

**CHENNAI – PONDICHERRY**

**Space-efficient Verifiable Secret Sharing Using Polynomial Interpolation**

**Abstract:**

Preserving data confidentiality in clouds is a key issue. Secret Sharing, a cryptographic primitive for the distribution of a secret among a group of n participants designed so that only subsets of shareholders of cardinality 0 < t \_ n are allowed to reconstruct the secret by pooling their shares, can help mitigating and minimizing the problem. A desirable feature of Secret Sharing schemes is cheater detection, i.e. the ability to detect one or more malicious shareholders trying to reconstruct the secret by obtaining legal shares from the other shareholders while providing them with fake shares. Verifiable Secret Sharing schemes solve this problem by allowing shareholders verifying the others’ shares. We present new verification algorithms providing arbitrary secret sharing schemes with cheater detection capabilities, and prove their space efficiency with regard to other schemes appeared in the literature. We also introduce, in one of our schemes, the Exponentiating Polynomial Root Problem (EPRP), which is believed to be NP-Intermediate and therefore difficult.

**Existing System:**

The design of a secret sharing protocol is its robustness against cheaters: common solutions proposed in literature rely on checking consistency of the secret information after reconstruction from more than one group of shareholders, or on adding helpful data to the shares in order to detect and/or identify mistrustful behavior. Verifiable Secret Sharing (VSS) is therefore secret sharing augmented with features that allow only detection or also identification of any cheater in a coalition, unconditionally or with respect to the scheme parameters (threshold value, total number of dishonest shareholders, etc.). Several VSS schemes have been proposed, including, for instance, Publicly Verifiable Secret Sharing (PVSS) or schemes focusing on Asynchronous Verifiable Secret Sharing (AVSS).

**Proposed system:**

The design of a secret sharing protocol is its robustness against cheaters: common solutions proposed in literature rely on checking consistency of the secret information after reconstruction from more than one group of shareholders, or on adding helpful data to the shares in order to detect and/or identify mistrustful behavior. Verifiable Secret Sharing (VSS) is therefore secret sharing augmented with features that allow only detection or also identification of any cheater in a coalition, unconditionally or with respect to the scheme parameters (threshold value, total number of dishonest shareholders, etc.). Several VSS schemes have been proposed, including, for instance, Publicly Verifiable Secret Sharing (PVSS) or schemes focusing on Asynchronous Verifiable Secret Sharing (AVSS).