Universally Verifiable Multiparty Computation from Threshold Homomorphic Cryptosystems

Berry Schoenmakers and Meilof Veeningen(✉)

Department of Mathematics and Computer Science, TU Eindhoven,
Eindhoven, The Netherlands
berry@win.tue.nl, m.veeningen@tue.nl

Abstract. Multiparty computation can be used for privacy-friendly outsourcing of computations on private inputs of multiple parties. A computation is outsourced to several computation parties; if not too many are corrupted (e.g., no more than half), then they cannot determine the inputs or produce an incorrect output. However, in many cases, these guarantees are not enough: we need correctness even if *all* computation parties may be corrupted; and we need that correctness can be verified even by parties that did not participate in the computation. Protocols satisfying these additional properties are called "universally verifiable". In this paper, we propose a new security model for universally verifiable multiparty computation, and we present a practical construction, based on a threshold homomorphic cryptosystem. We also develop a multiparty protocol for jointly producing non-interactive zero-knowledge proofs, which may be of independent interest.

1 Introduction

Multiparty computation (MPC) provides techniques for privacy-friendly outsourcing of computations. Intuitively, MPC aims to provide a cryptographic "black box" which receives private inputs from multiple "input parties"; performs a computation on these inputs; and provides the result to a "result party" (an input party, any third party, or the public). This black box is implemented by distributing the computation between multiple "computation parties", with privacy and correctness being guaranteed in case of passive corruptions (e.g., [BCD+09]), active corruption of a minority of computation parties (e.g., [CDN01]), or active corruption of all-but-one computation parties (e.g., [DPSZ12]).

However, multiparty computation typically does *not* provide any guarantees in case all computation parties are corrupted. That is, the result party has to trust that at least some of the computation parties did their job, and has no way of independently verifying the result. In particular, the result party has no way of proving to an external party that his computation result is indeed correct. *Universally verifiable* multiparty computation addresses these issues by requiring that the correctness of the result can be verified by any party, even if all computation parties are corrupt [dH12]. It was originally introduced in the context of e-voting [CF85,SK95], but it is relevant whenever MPC is applied in a setting where not all of the parties that provide inputs or obtain outputs are

T. Malkin et al. (Eds.): ACNS 2015, LNCS 9092, pp. 3–22, 2015.
DOI: 10.1007/978-3-319-28166-7_1

participants in the computation. In particular, apart from contexts like e-voting where "the public" or an external watchdog wants to be sure of correctness, it is also useful in scenarios where (many) different input parties outsource a computation to the cloud and require a correctness guarantee.

Unfortunately, the state-of-the-art on universally verifiable MPC is unsatisfactory. The concept of universally verifiable MPC was first proposed in [dH12], where it was also suggested that it can be achieved for MPC based on threshold homomorphic cryptosystems. However, [dH12] does not provide a rigorous security model for universal verifiability or analysis of the proposed construction; and the construction has some technical disadvantages (e.g., a proof size depending on the number of computation parties). The scheme recently proposed in [BDO14] solves part of the problem. Their protocols provide "public auditability", meaning that anybody can verify the result of a computation, but *only* if that result is public. In particular, it is not possible for a result party to prove just that an encryption of the result is correct, which is important if this result is to be used in a later protocol without being revealed.

In this paper, we propose a new security model for universally verifiable multiparty computation, and a practical construction achieving it. As in [dH12], we adapt the well-known actively secure MPC protocols based on threshold homomorphic cryptosystems from [CDN01,DN03]. Essentially, these protocols perform computations on encrypted values; security against active adversaries is achieved by letting parties prove correctness of their actions using interactive zero-knowledge proofs. Such interactive proofs only convince parties present at the computation; but making them non-interactive makes them convincing also to external parties. Concretely, the result of a computation is a set of encryptions of the inputs, intermediate values, and outputs of the computation, along with non-interactive zero-knowledge proofs of their correctness. Correctness of the result depends just on the correct set-up of the cryptosystem. Privacy holds under the original conditions of [CDN01], i.e., if under half of the computation parties are corrupted; but as we discuss, this threshold can be raised to $n-1$ at the expense of sacrificing robustness. (Note that when computing with encryptions, we cannot hope to achieve privacy if all computation parties are corrupted: this would essentially require fully homomorphic encryption.)

We improve on [dH12] in two main ways. First, we provide a security model for universal verifiability (in the random oracle model), and security proofs for our protocols in that model. Second, we propose a new "multiparty" variant of the Fiat-Shamir heuristic to make the zero-knowledge proofs non-interactive, which may be of independent interest. Compared to [dH12], it eliminates the need for trapdoor commitments. Moreover, it makes the proof size independent of the number of parties performing the computation. We achieve this latter advantage by homomorphically combining contributions from the different parties.

As such, universally verifiable MPC provides a practical alternative to recent (single-party) techniques for verifiable outsourcing. Specifically, many papers on verifiable computation focus on efficient verification, but do not cover privacy [PHGR13,WB13]. Those works that do provide privacy, achieve this by combining costly primitives, e.g., fully homomorphic encryption with verifiable

$a \in_R S$	sample a uniformly at random from S
$\mathsf{send}(v;\mathcal{P}), \mathsf{recv}(\mathcal{P})$	send v to/receive from $\mathcal{P}$ over secure channel
$\mathsf{bcast}(v)$	exchange v over broadcast channel
party $\mathcal{P}$ **do** S	let party $\mathcal{P}$ perform S; other parties do nothing
parties $i \in \mathcal{Q}$ **do** S	let parties $i \in \mathcal{Q}$ perform S in parallel
$\mathcal{H} : \{0,1\}^* \to \{0,1\}^{2l}$	cryptographic hash function (l security parameter)
$F \subset \mathcal{I} \cup \mathcal{P} \cup \{\mathcal{R}, \mathcal{V}\}$	global variable: set of parties found to misbehave
$\mathsf{paillierdecode}(x)$	threshold Paillier decoding (p. 6): $((x-1) \div N)(4\Delta^2)^{-1} \bmod N$
$\mathsf{fsprove}(\Sigma; v; w; aux)$	Fiat-Shamir proof (p. 8): $(a, s) := \Sigma.\mathsf{ann}(v, w)$; $c := \mathcal{H}(v \vert\vert a \vert\vert aux); r := \Sigma.\mathsf{res}(v, w, a, s, c); \pi := (a, c, r)$
$\mathsf{fsver}(\Sigma; v; a, c, r; aux)$	verification of Fiat-Shamir Σ-proof (p. 8): $\mathcal{H}(v \vert\vert a \vert\vert aux) = c \wedge \Sigma.\mathsf{ver}(v; a; c; r)$

Fig. 1. Notation in algorithms, protocols, and processes

computation [FGP14]; or functional encryption with garbled circuits [GKP+13]. A recent work [ACG+14] also considers the possibility of achieving verifiable computation with privacy by distributing the computation; but it does not guarantee correctness if all computation parties are corrupted, nor does it allow third parties to be convinced of this fact. In contrast, our methods guarantee correctness even if all computation parties are corrupted, and even convince other parties than the input party. In particular, any third party can be convinced, and the computation may involve the inputs of multiple mutually distrusting input parties. Moreover, in contrast to the above works, our methods rely on basic cryptographic primitives such as Σ-protocols and the threshold homomorphic Paillier cryptosystem, readily available nowadays in cryptographic libraries like SCAPI [EFLL12].

Outline. First, we briefly recap the CDN scheme for secure computation in the presence of active adversaries from [CDN01,DN03], instantiated using Paillier encryption (Sect. 2). Then, we show how the proofs in this protocol can be made non-interactive using the Fiat-Shamir heuristic and our new multiparty variant (Sect. 3). Finally, we propose a security model for universally verifiable MPC, and show that CDN with non-interactive proofs is universally verifiable (Sect. 4). We conclude in Sect. 5. We list potentially non-obvious notation in our pseudocode in Fig. 1.

2 Secure Computation from Threshold Cryptography

We review the "CDN protocol" [CDN01] for secure computation in the presence of active adversaries based on a threshold homomorphic cryptosystem. The protocol involves m input parties $i \in \mathcal{I}$, n computation parties $i \in \mathcal{P}$, and a result party $\mathcal{R}$. The aim of the protocol is to compute a function $f(x_1, \ldots, x_m)$ (seen as an arithmetic circuit) on private inputs x_i of the input parties, such that the result party obtains the result.

2.1 Computation Using a Threshold Homomorphic Cryptosystem

The protocol uses a (t, n)-threshold homomorphic cryptosystem, with $t = \lceil n/2 \rceil$. In such a cryptosystem, anybody can encrypt a plaintext using the public key; add two ciphertexts to obtain a (uniquely determined) encryption of the sum of the corresponding plaintexts; and multiply a ciphertext by a constant to obtain a (uniquely determined) encryption of the product of the plaintext with the constant. Decryption is only possible if at least t out of the n decryption keys are known. A well-known homomorphic cryptosystem is the Paillier cryptosystem [Pai99]: here, the public key is an RSA modulus $N = pq$; $a \in \mathbb{Z}_N$ is encrypted with randomness $r \in \mathbb{Z}_N^*$ as $(1+N)^a r^N \in \mathbb{Z}_{N^2}^*$; and the product of two ciphertexts is an encryption of the sum of the two corresponding plaintexts. (From now on, we suppress moduli for readability.) A threshold variant of this cryptosystem was presented in [DJ01]. The (threshold) decryption procedure is a bit involved; we postpone its discussion until Sect. 2.2. The CDN protocol can also be instantiated with other cryptosystems; but in this paper, we will focus on the Paillier instantiation.

Computation of $f(x_1, \ldots, x_m)$ is performed in three phases: the input phase, the computation phase, and the output phase. In the input phase, each input party encrypts its input x_i, and broadcasts the encryption X_i. In the computation phase, the function f is evaluated gate-by-gate. Addition and subtraction are performed using the homomorphic property of the encryption scheme. For multiplication[1] of X and Y, each computation party $i \in \mathcal{P}$ chooses a random value d_i, and broadcasts encryptions D_i of d_i and E_i of $d_i \cdot y$. The computation parties then compute $X \cdot D_1 \cdots D_n$, and threshold decrypt it to learn $x + d_1 + \ldots + d_n$. Observe that this allows them to compute an encryption of $(x + d_1 + \ldots + d_n) \cdot y$, and hence, using the E_i, also an encryption of $x \cdot y$. Finally, in the output phase, when the result of the computation has been computed as encryption X of x, the result party obtains x by broadcasting random encryption D of d and obtaining a threshold decryption $x - d$ of $X \cdot D^{-1}$.

Active security is achieved by letting the parties prove correctness of all information they exchange. Namely, the input parties prove knowledge of their inputs X_i (this prevents parties from choosing inputs depending on other inputs). The computation parties prove knowledge of D_i, and prove that E_i is indeed a correct multiplication of D_i and Y; and they prove the correctness of their contributions to the threshold decryption of $X \cdot D_1 \cdots D_n$ and $X \cdot D^{-1}$. Finally, the result party proves knowledge of D. We now discuss these proofs of correctness and their influence on the security of the overall protocol.

2.2 Proving Correctness of Results

The techniques in the CDN protocol for proving correctness are based on Σ-protocols. Recall that a Σ-protocol for a binary relation R is a three-move protocol in which a potentially malicious prover convinces a honest verifier that he

[1] Here, we use the improved multiplication protocol from [DN03]: the multiplication protocol from [CDN01] has a subtle problem, in which the subroutine for additively sharing an encrypted value requires unknown encryption randomness to be returned.

Σ-Protocol 1. Σ_{PK}: Proof of plaintext knowledge

[Relation] $R = \{(X; x, r) \mid X = (1+N)^x r^N\}$

[Announcement] $\Sigma.\mathsf{ann}(X; x, r) :=$

$a \in_R \mathbb{Z}_N; u \in_R \mathbb{Z}_N^*; A := (1+N)^a u^N;$ **return** $(A; a, u)$

[Response] $\Sigma.\mathsf{res}(X; x, r; A; a, u; c) :=$

$t := \lfloor (a + cx)/N \rfloor; d := a + cx; e := ur^c(1+N)^t;$ **return** (d, e)

[Verification] $\Sigma.\mathsf{ver}(X; A; c; d, e) := (1+N)^d e^N \overset{?}{=} AX^c$

[Extractor] $\Sigma.\mathsf{ext}(X; A; c; c'; d, e; d', e') :=$

$\alpha, \beta :=$ "values such that $\alpha(c - c') + \beta N = 1$"; **return** $((d - d')\alpha, (e/e')^\alpha X^\beta)$

[Simulator] $\Sigma.\mathsf{sim}(X; c) :=$

$d \in_R \mathbb{Z}_N; e \in_R \mathbb{Z}_N^*; A := (1+N)^d e^N X^{-c};$ **return** $(A; c; d, e)$

knows a *witness* w for *statement* v such that $(v; w) \in R$. First, the prover sends an *announcement* (computed using algorithm $\Sigma.\mathsf{ann}$) to the verifier; the verifier responds with a uniformly random *challenge*; and the prover sends his *response* (computed using algorithm $\Sigma.\mathsf{res}$), which the verifier verifies (using predicate $\Sigma.\mathsf{ver}$). Σ-protocols satisfy the following properties:

Definition 1. *Let $R \subset V \times W$ be a binary relation and $L_R = \{v \in V \mid \exists w \in W : (v; w) \in R\}$ its language. Let Σ be a collection of p.p.t. algorithms $\Sigma.\mathsf{ann}$, $\Sigma.\mathsf{res}$, $\Sigma.\mathsf{sim}$, $\Sigma.\mathsf{ext}$, and polynomial time predicate $\Sigma.\mathsf{ver}$. Let C be a finite set called the* challenge space*. Then Σ is a* Σ-protocol *for relation R if:*

Completeness. *If $(a; s) \leftarrow \Sigma.\mathsf{ann}(v; w)$, $c \in C$, and $r \leftarrow \Sigma.\mathsf{res}(v; w; a; s; c)$, then $\Sigma.\mathsf{ver}(v; a; c; r)$.*

Special Soundness. *If $v \in V$, $c \neq c'$, $\Sigma.\mathsf{ver}(v; a; c; r)$, and $\Sigma.\mathsf{ver}(v; a; c'; r')$, then $w \leftarrow \Sigma.\mathsf{ext}(v; a; c; c'; r; r')$ satisfies $(v; w) \in R$.*

Special Honest-Verifier Zero-Knowledgeness. *If $v \in L_R$, $c \in C$, then $(a; r) \leftarrow \Sigma.\mathsf{sim}(v; c)$ has the same probability distribution as $(a; r)$ obtained by $(a; s) \leftarrow \Sigma.\mathsf{ann}(v; w)$, $r \leftarrow \Sigma.\mathsf{res}(v; w; a; s; c)$. If $v \notin L_R$, then $(a; r) \leftarrow \Sigma.\mathsf{sim}(v; c)$ satisfies $\Sigma.\mathsf{ver}(v; a; c; r)$.*

Completeness states that a protocol between a honest prover and verifier succeeds; special soundness states that there exists an extractor $\Sigma.\mathsf{ext}$ that can extract a witness from two conversations with the same announcement; and special honest-verifier zero-knowledgeness states that there exists a simulator $\Sigma.\mathsf{sim}$ that can generate conversations with the same distribution as full protocol runs without knowing the witness. While special honest-verifier zero-knowledgeness demands an identical distribution for the simulation, statistical indistinguishability is sufficient for our purposes; in this case, we speak of a "statistical Σ-protocol". In the remainder, we will need that our Σ-protocols have "non-trivial announcements", in the sense that when $(a; r)$ and $(a'; r')$ are both obtained from $\Sigma.\mathsf{sim}(v; c)$, then with overwhelming probability, $a \neq a'$. (Indeed, this will be the case for all Σ-protocols in this paper.) This property, which is required

Σ-Protocol 2. Σ_{CM}: Proof of correct multiplication

```
[Relation] $R = \{(X, Y, Z; y, r, s) \mid Y = (1+N)^y r^N \wedge Z = X^y s^N\}$
[Announcement] $\Sigma.\mathsf{ann}(X, Y, Z; y, r, s) :=$
    $a \in_R \mathbb{Z}_N; u, v \in_R \mathbb{Z}_N^*; A := (1+N)^a u^N; B := X^a v^N;$ return $(A, B; a, u, v)$
[Response] $\Sigma.\mathsf{res}(X, Y, Z; y, r, s; A, B; a, u, v; c) :=$
    $t := \lfloor (a+cy)/N \rfloor; d := a + cy;\ e := ur^c(1+N)^t; f := vX^t s^c;$ return $(d, e, f)$
[Verification] $\Sigma.\mathsf{ver}(X, Y, Z; A, B; c; d, e, f) := (1+N)^d e^N \overset{?}{=} AY^c \wedge X^d f^N \overset{?}{=} BZ^c$
[Extractor] $\Sigma.\mathsf{ext}(X, Y, Z; A, B; c; c'; d, e, f; d', e', f') :=$
    $\alpha, \beta :=$ "values such that $\alpha(c - c') + \beta N = 1$"
    return $((d - d')\alpha, (e/e')^\alpha Y^\beta, (f/f')^\alpha Z^\beta)$
[Simulator] $\Sigma.\mathsf{sim}(X, Y, Z; c) :=$
    $d \in_R \mathbb{Z}_N; e, f \in_R \mathbb{Z}_N^*; A := (1+N)^d e^N Y^{-c}; B := X^d f^N Z^{-c}$
    return $(A, B; c; d, e, f)$
```

by the Fiat-Shamir heuristic [AABN08], essentially follows from the hardness of the relation; see [SV15] for details.

The CDN protocol uses a sub-protocol in which multiple parties simultaneously provide proofs based on the same challenge, called the "multiparty Σ-protocol". Namely, suppose each party from a set P wants to prove knowledge of a witness for a statement $v_i \in L_R$ with some Σ-protocol. To achieve this, each party in P broadcasts a commitment to its announcement; then, the computation parties jointly generate a challenge; and finally, all parties in P broadcast their response to this challenge, along with an opening of their commitment. The multiparty Σ-protocol is used as a building block in the CDN protocol by constructing a simulator that provides proofs on behalf of honest parties without knowing their witnesses ("zero-knowledgeness"), and extracts witnesses from corrupted parties that give correct proofs ("soundness").

The CDN protocol uses three Σ-protocols: Σ_{PK} proving plaintext knowledge, Σ_{CM} proving correct multiplication, and Σ_{CD} proving correct decryption. The first two are due to [CDN01] (which also proves that they are Σ-protocols). Σ_{PK} (Σ-Protocol 1) proves knowledge of x, r such that $X = (1+N)^x r^N$ is an encryption of x with randomness r. Σ_{CM} (Σ-Protocol 2) proves knowledge of (y, r, s) for (X, Y, Z) such that $Y = (1+N)^y r^N$ is an encryption of y with randomness r and $Z = X^y s^N$ is an encryption of the product of the plaintexts of X and Y randomised with s.

Proof Σ_{CD} of correct decryption (Σ-protocol 3) is due to [Jur03]. In the threshold variant of Paillier encryption due to Damgård and Jurik [DJ01, Jur03], safe primes $p = 2p' + 1, q = 2q' + 1$ are used for the RSA modulus $N = pq$. Key generation involves generating a secret value d such that, given $c' = c^{4\Delta^2 d}$, anybody can compute the plaintext of c by "decoding" c' as $\mathsf{paillierdecode}(c') := ((c' - 1) \div N)(4\Delta^2)^{-1} \bmod N$. Here, $\Delta = n!$ and $\div$ denotes division as integers (using $N | c' - 1$). The value d is then (t, n) Shamir-shared modulo $Np'q'$ between the computation parties as shares s_i. Threshold decryption is done by letting t

Σ-Protocol 3. Σ_{CD}: Proof of correct decryption (statistical)

```
[Relation] $R = \{(d, d_i, v, v_i; \Delta s_i) \mid d_i^2 = d^{4\Delta s_i} \wedge v_i = v^{\Delta s_i}\}$
[Announcement] $\Sigma.\mathsf{ann}(d, d_i, v, v_i; \Delta s_i) :=$ // $k = \log_2 N$; $k_2$ stat. sec. param
    $u \in_R [0, 2^{2k+2k_2}]$; $a := d^{4u}$; $b := v^u$; return $(a, b; u)$
[Response] $\Sigma.\mathsf{res}(d, d_i, v, v_i; \Delta s_i; a, b; u, c) :=$
    $r := u + c\Delta s_i$; return $r$
[Verification] $\Sigma.\mathsf{ver}(d, d_i, v, v_i; a, b; c; r) :=$ $d^{4r} \overset{?}{=} a(d_i)^{2c} \wedge v^r \overset{?}{=} b(v_i)^c$
[Extractor] $\Sigma.\mathsf{ext}(d, d_i, v, v_i; a, b; c; c'; r; r') :=$ return $(r - r')/(c - c')$
[Simulator] $\Sigma.\mathsf{sim}(d, d_i, v, v_i; c) :=$
    $r \in_R [0, 2^{2k+2k_2}]$; return$(d^{4r}(d_i)^{-2c}, v^r(v_i)^{-e}; c; r)$
```

parties each compute $c_i = c^{2\Delta s_i}$; the value $c^{4\Delta^2 d}$ is obtained by applying Shamir reconstruction "in the exponent". Correct decryption is proven with respect to a public set of verification values. Namely, the public key includes values v, $v_0 = v^{\Delta^2 d}$, and $v_i = v^{\Delta s_i}$ for all computation parties $i \in \mathcal{P}$. Hence, in Σ_{CD}, parties prove correctness of their decryption shares c_i of c by proving knowledge of $\Delta s_i = \log_{c^4}(c_i^2) = \log_v(v_i)$ for (c, c_i, v, v_i). (In the same way, v_0 can be used to prove correctness of c' with respect to c using a single instance of Σ_{CD}.) Note that this is a statistical Σ-protocol: this is because witness Δs_i is a value modulo the secret value $Np'q'$, so modulo reduction is not possible.

2.3 Security of the CDN Protocol

In [CDN01], it is shown that the CDN protocol implements secure function evaluation in Canetti's non-concurrent model [Can98] if only a minority of computation parties are corrupted. Essentially, this means that in this case, the computation succeeds; the result is correct; and the honest parties' inputs remain private. This conclusion is true assuming honest set-up and security of the Paillier encryption scheme and the trapdoor commitment scheme used. If a majority of computation parties is corrupted, then because threshold $\lceil n/2 \rceil$ is used for the threshold cryptosystem, privacy is broken. As noted [ST06, IPS09], this can be remedied by raising the threshold, but in that case, the corrupted parties can make the computation break down at any point by refusing to cooperate. In Sect. 4.1, we present a variant of this model in which we prove the security of our protocols (using random oracles but no trapdoor commitments).

3 Multiparty Non-interactive Proofs

In this section, we show how to produce non-interactive zero-knowledge proofs in a multiparty way. At several points in the above CDN protocol, all parties from a set P prove knowledge of witnesses for certain statements; the computation parties are convinced that those parties that succeed, do indeed know a witness.

In CDN, these proofs are interactive; but for universal verifiability, we need non-interactive proofs that convince any third party. The traditional method to make proofs non-interactive is the Fiat-Shamir heuristic; in Sect. 3.1, we outline it, and show that it is problematic in a multiparty setting. In Sect. 3.2, we present a new, "multiparty" Fiat-Shamir heuristic that works in our setting, and has the advantage of achieving smaller proofs by "homomorphically combining" the proofs of individual parties. In the remainder, $C \subset \mathcal{I} \cup \mathcal{P} \cup \{\mathcal{R}, \mathcal{V}\}$ denotes the set of corrupted parties; and F denotes the set of parties who failed to provide a correct proof when needed; this only happens for corrupted parties, so $F \subset C$.

Our results are in the random oracle model [BR93, Wee09], an idealised model of hash functions. In this model, evaluations of the hash function $\mathcal{H}$ are modelled as queries to a "random oracle" $\mathcal{O}$ that evaluates a perfectly random function. When simulating an adversary, a simulator can intercept these oracle queries and answer them at will, as long as the answers look random to the adversary. Security in the random oracle model does not generally imply security in the standard model [GK03], but it is often used because it typically gives simple, efficient protocols, and its use does not seem to lead to security problems in practice [Wee09]. See [SV15] for a detailed description of our use of random oracles; and Sect. 5 for a discussion of the real-world implications of the particular flavour of random oracles we use.

3.1 The Fiat-Shamir Heuristic and Witness-Extended Emulation

The obvious way of making the proofs in the CDN protocol non-interactive, is to apply the Fiat-Shamir heuristic to all individual Σ-protocols. That is, party $i \in P$ produces proof of knowledge π of a witness for statement v as follows[2]:

$$(a; s) := \Sigma.\mathsf{ann}(v; w); c := \mathcal{H}(v||a||aux); r := \Sigma.\mathsf{res}(v; w; a; s; c); \pi := (a; c; r).$$

Let us denote this procedure $\mathsf{fsprove}(\Sigma; v; w; aux)$. A verifier accepts those proofs $\pi = (a; c; r)$ for which $\mathsf{fsver}(\Sigma; v; \pi; aux)$ holds, where $\mathsf{fsver}(\Sigma; v; a, c, r; aux)$ is defined as $\mathcal{H}(v||a||aux) = c \wedge \Sigma.\mathsf{ver}(v; a; c; r)$.

Recall that security proofs require a simulator that simulates proofs of honest parties (zero-knowledgeness) and extracts witnesses of corrupted parties (soundness). In the random oracle model, Fiat-Shamir proofs for honest parties can be simulated by simulating a Σ-protocol conversation (a, c, r) and programming the random oracle so that $\mathcal{H}(v||a||aux) = c$. Witnesses of corrupted parties can be extracted by rewinding the adversary to the point where it made an oracle query for $v||a||aux$ and supplying a different value; but, as we discuss in [SV15], this extraction can make the simulator very inefficient. In fact, if Fiat-Shamir proofs take place in R different rounds, then extracting witnesses may increase the running time of the simulator by a factor $O(R!)$. The reason is that the oracle query

[2] Here, aux should contain at least the prover's identity. Otherwise, corrupted parties could replay proofs by honest parties, which breaks the soundness property below because witnesses for these proofs cannot be extracted by rewinding the adversary to the point of the oracle query and reprogramming the random oracle.

for a proof in one round may have in fact already been made in a previous round, in which case rewinding the adversary to extract one witness requires recursively extracting witnesses for all intermediate rounds. Hence, we can essentially only use the Fiat-Shamir heuristic in a constant number of rounds.

Moreover, in the CDN protocol, applying the Fiat-Shamir heuristic to each individual proof has the disadvantage that the verifier needs to check a number of proofs that depends linearly on the number of computation parties. In particular, for each multiplication gate, the verifier needs to check n proofs of correct multiplication and t proofs of correct decryption. Next, we show that we can avoid both the technical problems with witness extended emulation and the dependence on the number of computation parties by letting the computation parties collaboratively produce "combined proofs". (As discussed in [SV15], there are other ways of just solving the technical problems with witness extended emulation, but they are not easier than the method we propose.)

3.2 Combined Proofs with the Multiparty Fiat-Shamir Heuristic

The crucial observation (e.g., [Des93, KMR12]) allowing parties to produce non-interactive zero-knowledge proofs collaboratively is that, for many Σ-protocols, conversations of proofs with the same challenge can be "homomorphically combined". For instance, consider the classical Σ-protocol for proving knowledge of a discrete logarithm due to Schnorr [Sch89]. Suppose we have two Schnorr conversations proving knowledge of $x_1 = \log_g h_1$, $x_2 = \log_g h_2$, i.e., two tuples $(a_1; c; r_1)$ and $(a_2; c; r_2)$ such that $g^{r_1} = a_1(h_1)^c$ and $g^{r_2} = a_2(h_2)^c$. Then $g^{r_1+r_2} = (a_1 a_2)(h_1 h_2)^c$, so $(a_1 a_2; c; r_1 + r_2)$ is a Schnorr conversation proving knowledge of discrete logarithm $x_1 + x_2 = \log_g(h_1 h_2)$. For our purposes, we demand that such homomorphisms satisfy two properties. First, when conversations of at least $\lceil n/2 \rceil$ parties are combined, the result is a valid conversation (the requirement of having at least $\lceil n/2 \rceil$ conversations is needed for decryption proofs to ensure that there are enough decryption shares). Second, when fewer than $\lceil n/2 \rceil$ parties are corrupted, the combination of different honest announcements with the same corrupted announcements is likely to lead to a different combined announcement. This helps to eliminate the rewinding problems for Fiat-Shamir discussed above.

Definition 2. *Let Σ be a Σ-protocol for relation $R \subset V \times W$. Let Φ be a collection of partial functions $\Phi.\mathsf{stmt}$, $\Phi.\mathsf{ann}$, and $\Phi.\mathsf{resp}$. We call Φ a* homomorphism *of Σ if:*

- **Combination.** *Let c be a challenge; I a set of parties such that $|I| \geq \lceil n/2 \rceil$; and $\{(v_i; a_i; r_i)\}_{i \in I}$ a collection of statements, announcements, and responses. If $\Phi.\mathsf{stmt}(\{v_i\}_{i \in I})$ is defined and for all i, $\Sigma.\mathsf{ver}(v_i; a_i; c; r_i)$ holds, then also $\Sigma.\mathsf{ver}(\Phi.\mathsf{stmt}(\{v_i\}_{i \in I}); \Phi.\mathsf{ann}(\{a_i\}_{i \in I}); c; \Phi.\mathsf{resp}(\{r_i\}_{i \in I}))$.*
- **Randomness.** *Let c be a challenge; $C \subset I$ sets of parties such that $|C| < \lceil n/2 \rceil \leq |I|$; $\{v_i\}_{i \in I}$ statements s.t. $\Phi.\mathsf{stmt}(\{v_i\}_{i \in I})$ is defined; and $\{a_i\}_{i \in I \cap C}$ announcements. If $(a_i; \cdot), (a_i'; \cdot) \leftarrow \Sigma.\mathsf{sim}(v_i; c)$ $\forall i \in I \setminus C$, then with overwhelming probability, $\Phi.\mathsf{ann}(\{a_i\}_{i \in I}) \neq \Phi.\mathsf{ann}(\{a_i\}_{i \in I \cap C} \cup \{a_i'\}_{i \in I \setminus C})$.*

Protocol 4. MΣ: The Multi-Party Fiat-Shamir Heuristic

```
 1. // pre: $\Sigma$ is a $\Sigma$-protocol with homomorphism $\Phi$, $P$ is a set of non-failed
 2. //      parties ($P \cap F = \emptyset$), $v_P = \{v_i\}_{i \in P}$ statements w/ witnesses $w_P = \{w_i\}_{i \in P}$
 3. // post: if $|P \setminus F| \geq \lceil n/2 \rceil$, then $v_{P \setminus F}$ is the combined statement
 4. //         $\Phi.\mathsf{stmt}(\{v_i\}_{i \in P \setminus F})$, and $\pi_{P \setminus F}$ is a corresponding Fiat-Shamir proof
 5. // invariant: $F \subset C$: set of failed parties only includes corrupted parties
 6. $(v_{P \setminus F}, \pi_{P \setminus F}) \leftarrow \mathrm{M}\Sigma(\Sigma, \Phi, P, v_P, w_P, aux) :=$
 7.     repeat
 8.         parties $i \in P \setminus F$ do
 9.             $(a_i; s_i) := \Sigma.\mathsf{ann}(v_i; w_i); h_i := \mathcal{H}(a_i||i); \mathsf{bcast}(h_i)$
10.         parties $i \in P \setminus F$ do $\mathsf{bcast}(a_i)$
11.         $F' := F; F := F \cup \{i \in P \setminus F \mid h_i \neq \mathcal{H}(a_i||i)\}$
12.         if $F = F'$ then                    // all parties left provided correct hashes
13.             $c := \mathcal{H}(\Phi.\mathsf{stmt}(\{v_i\}_{i \in P \setminus F})||\Phi.\mathsf{ann}(\{a_i\}_{i \in P \setminus F})||aux)$
14.             parties $i \in P \setminus F$ do $r_i := \Sigma.\mathsf{res}(v_i; w_i; a_i; s_i; c); \mathsf{bcast}(r_i)$
15.             $F := F \cup \{i \in P \setminus F \mid \neg\Sigma.\mathsf{ver}(v_i; a_i; c; r_i)\}$
16.             if $F = F'$ then                // all parties left provided correct responses
17.                 return $(\Phi.\mathsf{stmt}(\{v_i\}_{i \in P \setminus F}),$
18.                            $(\Phi.\mathsf{ann}(\{a_i\}_{i \in P \setminus F}); c; \Phi.\mathsf{resp}(\{r_i\}_{i \in P \setminus F})))$
19.     until $|P \setminus F| < \lceil n/2 \rceil$                // until not enough parties left
20.     return $(\bot, \bot)$
```

Given a Σ-protocol with homomorphism Φ, parties holding witnesses $\{w_i\}$ for statements $\{v_i\}$ can together generate a Fiat-Shamir proof $(a; \mathcal{H}(v||a||aux); r)$ of knowledge of a witness for the "combined statement" $v = \Phi.\mathsf{stmt}(\{v_i\})$. Namely, the parties each provide announcement a_i for their own witness; compute $a = \Phi.\mathsf{ann}(\{a_i\})$ and $\mathcal{H}(v||a||aux)$; and provide responses r_i. Taking $r = \Phi.\mathsf{resp}(\{r_i\})$, the combination property from the above definition guarantees that we indeed get a validating proof. However, we cannot simply let the parties broadcast their announcements in turn, because to prove security in that case, the simulator needs to provide the announcements for the honest parties without knowing the announcements of the corrupted parties, hence without being able to program the random oracle on the combined announcement. We solve this by starting with a round in which each party commits to its announcement (the same trick was used in a different setting in [NKDM03])[3].

The *multiparty Fiat-Shamir heuristic* (Protocol 4) let parties collaboratively produce Fiat-Shamir proofs based on the above ideas. Apart from the above procedure (lines 8, 9, 10, 13, and 14), the protocol also contains error handling. Namely, we throw out parties that provide incorrect hashes to their announcements (line 11) or incorrect responses (line 15). If we have correct responses for all correctly hashed announcements, then we apply the homomorphism (line 17–18); otherwise, we try again with the remaining parties. If the number of parties drops below $\lceil n/2 \rceil$, the homomorphism can no longer be applied, so we

[3] As in [NKDM03], it may be possible to remove the additional round under the non-standard known-target discrete log problem.

return with an error (line 20). Note that, as in the normal Fiat-Shamir heuristic, the announcements do not need to be stored if they can be computed from the challenge and response (as will be the case for the Σ-protocols we consider).

Concerning security, recall that we need a simulator that simulates proofs of honest parties without their witnesses (zero-knowledgeness) and extracts the witnesses of corrupted parties (soundness). In [SV15], we present such a simulator. Essentially, it "guesses" the announcements of the corrupted parties based on the provided hashes; then simulates the Σ-protocol for the honest parties; and programs the random oracle on the combined announcement. It obtains witnesses for the corrupted parties by rewinding to just before the honest parties provide their announcements: this way, the corrupted parties are forced to use the announcements that they provided the hashes of (hence special soundness can be invoked), whereas the honest parties can provide new simulated announcements by reprogramming the random oracle. The simulator requires that fewer than $\lceil n/2 \rceil$ provers are corrupted so that we can use the randomness property of the Σ-protocol homomorphism (Definition 2). (When more than $\lceil n/2 \rceil$ provers are corrupted, we use an alternative proof strategy that uses witness-extended emulation instead of this simulator.)

3.3 Homomorphisms for the CDN Protocol

In the CDN protocol, the multiparty Fiat-Shamir heuristic allows us to obtain a proof that multiplication was done correctly that is independent of the number of computation parties. Recall that, for multiplication of encryptions X of x and Y of y, each computation party provides encryptions D_i of d_i and E_i of $d_i \cdot y$, and proves that E_i encrypts the product of the plaintexts of Y and D_i; and each computation party provides decryption share S_i of encryption $XD_1 \cdots D_n$, and proves it correct. As we will show now, the multiplication proofs can be combined with homomorphism Φ_{CM} into one proof that $\prod E_i$ encrypts the product of the plaintexts of Y and $\prod D_i$; and the decryption proofs can be combined with homomorphism Φ_{CD} into one proof that a combination S_0 of the decryption shares is correct. In the CDN protocol, the individual D_i, E_i, and S_i are not relevant, so also the combined values convince a verifier of correct multiplication.

In more detail, the homomorphism Φ_{CM} for Σ_{CM} is defined on statements $\{(X, Y_i, Z_i)\}_{i \in I}$ which share encryption X, and it proves that the multiplication on plaintexts of X with $\prod Y_i$ is equal to $\prod Z_i$. We let $\Phi.\mathsf{stmt}(\{(X, Y_i, Z_i)\}_{i \in I}) = \left(X, \prod_{i \in I} Y_i, \prod_{i \in I} Z_i\right)$ and $\Phi.\mathsf{ann}(\{A_i, B_i\}_{i \in I}) = \left(\prod_{i \in I} A_i, \prod_{i \in I} B_i\right)$. For the response, we would like to define $d = \sum_{i \in I} d_i$, $e = \prod_{i \in I} e_i$, and $f = \prod_{i \in I} f_i$; but because $\sum_{i \in I} d_i$ is computed modulo N, we need to add correction factors to e and f: $e = \left(\prod_{i \in I} e_i\right)(1+N)^k$ and $f = \left(\prod_{i \in I} f_i\right) Y^k$ (where $k = \lfloor (\sum_{i \in I} d_i)/N \rfloor$).

The homomorphism Φ_{CD} for Σ_{CD} combines correctness proofs of decryption shares into a proof of correct decryption with respect to an overall verification value. Let $I \geq \lceil n/2 \rceil$ be sufficiently many parties to decrypt a ciphertext, let $\{\lambda_i\}_{i \in I}$ be Lagrange interpolation coefficients for these parties. (Note that λ_i are not always integral; but we will always use $\Delta\lambda_i$, which *are* integral.) Let s_i be their shares of the decryption key $d = \sum_{i \in I} \Delta\lambda_i s_i$. Recall that decryption works by letting each party $i \in I$ provide decryption share $c_i = c^{2\Delta s_i}$; computing $c' = \prod_{i\in I} c_i^{2\Delta\lambda_i}$; and from this determining the plaintext as $\mathsf{paillierdecode}(c')$. Parties prove correctness of their decryption shares c_i by proving that $\log_{c^4} c_i^2 = \log_v v_i$, where v, v_i are publicly known verification values such that $v_i = v^{\Delta s_i}$. Now, if $\log_{c^4} c_i^2 = \log_v v_i$ for all i, then

$$\log_{c^4} c' = \log_{c^4} \prod_{i\in I} c_i^{2\Delta\lambda_i} = \log_v \prod_{i\in I} v_i^{\Delta\lambda_i} = \log_v \prod_{i\in I} (v^{\Delta s_i})^{\Delta\lambda_i} = \log_v v^{\Delta^2 d}.$$

Hence, decryption proofs for shares c_i with respect to verification values v_i can be combined into a decryption proof for c' with respect to verification value $v_0 := v^{\Delta^2 d}$. Formally, $\Phi.\mathsf{stmt}(\{(d, d_i, v, v_i)\}_{i\in I} = \left(d, \prod_{i\in I} c_i^{\Delta\lambda_i}, v, \prod_{i\in I} v_i^{\Delta\lambda_i}\right)$; $\Phi.\mathsf{ann}(\{(a_i, b_i)\}_{i\in I}) = \left(\prod_{i\in I} a_i^{\Delta\lambda_i}, \prod_{i\in I} b_i^{\Delta\lambda_i}\right)$; and $\Phi.\mathsf{resp}(\{r_i\}_{i\in I}) = \sum \Delta\lambda_i r_i$. For the combination property of Definition 2, note that we really need $I \geq \lceil n/2 \rceil$ in order to apply Lagrange interpolation. For the randomness property, note that if $|C| < \lceil n/2 \rceil$, then at least one party in $I \notin C$ has a non-zero interpolation coefficient, hence the contribution of this party to the announcement ensures that the two combined announcements are different.

4 Universally Verifiable MPC

In the previous section, we have shown how to produce non-interactive zero-knowledge proofs in a multiparty way. We now use this observation to obtain universally verifiable MPC. We first define security for universally verifiable MPC; and then obtain universally verifiable MPC by adapting the CDN protocol.

4.1 Security Model for Verifiable MPC

Our security model is an adaptation of the model of [Can98, CDN01] to the setting of universal verifiability in the random oracle model. We first explain the general execution model, which is as in [Can98, CDN01] but with a random oracle added; we then explain how to model verifiability in this execution model as the behaviour of the ideal-world trusted party. The general execution model compares protocol executions in the real and ideal world.

In the real world, a protocol π between m input parties $i \in \mathcal{I}$, n computation parties $i \in \mathcal{P}$, a result party $\mathcal{R}$ and a verifier $\mathcal{V}$ is executed on an open broadcast network with rushing in the presence of an active static adversary $\mathcal{A}$ corrupting parties $C \subset \mathcal{I} \cup \mathcal{P} \cup \{\mathcal{R}, \mathcal{V}\}$. The protocol execution starts by incorruptibly setting up the Paillier threshold cryptosystem, i.e., generating public key $\mathsf{pk} = (N, v, v_0, \{v_i\}_{i\in\mathcal{P}})$ with RSA modulus N and verification values v, v_0, v_i, and secret key shares $\{s_i\}_{i\in\mathcal{P}}$ (see Sect. 2.2). Each input party $i \in \mathcal{I}$ gets input (pk, x_i); each computation party $i \in \mathcal{P}$ gets input (pk, s_i); and the result party $\mathcal{R}$ gets input pk. The adversary gets the inputs $(\mathsf{pk}, \{x_i\}_{i\in\mathcal{I}\cap C}, \{s_i\}_{i\in\mathcal{P}\cap C})$ of the corrupted parties, and has an auxiliary input a. During the protocol, parties can query the random oracle; the oracle answers new queries randomly, and

Process 5. $\mathcal{T}_{\text{VSFE}}$: trusted party for verifiable secure function evaluation

```
// compute $f$ on $\{x_i\}_{i\in\mathcal{I}}$ for $\mathcal{R}$ with corrupted parties $C$; $\mathcal{V}$ learns encryption
$\mathcal{T}_{\text{VSFE}}(C, (N, v, v_0, \{v_i\}_{i\in\mathcal{P}})) :=$
    // input phase
    foreach $i \in \mathcal{I} \setminus C$ do  $x_i := \mathsf{recv}(\mathcal{I}_i)$                // honest inputs
    $\{x_i\}_{i\in\mathcal{I}\cap C} := \mathsf{recv}(\mathcal{S})$                              // corrupted inputs
    if $|\mathcal{P} \cap C| \geq \lceil n/2 \rceil$ then $\mathsf{send}(\{x_i\}_{i\in\mathcal{I}\setminus C}, \mathcal{S})$   // send to corrupted majority
    // computation phase
    $r := f(x_1, \ldots, x_m)$
    // output phase
    if $\mathcal{R} \notin C$ then      // honest $\mathcal{R}$: adversary learns encryption, may block result
        $s \in_R \mathbb{Z}_N^*$;  $R := (1+N)^r s^N$; $res := (r, s)$;  $\mathsf{send}(R, \mathcal{S})$
        if $|\mathcal{P} \cap C| \geq \lceil n/2 \rceil$ and $\mathsf{recv}(\mathcal{S}) = \perp$ then $res := \perp$;  $R := \perp$
        $\mathsf{send}(res, \mathcal{R})$
    else              // corrupted $\mathcal{R}$: adversary learns output, may block result to $\mathcal{V}$
        $\mathsf{send}(r, \mathcal{S})$; $s := \mathsf{recv}(\mathcal{S})$
        if $s = \perp$ then $R := \perp$ else $R := (1+N)^r s^N$
    // proof phase
    if $\mathcal{V} \notin C$ then $\mathsf{send}(R, \mathcal{V})$
```

repeated queries consistently. At the end of the protocol, each honest party outputs a value according to the protocol; the corrupted parties output $\perp$; and the adversary outputs a value at will. Define $\text{EXEC}_{\pi,\mathcal{A}}(k, (x_1, \ldots, x_m), C, a)$ to be the random variable, given security parameter k, consisting of the outputs of all parties (including the adversary) and the set $\mathcal{O}$ of oracle queries and responses.

The ideal-world execution similarly involves m input parties $i \in \mathcal{I}$, n computation parties $i \in \mathcal{P}$, result party $\mathcal{R}$, verifier $\mathcal{V}$, and an adversary $\mathcal{S}$ corrupting parties $C \subset \mathcal{I} \cup \mathcal{P} \cup \{\mathcal{R}, \mathcal{V}\}$; but now, there is also an incorruptible trusted party $\mathcal{T}$. As before, the execution starts by setting up the keys $(\mathsf{pk}, \{s_i\}_{i\in\mathcal{P}})$ of the Paillier cryptosystem. The input parties receive x_i as input; the trusted party receives a list C of corrupted parties and the public key pk. Then, it runs the code $\mathcal{T}_{\text{VSFE}}$ shown in Process 5, which we explain later. The adversary gets inputs $(\mathsf{pk}, C, \{x_i\}_{i\in\mathcal{I}\cap C}, \{s_i\}_{i\in\mathcal{P}\cap C})$, and outputs a value at will. In this model, there is no random oracle; instead, the adversary chooses the set $\mathcal{O}$ of oracle queries and responses (typically, those used to simulate a real-world adversary). As in the real-world case, $\text{IDEAL}_{\mathcal{T}_{\text{SFE}},\mathcal{S}}(k, (x_1, \ldots, x_m), C, a)$ is the random variable, given security parameter k, consisting of all parties' outputs and $\mathcal{O}$.

Definition 3. *Protocol* π implements verifiable secure function evaluation in the random oracle model *if, for every probabilistic polynomial time real-world adversary* $\mathcal{A}$*, there exists a probabilistic polynomial time ideal-world adversary* $\mathcal{S}_{\mathcal{A}}$ *such that, for all inputs* $x_1, \ldots, x_m$*; all sets of corrupted parties* C*; and all auxiliary input* a*:* $\mathit{EXEC}_{\pi,\mathcal{A}}(k; x_1, \ldots, x_m; C; a)$ *and* $\mathit{IDEAL}_{\mathcal{T}_{\mathit{VSFE}},\mathcal{S}_{\mathcal{A}}}(k; x_1, \ldots, x_m; C; a)$ *are computationally indistinguishable in security parameter* k*.*

We remark that, while security in non-random-oracle secure function evaluation [Can98, CDN01] is preserved under (subroutine) composition, this is not the case for our random oracle variant. The reason is that our model and protocols assume that the random oracle is not used outside of the protocol. Using the random oracle model with dependent auxiliary input [Unr07, Wee09] might be enough to obtain a composition property; but adaptations are needed to make our protocol provably secure in that model. See Sect. 5 for a discussion.

We now discuss the trusted party $\mathcal{T}_{\text{VSFE}}$ for verifiable secure function evaluation. Whenever the computation succeeds, $\mathcal{T}_{\text{VSFE}}$ guarantees that the results are correct. Namely, $\mathcal{T}_{\text{VSFE}}$ sends the result r of the computation and randomness s to $\mathcal{R}$ (line 13), and it sends encryption $(1+N)^r s^N$ of the result with randomness s to $\mathcal{V}$ (line 18); if the computation failed, $\mathcal{R}$ gets $(\perp, \perp)$ and $\mathcal{V}$ gets $\perp$.[4] Whether $\mathcal{T}_{\text{VSFE}}$ guarantees privacy (i.e., only $\mathcal{R}$ can learn the result) and robustness (i.e., the computation does not fail) depends on which parties are corrupted. Privacy and robustness with respect to $\mathcal{R}$ are guaranteed as long as only a minority of computation parties are corrupted. If not, then in line 6, $\mathcal{T}_{\text{VSFE}}$ sends the honest parties' inputs to the adversary; and in line 12, it gives the adversary the option to block the computation by sending $\perp$. Note that the adversary receives the inputs of the honest parties after it provides the inputs of the corrupted parties, so even if privacy is broken, the adversary cannot choose the corrupted parties' inputs based on the honest parties' inputs. For robustness with respect to $\mathcal{V}$, the result party needs to be honest. If not, then in line 15, $\mathcal{T}_{\text{VSFE}}$ gives the adversary the option to block $\mathcal{V}$'s result by sending $\perp$; in any case, it can choose the randomness. (Note that these thresholds are specific to CDN's "honest majority" setting; e.g., other protocols may satisfy privacy if all computation parties except one are corrupted.)

Note that this model does not cover the "universality" aspect of universally verifiable MPC. This is because the security model for secure function evaluation only covers the input/output behaviour of protocols, not the fact that "the verifier can be anybody". Hence, we design universally verifiable protocols by proving that they are verifiable, and then arguing based on the characteristics of the protocol (e.g., the verifier does not have any secret values) that this verifiability is "universal".

4.2 Universally Verifiable CDN

We now present the UVCDN protocol (Protocol 6) for universally verifiable secure function evaluation. At a high level, this protocol consists of the input,

[4] Although we only guarantee computational indistinguishability and the verifier does not know what value is encrypted, this definition *does* guarantee that $\mathcal{V}$ receives the correct result. This is because the ideal-world output of the protocol execution contains $\mathcal{R}$'s r and s and $\mathcal{V}$'s $(1+N)^r s^N$, so a distinguisher between the ideal and real world can check correctness of $\mathcal{V}$'s result. (If s were not in $\mathcal{R}$'s result, this would not be the case, and correctness of $\mathcal{V}$'s result would *not* be guaranteed.) Also, note that although privacy depends on the security of the encryption scheme, correctness *does not rely on any knowledge assumption*.

Protocol 6. UVCDN: universally verifiable CDN

```
// **pre**: $\mathsf{pk}/\{s_i\}_{i\in\mathcal{P}}$ threshold Paillier public/secret keys, $\{x_i\}_{i\in\mathcal{I}}$ function input
// **post**: output $R$ according to ideal functionality ITM 5
$R \leftarrow \mathrm{UVCDN}(\mathsf{pk} = (N, v, v_0, \{v_i\}_{i\in\mathcal{P}}), \{s_i\}_{i\in\mathcal{P}}, \{x_i\}_{i\in\mathcal{I}}) :=$
    **parties** $i \in \mathcal{I}$ **do**                                             // input phase
        $r_i \in_R \mathbb{Z}_N^*; X_i := (1+N)^{x_i} r_i^N; \pi_{\mathrm{PK},i} := \mathsf{fsprove}(\Sigma_{\mathrm{PK}}; X_i; x_i, r_i; i)$
        $h_i := \mathcal{H}(X_i || \pi_{\mathrm{PK},i} || i); \mathsf{bcast}(h_i); \mathsf{bcast}(X_i, \pi_{\mathrm{PK},i})$
    $F := \{i \in \mathcal{I} \mid h_i \neq \mathcal{H}(X_i || \pi_{\mathrm{PK},i} || i) \vee \neg\mathsf{fsver}(\Sigma_{\mathrm{PK}}; X_i; \pi_{\mathrm{PK},i}; i)\}$
    **foreach** $i \in F$ **do** $X_i := 1$
    **foreach** gate **do**                                                // computation phase
        **if** ⟨constant gate $c$ with value $v$⟩ **then** $X_c := (1+N)^v$
        **if** ⟨addition gate $c$ with inputs $a$, $b$⟩ **then** $X_c := X_a X_b$
        **if** ⟨subtraction gate $c$ with inputs $a$, $b$⟩ **then** $X_c := X_a X_b^{-1}$
        **if** ⟨multiplication gate $c$ with inputs $a$, $b$⟩ **then**     // [DN03] multiplication
            **parties** $i \in \mathcal{P} \setminus F$ **do**
                $d_i \in_R \mathbb{Z}_N; r_i, t_i \in_R \mathbb{Z}_N^*; D_i := (1+N)^{d_i} r_i^N; E_i := (X_b)^{d_i} t_i^N$
                $\mathsf{bcast}(D_i, E_i)$
            $(\cdot, D_c, E_c; \pi_{\mathrm{CM}c}) :=$
                    $\mathrm{M}\Sigma(\Sigma_{\mathrm{CM}}, \Phi_{\mathrm{CM}}, \mathcal{P} \setminus F, \{(X_b, D_i, E_i)\}_{i\in\mathcal{P}\setminus F}, \{(d_i, r_i, t_i)\}_{i\in\mathcal{P}\setminus F})$
            **if** $|\mathcal{P} \setminus F| < \lceil n/2 \rceil$ **then break**
            $S_c := X_a \cdot D_c$
            **parties** $i \in \mathcal{P} \setminus F$ **do** $S_i := (S_c)^{2\Delta s_i}; \mathsf{bcast}(S_i)$
            $(\cdot, S_{0,c}, \cdot, \cdot; \pi_{\mathrm{CD}c}) :=$
                    $\mathrm{M}\Sigma(\Sigma_{\mathrm{CD}}, \Phi_{\mathrm{CD}}, \mathcal{P} \setminus F, \{(S_c, S_i, v, v_i)\}_{i\in\mathcal{P}\setminus F}, \{\Delta s_i\}_{i\in\mathcal{P}\setminus F})$
            **if** $|\mathcal{P} \setminus F| < \lceil n/2 \rceil$ **then break**
            $s := \mathsf{paillierdecode}(S_{0,c}); X_c := (X_b)^s \cdot E_c^{-1}$
    **if** $|\mathcal{P} \setminus F| < \lceil n/2 \rceil$ **then parties** $i \in \mathcal{I} \cup \mathcal{P} \cup \{\mathcal{R}\}$ **do return** $\perp$
    **party** $\mathcal{R}$ **do** $d \in_R \mathbb{Z}_N; s \in_R \mathbb{Z}_N^*; D := (1+N)^d s^N$          // output phase
    **party** $\mathcal{R}$ **do** $\pi_{\mathrm{PK}d} := \mathsf{fsprove}(\Sigma_{\mathrm{PK}}; D; d, s; \mathcal{R}); \mathsf{bcast}(D, \pi_{\mathrm{PK}d})$
    **if** $\neg\mathsf{fsver}(\Sigma_{\mathrm{PK}}; D; \pi_{\mathrm{PK}d}; \mathcal{R})$ **then parties** $i \in \mathcal{I} \cup \mathcal{P} \cup \{\mathcal{R}\}$ **do return** $\perp$
    $Y := X_{\mathrm{outgate}} \cdot D^{-1}$; **parties** $i \in \mathcal{P} \setminus F$ **do** $Y_i := Y^{2\Delta s_i}; \mathsf{bcast}(Y_i)$
    $(\cdot, Y_0, \cdot, \cdot; \pi_{\mathrm{CD}}; y) := \mathrm{M}\Sigma(\Sigma_{\mathrm{CD}}, \Phi_{\mathrm{CD}}, \mathcal{P} \setminus F, \{(Y, Y_i, v, v_i)\}_{i\in\mathcal{P}\setminus F}, \{\Delta s_i\}_{i\in\mathcal{P}\setminus F}, D)$
    **if** $|\mathcal{P} \setminus F| < \lceil n/2 \rceil$ **then parties** $i \in \mathcal{I} \cup \mathcal{P} \cup \{\mathcal{R}\}$ **do return** $\perp$
    **party** $\mathcal{R}$ **do**
        $y := \mathsf{paillierdecode}(Y_0); r := y + d$
        $\mathsf{send}(\{(D_c, E_c, \Pi_{\mathrm{CM}c}, S_{0,c}, \Pi_{\mathrm{CD}c})\}_{c\in\mathrm{gates}}, (D, \pi_{\mathrm{PK}d}, Y_0, \pi_{\mathrm{CD}y}); \mathcal{V})$     // proof
        **return** $(r, s)$                                                    // phase
    **parties** $i \in \mathcal{I} \cup \mathcal{P}$ **do return** $\perp$
    **party** $\mathcal{V}$ **do** $\pi := \mathsf{recv}(\mathcal{R})$; **return** $\mathsf{vercomp}(\mathsf{pk}, \{X_i\}_{i\in\mathcal{I}}, \pi)$
```

computation, and multiplication phases of the CDN protocol, with all proofs made non-interactive, followed by a new *proof phase*. As discussed, we can use the normal Fiat-Shamir (FS) heuristic in only a constant number of rounds; and we can use the multiparty FS heuristic only when it gives a "combined statement" that makes sense. Hence, we choose to use the FS heuristic for the proofs by the input and result parties, and the multiparty FS heuristic for the proofs by the computation parties.

Algorithm 7. vercomp: verifier's gate-by-gate verification of the computation

```
// **pre**: pk public key, $\{X_i\}_{i \in \mathcal{I}}$ encryptions, $(\{\Pi_{\mathrm{mul}\,i}\}, \Pi_{\mathrm{result}})$ tuple
// **post**: if $(\{\Pi_{\mathrm{mul}\,i}\}, \Pi_{\mathrm{result}})$ proves correctness of $Y$, $X_o = Y$; otherwise, $X_o = \perp$
$X_o \leftarrow \mathsf{vercomp}(\mathsf{pk} = (N, v, v_0, \{v_i\}_{i \in \mathcal{P}}), \{X_i\}_{i \in \mathcal{I}}, (\{\Pi_{\mathrm{mul}\,i}\}, \Pi_{\mathrm{result}})) :=$
    // verification of input phase: see lines 6–8 of UVCDN
    // verification of computation phase
    **foreach** gate **do**
        **if** $\langle$constant gate $c$ with value $v\rangle$ **then** $X_c := (1+N)^v$
        **if** $\langle$addition gate $c$ with inputs $a$, $b\rangle$ **then** $X_c := X_a X_b$
        **if** $\langle$subtraction gate $c$ with inputs $a$, $b\rangle$ **then** $X_c := X_a X_b^{-1}$
        **if** $\langle$multiplication gate $c$ with inputs $a$, $b\rangle$ **then**
            $(D; E; a, c, r; S_0; a', c', r') := \Pi_{\mathrm{mul}\,c}$;  $S := X_a \cdot D^{-1}$
            **if** $\neg\mathsf{fsver}(\Sigma_{\mathrm{CM}}; X_b, D, E; a; c; r)$ **then return** $\perp$
            **if** $\neg\mathsf{fsver}(\Sigma_{\mathrm{CD}}; S, S_0, v, v_0; a'; c'; r')$ **then return** $\perp$
            $s := \mathsf{paillierdecode}(S_0)$; $X_c := (X_b)^s E^{-1}$
    // verification of output phase
    $(D; a_{\mathrm{out}}, c_{\mathrm{out}}, r_{\mathrm{out}}; Y_0; a_{\mathrm{dec}}, c_{\mathrm{dec}}, r_{\mathrm{dec}}) := \Pi_{\mathrm{result}}$
    **if** $\neg\mathsf{fsver}(\Sigma_{\mathrm{PK}}; D; a_{\mathrm{out}}, c_{\mathrm{out}}, r_{\mathrm{out}}; \mathcal{R})$ **then return** $\perp$
    $Y := X_{\mathrm{outgate}} \cdot D^{-1}$
    **if** $\neg\mathsf{fsver}(\Sigma_{\mathrm{CD}}; Y, Y_0, v, v_0; a_{\mathrm{dec}}, c_{\mathrm{dec}}, r_{\mathrm{dec}}; D)$ **then return** $\perp$
    $y := \mathsf{paillierdecode}(Y_0)$
    **return** $(1+N)^y D$                                   // encryption of $y + d = r$
```

In more detail, during the *input phase* of the protocol, the input parties provide their inputs (lines 4–8). As in the CDN protocol, each party encrypts its input and compiles a FS proof of knowledge (line 5). In the original CDN protocol, these encryptions and proofs would be broadcast directly; however, if a majority of computation parties are corrupted, then this allows corrupted parties to adapt their inputs based on the inputs of the honest parties. To prevent this, we let each party first broadcast a hash of its input and proof; only after all parties have committed to their inputs using this hash are the actual encrypted inputs and proofs revealed (line 6). All parties that provide an incorrect hash or proof have their inputs set to zero (line 7–8).

The remainder of the computation follows the CDN protocol. During the *computation phase*, the function is evaluated gate-by-gate; for multiplication gates, the multiplication protocol from [DN03] is used, with proofs of correct multiplication and decryption using the multiparty FS heuristic (lines 14–25). During the *output phase*, the result party obtains the result by broadcasting an encryption of a random d and proving knowledge using the normal FS heuristic (lines 27–28); the computation parties decrypt the result plus d, proving correctness using the multiparty FS heuristic (line 31). From this, the result party learns result r (line 34); and it knows the intermediate values from the protocol and the proofs showing they are correct.

Finally, we include a *proof phase* in the UVCDN protocol in which the result party sends these intermediate values and proofs to the verifier (line 35). The verifier runs procedure vercomp (Algorithm 7) to verify the correctness of the computation (line 38). The inputs to this verification procedure are the public key of the Paillier cryptosystem; the encrypted inputs $\{X_i\}_{i\in\mathcal{I}}$ by the input parties; and the proof π by the result party (which consists of proofs for each multiplication gate, and the two proofs from the output phase of the protocol). The verifier checks the proofs for each multiplication gate from the computation phase (lines 6–14); and the proofs from the output phase (lines 16–20), finally obtaining an encryption of the result (line 21). While not specified in vercomp, the verifier does also verify the proofs from the input phase: namely, in lines 7–8 of UVCDN, the verifier receives encrypted inputs and verifies their proofs to determine the encrypted inputs $\{X_i\}_{i\in\mathcal{I}}$ of the computation.

Apart from checking the inputs during the input phase, the verifier does not need to be present for the remainder of the computation until receiving π from $\mathcal{R}$. This is what makes verification "universal": in practice, we envision that a trusted party publicly announces the Paillier public keys, and the input parties publicly announce their encrypted inputs with associated proofs: then, anybody can use the verification procedure to verify if a given proof π is correct with respect to these inputs. In [SV15], we prove that:

Theorem 1. *Protocol UVCDN implements verifiable secure function evaluation in the random oracle model.*

The proof uses two simulators: one for a honest majority of computation parties; one for a corrupted majority. The former simulator extends the one from [CDN01], obtaining privacy with a reduction to semantic security of the threshold Paillier cryptosystem. The latter does not guarantee privacy, and so can simulate the adversary by running the real protocol, ensuring correctness by witness-extended emulation.

5 Concluding Remarks

Our security model is specific to the CDN setting in two respects. First, we explicitly model that the verifier receives a Paillier encryption of the result (as opposed to another kind of encryption or commitment). We chose this formulation for concreteness; but our model generalises easily to other representations of the result. Second, it is specific to the setting where a minority of parties may be actively corrupted; but it is possible to change the model to other corruption models. For instance, it is possible to model the setting from [BDO14] where privacy is guaranteed when there is at least one honest computation party (and our protocols can be adapted to that setting). The combination of passively secure multiparty computation with universal verifiability is another interesting possible adaptation.

Our protocols are secure in the random oracle model "without dependent auxiliary input" [Wee09]. This means our security proofs assume that the random oracle has not been used before the protocol starts. Moreover, our simulator can only simulate logarithmically many sequential runs of our protocol due to technical limits of witness-extended emulation. These technical issues reflect the real-life problem that a verifier cannot see if a set of computation parties have just performed a computation, or they have simply replayed an earlier computation transcript. As discussed in [Unr07], both problems can be solved in practice by instantiating the random oracle with a keyed hash function, with every computation using a fresh random key. Note that all existing constructions require the random oracle model; achieving universally verifiable (or publicly auditable) multiparty computation in the standard model is open.

Several interesting variants of our protocol are possible. First, it is easy to achieve publicly auditable multiparty computation [BDO14] by performing a public decryption of the result rather than a private decryption for the result party. Another variant is basic outsourcing of computation, in which the result party does not need to be present at the time of the computation, but afterwards gets a transcript from which it can derive the computation result. Finally, it is possible to achieve universal verifiability using other threshold cryptosystems than Paillier. In particular, while the threshold ElGamal cryptosystem is much more efficient than threshold Paillier, it cannot be used directly with our protocols because it does not have a general decryption operation; but universally verifiable multiparty using ElGamal should still be possible by instead adapting the "conditional gate" variant of the CDN protocol from [ST04].

Finally, to close the loop, we note that our techniques can also be applied to reduce the cost of verification in universally verifiable voting schemes. Namely, for voting schemes relying on homomorphic tallying, we note that the Σ-proofs for correct decryption of the election result by the respective talliers can be combined into a single Σ-proof of constant size (independent of the number of talliers). Similarly, for voting schemes relying on mix-based tallying, the Σ-proofs for correct decryption of each vote by the respective talliers is reduced to a constant size per vote.

Acknowledgements. The authors thank Sebastiaan de Hoogh, Thijs Laarhoven, and Niels de Vreede for useful discussions. This work was supported in part by the European Commission through the ICT program under contract INFSO-ICT-284833 (PUFFIN). The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement no 609611 (PRACTICE).

References

[AABN08] Abdalla, M., An, J.H., Bellare, M., Namprempre, C.: From Identification to signatures via the Fiat-Shamir transform: necessary and sufficient conditions for security and forward-security. IEEE Trans. Inf. theory **54**(8), 3631–3646 (2008)

[ACG+14] Ananth, P., Chandran, N., Goyal, V., Kanukurthi, B., Ostrovsky, R.: Achieving privacy in verifiable computation with multiple servers – without FHE and without pre-processing. In: Krawczyk, H. (ed.) PKC 2014. LNCS, vol. 8383, pp. 149–166. Springer, Heidelberg (2014)

[BCD+09] Bogetoft, P., Christensen, D.L., Damgård, I., Geisler, M., Jakobsen, T., Krøigaard, M., Nielsen, J.D., Nielsen, J.B., Nielsen, K., Pagter, J., Schwartzbach, M., Toft, T.: Secure multiparty computation goes live. In: Dingledine, R., Golle, P. (eds.) FC 2009. LNCS, vol. 5628, pp. 325–343. Springer, Heidelberg (2009)

[BDO14] Baum, C., Damgård, I., Orlandi, C.: Publicly auditable secure multi-party computation. In: Abdalla, M., De Prisco, R. (eds.) SCN 2014. LNCS, vol. 8642, pp. 175–196. Springer, Heidelberg (2014)

[BR93] Bellare, M., Rogaway, P.: Random oracles are practical: a paradigm for designing efficient protocols. In: Proceedings of CCS 1993, pp. 62–73. ACM (1993)

[Can98] Canetti, R.: Security and composition of multi-party cryptographic protocols. J. Cryptol. **13**, 2000 (1998)

[CDN01] Cramer, R., Damgård, I.B., Nielsen, J.B.: Multiparty computation from threshold homomorphic encryption. In: Pfitzmann, B. (ed.) EUROCRYPT 2001. LNCS, vol. 2045, pp. 280–300. Springer, Heidelberg (2001)

[CF85] Cohen, J., Fischer, M.: A robust and verifiable cryptographically secure election scheme. In: Proceedings of FOCS 1985, pp. 372–382. IEEE (1985)

[Des93] Desmedt, Y.: Threshold cryptosystems. In: Seberry, J., Zheng, Y. (eds.) AUSCRYPT 1992. LNCS, vol. 718, pp. 1–14. Springer, Heidelberg (1993)

[dH12] de Hoogh, S.: Design of large scale applications of secure multiparty computation: secure linear programming. Ph.D. thesis, Eindhoven University of Technology (2012)

[DJ01] Damgård, I., Jurik, M.: A generalisation, a simpli.cation and some applications of paillier's probabilistic public-key system. In: Kim, K. (ed.) PKC 2001. LNCS, vol. 1992, pp. 119–136. Springer, Heidelberg (2001)

[DN03] Damgård, I.B., Nielsen, J.B.: Universally composable efficient multiparty computation from threshold homomorphic encryption. In: Boneh, D. (ed.) CRYPTO 2003. LNCS, vol. 2729, pp. 247–264. Springer, Heidelberg (2003)

[DPSZ12] Damgård, I., Pastro, V., Smart, N., Zakarias, S.: Multiparty computation from somewhat homomorphic encryption. In: Safavi-Naini, R., Canetti, R. (eds.) CRYPTO 2012. LNCS, vol. 7417, pp. 643–662. Springer, Heidelberg (2012)

[EFLL12] Ejgenberg, Y., Farbstein, M., Levy, M., Lindell, Y.: SCAPI: The secure computation application programming interface. IACR Cryptology ePrint Archive 2012:629 (2012)

[FGP14] Fiore, D., Gennaro, R., Pastro, V.: Efficiently verifiable computation on encrypted data. In: Proceedings of CCS 2014, pp. 844–855. ACM (2014)

[GK03] Goldwasser, S., Kalai, Y.T.: On the (In)security of the Fiat-Shamir paradigm. In: Proceedings of FOCS 2003, pp. 102–113. IEEE Computer Society (2003)

[GKP+13] Goldwasser, S., Kalai, Y.T., Popa, R.A., Vaikuntanathan, V., Zeldovich, N.: Reusable garbled circuits and succinct functional encryption. In: Proceedings of STOC 2013, pp. 555–564. ACM (2013)

[IPS09] Ishai, Y., Prabhakaran, M., Sahai, A.: Secure arithmetic computation with no honest majority. In: Reingold, O. (ed.) TCC 2009. LNCS, vol. 5444, pp. 294–314. Springer, Heidelberg (2009)

[Jur03] Jurik, M.J.:. Extensions to the Paillier cryptosystem with applications to cryptological protocols. Ph.D. thesis, University of Aarhus (2003)

[KMR12] Keller, M., Mikkelsen, G.L., Rupp, A.: Efficient threshold zero-knowledge with applications to user-centric protocols. In: Smith, A. (ed.) ICITS 2012. LNCS, vol. 7412, pp. 147–166. Springer, Heidelberg (2012)

[NKDM03] Nicolosi, A., Krohn, M.N., Dodis, Y., Mazières, D.: Proactive two-party signatures for user authentication. In: Proceedings of NDSS 2003. The Internet Society (2003)

[Pai99] Paillier, P.: Public-key cryptosystems based on composite degree residuosity classes. In: Stern, J. (ed.) EUROCRYPT 1999. LNCS, vol. 1592, pp. 223–238. Springer, Heidelberg (1999)

[PHGR13] Parno, B., Howell, J., Gentry, C., Raykova, M.: Pinocchio: nearly practical verifiable computation. In: Proceedings of S&P 2013, pp. 238–252. IEEE (2013)

[Sch89] Schnorr, C.-P.: Efficient identification and signatures for smart cards. In: Brassard, G. (ed.) CRYPTO 1989. LNCS, vol. 435, pp. 239–252. Springer, Heidelberg (1990)

[SK95] Sako, K., Kilian, J.: Receipt-free mix-type voting scheme. In: Guillou, L.C., Quisquater, J.-J. (eds.) EUROCRYPT 1995. LNCS, vol. 921, pp. 393–403. Springer, Heidelberg (1995)

[ST04] Schoenmakers, B., Tuyls, P.: Practical two-party computation based on the conditional gate. In: Lee, P.J. (ed.) ASIACRYPT 2004. LNCS, vol. 3329, pp. 119–136. Springer, Heidelberg (2004)

[ST06] Schoenmakers, B., Tuyls, P.: Efficient binary conversion for Paillier encrypted values. In: Vaudenay, S. (ed.) EUROCRYPT 2006. LNCS, vol. 4004, pp. 522–537. Springer, Heidelberg (2006)

[SV15] Schoenmakers, B., Veeningen, M.: Universally verifiable multiparty computation from threshold homomorphic cryptosystems. Cryptology ePrint Archive, Report 2015/058 (full version of this paper) (2015). http://eprint.iacr.org/

[Unr07] Unruh, D.: Random oracles and auxiliary input. In: Menezes, A. (ed.) CRYPTO 2007. LNCS, vol. 4622, pp. 205–223. Springer, Heidelberg (2007)

[WB13] Walfish, M., Blumberg, A.J.: Verifying computations without reexecuting them: from theoretical possibility to near-practicality. Electron. Colloquium Computat. Complex. **20**, 165 (2013)

[Wee09] Wee, H.: Zero knowledge in the random oracle model, revisited. In: Matsui, M. (ed.) ASIACRYPT 2009. LNCS, vol. 5912, pp. 417–434. Springer, Heidelberg (2009)