# Publicly Verifiable Shared Dynamic Electronic Health Record Databases With Functional Commitment Supporting Privacy-Preserving Integrity Auditing

Abstract:

Electronic health record (EHR) is a system that collects patients' digital health information and shares it with other healthcare providers in the cloud. Since EHR contains a large amount of significant and sensitive information about patients, it is required that the system ensures response correctness and storage integrity. Meanwhile, with the rise of IoT, more low-performance terminals are deployed for receiving and uploading patient data to the server, which increases the computational and communication burden of the EHR systems. The verifiable database (VDB), where a user outsources his large database to a cloud server and makes queries once he needs certain data, is proposed as an efficient updatable cloud storage model for resource-constrained users. To improve efficiency, most existing VDB schemes utilize proof reuse and proof updating technique to prove correctness of the query results. However, it ignores the “real-time” of proof generation, which results in an overhead that the user has to perform extra process (e.g., auditing schemes) to check storage integrity. In this article, we propose a publicly verifiable shared updatable EHR database scheme that supports privacy-preserving and batch integrity checking with minimum user communication cost. We modify the existing functional commitment (FC) scheme for the VDB design and construct a concrete FC under the computational l -BDHE assumption. In addition, the use of an efficient verifier-local revocation group signature scheme makes our scheme support dynamic group member operations, and gives nice features, such as traceability and non-frameability.