**LITERATURE SURVEY**

**Toward Efficient And Privacy-Preserving Computing In Big Data Era**

Big data, because it can mine new knowledge for economic growth and technical innovation, has recently received considerable attention, and many research efforts have been directed to big data processing due to its high volume, velocity, and variety (referred to as "3V") challenges. However, in addition to the 3V challenges, the flourishing of big data also hinges on fully understanding and managing newly arising security and privacy challenges. If data are not authentic, new mined knowledge will be unconvincing; while if privacy is not well addressed, people may be reluctant to share their data. Because security has been investigated as a new dimension, "veracity," in big data, in this article, we aim to exploit new challenges of big data in terms of privacy, and devote our attention toward efficient and privacy-preserving computing in the big data era. Specifically, we first formalize the general architecture of big data analytics, identify the corresponding privacy requirements, and introduce an efficient and privacy-preserving cosine similarity computing protocol as an example in response to data mining's efficiency and privacy requirements in the big data era.

**Expressive, Efficient, And Revocable Data Access Control For Multi-Authority Cloud Storage**

Data access control is an effective way to ensure the data security in the cloud. Due to data outsourcing and untrusted cloud servers, the data access control becomes a challenging issue in cloud storage systems. Ciphertext-Policy Attribute-based Encryption (CP-ABE) is regarded as one of the most suitable technologies for data access control in cloud storage, because it gives data owners more direct control on access policies. However, it is difficult to directly apply existing CP-ABE schemes to data access control for cloud storage systems because of the attribute revocation problem. In this paper, we design an expressive, efficient and revocable data access control scheme for multi-authority cloud storage systems, where there are multiple authorities co-exist and each authority is able to issue attributes independently. Specifically, we propose a revocable multi-authority CP-ABE scheme, and apply it as the underlying techniques to design the data access control scheme. Our attribute revocation method can efficiently achieve both forward security and backward security. The analysis and simulation results show that our proposed data access control scheme is secure in the random oracle model and is more efficient than previous works.

**Enabling Fine-Grained Access Control With Efficient Attribute Revocation And Policy Updating In Smart Grid**

In smart grid, electricity consumption data may be handed over to a third party for various purposes. While government regulations and industry compliance prevent utility companies from improper or illegal sharing of their customers’ electricity consumption data, there are some scenarios where it can be very useful. For example, it allows the consumers’ data to be shared among various energy resources so the energy resources are able to analyze the data and adjust their operation to the actual power demand. However, it is crucial to protect sensitive electricity consumption data during the sharing process. In this paper, we propose a fine-grained access control scheme (FAC) with efficient attribute revocation and policy updating in smart grid. Specifically, by introducing the concept of Third-party Auditor (TPA), the proposed FAC achieves efficient attribute revocation. Also, we design an efficient policy updating algorithm by outsourcing the computational task to a cloud server. Moreover, we give security analysis and conduct experiments to demonstrate that the FAC is both secure and efficient compared with existing ABE-based approaches.

**Time-Domain Attribute-Based Access Control For Cloud-Based Video Content Sharing: A Cryptographic Approach**

With the ever-increasing demands on multimedia applications, cloud computing, due to its economical but powerful resources, is becoming a natural platform to process, store, and share multimedia contents. However, the employment of cloud computing also brings new security and privacy issues as few public cloud servers can be fully trusted by users. In this paper, we focus on how to securely share video contents to a certain group of people during a particular time period in cloud-based multimedia systems, and propose a cryptographic approach, a provably secure time-domain attribute-based access control (TAAC) scheme, to secure the cloud-based video content sharing. Specifically, we first propose a provably secure time-domain attribute-based encryption scheme by embedding the time into both the ciphertexts and the keys, such that only users who hold sufficient attributes in a specific time slot can decrypt the video contents. We also propose an efficient attribute updating method to achieve the dynamic change of users' attributes, including granting new attributes, revoking previous attributes, and regranting previously revoked attributes. We further discuss on how to control those video contents that can be commonly accessed in multiple time slots and how to make special queries on video contents generated in previous time slots. The security analysis and performance evaluation show that TAAC is provably secure in generic group model and efficient in practice.

**Secure Threshold Multi Authority Attribute Based Encryption Without A Central Authority**

An attribute based encryption scheme (ABE) is a cryptographic primitive in which every user is identified by a set of attributes, and some function of these attributes is used to determine the ability to decrypt each ciphertext. Chase proposed the first multi authority ABE scheme in TCC 2007 as an answer to an open problem presented by Sahai and Waters in EUROCRYPT 2005. However, her scheme needs a fully trusted central authority which can decrypt every ciphertext in the system. This central authority would endanger the whole system if it’s corrupted.

This paper presents a threshold multi authority fuzzy identity based encryption(MA-FIBE) scheme without a central authority for the first time. An encrypter can encrypt a message such that a user could only decrypt if he has at least dk of the given attributes about the message for at least t + 1, t ≤ n/2 honest authorities of all the n attribute authorities in the proposed scheme. The security proof is based on the secrecy of the underlying joint random secret sharing protocol and joint zero secret sharing protocol and the standard decisional bilinear Diffie-Hellman assumption. The proposed MA-FIBE could be extended to the threshold multi authority attribute based encryption (MA-ABE) scheme and be further extended to a proactive MA-ABE scheme.

**Attribute-Based Encryption With Partially Hidden Encryptor-Specified Access Structures**

We propose attribute-based encryption schemes where encryptor-specified access structures (also called ciphertext policies) are hidden. By using our schemes, an encryptor can encrypt data with a hidden access structure. A decryptor obtains her secret key associated with her attributes from a trusted authority in advance and if the attributes associated with the decryptor’s secret key do not satisfy the access structure associated with the encrypted data, the decryptor cannot decrypt the data or guess even what access structure was specified by the encryptor. We prove security of our construction based on the Decisional Bilinear Diffie-Hellman assumption and the Decision Linear assumption. In our security notion, even the legitimate decryptor cannot obtain the information about the access structure associated with the encrypted data more than the fact that she can decrypt the data.

**Privacy-Aware Attribute-Based Encryption With User Accountability**

As a new public key primitive, attribute-based encryption (ABE) is envisioned to be a promising tool for implementing fine-grained access control. To further address the concern of user access privacy, privacy-aware ABE schemes are being developed to achieve hidden access policy recently. For the purpose of secure access control, there is, however, still one critical functionality missing in the existing ABE schemes, which is user accountability. Currently, no ABE scheme can completely prevent the problem of illegal key sharing among users. In this paper, we tackle this problem by firstly proposing the notion of accountable, anonymous, and ciphertext-policy ABE (CP-A3BE, in short) and then giving out a concrete construction. We start by improving the state-of-the-art of anonymous CP-ABE to obtain shorter public parameters and ciphertext length. In the proposed CP-A3BE construction, user accountability can be achieved in black-box model by embedding additional user-specific information into the attribute private key issued to that user, while still maintaining hidden access policy. The proposed constructions are provably secure.