ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 6, Special Issue 3, March 2017

5th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '17)

13th-14th March 2017

Organized by

Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India.

Creating User Security Guarantees by KPABE Scheme Search over Cloud Data

S.Sindhu[1], A.Kannammal[2], Sathish Kumar[3]

UG Scholar, Jayam College of Engg &Tech, Dharmapuri, India[1]

Head of the Department (CSE), Jayam College of Engg &Tech Dharmapuri, India [2]

Assistant Professor, Jayam College of Engg & Tech, Dharmapuri, India [3]

ABSTRACT: Cloud brokers have been recently introduced as an additional computational layer to facilitate cloud selection and service management tasks for cloud consumers. However, existing brokerage schemes on cloud service selection typically assume that brokers are completely trusted, and do not provide any guarantee over the correctness of the service recommendations. It is then possible for a compromised or dishonest broker to easily take advantage of the limited capabilities of the clients and provide incorrect incomplete responses. We propose a cloud based secure data system, which allows trusted authority to securely store their secret data on the semi-trusted cloud service providers, and selectively share their secret data with a wide range of data receiver. Different from previous cloud-based data system, Data owners encrypt their secret data for the data receivers using KP-ABE Encryption scheme. Another advanced specification is, if any data receiver want personal file to download, the data receiver will send the request to the authority. The authority owner has the Access Control. If the Owner wants to share the original file with the data receiver, he shares these keys to data receiver. After accepts request the data receiver download the secret key and use this key to download the original data. In addition for classification of data files a new classification algorithm is proposed

KEYWORDS: Cloud computing, KP-ABE, SVM, Data sharing.

I. INTRODUCTION

Nowadays, as an emerging and efficient computing model, cloud computing has attracted widespread attention and support in many fields. In the cloud computing environment, many services such as resource renting, application hosting, and service outsourcing show the core concept of an on-demand service in the IT field. In recent years, many IT tycoons are developing their business cloud computing system, e.g. Amazon'sEC2[1], Amazon's S3[2], Google App Engine[3] and Microsoft's Azure[4] etc. Cloud computing can provide flexible computing capabilities, reduce costs and capital computing capabilities, reduce costs and capital expenditures and charge according to usage.Although the cloud computing paradigm brings manybenefits, there are many unavoidable security problems caused by its inherent characteristics such as the dynamic complexity of the cloud computing environment, the openness of the cloud platform and the high concentration of resources. One of the important problems is how to ensure the security of user data. Security problems, such as data security and privacy protection in cloud computing, have become serious obstacles which, if not appropriately addressed, will prevent the development and wide application of cloud computing in the future. Security concern in a distributed file system has been a major issue during the last decades. There are many security concerns in distributed file systems. Some of the concerns are how to make a distributed file confidential and to control its access. Traditional user control mechanisms keep user authorities in an access control list (ACL) in a group or a hierarchical structure. Then, it adds access control attribute to a file using a trusted server for authentication and authorization.

However, these traditional approaches heavily depend on security of the access control list. Once ACL were compromised, it would im-plicate the access control service. In general the access control mechanisms usually de-ploy symmetric and public cryptographic schemes to secure the access control list. Symmetric and public cryptography are employed for realizing access control mechanisms. However, traditional public key encryption schemes are not suitable for ABAC systems because it has simple one-to-one relation between cipher-texts and

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 6, Special Issue 3, March 2017

5th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '17)

13th-14th March 2017

Organized by

Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India.

user's key. Meanwhile, ABAC system requires complex relations between ciphertexts and user's such as a ciphertext can be decrypted by a class of users.

A new type of encryption scheme called ciphertextpolicy attributed-based encryption (CP-ABE) can be used for realizing ABAC system. CP-ABE is a class of encryption scheme which al-lows fine grained relations between ciphertexts and user's keys. In CPABE, a set of at-tributes is used to parameterize a user's secret key. On other hand, an access structure from the same attribute space is used to parameterize a ciphertext. The ciphertext can be decrypted if the attribute set satisfies the access structure. Attributedbased encryption schemes already been used in many systems for example oblivious transfer, vehicular adhoc network, and cloud computing. We propose a cloud-based secure data system, which allows trusted authority to securely store their secret data on the semi-trusted cloud service providers, and selectively share their secret data with a wide range of data receiver.To reduce the key management complexity for authority owners and data receivers. Different from previous cloud-based data system, Data ownersencrypt their secret data for the data receiver's usi

II. CLOUD COMPUTING

Cloud computing, also known as on-the-line computing, is a kind of Internet-based computing that provides shared processing resources and data to computers and other devices on demand. Cloud computing and storage solutions provide users and enterprises with various capabilities to store and process their data in third-party centers.. Proponents also claim that cloud computing allows enterprises to get their applications up and running faster, with improved manageability and less maintenance, and enables IT to more rapidly adjust resources to meet fluctuating and unpredictable business demand. Cloud providers typically use a "pay as you go" model. This can lead to unexpectedly high charges if administrators do not adapt to the cloud pricing model. The present availability of highcapacity networks, low-cost computers and storage devices as well as the widespread adoption of hardware virtualization,service-oriented architecture, andautonomicand utility computing have led to a growth in cloud computing. Companies can scale up as computing needs increase and then scale down again as demands decrease. Cloud computing has become a highly demanded service or utility due to the advantages of high computing power, cheap cost of services, high performance, Scalability, accessibility as well as availability. Some cloud vendors are experiencing growth rates of 50% per year, but being still in a stage of infancy, it has pitfalls that need to be addressed to make cloud computing services more reliable and user friendly

III. METHODOLOGY OF PROPOSED SYSTEM SECURE INFORMATION RETRIEVAL

In this study, an efficient encryption scheme based on layered model of the access structure is proposed in Social network, which is named file hierarchy CP-ABE scheme (or FH-CP-ABE, for short). FH-CP-ABE extends typical CP-ABE with a hierarchical structure of access policy, so as to achieve simple, flexible and fine-grained access control. The contributions of our scheme are three aspects.

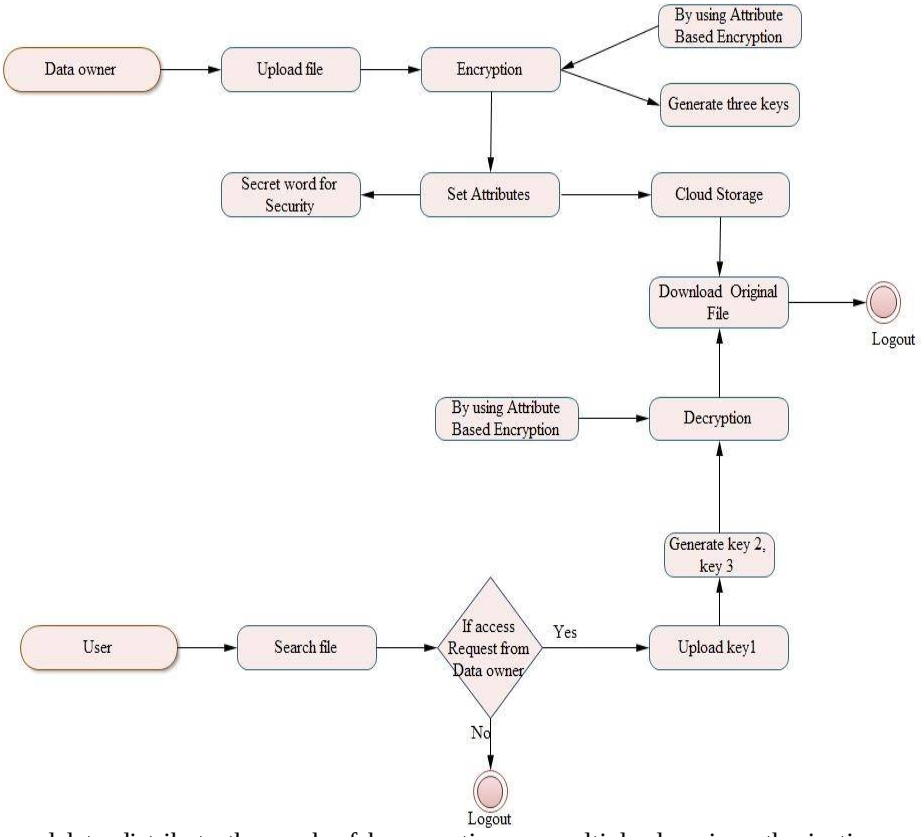
- Firstly, we propose the layered model of access structure to solve the problem of multiple hierarchical files sharing. The files are encrypted with one integrated access structure.
- Secondly, we also formally prove the security of FH-CP-ABE scheme that can successfully resist chosen plaintext attacks (CPA) under the Decisional Bilinear Diffie-Hellman (DBDH) assumption.
- Thirdly, we conduct and implement comprehensive experiment for FH-CP-ABE scheme, and the simulation results show that FH-CP-ABE has low storage cost and computation complexity in terms of encryption and decryption.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology
An ISO 3297: 2007 Certified Organization Volume 6, Special Issue 3, March 2017
5th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '17)
13th-14th March 2017
Organized by
Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India.

A. SYSTEM FLOW DIAGRAM

It should be noticed that the proposed scheme differs from the subsequent CP-ABE schemes, which utilize the



user layered model to distribute the work of key creation on multiple domain authorizations and lighten the burden of key authority center

B. ATTRIBUTE-BASED ENCRYPTION (ABE)

Attribute-based encryption (ABE) is a relatively recent approach that reconsiders the concept of public-key cryptography. In traditional public-key cryptography, a message is encrypted for a specific receiver using the receiver's public-key. Identity-based cryptography and in particular identity-based encryption (IBE) changed the traditional understanding of public-key cryptography by allowing the public-key to be an arbitrary string, e.g., the email address of the receiver. ABE goes one step further and defines the identity not atomic but as a set of attributes, e.g., roles, and messages can be encrypted with respect to subsets of attributes (keypolicy ABE - KP-ABE) or policies defined over a set of attributes (ciphertext-policy ABE - CP-ABE). The key issue is, that someone should only be able to decrypt a ciphertext if the person holds a key for "matching attributes" (more below) where user keys are always issued by some trusted party.

C. KEY-POLICY ABE

An important property which has to be achieved by both, CP- and KP-ABE is called collusion resistance. this basically means that it should not be possible for distinct users to "pool" their secret keys such that they could together decrypt a ciphertext that neither of them could decrypt on their own (which is achieved by independently randomizing users' secret keys)

D. SUPPORT VECTOR MACHINE

SVM is a useful technique for data classification. Even though it's considered that Neural Networks are easier to use than this, however, sometimes unsatisfactory results are obtained. A classification task usually involves

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 6, Special Issue 3, March 2017

5th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '17)

13th-14th March 2017

Organized by

Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India.

with training and testing data which consist of some data instances. Each instance in the training set contains one target values and several attributes. The goal of SVM is to produce a model which predicts target value of data instances in the testing set which are given only the attributes.

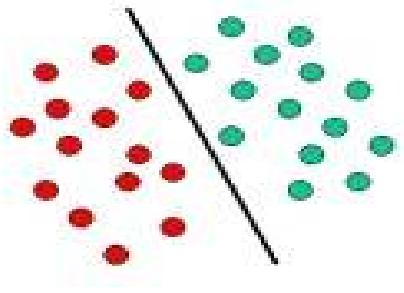
Classification in SVM is an example of Supervised Learning. Known labels help indicate whether the system is performing in a right way or not. This information points to a desired response, validating the accuracy of the system, or be used to help the system learn to act correctly. A step in SVM classification involves identification as which are intimately connected to the known classes. This is called feature selection or feature extraction. Feature selection and SVM classification together have a use even when prediction of unknown samples is not necessary. They can be used to identify key sets which are involved in whatever processes distinguish the classes.

The above is a classic example of a linear classifier, i.e., a classifier that separates a set of objects into their respective groups (GREEN and RED in this case) with a line. Most classification tasks, however, are not that simple, and often more complex structures are needed in order to make an optimal separation, i.e., correctly classify new objects (test cases) on the basis of the examples that are available (train cases). This situation is depicted in the illustration below. Compared to the previous schematic, it is clear that a full separation of the GREEN and RED objects would require a curve

(which is more complex than a line). Classification tasks based on drawing separating lines to distinguish between objects of different class memberships are known as hyperplane classifiers. Support Vector Machines are particularly suited to handle such tasks.

IV. RELATEDWORK

Kaitai Liang [1] et al propose the first cloud-based revocable identity-based proxy re-encryption (CRIB-PRE) scheme that supports user revocation but also delegation of decryption rights. No matter a user is revoked or not, at the end of a given time period the cloud acting as a proxy will re-encrypt all ciphertexts of the user under the current time period to the next time period. If the user is revoked in the forthcoming time period, he cannot decrypt the ciphertexts by using the expired private key anymore. We state that this primitive is applicable to many practical network applications, such as subscriptionbased cloud storage services. Comparing to some naive solutions which require a private key generator (PKG) to interact with non-revoked users in each time period, the new scheme provides definite advantages in terms of communication and computation effciency. Our scheme only requires the PKG to publish a constant-size public string for each time period and meanwhile, the workload of ciphertexts update is loaded to the cloud server. More importantly, the scheme can be proven secure in the standard model.



Youngho park [2] et al present a fully secure CPABE system with non-monotonic access structure for large attribute space. Our system achieves fully secure definition by giving a proof that any polynomial time attacker cannot distinguish the distribution in a real game and a final game by using dual encryption framework. In final game, the challenger always receives a semi-functional type 2 version of secret key or ciphertext. This mean the challenger can-not make decryption to the challenge ciphertext with queried secret key include those that satisfy the challenge access structure. Moreover, our scheme also allows user to define NOT gates in the access tree besides AND, OR and threshold gates which add the ex-pressibility of access control. Our present CP-ABE system also allows large attribute universe since the public parameter in the present CP-ABE does not grow linearly with attribute space size. Furthermore, from analysis of memory requirement and computation cost, our proposed CPABE is feasible to be used in real application.

Joseph K. Liu [3] et al tackle the open problem of proposing a leakage resilience encryption model that can capture leakage from both the secret key owner (the data user or control centre) and the encryptor (the data owner or sensor), in the auxiliary input model. Existing models only allow the leakage of the secret key and do not allow adversaries to query more leakage information after seeing the challenge ciphertext of the security

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology
An ISO 3297: 2007 Certified Organization Volume 6, Special Issue 3, March 2017
5th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '17)
13th-14th March 2017
Organized by
Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India.

games. We solve this problem by defining the post-challenge auxiliary input model in which the family of leakage functions must be defined before the adversary is given the public key. The post-challenge query will return the leakage of the encryption randomness used by the encryptor. This model is able to capture a wider class of real-world attacks.

Yanjiang Yang [4] et al presented an extended proxyassisted approach in order to overcome the limitation of needing to trust the cloud server not to disclose users' proxy keys inherent in proxy/mediator assisted user revocation approaches. In our approach, we bind the cloud server's private key to the data decryption operation, which requires the cloud server to reveal its private key should the cloud server decide to collude with revoked users. We then formulated a primitive, 'revocable cloud data encryption', under the approach. We presented a concrete construction of the primitive and implemented the construction using a proof-of-concept. The experimental results suggested that our construction is suitable for deployment even on smart mobile devices.

Willy Susilo [5] et al proposed a message is encrypted in a ciphertext associated with an arbitrary length index string, and a decryptor is legitimate if and only if a DFA associated with his/her secret key accepts the string. Furthermore, the above encryption is allowed to be transformed to another ciphertext associated with a new string by a semitrusted proxy to whom a re-encryption key is given. Nevertheless, the proxy cannot gain access to the underlying plaintext. This new primitive can increase the flexibility of users to delegate their decryption rights to others. We also prove it as fully chosen-ciphertext secure in the standard model.

Tao Jiang [6] et al proposed probabilistic challengeresponse scheme is proposed to prove that the clients' _les are available and stored in a specified cloud server. In order to resist the collusion of cloud servers, common cloud infrastructure with some reasonable limits, such as rational economic security model, semi-collusion security model and response time bound, are exploited. These limits guarantee that a malicious cloud server could not conduct a *t*-round communication in a _nite time. We analyze the security and performance of the proposed scheme and demonstrate that our scheme pro-vides strong incentives for economically rational cloud providers against re-outsourcing the clients' data to some other cloud providers.

Man Ho Au [7] et al introduce a new fine-grained two-factor authentication (2FA) access control system for web-based cloud computing services. Specifically, in our proposed 2FA access control system, an attribute-based access control mechanism is implemented with the necessity of both user secret key and a lightweight security device. As a user cannot access the system if s/he does not hold both, the mechanism can enhance the security of the system, especially in those scenarios where many users share the same computer for web-based cloud services. In addition, attribute-based control in the system also enables the cloud server to restrict the access to those users with the same set of attributes while preserving user privacy, i.e., the cloud server only knows that the user fulfills the required predicate, but has no idea on the exact identity of the user. Finally, we also carry out a simulation to demonstrate the practicability of our proposed 2FA system.

V. CONCLUSION

In this paper, we tackle the open problem of proposing a leakage of data. We propose a cloud based secure data system, which allows trusted authority to securely store their secret data on the semi-trusted cloud service providers, and selectively share their secret data with a wide range of data receiver. Different from previous cloud-based data system, Data owners encrypt their secret data for the data receivers using KP-ABE Encryption scheme. In addition for classification of data files a new classification algorithm is proposed

REFERENCES

[1]Kaitai Liang, Joseph K. Liu, Duncan S. Wong, Willy Susilo, "An Efficient Cloud-based Revocable Identity-based Proxy Re-encryption Scheme for Public Clouds Data Sharing", vol. 8712. Sep. 2014, pp. 257–272.
[2]SADIKIN RIFKI, YOUNGHO PARK, SANGJAE MOON , " A Fully Secure Cipher textPolicy Attribute-Based Encryption With A TreeBased Access Structure".
[3]Tsz Hon Yuen, Ye Zhang, Siu Ming Yiu, and Joseph K. Liu. "Identity-based Encryption with PostChallenge Auxiliary Inputs for Secure Cloud Applications and Sensor Networks", in Proc. 19t Eur. Symp. Res. Comput. Secur., vol. 8712. Sep. 2014, pp. 130–147.
[4]Y. Yang, J. K. Liu, K. Liang, K.-K. R. Choo, and J. Zhou, "Extended proxy-assisted approach: Achieving revocable fine-grained encryption of cloud data," in Proc. 20th Eur. Symp. Res. Comput. Secur. (ESORICS), vol. 9327. Sep. 2015, pp. 146– 166.
[5]K. Liang et al., "A DFA-based functional proxy re-encryption scheme for secure public cloud data sharing," IEEE Trans. Inf. Forensics Security, vol. 9,no. 10, pp. 1667–1680, Oct. 2014.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 6, Special Issue 3, March 2017

5th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '17)

13th-14th March 2017

Organized by

Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India.

[6]T. Jiang, X. Chen, J. Li, D. S. Wong, J. Ma, and J. Liu, "TIMER: Secure and reliable cloud storage against data re-outsourcing," in Proc. 10th Int. Conf. Inf. Secur. Pract. Exper., vol. 8434. May 2014, pp. 346–358.
[7]J. K. Liu, M. H. Au, X. Huang, R. Lu, and J. Li, "Fine-grained two factor access control for Webbased cloud computing services," IEEE Trans. Inf. Forensics Security, vol. 11, no. 3, pp. 484–497, Mar. 2016.
[8]F. Xhafa, J. Wang, X. Chen, J. K. Liu, J. Li, andP. Krause, "An efficient PHR service system supporting fuzzy keyword search and fine-grained access control," Soft Comput., vol. 18, no. 9, pp. 1795–1802, Sep. 2014.
[9]Y. Sreenivasa Rao, "A Secure and Efficient Ciphertext-Policy Attribute-Based Signcryption for Personal Health Records Sharing in Cloud Computing", June 14, 2016.
[10]Z. Wan, J. Liu, and R. H. Deng, "HASBE: A hierarchical attributebased solution for flexible andscalable access control in cloud computing," IEEETrans. Inf. Forensics Security, vol. 7, no. 2, pp. 743–754, Apr. 2012.
[11]Y. Dodis, S. Goldwasser, Y. T. Kalai, C. Peikert, and V. Vaikuntanathan. Public-key encryption schemes with auxiliary inputs. In D.Micciancio, editor, TCC 2010, volume 5978 of LNCS, pages 361{381. Springer, 2010.
[12]Y. Dodis, Y. T. Kalai, and S. Lovett. On cryptography with auxiliary input. In M. Mitzenmacher, editor, STOC 2009, pages 621{630. ACM, 2009.
[13]S. Faust, C. Hazay, J. B. Nielsen, P. S. Nordholt, and A. Zottarel. Signature schemes secure against hard-to-invert leakage. In X. Wang and K. Sako, editors, ASIACRYPT, volume 7658 of LNCS, pages 98{115. Springer, 2012.
[14]C. Franke and P. Robinson. Autonomic provisioning of hosted applications with level of isolation terms. 2010 Seventh IEEE International Conference and Work- shops on EngineeringofAutonomic and Autonomous Systems, 0:131{142, 2008.
[15]S. Halevi and H. Lin. After-the-fact leakage inpublic-key encryption. In Y. Ishai, editor, TCC 2011, volume 6597 of LNCS, pages 107{124. Springer, 2011.
[16]A. Hough. Google engineer _red for privacybreach after \staking and harassing teenagers". The Telegraph. Sept 15, 2010.
[17]A. K. Lenstra, J. P. Hughes, M. Augier, J. W. Bos, T. Kleinjung, and C. Wachter. Public keys. In R. Safavi-Naini and R. Canetti, editors, CRYPTO, volume 7417 of LNCS, pages 626{642. Springer, 2012.
[18]K. Michaelis, C. Meyer, and J. Schwenk. Randomly failed! the state of randomness in current java implementations. In E. Dawson, editor, CT-RSA 2013, volume 7779 of LNCS, pages 129{144. Springer, 2013.
[19]H. Namiki, K. Tanaka, and K. Yasunaga. Randomness leakage in the kem/dem framework. In X. Boyen and X. Chen, editors, ProvSec, volume 6980 of LNCS, pages 309{323. Springer, 2011.
[20]M. Naor and G. Segev. Public-key cryptosystems resilient to key leakage. In S. Halevi, editor, CRYPTO 2009, volume 5677 of LNCS, pages 18{35. Springer, 2009. [21]. N. Perlroth, J. Larson, and S. Shane. N.S.A. able to foil basic safeguards of privacy on web. New York Times, September 5,2013. http://www.nytimes.com/2013/09/06/us/nsa-foilsmuch-internet encryption.html.
[21]D. Shumow and N. Ferguson. On the possibility of a back door in the NIST SP800-90 dual ecprng.http://rump2007.cr.yp.to/15-shumow.pdf.
[22]T. H. Yuen, S. S. M. Chow, Y. Zhang, and S. M. Yiu. Identity-based encryption resilient to continual auxiliary leakage. In D. Pointcheval and T