Journal of Information Security and Applications 39 (2018) 10–18

Contents lists available at ScienceDirect

Journal of Information Security and Applications

journal homepage: www.elsevier.com/locate/jisa

# A dynamic integrity verification scheme of cloud storage data based on lattice and Bloom filter

Yunxue Yan[a], Lei Wu[a,b,*], Ge Gao[a], Hao Wang[a,b], Wenyu Xu[a]

[a] School of Information Science & Engineering, Shandong Normal University, China
[b] Shandong Provincial Key Laboratory for Novel Distributed Computer Software Technology, China

ARTICLE INFO

*Article history:*

*Keywords:*
Lattice cryptography
SIS problems
Cloud storage system
Bloom filter
Quantum theory

ABSTRACT

With the development of quantum computer, making the traditional cloud storage program data integrity verification protocol is no longer safe anymore, so how to establish a safe and efficient, cost-effective cloud storage system becomes the industry's research hotspot. This paper makes improvements on the basis of the previous schemes. On the cloud storage model, we focus on the protection of user data privacy, and send the file and user signature to CSP and TPA respectively, so these methods will improve the privacy of signature information. In the cloud storage data calculation, using of lattice and Bloom filter methods, can not only resist the quantum computer attacks, but also based on the realization of dynamic integrity, improving the utilization of cloud storage space ultimately.



## 1. Introduction

In today's society, information technology has changed people's traditional way of life, people's dependence on information technology continues to increase in recent years. With the increase in the amount of data explosion, cloud computing came into being, greatly improving people's work efficiency. Cloud storage is based on the development of cloud computing. The birth and development of Cloud storage services provide cloud users a lot of storage space, but nevertheless, cloud storage still has some shortcomings, such as data missing, data is tampered or deleted. So cloud storage data security issues become a key step in improving cloud storage services. With the development of quantum computers, it is necessary to design a signature scheme that can resist quantum computer attacks, because the difficult problems in the traditional cryptography system can be solved in the polynomial time, so that the security of various encryption schemes is threatened.

### 1.1. Research background of cloud storage integrity

The concept of cloud storage is based on the development and expansion of cloud computing. As a data storage and management as the core of the cloud computing system, cloud storage for the cloud era of large data processing provides a new solution. To occupy the core position in cloud computing, cloud storage platform construction is very important. In general, the cloud storage platform [28] is divided into four layers (user access layer, application interface layer, the basic management layer, storage layer), as shown in Fig. 1. Although cloud storage has been recognized by everyone, but there are still some of the advantages and disadvantages that we need attention [27], as shown in Table 1.

With the continuous development of information technology and economic times, the arrival of digital society has become an inevitable trend. The traditional way of storage is not able to meet the current large amount of data clearly. Cloud storage came into being. Cloud storage security includes confidentiality, integrity, unforgeability. The first proposed validation data integrity is based on the integrity of RSA algorithm proposed by Ateniese et al. [5], but due to the large number of modulo exponents in RSA, so when we need to modify the data calculation efficiency will be very low. So it is not suitable for big data dynamic storage. Wang et al. [6] proposed in the cloud computing security background of the public verification method and dynamic storage, but it could not resist the quantum computer attacks.

### 1.2. Research background of lattice signature

The rapid development of information technology has also brought about increasingly serious security issues. With the rapid development of computer technology and network technology, people's understanding of information security more and more profound, the information security requirements of the property is also increasing, from the initial confidentiality, to the present integrity, certification, non-repudiation. As well as availability re-

* Corresponding author at: School of Information Science & Engineering, Shandong Normal University, China.
*E-mail address:* wulei@sdnu.edu.cn (L. Wu).

https://doi.org/10.1016/j.jisa.2018.01.004
2214-2126/

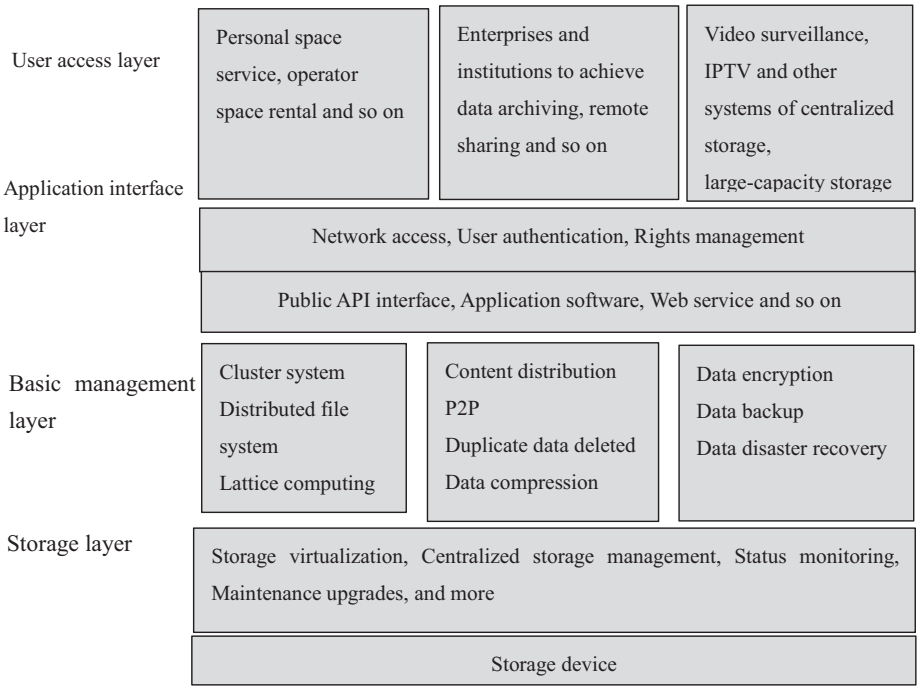


**Fig. 1.** Cloud storage system architecture.

**Table 1**
Cloud storage system advantages and disadvantages of contrast.

| Advantage | Disadvantage |
|---|---|
| Low cost | The possibility of user privacy disclosure is enhanced |
| The management authority is clearly assigned | Data missing |
| Provide services on demand | Data tampering |
| Not subject to location constraints | Storage performance is affected by the network |
| Adapt to large data storage | |

quirements. In order to meet people's information security requirements, we usually need to adopt the most critical and most core technology is cryptography. Early cryptography security is often based on some complex mathematical difficulties. For example, large integer decomposition problems and discrete logarithm problems. In addition, the development of elliptic curve cryptography has received a lot of attention. Zhe Liu, Johann Großschädl, Zhi Hu and so on in the new elliptic curve is very innovative put forward their own ideas, and has a better realization. For example, in the article "On Emerging Family of Elliptic Curves to Secure Internet of Things: ECC Comes of Age [29]", a study was conducted to study the calculation of the operation on a twisted Edwards curve with an effective computable internal shape, compared to conventional implementations, The number of points can be reduced by about 50%. Their design provides a variety of trade-offs and optimizations between performance and resource requirements. In the article "Elliptic Curve Cryptography with Efficiently Computable Endomorphisms and Its Hardware Implementations for the Internet of Things [30]" by defining an emerging lightweight elliptic curve family to meet the requirements of some resource-constrained devices and which has two optimized designs, High-speed version (HS) and efficient (ME) version.

Based on the traditional cryptography system is faced with the risk of quantum attack, In 1994, Shor [1] found a polynomial time algorithm for solving factorization and discrete logarithm problems in quantum computer models, which prompted cryptographers to post-quantum time's cryptographic system analysis and design research. At present, under the quantum computer model, an effective algorithm for solving difficult problems has not been found, and many problems in lattice theory have proved difficult. Therefore, the analysis and design of the cryptographic system based on the difficult problem in the lattice theory has become one of the hotspots of the "post-quantum era cryptography system". In 1996, Ajtai [2] gave a landmark conclusion on the basis of the issues of lattice problems, and proposed the possibility of constructing the cryptographic scheme based on the problem of lattice problem, and provided a new idea for constructing the new public key system. In 2008, Gentry et al. [3] proposed a lattice-based digital signature scheme, which became the basic tool for designing public key cryptography. In 2013, Wang [4] proposed a lattice-based linear homomorphic signature scheme based on GPV, but this scheme does not support data dynamic verification, Therefore, in the background of cloud storage applications, the data often need to be updated, so it does not have practical value.

### *1.3. Research background of Bloom filter*

With the increasing amount of data, the query and modification of data become one of the core problems of cloud computing research. In the development of computer science, we often explore the question of how to improve efficiency, but often need to pay the time or space in exchange for. In 1970, Bloom Filter was proposed by Howard Bloom, which is a very long binary vector data structure. The main function is to query the collection of elements in the attribution of the problem. His obvious advantage is that it can efficiently meet the needs of the search. Bloom filter can not only represent the collection, but also can support the collection of elements to insert and query. Bloom filter Compared with the tra-