**LITERATURE SURVEY**

**1) Searchable encryption revisited: Consistency properties, relation to anonymous IBE, and extensions**

**AUTHORS:**  M. Abdalla, M. Bellare, D. Catalano, E. Kiltz, T. Kohno, T. Lange,

J. Malone-Lee, G. Neven, P. Paillier, and H. Shi

We identify and fill some gaps with regard to consistency (the extent to which false positives are produced) for public-key encryption with keyword search (PEKS). We define computational and statistical relaxations of the existing notion of perfect consistency, show that the scheme of Boneh et al. in Eurocrypt 2004 is computationally consistent, and provide a new scheme that is statistically consistent. We also provide a transform of an anonymous IBE scheme to a secure PEKS scheme that, unlike the previous one, guarantees consistency. Finally, we suggest three extensions of the basic notions considered here, namely anonymous HIBE, public-key encryption with temporary keyword search, and identity-based encryption with keyword search.

**2) Improved proxy re-encryption schemes with applications to secure distributed storage**

**AUTHORS:** G. Ateniese, K. Fu, M. Green, and S. Hohenberger

In 1998, Blaze, Bleumer, and Strauss (BBS) proposed an application called atomic proxy re-encryption, in which a semi-trusted proxy converts a ciphertext for Alice into a ciphertext for Bob without seeing the underlying plaintext. We predict that fast and secure re-encryption will become increasingly popular as a method for managing encrypted file systems. Although efficiently computable, the wide-spread adoption of BBS re-encryption has been hindered by considerable security risks. Following recent work of Dodis and Ivan, we present new re-encryption schemes that realize a stronger notion of security, and we demonstrate the usefulness of proxy re-encryption as a method of adding access control to a secure file system. Performance measurements of our experimental file system demonstrate that proxy re-encryption can work effectively in practice.

**3) Public key encryption with keyword search revisited**

**AUTHORS:** J. Baek, R. Safavi-Naini, and W. Susilo

The public key encryption with keyword search (PEKS) scheme, proposed by Boneh, Di Crescenzo, Ostrovsky and Persiano, enables one to search for encrypted keywords without compromising the security of the original data. In this paper, we address two important issues of a PEKS scheme, “removing secure channel” and “refreshing keywords”, which have not been considered in Boneh et al.’s paper. We point out the inefficiency of the original PEKS scheme due to the use of the secure channel. We resolve this problem by constructing an efficient PEKS scheme that removes a secure channel. We then argue that care must be taken when keywords are used frequently in the PEKS scheme as this situation might contradict the security of PEKS.

**4) Towards a secure incremental proxy re-encryption for e-healthcare data sharing in mobile cloud computing**

**AUTHORS:** T. Bhatia, A. K. Verma, and G. Sharma

Cloud computing provides universal access to a pool of shared resources to numerous stakeholders/shareholders of the e‐healthcare industry. The speedy adoption of cloud computing has inevitably raised security concerns for the outsourced data. Since mobile devices are resource constrained, the security solutions must discharge the computing comprehensive operations on the cloud for implementation. Conventionally, any modification to uploaded record would compel the mobile client to encrypt and compute the hash value from scratch. Through this paper, we intend to propose a pairing‐free incremental proxy re‐encryption scheme, without certificates, which would run proportionate to the number of modifications in time, instead of the document length for improvement in the file modification tasks. The proposed scheme shows a significant improvement in the file modification system regarding the energy consumption and the turnaround timer taken. The proposed scheme has been verified through a formal method using Z3 solver.

**5) Secure sharing of mobile personal healthcare records using certificateless proxy re-encryption in cloud**

**AUTHORS:** T. Bhatia, A. K.Verma, and G. Sharma

The ubiquitous and timely access to personal health records help physicians to take critical decisions and save lives. Cloud computing has a potential to provide ubiquitous and on-demand instant access to common pool of shared resources and services to various stakeholders involved in electronic healthcare industry such as patients, healthcare professionals, insurance companies, etc. The speedy evolution and adoption of cloud computing in electronic healthcare systems have inevitably raised concerns enveloping outsourced data in a myriad of safety issues. In this paper, cryptanalysis of Qin's scheme is performed breaching confidentiality of their scheme. We further proposed a lightweight and pairing free single-hop unidirectional certificateless proxy re-encryption scheme based on elliptic curves for secure sharing of mobile personal health records with public cloud competent for low-power mobile devices. In certificateless proxy re-encryption, patients encrypt the data with their public keys before outsourcing to the cloud and cloud resident semitrusted proxy further re-encrypts into ciphertext under intended recipient's public key without learning anything about encrypted message. We prove its security through formal analysis against chosen ciphertext attack in the random oracle model. Our proposed scheme is more efficient and suitable for low-power mobile devices in comparison with existing schemes.