Privacy-Preserving and Publicly Verifiable Protocol for Outsourcing Polynomials Evaluation to a Malicious Cloud

Dawei Xie, Shandong University, Jinan, China
Haining Yang, School of Mathematics, Shandong University, Jinan, China
Jing Qin, Shandong University, Jinan, China
Jixin Ma, Greenwich University, London, UK

ABSTRACT

As cloud computing provides affordable and scalable computational resources, delegating heavy computing tasks to the cloud service providers is appealing to individuals and companies. Among different types of specific computations, the polynomial evaluation is an important one due to its wide usage in engineering and scientific fields. Cloud service providers may not be trusted, thus, the validity and the privacy of such computation should be guaranteed. In this article, the authors present a protocol for publicly verifiable delegations of high degree polynomials. Compared with the existing solutions, it ensures the privacy of outsourced functions and actual results. And the protocol satisfies the property of blind verifiability such that the results can be publicly verified without learning the value. The protocol also improves in efficiency.

KEYWORDS
Blind Verification, Cloud Computing, Large Polynomials, Privacy, Publicly Verifiable

1. INTRODUCTION

It is increasingly common for mobile devices with relatively weak computing power to be used as general computing devices, such as smart phones and netbooks. This trend, coupled with their increasing desire to execute computationally intensive tasks, makes outsourcing computation to the cloud service providers a promising solution. The outsourcing computation enables resource-constrained clients to enjoy almost unlimited computational resources. The clients deliver their computational tasks to cloud service providers and receive computational result from the providers in a pay-per-use manner. Hence, the clients are no longer restricted to their limited CPU, storage and bandwidth. Moreover, outsourcing computation provides economic benefits to the clients and allows them to avoid or minimize up-front IT infrastructure costs.

Despite the tremendous advantages, outsourcing computation raises several new security challenges, which make the clients reluctant to outsource their computations to cloud service providers. The first concern is the correctness of the computational results done by the providers, since the cloud service providers may not be trusted. Their misbehaviors are motivated by financial incentives (e.g., saving the computing resources for other transactions) or caused by hacking and bug in system. It means that there is no guarantee on the correctness of the computational results.
In order to address this problem, the notion of Verifiable Computation (VC) was introduced, which enables the clients to verify correctness of the results. Clearly, the verification of correctness must be substantially easier than the computation that was initially outsourced. Next, Parno, Raykova, and Vaikuntanathan (2012) proposed a new notion of Publicly Verifiable Computation (PVC) by extending the definition of VC, which makes the computational results can be verified by any third party besides the delegators. This is important in the contexts where the results have to be checked by several clients who cannot share a secret key in advance. Another concern is the privacy, since the relevant data may contain sensitive information, such as personal health assessment, stock prediction, financial performance analysis and so on, the computational results and the outsourced functions should be hidden. Encryption does not fundamentally solve this problem, because it is very difficult or inefficient to perform meaningful operations on ciphertext. One common approach is that the client does some carefully designed local disguise process of the function before sending it to cloud service providers. Consider the privacy of results, blind verifiability is an important property of outsourcing computation such that the results can be publicly verified without learning the value. For example, a financial company delegates a certain computational task to cloud service providers, and it wants to ensure the privacy of the results. Further, efficiency is also a crucial challenge. Thus, an outsourcing computation protocol should satisfy the following four design goals: public verifiability, privacy of result/function, blind verifiability and efficiency.

In this paper, the authors study the particular problem of polynomial evaluation. Among all types of computations, the polynomial function evaluation is an important one due to its wide usage in engineering and scientific problems. For instance, the medical center executes polynomial functions over the personal health data, which uploaded from various wearable devices. Based on these data, the medical center assesses personal health and makes suggestions for people to keep healthy. Also, the securities company utilizes the financial software to analyze the economic performance of stocks, by executing polynomial functions over the past data. Benabbas, Gennaro, and Vahlis (2011) proposed the first practical verifiable computation protocol for high degree polynomial functions, by using the algebraic pseudorandom functions (PRFs). Nevertheless, their protocol does not satisfy public verifiability. In the same line of work, Fiore and Gennaro (2012) devised new algebraic PRFs to develop a publicly verifiable computation protocol for the delegated polynomials. After that, researchers proposed numerous protocols for secure outsourcing of polynomials (e.g., Catalano & Fiore, 2013; Elkhiyaoui, Azraoui, & Molva, 2016; Luo, Yang, & Cong, 2018; Papamanthou, Shi, & Tamassia, 2013; Ye, Zhang, & Fu, 2016; Zhang & Safavi-Naini, 2014).

From the practical perspective, however, the existing protocols for outsourcing polynomials computation still have some limitations, which make it not practical in real world application scenarios. The first limitation is that the actual polynomials and the actual results are revealed to the cloud servers. In many practical delegation scenarios, the privacy of the polynomials and the results must be ensured. The second limitation is that almost all protocols do not satisfy the blind verifiability. Consider a financial company that wishes to delegate the computation of a certain expensive data analysis polynomial function to a cloud server. Since the company will make an investment strategy for the next year based on the results, it would like to ensure the privacy of the polynomial and the results. Meanwhile, the blind verifiability is also a necessary requirement. Once the relevant data are leaked, rivals will speculate on its investment plans and sabotage the investments. The damage could result in huge economic losses for the company. The gaps in the existing protocols motivate the authors to investigate the outsourcing polynomials computation.

In this paper, the authors propose an efficient publicly verifiable outsourcing computation protocol for polynomial functions. The key characteristics of the protocol are that it can ensure the privacy (of the polynomials and the actual results) and support blind verifiability.

1.1. Our Contributions
The main contributions in this paper can be summarized as follows.
Bitstream-Based JPEG Encryption in Real-time
www.igi-global.com/article/bitstream-based-jpeg-encryption-in-real-time/84133?camid=4v1a

An Improved Fingerprinting Algorithm for Detection of Video Frame Duplication Forgery
www.igi-global.com/chapter/improved-fingerprinting-algorithm-detection-video/75664?camid=4v1a