**INTRODUCTION**

WITH the explosive increase of global information, the cloud service industry has been developing unprecedentedly. Many cloud service providers are rushing to launch cloud service platforms and products, such as Amazon, GOOGLE, Alibaba, Microsoft, and Huawei, etc. People start to outsource their large data storage tasks to cloud service providers (CSPs). It makes them no longer constrained by limited local storage and computing resources. As a concrete and high-quality application example of cloud storage, the cloud-based electronic health record (EHR), which is a system that collects the patients’ digital health information, is being vigorously promoted by many organizations, such as the Office of the National Coordinator for Health Information Technology (ONC) [6] in the United States and Canada Health Infoway [7]. The patient EHRs are written on the workstation or mobile device, and can be accessed and modified later. The patient EHRs uploaded to the cloud can be shared among different medical institutions to help patients get better treatment, help

scientific researchers to carry out disease analysis and research, and help public health departments predict, detect and potentially prevent the outbreak of epidemic diseases, etc. Since the cloud service provider (CSP) is an independent management entity, users actually give up the ultimate control over their EHRs. This brings security challenges for outsourcing tasks. For example, the cloud servers may return incorrect results for various reasons, such as malfunctioning cloud equipments and a hacker’s attack. The incorrect returned values can have serious consequences for every part of the medical system. Therefore, the primary problem faced by the EHR system is on how to verify that the server responses correctly each time

Benabbas et al.. proposed the verifiable database (VDB) as a secure and efficient updatable cloud storage model for resource-limited users. In a VDB scheme, a client can outsource the storage of a collection of data items to an untrusted server. Later, the client can query the server for an item (a message) at position i, the server returns the stored message at this position along with a proof that it is the correct answer. However, the security of only verifying the server response correctness is far from enough for the EHR system, and it is not clear whether data that is not frequently accessed is still stored correctly. If these data are destroyed and not discovered in time, it can cause huge losses in the event of an emergency

Many audit schemes exist to check the data storage integrity. A simple idea to realize the server response correctness and the data storage integrity of EHR system is to use the VDB scheme and an audit scheme respectively. But there will be a lot of authentication tags generated and transmitted for verification. At present, with the development of the Internet of things, emerging wearable devices are also deployed for receiving and uploading users' EHR information. For example, a smartwatch can upload information about a user's heartbeat and breathing, and an insertable cardiac monitor called Reveal LINQ [21] provides long-term heart monitoring. Similarly, mobile terminals with limited performance used in such applications. The main computation and communication of these low-performing terminals occurs when the user first uploads the database and updates the data each time. In the traditional data integrity checking scheme, the user generates an authentication tag for each data block and uploades it to the cloud server together with the data in the above two stages. This 1-to-1 tag generation method results in the fact that low performance terminals have to reserve more storage space for temporary storage tags and spend more transport resources for transport tags

Some audit schemes provide methods to reduce the number of tags. The scheme [23] proposed a method to reduce the number of tags by expanding the size of each data block, but it still cannot realize the aggregation of tags of each data block. Jiang et al. 's scheme [14] proposed to use vector commitment scheme to construct the audit scheme. Although the reduction of tags has been achieved, their scheme fails to achieve the expected security due to the neglect of the real-time performance of proof generation. There is still no good way to minimize the communication for low performance users.

The biggest feature of the EHR system is that patients' health information is shared in a group, including clinic, healthcare, hospital, medicine center, in-surance and so on. Anyone in the group can upload, download, and modify the database. In most cases, the members in such group are not fixed. And a group manager (GM) is appointed to control members’ join or quit. The scheme [28] provided an efficient audit scheme for group members to share cloud data, but only GM can upload the database. Jiang et al. [14] scheme involved the dynamic problem of group members, but their scheme can only realize the revocation and the case of users joining group is not considered. They used the group signature scheme with verifier-local revocation (VLR) [2] proposed by Boneh et al. to make group members revocable. However, their VLR group signature scheme does not have backward unlink ability (BU), which means that even if a member is revoked at a certain time, the signature before that time remains anonymous. It poses a threat to user identity privacy

Also, security and privacy of medical data storage and access must be enforced by legal legislations. Therefore, a powerful tool for EHR systems is needed to fulfill the legal requirements in protecting the security and privacy of the medical data

Database storage, such as EHR. According to the characteristics of EHR system, two aspects of security deserve our attention, namely, the server response correctness and the data storage integrity. In order to deal with above problems, we use a new tool called functional commitment (FC) and design a publicly verifiable updatable database scheme based on functional commitment supporting privacy-preserving integrity auditing and dynamic group operation. Our contributions can be summarized as follows:

1. We modify the existing functional commitment scheme in order to use the function binding of functional commitment to design an auditable VDB scheme. Two algorithms for updating are added based on the original scheme in. And a modified concrete FC with updates under the computational l - BDHE assumption is constructed. Our construction has fewer parameters and is more efficient than the original scheme in.
2. We point out security problems with scheme and propose a publicly verifiable updatable VDB scheme based on the functional commitment and group signature without incurring too much computational overhead and storage cost. Moreover, our scheme is applicable for large-scale data storage with minimum user communication cost. Our proposed scheme not only preserves all the properties of the original VDB scheme, but also implements efficient privacy-preserving integrity auditing, non frame ability and traceability. The scheme preserves data privacy from the auditor by using a random masking technique and the sparse vector is used for sampling auditing. Our scheme supports dynamic group member operations which include join and revocation. In addition, our VDB supports batch auditing and it supports multi-cloud server, multiuser and multi-storage vector scenarios
3. Security analysis and experimental comparison with existing schemes are provided and it shows that our VDB is secure and efficient.