**LITERATURE SURVEY**

1. **Efficient Statically-Secure Large-Universe Multi-Authority Attribute-Based Encryption**

**AUTHORS:** Y. Rouselakis and B. Waters

We propose an efficient large-universe multi-authority ciphertext-policy attribute-based encryption system. In a large-universe ABE scheme, any string can be used as an attribute of the system, and these attributes are not necessarily enumerated during setup. In a multi-authority ABE scheme, there is no central authority that distributes the keys to users. Instead, there are several authorities, each of which is responsible for the authorized key distribution of a specific set of attributes. Prior to our work, several schemes have been presented that satisfy one of these two properties but not both. Our construction achieves maximum versatility by allowing multiple authorities to control the key distribution for an exponential number of attributes. In addition, the ciphertext policies of our system are sufficiently expressive and overcome the restriction that “each attribute is used only once” that constrained previous constructions. Besides versatility, another goal of our work is to increase efficiency and practicality. As a result, we use the significantly faster prime order bilinear groups rather than composite order groups. The construction is non-adaptively secure in the random oracle model under a non-interactive q-type assumption, similar to one used in prior works. Our work extends existing “program-and-cancel” techniques to prove security and introduces two new techniques of independent interest for other ABE constructions. We provide an implementation and some benchmarks of our construction in Charm, a programming framework developed for rapid prototyping of cryptographic primitives

1. **Using Erasure Codes Efficiently for Storage in a Distributed System**

**AUTHORS:** M. K. Aguilera, R. Janakiraman, and L.

Erasure codes provide space-optimal data redundancy to protect against data loss. A common use is to reliably store data in a distributed system, where erasure-coded data are kept in different nodes to tolerate node failures without losing data. In this paper, we propose a new approach to maintain ensure-encoded data in a distributed system. The approach allows the use of space efficient k-of-n erasure codes where n and k are large and the overhead n-k is small. Concurrent updates and accesses to data are highly optimized: in common cases, they require no locks, no two-phase commits, and no logs of old versions of data. We evaluate our approach using an implementation and simulations for larger systems

**3)** **The security of all-or-nothing encryption: Protecting against exhaustive**

**key search**

**AUTHORS:** Anand Desai

We investigate the all-or-nothing encryption paradigm which was introduced by Rivest as a new mode of operation for block ciphers. The paradigm involves composing an all-or-nothing transform (AONT) with an ordinary encryption mode. The goal is to have secure encryption modes with the additional property that exhaustive key-search attacks on them are slowed down by a factor equal to the number of blocks in the ciphertext. We give a new notion concerned with the privacy of keys that provably captures this key-search resistance property. We suggest a new characterization of AONTs and establish that the resulting all-or-nothing encryption paradigm yields secure encryption modes that also meet this notion of key privacy. A consequence of our new characterization is that we get more efficient ways of instantiating the all-or-nothing encryption paradigm. We describe a simple block-cipher-based AONT and prove it secure in the Shannon Model of a block cipher. We also give attacks against alternate paradigms that were believed to have the above keysearch resistance property.

**4)Transparent Data Deduplication in the Cloud**

**AUTHORS**: F. Armknecht, J.-M. Bohli, G. O. Karame, and F. Youssef

Cloud storage providers such as Dropbox and Google drive heavily rely on data deduplication to save storage costs by only storing one copy of each uploaded file. Although recent studies report that whole file deduplication can achieve up to 50% storage reduction, users do not directly benefit from these savings—as there is no transparent relation between effective storage costs and the prices offered to the users. In this paper, we propose a novel storage solution, ClearBox, which allows a storage service provider to transparently attest to its customers the deduplication patterns of the (encrypted) data that it is storing. By doing so, ClearBox enables cloud users to verify the effective storage space that their data is occupying in the cloud, and consequently to check whether they qualify for benefits such as price reductions, etc. ClearBox is secure against malicious users and a rational storage provider, and ensures that files can only be accessed by their legitimate owners. We evaluate a prototype implementation of ClearBox using both Amazon S3 and Dropbox as back-end cloud storage. Our findings show that our solution works with the APIs provided by existing service providers without any modifications and achieves comparable performance to existing solutions.

**5)Decentralizing Attribute-Based Encryption**

**AUTHORS**: A. B. Lewko and B.Waters

We propose a Multi-Authority Attribute-Based Encryption (ABE) system. In our system, any party can become an authority and there is no requirement for any global coordination other than the creation of an initial set of common reference parameters. A party can simply act as an ABE authority by creating a public key and issuing private keys to different users that reflect their attributes. A user can encrypt data in terms of any boolean formula over attributes issued from any chosen set of authorities. Finally, our system does not require any central authority. In constructing our system, our largest technical hurdle is to make it collusion resistant. Prior Attribute-Based Encryption systems achieved collusion resistance when the ABE system authority “tied” together different components (representing different attributes) of a user’s private key by randomizing the key. However, in our system each component will come from a potentially different authority, where we assume no coordination between such authorities. We create new techniques to tie key components together and prevent collusion attacks between users with different global identifiers. We prove our system secure using the recent dual system encryption methodology where the security proof works by first converting the challenge ciphertext and private keys to a semi-functional form and then arguing security. We follow a recent variant of the dual system proof technique due to Lewko and Waters and build our system using bilinear groups of composite order. We prove security under similar static assumptions to the LW paper in the random oracle model.