RMC-PVC: A Multi-Client Reusable Verifiable Computation Protocol (Long version)

Anonymous Author(s)

ABSTRACT

The verification of computations performed by an untrusted server is a cornerstone for delegated computations, especially in multi-clients setting where inputs are provided by different parties. Assuming a common secret between clients, a *garbled circuit* offers the attractive property to ensure the correctness of a result computed by the untrusted server while keeping the input and the function private. Yet, this verification can be guaranteed only *once.*

Based on the notion of *multi-key homomorphic encryption* (MKHE), we propose RMC-PVC a multi-client verifiable computation protocol, able to verify the correctness of computations performed by an untrusted server for inputs (encoded for a garbled circuit) provided by multiple clients. Thanks to MKHE, the garbled circuit is reusable an arbitrary number of times. In addition, each client can verify the computation by its own. Compared to a single-key FHE scheme, the MKHE usage in RMC-PVC allows to reduce the workload of the server and thus the response delay for the client. It also enforce the privacy of inputs, which are provided by different clients.

ACM Reference Format:

Anonymous Author(s). 2022. RMC-PVC: A Multi-Client Reusable Verifiable Computation Protocol (Long version). In *Proceedings of ACM Conference (Conference'17).* ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

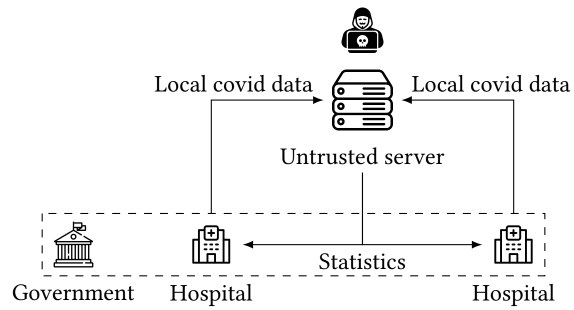


Figure 1: Use-case of RMC-PVC where two hospitals depending on a trusted government want to compute jointly some statistics over local covid data through an untrusted server.

1 INTRODUCTION

Consider public hospitals, who depend on a trusted authority such as some government, which want to perform some statistics over COVID-19 statistics (see Fig. 1). In an ideal world, each hospital sends its sensitive data as daily contamination statistics to the server, which then returns the valid result. However, a server can be either compromised by an attacker or malicious in the first place. Therefore, hospitals are facing two problems when outsourcing their data: first, an attacker could learn information about the sensitive data provided by the hospitals and secondly, the attacker could modify the behavior of the server in order to compute an invalid result. Thus, it is crucial that both privacy of the data and integrity of the computations must be ensured when outsourcing computations. Additionnally, each hospital depends on the general authority such as a governement and hence is honest. However, each hospital has local data that must remain private even after the computation of the statistics.

In a more general point of view, ensuring the privacy of data and the correctness of computations when outsourcing computation in a multi-client setting have been intensively studied by many researchers. In [Gennaro et al. 2010], Gennaro *et al.* introduced the notion of *non-interactive verifiable-computation scheme* allowing a client to verify the computation $f(x) = y$ of a function f over an input x, performed by a malicious server. In a verifiable-computation scheme, the server does not perform the function f over the input x but over an encoding of x denoted σ_x. It is possible to retrieve x from σ_x by knowing some secret. Hence, given σ_x only, then server cannot learn information about the input x. The evaluation of the function f over the encoded input σ_x produces the encoding of the result y denoted σ_y. At the end, if the computations done by the server are valid, then the client can retrieve $f(x) = y$ from σ_y. Otherwise, the client can detect that the computed result is not correct. Note that the server cannot retrieve y from σ_y (as explained in more details in Section 2.1).

The seminal work of Andrew Yao in 1986 introduced the notion of *garbled circuit* [Yao 1986] where non-interactive verifiable-computation scheme was proposed. Garbled circuits ensure the privacy of the input, but also the correctness of computation for a single-evaluation of f represented as a boolean circuit. Some works have shown how to address the one-time limitation of the garbled circuit such as in [Gennaro et al. 2010] using Fully Homomorphic Encryption (FHE). Introduced in [Gentry 2009], FHE allows a server to perform any computations over encrypted data without relying on the decryption key. The idea presented in [Gennaro et al. 2010] is to evaluate the garbled circuit homomorphically over encrypted encoded input, allowing to reuse the garbled circuit an arbitrary number of times.

The secure function evaluation in a multi-client setting has been widely studied by researchers leading to a variety of approaches. Garbled circuits and Multi-Key Homomorphic Encryption (MKHE) have received less attention. This paper shows that MKHE is notably

Conference'17, July 2017, Washington, DC, USA

ACM ISBN 978-x-xxxx-xxxx-x/YY/MM…$15.00
https://doi.org/10.1145/nnnnnnn.nnnnnnn

an interesting primitive to obtain privacy, but also surprisingly more efficient compared to single-key FHE in [Gennaro et al. 2010].

Contribution. We propose RMC-PVC a Reusable Multi-Client Protocol for Verifiable Computation designed to verify the computations of any function (common to every clients) performed by an untrusted server using garbled circuits, over inputs provided by multiple clients. The usage of a MKHE scheme instead of a single-key FHE is motivated to make the garbled circuit reusable an arbitrary number of times, to ensure input-privacy against both the server and other clients, and to obtain a shorter response delay from the server to the clients by encrypting the garbled circuit *once* (hence not at every computation as done in [Gennaro et al. 2010]). Our protocol uses one key uses to encrypt the garbled circuit *once* and another key to encrypt the input.

More than the aforementionned properties ensured by our construction, we present a feasability result in combining MKHE and garbled circuits in the multi-client setting. Combining FHE and garbled circuits has already been shown to be feasible in [Gennaro et al. 2010], which relies on a single-key FHE scheme. However, generalizing this approach in the multi-client setting using the same homomorphic encryption key for each client, does *not* prevent a client to learn input of the other clients. In contrast, the usage of a MKHE scheme instead of a single-key FHE scheme, and providing for each client its own encryption key can overcome this problem, but remains an interesting question. However, with MKHE, we expect the result to be encrypted under multiple public encryption keys. In a setting where related secret keys are owned by different clients, the decryption is a *non-trivial question*. To overcome this issue, we use a particular MKHE scheme having a *distributed decryption* property [Chen et al. 2019], allowing each client to verify the untrusted server's computations by its own.

Related Work. The notion of non-interactive verifiable computing, introduced in [Gennaro et al. 2010], have been widely studied and have led to a variety of solutions. The notion *non-interactive* proofs are crucial for looking at correctness of computations over a minimal number of rounds, to reduce as much as possible the communications between clients and the server. Micali's Computational Sound proofs [Micali 2000] are adapted for non-interactive verifiable computations under the Random Oracle Model, as well as [Goldwasser et al. 2015] but only for restricted class of functions. We move away from this paradigm to focus on garbled circuits, allowing to ensure the correctness of computations within two rounds, independently of the size of the function to be evaluated.

The one-time limitation of garbled circuits has been addressed in different approaches, either by using *Cut-And-Choose* [Gennaro et al. 2010; Huang et al. 2014; Lindell and Pinkas 2015] technique, or by using homomorphic encryption [Gennaro et al. 2010], but only in a single-client setting. Multi-client verifiable computation setting has been addressed in numerous ways. For instance, Goldwasser *et al.* used multi-party functional encryption, however restricted to binary function [Goldwasser et al. 2014] whereas our work handles an arbitrary function.

The work of [Kamara et al. 2011] proposed a multi-client verifiable computation scheme where every client shares the same pool of entropy in order to generate the same garbled circuit. The main drawback of this solution is that a new garbled circuit has to be generated for each round of computations, even if the function remains the same. Our work adds a reusability property meaning that the garbled circuit is computed only once for a given function (even if the evaluation is done multiple times). Closer to our work, [Choi et al. 2013] studied a multi-client verifiable computation scheme based on garbled circuit using Proxy Oblivious Transfer, where the first client is in charge of the creation of the garbled circuit and the encoding of the input for the other clients. Rather to create an unbalanced execution time among clients, only the first client verifies computations performed by the server. In our protocol, every client has the same workload and can verify computations by its own.

Functional Encryption (FE) has been shown to be an interesting cryptographic primitive. Indeed, [Goldwasser et al. 2013] has exposed a reusable garbled circuit. In summary, they rely on an universal circuit which given a circuit C and an input x, outputs $C(x)$. The circuit is given to the server, as well as x encrypted using the functional encryption scheme. The universal circuit, viewed as a function, is linked with the decryption key of the FE scheme. To obtain the result, they rely on the decryption function of the FE scheme, by decrypting the encryption of x, producing the desired output. Their approach does not ensure the privacy of the output, in constrast to our construction where the output privacy is ensured.

More recent work such that the construction of [Fiore et al. 2020] proposed to compute the function f homomorphically and later proof the validity of the computation using a Succint Non-interactive Argument of Knowledge. Similarly in [Bois et al. 2021], they suggested a verifiable computation scheme using Somewhat Homomorphic Encryption (a FHE scheme supporting a bounded-degree algebraic circuit) and an Homomorphic Hash function allowing to operate over hashs. Althrough efficient for the proving and verification, both of these works are limited to the single-client setting. Moreover, work of [Bois et al. 2021] supports only a bounded-degree functions. It contrast our work, designed for the multi-client setting and supporting arbitratry functions.

Close to our work, [Lafourcade et al. 2022] presents a non-interactive verifiable computation based on MKHE and garbled circuits for the single-client setting. Conceptually, the client sends to the server his input σ_x encrypted under an MKHE key pk_x (with sk_x kept secret by the client). Then, given a garbled circuit encrypted under pk_f (with sk_f owned by the client), the server sends back σ_y encrypted under both pk_x and pk_f. Their approach *cannot* be generalized to the multi-client setting: assuming a client sending its input encrypted under its own key, then the obtained encoded result would be encrypted under the public key of all clients, rendering the encoded output impossible without sharing the secret keys to other clients, exposing the sent inputs. Our paper proposes a solution for the multi-client setting where σ_y can be obtained by other clients without exposing their secret keys and hence ensuring the input privacy.

Outline. We recall in Section 2 the definition of a verifiable-computation scheme as well as the building blocks used for RMC-PVC. In Section 3, we detail the design of RMC-PVC. Finally, we analyse the complexity of our scheme in Section 5.

2 PRELIMINARIES

We present the definition of a verifiable-computation scheme in the general setting. We also describe the core primitives of RMC-PVC, namely the Yao's garbled circuit and MKHE scheme.

2.1 Definition of Verifiable Computation Scheme

A verifiable computation scheme aims to verify outsourced computations over an untrusted server. Suppose that a client wants to delegate $y = f(x)$ the computation of the function f over an input x to a server. We provide the model of the verifiable computation defined in [Gennaro et al. 2010]:

Definition 2.1 (verifiable computation scheme [Gennaro et al. 2010]). A *verifiable computation scheme* VC is composed of four algorithms VC.KeyGen, VC.ProbGen, VC.Compute, VC.Verify defined as:

- $\mathsf{VC.KeyGen}(f, \lambda) \rightarrow (\mathsf{PK}, \mathsf{SK})$: Given a function f and a security parameter λ, output public key PK (that encodes the function f) and secret key SK.
- $\mathsf{VC.ProbGen}_{\mathsf{SK}}(x) \rightarrow (\sigma_x, \tau_x)$: Given the input x and the private key SK, return σ_x, the public encoding of input x, (used by the server to compute $y = f(x)$) and τ_x, a secret verification string, (used for to verify the correctness of computations).
- $\mathsf{VC.Compute}_{\mathsf{PK}}(\sigma_x) \rightarrow \sigma_y$: Given the public key PK and the encoded input σ_x, return σ_y the encoded output.
- $\mathsf{VC.Verify}_{\mathsf{SK}}(\tau_x, \sigma_y) \rightarrow y \cup \bot$: Given SK the private key, τ_x the secret verification string and σ_y the encoded output, output y if the output is verified, $\bot$ otherwise.

A verifiable computation scheme VC must be *correct, secure* and *outsourceable.* A VC scheme is *correct* for any input x, an honest server can compute $f(x)$. A VC scheme is *secure* if the client is able to detect if a malicious server returns $\hat{y}$ an invalid result instead of the valid result $f(x)$. A VC scheme is *outsourceable* meaning that the client must perform strictly less operations than computing the function by himself. We give the formal definitions of usual security properties of a verifiable computation scheme. Optionally, a VC scheme is said *private* if the server cannot learn some information about the inputs x and the output $f(x)$.

Definition 2.2 (Correctness [Gennaro et al. 2010]). Let VC be a verifiable computation scheme. For every function f, every input x, given $(\mathsf{PK}, \mathsf{SK}) \leftarrow \mathsf{VC.KeyGen}(f, \lambda)$, the equality holds:

$$f(x) = \mathsf{VC.Verify}_{\mathsf{SK}}(\mathsf{VC.Compute}_{\mathsf{PK}}(\mathsf{VC.ProbGen}_{\mathsf{SK}}(x)))$$

Definition 2.3 (Outsourceability). For every function f, a verifiable computation scheme VC is *outsourceable* if the asymptotic complexities of VC.ProbGen and VC.Verify are strictly lower than the asymptotic complexity of the fastest algorithm to compute f.

A verifiable computation scheme is *secure* if the server manages to return an invalid result accepted by the client only with a negligible probability. We formalize the security of the verifiable computation scheme with the game $\mathsf{Exp}^{\mathcal{A}}_{\mathsf{Sec}}$ presented in Fig. 2; the challenger expects from the adversary to produce invalid encoded result $\sigma_{\hat{y}}$ where $\hat{y} \neq f(x)$ for an input x chosen by the adversary. The adversary must also produce σ_x the encoding of the input x. The adversary has access to an oracle $O^{\mathsf{PubProbGen}}$ which for an input x, computes the encoding σ_x as well as the private encoding τ_x before to output only σ_x. The oracle $O^{\mathsf{PubProbGen}}$ can be called by the adversary a polynomial number of times and until to output the result. The adversary wins at $\mathsf{Exp}^{\mathcal{A}}_{\mathsf{Sec}}$ if the provided encoded result is accepted by the verifiable computation scheme.

Definition 2.4 (Security [Gennaro et al. 2010]). Let VC be a verifiable computation scheme and λ the security parameter, then for every function f, and every $(\mathsf{PK}, \mathsf{SK}) \leftarrow \mathsf{VC.KeyGen}(f, \lambda)$, for every PPT adversary $\mathcal{A}$ we have: $\Pr[\mathsf{Exp}^{\mathcal{A}}_{\mathsf{Sec}}[\mathsf{VC}, f, \lambda] = 1] = \mathsf{negl}(\lambda)$.

Game $\mathsf{Exp}^{\mathcal{A}}_{\mathsf{Sec}}[\mathsf{VC}, f, \lambda]$**:**
$\mathcal{T} \leftarrow \emptyset$
$(\mathsf{PK}, \mathsf{SK}) \leftarrow \mathsf{VC.KeyGen}(f, \lambda)$
$x, \sigma_x, \sigma_{\hat{y}} \leftarrow \mathcal{A}^{O^{\mathsf{PubProbGen}}(\mathcal{T}, \mathsf{VC}, \mathsf{SK}, \cdot)}(\mathsf{PK})$
retrieve τ_x associated with σ_x from $\mathcal{T}$
$\hat{y} \leftarrow \mathsf{VC.Verify}_{\mathsf{SK}}(\sigma_{\hat{y}}, \tau_x)$
Outputs 1 if $\hat{y} \neq \bot \bigwedge \hat{y} \neq f(x)$ else 0

Oracle $O^{\mathsf{PubProbGen}}(\underline{\mathcal{T}, \mathsf{VC}, \mathsf{SK}}, x)$:

$(\sigma_x, \tau_x) \leftarrow \mathsf{VC.ProbGen}_{\mathsf{SK}}(x)$
$\mathcal{T} \leftarrow \mathcal{T} \cup \{(\sigma_x, \tau_x)\}$
Outputs σ_x

Figure 2: Experiment for *security* of a verifiable computation scheme. By $\mathsf{poly}(\lambda)$, we denote a polynomial function depending on the security parameter λ. Parameters provided by the challenger are underlined.

A verifiable computation scheme is *private* if the server does not learn information about the input, or with a negligible probability. We formalize the privacy of a verifiable computation scheme with the game $\mathsf{Exp}^{\mathcal{A}}_{\mathsf{Priv}}$ introduced in Fig. 3. The challenger chooses one input x_b among x_0 and x_1 provided by the adversary $\mathcal{A}$, where b is a random bit. Then, the challenger computes and sends σ_{x_b} the encoding of the input x_b to the adversary $\mathcal{A}$, which responds with $\hat{b}$ a prediction over the bit b. The adversary $\mathcal{A}$ wins at $\mathsf{Exp}^{\mathcal{A}}_{\mathsf{Priv}}$ if his prediction $\hat{b}$ is valid *i.e.,* $\hat{b} = b$. Before the prediction, the adversary has access to the oracle $O^{\mathsf{PubProbGen}}$ (defined in Fig. 2) a polynomial number of times.

Definition 2.5 (Privacy [Gennaro et al. 2010]). Let VC be a verifiable computation scheme and λ a security parameter. Then, for every function f and every $(\mathsf{PK}, \mathsf{SK}) \leftarrow \mathsf{VC.KeyGen}(f, \lambda)$, for every PPT adversary $\mathcal{A}$ we have $\Pr[\mathsf{Exp}^{\mathcal{A}}_{\mathsf{Priv}}[\mathsf{VC}, f, \lambda] = 1] = \frac{1}{2} + \mathsf{negl}(\lambda)$.

2.2 Yao's Garbled Circuit

Suppose that a client wants to delegate $f(x)$, the computation of a function f over an input x to an untrusted server. The first step performed by the client is to compute $\Delta_f = (\mathcal{G}, \mathcal{W}, \mathcal{W}_{\text{in}}, \mathcal{W}_{\text{out}})$ the boolean circuit corresponding to f, where $\mathcal{G}$ is the set of gates in Δ_f, $\mathcal{W}$ is the set of wires in Δ_f, $\mathcal{W}_{\text{in}}$ (resp. $\mathcal{W}_{\text{out}}$) are the wires at the input (resp. output) of Δ_f, with $\mathcal{W}_{\text{in}} \subset \mathcal{W}$ (resp. $\mathcal{W}_{\text{out}} \subset \mathcal{W}$).

Game $\mathsf{Exp}^{\mathcal{A}}_{\mathsf{Priv}}[\mathsf{VC}, f, \lambda]$

$\mathcal{T} \leftarrow \emptyset$
$(\mathsf{PK}, \mathsf{SK}) \leftarrow \mathsf{VC.KeyGen}(f, \lambda)$
$(x_0, x_1) \leftarrow \mathcal{A}^{O^{\mathsf{PubProbGen}}(\mathcal{T}, \mathsf{VC}, \mathsf{SK}, \cdot)}(\mathsf{PK})$
$b \xleftarrow{\$} \{0, 1\}$
$(\sigma_{x_b}, \tau_{x_b}) \leftarrow \mathsf{VC.ProbGen}_{\mathsf{SK}}(x_b)$
$\hat{b} \leftarrow \mathcal{A}(\sigma_{x_b})$

Outputs 1 if $b = \hat{b}$ else 0

Figure 3: Experiment for *privacy* property of a verifiable computation scheme. Parameters provided by the challenger are underlined.

Each gate $g \in \mathcal{G}$ (see Fig. 4) takes as input two wires $w_0, w_1 \in \mathcal{W}$ and as an output a wire $w_2 \in \mathcal{W}$, denoted by $g(w_0, w_1) \to w_2$.

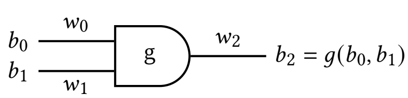


Figure 4: Representation of the gate $g(w_0, w_1) \to w_2 \in \mathcal{G}$.

To generate the garbled circuit, we require a symmetric encryption scheme denoted Sym composed of three functions Sym.KeyGen, Sym.Enc and Sym.Dec:

- $\mathsf{Sym.KeyGen}(1^\lambda) \to k$: Given a security parameter λ, output a λ-string k.
- $\mathsf{Sym.Enc}_k(m) \to \mathsf{c}$: Given a message m, output ct the message m encrypted under the key k.
- $\mathsf{Sym.Dec}_k(\mathsf{c}) \to m$: Given a ciphertext c representing the message m encrypted under the key k, output m.

Garbled circuit relies on a *Yao-Secure* symmetric encryption scheme.

Definition 2.6 (Yao-Secure Symmetric Encryption [Yao 1986]). A *Yao-Secure* symmetric encryption scheme Sym has the following properties:

- *Indistinguishable under multiple messages*, meaning that for every two vectors of polynomial length $\bar{x}$ and $\bar{y}$, no polynomial time adversary can distinguish between an encryption of $\bar{x}$ or $\bar{y}$.
- *Elusive range* meaning that the encryption of a message falls under different key spaces depending on the encryption key used.
- *Efficient checkable range* where given a key k and a ciphertext c, there is a polynomial time algorithm able to check if c has been encrypted under k.

For each wire $w \in \mathcal{W}$, the client chooses uniformly random *labels* $k_w^0 \leftarrow \mathsf{Sym.KeyGen}(1^\lambda)$, $k_w^1 \leftarrow \mathsf{Sym.KeyGen}(1^\lambda)$ corresponding respectively to 0 (wire off) and 1 (wire on). Once each wire has been affected with two labels, then for each gate $g(w_0, w_1) \to w_2$ we compute γ_g as follows:

$$\begin{aligned}
\gamma_g &= (\gamma_g^{00}, \gamma_g^{01}, \gamma_g^{10}, \gamma_g^{11}) \\
\gamma_g^{00} &= \mathsf{Sym.Enc}_{k_{w_0}^0}(\mathsf{Sym.Enc}_{k_{w_1}^0}(k_{w_2}^{g(0,0)})) \\
\gamma_g^{01} &= \mathsf{Sym.Enc}_{k_{w_0}^0}(\mathsf{Sym.Enc}_{k_{w_1}^1}(k_{w_2}^{g(0,1)})) \\
\gamma_g^{10} &= \mathsf{Sym.Enc}_{k_{w_0}^1}(\mathsf{Sym.Enc}_{k_{w_1}^0}(k_{w_2}^{g(1,0)})) \\
\gamma_g^{11} &= \mathsf{Sym.Enc}_{k_{w_0}^1}(\mathsf{Sym.Enc}_{k_{w_1}^1}(k_{w_2}^{g(1,1)}))
\end{aligned} \tag{1}$$

From Equation (1), we construct the *garbled circuit* $\gamma = \{\gamma_g | g \in \mathcal{G}\}$.

Definition 2.7 (Yao's garbled circuit[Yao 1986]). Suppose Sym a Yao-Secure symmetric encryption scheme. The verifiable computation scheme VCYao is composed of VCYao.KeyGen, VCYao.ProbGen, VCYao.Compute, VCYao.Verify where:

- $\mathsf{VCYao.KeyGen}(f, \lambda) \to (\mathsf{PK}, \mathsf{SK})$: Compute the boolean circuit $\Delta_f = (\mathcal{G}, \mathcal{W}, \mathcal{W}_{\text{in}}, \mathcal{W}_{\text{out}})$ corresponding to f, where $\mathcal{G}$ is the set of gates, $\mathcal{W}$ the set of wires, $\mathcal{W}_{\text{in}}$ the set of input wires and $\mathcal{W}_{\text{out}}$ the set of output wires. For each wire $w \in \mathcal{W}$, compute $k_w^0 \leftarrow \mathsf{Sym.KeyGen}(1^\lambda)$, $k_w^1 \leftarrow \mathsf{Sym.KeyGen}(1^\lambda)$. Compute the *garbled circuit* $\gamma = \{\gamma_g | g \in \mathcal{G}\}$. Output $\mathsf{PK} = \gamma$ and $\mathsf{SK} = \cup_{w \in \mathcal{W}} \{k_w^0, k_w^1\}$.
- $\mathsf{VCYao.ProbGen}_{\mathsf{SK}}(x) \to \sigma_x$: We denote the binary representation of input x composed of n bits by $x_1, \ldots, x_n$. Output $\sigma_x = \{k_{w_1}^{x_1}, \ldots, k_{w_n}^{x_n}\}$ the set of labels associated to the wire $w_i \in \mathcal{W}_{\text{in}}$ regarding on the input bits.
- $\mathsf{VCYao.Compute}_{\mathsf{PK}}(\sigma_x) \to \sigma_y$: Output $\sigma_y = \{k_{w_1}^{y_1}, \ldots, k_{w_m}^{y_m}\}$ the set of labels representing the binary encoding $y_1, \ldots, y_m$ of the output $y = f(x)$ using the garble circuit γ (simulating the function f) over the encoded input σ_x.
- $\mathsf{VCYao.Verify}_{\mathsf{SK}}(\sigma_y) \to y \cup \perp$: Output $y = y_1, \ldots, y_m$ only if for all $i \in [1, m]$ we have $k_{w_i}^{y_i} \in \{k_{w_i}^0, k_{w_i}^1\}$, otherwise the server is cheating, thus we refuse the result with $\perp$.

2.3 Multi-Key Homomorphic Encryption

Introduced in 2009 by Gentry [Gentry 2009], the Fully Homomorphic Encryption (FHE) allows to perform any circuit over encrypted data. A traditional use-case of FHE starts by a client who sends to a server an input x encrypted under a public key *pk*. Then, the server sends back the result of the function f over x, without relying on the decryption key *sk*. Multi-Key Homomorphic Encryption (MKHE) is a natural extension of FHE where the evaluation of a circuit is performed over inputs encrypted under different keys. In this work, we consider the MKHE scheme in [Chen et al. 2017].

Definition 2.8 (Multi-Key Homomorphic Encryption). A MKHE scheme with MKHE.KeyGen, MKHE.Enc, MKHE.Eval, MKHE.Dec:

- $\mathsf{MKHE.KeyGen}(1^\lambda) \to (pk, sk)$: Given the unary representation of the security parameter λ, output a new key pair (pk, sk) with pk the public key and sk the secret key.
- $\mathsf{MKHE.Enc}(pk, m) \to \{m\}_{\mathsf{PK}}$: Given a message m and a public key pk, output $\{m\}_{\mathsf{PK}}$ the message m encrypted under the set of public keys PK containing exactly one public key pk.
- $\mathsf{MKHE.Eval}(f, \{m_0\}_{\mathsf{PK}_0}, \{m_1\}_{\mathsf{PK}_1}) \to \{f(m_0, m_1)\}_{\mathsf{PK}_0 \cup \mathsf{PK}_1}$: Given a boolean circuit f, a ciphertext $\{m_0\}_{\mathsf{PK}_0}$ containing the message m_0 encrypted under the set of public keys PK_0,

a ciphertext $\{m_1\}_{\mathsf{PK}_1}$ containing a message m_1 encrypted under the set of public keys PK_1, output $\{f(m_0, m_1)\}_{\mathsf{PK}_0 \cup \mathsf{PK}_1}$ the evaluation of the function f over the inputs m_0 and m_1 encrypted under the union of the sets of public keys PK_0 and PK_1.

- $\mathsf{MKHE.Dec}(\mathsf{SK}, \{m\}_{\mathsf{PK}}) \rightarrow m$: Given the set of secret keys SK and a ciphertext $\{m\}_{\mathsf{PK}}$ containing a message m encrypted under the set of public keys PK, output m.

In this paper, we consider the MKHE scheme of [Chen et al. 2019] having the *distributed decryption* property. Conceptually, given a ciphertext and its secret key, a party can extract a so-called partial decryption. To obtain the plaintext, each party requires the partial decryption of the other parties. Then, by merging all partial decryptions, the party recover the underlying plaintext.

Definition 2.9 (Distributed Decryption[Chen et al. 2019]). Suppose the set of public encryption keys $\mathsf{PK} = \{pk_0, \ldots, pk_n\}$. Distributed decryption property of a MKHE scheme considers two additional functions MKHE.PartDec and MKHE.Merge where:

- $\mathsf{MKHE.PartDec}(sk_i, \{m\}_{\mathsf{PK}}) \rightarrow \mathsf{Part}_i(m)$: Given a secret key sk_i and a ciphertext $\{m\}_{\mathsf{PK}}$ containing a message m encrypted under the set of public keys PK, output $\mathsf{Part}_i(m)$ a partial decryption of $\{m\}_{\mathsf{PK}}$ using sk_i.
- $\mathsf{MKHE.Merge}(\mathsf{Part}_0(m), \ldots, \mathsf{Part}_n(m)) \rightarrow m$: Given partial decryption $\mathsf{Part}_i(m)$ where $i \in \{0, \ldots, n\}$, output m.

For clarity, given a ciphertext $c = \{m\}_{\mathsf{PK}}$ a message m encrypted under a *short* set of public keys *e.g.,* $\mathsf{PK} = \{pk_0, pk_1\}$, we denote c directly by $\{m\}_{pk_0, pk_1}$.

In Fig. 5, we present the game modeling the semantic security of the MKHE scheme having the distributed decryption property. In this game, the adversary $\mathcal{A}$ is called by the challenger to produce two inputs x_0 and x_1 of his choice. The challenger samples a random bit b and encrypts x_b under the key pk_m, denoted $\{x_b\}_{pk_m}$. Then, the adversary $\mathcal{A}$ is called with the public encryption key pk_m and the ciphertext $\{x_b\}_{pk_m}$, which responds with a prediction bit $\hat{b}$. The challenger outputs 1 if $\hat{b}$ is equals to b, 0 otherwise. During the game, the adversary $\mathcal{A}$ can call a polynomial number of times two oracles O^{Enc} and O^{PartDec}. Both have in common a set $\mathcal{K}$ allowing to share generated keys among the oracles. Every parameters given by the challenger to the oracles, underlined in the game, are assumed to be hidden from $\mathcal{A}$. The first oracle O^{Enc} takes as an input three parameters. Two first parameters, provided are the set $\mathcal{K}$ and the security parameter λ. The last parameter is a bitstring x provided by the adversary, which expects as an output the encryption of x. The second oracle O^{PartDec} takes as an input four parameters. The two first parameters, provided by the challenger, are the set $\mathcal{K}$ and the public encryption key pk_m. The two last parameters, provided by the adversary, are a bistring ψ and a public encryption key pk. The adversary expects from O^{PartDec} to produce a partial decryption of the bistring ψ with sk (obtained by the oracle by searching in $\mathcal{K}$ with pk). If the adversary sends either a malformed ciphertext ψ or public encryption key pk or a pk not contained in $\mathcal{K}$, then the oracle returns $\perp$ and the adversary would not get any advantage.

Game $\mathsf{Exp}^{\mathcal{A}}_{\mathsf{MKICDD}}[\lambda]$:

$\mathcal{K} \leftarrow \emptyset$
$(pk_m, sk_m) \leftarrow \mathsf{MKHE.KeyGen}(1^\lambda)$
$x_0, x_1 \leftarrow \mathcal{A}^{O^{\mathsf{Enc}}(\mathcal{K},\lambda,\cdot), O^{\mathsf{PartDec}}(\mathcal{K},pk_m,\cdot,\cdot)}(pk_m)$
$b \leftarrow_{\$} \{0,1\}$
$\{x_b\}_{pk_m} \leftarrow \mathsf{MKHE.Enc}(pk_m, x_b)$
$b' \leftarrow \mathcal{A}^{O^{\mathsf{Enc}}(\mathcal{K},\lambda,\cdot), O^{\mathsf{PartDec}}(\mathcal{K},pk_m,\cdot,\cdot)}(pk_m, \{x_b\}_{pk_m})$

Output 1 if $b = \hat{b}$ else 0

Oracle $O^{\mathsf{Enc}}(\underline{\mathcal{K}, \lambda}, x)$:

$(pk, sk) \leftarrow \mathsf{MKHE.KeyGen}(1^\lambda)$
$\{x\}_{pk} \leftarrow \mathsf{MKHE.Enc}(pk, x)$
$\mathcal{K} \leftarrow \mathcal{K} \cup \{(pk, sk)\}$

Output $\{pk, \{x\}_{pk}\}$

Oracle $O^{\mathsf{PartDec}}(\underline{\mathcal{K}, pk_m}, \psi, pk)$:

if $pk \neq pk_m$
  Retreive (pk, sk) from $\mathcal{K}$
  Return $\mathsf{MKHE.PartDec}(sk, \psi)$
else
  Return $\perp$

Figure 5: Experiment for the semantic security of a MKHE scheme having the distributed decryption property.

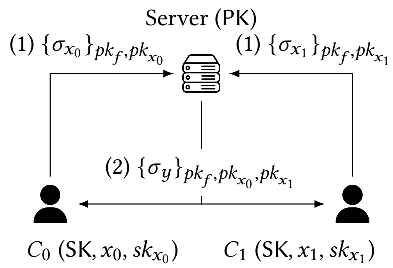
3 OUR PROTOCOL RMC-PVC

We present our verifiable-computation protocol called RMC-PVC (for Reusable Multi-Clients Protocol for Verifiable Computing) designed to verify computations performed by an untrusted server of an arbitrary function f over inputs provided by multiple clients. RMC-PVC is non-interactive: Communications between the server and the clients occurs during the input providing, and during the result verification steps.

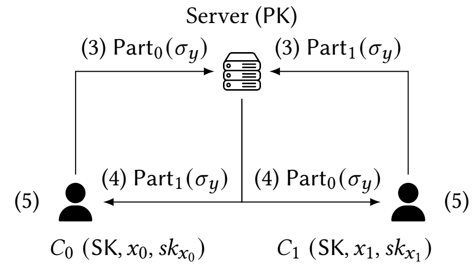
For the sake of clarity, we present our protocol RMC-PVC in a two-clients setting. We stress that RMC-PVC works for an *arbitrary* number of clients. After the presentation for two clients, we show how to generalize our protocol for any number of clients.

3.1 Initial Setup

The initial setup of our protocol requires the knowledge of the key pair $(\mathsf{PK}, \mathsf{SK})$ by clients C_0 and C_1. In our use-case, the key pair $(\mathsf{SK}, \mathsf{PK})$ is initially computed by a trusted honest party such as the government, and then shared to hospitals. The key pair is constructed as follows: Assume a boolean circuit f represented by the tuple $(\mathcal{G}, \mathcal{W}, \mathcal{W}_{\text{in}}, \mathcal{W}_{\text{out}})$ where $\mathcal{G}$ is the set of gates, $\mathcal{W}$ the set of wires, $\mathcal{W}_{\text{in}} \subset \mathcal{W}$ the set of input wires and $\mathcal{W}_{\text{out}} \subset \mathcal{W}_{\text{in}}$ the set of output wires. The trusted authority computes $(\mathsf{PK}_{\mathsf{Yao}}, \mathsf{SK}_{\mathsf{Yao}}) \leftarrow \mathsf{VCYao.KeyGen}(f, \lambda)$ where $\mathsf{PK}_{\mathsf{Yao}} = \{\gamma\} = \{\gamma_g | g \in \mathcal{G}\}$ and $\mathsf{SK}_{\mathsf{Yao}} = \cup_{w \in \mathcal{W}} \{k^0_w, k^1_w\}$. Then, it generates the function-related key pair with $(pk_f, sk_f) \leftarrow \mathsf{MKHE.KeyGen}(1^\lambda)$, and finally computes the



(a) Computation of $y = f(x_0, x_1)$ where the function f is simulated by the server using PK over σ_{x_0} and σ_{x_1} the encoding of respectively the input x_0 and x_1.



(b) Decryption of the encrypted encoded result $\{\sigma_y\}_{pk_f,pk_{x_0},pk_{x_1}}$, where each client shares his own partial decryption to other clients through the server.

Figure 6: Overview of RMC-PVC. Computation is presented in Figure 6a. Decryption and verification is presented in Figure 6b.

encrypted garbled circuit denoted $\{\gamma\}_{pk_f}$, which is equivalent to $\{\mathsf{MKHE.Enc}(pk_f, \gamma_g) | g \in \mathcal{G}\}$. By $\{0\}_{pk_f}$, we denote the bit 0 encrypted the key pk_f. We set PK $= \{\{\gamma\}_{pk_f}\}$ and SK $= \mathsf{SK}_{\mathsf{Yao}} \cup \{sk_f\}$. In the general case with multi-clients, all clients must share SK.

3.2 RMC-PVC with Two Clients

Suppose two clients C_0 and C_1 having respectively inputs x_0 and x_1, and want the server to compute $y = f(x_0, x_1)$ with $f : \{0,1\}^2 \to \{0,1\}^m$. Our protocol RMC-PVC works in five steps. Steps (1) and (2) are presented in Fig. 6a while Steps (3), (4) and (5) are depicted in Fig. 6b.

Step (1): Inputs encoding. Given his input x_0, client C_0 computes $(\sigma_{x_0}, \tau_{x_0})$ by executing $\mathsf{VCYao.ProbGen}_{\mathsf{SK}_{\mathsf{Yao}}}(x_0)$. Then, client C_0 generates the *input key pair* (pk_{x_0}, sk_{x_0}) with $\mathsf{MKHE.KeyGen}(1^\lambda)$, dedicated for input x_0. The public encoding σ_{x_0} of the input x_0 is encrypted under both pk_f and pk_{x_0}, producing $\{\sigma_{x_0}\}_{pk_f,pk_{x_0}}$, obtained by doing an homomorphic addition of the ciphertexts $\mathsf{MKHE.Enc}(pk_{x_0}, \sigma_{x_0})$ and $\mathsf{MKHE.Enc}(pk_f, 0)$. Client C_1 does the same operations over its own input x_1 in order to obtain $\{\sigma_{x_1}\}_{pk_f,pk_{x_1}}$. Then, client C_0 (resp. C_1) sends $\{\sigma_{x_0}\}_{pk_f,pk_{x_0}}$ (resp. $\{\sigma_{x_1}\}_{pk_f,pk_{x_1}}$) to the server as depicted in Fig. 6a.

Step (2): Function evaluation. The server evaluates the function f using the encrypted garbled circuit $\{\gamma\}_{pk_f}$ and encrypted encoded inputs $\{\sigma_{x_0}\}_{pk_f,pk_{x_0}}$ and $\{\sigma_{x_1}\}_{pk_f,pk_{x_1}}$, provided by clients at Step (1). The function evaluation assumes a circuit denoted Γ working at level of a gate $g(w_0, w_1) \to w_2 \in \mathcal{G}$, which given two labels $k_{w_0}^{b_0}, k_{w_1}^{b_1}$ (corresponding to bits b_0 and b_1) and the set of ciphertexts γ_g (detailed in Equation (1)), produces $k_{w_2}^{g(b_0,b_1)}$. Executed homomorphically, Γ allows to run a garbled circuit homomorphically without revealing the produced label $k_{w_2}^{g(b_0,b_1)}$, ensuring the reusability of the garbled circuit. Therefore, the server performs the evaluation of the circuit f by executing gate-by-gate $g(w_0, w_1) \to w_2 \in \mathcal{G}$ the homomorphic evaluation function $\mathsf{MKHE.Eval}(\Gamma, \{k_{w_0}^{b_0}\}_{pk_f,pk_{x_0},pk_{x_1}}, \{k_{w_1}^{b_1}\}_{pk_f,pk_{x_0},pk_{x_1}}, \{\gamma_g\}_{pk_f})$, which produces the ciphertext $\{k_{w_2}^{g(b_0,b_1)}\}_{pk_f,pk_{x_0},pk_{x_1}}$ the label $k_{w_2}^{g(b_0,b_1)}$ corresponding to bit $g(b_0, b_1)$ for the wire $w_2 \in \mathcal{W}$, encrypted under pk_f, pk_{x_0} and pk_{x_1}. At the end of the circuit, the server obtains a set of outputs labels $\{\{k_{w_i}^{y_i}\}_{pk_f,pk_{x_0},pk_{x_1}}\}_{m}^{i=1}$ denoted as $\{\sigma_y\}_{pk_f,pk_{x_0},pk_{x_1}}$, sent by as a response to every client (see Fig. 6a).

Step (3): Partial decryption. From $\{\sigma_y\}_{pk_f,pk_{x_0},pk_{x_1}}$, the client C_0 computes $\mathsf{Part}_0(\sigma_y) \leftarrow \mathsf{MKHE.PartDec}(sk_{x_0}, \{\sigma_y\}_{pk_f,pk_{x_0},pk_{x_1}})$ its own partial decryption. Client C_1 does the same operations in order to obtain the partial decryption $\mathsf{Part}_1(\sigma_y)$, sent to the server, as depicted in Fig. 6b.

Step (4): Partial decryptions sharing. In this step, the server is in charge to perform the sharing of partial decryptions. The server sends $\mathsf{Part}_0(\sigma_y)$ the partial decryption (computed and sent by C_0) to C_1. Symmetrically, the server sends $\mathsf{Part}_1(\sigma_y)$ the partial decryption computed by C_1, to C_0 as depicted in Fig. 6b. Note that to retreive σ_y, the server has to merge every partial decryptions, including $\mathsf{Part}_f(\sigma_y)$. However, $\mathsf{Part}_f(\sigma_y)$ cannot be computed by the server since it does not know sk_f kept secret by the clients. Hence, the usage of pk_f is legitimated both for efficiency (*i.e.,* garbled circuit is encrypted once) but also to prevent the server to recover information.

Step (5): Result verification. Before ensuring the integrity of the computation, client C_0 retrieves the encoding of the result returned by the server. To retreive the encoded output σ_y, C_0 requires the last partial decryption related the with the public key pk_f, computed as $\mathsf{Part}_f(\sigma_y) \leftarrow \mathsf{MKHE.PartDec}(sk_f, \{\sigma_y\}_{pk_f,pk_{x_0},pk_{x_1}})$. Then, C_0 computes $\sigma_y \leftarrow \mathsf{MKHE.Merge}(\mathsf{Part}_f(\sigma_y), \mathsf{Part}_0(\sigma_y), \mathsf{Part}_1(\sigma_y))$. Then, to verify the encoding σ_y, C_0 computes the output $y \leftarrow \mathsf{VCYao.Verify}_{\mathsf{SK}_{\mathsf{Yao}}}(\sigma_y)$. Note that this step does not require communication. Client C_1 does the same to verify the computation.

3.3 Generalization for multiple clients

Our protocol RMC-PVC can be generalized for any number of clients without modification. Assume $f : \{0,1\}^n \to \{0,1\}^m$ a boolean function where n denotes the number of clients. By C_i with $i \in \{1, \ldots, n\}$ we denote a client. All clients want to compute $f(x_1, \ldots, x_n) = y$ where x_i is an input known by C_i. As stated in the initial setup, we consider that all clients share SK. Each client C_i sends $\{\sigma_{x_i}\}_{pk_f,pk_{x_i}} \leftarrow \mathsf{MKHE.Enc}(pk_{x_i}, \sigma_{x_i}) + \{0\}_{pk_f}$ to the server as explained in the two-client case. The server computes and sends back to every client $\{\sigma_y\}_{pk_f,pk_{x_1},\ldots,pk_{x_n}}$ using PK. Each client C_i sends $\mathsf{Part}_i(\sigma_y)$ to the server. The server sends to all clients $\{\mathsf{Part}_1(\sigma_y), \ldots, \mathsf{Part}_n(\sigma_y)\}$ the set of partial decryptions. As presented in the two-case presentation, each client computes the partial decryption of the encrypted encoded result $\mathsf{Part}_f(\sigma_y) \leftarrow \mathsf{MKHE.PartDec}(sk_f, \{\sigma_y\}_{pk_f, pk_{x_1}, \ldots, pk_{x_n}})$ (with sk_f obtained from SK). From $\mathsf{Part}_f(\sigma_y)$ and the received set of partial decryptions, each client C_i computes the merge encoded output defined as $\sigma_y \leftarrow \mathsf{MKHE.Merge}(\mathsf{Part}_f(\sigma_y), \mathsf{Part}_1(\sigma_y), \ldots, \mathsf{Part}_n(\sigma_y))$. Each client C_i is able to retrieve y and to verify the computation performed by the server by computing $y \leftarrow \mathsf{VCYao.Verify}_{\mathsf{SK}_{\mathsf{Yao}}}(\sigma_y)$. If the function outputs $\perp$, then the evaluation performed by the server is invalid and therefore rejected by the clients. Otherwise, each client accepts the result y.

4 SECURITY ANALYSIS OF RMC-PVC

We first present the security assumptions in which our protocol is proven to be a verifiable computation scheme, before to present the security properties ensured by RMC-PVC.

4.1 Correctness

We state that RMC-PVC is correct. Intuitively, this means that the server can return a valid result by following our protocol, accepted by all clients.

Theorem 4.1 (Correctness of RMC-PVC). *Assuming* Sym *a Yao-Secure symmetric encryption scheme and* MKHE *a correct semantically secure homomorphic encryption scheme with distributed decryption property, then* RMC-PVC *is a correct verifiable-computation protocol.*

Proof. Since the correctness does not imply a behavior on the server, we consider the server to be honest. From the Sym scheme, we can construct VCYao the Yao verifiable computationf scheme [Yao 1986], which is by definition *correct*. By assumption, we have a *correct* MKHE scheme having the distributed decryption property.

At step (1), clients encodes their inputs using VCYao.ProbGen, next encrypted using MKHE.Enc. At step (2), assuming the server evaluates correctly the boolean circuit f and that MKHE is correct, then the server is able executed the garbled circuit homomorphically, producing a valid output labels encrypted with the public key of every clients and the function-related key. Steps (3) and (4) are focused on the decryption of the encrypted output labels. Assuming a correct multi-key homomorphic encryption scheme, then each client is able to retrieve the output labels as computed by the server. Finally, at step (5), output labels are verified by each client using VCYao.Verify which accept the labels since we assumed the server has computed the function as expected. Therefore, RMC-PVC is correct. □

4.2 Privacy

The privacy property ensured by RMC-PVC states that the server cannot learn information about the input provided by the clients. We formalize the privacy with the indistinguishability-based game $\mathsf{Exp}^{\mathcal{A}}_{\mathsf{MPriv}}$ (presented in Fig. ??) simulated by the challenger C against an adversary $\mathcal{A}$. In this game, the challenger generates the Yao's garbled circuits $(\mathsf{PK}_{\mathsf{Yao}}, \mathsf{SK}_{\mathsf{Yao}})$, a MKHE key pair (pk_f, sk_f) and the scheme key pair $(\mathsf{PK}, \mathsf{SK})$ containing in particular the encryption of the garbled circuit. The adversary $\mathcal{A}$ sends to the challenger two distinct inputs $\{x_i^0\}_{i=1}^n$ and $\{x_i^1\}_{i=1}^n$, where n is the number of clients, given as an input of the experiment. The challenger samples a random bit b and then computes $\{\sigma_{x_i^b}\}_{pk_f, pk_i}$ the encoded input encrypted under both pk_f, pk_i, and the private encoding $\tau_{x_i^b}$ for each i from 1 to n. The adversary is called by the challenger with the public key PK and the encryption of encoding of inputs $\{\{\sigma_{x_i^b}\}_{pk_f, pk_i}\}_{i=1}^n$. The adversary $\mathcal{A}$ responds with a prediction bit $\hat{b}$. At the end of the game, C outputs 1 if the $\mathcal{A}$ has successfully guess the bit b chosen by C *i.e.,* when $\hat{b}$ is equals to b.

During the game, $\mathcal{A}$ is allowed to call a polynomial times two distinct oracles $O^{\mathsf{MPubProbGen}}$ and O^{PartDec} defined in Fig. ??. Both oracles have in common the set $\mathcal{K}$ own by the challenger allowing to communicate keys generated by oracles to the other oracles. Every parameters provided by the challenger (including $\mathcal{K}$), underlined in the game, are assumed to be hidden from $\mathcal{A}$. The first oracle $O^{\mathsf{MPubProbGen}}$ takes as an input five parameters. The four three parameters, provided by the challenger, are the set $\mathcal{K}$, the Yao's garbled circuit secret key $\mathsf{SK}_{\mathsf{Yao}}$, the public encryption key pk_f and the security parameter λ. The adversary provides the input x. The oracle computes the encoding of x (as described in the protocol) and returns the public part of the encoding $\{\sigma_x\}_{pk_f, pk}$ where pk_f is owned by the challenger and pk is a fresh encryption key generated by the oracle. The second oracle O^{PartDec} takes as an input four parameters. The first two parameters, provided by the challenger, are the set $\mathcal{K}$, the public encryption key pk_f. The two last parameters, provided by the adversary, are a bitstring ψ and a public encryption key pk. The feature brought by this oracle to the adversary is the possibility to partially decrypt a ciphertext ψ using the secret sk (retreive by the oracle by searching the key pair (pk, sk) in the set of keys $\mathcal{K}$). However, we prevent the oracle to produce a partial decryption for the public key pk_f. Indeed, in our protocol, the adversary does not have access to the partial decryption related with pk_f. We assume that if an adversary provide either a malformed bitstring ψ or a public key pk, or if pk has not been generated by the oracle $O^{\mathsf{MPubProbGen}}$, then the oracle responds with $\perp$ and $\mathcal{A}$ would not get any advantage.

Theorem 4.2 (Privacy of RMC-PVC). *Suppose* Sym *a Yao-Secure symmetric encryption scheme and* MKHE *a correct semantically secure homomorphic encryption scheme with distributed decryption property. Suppose a security parameter* λ *and a number of clients* n*. Then for every PPT adversary* $\mathcal{A}$ *playing at* $\mathsf{Exp}^{\mathcal{A}}_{\mathsf{MPriv}}$*:*

$$\mathsf{Adv}^{\mathsf{MPriv}}_{\mathcal{A}}[f, \lambda, n] = |\frac{1}{2} - \Pr[\mathsf{Exp}^{\mathcal{A}}_{\mathsf{MPriv}}[f, \lambda, n] = 1]| \leq \mathsf{negl}(\lambda)$$

Sketch of the proof. With original garbled circuits, the privacy holds since the input provided by the client to the server is encoded. At each bit b of the input for a wire $w \in \mathcal{W}_{\text{in}}$ corresponds a label k_w^b. The server is not able to distinguish from label k_w^b either if $b = 0$ or $b = 1$, since the label is randomly chosen independantly of b. In RMC-PVC, the privacy holds on the same principle. Therefore, we show that if an adversary $\mathcal{A}$ is able to break the privacy of RMC-PVC, then we can create an adversary $\mathcal{B}$ able to break the privacy of the garbled circuit.

Game $\underline{\mathsf{Exp}^{\mathcal{A}}_{\mathsf{MPriv}}[f,\lambda,n]}$:

$\mathcal{K} \leftarrow \emptyset$
$(\mathsf{PK}_{\mathsf{Yao}} = \{\gamma\}, \mathsf{SK}_{\mathsf{Yao}} = \{\cup_{w\in\mathcal{W}}\{k^0_w, k^1_w\}\}) \leftarrow \mathsf{VCYao.KeyGen}(f,\lambda)$
$(pk_f, sk_f) \leftarrow \mathsf{MKHE.KeyGen}(1^\lambda)$
$(\mathsf{PK},\mathsf{SK}) \leftarrow (\{\mathsf{MKHE.Enc}(pk_f,\gamma)\}, \mathsf{SK}_{\mathsf{Yao}} \cup \{sk_f\})$
$(\{x^0_i\}^{i=1}_n, \{x^1_i\}^{i=1}_n) \leftarrow \mathcal{A}^{O^{\mathsf{MPubProbGen}}(\mathcal{K},\mathsf{SK}_{\mathsf{Yao}},pk_f,\lambda,\cdot), O^{\mathsf{PartDec}}(\mathcal{K},pk_f,\cdot,\cdot)}(\mathsf{PK})$
$b \xleftarrow{\$} \{0,1\}$
for $i \in \{1,\ldots,n\}$
  $\sigma_{x^b_i}, \tau_{x^b_i} \leftarrow \mathsf{VCYao.ProbGen}_{\mathsf{SK}_{\mathsf{Yao}}}(x^b_i)$
  $(pk_i, sk_i) \leftarrow \mathsf{MKHE.KeyGen}(1^\lambda)$
  $\{\sigma_{x^b_i}\}_{pk_i} \leftarrow \mathsf{MKHE.Enc}(pk_i, x^b_i)$
  $\{\sigma_{x^b_i}\}_{pk_f,pk_i} \leftarrow \{\sigma_{x^b_i}\}_{pk_i} \cdot \mathsf{MKHE.Enc}(pk_f, 1)$
$\hat{b} \leftarrow \mathcal{A}^{O^{\mathsf{MPubProbGen}}(\mathcal{K},\mathsf{SK}_{\mathsf{Yao}},pk_f,\cdot), O^{\mathsf{PartDec}}(\mathcal{K},pk_f,\cdot,\cdot)}(\mathsf{PK}, \{\{\sigma_{x^b_i}\}_{pk_f,pk_i}\}^{i=1}_n)$
Output 1 if $b = \hat{b}$ else 0

Oracle $O^{\mathsf{MPubProbGen}}(\underline{\mathcal{K}, \mathsf{SK}_{\mathsf{Yao}}, pk_f}, \lambda, x)$:

$(pk, sk) \leftarrow \mathsf{MKHE.KeyGen}(1^\lambda)$
$\sigma_x, \tau_x \leftarrow \mathsf{VCYao.ProbGen}_{\mathsf{SK}_{\mathsf{Yao}}}(x)$
$\{\sigma_x\}_{pk} \leftarrow \mathsf{MKHE.Enc}(pk, x)$
$\{\sigma_x\}_{pk_f,pk} \leftarrow \{\sigma_x\}_{pk} \cdot \mathsf{MKHE.Enc}(pk_f, 1)$
$\mathcal{K} \leftarrow \mathcal{K} \cup \{(pk, sk)\}$
Output $\{\sigma_x\}_{pk_f,pk}$

Oracle $O^{\mathsf{PartDec}}(\underline{\mathcal{K}, pk_f}, \psi, pk)$:

if $pk \neq pk_f$
  Retreive (pk, sk) from $\mathcal{K}$
  Return $\mathsf{MKHE.PartDec}(sk, \psi)$
else
  Return $\perp$

Figure 7: Experiment for the *privacy* of RMC-PVC. Parameters provided by the challenger to the oracles are underlined

Proof. For the sake of contradiction, assume a PPT adversary $\mathcal{A}$ able to break the $\mathsf{Exp}^{\mathcal{A}}_{\mathsf{MPriv}}$ (presented in Fig. ??) with a non-negligible advantage ε. Hence:

$$\mathsf{Adv}^{\mathsf{MPriv}}_{\mathcal{A}}[f,\lambda,n] = \varepsilon + \mathsf{negl}(\lambda)$$

Consider the game $\mathsf{Exp}^{\mathcal{B}}_{\mathsf{Priv}}[\mathsf{VCYao}, f, \lambda]$ (the instantiation of $\mathsf{Exp}^{\mathcal{A}}_{\mathsf{Priv}}[\mathsf{VC}, f, \lambda]$ for garbled circuits) challenging an adversary $\mathcal{B}$ to break the privacy of the Yao's garbled circuits scheme. We want to prove that given the non-negligible advantage ε of $\mathcal{A}$ to win at game $\mathsf{Exp}^{\mathcal{A}}_{\mathsf{MPriv}}$, we can create the adversary $\mathcal{B}$ able to win at game $\mathsf{Exp}^{\mathcal{B}}_{\mathsf{Priv}}[\mathsf{VCYao}, f, \lambda]$ with same advantage ε. By C, we denote the challenger which simulates the game $\mathsf{Exp}^{\mathcal{B}}_{\mathsf{Priv}}[\mathsf{VCYao}, f, \lambda]$ against the adversary $\mathcal{B}$. The reduction works as follows:

- The challenger C generates $(\mathsf{PK}_{\mathsf{Yao}}, \mathsf{SK}_{\mathsf{Yao}}) \leftarrow \mathsf{VCYao.KeyGen}(\lambda)$, where $\mathsf{PK}_{\mathsf{Yao}}$ contains the garbled circuit γ. In parallel, $\mathcal{B}$ generates a new MKHE key pair $(pk_f, sk_f) \leftarrow \mathsf{MKHE.KeyGen}(1^\lambda)$ and computes $\mathsf{PK} \leftarrow \mathsf{MKHE.Enc}(\gamma, pk_f)$.
- The adversary $\mathcal{A}$ (playing against $\mathcal{B}$ which simulates the game $\mathsf{Exp}^{\mathcal{A}}_{\mathsf{MPriv}}$) sends to $\mathcal{B}$ two distinct inputs $\{x^0_i\}^{i=1}_n$ and $\{x^1_i\}^{i=1}_n$.
- $\mathcal{B}$ sent to the challenger C the concatened inputs $x_0 = x^0_1\|\ldots\|x^0_n$ and $x_1 = x^1_1\|\ldots\|x^1_n$.
- C chooses a random bit b and sends the encoding of x_b denoted $(\sigma_{x_b}, \tau_{x_b}) \leftarrow \mathsf{VCYao.ProbGen}_{\mathsf{SK}}(x_b)$ to $\mathcal{B}$.
- $\mathcal{B}$ splits the concatened encoded inputs σ_{x_b} into the n-sized set $\{\sigma_{x^b_i}\}^{i=1}_n$.
- At each index $i \in (1,\ldots,n)$, $\mathcal{B}$ generates a new MKHE key pair $(pk_i, sk_i) \leftarrow \mathsf{MKHE.KeyGen}(1^\lambda)$. $\mathcal{B}$ encrypts the encoding σ_{x_i} with the public encryption key pk_i, producing the ciphertext denoted $\{\sigma_{x^b_i}\}_{pk_i} \leftarrow \mathsf{MKHE.Enc}(\sigma_{x^b_i}, pk_i)$. In order to integrate the public encryption key pk_f in the ciphertext, $\mathcal{B}$ multiplies the encryption of the encoding $\sigma_{x^b_i}$ with the bit 1 encrypted under pk_f, denoted as $\{\sigma_{x^b_i}\}_{pk_f,pk_i} \leftarrow \{\sigma_{x^b_i}\}_{pk_i} \cdot \mathsf{MKHE.Enc}(pk_f, 1)$.
- Once every part of the input encoded and encrypted, the adversary $\mathcal{B}$ provides to the adversary $\mathcal{A}$ every encrypted encoded inputs $\{\{x^b_i\}_{pk_f,pk_i}\}^{i=1}_n$. The adversary $\mathcal{A}$ responds with the prediction bit $\hat{b}$, forwarded by $\mathcal{B}$ to C as the prediction for the game $\mathsf{Exp}^{\mathcal{B}}_{\mathsf{Priv}}[\mathsf{VCYao}, f, \lambda]$.

The advantage of $\mathcal{B}$ to predict correctly the bit b chosen by the challenger C depends only on the prediction $\hat{b}$ of $\mathcal{A}$. Therefore, the advantage of $\mathcal{B}$ to predict correctly b is equals to the advantage of $\mathcal{A}$ to have a valid prediction $\hat{b}$. Hence, we conclude that given the non-negligible advantage ε to win at $\mathsf{Exp}^{\mathcal{A}}_{\mathsf{MPriv}}$, then the adversary $\mathcal{B}$ has a non-negligible advantage ε to win at game $\mathsf{Exp}^{\mathcal{B}}_{\mathsf{Priv}}[\mathsf{VCYao}, f, \lambda]$, leading to equation $\Pr\left[\mathsf{Exp}^{\mathcal{B}}_{\mathsf{Priv}}[\mathsf{VCYao}, f, \lambda] = 1\right] = \varepsilon + \mathsf{negl}(\lambda)$. However, VCYao is a private verifiable-computation scheme as shown in [Lindell and Pinkas 2008]. Thus, there is no PPT adversary to break the privacy of VCYao *i.e.,* to have a non-negligible advantage to win at game $\mathsf{Exp}^{\mathcal{B}}_{\mathsf{Priv}}[\mathsf{VCYao}, f, \lambda]$. □

4.3 Security

The security property ensures that the server cannot manage to return an invalid result accepted by the clients. To produce an invalid result with garbled circuits, the server should return a computation where at least one output label k^b_w as been replaced by k^{1-b}_w for some wire $w \in \mathcal{W}$. Nevertheless, the server has only a negligible probability to recover the label k^{1-b}_w, at the condition that the garbled circuit is executed *only one time*. Otherwise, the next executions could return the other label k^{1-b}_w, letting the server to cheat without being detected.

In RMC-PVC, the garbled circuit can be used an arbitrary number of times, thanks to the MKHE scheme. Indeed, at each new execution of the garbled circuit, a fresh MKHE key pair is generated by clients. The server cannot reuse the labels from previous executions since the keys differs between each execution.

We formalize the security property of RMC-PVC by introducing the game $\mathsf{Exp}^{\mathcal{A}}_{\mathsf{MSec}}$ presented in Fig. ??, working as follows: the challenger expects from the adversary to generate an input $\{x_i\}_{i=1}^n$ where n denotes the number of clients. The adversary also provides the encryption of the (possibly invalid) encoded result computed by the adversary $\{\sigma_{\hat{y}}\}_{pk_f \cup \{pk_i\}_{i=1}^n}$, as well as $\{\mathsf{Part}_i(\sigma_{\hat{y}})\}_{i=1}^n$ the set of partial decryptions associated with the encrypted encoded result. The challenger computes $\mathsf{Part}_f(\sigma_{\hat{y}})$ the partial decryption obtained using the secret key sk_f. The challenger merges partial decryptions to obtain $\sigma_{\hat{y}}$ the encoded result, which is then verified by the challenger. The adversary wins at the game $\mathsf{Exp}^{\mathcal{A}}_{\mathsf{MSec}}$ if the provided encoded result is accepted, but in the same time does not correspond to a valid evaluation of the function f over the inputs $\{x_i\}_{i=1}^n$. Until his answer to the challenger, the adversary has access a polynomial number of times to two oracles $\mathcal{O}^{\mathsf{MPubProbGen}}$ and $\mathcal{O}^{\mathsf{PartDec}}$ presented in Fig. 5.

Theorem 4.3 (Security). *Suppose* Sym *a Yao-Secure symmetric encryption scheme and* MKHE *a correct semantically secure homomorphic encryption scheme with distributed decryption property. Suppose a security parameter $\lambda$and a number of clients n. Then for every PPT adversary $\mathcal{A}$ playing against* $\mathsf{Exp}^{\mathcal{A}}_{\mathsf{MSec}}$*:*

$$\mathsf{Adv}^{\mathsf{MSec}}_{\mathcal{A}}[f, \lambda, n] = \Pr[\mathsf{Exp}^{\mathcal{A}}_{\mathsf{MSec}}[f, \lambda, n] = 1] \leq \mathsf{negl}(\lambda)$$

Sketch of the proof. We want to prove that there is no PPT adversary $\mathcal{A}$ able to break the security property of our protocol. More precisely, we want to show that there is no adversary $\mathcal{A}$ able to win at game $\mathsf{Exp}^{\mathcal{A}}_{\mathsf{MSec}}$ with a non-negligible advantage. To prove the non-existence of a such adversary, we consider an hybrid argument where the initial game is $\mathsf{Exp}^{\mathcal{A}}_{\mathsf{MSec}}$ and the target game denoted H_p with $p = \mathrm{Card}(\mathcal{G})$ and $\mathcal{G}$ the gates composing the boolean circuit of the function f, is the same as $\mathsf{Exp}^{\mathcal{A}}_{\mathsf{MSec}}$, except that the adversary $\mathcal{A}$ is mandatory to cheat with a negligible advantage. In details, at each game, we replace one gate by a fake gate returning only one label, whathever the inputs. In the final game, each gate of the garbled circuit contains only label k_w^b amongst labels $\{k_w^b, k_w^{1_b}\}$ is present for each wire $w \in \mathcal{W}$. To win at the game $\mathsf{Exp}^{\mathcal{A}}_{\mathsf{MSec}}$, the adversary $\mathcal{A}$ must replace a valid output label k_w^b with label k_w^{1-b} for a wire $w \in \mathcal{W}_{\mathrm{out}}$ of this choice. However, $\mathcal{A}$ knows k_w^b only and the garbled circuit does *not* contains any occurence (even encryptions) of the other label k_w^{1-b}. Hence, $\mathcal{A}$ is able to predict the label k_w^{1-b} only with the probability $\frac{1}{2^\lambda}$ since a label is a key parameterized by the security parameter λ.

Proof. Consider H_0 the game working exactly as the same as $\mathsf{Exp}^{\mathcal{A}}_{\mathsf{MSec}}$. Let $\mathsf{Fake}(\gamma_g) \to \gamma'_g$ the function with for a gabled table γ_g, returns the fake gate γ'_g outputting only the bit 0 whatever the provided inputs. For k ranging from 0 to $p = \mathrm{Card}(\mathcal{G})$, the game H_k differ from H_{k-1} with the gate g_k which is replaced by a fake gate $\mathsf{Fake}(g_k)$. Therefore, the fake gate $\mathsf{Fake}(g_k)$ contains only one output label representing the bit 0. We show that H_{k-1} and H_k are computationally indishtinguishable.

For the sake of contradiction, let assume an adversary $\mathcal{A}$ able to dishtinguish between the game H_{k-1} and H_k. From $\mathcal{A}$, we construct an adversary $\mathcal{B}$ able to break the indishtinguishability of the MKHE scheme, expressed in Figure 5. The idea behind the reduction is to challenge $\mathcal{A}$ to predict if is playing at game H_{k-1} or H_k. Let C the challenger for the $\mathsf{Exp}_{\mathsf{MKICDD}}$ game. The reduction works as follows:

- $\mathcal{B}$ generates a garbled circuit where the $k-1$ first gates are replaced by faked ones, denoted by $\gamma_0 = \{\mathsf{Fake}(\gamma_{g_i}) | g_i \in \mathcal{G}, i < k\} \cup \{\gamma_{g_i} | g_i \in \mathcal{G}, i \geq k\}$.
- The challenger C generates a MKHE key pair (pk_f, sk_f).
- From γ_0, $\mathcal{B}$ derive the garbled circuit where the k first gates are replaced by faked ones, denoted by $\gamma_1 = \{\mathsf{Fake}(\gamma_{g_i}) | g_i \in \mathcal{G}, i \leq k\} \cup \{\gamma_{g_i} | g_i \in \mathcal{G}, i > k\}$.
- $\mathcal{B}$ asks to the challenger C to encrypt $\{\mathsf{Fake}(\gamma_{g_i}) | g_i \in \mathcal{G}, i < k\}$ and $\{\gamma_{g_i} | g_i \in \mathcal{G}, i > k\}$, in order to obtain $\{\{\mathsf{Fake}(\gamma_{g_i})\}_{pk_f} | g_i \in \mathcal{G}, i < k\}$ and $\{\{\gamma_{g_i}\}_{pk_f} | g_i \in \mathcal{G}, i > k\}$.
- $\mathcal{B}$ sends to the challenger C two messages $m_0 = \gamma_{g_k}$ and $m_1 = \mathsf{Fake}(\gamma_{g_k})$, which responds with the encryption of m_b for a chosen bit $b \in \{0,1\}$, denoted $\{m_b\}_{pk_f}$.
- The adversary $\mathcal{B}$ constructs the encrypted garbled circuit as follows: $\{\gamma_b\}_{pk_f} = \{\{\mathsf{Fake}(\gamma_{g_i})\}_{pk_f} | g_i \in \mathcal{G}, i < k\} \cup \{m_b\}_{pk_f} \cup \{\{\gamma_{g_i}\}_{pk_f} | g_i \in \mathcal{G}, i > k\}$
- $\mathcal{B}$ provides $\{\gamma_b\}_{pk_f}$ to the adversary $\mathcal{A}$, which responds with the prediction bit $\hat{b} \in \{0,1\}$, equals to 0 if $\mathcal{A}$ predicts that he is challenged at game H_{k-1}, and 1 for the game H_k.
- $\mathcal{B}$ forward the bit $\hat{b}$ to C the challenger C.

The advantage of $\mathcal{A}$ to distinguish between H_{k-1} and H_k highly depends on the gate g. Indeed, if the gate always produce the same label (before to be faked), therefore the adversary cannot distinguish. This situation when the gate g always outputs the bit 0 or the bit 1 occurs with a probability $\frac{2}{2^4}$ (since we consider a gate taking two inputs). Hence, the adversary $\mathcal{A}$ is able to distinguish between H_{k-1} and H_k only where the original gate g outputs both bit 0 and 1, which occurs with probability $1 - \frac{2}{2^4} = \frac{7}{8}$. By hypothesis, $\mathcal{A}$ has a non-negligible probability α to distinguish between H_{k-1} and H_k. We provide the probability of $\mathcal{B}$ to break the indishtinguishability of $\mathsf{Exp}_{\mathsf{MKICDD}}$ is $\Pr\left[\mathsf{Exp}^{\mathcal{B}}_{\mathsf{MKICDD}}[\mathsf{MKHE}, \lambda] = 1\right] = \frac{7}{8}\alpha$. We can conclude this reduction by saying that if an adversary $\mathcal{A}$ is able to distinguish between games H_{k-1} and H_k, then we can construct an adversary $\mathcal{B}$ able to win with a non-negligible probability at MKICDD game for the MKHE scheme. Hence, H_{k-1} and H_k are computionnally indishtinguishable.

At the end of the hybrid argument, we obtain the game H_p for $p = |\mathcal{G}|$ which corresponds to the game where the adversary $\mathcal{A}$ has no advantage and must predict the output label k_w^{1-b} randomly. By induction, we have shown that the game H_0 is is dishtinguishable from the game H_p with a probability $|\Pr[\mathsf{Exp}^{\mathcal{A}}_{\mathsf{H}_0} = 1]| = |\mathsf{Exp}^{\mathcal{A}}_{\mathsf{H}_p} = 1]| + (\frac{7}{8}\alpha)p$. By contradiction, we know that α is negligible. Then, we can rewrite the equation as $|\Pr[\mathsf{Exp}^{\mathcal{A}}_{\mathsf{MSec}} = 1]| = |\mathsf{Exp}^{\mathcal{A}}_{\mathsf{H}_p} = 1]| + \mathsf{negl}(\lambda)$. Since $|\mathsf{Exp}^{\mathcal{A}}_{\mathsf{H}_p} = 1]|$ is negligible, then we can conclude that $|\Pr[\mathsf{Exp}^{\mathcal{A}}_{\mathsf{MSec}} = 1]|$ is negligible. ◻

Game $\mathsf{Exp}^{\mathcal{A}}_{\mathsf{MSec}}[f, \lambda, n]$:

$\mathcal{K} \leftarrow \emptyset$
$(\mathsf{PK}_{\mathsf{Yao}} = \{\gamma\}, \mathsf{SK}_{\mathsf{Yao}} = \{\cup_{w \in \mathcal{W}}\{k^0_w, k^1_w\}\}) \leftarrow \mathsf{VCYao.KeyGen}(f, \lambda)$
$(pk_f, sk_f) \leftarrow \mathsf{MKHE.KeyGen}(^{\lambda})$
$(\mathsf{PK}, \mathsf{SK}) \leftarrow (\{\mathsf{MKHE.Enc}(pk_f, \gamma)\}, \mathsf{SK}_{\mathsf{Yao}} \cup \{sk_f\})$
$\{x_i\}^n_{i=1}, \{\sigma_{\hat{y}}\}_{pk_f \cup \{pk_i\}^n_{i=1}}, \{\mathsf{Part}_i(\sigma_{\hat{y}})\}^n_{i=1} \leftarrow$
$\quad \mathcal{A}^{\mathcal{O}^{\mathsf{MPubProbGen}}(\mathcal{K}, \mathsf{SK}_{\mathsf{Yao}}, pk_f, \lambda, \cdot), \mathcal{O}^{\mathsf{PartDec}}(\mathcal{K}, pk_f, \cdot, \cdot)}(\mathsf{PK})$
$\mathsf{Part}_f(\sigma_{\hat{y}}) \leftarrow \mathsf{MKHE.PartDec}(\{\sigma_{\hat{y}}\}_{pk_f \cup \{pk_i\}^n_{i=1}}, sk_f)$
$\sigma_{\hat{y}} \leftarrow \mathsf{MKHE.Merge}(\mathsf{Part}_f(\sigma_{\hat{y}}), \{\mathsf{Part}_i(\sigma_{\hat{y}})\}^n_{i=1})$
$\hat{y} \leftarrow \mathsf{VCYao.Verify}_{\mathsf{SK}_{\mathsf{Yao}}}(\sigma_{\hat{y}})$

Output 1 if $\hat{y} \neq \bot \bigwedge \hat{y} \neq f(\{x_i\}^n_{i=1})$ else 0

Figure 8: Experiment $\mathsf{Exp}^{\mathcal{A}}_{\mathsf{MSec}}$ for *security* property of RMC-PVC.

5 COMPLEXITY ANALYSIS OF RMC-PVC

We study the asymptotic execution time of RMC-PVC. Consider an arbitrary boolean circuit f represented by $(\mathcal{G}, \mathcal{W}, \mathcal{W}_{\text{in}}, \mathcal{W}_{\text{out}})$ where $\mathcal{G}$ is the set of gates, $\mathcal{W}$ the set of wires, $\mathcal{W}_{\text{in}}$ the set of input wires and $\mathcal{W}_{\text{out}}$ the set of output wires.

Step (1). During step (1), each client encodes and encrypts his input. We recall the considered function f is expected to be a boolean circuit, having $\mathcal{W}_{\text{in}}$ input bits, the step (1) requires a $O(O(\mathcal{W}_{\text{in}}) \times O(\mathsf{MKHE.Enc}))$ complexity.

Step (2). In this step, the server evaluates the function f using the encrypted garbled circuits $\{\gamma\}_{pk_f}$, over the encrypted encoded inputs $\{\{\sigma_{x_i}\}_{pk_f, pk_{x_i}}\}^{i=1}_n$ sent by clients. The server executes the boolean circuit gate by gate as described in Section 3 until to get $\{\sigma_y\}_{pk_f, pk_{x_1}, \ldots, pk_{x_n}}$. The server evaluates gate after gate from the input to the output of the boolean circuits. At each gate, the server must executed the circuit Γ in order to obtain the label for the next gate. Hence, the server requires a $O(|\mathcal{G}| \times O(\Gamma))$ complexity. We can refine the $O(\Gamma)$ complexity, since Γ tries to decrypt a ciphertext (produced by the Sym scheme) among γ_g containing 2^i inputs where i is the number of inputs of each gate. Since we consider gates with two input wires, then i is equals to 2, leading to get four ciphertexts in γ_g. For each ciphertext, Γ executes the decryption algorithm Sym.Dec twice, with the two provided labels. At most, there is four decryptions using Sym.Dec, leading to the complexity of $O(|\mathcal{G}| \times 8O(\mathsf{Sym.Dec}))$.

Step (3). In this step, each client C_i computes $\mathsf{Part}_i(\sigma_y)$ the partial decryption of the ciphertext. Clearly, the complexity of this step depends of the complexity of the MKHE.PartDec function, leading to the complexity $O(\mathsf{MKHE.PartDec})$.

Step (4). During this step, the server is in charge to broadcast the partial decryptions to all clients. Only communications are required in this step: the server receives the partial decryptions provided by each client, creates a set of received partial decryptions then sent to every clients. Therefore, the complexity is constant.

Step (5). Each client starts by computing the partial decryption $\mathsf{Part}_f(\sigma_y)$. Given this last partial decryption, each client computes the result using the function MKHE.Merge, which is verified with VCYao.Verify working in a constant time. Hence, we obtain $O(O(\mathsf{MKHE.PartDec}) + O(\mathsf{MKHE.Merge}) + |\mathcal{W}_{\text{out}}|)$.

Compared to the closest work of this paper [Gennaro et al. 2010], a client performs the same operations to encode his input *i.e.,* $O(|\mathcal{W}_{\text{in}}|) \times O(\mathsf{MKHE.Enc})$. Still on the client side, the result decryption differs from [Gennaro et al. 2010] since we rely on the distributed decryption. In their protocol a client is able to verify the result in $|\mathcal{W}_{\text{out}}|O(\mathsf{FHE.Dec})$ operations whereas we requires $|\mathcal{W}_{\text{out}}|(O(\mathsf{MKHE.PartDec}) + O(\mathsf{MKHE.Merge}))$ operations. On the other side, the server requires $|\mathcal{G}|O(\mathsf{Sym.Dec})$ operations for the function evaluation which is stricly less than $|\mathcal{G}|O(\mathsf{Sym.Dec} + \mathsf{FHE.Enc})$ obtained in [Gennaro et al. 2010]. Hence, the function evaluation in our protocol requires $|\mathcal{G}|\mathsf{FHE.Enc}$ operations.

6 CONCLUSION

In RMC-PVC, each client can verify the correctness of the evaluation performed by the server, thanks to the partial decryption property. We proved that RMC-PVC is *correct.* More importantly, we proved that RMC-PVC is *private* in the sense that the server as well as the other clients cannot learn a clinet's input. RMC-PVC is *secure* meaning that the server cannot produce an invalid result accepted by the cients. Finally, we study the complexity of our protocol and shows that a client outsoucing computations performs less computations compared to the case where the function is computed locally.

In future, we plan to prepare an open-source implementation of this protocol, proving the effectiveness we have claimed in this paper. Moreover, developping a protocol secure even with verification queries and against server-clients collusions will be an intersting way of improvements.

REFERENCES

2022. RMC-PVC: A Multi-Client Reusable Verifiable Computation Protocol (Long version). https://github.com/anonymized-submissions/verifiable-computation-mkhe-gc.

Alexandre Bois, Ignacio Cascudo, Dario Fiore, and Dongwoo Kim. 2021. Flexible and Efficient Verifiable Computation on Encrypted Data. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* 12711 LNCS (2021), 528–558. https://doi.org/10.1007/978-3-030-75248-4_19/COVER

Hao Chen, Wei Dai, Miran Kim, and Yongsoo Song. 2019. Efficient Multi-Key Homomorphic Encryption with Packed Ciphertexts with Application to Oblivious Neural Network Inference. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security* (London, United Kingdom) *(CCS '19)*. Association for Computing Machinery, New York, NY, USA, 395–412. https://doi.org/10.1145/3319535.3363207

Long Chen, Zhenfeng Zhang, and Xueqing Wang. 2017. Batched Multi-hop Multi-key FHE from Ring-LWE with Compact Ciphertext Extension. In *Theory of Cryptography*, Yael Kalai and Leonid Reyzin (Eds.). Springer International Publishing, Cham, 597–627.

Seung Geol Choi, Jonathan Katz, Ranjit Kumaresan, and Carlos Cid. 2013. Multi-Client Non-interactive Verifiable Computation. In *Theory of Cryptography*, Amit Sahai (Ed.). Springer Berlin Heidelberg, Berlin, Heidelberg, 499–518.

Dario Fiore, Anca Nitulescu, and David Pointcheval. 2020. Boosting Verifiable Computation on Encrypted Data. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* 12111 LNCS (2020), 124–154. https://doi.org/10.1007/978-3-030-45388-6_5

Rosario Gennaro, Craig Gentry, and Bryan Parno. 2010. Non-interactive Verifiable Computing: Outsourcing Computation to Untrusted Workers. In *Advances in Cryptology – CRYPTO 2010*, Tal Rabin (Ed.). Springer Berlin Heidelberg, Berlin, Heidelberg, 465–482.

Craig Gentry. 2009. Fully Homomorphic Encryption Using Ideal Lattices. In *Proceedings of the Forty-First Annual ACM Symposium on Theory of Computing* (Bethesda, MD, USA) *(STOC '09)*. Association for Computing Machinery, New York, NY, USA, 169–178. https://doi.org/10.1145/1536414.1536440

Shafi Goldwasser, S. Dov Gordon, Vipul Goyal, Abhishek Jain, Jonathan Katz, Feng-Hao Liu, Amit Sahai, Elaine Shi, and Hong-Sheng Zhou. 2014. Multi-input Functional Encryption. In *33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques* (33rd annual international conference on the theory and applications of cryptographic techniques ed.). Springer Berlin Heidelberg, 578–602. https://www.microsoft.com/en-us/research/publication/multi-input-functional-encryption/

Shafi Goldwasser, Yael Tauman Kalai, and Raluca Ada Popa. 2013. Reusable Garbled Circuits and Succinct Functional Encryption. In *In Proceedings of the 45th annual ACM symposium on Theory of computing (STOC)* (in proceedings of the 45th annual acm symposium on theory of computing (stoc) ed.). ACM. https://www.microsoft.com/en-us/research/publication/reusable-garbled-circuits-succinct-functional-encryption/

Shafi Goldwasser, Yael Tauman Kalai, and Guy N. Rothblum. 2015. Delegating Computation: Interactive Proofs for Muggles. *J. ACM* 62, 4, Article 27 (sep 2015), 64 pages. https://doi.org/10.1145/2699436

Yan Huang, Jonathan Katz, Vladimir Kolesnikov, Ranjit Kumaresan, and Alex J. Malozemoff. 2014. Amortizing garbled circuits. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* 8617 LNCS. Issue PART 2. https://doi.org/10.1007/978-3-662-44381-1_26

Seny Kamara, Payman Mohassel, and Mariana Raykova. 2011. Outsourcing Multi-Party Computation. *IACR Cryptol. ePrint Arch.* 2011 (2011), 272.

Pascal Lafourcade, Gael Marcadet, and Léo Robert. 2022. Faster Non-interactive Verifiable Computing. Cryptology ePrint Archive, Paper 2022/646. https://eprint.iacr.org/2022/646 https://eprint.iacr.org/2022/646.

Yehuda Lindell and Benny Pinkas. 2008. A Proof of Security of Yao's Protocol for Two-Party Computation. *Journal of Cryptology* 22 (2008), 161–188.

Yehuda Lindell and Benny Pinkas. 2015. An Efficient Protocol for Secure Two-Party Computation in the Presence of Malicious Adversaries. *Journal of Cryptology* 28 (2015). Issue 2. https://doi.org/10.1007/s00145-014-9177-x

Silvio Micali. 2000. Computationally Sound Proofs. *SIAM J. Comput.* 30, 4 (oct 2000), 1253–1298. https://doi.org/10.1137/S0097539795284959

Andrew Chi-Chih Yao. 1986. How to generate and exchange secrets. In *27th Annual Symposium on Foundations of Computer Science (sfcs 1986)*. 162–167. https://doi.org/10.1109/SFCS.1986.25