Poster: Practical and Provably Secure Distributed Aggregation: Verifiable Additive Homomorphic Secret Sharing

Georgia Tsaloli
Chalmers University of Technology
tsaloli@chalmers.se

Gustavo Banegas
Chalmers University of Technology
gustavo@cryptme.in

Aikaterini Mitrokotsa
Chalmers University of Technology
aikaterini.mitrokotsa@chalmers.se

***Abstract*—In this poster, we present our recently published work. Often clients (e.g., sensors, organizations) need to outsource joint computations that are based on some joint inputs to external untrusted servers. These computations often rely on the aggregation of data collected from multiple clients, while the clients want to guarantee that the results are correct and, thus, an output that can be publicly verified is required. However, important security and privacy challenges are raised, since clients may hold sensitive information. In this paper, we propose an approach, called verifiable additive homomorphic secret sharing (VAHSS), to achieve practical and provably secure aggregation of data, while allowing for the clients to protect their secret data and providing public verifiability i.e., everyone should be able to verify the correctness of the computed result. We propose three VAHSS constructions by combining an additive homomorphic secret sharing (HSS) scheme, for computing the sum of the clients' secret inputs, and three different methods for achieving public verifiability, namely: (i) homomorphic collision-resistant hash functions; (ii) linear homomorphic signatures; as well as (iii) a threshold RSA signature scheme. In all three constructions, we provide a detailed correctness, security, and verifiability analysis and detailed experimental evaluations. Our results demonstrate the efficiency of our proposed constructions, especially from the client side.**

I. Introduction

The rise of communication technologies has formed multiple smart electronic devices (e.g., cell phones, sensors, wearables) with network connection, which produce a big amount of data every day. Remote, often untrusted, cloud servers are employed to store and process these data to be used by third parties, such as research institutions, hospitals, or electricity companies. Many applications (e.g., environmental monitoring, updating parameters in machine learning, statistics about electricity consumption) require joint computations on data coming from multiple clients. For example, using smart metering, data that are collected from sensors/clients can be used to compute statistics for the electricity consumption, while environmental sensors collect data that can be used to measure emissions and data collected from mobile phones can be aggregated and processed to appropriately update parameters in machine learning models for accurate user profiling.

Although decentralization has been a recent trend, we have witnessed a steady rise of massively distributed but not decentralized systems. When multiple clients outsource a joint computation using their joint inputs, multiple servers can be employed in order to avoid single points of failure and perform a reliable joint computations on the clients' inputs. Although this distributed cloud-assisted environment is very appealing and offers exceptional advantages, it is also followed by serious security and privacy challenges. Thus, in this work, we present the formal and practical analysis of verifiable additive homomorphic secret sharing (VAHSS), a novel cryptographic primitive introduced [1], which allows for multiple clients to outsource the joint addition of their inputs to multiple untrusted servers, providing guarantees that the clients' inputs remain secret as well as that the computed result is correct (i.e., verifiability property). More precisely, this paper is an extended version of the preliminary article [1].

We address the problem of cloud-assisted computing characterized by the following constraints: (i) multiple servers are recruited to perform joint additions on the inputs of n clients; (ii) the inputs of the clients need to remain secret; (iii) the servers are untrusted; (iv) no communication between the clients is possible; and, (v) anyone should be able to confirm that the computed result is correct (i.e., public verifiability property). More precisely, let us consider n clients (as illustrated in Figure 1), which hold n individual secret inputs $x_1, x_2, \dots x_n$, and they want to deploy the joint computation of the function $f(x_1, x_2, \dots, x_n) = x_1 + x_2 + \dots + x_n$ on their joint inputs by releasing shares of their inputs to multiple untrusted servers (the latter denoted by s_j for $j \in [m]$). We denote the share of a client c_i given to the server s_j by x_{ij}. Tsaloli et al. [2] addressed the problem of computing the joint multiplications of n inputs corresponding to n clients and introduced the concept of verifiable homomorphic secret sharing (VHSS). More precisely, VHSS allows to jointly perform the computation of a function $f(x_1, x_2, \dots, x_n) = y$, including no communication between the clients, and allowing anyone to get a proof π that the computed result is correct, i.e., providing to anyone a pair (y, π) which confirms the correctness of y (i.e., public verification). However, the possibility to achieve verifiable homomorphic secret sharing for other functions (e.g., addition) has been left open.

In this paper, we revisit the concept of verifiable homomorphic secret sharing (VHSS) and we explore the possibility to achieve verifiable additive homomorphic secret sharing. Our research shows that the latter is possible and we pro-

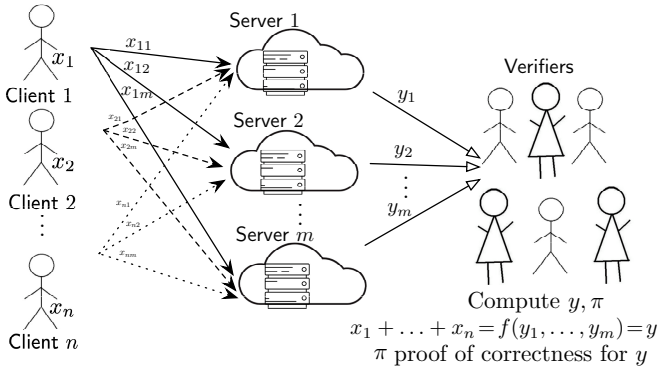


Fig. 1: n clients outsourcing the joint addition of their joint inputs to m servers.

pose three concrete constructions that employ m servers to jointly compute the additions of n clients' inputs securely and privately, while, additionally, ensuring public verifiability. The proposed constructions can be utilized, for example, to compute statistics over electricity consumption when data are collected from multiple clients, in order to remotely monitor and determine a diagnosis for multiple patients according to their collected data, as well as to measure environmental conditions while using multiple sensors' data that come from environmental sensors (e.g., temperature, humidity). We have substantially extended the preliminary article [1] and added a detailed evaluation (both theoretical and experimental) of the three proposed VAHSS constructions. In the submitted paper, we present a detailed analysis for each of the constructions based on different conditions, providing both theoretical and experimental results.

Our Contribution. We address the problem of computing joint additions with privacy and security guarantees as the main requirements. More precisely, we treat the problem of verifiable multi-client aggregation that involves the following parties: (i) n clients, which hold secret inputs $x_1, x_2, \ldots, x_n$, respectively; (ii) m untrusted servers to whom the sum computation is outsourced; and, (iii) any verifier that would like to confirm that the computed sum is correct. We present, for the first time, three concrete constructions of verifiable additive homomorphic secret sharing (VAHSS).

We employ three different primitives (i.e., homomorphic hash functions, linearly homomorphic signatures, and threshold signatures) as the baseline for the generation of partial proofs (values that are used to confirm the correctness of the computed sum). The partial proofs are computed by either the servers or the clients. These characteristics lead to three different instantiations of VAHSS. Additionally, we have altered the original VHSS definition to capture the different scenarios on the proofs' generation; therefore, allowing for the employment of VHSS in several application settings.

Our constructions rely on casting Shamir's secret sharing scheme over a finite field $\mathbb{F}$ as an n-client, m-server, and t-perfectly secure additive homomorphic secret sharing (HSS) for the function that sums n field elements. Firstly, employing homomorphic collision-resistant hash functions [3, 4] and incorporating them to the additive HSS, we design a construction, such that each server produces a partial proof. Next, a linearly homomorphic signature scheme [5] is combined with the additive HSS, which results in an instantiation where each client generates a partial proof. Ultimately, the employment of a threshold RSA signature scheme [6] in additive HSS allows a subset of servers to generate partial proofs that correspond to each client. In all three proposed constructions, we have provided detailed correctness, security, and verifiability analysis. Furthermore, we provide an evaluation of the three proposed constructions, in which we describe the cost of the required operations for each of the employed algorithms as well as present a detailed experimental evaluation. More precisely, we evaluate the performance of all three proposed VAHSS constructions and compare and illustrate how the employed algorithms perform, depending on the amount of the clients that participate during the computation and the required computation time for the verification process.

References

[1] Tsaloli, G.; Mitrokotsa, A. Sum It Up: Verifiable Additive Homomorphic Secret Sharing. In *Information Security and Cryptology—ICISC 2019*; Seo, J.H., Ed.; Springer International Publishing, 2020; pp. 115–132. [CrossRef]

[2] Tsaloli, G.; Liang, B.; Mitrokotsa, A. Verifiable Homomorphic Secret Sharing. In Proceedings of the 12th International Conference on Provable Security, ProvSec 2018, Jeju, Korea, 25–28 October 2018; pp. 40–55. [CrossRef]

[3] Yao, H.; Wang, C.; Hai, B.; Zhu, S. Homomorphic Hash and Blockchain Based Authentication Key Exchange Protocol for Strangers. In Proceedings of the International Conference on Advanced Cloud and Big Data (CBD), Lanzhou, China, 12–15 August 2018; pp. 243–248. [CrossRef]

[4] Krohn, M.; Freedman, M.; Mazieres, D. On-the-fly verification of rateless erasure codes for efficient content distribution. In Proceedings of the IEEE Symposium on Security and Privacy, Berkeley, CA, USA, 12 May 2004; pp. 226–240. [CrossRef]

[5] Catalano, D.; Marcedone, A.; Puglisi, O. Authenticating Computation on Groups: New Homomorphic Primitives and Applications. In *Advances in Cryptology—ASIACRYPT 2014*; Sarkar, P., Iwata, T., Eds.; Springer: Berlin/Heidelberg, Germany, 2014; pp. 193–212.

[6] Bozkurt, İ.N.; Kaya, K.; Selçuk, A.A. Practical Threshold Signatures with Linear Secret Sharing Schemes. In *Progress in Cryptology—AFRICACRYPT 2009*; Preneel, B., Ed.; Springer: Berlin/Heidelberg, Germany, 2009; pp. 167–178.

Poster: Practical and Provably Secure Distributed Aggregation: Verifiable Additive Homomorphic Secret Sharing

Georgia Tsaloli, Gustavo Banegas and Aikaterini Mitrokotsa

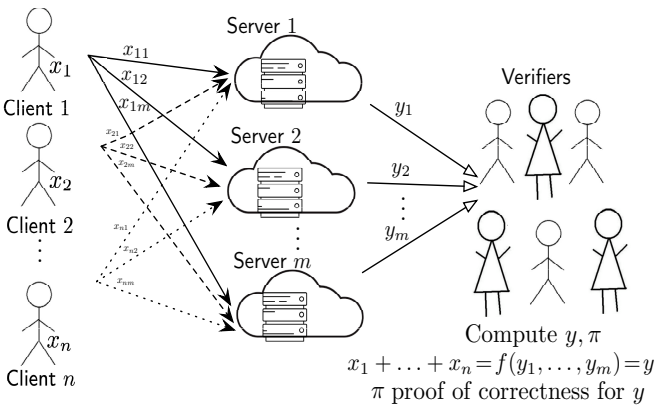
Challenges:

- Outsourcing the sum computation of clients' aggregated data to untrusted cloud servers while protecting clients' sensitive input values
- Allowing a subset of the untrusted servers to collude
- Untrusted cloud servers might want to alter/control the computed result

Results:

- Develop three concrete constructions to securely compute the sum of data given from n clients without compromising clients' secret inputs
- Provide three solutions to convince about the correctness of the computed result, i.e., provide public verifiability to the proposed solutions
- Present the experimental analysis of the proposed constructions to show their efficiency

Overview of our setting:



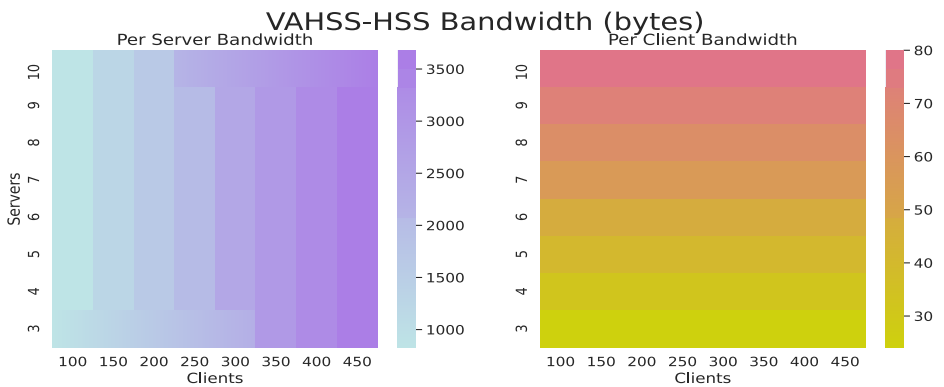
Methods Used for Verifiability:

- First construction uses homomorphic collision resistant hash functions (VAHSS-HSS)
- Second construction uses linear homomorphic signatures (VAHSS-LHS)
- Third construction uses a threshold RSA signature scheme (VAHSS-TSS)

Evaluation results:

- Theoretical analysis of the constructions
- Prototype analysis including Timing for the different algorithms used and Bandwidth per server or per client

Bandwidth for VAHSS-HSS construction per server and per client*:



* *Scan the QR code below to read detailed analysis for all the constructions.*