr.R.Udayakumar, Cloud Information Accountability (Cia) Framework Ensuring Accountability Of Data In Cloud And Security In End To End Process In Cloud Terminology, International Journal Of Civil Engineering And Technology (Ijciet)Volume 8, Issue 4, Pp. 376–385, April 2017.
[15]R.Elankavi, R.Kalaiprasath, Dr.R.Udayakumar, A fast clustering algorithm for high-dimensional data, International Journal Of Civil Engineering And Technology (Ijciet), Volume 8, Issue 5, Pp. 1220–1227, May 2017.
[16]R. Kalaiprasath, R. Elankavi and Dr. R. Udayakumar. Cloud. Security and Compliance - A Semantic Approach in End to End Security, International Journal Of Mechanical Engineering And Technology (Ijmet), Volume 8, Issue 5, pp-987-994, May 2017.
[17]Thooyamani K.P., Khanaa V., Udayakumar R., Virtual instrumentation based process of agriculture by automation, Middle - East Journal of Scientific Research, v-20, i-12, pp-2604-2612, 2014.
[18]Udayakumar R., Thooyamani K.P., Khanaa, Random projection based data perturbation using geometric transformation, World Applied Sciences Journal, v-29, i-14, pp-19-24, 2014.
[19]Udayakumar R., Thooyamani K.P., Khanaa, Deploying site-to-site VPN connectivity: MPLS Vs IPSec, World Applied Sciences Journal, v-29, i-14, pp-6-10, 2014.