Group Encryption

Aggelos Kiayias[*] Yiannis Tsiounis[†] Moti Yung[‡]

January 19, 2007

Abstract

We present group encryption, a new cryptographic primitive which is the encryption analogue of a group signature. It possesses similar verifiability, security and privacy properties, but whereas a group signature is useful whenever we need to conceal the source (signer) within a group of legitimate users, a group encryption is useful whenever we need to conceal a recipient (decryptor) within a group of legitimate receivers.

We introduce and model the new primitive and present sufficient as well as necessary conditions for its generic implementation. We then develop an efficient novel number theoretic construction for group encryption of discrete logarithms whose complexity is independent of the group size. To achieve this we construct a new public-key encryption for discrete logarithms that satisfies CCA2-key-privacy and CCA2-security in the standard model. Applications of group encryption include settings where a user wishes to hide her preferred trusted third party or even impose a hidden hierarchy of trusted parties, or settings where verifiable well-formed ciphertexts are kept in a untrusted storage server that must be prevented from both learning the content of records as well as analyzing the identities of their retrievers.

[*]University of Connecticut, Storrs, CT, USA, aggelos@cse.uconn.edu.
[†]Independent Consultant, NY, USA, yiannis@ccs.neu.edu
[‡]RSA Laboratories, Bedford MA, and Computer Science, Columbia University, NY, USA moti@cs.columbia.edu

Contents

1 Introduction

Group signatures were introduced in [CvH91] and further developed in a line of works, e.g., [CP94, CS97, CM98, CM99, Cam97, KP98, AT99, ACJT00, CL01b, KY03, BBS04, CL04, BSZ05, KY05, ACHdM05, TW05, BW06, KY06, Gro06]. In a nutshell a group signature allows a registered member of a PKI (a.k.a. a group of registered users) to issue a signature on behalf of the group so that the issuer's identity is assured to be valid but is hidden from the verifier.

We introduce a novel cryptographic primitive that is the encryption analogue of a group signature; we call it *group encryption* (not to be confused with group-oriented cryptography as in [Des87, CD00], which is essentially threshold cryptosystems). A group encryption scheme allows a sender to prepare a ciphertext and convince a verifier that it can be decrypted by a member of the PKI group. As in a group signature, in a group encryption there can be an opening authority that when the appropriate circumstances are triggered it can reveal the identity of the group member who is the recipient of the ciphertext. A group encryption provides "receiver anonymity" in the same way that a group signature provides "sender anonymity." This primitive was never considered in the group-signature literature before, even though public-key encryption and signatures are typically dual primitives that have been developed in parallel in many other settings.

We note that in protocols that attempt to maintain privacy/ anonymity, it has been often advocated as a flexible service to allow a user to choose its recipient trustee (e.g., a trusted third party for conditionally opening the ciphertext) among a set of available authorized parties. However, the choice of a third party, while increasing flexibility, might also reveal some preference of the user, thus reducing privacy. Group encryption is motivated by such applications.

1.1 Contributions

In this work we first contribute the definition, formalization and generic feasibility of group encryption. We then construct an efficient concrete implementation and investigate its related number theoretic properties.

– *Definition and Model.* The group encryption primitive (GE) involves a public-key encryption scheme with special properties, a group joining protocol (involving public-key certification) and a message space that may have a required structure. Besides correctness, there are three security properties that pertain to GE schemes. The first two of these properties, called *Security* and *Anonymity* protect the sender from a hostile environment that tries to either extract information about the message (security) or to extract information about who the recipient is (anonymity). We require both properties to have the strongest notion of immunity to attack, namely CCA2 [DDN91, RS92]. The third property, that we call *Soundness* protects the verifier from a hostile environment in which the sender, the group manager and the recipients collude against him, so that he accepts a ciphertext (e.g., an encrypted record to be stored) that either does not have the required structure or cannot be decrypted by a registered group member.

– *Necessary and Sufficient Conditions and Generic Design.* We identify the necessary cryptographic components of a GE scheme that include: a digital signature with adaptive chosen message security, a public-key encryption scheme that satisfies both CCA2-key-privacy and CCA2-security, and zero-knowledge proofs for NP statements. Using such appropriate components we demonstrate how a generic GE scheme can be implemented and how, in turn, the scheme implies these components (where a signature and encryption are derived directly with a relatively tight reduction).

– *Efficient Design.* We design a GE scheme for the discrete logarithm relation, which is one of the most useful relations in cryptography. To this end we instantiate the modular design but with primitives that algebraically suit its structure, to give a relatively efficient design where the ciphertext and the proof associated with it has size independent of the size of the group of potential receivers.

– *Efficient Encryption of Discrete Logarithm with CCA2-Security and CCA2-key-privacy.* As our first step in the overall group encryption design, we point out that no existing public-key encryption scheme is suitable for designing a GE for discrete logarithm relations, since the compound set of the requirements that include verifiability, CCA2-security and CCA2-key-privacy for anonymity has not been achieved before and requires special attention. We then design a public-key encryption with key-privacy suitable for verifiable encryption of discrete-logarithms. The security of the scheme is based on the *Decisional Composite Residuosity* (DCR) assumption of Paillier [Pai99] (and its design is motivated by earlier works of [CS98], [GL03] and [CS03]). We note that our encryption is the first Paillier-based scheme that satisfies key-privacy, a fact which may be of independent interest.
– *Algebraic Structure and Intractability Assumption.* A new intractability assumption is required for proving the key-privacy property of our encryption scheme: *Decisional Diffie Hellman assumption for the subgroup of square (quadratic) n-th residues* ($\mathsf{DDH}_{\mathsf{SQNR}}$). We explain why this is a natural variation of DDH over a cyclic subgroup of $\mathbb{Z}^*_{n^2}$ that has order without small prime divisors and moreover, to strengthen the claim of intractability, we prove that the DCR (which is needed for arguing the security of the scheme anyway) implies the computational Diffie Hellman (CDH) assumption in this subgroup. Note that we know of no arithmetic cyclic group without small order divisors where CDH holds but where DDH does not hold.

1.2 Applications of Group Encryption

The combination of security of ciphertexts, anonymity of receivers and verifiability is a strong one and supports some enhanced properties of known constructions as well as opens the door for new applications.
– *Anonymous Trusted Third Party Applications.* Many protocols such as Fair Encryption, Escrow Encryption, Group Signatures, Fair Exchange, employ a trustee, namely a trusted third party who is off-line during the protocol and gets invoked in case something goes wrong. In an actual deployment of any of the above primitives it is expected that there will be a multitude of these trustees. In this case the identity of a chosen trustee may reveal certain aspects of the user, whereas the user prefers to retain her privacy. For example, imagine an "International Key Escrow" scenario where a user wants to deposit (decrypt) a key with her own national trusted representative. However, such a choice, if made public, may reveal the user's nationality (in violation of privacy). The new group encryption primitive enables the user to trust her own representative, but without revealing its identity, yet to assure others that indeed a designated trustee has been chosen. Note that two models are possible for taking keys off escrow: In the first one, each trustee tries to retrieve all the keys from the available ciphertext repository, and will be successful only when the ciphertext is his to open. In the second model, there is an opening authority which can open the identity of the trustee (but not the encrypted key, due to separation of duties). The opening authority, in turn, directs the ciphertext to the chosen trustee to be decrypted. Another scenario that is similar to the above, is proxy voting where users deposit their votes encrypted under the public-key of a proxy of their choice. A proxy is a designated trustee in this case and each user may prefer (or even be required due to legislation) to hide her choice when depositing her vote. In this manner, the proxies can be called upon later, in the tallying phase, to recover the votes entrusted to them.
– *Secure Oblivious Retriever Storage.* In the area of ubiquitous computing, secure and anonymous credentials may move between computing elements (computer, mobile unit, embedded device, etc.). A user may want to pass a credential secretly and anonymously between devices (either between her own devices, or devices of her peers, all belonging to the same group). Asynchronous transfer that does not require all devices to be present at the same time requires a storage server (similar to a mail server). We can employ group encryption in implementing such a storage server safely, where it is guaranteed that (1) the server only stores valid credentials (i.e., well formed ones) that have

a legitimate retriever; (2) the credentials are encrypted and thus the server (or anyone who may compromise it) cannot employ them; and (3) the identity of retrievers of credentials is hidden. A device reading the storage can recover its credentials by scanning the storage sequentially and being successful in decrypting the credentials directed to it (no opening authority is needed).
– *Ad-Hoc Access Structure Group Signature.* We may implement the opening authority in group encryption as a multitude of trustees and use it to encrypt a signing credential. In this way we can build a group signature where signers can organize the set of trustees to open their signature by acting on it in a predetermined order following an ad-hoc flexible structure that is only partially revealed to the verifier. This can be achieved by cascading the group encryption primitive so that a sequence of hops (identity discoveries and transfers) will be required to recover the identity of the signer in the signature opening step. This notion generalizes "hierarchical group signatures" a primitive introduced in [TW05] where the trustee access structure was determined as a fixed tree.

1.3 Preliminaries

In this section we provide some standard definitions for reference purposes.
Adaptively Chosen Message Secure Digital Signatures. This is the classic security notion for digital signatures [GMR84] that we reiterate here for completeness. Consider a digital signature $\langle \mathcal{G}_\mathsf{s}, \mathcal{S}, \mathcal{V}_\mathsf{s} \rangle$ and the following game with a PPT adversary $\mathcal{A}$ that is allowed to pose adaptively q signing queries:

1. $\langle \mathsf{sik}, \mathsf{vek} \rangle \leftarrow \mathcal{G}_\mathsf{s}(1^\nu)$.
2. $\langle m^*, \sigma^* \rangle \leftarrow \mathcal{A}^{\mathcal{S}(\mathsf{sik}, \cdot)}(1^\nu, \mathsf{vik})$.
3. $\mathsf{out} \leftarrow \mathcal{V}_\mathsf{s}(m^*, \sigma^*) \wedge (m^* \notin \{m_1, \ldots, m_q\})$.

where the values $m_1, \ldots, m_q$ correspond to the queries of $\mathcal{A}$ to the signing oracle. The digital signature is adaptive chosen message secure provided that $\mathbf{Prob}[\mathsf{out} = \mathsf{true}] = \mathsf{negl}(\nu)$.
Commitment Schemes. A commitment scheme is defined by three procedures $\langle \mathcal{Z}_\mathsf{c}, \mathcal{C}, \mathcal{T} \rangle$ with the following properties: (hiding) for any given $\mathsf{cpk} \leftarrow \mathcal{G}_\mathsf{c}(1^\nu)$ and any x, the procedure $\mathcal{C}(\mathsf{cpk}, x)$ produces the commitment ψ and the decommitment information ρ so that ψ reveals no information about x. (binding) for any x, if $\langle \psi, \rho \rangle \leftarrow \mathcal{C}(\mathsf{cpk}, x)$ it is computationally hard to find $x' \neq x$ and ρ' so that $\mathcal{T}(\rho, x, \psi) = \mathcal{T}(\rho', x', \psi) = \mathtt{true}$.
Extractable Commitments. A commitment scheme is called extractable if $\mathcal{Z}_\mathsf{c}$ produces in addition to cpk a trapdoor τ_ext and there is a procedure $\mathcal{D}_\mathsf{c}$ such that $\mathcal{D}_\mathsf{c}(\tau_\mathsf{ext}, \mathcal{C}(\mathsf{cpk}, x)) = x$.
Equivocal Commitments. A commitment scheme is called equivocal if $\mathcal{Z}_\mathsf{c}$ produces in addition to cpk a string τ_equ and there is a procedure $\mathcal{Q}_\mathsf{c}$ that given τ_equ, x, x' with $x \neq x'$ and $\langle \psi, \rho \rangle \leftarrow \mathcal{C}(\mathsf{cpk}, x)$, $\mathcal{Q}_\mathsf{c}$ returns ρ' such that $\mathcal{T}(\rho, x, \psi) = \mathcal{T}(\rho', x', \psi) = \mathtt{true}$. Moreover, the distribution of ρ should be indistinguishable from that of ρ'.
Public-Key encryption with CCA2-security. Consider a cryptosystem $\langle \mathcal{Z}, \mathcal{G}_\mathsf{e}, \mathcal{E}, \mathcal{D} \rangle$ and the following game:

1. $\mathsf{param} \leftarrow \mathcal{Z}(1^\nu)$.
2. $\langle \mathsf{pk}, \mathsf{sk} \rangle \leftarrow \mathcal{G}_\mathsf{e}(\mathsf{param})$.
3. $\langle m_0, m_1, \mathsf{aux}, L \rangle \leftarrow \mathcal{A}^{\mathcal{D}(\mathsf{sk}, \cdot)}(\mathtt{FIND}, \mathsf{pk})$.
4. $b \leftarrow_R \{0, 1\}$.
5. if $m_0 = m_1$ then abort;
6. $\psi \leftarrow \mathcal{E}(\mathsf{pk}, m_b, L)$.
7. $b^* \leftarrow \mathcal{A}^{\mathcal{D}^{\neg \langle \psi, L \rangle}(\mathsf{sk}, \cdot)}(\mathtt{GUESS}, \psi, \mathsf{aux})$.

The cryptosystem satisfies CCA2-security if it holds that for any PPT $\mathcal{A}$ playing the above game, $|\mathbf{Prob}[b = b^*] - \frac{1}{2}| = \mathsf{negl}(\nu)$. We note that CPA-security is defined as above with the difference that

at steps 3 and 7 the adversary has no access to the decryption oracles. Moreover observe that in many cases $\mathcal{Z}$ can be simply assumed to be the identity function. In cases though that many users share the same parameters (for example in the case of ElGamal encryption this can be the prime number that defines the modular group) it is helpful to consider a $\mathcal{Z}$ that is separate from $\mathcal{G}_{\mathsf{e}}$.
Public-Key encryption with CCA2-key-privacy. Consider a cryptosystem $\langle \mathcal{Z}, \mathcal{G}_{\mathsf{e}}, \mathcal{E}, \mathcal{D} \rangle$ and the following game:

1. $\mathsf{param} \leftarrow \mathcal{Z}(1^\nu)$.
2. $\langle \mathsf{pk}_0, \mathsf{sk}_0 \rangle \leftarrow \mathcal{G}_{\mathsf{e}}(\mathsf{param})$; $\langle \mathsf{pk}_1, \mathsf{sk}_1 \rangle \leftarrow \mathcal{G}_{\mathsf{e}}(\mathsf{param})$.
3. $\langle m, \mathsf{aux}, L \rangle \leftarrow \mathcal{A}^{\mathcal{D}(\mathsf{sk}_0,\cdot),\mathcal{D}(\mathsf{sk}_1,\cdot)}(\mathtt{FIND}, \mathsf{pk}_0, \mathsf{pk}_1)$.
4. $b \leftarrow_R \{0,1\}$.
5. $\psi \leftarrow \mathcal{E}(\mathsf{pk}_b, m, L)$.
6. $b^* \leftarrow \mathcal{A}^{\mathcal{D}^{\neg\langle\psi,L\rangle}(\mathsf{sk}_0,\cdot),\mathcal{D}^{\neg\langle\psi,L\rangle}(\mathsf{sk}_1,\cdot)}(\mathtt{GUESS}, \psi, \mathsf{aux})$.

The cryptosystem satisfies CCA2-key-privacy if it holds that for any PPT $\mathcal{A}$ playing the above game, $|\mathbf{Prob}[b = b^*] - \frac{1}{2}| = \mathsf{negl}(\nu)$. We note that CPA-key-privacy is defined as above with the difference that at steps 3 and 6 the adversary has no access to the decryption oracles. This notion was first investigated in [BBDP01].

2 Group Encryption: Model and Definitions

The parties involved in a GE scheme are the sender, the verifier, a group manager (GM) that manages the group of receivers and an opening authority (OA) that is capable of discovering the identity of the receiver. Formally, a GE scheme that is verifiable for a public-relation $\mathcal{R}$ is a collection of procedures and protocols that are denoted as follows:

$$\left\langle \mathtt{SETUP}, \mathtt{JOIN}, \langle \mathcal{G}_{\mathsf{r}}, \mathcal{R}, \mathsf{sample}_{\mathcal{R}} \rangle, \mathtt{ENC}, \mathtt{DEC}, \mathtt{OPEN}, \langle \mathcal{P}, \mathcal{V}, \mathsf{recon} \rangle \right\rangle$$

The functionality of the above procedures is as follows: the $\mathtt{SETUP}$ is a set of intialization procedures for the system, one for the GM, one for the OA and one to produce public-parameters (denoted by $\mathtt{SETUP}_{\mathsf{GM}}, \mathtt{SETUP}_{\mathsf{OA}}, \mathtt{SETUP}_{\mathsf{init}}$ respectively). Using their respective setup procedures, the GM and the OA will produce their public/secret-key pairs $\langle \mathsf{pk}_{\mathsf{GM}}, \mathsf{sk}_{\mathsf{GM}} \rangle$ and $\langle \mathsf{pk}_{\mathsf{OA}}, \mathsf{sk}_{\mathsf{OA}} \rangle$; $\mathtt{JOIN} = \langle \mathsf{J}_{\mathsf{user}}, \mathsf{J}_{\mathsf{GM}} \rangle$ is a protocol between a prospective group member and the GM. After an execution of a $\mathtt{JOIN}$ protocol the group member will output his public/secret-key pair $(\mathsf{pk}, \mathsf{sk})$; the new member's public-key pk along with a certificate cert will be published in the public directory $\mathsf{database}$ by the GM. We will denote by $\mathcal{L}_{pk}^{\mathsf{param}}$ the language of all valid public-keys where param is a public parameter produced by the $\mathtt{SETUP}_{\mathsf{init}}$ procedure.

To employ GE in a transaction, it is assumed that the sender (call her Alice) has obtained a pair (x, w) that is sampled according to the procedure $\mathsf{sample}_{\mathcal{R}}(\mathsf{pk}_{\mathcal{R}}, \mathsf{sk}_{\mathcal{R}})$, where $\mathsf{pk}_{\mathcal{R}}, \mathsf{sk}_{\mathcal{R}}$ are produced by the generation procedure $\mathcal{G}_{\mathsf{r}}(1^\nu)$ that samples the public/secret parameters for the relation $\mathcal{R}$. We remark that the secret-parameter $\mathsf{sk}_{\mathcal{R}}$ may be empty depending on the relation (e.g., in the case of discrete logarithm the relation is typically publicly samplable, hence $\mathsf{sk}_{\mathcal{R}}$ is empty – but this is not be the case in general). The polynomial-time testing procedure $\mathcal{R}(x, w)$ returns true iff (x, w) belongs to the relation based on the public-parameter $\mathsf{pk}_{\mathcal{R}}$. We note that given the relation $\mathcal{R}(\cdot,\cdot)$ it will be useful that it is hard to extract a "witness" w given an instance x; however this is not be included in the formal requirements for a GE scheme. Note that if verifiability is not desired from the GE, the relation $\mathcal{R}$ will be set to be the trivial relation that includes any string of a fixed size as a witness (and in such case x will be simply equal to $1^{|w|}$).

Alice possessing the pair (x, w), she wishes to encrypt w for her chosen receiver, call him Bob. She obtains Bob's certified public-key $\langle \mathsf{pk}, \mathsf{cert}\rangle$ from $\mathsf{database}$, and employing the public-keys $\mathsf{pk}_{\mathsf{GM}}$ and $\mathsf{pk}_{\mathsf{OA}}$ she encrypts w as $\mathtt{ENC}(\mathsf{pk}_{\mathsf{GM}}, \mathsf{pk}_{\mathsf{OA}}, \mathsf{pk}, w, L)$ to obtain the ciphertext ψ with a certain label L (L is a public string bound to the ciphertext that may contain some transaction related data or be empty; we call it the "context" of ψ). Alice will give x, ψ, L to the verifier. Subsequently, Alice and the verifier will engage in the proof of knowledge $\langle \mathcal{P}, \mathcal{V}\rangle$ that will ensure the following regarding the ciphertext ψ and label L: there exists a group member whose key is registered in the database (i.e., Bob in this case) that is capable of decrypting ψ in context L and obtaining a value w' for which it holds that if $w \leftarrow \mathsf{recon}(w')$ we have that $(x, w) \in \mathcal{R}$. Note that, for $\mathcal{P}, \mathcal{V}$, the input to the verifier will be the values $\mathsf{param}, \mathsf{pk}_{\mathsf{GM}}, \mathsf{pk}_{\mathsf{OA}}, \mathsf{pk}_{\mathcal{R}}, x, \psi, L$, whereas the prover (Alice) will have as additional input the values $\mathsf{pk}, \mathsf{cert}, w$ as well as the coin tosses used for the formation of ψ. The function $\mathsf{recon}(\cdot)$ reconstructs a witness based on the decryption of ψ and may be the identity function.

In the remaining of the section we give four definitions, correctness and the three security related properties of GE, security, anonymity, and soundness. For simulating two-party protocols we use the following notation: $\langle \mathsf{output}_A \mid \mathsf{output}_B\rangle \leftarrow \langle A(\mathsf{input}_A),\ B(\mathsf{input}_B)\rangle(\mathsf{common\_input})$.

Definition 2.1 (Correctness) *A GE scheme is correct if the following "correctness game" returns 1 with overwhelming probability.*

1. $\mathsf{param} \leftarrow \mathtt{SETUP}_{\mathsf{init}}(1^\nu)$; $\langle \mathsf{pk}_{\mathcal{R}}, \mathsf{sk}_{\mathcal{R}}\rangle \leftarrow \mathcal{G}_{\mathsf{r}}(1^\nu)$; $(x, w) \leftarrow \mathsf{sample}_{\mathcal{R}}(\mathsf{pk}_{\mathcal{R}}, \mathsf{sk}_{\mathcal{R}})$.
2. $\langle \mathsf{pk}_{\mathsf{GM}}, \mathsf{sk}_{\mathsf{GM}}\rangle \leftarrow \mathtt{SETUP}_{\mathsf{GM}}(\mathsf{param})$; $\langle \mathsf{pk}_{\mathsf{OA}}, \mathsf{sk}_{\mathsf{OA}}\rangle \leftarrow \mathtt{SETUP}_{\mathsf{OA}}(\mathsf{param})$;
3. $\langle \mathsf{pk}, \mathsf{sk}, \mathsf{cert} \mid \mathsf{pk}, \mathsf{cert}\rangle \leftarrow \langle \mathsf{J}_{\mathsf{user}}, \mathsf{J}_{\mathsf{GM}}(\mathsf{sk}_{\mathsf{GM}})\rangle(\mathsf{pk}_{\mathsf{GM}})$. If $\mathsf{pk} \notin \mathcal{L}_{pk}^{\mathsf{param}}$ then abort;
4. $\psi \leftarrow \mathtt{ENC}(\mathsf{pk}_{\mathsf{GM}}, \mathsf{pk}_{\mathsf{OA}}, \mathsf{pk}, \mathsf{cert}, w, L)$.
5. $\mathsf{out}_1 \leftarrow w \stackrel{?}{=} \mathsf{recon}(\mathtt{DEC}(\mathsf{sk}, \psi, L))$.
6. $\mathsf{out}_2 \leftarrow \mathsf{pk} \stackrel{?}{=} \mathtt{OPEN}(\mathsf{sk}_{\mathsf{OA}}, [\psi]_{\mathsf{oa}}, L)$.
7. $\langle \mathsf{done} \mid \mathsf{out}_3\rangle \leftarrow \langle \mathcal{P}(w, \psi, coins_\psi), \mathcal{V}\rangle(\mathsf{param}, \mathsf{pk}_{\mathsf{GM}}, \mathsf{pk}_{\mathsf{OA}}, \mathsf{pk}_{\mathcal{R}}, x, \psi, L)$.
8. if $(\mathsf{out}_1 = \mathsf{out}_2 = \mathsf{out}_3 = \mathsf{true})$ return 1.

As shown above the opening procedure $\mathtt{OPEN}$ may not operate on the ciphertext ψ but on a substring of the ciphertext ψ that is denoted by $[\psi]_{\mathsf{oa}}$; we make the distinction explicit as it is relevant in terms of chosen ciphertext security.

There are three "security notions" for GE schemes: security, anonymity and soundness (that includes verifiability). Security and anonymity are properties that protect Alice (the prover) against a system that acts against her.

2.1 Formulation of the Security Property

In our definitions we use a number of oracles: we distinguish between oracles that are stateless (those that maintain no state across queries) and those that are stateful (those that do maintain state). Stateful oracles are useful to express the adversarial interactions with the protocols that are used in our scheme. Next we introduce the decryption oracle, the challenge procedures and the prover simulator oracle.

$\mathsf{DEC}(\mathsf{sk}, \cdot)$: This is a stateless decryption oracle for the GE decryption function $\mathtt{DEC}$. The value sk is a secret-key that will be clarified from the context. If ψ is some "forbidden" ciphertext with label L that the oracle must reject we will write $\mathsf{DEC}^{\neg\langle\psi,L\rangle}(\mathsf{sk}, \cdot)$.

$\mathsf{CH}^b_{\mathsf{ror}}(1^\nu, \mathsf{pk}, w, L)$: This a real-or-random challenge procedure for the GE encryption scheme. It returns two values denoted as $\langle \psi, coins_\psi\rangle$ so that if $b = 1$ then $\psi \leftarrow \mathtt{ENC}(\mathsf{pk}_{\mathsf{GM}}, \mathsf{pk}_{\mathsf{OA}}, \mathsf{pk}, \mathsf{cert}, w, L)$, whereas if $b = 0$, $\psi \leftarrow \mathtt{ENC}(\mathsf{pk}_{\mathsf{GM}}, \mathsf{pk}_{\mathsf{OA}}, \mathsf{pk}, \mathsf{cert}, w', L)$ where w' is a plaintext sampled at random from the space of all possible plaintexts of length 1^ν for the encryption function (it is assumed at least two plaintexts exist). In either case $coins_\psi$ are the random coin tosses that are used for the computation of ψ.

$\mathsf{PROVE}^b_{\mathcal{P},\mathcal{P}'}(\mathsf{pk_{GM}}, \mathsf{pk_{OA}}, \mathsf{pk}, \mathsf{cert}, \mathsf{pk}_{\mathcal{R}}, x, w, \psi, L, coins_\psi)$: this is a stateful oracle that if $b = 1$, it simulates an execution of the prover procedure of $\mathcal{P}$ of the GE scheme (i.e., Alice), on $\mathsf{pk_{GM}}, \mathsf{pk_{OA}}, \mathsf{pk}, \mathsf{cert}, \mathsf{pk}_{\mathcal{R}}, x, w, \psi, L, coins_\psi$. On the other hand, if $b = 0$, it simulates the protocol $\mathcal{P}'$ that takes the same input as $\mathcal{P}$ with the exception of the values of w and $coins_\psi$ (the design of $\mathcal{P}'$ is part of proving the security property).

Based on the above three procedures we are ready to give the security definition, which is reminiscent of a real-or-random attack on the underlying encryption scheme. In the game below the adversary controls the GM and OA and all group members except the member that Alice chooses as her recipient, i.e., Bob. In fact, the adversary is the entity that introduces Bob into the group and issues a certificate for his public-key. Moreover, the adversary has CCA2 access to Bob's secret-key. The adversary also selects some public relation $\mathcal{R}$ based on $\mathsf{pk}_{\mathcal{R}}$ as well as a pair (x, w). Subsequently a coin is tossed and the adversary either receives the encryption of w and engages with Alice in the proof of ciphertext validity or the adversary receives an encryption of a random plaintext and engages in a simulated proof of validity. A GE would satisfy security if the adversary is unable to tell the difference. More formally (note that $\mathsf{negl}(\nu)$ is a function that for any c, is less than ν^{-c} for sufficiently large ν):

Definition 2.2 *A* GE *scheme satisfies* security *if there exists a protocol $\mathcal{P}'$ s.t. the "security game" below when instantiated by any PPT $\mathcal{A}$, returns 1 with probability less or equal to* $1/2 + \mathsf{negl}(\nu)$.

1. $\mathsf{param} \leftarrow \mathtt{SETUP}_{\mathsf{init}}(1^\nu)$; $\langle \mathsf{aux}, \mathsf{pk_{GM}}, \mathsf{pk_{OA}} \rangle \leftarrow \mathcal{A}(\mathsf{param})$;
2. $\langle \mathsf{pk}, \mathsf{sk}, \mathsf{cert} \mid \mathsf{aux} \rangle \leftarrow \langle \mathsf{J_{user}}, \mathcal{A}(\mathsf{aux}) \rangle(\mathsf{pk_{GM}})$;
3. $\langle \mathsf{aux}, x, w, L, \mathsf{pk}_{\mathcal{R}} \rangle \leftarrow \mathcal{A}^{\mathsf{DEC}(\mathsf{sk},\cdot)}(\mathsf{aux})$; *if* $(x, w) \notin \mathcal{R}$ *then abort;*
4. $b \xleftarrow{r} \{0, 1\}$; $\langle \psi, coins_\psi \rangle \leftarrow \mathsf{CH}^b_{\mathsf{ror}}(1^\nu, \mathsf{pk}, w, L)$;
5. $b^* \leftarrow \mathcal{A}^{\mathsf{PROVE}^b_{\mathcal{P},\mathcal{P}'}(\mathsf{pk_{GM}},\mathsf{pk_{OA}},\mathsf{pk},\mathsf{cert},\mathsf{pk}_{\mathcal{R}},x,w,\psi,L,coins_\psi),\mathsf{DEC}^{\neg\langle\psi,L\rangle}(\mathsf{sk},\cdot)}(\mathsf{aux}, \psi)$
6. *if* $b = b^*$ *return 1 else 0.*

2.2 Formulation of the Anonymity Property

In the anonymity attack the adversary controls the system except the opening authority. Anonymity can be thought of as a CCA2 attack against the encryption system of the OA. The adversary registers the two possible recipients into the PKI database and provides the relation and the witness to Alice. Alice will encrypt the same witness always as provided by the adversary but will use the key of one of the two recipients at random. The adversary, who has CCA2 decryption access to both recipients as well as teh OA, will have to guess which one of the two is Alice's choice. We define the following procedures:

$\mathsf{CH}^b_{\mathsf{anon}}(\mathsf{pk_{GM}}, \mathsf{pk_{OA}}, \mathsf{pk}_0, \mathsf{pk}_1, w, L)$: The challenge procedure receives a plaintext w and two public-keys $\mathsf{pk}_0, \mathsf{pk}_1$, and returns two values, $\langle \psi, coins_\psi \rangle$ so that $\psi \leftarrow \mathtt{ENC}(\mathsf{pk_{GM}}, \mathsf{pk_{OA}}, \mathsf{pk}_b, \mathsf{cert}_b, w, L)$ and $coins_\psi$ are the random coin tosses that are used for the computation of ψ.

$\mathsf{USER}(\mathsf{pk_{GM}})$: this is a stateful oracle that simulates two instantiations of $\mathsf{J_{user}}$, i.e., it is given $\mathsf{pk_{GM}}$ and simulates two users that wish to become members of the group; the oracle has access to a string denoted by keys in which USER will write the output of the two $\mathsf{J_{user}}$ instances.

$\mathsf{OPEN}(\mathsf{sk_{OA}}, \cdot)$: this is a stateless oracle that simulates the $\mathtt{OPEN}$ operation of the opening authority; recall that $\mathtt{OPEN}$ may not operate on the whole ciphertext ψ but rather on substring of it that will be denoted by $[\psi]_{\mathsf{oa}}$.

Definition 2.3 *A* GE *scheme satisfies* anonymity *if the following game instantiated for any PPT $\mathcal{A}$, it returns 1 with probability less or equal* $1/2 + \mathsf{negl}(\nu)$.

1. $\mathsf{param} \leftarrow \mathtt{SETUP}_{\mathsf{init}}(1^\nu)$; $\langle \mathsf{pk}_{\mathsf{OA}}, \mathsf{sk}_{\mathsf{OA}} \rangle \leftarrow \mathtt{SETUP}_{\mathsf{OA}}(\mathsf{param})$; $\langle \mathsf{pk}_{\mathsf{GM}}, \mathsf{aux} \rangle \leftarrow \mathcal{A}(\mathsf{param}, \mathsf{pk}_{\mathsf{OA}})$;
2. $\mathsf{aux} \leftarrow \mathcal{A}^{\mathsf{USER}(\mathsf{pk}_{\mathsf{GM}}),\mathsf{OPEN}(\mathsf{sk}_{\mathsf{OA}},\cdot)}(\mathsf{aux})$; *if* $\mathsf{keys} \neq \langle \mathsf{pk}_0, \mathsf{sk}_0, \mathsf{cert}_0, \mathsf{pk}_1, \mathsf{sk}_1, \mathsf{cert}_1 \rangle$ *then abort;*
3. $\langle \mathsf{aux}, x, w, L, \mathsf{pk}_{\mathcal{R}} \rangle \leftarrow \mathcal{A}^{\mathsf{OPEN}(\mathsf{sk}_{\mathsf{OA}},\cdot),\mathsf{DEC}(\mathsf{sk}_0,\cdot),\mathsf{DEC}(\mathsf{sk}_1,\cdot)}(\mathsf{aux})$; *if* $(x, w) \notin \mathcal{R}$ *then abort;*
4. $b \xleftarrow{r} \{0,1\}$; $\langle \psi, coins_\psi \rangle \leftarrow \mathsf{CH}^b_{\mathsf{anon}}(\mathsf{pk}_{\mathsf{GM}}, \mathsf{pk}_{\mathsf{OA}}, \mathsf{pk}_0, \mathsf{pk}_1, w, L)$;
5. $b^* \leftarrow \mathcal{A}^{\mathcal{P}(\mathsf{pk}_{\mathsf{GM}},\mathsf{pk}_{\mathsf{OA}},\mathsf{pk}_{\mathcal{R}},\mathsf{pk}_b,\mathsf{cert}_b,x,w,\psi,L,coins_\psi),\mathsf{OPEN}^{\neg\langle[\psi]_{\mathsf{oa}},L\rangle}(\mathsf{sk}_{\mathsf{OA}},\cdot),\mathsf{DEC}^{\neg\langle\psi,L\rangle}(\mathsf{sk}_0,\cdot),\mathsf{DEC}^{\neg\langle\psi,L\rangle}(\mathsf{sk}_1,\cdot)}(\mathsf{aux}, \psi)$;
6. *if* $b = b^*$ *return 1 else 0;*

This completes the security definition as far as Alice is concerned. From the point of view of the verifier, the goal of a malicious environment in which the verifier operates is to provide him with a ciphertext that encrypts a witness for a public relation that does not open to a witness even if all the group members apply their decryption function to it. Immunity to this attack, which we call soundness, guarantees that at least one group key will open to a valid witness.

2.3 Formulation of the Soundness Property

A soundness attack proceeds as follows: the adversary will create adaptively the group of recipients communicating with the GM. In this attack game, the adversary wins if, while playing the role of Alice, she convinces the verifier that a ciphertext is valid with respect to a public-relation $\mathcal{R}$ of the adversary's choice, but it holds that either (1) if the opening authority applies $\mathsf{sk}_{\mathsf{OA}}$ to the ciphertext the result is a value that is not equal to a public-key of any group member, or (2) the revealed key satisfies $\mathsf{pk} \notin \mathcal{L}^{\mathsf{param}}_{pk}$. To formalize soundness we introduce the following group registration oracle:

$\mathsf{REG}(\mathsf{sik}, \cdot)$: this is a stateful oracle that simulates J_{GM}, i.e., it is given $\mathsf{sk}_{\mathsf{GM}}$ and registers users in the group; the oracle has access to a string $\mathsf{database}$ that stores the public-keys and their certificates.

Definition 2.4 *A* GE *scheme satisfies* soundness *if the following "soundness game", when instantiated with any PPT adversary $\mathcal{A}$, the probability it returns 1 is negligible.*

1. $\mathsf{param} \leftarrow \mathtt{SETUP}_{\mathsf{init}}(1^\nu)$; $\langle \mathsf{pk}_{\mathsf{OA}}, \mathsf{sk}_{\mathsf{OA}} \rangle \leftarrow \mathtt{SETUP}_{\mathsf{OA}}(\mathsf{param})$; $\langle \mathsf{pk}_{\mathsf{GM}}, \mathsf{sk}_{\mathsf{GM}} \rangle \leftarrow \mathtt{SETUP}_{\mathsf{GM}}(\mathsf{param})$;
2. $\langle \mathsf{pk}_{\mathcal{R}}, x, \psi, L, \mathsf{aux} \rangle \leftarrow \mathcal{A}^{\mathsf{REG}(\mathsf{sk}_{\mathsf{GM}},\cdot)}(\mathsf{param}, \mathsf{pk}_{\mathsf{GM}}, \mathsf{pk}_{\mathsf{OA}}, \mathsf{sk}_{\mathsf{OA}})$;
3. $\langle \mathsf{aux}, \mathsf{out} \rangle \leftarrow \langle \mathcal{A}(\mathsf{aux}), \mathcal{V} \rangle(\mathsf{param}, \mathsf{pk}_{\mathsf{GM}}, \mathsf{pk}_{\mathsf{OA}}, \mathsf{pk}_{\mathcal{R}}, x, \psi, L)$;
4. $\mathsf{pk} \leftarrow \mathtt{OPEN}(\mathsf{sk}_{\mathsf{OA}}, [\psi]_{\mathsf{oa}}, L)$;
5. if $\mathsf{pk} \notin \mathsf{database}$ or $\mathsf{pk} \notin \mathcal{L}^{\mathsf{param}}_{pk}$ or $\psi \notin \mathcal{L}^{x,L,\mathsf{pk}_{\mathcal{R}},\mathsf{pk}_{\mathsf{GM}},\mathsf{pk}_{\mathsf{OA}},\mathsf{pk}}_{ciphertext}$ then return 1 else 0;

Note that $\mathcal{L}^{x,L,\mathsf{pk}_{\mathcal{R}},\mathsf{pk}_{\mathsf{GM}},\mathsf{pk}_{\mathsf{OA}},\mathsf{pk}}_{ciphertext} = \{\mathtt{ENC}(\mathsf{pk}_{\mathsf{GM}}, \mathsf{pk}_{\mathsf{OA}}, \mathsf{pk}, \mathsf{cert}, w, L) \mid w : (x, w) \in \mathcal{R}, \langle \mathsf{pk}, \mathsf{cert} \rangle \in \mathsf{Valid}\}$. This means that the soundness adversary wins if the key obtained by OA after opening is either not in the database, or is invalid, or the ciphertext ψ is not a valid ciphertext under pk encrypting a witness for x under $\mathcal{R}$.

A GE scheme should satisfy correctness, security, anonymity and soundness. Note that: (1) By defining the oracles USER and REG one can allow concurrent attacks or force sequential execution of the group registration process. (2) CPA variants of the security and anonymity definition w.r.t. either group members or the OA can be obtained by dropping the corresponding DEC oracles.

2.4 Related Primitives

Above we have presented the compound set of requirements for group encryption; we are now ready to compare it to prior cryptographic primitives which were originally designed to achieve only subsets of the group encryption's properties. Key-privacy was given in [BBDP01, Hal05] who showed that there exist encryption schemes where it is impossible for an adversary to distinguish what public-key has been used for the message encryption. Verifiable encryption on the other hand allows the sender to prove certain properties of the encrypted message (cf. [CS03] and references there). Finally, for the setting where users are encrypting with their own public keys (and thus, know the corresponding secret key), verifiable encryption was composed with key-privacy (called key-obliviousness) in [CL01a].

3 Necessary and Sufficient Conditions for GE schemes

Given that a GE scheme is a complex primitive it would be helpful to break down its construction to more basic primitives and provide a general methodology for constructing GE schemes. The necessary components for building a GE scheme will be the following:

1. Adaptively Chosen Message Secure Digital Signature. It will be used to generate the public-key certificates by the GM during the $\mathtt{JOIN}$ procedure.

2. Public-key Encryption with CCA2 Security and Key-Privacy. We will employ an encryption scheme $\langle \mathcal{G}_{\mathsf{e}}, \mathcal{E}, \mathcal{D} \rangle$ that satisfies (1) CCA2-security and (2) CCA2-Key-privacy. Refer to the appendix for definitions of these security notions. We note that in public-key encryption with key-privacy the key-generation has two components, one called $\mathcal{Z}_{\mathsf{e}}$ that produces public-parameters shared by all key-holders and the key-generation $\mathcal{G}_{\mathsf{e}}$ that given the public-parameter of the system produces a public/secret-key pair. Note that the inclusion of $\mathcal{Z}_{\mathsf{e}}$ is mandatory since some agreement between the receivers is necessary to enable key-privacy (at minimum all users should employ public-keys of the same length).

3. Proofs of Knowledge. Such protocols in the zero-knowledge setting satisfy three properties: completeness, soundness with knowledge extraction and zero-knowledge. These proofs exist for any NP language assuming one-way functions by reduction, e.g., to the graph 3-colorability proof of knowledge [Gol04]. In certain settings, zero-knowledge proofs can be constructed more efficiently by starting with a honest-verifier zero-knowledge (HVZK) proof of language membership protocol (i.e., a protocol that requires no knowledge extraction and it is only zero-knowledge against honest verifiers) and then coupling such protocol with an extractable commitment scheme (to achieve knowledge extraction) and with an equivocal commitment (to enforce zero-knowledge against dishonest verifiers, cf. [Dam00a]). See appendix 1.3 for more detailed definitions of the these standard primitives.

3.1 Modular Design of GE schemes

Consider an arbitrary relation $\langle \mathcal{G}_{\mathsf{r}}, \mathcal{R}, \mathsf{sample}_{\mathcal{R}} \rangle$. In the modular construction we will employ: (1) a digital signature scheme $\langle \mathcal{G}_{\mathsf{s}}, \mathcal{S}, \mathcal{V}_{\mathsf{s}} \rangle$ that is adaptively chosen message secure; (2) a public-key encryption scheme $\langle \mathcal{Z}_{\mathsf{e}}, \mathcal{G}_{\mathsf{e}}, \mathcal{E}, \mathcal{D} \rangle$ that satisfies CCA2 security and Key-privacy; (3) two zero-knowledge proofs of language membership (defined below); to facilitate knowledge extraction we will employ also an extractable commitment scheme $\langle \mathcal{Z}_{\mathsf{c},1}, \mathcal{C}_1, \mathcal{T}_1 \rangle$. Without loss of generality we will assume that all employed primitives operate over bitstrings. The construction of a GE scheme $\langle \mathtt{SETUP}, \mathtt{JOIN}, \langle \mathcal{G}_{\mathsf{r}}, \mathcal{R}, \mathsf{sample}_{\mathcal{R}} \rangle, \mathtt{ENC}, \mathtt{DEC}, \mathtt{OPEN}, \langle \mathcal{P}, \mathcal{V} \rangle, \mathsf{recon} \rangle$ is as follows:

$\mathtt{SETUP}$. The $\mathtt{SETUP}_{\mathsf{init}}$ procedure will select the parameters param by performing a sequential execution of $\mathcal{Z}_{\mathsf{e}}, \mathcal{Z}_{\mathsf{c},1}$. The $\mathtt{SETUP}_{\mathsf{GM}}$ procedure will be the signature-setup $\mathcal{G}_{\mathsf{s}}$ and the $\mathtt{SETUP}_{\mathsf{OA}}$ will be the encryption-setup $\mathcal{G}_{\mathsf{e}}$.

$\mathtt{JOIN}$. Each prospective user will execute $\mathcal{G}_{\mathsf{e}}$ to obtain pk, sk and then engage in a protocol $\langle \mathcal{P}_{pk}, \mathcal{V}_{pk} \rangle$ which is proof of language membership with the GM for the language $\mathcal{L}_{pk}^{\mathsf{param}} = \{\mathsf{pk} \mid \exists \mathsf{sk}, \rho : \langle \mathsf{pk}, \mathsf{sk} \rangle \leftarrow \mathcal{G}_{\mathsf{e}}(\mathsf{param}; \rho)\}$. The GM will respond with the signature $\mathsf{cert} \leftarrow \mathcal{S}(\mathsf{sk}_{\mathsf{GM}}, \mathsf{pk})$.

$\mathtt{ENC}$. The procedure $\mathtt{ENC}$ will perform the following given a witness w for a value x such that $(x, w) \in \mathcal{R}$ and a label L: it will return the pair $\psi =_{\mathsf{df}} \langle \psi_1, \psi_2, \psi_3, \psi_4 \rangle$ where $\psi_1 \leftarrow \mathcal{E}(\mathsf{pk}, w, L_1)$,

$\psi_2 \leftarrow \mathcal{E}(\mathsf{pk_{OA}}, \mathsf{pk}, L_2)$, $\psi_3 \leftarrow \mathcal{C}_1(\mathsf{cpk}, \mathsf{pk})$ $\psi_4 \leftarrow \mathcal{C}_1(\mathsf{cpk}, \mathsf{cert})$ where $L_1 = \psi_2||\psi_3||\psi_4||L$ and $L_2 = \psi_3||\psi_4||L$.

$\texttt{DEC}$. Given sk, a ciphertext $\langle\psi_1, \psi_2, \psi_3, \psi_4\rangle$ and a label L, it will return $\mathcal{D}(\mathsf{sk}, \psi_1, \psi_2||\psi_3||\psi_4||L)$.

$\texttt{OPEN}$. Given $\mathsf{sk_{OA}}$, a ciphertext $\langle\psi_2, \psi_3, \psi_4\rangle =_{\mathsf{df}} [\psi]_{\mathsf{oa}}$ and a label L it will return $\mathcal{D}(\mathsf{sk_{OA}}, \psi_2, \psi_3||\psi_4||L)$.

Finally, the protocol $\langle\mathcal{P}, \mathcal{V}\rangle$ is a zero-knowledge proof of language membership for the language:

$$\Big\{\langle \mathsf{param}, \mathsf{pk_{GM}}, \mathsf{pk_{OA}}, \mathsf{pk}_{\mathcal{R}}, x, \psi_1, \psi_2, \psi_3, \psi_4, L\rangle \mid \exists\, (coins_{\psi_1}, coins_{\psi_2}, coins_{\psi_3}, coins_{\psi_4}, \mathsf{pk}, \mathsf{cert}, w):$$

$$\wedge(\mathcal{C}_1(\mathsf{cpk}, \mathsf{pk}; coins_{\psi_3}) = \psi_3) \wedge (\mathcal{C}_1(\mathsf{cpk}, \mathsf{cert}; coins_{\psi_4}) = \psi_4) \wedge (\mathcal{V}_\mathsf{s}(\mathsf{pk}, \mathsf{cert}) = \mathsf{true})$$

$$\wedge(\mathcal{E}(\mathsf{pk}, w, (\psi_2||\psi_3||\psi_4||L); coins_{\psi_1}) = \psi_1) \wedge (\mathcal{E}(\mathsf{pk_{OA}}, \mathsf{pk}, (\psi_3||\psi_4||L); coins_{\psi_2}) = \psi_2) \wedge ((x, w) \in \mathcal{R})\Big\}$$

Note that the reconstruction procedure recon will be set to simply the identity function.

Theorem 3.1 *The* GE *scheme above satisfies (i)* Correctness*, given that all involved primitives are correct and the protocols* $\langle\mathcal{P}_{pk}, \mathcal{V}_{pk}\rangle, \langle\mathcal{P}, \mathcal{V}\rangle$ *satisfy completeness. (ii)* Anonymity*, given that the encryption scheme for users satisfies CCA2-key-privacy, the encryption scheme for OA satisfies CCA2-security, the commitment scheme* $\mathcal{C}_1$ *is hiding and the protocols* $\langle\mathcal{P}_{pk}, \mathcal{V}_{pk}\rangle$ *and* $\langle\mathcal{P}, \mathcal{V}\rangle$ *are zero-knowledge. (iii)* Security*, given that the employed encryption scheme for users satisfies CCA2-security, the commitment scheme* $\mathcal{C}_1$ *is hiding and the protocols* $\langle\mathcal{P}_{pk}, \mathcal{V}_{pk}\rangle$, $\langle\mathcal{P}, \mathcal{V}\rangle$ *are zero-knowledge. (iv)* Soundness*, given that the employed digital signature scheme satisfies adaptive chosen message security, the commitment scheme* $\mathcal{C}_1$ *is binding and extractable and the protocols* $\langle\mathcal{P}_{pk}, \mathcal{V}_{pk}\rangle$ *and* $\langle\mathcal{P}, \mathcal{V}\rangle$ *satisfy soundness.*

Proof. (i) correctness is easy and we omit the proof.
(ii) Let $\mathcal{A}$ be an anonymity attacker against the GE scheme. The anonymity game for the GE construction employed here can be rewritten as follows:

1. $\mathsf{param} \leftarrow \mathsf{SETUP_{init}}(1^\nu)$;
2. $\langle \mathsf{pk_{OA}}, \mathsf{sk_{OA}}\rangle \leftarrow \mathcal{G}_\mathsf{e}(\mathsf{param})$;
3. $\langle \mathsf{pk}_0, \mathsf{sk}_0\rangle \leftarrow \mathcal{G}_\mathsf{e}(\mathsf{param})$;
4. $\langle \mathsf{pk}_1, \mathsf{sk}_1\rangle \leftarrow \mathcal{G}_\mathsf{e}(\mathsf{param})$;
5. $\langle \mathsf{pk_{GM}}, \mathsf{aux}\rangle \leftarrow \mathcal{A}(\mathsf{param}, \mathsf{pk_{OA}})$;
6. $\langle \mathsf{aux}, \mathsf{cert}_0, \mathsf{cert}_1\rangle \leftarrow \mathcal{A}^{\mathcal{P}_{pk}(\mathsf{pk}_0,\mathsf{sk}_0),\mathcal{P}_{pk}(\mathsf{pk}_1,\mathsf{sk}_1),\mathsf{OPEN}(\mathsf{sk_{OA}},\cdot)}(\mathsf{aux}, \mathsf{pk}_0, \mathsf{pk}_1)$;
7. $\langle \mathsf{aux}, x, w, L, \mathsf{pk}_{\mathcal{R}}\rangle \leftarrow \mathcal{A}^{\mathsf{OPEN}(\mathsf{sk_{OA}},\cdot),\mathsf{DEC}(\mathsf{sk}_0,\cdot),\mathsf{DEC}(\mathsf{sk}_1,\cdot)}(\mathsf{aux})$; if $(x, w) \notin \mathcal{R}$ then abort;
8. $b \xleftarrow{\mathtt{r}} \{0, 1\}$;
9. $\langle \psi_1, \psi_2, \psi_3, \psi_4, coins_{\psi_1}, coins_{\psi_2}, coins_{\psi_3}, coins_{\psi_4}\rangle \leftarrow \mathsf{CH}^b_{\mathsf{anon}}(\mathsf{pk_{GM}}, \mathsf{pk_{OA}}, \mathsf{pk}_0, \mathsf{pk}_1, w, L)$;
10. $\psi \leftarrow \langle \psi_1, \psi_2, \psi_3, \psi_4\rangle$;
11. $coins_\psi \leftarrow \langle coins_{\psi_1}, coins_{\psi_2}, coins_{\psi_3}, coins_{\psi_4}\rangle$;
12. $b^* \leftarrow \mathcal{A}^{\mathcal{P}(\mathsf{pk_{GM}},\mathsf{pk_{OA}},\mathsf{pk}_{\mathcal{R}},\mathsf{pk}_b,\mathsf{cert}_b,x,w,\psi,L,coins_\psi),\mathsf{OPEN}^{\neg\langle[\psi]_{\mathsf{oa}},L\rangle}(\mathsf{sk_{OA}},\cdot),\mathsf{DEC}^{\neg\langle\psi,L\rangle}(\mathsf{sk}_0,\cdot),\mathsf{DEC}^{\neg\langle\psi,L\rangle}(\mathsf{sk}_1,\cdot)}(\mathsf{aux}, \psi)$;
13. if $b = b^*$ return 1 else 0;

Note that $\mathcal{P}_{pk}$ is an interactive prover machine for the language $\mathcal{L}^{\mathsf{param}}_{pk}$ and $\mathcal{P}$ is an interactive prover machine for the language $\mathcal{L}^{x,L,\mathsf{pk}_{\mathcal{R}},\mathsf{pk}_{GM},\mathsf{pk_{OA}},\mathsf{pk}}_{ciphertext}$.

The above game will be denoted by G_0. We will provide a sequence of modifications to this game till it is established that the probability the game returns 1 differs from 1/2 only by a negligible amount.

Consider the modification of the above game to game G_1 where the first of the two oracles available to $\mathcal{A}$ at step $\mathsf{6}$ is substituted with its zero-knowledge simulator. Clearly the distance between S_0 and

S_1 is bounded by the distance of the best polynomial-time distinguisher between the zero-knowledge protocol and its simulation. In a similar way we define G_2 as the game where the second oracle at step 6 is substitued with the zero-knowledge simulator. Game G_3 is defined in a similar way with the zero-knowledge simulator substituting protocol $\mathcal{P}$ at step 12. The resulting game G_3 has the following structure in the affected lines:

6. $\langle \mathsf{aux}, \mathsf{cert}_0, \mathsf{cert}_1 \rangle \leftarrow \mathcal{A}^{\mathcal{S}_{pk}(\mathsf{pk}_0), \mathcal{S}_{pk}(\mathsf{pk}_1), \mathsf{OPEN}(\mathsf{sk}_{\mathsf{OA}}, \cdot)}(\mathsf{aux}, \mathsf{pk}_0, \mathsf{pk}_1);$

12. $b^* \leftarrow \mathcal{A}^{\mathcal{S}(\mathsf{pk}_{\mathsf{GM}}, \mathsf{pk}_{\mathsf{OA}}, \mathsf{pk}_{\mathcal{R}}, x, \psi, L), \mathsf{OPEN}^{\neg\langle[\psi]_{\mathsf{oa}}, L\rangle}(\mathsf{sk}_{\mathsf{OA}}, \cdot), \mathsf{DEC}^{\neg\langle\psi, L\rangle}(\mathsf{sk}_0, \cdot), \mathsf{DEC}^{\neg\langle\psi, L\rangle}(\mathsf{sk}_1, \cdot)}(\mathsf{aux}, \psi);$

We proceed next to modify game G_3 to game G_4 so that the commitment ψ_3 is selected at random and the values ψ_1, ψ_2, ψ_4 are calculated directly (without going through the $\mathsf{CH}^b_{\mathsf{anon}}$ challenge procedure. In particular,

9. $\psi_1 \leftarrow \mathcal{E}(\mathsf{pk}_b, w, (\psi_2||\psi_3||\psi_4||L), coins_{\psi_1});$
10. $\psi_2 \leftarrow \mathcal{E}(\mathsf{pk}_{\mathsf{OA}}, \mathsf{pk}_b, (\psi_3||\psi_4||L), coins_{\psi_2});$
11. $\psi_3 \leftarrow \mathcal{C}_1(\mathsf{cpk}, r_3, coins_{\psi_3});\ r_3 \xleftarrow{r} \{0,1\}^l;\ \psi_4 \leftarrow \mathcal{C}_1(\mathsf{cpk}, \mathsf{cert}_b, coins_{\psi_4});\ \psi \leftarrow \langle \psi_1, \psi_2, \psi_3, \psi_4 \rangle;$

where l is the appropriate length employed for inputs to the commitment $\mathcal{C}_1(\mathsf{cpk}, \cdot)$. It is easy to show that based on the hiding property of $\mathcal{C}_1$ the distance between S_3 and S_4 is negligible. Next, we obtain game G_5 with a similar modification :

11. $\psi_3 \leftarrow \mathcal{C}_1(\mathsf{cpk}, r_3, coins_{\psi_3});\ \psi_4 \leftarrow \mathcal{C}_1(\mathsf{cpk}, r_4, coins_{\psi_4});\ r_3, r_4 \xleftarrow{r} \{0,1\}^l;\ \psi \leftarrow \langle \psi_1, \psi_2, \psi_3, \psi_4 \rangle;$

Again it is easy to show that based on the hiding properties of the commitment the distance S_4 and S_5 is negligible. Next we perform the following modification to obtain game G_6:

10. $\psi_2 \leftarrow \mathcal{E}(\mathsf{pk}_{\mathsf{OA}}, \mathsf{pk}_0, (\psi_3||\psi_4||L), coins_{\psi_2});$

Observe that games G_5 and G_6 are defined over the same probability space. Moreover if Z is the event $b = 0$ it is obvious that the two games are identical; from this we obtain that $\mathbf{Prob}[\mathsf{S}_5|\mathsf{Z}] = \mathbf{Prob}[\mathsf{S}_6|\mathsf{Z}]$. We consider next the two games conditioned on the event $\neg\mathsf{Z}$. The two games proceed identically to step 8. Then, G_5 executes the following code:

9. $\psi_1 \leftarrow \mathcal{E}(\mathsf{pk}_1, w, (\psi_2||\psi_3||\psi_4||L), coins_{\psi_1});$
10. $\psi_2 \leftarrow \mathcal{E}(\mathsf{pk}_{\mathsf{OA}}, \mathsf{pk}_1, (\psi_3||\psi_4||L), coins_{\psi_2});$
11. $\psi_3 \leftarrow \mathcal{C}_1(\mathsf{cpk}, r_3, coins_{\psi_3});\ \psi_4 \leftarrow \mathcal{C}_1(\mathsf{cpk}, r_4, coins_{\psi_4});\ r_3, r_4 \xleftarrow{r} \{0,1\}^l;\ \psi \leftarrow \langle \psi_1, \psi_2, \psi_3, \psi_4 \rangle;$
12. $b^* \leftarrow \mathcal{A}^{\mathcal{S}(\mathsf{pk}_{\mathsf{GM}}, \mathsf{pk}_{\mathsf{OA}}, \mathsf{pk}_{\mathcal{R}}, x, \psi, L), \mathsf{OPEN}^{\neg\langle[\psi]_{\mathsf{oa}}, L\rangle}(\mathsf{sk}_{\mathsf{OA}}, \cdot), \mathsf{DEC}^{\neg\langle\psi, L\rangle}(\mathsf{sk}_0, \cdot), \mathsf{DEC}^{\neg\langle\psi, L\rangle}(\mathsf{sk}_1, \cdot)}(\mathsf{aux}, \psi);$
13. if $b^* = 1$ return 1 else 0;

The code executed by G_6 is identical but with line 10 switched to use the pk_0 key in the encryption of $\mathcal{E}(\mathsf{pk}_{\mathsf{OA}}, \cdot)$. Consider now the following adversary $\mathcal{B}$ that operates as follows: in a stage called `FIND`, it takes as input $\mathsf{pk}_{\mathsf{OA}}$ and param, it runs lines 3, 4, 5, 6, 7, 9, 11 of game G_5 simulating the oracles $\mathsf{DEC}(\mathsf{sk}_i, \cdot)$ internally (it knows both secret-keys) and using $\mathsf{OPEN}(\mathsf{sk}_{\mathsf{OA}}, \cdot)$ as an external oracle. Then $\mathcal{B}(\mathtt{FIND}, \cdot)$ terminates returning two challenge plaintexts $\mathsf{pk}_0, \mathsf{pk}_1$ as well as the auxiliary ifnormation $\mathsf{aux}' = \langle \mathsf{aux}, x, w, \mathsf{pk}_{\mathcal{R}} L, \psi_1, \psi_3, \psi_4 \rangle$ and the label $L' = \psi_3||\psi_4||L$. In a second stage, `GUESS` it receives a challenge ciphertext ψ_2 and using the auxiliary information aux' it proceeds in the simulation of lines 11, 12 using $\mathsf{OPEN}^{\neg\langle\psi_2,L_{\psi_2}\rangle}$ as an external oracle. Observe now that $\mathcal{B}$ is a CCA2 attacker against $\langle\mathcal{Z}_\mathsf{e},\mathcal{G}_\mathsf{e},\mathcal{E},\mathsf{D}\rangle$ public-key encryption scheme as employed by the opening authority.

Consider the CCA2-attack game that is launched by $\mathcal{B}$. Given that the two challenge plaintexts provided by $\mathcal{B}$ at the end of the FIND stage are $\mathsf{pk}_0,\mathsf{pk}_1$, it holds that if at the challenge stage the plaintext pk_0 is selected the output of $\mathcal{B}$ is identical to the output of G_6 whereas if pk_1 is selected, the output of $\mathcal{B}$ is identical to the output of G_5. Observe now the following: $|\mathbf{Prob}[\mathsf{G}^{\mathsf{cca2}}(1^\nu)=1]-\frac{1}{2}||=\frac{1}{2}|\mathbf{Prob}[\mathsf{G}^{\mathsf{cca2}}(1^\nu)=1\mid b=0]+\mathbf{Prob}[\mathsf{G}^{\mathsf{cca2}}(1^\nu)=1\mid b=1]-1|$. This in turn is equal to $\frac{1}{2}|\mathbf{Prob}[\mathsf{G}^{\mathsf{cca2}}(1^\nu)=0\mid b=0]-\mathbf{Prob}[\mathsf{G}^{\mathsf{cca2}}(1^\nu)=1\mid b=1]|=\frac{1}{2}|\mathsf{S}_5-\mathsf{S}_6|$. It follows that $|\mathsf{S}_5-\mathsf{S}_6|=2\cdot\mathsf{Adv}^{\mathsf{cca2}}_{\mathsf{sec}}(\nu)$.

Next, consider an adversary $\mathcal{B}'$ that operates as follows using the code of game G_6. In stage FIND it receives two public-keys $\mathsf{pk}_0,\mathsf{pk}_1$ and param and then executes lines 2, 5, 6, 7, 10, 11 of game G_6; during this stage it queries two external oracles $\mathsf{DEC}(\mathsf{sk}_i,\cdot)$ for $i=1,2$, while it simulates internally the oracle $\mathsf{OPEN}(\mathsf{sk}_{\mathsf{OA}},\cdot)$ (it knows the secret-key $\mathsf{sk}_{\mathsf{OA}}$). It returns the plaintext w as well as the label $L'=\psi_2||\psi_3||\psi_4||L$ and the auxiliary information $\mathsf{aux}'=\langle\mathsf{aux},x,L,\mathsf{pk}_\mathcal{R},\mathsf{pk}_0,\mathsf{pk}_1,\psi_2,\psi_3,\psi_4,\mathsf{pk}_{\mathsf{OA}},\mathsf{pk}_{\mathsf{GM}}\rangle$.

In a second stage GUESS, $\mathcal{B}$ receives a challenge ciphertext ψ_1 on context L' that is encrypted with one of the two public-keys $\mathsf{pk}_0,\mathsf{pk}_1$ at random. It simulates step 12 of gameG_6 and returns b^*.

It is easy to see that $\mathcal{B}'$ as described above is an CCA2-key-privacy attacker for the underlying cryptosystem $\mathcal{Z}_\mathsf{e},\mathcal{G}_\mathsf{e},\mathcal{E},\mathcal{D}$. It follows immediately that $|\mathsf{S}_6-\frac{1}{2}|\le\mathsf{Adv}^{\mathsf{cca2}}_{\mathsf{kp}}(1^\nu)$. This concludes the proof of anonymity.

(iii). Suppose that $\mathcal{A}$ is a security attacker against the GE scheme. The security game for the encryption scheme as defined in the theorem's statement is as follows

1. $\mathsf{param}\leftarrow\mathtt{SETUP}_{\mathsf{init}}(1^\nu)$;
2. $\langle\mathsf{aux},\mathsf{pk}_{\mathsf{GM}},\mathsf{pk}_{\mathsf{OA}}\rangle\leftarrow\mathcal{A}(\mathsf{param})$;
3. $\langle\mathsf{pk},\mathsf{sk}\rangle\leftarrow\mathcal{G}_\mathsf{e}(1^\nu)$;
4. $\langle\mathsf{aux},\mathsf{cert}\rangle\leftarrow\mathcal{A}^{\mathcal{P}_{pk}(\mathsf{pk},\mathsf{sk})}(\mathsf{aux},\mathsf{pk})$;
5. $\langle\mathsf{aux},x,w,L,\mathsf{pk}_\mathcal{R}\rangle\leftarrow\mathcal{A}^{\mathsf{DEC}(\mathsf{sk},\cdot)}(\mathsf{aux})$; if $(x,w)\notin\mathcal{R}$ then abort;
6. $b\xleftarrow{\mathtt{r}}\{0,1\}$;
7. $\psi_3\leftarrow\mathcal{C}_1(\mathsf{cpk},\mathsf{pk})$;
8. $\psi_4\leftarrow\mathcal{C}_1(\mathsf{cpk},\mathsf{cert})$;
9. $\psi_2\leftarrow\mathcal{E}(\mathsf{pk}_{\mathsf{OA}},\mathsf{pk},\psi_3||\psi_4||L)$;
10. if $b=1$ then $\psi_1\leftarrow\mathcal{E}(\mathsf{pk},w,\psi_2||\psi_3||\psi_4||L)$ else $\psi_1\leftarrow\mathcal{E}(\mathsf{pk},w',\psi_2||\psi_3||\psi_4||L)$; $w'\xleftarrow{\mathtt{r}}\{0,1\}^l$;
11. $\psi\leftarrow\langle\psi_1,\psi_2,\psi_3,\psi_4\rangle$;
12. $coins_\psi\leftarrow\langle coins_{\psi_1},coins_{\psi_2},coins_{\psi_3},coins_{\psi_4}\rangle$;
13. if $b=1$ then $b^*\leftarrow\mathcal{A}^{\mathcal{P}(\mathsf{pk}_{\mathsf{GM}},\mathsf{pk}_{\mathsf{OA}},\mathsf{pk}_\mathcal{R},\mathsf{pk},\mathsf{cert},x,w,\psi,L,coins_\psi),\mathsf{DEC}^{\neg\langle\psi,L\rangle}(\mathsf{sk},\cdot)}(\mathsf{aux},\psi)$;
    else $b^*\leftarrow\mathcal{A}^{\mathcal{S}(\mathsf{pk}_{\mathsf{GM}},\mathsf{pk}_{\mathsf{OA}},\mathsf{pk}_\mathcal{R},x,\psi,L),\mathsf{DEC}^{\neg\langle\psi,L\rangle}(\mathsf{sk},\cdot)}(\mathsf{aux},\psi)$;
14. if $b=b^*$ return 1 else 0;

Note that we use the simulator $\mathcal{S}$ as the prover $\mathcal{P}'$ mandated in the security definition for GE schemes (clearly $\mathcal{S}$ is more than sufficient for the task as not only it does not require w or $coins_\psi$ but also does not require $\mathsf{pk},\mathsf{cert}$). We call this game G_0.

We first modify game G_0 into a game G_1 so that line 13 is modified as follows:

13. $b^*\leftarrow\mathcal{A}^{\mathcal{S}(\mathsf{pk}_{\mathsf{GM}},\mathsf{pk}_{\mathsf{OA}},\mathsf{pk}_\mathcal{R},x,\psi,L),\mathsf{DEC}^{\neg\langle\psi,L\rangle}(\mathsf{sk},\cdot)}(\mathsf{aux},\psi)$;

Clearly this modification is indistinguishable as long as the event Z defined as $b=0$ is happening. On the other hand, in the conditional space $\neg\mathsf{Z}$ it follows easily that the events S_0 and S_1 will be statistically close based on the zero-knowledge property of protocol $\mathcal{P}$ (and its negligible distance from the simulator $\mathcal{S}$).

In a similar way we define game G_2 so that in step 4 we have the following modification:

4. $\langle \mathsf{aux}, \mathsf{cert}\rangle \leftarrow \mathcal{A}^{\mathcal{S}_{pk}(\mathsf{pk})}(\mathsf{aux}, \mathsf{pk})$;

It is easy to see that the distance between G_1 and G_2 is bounded by the distance between the zero-knowledge simulator $\mathcal{S}$ from $\mathcal{P}_{pk}$.

Next consider the following procedure $\mathcal{B}$: in a first stage FIND it takes as input a public-key $\mathsf{param}, \mathsf{pk}$; then it simulates steps $2, 4, 5, 7, 8, 9$ using an external oracle $\mathsf{DEC}(\mathsf{sk}, \cdot)$ and returns a tuple $\langle \mathsf{aux}', w, L'\rangle$. where $\mathsf{aux}' = \mathsf{aux}||\mathsf{pk}_{\mathsf{GM}}||\mathsf{pk}_{\mathsf{OA}}||\mathsf{pk}_{\mathcal{R}}$, $L' = \psi_2||\psi_3||\psi_4||L$. Then $\mathcal{B}$ receives a challenge ciphertext ψ_1 and executes the steps $11, 13$ of game G_2 using an external oracle $\mathsf{DEC}^{\neg\langle \psi_1, L'\rangle}$ (which can be used to simulate the $\mathsf{DEC}^{\neg\langle \psi, L\rangle}$ oracle required from $\mathcal{A}$) and returns b^*.

It is easy to see that $\mathcal{B}$ is a real-or-random CCA2 attacker against the public-key encryption $\langle \mathcal{G}'_{\mathsf{e}}, \mathcal{E}, \mathcal{D}\rangle$ with $\mathcal{G}'_{\mathsf{e}}$ being the parallel composition of $\mathtt{SETUP}_{\mathsf{init}}$ and $\mathcal{G}_{\mathsf{e}}$. It follows easily from this that S_2 will be bounded by $\mathsf{Adv}^{\mathsf{cca2}}_{ind}(\nu)$ which completes the proof for item (iii).
(iv). Given a soundness attacker for GE we construct an adaptive chosen message attacker $\mathcal{B}$ for the employed digital signature algorithm $\langle \mathcal{G}_{\mathsf{s}}, \mathcal{S}, \mathcal{V}_{\mathsf{s}}\rangle$. $\mathcal{B}$ is given first $\mathsf{pk}_{\mathsf{GM}}$. $\mathcal{B}$ samples param for the GE scheme so that the commitment scheme $\mathcal{C}_1$ becomes extractable (i.e., $\mathcal{B}$ will possess the trapdoor). $\mathcal{B}$ also samples $\mathsf{pk}_{\mathsf{OA}}, \mathsf{sk}_{\mathsf{OA}}$. Then $\mathcal{B}$ starts the simulation of $\mathcal{A}$ on param and $\mathsf{pk}_{\mathsf{OA}}$; in order to simulate $\mathcal{A}$, the oracle REG needs to be simulated. This is done as follows: first it receives a candidate public-key pk by $\mathcal{A}$, then $\mathcal{A}$ starts the proof of language membership for the public-key pk; $\mathcal{B}$ playing the role of the verifier, if it accepts the proof it forwards pk to its signing oracle $\mathcal{S}(\mathsf{sk}_{\mathsf{GM}}, \cdot)$ otherwise it rejects the public-key pk. Based on the soundness properties of the proof of knowledge with overwhelming probability only $\mathsf{pk} \in \mathcal{L}^{\mathsf{param}}_{pk}$ will be forwarded to the signing oracle $\mathcal{S}(\mathsf{sk}_{\mathsf{OA}}, \cdot)$.

In this way $\mathcal{B}$ obtains from $\mathcal{A}$ the tuple $\langle \mathsf{pk}_{\mathcal{R}}, x, \psi, L, \mathsf{aux}\rangle$ where $\psi = \langle \psi_1, \psi_2, \psi_3, \psi_4\rangle$. Subsequently $\mathcal{B}$ continues the simulation of $\mathcal{A}$ that has access to the verifier oracle $\mathcal{V}$. Upon termination of the simulation, $\mathcal{B}$ using the extractability of the commitment scheme it obtains the values $\mathsf{pk}, \mathsf{cert}$ from ψ_3, ψ_4 respectively. Based on the soundness of the proof of ciphertext validity protocol it holds that $\mathcal{V}_{\mathsf{s}}(\mathsf{pk}_{\mathsf{GM}}, \mathsf{pk}, \mathsf{cert}) = \mathsf{true}$ i.e., the pair $(\mathsf{pk}, \mathsf{cert})$ is a valid digital signature for the scheme that is being attacked by $\mathcal{B}$. Moreover it holds that $\mathsf{pk} = \mathtt{DEC}(\mathsf{sk}_{\mathsf{OA}}, \psi)$.

Now it holds that based on the soundness property of $\langle \mathcal{P}_{\mathsf{pk}}, \mathcal{V}_{\mathsf{pk}}\rangle$ we have that $\mathsf{pk} \in \mathcal{L}^{\mathsf{param}}_{pk}$; moreover based on the soundness of $\mathcal{P}, \mathcal{V}$ we have that $(x, \mathtt{DEC}(\mathsf{sk}, \psi)) \in \mathcal{R}$. It follows that if the adversary wins it must be that $pk \notin \mathsf{database}$ and thus it is a forgery of the underlying digital signature scheme $\langle \mathcal{G}_{\mathsf{s}}, \mathcal{S}, \mathcal{V}_{\mathsf{s}}\rangle$. ■

The above theorem has as direct corollary the feasibility of GE in the generic sense.

3.2 Necessity of the basic primitives

Next we deal with the question whether GE by itself would yield a public-key encryption scheme, a digital signature and in general any of the components we employed for the GE modular design in the theorem above; we find that these sufficient components are also in fact necessary; in particular we will show that most GE schemes would imply them. Given that a GE scheme is used to encrypt witnesses for a relation $\mathcal{R}$ it should be the case that the witnesses for statements of the relation $\mathcal{R}$ are unpredictable for an adversary. We formalize this notion below:

Definition 3.2 *Given a relation $\langle \mathcal{G}_{\mathsf{r}}, \mathcal{R}, \mathsf{sample}_{\mathcal{R}}\rangle$, a deterministic predicate B is called a hard-to-guess predicate for the relation $\mathcal{R}$ if the following holds for any PPT $\mathcal{A}$:*

$$|\mathbf{Prob}[\mathcal{A}(x) = \mathsf{B}(w)] - \frac{1}{2}| = \mathsf{negl}(\nu)$$

where $\langle \mathsf{pk}_{\mathcal{R}}, \mathsf{sk}_{\mathcal{R}}\rangle \leftarrow \mathcal{G}_{\mathsf{r}}(1^{\nu})$ and $(x, w) \leftarrow \mathsf{sample}_{\mathcal{R}}(\mathsf{pk}_{\mathcal{R}}, \mathsf{sk}_{\mathcal{R}})$.

While a hard-to-guess predicate coincides with the notion of a hard-core bit of a strong one-way function (when the relation $\mathcal{R}$ is a function), in general it is fairly simple to consruct relations that have hard-to-guess predicates without relying on any complexity assumption; for example, the relation $\mathcal{R}$ that contains (ν, w) such that $|w| = \nu$; for $\nu \geq 1$ a random witness of the relation will satisfy that all its bits are hard-to-guess for any adversary. Moreover, we note that the above definition, while sufficient for showing that group encryption implies public-key encryption with key-privacy, it is not necessary and it is possible to weaken the hard-to-guess formulation further (to become equivalent to a weak one-way function hard bit); in this case, one would need to apply standard techniques of amplification [Yao82, GIL$^+$90].

We proceed to the statement of the necessity of public-key encryption that is CCA2-secure and key-private as well as of digital signatures based on a given GE scheme.

Theorem 3.3 *The existence of a* GE *scheme implies (i) public key encryption with CCA2-security based on the anonymity of the* GE *scheme, (ii) public-key encryption with CCA2-security and CCA2-key-privacy based on the security of the* GE *scheme provided that the relation* $\mathcal{R}$ *possesses a hard-to-guess predicate* B*; moreover, (iii) adaptive chosen message secure digital signature, (iv) extractable commitments and (v) zero-knowledge proofs for any* NP*-language.*

Proof. Consider a GE scheme :

$$\Big\langle \mathtt{SETUP}, \mathtt{JOIN}, \langle \mathcal{G}_{\mathsf{r}}, \mathcal{R}, \mathsf{sample}_{\mathcal{R}} \rangle, \mathtt{ENC}, \mathtt{DEC}, \mathtt{OPEN}, \langle \mathcal{P}, \mathcal{V}, \mathsf{recon} \rangle \Big\rangle$$

(i) We first build a cryptosystem based on the anonymity property of the GE scheme. In this case the system will be based on the following components $\langle \mathtt{SETUP}_{\mathsf{init}} || \mathtt{SETUP}_{\mathsf{OA}} || \mathtt{SETUP}_{\mathsf{GM}} || \mathcal{G}_{\mathsf{r}} || \mathsf{J}_{\mathsf{user}} || \mathsf{J}_{\mathsf{GM}}, \mathtt{ENC}'', \mathtt{DEC}'' \rangle$. The public-key of the system is param and $\mathsf{pk}_{\mathsf{OA}}$ as well as $\mathsf{sk}_{\mathsf{OA}}, \mathsf{pk}_{\mathcal{R}}, \mathsf{sk}_{\mathcal{R}}$. The procedure $\mathtt{SETUP}_{\mathsf{GM}}$ is executed to obtain $\mathsf{pk}_{\mathsf{OA}}, \mathsf{sk}_{\mathsf{OA}}$ and then the protocol $\mathsf{J}_{\mathsf{user}}, \mathsf{J}_{\mathsf{GM}}$ is simulated a sufficient number of times so that at least two distinct $\mathsf{pk}_0, \mathsf{sk}_0, \mathsf{pk}_1, \mathsf{sk}_1$ pairs of public-keys are produced together with their corresponding certificates $\mathsf{cert}_0, \mathsf{cert}_1$.

The encryption function $\mathtt{ENC}''$ employs $\mathsf{sample}_{\mathcal{R}}(\mathsf{pk}_{\mathcal{R}}, \mathsf{sk}_{\mathcal{R}})$ to sample (x, w) and then encrypts a message $m \in \{0, 1\}$ with label L as follows $\psi \leftarrow \mathtt{ENC}(\mathsf{pk}_{\mathsf{GM}}, \mathsf{pk}_{\mathsf{OA}}, \mathsf{pk}_m, \mathsf{cert}_m, w, L)$. To decrypt a ciphertext the receiver applies $\mathtt{OPEN}$ to obtain pk_m and then recovers m by comparing pk_m to $\mathsf{pk}_0, \mathsf{pk}_1$. Extending the message space to $\{0, 1\}^{\log \nu}$ is trivial. It is easy to see that the security of the cryptosystem is directly based on the anonymity property of the GE scheme.

(ii) Next we show how to build a public-key cryptosystem relying only on the security property of a GE scheme. In particular, we will show that $\langle \mathtt{SETUP}_{\mathsf{init}} || \mathtt{SETUP}_{\mathsf{GM}} || \mathtt{SETUP}_{\mathsf{OA}}, \mathsf{J}_{\mathsf{user}} || \mathsf{J}_{\mathsf{GM}} || \mathcal{G}_{\mathsf{r}}, \mathtt{ENC}', \mathtt{DEC}' \rangle$ constitutes a CCA2-key private CCA2-secure public-key encryption scheme. The public-parameters of the encryption scheme will be $\langle \mathsf{param}, \mathsf{pk}_{\mathsf{OA}}, \mathsf{sk}_{\mathsf{OA}}, \mathsf{pk}_{\mathsf{GM}}, \mathsf{sk}_{\mathsf{OA}}, \mathsf{pk}_{\mathcal{R}}, \mathsf{sk}_{\mathcal{R}} \rangle$ as produced by the corresponding procedures of the GE scheme. A receiver, in order to construct its public/secret-key pair, it simulates locally the $\mathsf{J}_{\mathsf{user}}, \mathsf{J}_{\mathsf{GM}}$, $\mathtt{JOIN}$ protocol to obtain $\mathsf{pk}, \mathsf{sk}, \mathsf{cert}$. The public-key is set to $\mathsf{pk}, \mathsf{cert}$ and the secret-key is sk.

The message space of the cryptosystem will be $\{0, 1\}$. The encryption $\mathtt{ENC}'$ of a message m with context L is as follows: the sender samples (x, w) according to $\mathsf{sample}_{\mathcal{R}}(\mathsf{pk}_{\mathcal{R}}, \mathsf{sk}_{\mathcal{R}})$ until it holds that $\mathsf{B}(w) = m$. Then it forms the ciphertext $\psi \leftarrow \mathtt{ENC}(\mathsf{pk}_{\mathsf{GM}}, \mathsf{pk}_{\mathsf{OA}}, \mathsf{pk}, \mathsf{cert}, w, L)$. The decryption operation employs $\mathtt{DEC}$ as well as B to recover the message m from w. Note that the expected number of trials till the sender obtains some pair (x, w) from $\mathsf{sample}_{\mathcal{R}}(\mathsf{pk}_{\mathcal{R}}, \mathsf{sk}_{\mathcal{R}})$ is 2; otherwise it would be the case that a trivial adversary that always returns the same value would violate the hard-to-guess property of the predicate B.

The CCA2-security and CCA2-key-privacy of the cryptosystem as described above follows directly from the security and anonymity property respectively of the underlying GE scheme.

(iii) The existence of a digital signature scheme follows easily using the result of item (i) above that states that GE implies a CCA2 public-key encryption scheme. A CCA2 encryption scheme implies immediately that the encryption function is a one-way mapping from the set of coins and plaintexts to the set of ciphertexts. One-way functions imply adaptively secure digital signatures [NY89, Rom90].

Finally, recall that (i) extractable commitments follow directly from public-key encryption, (ii) zero-knowledge proofs for any NP-language follow from commitments [GMW91]. ■

4 Efficient GE of Discrete-Logarithms

In this section we will consider the discrete-logarithm relation $\langle \mathcal{G}_{\mathsf{dl}}, \mathcal{R}_{\mathsf{dl}}, \mathsf{sample}_{\mathsf{dl}} \rangle$: $\mathcal{G}_{\mathsf{dl}}$ given 1^ν samples a description of a cyclic group of ν-bits order and a generator γ of that group; $\mathcal{R}$ contains pairs of the form (x, w) where $x = \gamma^w$; note that $\mathsf{pk}_{\mathcal{R}} = \langle \mathrm{desc}(G), \gamma \rangle$ and $\mathsf{sk}_{\mathcal{R}}$ is empty. Finally $\mathsf{sample}_{\mathsf{dl}}$ on input $\mathsf{pk}_{\mathcal{R}}$ selects a witness w and returns the pair $(x = \gamma^w, w)$. In this section we will present a GE scheme for the above relation. Note that the results of this section can be easily extended to other relations based on discrete-logs such as a commitment to w.

4.1 Design of a public-key encryption for discrete-logarithms with key-privacy and security

One of the hurdles in designing a GE for discrete-logarithms is finding a suitable encryption scheme for the group members. In this section we will present a public-key encryption scheme that is suitable for verifiable encryption of discrete-logarithms while it satisfies CCA2-key-privacy and CCA2-security. The scheme is related to previous public-key encryption schemes of [CS98, Pai99, GL03, CS03] and it is the first Paillier-based public-key encryption that satisfies key-privacy and security against chosen ciphertext attacks. Below we give a detailed description of our public-key encryption $\langle \mathcal{Z}_{\mathsf{e}}, \mathcal{G}_{\mathsf{e}}, \mathcal{E}, \mathcal{D} \rangle$ and of the accompanying intractability assumptions that ensure its properties.

Public-parameters. The parameter selection function $\mathcal{Z}_{\mathsf{e}}$, given 1^ν selects a composite modulus $n = pq$ so that n is a ν-bit number, $p = 2p' + 1, q = 2q' + 1$ and p, p', q, q' are all prime numbers with p, q of equal size at least $\lfloor \nu/2 \rfloor + 1$. Then it samples $g \leftarrow \mathbb{Z}^*_{n^2}$ and computes $g_1 \leftarrow g^{2n}(\mathrm{mod} n^2)$. Observe that $\langle g_1 \rangle$ with very high probability is a subgroup of order $p'q'$ within $\mathbb{Z}^*_{n^2}$. In such case $\langle g_1 \rangle$ is a group that contains all square n-th residues of $\mathbb{Z}^*_{n^2}$ and we will call this group $\mathcal{X}_{n^2}$. We note further that all elements of $\mathbb{Z}^*_{n^2}$ can be written in a unique way in the form $g_1^r(1+n)^v(-1)^\alpha(p_2p - q_2q)^\beta$ where $r \in [p'q'], v \in [n], \alpha, \beta \in \{0, 1\}$ (in this decomposition, p_2, q_2 are integers that satisfy $p_2p^2 \equiv_{q^2} 1, q_2q^2 \equiv_{p^2} 1$). We will denote by $\mathcal{Q}_{n^2}$ the subgroup of quadratic residues modulo n^2 which can be easily seen to contain all elements of the form $g_1^r(1+n)^v$ with $r \in \mathbb{Z}_{p'q'}$ and $v \in \mathbb{Z}_n$ and has order $np'q'$ (precisely one fourth of $\mathbb{Z}^*_{n^2}$ and is generated by $g_1(1+n)$). Note that we will use the notation $h =_{\mathsf{df}} 1 + n$. Finally, a second value g_2 is selected as follows: w is sampled at random from $[\frac{n}{4}] =_{\mathsf{df}} \{0, \ldots, \lfloor \frac{n}{4} \rfloor\}$ and we set $g_2 \leftarrow g_1^w$. A random member $\mathcal{H}$ of a universal one-way hash function family UOWHF is selected [NY89]; the range of $\mathcal{H}$ is assumed to be $[0, 2^{\nu/2-2})$. The global parameters of the cryptosystem that will be shared by all recipients are equal to $\mathsf{param} = \langle n, g_1, g_2, \mathrm{desc}\mathcal{H} \rangle$, where $\mathrm{desc}\mathcal{H}$ is the description of $\mathcal{H}$.

Key-Generation. The key-generation algorithm $\mathcal{G}_{\mathsf{e}}$ receives the parameters $\langle n, g_1, g_2, \mathrm{desc}\mathcal{H} \rangle$, samples $x_1, x_2, y_1, y_2 \leftarrow_R [\frac{n^2}{4}]$ and sets $\mathsf{pk} = \langle c, d, y \rangle$ where $c = g_1^{x_1} g_2^{x_2}$, $d = g_1^{y_1} g_2^{y_2}$ and $y = g_1^z$; the secret-key is $\mathsf{sk} = \langle x_1, x_2, y_1, y_2, z \rangle$. Note that below we may include the string param as part of the pk and sk strings to avoid repeating it, nevertheless it should be recalled in all cases that $n, g_1, g_2, \mathrm{desc}\mathcal{H}$ are global parameters that are available to all parties.

Encryption. The encryption function $\mathcal{E}$ operates as follows: given the pk, a message w and a label L it samples $r \leftarrow_R [\frac{n}{4}]$ and outputs the triple $\langle u_1, u_2, e, v\rangle$ computed as follows: $u_1 \leftarrow g_1^r \bmod n^2$, $u_2 \leftarrow g_2^r \bmod n^2$, $e \leftarrow y^r(1+n)^w \bmod n^2$, $v \leftarrow ||c^r d^{r\mathcal{H}(u_1,u_2,e,L)} \bmod n^2||$ where $||\cdot|| : \mathbb{Z}_{n^2}^* \rightarrow \mathbb{Z}_{n^2}^*$ is defined as follows $||x|| = x$ if $x \leq n^2/2$ and $||x|| = -x$ if $x > n^2/2$. We note that the "absolute value" function $||\cdot||$ is used to disallow the malleability of a ciphertext with respect to multiplication with -1 (cf. the decryption test below). To summarize, encryption works as follows:

$$r \leftarrow_R \left[\frac{n}{4}\right] \quad : \quad u_1 \leftarrow g_1^r \quad u_2 \leftarrow g_2^r \quad e \leftarrow y^r h^m \quad v \leftarrow ||c^r d^{r\mathcal{H}(u_1,u_2,e,L)}||$$

Decryption. The decryption function $\mathcal{D}$ given a ciphertext (u_1, u_2, e, v) and a label L it performs the following checks:

$$v \stackrel{?}{=} ||v|| \qquad \wedge \qquad v^2 \stackrel{?}{=} (u_1^{x_1} u_2^{x_2})^2 (u_1^{y_1} u_2^{y_2})^{2\mathcal{H}(u_1,u_2,e,L)}$$

if all tests pass it computes $m' = e^2 {u_1}^{-2z} - 1 (\bmod n^2)$ and returns $(m' \cdot 2^{-1} \bmod n)/n$, otherwise it returns $\perp$.

This completes the description of the cryptosystem. Observe that the cryptosystem is correct, i.e., encryption inverts decryption: indeed, assuming that $\langle u_1, u_2, e, v\rangle \leftarrow \mathcal{E}(\mathsf{pk}, w, L)$, we have that $m' = e^2 u_1^{-2z} - 1 \equiv_{n^2} h^{2w} - 1$ and due to the fact that $h^x \equiv_{n^2} 1 + xn$ for all $x \in \mathbb{Z}_n$ we have that $w' \equiv_{n^2} (2m \bmod n) \cdot n$. It follows that $(w' \cdot 2^{-1} \bmod n)/n = w$.

We will next argue about the security of the cryptosystem. We note that the above cryptosystem has a "double trapdoor" property: for each public-key, c, d, y, based on parameters $n, g_1, g_2, \mathrm{desc}\mathcal{H}$, one trapdoor is the discrete-logarithm of y base g_1, whereas the the other trapdoor is the factorization of n. Indeed given the factorization of n, one can easily decrypt any ciphertext $\langle u_1, u_2, e, v\rangle$ by computing $e^{p'q'} \equiv_{n^2} h^{p'q'm}$. Subsequently m can be computed easily similarly to the regular decryption function. In GE the global trapdoor will not be used and the factorization of n will be assumed unknown by all parties. The intractability assumption that will be employed is the following:

Definition 4.1 *The* Decisional Composite Residuosity DCR *assumption [Pai99]: It is computationally hard to distinguish between: (i) tuples of the form* $(n, u^n \bmod n^2)$ *where* n *is a composite RSA modulus and* $u \leftarrow_R \mathbb{Z}_{n^2}^*$*, and (ii) tuples of the form* (n, v) *where* $v \leftarrow_R \mathbb{Z}_{n^2}^*$*.*

Next, we prove $\mathsf{IND\text{-}CCA2}$ security under the DCR.

Theorem 4.2 *The cryptosystem* $\langle \mathcal{Z}_{\mathsf{e}}, \mathcal{G}_{\mathsf{e}}, \mathcal{E}, \mathcal{D}\rangle$ *defined above satisfies CCA2-security under the* DCR *assumption and the target collision resistance of the employed* UOWH *family.*

Proof. (of theorem 4.2) We define a sequence of games, starting from game G_0 being the game corresponding to the $\mathsf{IND\text{-}CCA2}$ attack game according to the definition (see below).

1. $\mathsf{param} \leftarrow \mathcal{Z}(1^\nu)$.
2. $\langle \mathsf{pk}, \mathsf{sk}\rangle \leftarrow \mathcal{G}_{\mathsf{e}}(\mathsf{param})$.
3. $\langle m_0, m_1, \mathsf{aux}, L\rangle \leftarrow \mathcal{A}^{\mathcal{D}(\mathsf{sk},\cdot)}(\mathtt{FIND}, \mathsf{pk})$.
4. if $m_0 = m_1$ then abort;
5. $b \leftarrow_R \{0, 1\}$.
6. $\psi^* \leftarrow \mathcal{E}(\mathsf{pk}, m_b, L)$.
7. $b^* \leftarrow \mathcal{A}^{\mathcal{D}^{\neg\psi}(\mathsf{sk},\cdot)}(\mathtt{GUESS}, \psi^*, \mathsf{aux})$.

For the cryptosystem at hand the game looks as follows:

1. $\langle n, g_1, \mathsf{hk}\rangle \leftarrow \mathcal{Z}(1^\nu)$.
2. $g_2 \leftarrow g_1^w$; $w \xleftarrow{\mathtt{r}} [\frac{n}{4}]$
3. $c \leftarrow g_1^{x_1} g_2^{x_2}$; $x_1, x_2 \xleftarrow{\mathtt{r}} [\frac{n^2}{4}]$
4. $d \leftarrow g_1^{y_1} g_2^{y_2}$; $y_1, y_2 \xleftarrow{\mathtt{r}} [\frac{n^2}{4}]$
5. $y \leftarrow g_1^z$; $z \xleftarrow{\mathtt{r}} [\frac{n^2}{4}]$
6. $\mathsf{pk} = \langle c, d, y\rangle; \mathsf{sk} = \langle x_1, x_2, y_1, y_2, z\rangle$.
7. $\langle m_0, m_1, \mathsf{aux}, L^*\rangle \leftarrow \mathcal{A}^{\mathcal{D}(\mathsf{sk},\cdot)}(\mathtt{FIND}, \mathsf{pk})$.
8. $u_1^* \leftarrow g_1^r$; $u_2^* \leftarrow g_2^r$; $r \xleftarrow{\mathtt{r}} [\frac{n}{4}]$
9. $e^* \leftarrow y^r m_b$; $b \xleftarrow{\mathtt{r}} \{0,1\}$
10. $v^* \leftarrow c^r d^{r\mathsf{h}^*}$; $\mathsf{h}^* \leftarrow \mathcal{H}_{\mathsf{hk}}(u_1^*, u_2^*, e^*, L)$
11. $\psi^* = \langle u_1^*, u_2^*, e^*, v^*\rangle$
12. $b^* \leftarrow \mathcal{A}^{\mathcal{D}^{\neg\psi}(\mathsf{sk},\cdot)}(\mathtt{GUESS}, \psi^*, \mathsf{aux})$

We let S_0 be the event that the adversary is successful in game G_0, i.e., the event that $b = b^*$.

The decryption oracle operates as follows; first it performs the following test on a given ciphertext $\langle u_1, u_2, e, v\rangle$ and label L:

$$v \stackrel{?}{=} ||v|| \quad \wedge \quad v^2 \stackrel{?}{=} u_1^{2x_1+2y_1\mathsf{h}} u_2^{2x_2+2y_2\mathsf{h}}$$

where $\mathsf{h} = \mathcal{H}_{\mathsf{hk}}(u_1, u_2, e, L)$. If it passes it computes $m' = e^2 u_1^{-2z} - 1(\bmod n^2)$, and returns $(m'/2 \bmod n)/n$, otherwise it returns $\perp$. In the $\mathtt{GUESS}$ stage the oracle returns $\perp$ if the ciphertext $\langle u_1^*, u_2^*, e^*, v^*, L^*\rangle$ is given as a query.

Game G_1. This game modifies G_0 as follows.

The values c, d in the public-key are selected as $c \leftarrow g_1^{x'}, d \leftarrow g_1^{y'}$ where $x' = x_1 + wx_2, y' = y_1 + wy_2$ (over the integers). Additionally, the decryption oracle is modified to operate as follows: given a ciphertext $\langle u_1, u_2, e, v\rangle$ and a label L, the check performed is defined as,

$$v \stackrel{?}{=} ||v|| \quad \wedge \quad (u_2)^2 \stackrel{?}{=} u_1^{2w} \quad \wedge \quad v^2 \stackrel{?}{=} u_1^{2x'+2y'\mathcal{H}_{\mathsf{hk}}(u_1,u_2,e,L)}$$

It is easy to see that the public-key elements c, d as defined in games G_0 and G_1 are identically distributed, thus the modification to the public-key values c, d will incur no change in the adversary's behavior. Arguing the same thing about the modification to the decryption oracle requires some more work.

Let us consider the event F to be the event that includes those coin tosses for which the adversary produces a query ciphertext $\psi = \langle u_1, u_2, e, v\rangle$ and a label L for which it holds that ψ is answered differently in games G_0 and game G_1. Given that the two games are identical as long as $\neg\mathsf{F}$ happens using a standard argument (cf. [CS98]) it is easy to see that $|\mathbf{Prob}[\mathsf{S}_0] - \mathbf{Prob}[\mathsf{S}_1]| \leq \mathbf{Prob}[\mathsf{F}]$. Next we will bound $\mathbf{Prob}[\mathsf{F}]$.

Consider the event F' to be the event that the adversary produces a query ciphertext $\langle u_1, u_2, e, v\rangle$ and a label L that passes the decryption test of G_0 but it is such that either $(u_1)^2 \notin \mathcal{X}_{n^2}$ or $(u_2)^2 \notin \mathcal{X}_{n^2}$. From standard probability it holds that $\mathbf{Prob}[\mathsf{F}] \leq \mathbf{Prob}[\mathsf{F} \cap \neg\mathsf{F}'] + \mathbf{Prob}[\mathsf{F}']$.

Observe that the event $\neg\mathsf{F}'$ suggests that the adversary either produces ciphertexts that fail the decryption test of G_0 or it holds that they pass the decryption test of G_0 and $(u_1)^2, (u_2)^2 \in \mathcal{X}_{n^2}$.

Claim. $\mathbf{Prob}[\mathsf{F} \cap \neg\mathsf{F}']$ is negligible assuming the hardness of factoring.

Suppose first that a ciphertext $\langle u_1, u_2, e, v\rangle$ with label L fails the decryption test of G_0. Then it holds that either $v \neq ||v||$ or $v^2 \neq (u_1^{2x_1+2y_1\mathsf{h}} u_2^{2x_2+2y_2\mathsf{h}})$. If $v \neq ||v||$ then we have that the ciphertext is also rejected in G_1 and thus this is not included in the event F. Assume now that the given ciphertext passes the test of game G_1. This implies that $v = ||v||$, $u_2^2 = u_1^{2w}$ as well as

$v^2 = u_1^{2x'+2y'\mathsf{h}}$ where $\mathsf{h} = \mathcal{H}_{\mathsf{hk}}(u_1, u_2, e, L)$. These relations translate to: $v^2 = u_1^{2(x_1+wx_2)+2\mathsf{h}(y_1+wy_2)} = (u_1^{x_1}u_2^{x_2})^2(u_1^{y_1}u_2^{y_2})^{2\mathsf{h}}$, which means that the same exact ciphertext $\langle u_1, u_2, e, v, L\rangle$ passes the test in game G_0, a contradiction. It follows that if a ciphertext fails the decryption test of G_0 then it also fails the decryption test of G_1. This suggests that the event $\mathsf{F}\cap\neg\mathsf{F}'$ contains the coin tosses for which all the adversary's ciphertexts pass the decryption test of game G_0, satisfy $(u_1)^2, (u_2)^2 \in \mathcal{X}_{n^2}$ and fail the decryption test of game G_1.

Since the test of game G_0 is passed we know that $v = ||v||$ and that $v^2 = (u_1)^{2x_1+2y_1\mathsf{h}}(u_2)^{2x_2+2y_2\mathsf{h}}$. It follows that it must be that $u_2^2 \neq u_1^{2w}$ since in the case $u_2^2 = u_1^{2w}$ the test of game G_1 would also be passed. As a result it must be the case that $u_2^2 \neq u_1^{2w}$, i.e., $\log_{g_1}(u_1)^2 \neq \log_{g_1}(u_2)^2$.

We will show that the probability of $\mathsf{F}\cap\neg\mathsf{F}'$ will be negligible assuming the hardness of factoring. Observe that the values x_1, x_2, y_1, y_2 are used only through $x' = x_1 + wx_2 \bmod p'q'$ and $y' = y_1 + wy_2 \bmod p'q'$ (for this it is necessary to use the condition that $(u_1)^2, (u_2)^2 \in \mathcal{X}_{n^2}$). It follows that in the view of the adversary during the `FIND` stage the values x_1, x_2, y_1, y_2 satisfy the following system of equations in $\mathbb{Z}_{p'q'}$, where $r_1 = \log_{g_1}(u_1)^2, r_2 = \log_{g_2}(u_2)^2$ and the third equation will be induced by any ciphertext $\langle u_1, u_2, v, e\rangle$ with label L that triggers the event $\mathsf{F}\cap\neg\mathsf{F}'$.

$$\begin{pmatrix} 1 & w & 0 & 0 \\ 0 & 0 & 1 & w \\ r_1 & wr_2 & r_1\mathsf{h} & wr_2\mathsf{h} \end{pmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \\ y_1 \\ y_2 \end{bmatrix} = \begin{bmatrix} \log_{g_1} c \\ \log_{g_1} d \\ \log_{g_1} v \end{bmatrix}$$

Observe that the above system contains a square matrix with determinant $w(r_2 - r_1)$ over $\mathbb{Z}_{p'q'}$ that it is non-zero inside $\mathbb{Z}_{p'q'}$. It follows that: (1) in the case that $w(r_1 - r_2) \in \mathbb{Z}^*_{p'q'}$ the system is of full rank and as a result the probability that the adversary can produce the third equation of the linear system above is negligible (given that it will bind one degree of freedom of x_1, x_2, y_1, y_2 beyond the two degrees bound in the system's public-key); (2) regarding the case that $w(r_1 - r_2) \notin \mathbb{Z}^*_{p'q'}$ we have the following: on the one hand, the probability that $\gcd(w, p'q') > 1$ is negligible (given the random choice of w); on the other hand, if $1 < \gcd(r_1 - r_2, p'q') < p'q'$ then we can use the adversary to obtain the value $\alpha = g_2^{r_1-r_2}$ that will have order that belongs to $\{p', q'\}$ and as a result $\gcd(\alpha - 1, n) \in \{p, q\}$ i.e., we can split n. During the `GUESS` stage the above arguments lead to an identical conclusion. We conclude that under the assumption that factoring is hard the event $\mathsf{F}\cap\neg\mathsf{F}'$ is negligible probability event and this concludes the proof of the claim.

Claim. $\mathbf{Prob}[\mathsf{F}']$ is negligible.

We will split the event F' in a number of events F'_j that suggest that the adversary succeeds in triggering the event F' for the first time in the j-th query. It will follow from the union bound that $\mathbf{Prob}[\mathsf{F}'] \leq \sum_j \mathbf{Prob}[\mathsf{F}'_j]$. Each event F'_j is defined as follows: j is the first ciphertext query posed by the adversary for which it holds that the ciphertext passes the decryption test of game G_0 but $(u_1)^2 \notin \mathcal{X}_{n^2}$ or $(u_2)^2 \notin \mathcal{X}_{n^2}$. Consider integers $r_1, r_2 \in \mathbb{Z}_{p'q'} s_1, s_2 \in \mathbb{Z}_n$ such that $u_1^2 = g_1^{r_1}h^{s_1}$ and $u_2^2 = g_1^{r_2}h^{s_2}$. Based on the condition of the event, it holds that either $s_1 \neq 0 \bmod n$ or $s_2 \neq 0 \bmod n$. Since the decryption test of game G_0 is passed we have that $v^2 = u_1^{2x_1+2y_1\mathsf{h}}u_2^{2x_2+2y_2\mathsf{h}}$, and assuming that $v^2 = g^{r_3}h^{s_3}$ we obtain the following equation

$$x_1s_1 + y_1s_1\mathsf{h} + x_2s_2 + y_2s_2\mathsf{h} = s_3 \ \text{(in } \mathbb{Z}_n)$$

Now observe that for any fixed values of y_1, y_2 and conditioning on the progress of the game till the j-th query of the adversary, it holds that the variables $x_1(\bmod n), x_2(\bmod n)$ are statistically indistinguishable from the uniform distribution of $\mathbb{Z}_n$ (over the conditional probability space). From this it follows that the probability that the adversary produces a ciphertext that satisfies the above equation is bounded by $1/n$ and thus negligible.

Game G_2. Game G_2 modifies G_1 with respect to the choice of the public-key. In particular, in game G_2, the values c, d are selected as follows: $c \leftarrow g_1^{x'}$ and $d \leftarrow g_1^{y'}$ with $x', y' \leftarrow_R [\frac{n^2}{4}]$. It is easy to show that $|\mathbf{Prob}[\mathsf{S}_2] - \mathbf{Prob}[\mathsf{S}_1]|$ is negligible.

Game G_3. We modify the decryption oracle at step 12 so that it rejects an additional number of ciphertexts for which it holds that (1) $\mathsf{h} = \mathcal{H}_{\mathsf{hk}}(u_1, u_2, e, L) = \mathsf{h}^*$ but $\langle u_1, u_2, e, L\rangle \neq \langle u_1^*, u_2^*, e^*, L^*\rangle$ or that (2) $v \neq v^*$ but $(v)^2 = (v^*)^2$ and $v = ||v||$. The events that the adversary will produce a ciphertext that triggers one of the two new rejection rules will be called F_1 and F_2 respectively. It is easy to show that $|\mathbf{Prob}[\mathsf{S}_3] - \mathbf{Prob}[\mathsf{S}_2]| \leq \mathbf{Prob}[\mathsf{F}_1] + \mathbf{Prob}[\mathsf{F}_2]$. Moreover it holds that $\mathbf{Prob}[\mathsf{F}_1] \leq \mathsf{Adv}_{\mathcal{H}}^{\mathsf{GG}}(\nu)$ where $\mathsf{Adv}_{\mathcal{H}}^{\mathsf{GG}}(\nu)$ is the advantage of an adversary in breaking the security of the UOWHF. On the other hand observe that if $(v^*)^2 = v^2$ but $v \neq v^*$ it holds that $(v - v^*)(v + v^*) \equiv_{n^2} 0$; given that (1) $v \neq v^*$ and the fact that $v = ||v||$ and $v^* = ||v^*||$ we know also that $v^* \neq -v$. It follows that $\gcd(v - v^*, n^2)$ reveals a non-trivial divisor of n and as a result $\mathbf{Prob}[\mathsf{F}_2] \leq \mathsf{Adv}_{\mathsf{Fact}}(\nu)$.

Game G_4. We modify the computation of u_2^*, e^*, v^* as follows:

$$\langle u_2^*, e^*, v^*\rangle \leftarrow \langle (u_1^*)^w, (u_1^*)^z h^{m_b}, (u_1^*)^{x'+y'\mathsf{h}^*}\rangle$$

Observe that this modification is conceptual and it is easy to see that $\mathbf{Prob}[\mathsf{S}_3] = \mathbf{Prob}[\mathsf{S}_4]$.

Game G_5. We modify the computation of u_1^* so that u_1^* is selected at random from $\mathcal{Q}_{n^2}$. It is easy to see that $|\mathbf{Prob}[\mathsf{S}_4] - \mathbf{Prob}[\mathsf{S}_5]| \leq \mathsf{Adv}_{\mathsf{DCR}}(1^\nu)$.

Game G_6. We modify the parameter selection so that the primes p, q are known to the game execution and we further modify the decryption oracles so that any ciphertext $\langle u_1, u_2, v, e, L\rangle$ submitted for which it holds that $(u_1)^2 \notin \mathcal{X}_{n^2}$ is rejected. Clearly games G_5 and G_6 proceed identically unless the event F that the adversary produces a ciphertext that passes the decryption test of G_5 however $(u_1)^2 \notin \mathcal{X}_{n^2}$. It is easy to see that $|\mathbf{Prob}[\mathsf{G}_5] - \mathbf{Prob}[\mathsf{G}_6]| \leq \mathbf{Prob}[\mathsf{F}]$.

We proceed now to bound F. Let F_j be the event that in the j-th query for the first time the adversary triggers the event F. Clearly $\mathbf{Prob}[\mathsf{F}] \leq \sum_j \mathbf{Prob}[\mathsf{F}_j]$. We concentrate now on F_j where j is a query at the `GUESS` stage of the adversary. Let $\langle u_1, u_2, e, v, L\rangle$ be the j-th query ciphertext that satisfies $v = ||v||, u_2 = u_1^w$, and $v^2 = (u_1^2)^{x'+y'\mathsf{h}}$ while $(u_1)^2 \notin \mathcal{X}_{n^2}$. Suppose that $(u_1)^2 = g_1^r h^s$ and $v^2 = g_1^{r'} h^{s'}$. It follows from the above that we obtain two equations

$$rx' + ry'\mathsf{h} \equiv_{p'q'} r' \quad \text{and} \quad sx' + sy'\mathsf{h} \equiv_n s'$$

Given that in the view of the adversary the value $x' \bmod n, y' \bmod n$ are almost uniformly distributed over $\mathbb{Z}_n$ (no information is leaked about these values in any step of the game's operation till the j-th query) it follows that $\mathbf{Prob}[\mathsf{F}_j]$ is negligible.

Now let us consider the case that the j-th query is posed in the FIND stage of the adversary. This case is different since now the adversary possesses the challenge ciphertext $u_1^*, u_2^*, e^*, v^*, L^*$; suppose that $(u_1^*)^2 = g_1^{r^*} h^{s^*}$ and as a result $(v^*)^2 = g_1^{2(x'+y'\mathsf{h})r^*} h^{2(x'+y'\mathsf{h})s^*}$.

Let $\langle u_1, u_2, e, v, L\rangle$ be the ciphertext that triggers the event F_j in the j-th query of the adversary. It must hold then that $\langle u_1, u_2, e, v, L\rangle \neq \langle u_1^*, u_2^*, e^*, v^*, L^*\rangle$ (otherwise the ciphertext is rejected by the definition of the FIND oracle).

Suppose now that $\langle u_1, u_2, e, L\rangle$ and $\langle u_1^*, u_2^*, e^*, L^*\rangle$ are such that $\mathsf{h} = \mathsf{h}^*$; in this case, it follows that it must be $v \neq v^*$. Recall that the ciphertext $\langle u_1, u_2, e, v, L\rangle$ passes the test of G_5 which means that $v^2 = (u_1^2)^{x'+y'\mathsf{h}}$. The right-hand-side of the equality equals $(u_1^*)^{2x'+2y'\mathsf{h}^*}$ using the equality of $u_1 = u_1^*$ and $\mathsf{h} = \mathsf{h}^*$; it follows that $v^2 = (v^*)^2$. But the combination of $v \neq v^*$ and $v^2 = (v^*)^2$ means that the ciphertext should get rejected by the second rejection rule of the G_3 modification. We conclude that the ciphertext $\langle u_1, u_2, e, v, L\rangle$ if it triggers the event F_j it has the property that $\mathsf{h} \neq \mathsf{h}^*$.

Suppose now that $v^2 = g_1^{\tilde{r}} h^{\tilde{s}}$ and $(v^*)^2 = g_1^{\overline{r}} h^{\overline{s}}$. The equations regarding x', y' over $\mathbb{Z}_n$ are going to be as follows (using the equalities that $(u_1)^2 = g_1^r h^s$, $(u_1^*)^2 = g_1^{r^*} h^{s^*}$ and the facts that $(v^*)^2 = (u_1^*)^{2x'+2y'\mathsf{h}^*}$ (by definition) and $v^2 = (u_1)^{2x'+2y'\mathsf{h}}$):

$$s^* x' + s^* y' \mathsf{h}^* \equiv_n \overline{s} \quad \text{and} \quad sx' + sy'\mathsf{h} \equiv_n \tilde{s}$$

The above system defines two systems, one over $\mathbb{Z}_p$ and one over $\mathbb{Z}_q$ that each one has integer determinant $ss^*(\mathsf{h} - \mathsf{h}^*)$. By the definition of the event F_j we know that $s \neq 0 \bmod n$ which means that either $s \neq 0 \bmod p$ or $s \neq 0 \bmod q$; assume without loss of generality that $s \neq 0 \bmod p$. Moreover by the way that u_1^* is selected in game G_5 we have that $s^* \neq 0 \bmod p$ (with overwhelming probability). Moreover given that $\mathsf{h} \neq \mathsf{h}^*$ and employing the fact that $0 \leq \mathsf{h}, \mathsf{h}^* < p$ we have that $\mathsf{h} - \mathsf{h}^* \neq 0 \bmod p$. As a result the above system has an invertible determinant in $\mathbb{Z}_p$. It follows that the probability $\mathbf{Prob}[\mathsf{F}_j]$ is negligible.

Now observe that the probability G_6 of the adversary winning game G_6 is $1/2$. Indeed this is the case as u_1^* is selected at random from $\mathcal{Q}_{n^2}$ and as result it is of the form $g^{r''} h^{s''}$. Given that $z \xleftarrow{\mathsf{r}} [n^2/4]$ it holds that if $z_1 = z \bmod p'q'$ and $z_2 = z \bmod n$ it holds that $e^* = g^{z_1 r''} h^{m_b + z_2 s''}$. The key observation here is that the value z_2 is independent from the view of the adversary and thus the expression $m_b + \tilde{s} z_2$ is uniformly distributed over $\mathbb{Z}_n$, independently of b conditioning on $s'' \in \mathbb{Z}_n^*$ which is an event of overwhelming probability given the selection of u_1^*. The fact that z_2 is independent from the view of the adversary, i.e., the adversary has no information about z_2 beyond what is revealed from the e^* value follows from the following: the only way for the adversary to obtain information about z_2 is through the decryption oracle queries. In G_6 we made explicit that all oracle queries that do not satisfy $(u_1)^2 \in \mathcal{X}_{n^2}$ are rejected. This means that the adversary obtains output from the decryption oracle only for ciphertexts $\langle u_1, u_2, e, v, L\rangle$ that satisfy $(u_1)^2 \in \mathcal{X}_{n^2}$. Observe that in the computation of the oracle's response the value u_1 used as teh base of the exponent $-2z$ and as a result it follows that the value z_2 will be cancelled in any of these queries. This completes the proof. ■

Interestingly, it is not clear whether the DCR can be used for proving the key-privacy of the cryptosystem. To see why this is the case consider the following: Consider the CPA version of the cryptosystem using only a single generator over $\mathcal{X}_{n^2}$: in the CPA case the cryptosystem is similar to ElGamal, with ciphertexts pairs of the form $\langle g^r \bmod n^2, y^r h^m \bmod n^2\rangle$. Note that $\mathsf{IND\text{-}CPA}$ security can be easily shown under the DCR assumption. On the other hand, to show CPA-key-privacy one has to (essentially) establish the indistinguishability of the distributions $\langle g, y_0, y_1, g^r, y_0^r h^m\rangle$ and $\langle g, y_0, y_1, g^r, y_1^r h^m\rangle$. It is not apparent how to apply DCR to prove this indistinguishability; ultimately this is because the message m is the same in both of these distributions and its randomization (easily provided by DCR) appears to be immaterial to the indistinguishability of the two distributions. It should be noted that since the adversary is not interested in the h^m portion of the ciphertext he can easily cancel it out by raising everything to n. For this reason the power of DCR seems of little use in this case, and a Diffie-Hellman-like assumption in $\mathcal{X}_{n^2}$ would seem more appropriate. Hence, we introduce this intractability assumption:

Definition 4.3 *The Decisional Diffie Hellman assumption for square n-th residues ($\mathsf{DDH}_{\mathsf{SQNR}}$): Consider n a safe composite as above. The distribution $\langle n, g, y, g^r, y^r\rangle$ where g generates $\mathcal{X}_{n^2}$, $y \leftarrow_R \langle g\rangle$ and $r \leftarrow_R [p'q']$ is computationally indistinguishable from the distribution $\langle n, g, y, g^r, y^{r'}\rangle$ where g, y, r are as above and $r' \leftarrow_R [p'q']$.*

We argue that $\mathsf{DDH}_{\mathsf{SQNR}}$ is a plausible intractability assumption for the following reasons:

(I) The group $\mathcal{X}_{n^2}$ is a cyclic group whose order has no small prime divisors and typically DDH appears to hold in modular groups of prime and composite order that have no small prime divisors, cf. [Bon98]. Moreover, we note that the DDH over the group of quadratic residues $\mathcal{Q}_{n^2}$ can be easily seen to be a stronger assumption as it implies $\mathsf{DDH}_{\mathsf{SQNR}}$.

(II) While it is not apparent if DCR implies $\mathsf{DDH}_{\mathsf{SQNR}}$ we will see next that DCR implies the computational version of the assumption $\mathsf{CDH}_{\mathsf{SQNR}}$ in theorem 4.4. It should be pointed out that there are no examples of elementary modular arithmetic groups of order without small prime divisors where CDH is hard while DDH is easy (groups with such behavior have only been demonstrated in the elliptic curve setting).

Theorem 4.4 $\mathsf{DCR} \Longrightarrow \mathsf{CDH}_{\mathsf{SQNR}}$

Proof. First, It is easy to see that the DCR implies that the two ensembles,

$$\langle N, G\rangle : G \leftarrow_R \mathcal{X}_{n^2} \quad \langle N, Y\rangle : Y \leftarrow_R \mathcal{Q}_{n^2}$$

are indistinguishable, where $\mathcal{Q}_{n^2}$ is the group of quadratic residues modulo n^2 (the reduction is straightforward: given the challenge for DCR simply square it to get something distributed in one of the above ensembles).

Claim. For any m_1, m_2, the following two distributions are computationally indistinguishable under the DCR.

$$\langle n, g, y, g^r, y^r h^{m_1}\rangle : g, y \leftarrow_R \mathcal{X}_{n^2}, r \leftarrow_R [p'q']$$

and

$$\langle n, g, y, g^r, y^r h^{m_2}\rangle : g, y \leftarrow_R \mathcal{X}_{n^2}, r \leftarrow_R [p'q']$$

Proof of the Claim. Consider the first distribution:

$$\langle n, g, y, g^r, y^r h^{m_1}\rangle : g, y \leftarrow_R \mathcal{X}_{n^2}, r \leftarrow_R [p'q']$$

First we modify the selection of r as follows:

$$\langle n, g, y, g^r, y^r h^{m_1}\rangle : g, y \leftarrow_R \mathcal{X}_{n^2}, r \leftarrow_R [np'q']$$

This is a statistically indistinguishable modification since r appears only over elements of order $p'q'$. Now this distribution, based on the DCR it is indistinguishable from:

$$\langle n, g, z, g^r, z^r h^{m_1}\rangle : g \leftarrow_R \mathcal{X}_{n^2}, z \leftarrow_R \mathcal{Q}_{n^2}, r \leftarrow_R [np'q']$$

which can also be rewritten as:

$$\langle n, g, y \cdot h^v, g^r, y^r h^{v \cdot r + m_1}\rangle : g, y \leftarrow_R \mathcal{X}_{n^2}, v \leftarrow_R \mathbb{Z}_n, r \leftarrow_R [np'q']$$

based on Chinese remaindering now we can rewrite the above distribution as:

$$\langle n, g, y \cdot h^v, g^{r_1}, y^{r_1} h^{v \cdot r_2 + m_1}\rangle : g, y \leftarrow_R \mathcal{X}_{n^2}, v, r_2 \leftarrow_R \mathbb{Z}_n, r_1 \leftarrow_R [p'q']$$

and without difficulty the above is seen to be statistically indistinguishable to

$$\langle n, g, y \cdot h^v, g^r, y^r h^{r'}\rangle : g, y \leftarrow_R \mathcal{X}_{n^2}, v, r' \leftarrow_R \mathbb{Z}_n, r \leftarrow_R [p'q']$$

The same steps can be performed for the case m_2 and thus the two distributions are indistinguishable. (*end of proof of claim*).

Let us turn now to the statement of the theorem: $\mathsf{DCR} \Longrightarrow \mathsf{CDH}$ in $\mathcal{X}_{\mathsf{n}^2}$

The following two distributions are indistinguishable under the DCR:

$$\langle n, g, y, g^r, y^r h^m \rangle : g, y \leftarrow_R \mathcal{X}_{n^2}, r \leftarrow_R [p'q'], m \leftarrow_R \mathbb{Z}_n$$

and

$$\langle n, g, y, g^r, y^r \rangle : g, y \leftarrow_R \mathcal{X}_{n^2}, r \leftarrow_R [p'q']$$

On the other hand, It is very easy to see that given a CDH oracle that has probability of success α we can produce the test $\mathsf{CDH}(n, g, y, G)/Y \stackrel{?}{=} 1$ for a given challenge n, g, y, G, Y. Given that $\mathsf{CDH}(n, g, y, G) = Y$ with probability α we have that if n, g, y, G, Y is drawn from the second distribution the test will return 1 with probability α. On the other hand, if the challlenge is drawn from the second distribution the test will return 1 with probability at most $1/n$ (since m is drawn at randomand is independent of the CDH solver). It follows that the test has distinguishing probability $\alpha - 1/n$. As a result if α is non-negligible the two distributions can be distinguished efficiently something that violates the DCR assumption. It follows that DCR implies the CDH assumption. ∎

Based on the above we formulate our key-privacy theorem for the cryptosystem:

Theorem 4.5 *The cryptosystem $\langle \mathcal{Z}, \mathcal{G}_{\mathsf{e}}, \mathcal{E}, \mathcal{D} \rangle$ defined above satisfies CCA2-key-privacy under the* $\mathsf{DDH}_{\mathsf{SQNR}}$ *assumption and the target collision resistance of the employed* UOWH *family.*

Proof. (of theorem 4.5) Let us recap the attack game for CCA2-key-privacy in more detail applied directly to our cryptosystem. The attack game is as follows:

1. $\langle n, g_1, \mathrm{desc}\mathcal{H} \rangle \leftarrow \mathcal{Z}(1^\nu)$.
2. $g_2 \leftarrow g_1^w;\ w \xleftarrow{\mathsf{r}} [\frac{n}{4}]$
3. $c_i \leftarrow g_1^{x_{1i}} g_2^{x_{2i}}$; $x_{1i}, x_{2i} \xleftarrow{\mathsf{r}} [\frac{n^2}{4}]$ for $i \in \{0, 1\}$
4. $d_i \leftarrow g_1^{y_{1i}} g_2^{y_{2i}}$; $y_{1i}, y_{2i} \xleftarrow{\mathsf{r}} [\frac{n^2}{4}]$ for $i \in \{0, 1\}$
5. $y_i \leftarrow g_1^{z_i};\ z_i \xleftarrow{\mathsf{r}} [\frac{n^2}{4}]$ for $i \in \{0, 1\}$
6. $\mathsf{pk}_i = \langle c_i, d_i, y_i \rangle; \mathsf{sk}_i = \langle x_{1i}, x_{2i}, y_{1i}, y_{2i}, z_i \rangle$ for $i \in \{0, 1\}$.
7. $\langle m, \mathsf{aux}, L^* \rangle \leftarrow \mathcal{A}^{\mathcal{D}(\mathsf{sk}_0, \cdot), \mathcal{D}(\mathsf{sk}_1, \cdot)}(\mathtt{FIND}, \mathsf{pk}_0, \mathsf{pk}_1)$.
8. $u_1^* \leftarrow g_1^r;\ u_2^* \leftarrow g_2^r$; $r \xleftarrow{\mathsf{r}} [\frac{n}{4}]$
9. $e^* \leftarrow y_b^r h^m$; $b \xleftarrow{\mathsf{r}} \{0, 1\}$
10. $v^* \leftarrow ||c_b^r d_b^{r\mathsf{h}^*}||;\ \mathsf{h}^* \leftarrow \mathcal{H}(u_1^*, u_2^*, e^*, L^*)$
11. $\psi^* = \langle u_1^*, u_2^*, e^*, v^* \rangle$
12. $b^* \leftarrow \mathcal{A}^{\mathcal{D}^{\neg\psi^*, L^*}(\mathsf{sk}_0, \cdot), \mathcal{D}^{\neg\psi^*, L^*}(\mathsf{sk}_1, \cdot)}(\mathtt{GUESS}, \psi^*, \mathsf{aux})$

The decryption oracle $\mathcal{D}(\mathsf{sk}_i, \cdot)$ during the FIND-stage of the adversary is implemented as follows

> `if` $v^2 = u_1^{2(x_{1i} + y_{1i}\mathsf{h})} u_2^{2(x_{2i} + y_{2i}\mathsf{h})}$ `and` $v = ||v||$ `then return` $\mathsf{L}(e^2 \cdot (u_1^2)^{-z_i})$ `else` $\perp$ where $\mathsf{h} = \mathcal{H}_{\mathsf{hk}_i}(u_1, u_2, e, L)$.

Note that $\mathsf{L}(v)$ is defined as $((v \bmod n^2 - 1) \cdot 2^{-1} \bmod n)/n$ and is well defined for elements of the form $(1 + n)^x \bmod n^2$. Similarly the decryption oracle $\mathcal{D}^{\neg\psi^*, L^*}$ in the GUESS-stage of the adversary is of the form:

> `if` $v^2 = u_1^{2(x_{1i} + y_{1i}\mathsf{h})} u_2^{2(x_{2i} + y_{2i}\mathsf{h})}$ `and` $v = ||v||$ `and` $\langle \psi, L \rangle \neq \langle \psi^*, L^* \rangle$ `then return` $\mathsf{L}(e^2 \cdot (u_1^2)^{-z_i})$ `else` $\perp$ where $\mathsf{h} = \mathcal{H}(u_1, u_2, e, L)$.

Let S_0 be the probability of the event $b = b^*$ in the above game (called G_0).

Game G_1. This game has the following modifications: first the components of the public-keys y_0, y_1 are selected so that $y_i = g_1^{z_{1i}} g_2^{z_{2i}}$ with z_{1i}, z_{2i} randomly selected from $[\frac{n^2}{4}]$. Moreover the decryption oracles in the GUESS and FIND stages are modified respectively as follows `if` $v^2 = u_1^{2(x_{1i}+y_{1i}\mathsf{h})} u_2^{2(x_{2i}+y_{2i}\mathsf{h})}$ `and` $v = ||v||$ `then` $\mathsf{L}(e^2 \cdot (u_1^2)^{-z_{1i}}(u_2^2)^{-z_{2i}})$ `else` $\perp$

`if` $v^2 = u_1^{2(x_{1i}+y_{1i}\mathsf{h})} u_2^{2(x_{2i}+y_{2i}\mathsf{h})}$ `and` $v = ||v||$ `and` $\langle \psi, L\rangle \neq \langle \psi^*, L^*\rangle$ `then` $\mathsf{L}(e^2 \cdot (u_1^2)^{-z_{1i}}(u_2^2)^{-z_{2i}})$ `else` $\perp$

It is easy to see that conditioned on all choices till the selection of values y_0, y_1, the probability distribution of y_0 in game G_0 is identical to the probability distribution of y_0 in game G_1 and likewise for the variable y_1.

Let us define by R the event that the adversary submits a ciphertext to the decryption oracle for which it holds that it passes the decryption test (it is the same for both games) and additionally it holds that $u_2^2 \neq u_1^{2w}$.

Observe first that whenever $\neg\mathsf{R}$ happens it holds that for all ciphertexts submitted by the adversary, either it holds that $u_2^2 = u_1^{2w}$ or they are rejected by the decryption oracle. Now in the case that $u_2^2 = u_1^{2w}$ it holds that $u_1^{2z_{1i}} u_2^{2z_{2i}} = u_1^{2(z_{1i}+wz_{2i})}$. Moreover it holds that $y_i = g_1^{z_{1i}+wz_{2i}}$ (by definition). Observe then that the distribution of the random variable $z_{1i} + wz_{2i}$ as an exponent to an element of order $pqp'q'$ (or any divisor of this number) is statistically indistinguishable from the distribution of z_i modulo the same number (where z_i is selected as specified in game G_0). It follows that in cases that the event $\neg\mathsf{R}$ happens the output behavior of the two games is statistically indistinguishable.

Given the above, in order to conclude that the distance between the probabilities S_0 and S_1 is negligible we have to argue that the probability of the event R is negligible itself.

Suppose that R_j is the event that in the j-th query of the adversary the event R is triggered for the first time. Clearly it holds that $\mathsf{R} \subseteq \cup_j \mathsf{R}_j$ and we can use the union-bound to bound the probability of the event R as long as we bound the probability of the events R_j.

Assume that R_j happens and the j-th query occurs in the `FIND` stage of the adversary. Given that the submitted ciphertext satisfies the decryption test we have that $v^2 = u_1^{2(x_{1i}+y_{1i}\mathsf{h})} u_2^{2(x_{2i}+y_{2i}\mathsf{h})}$. Based on the properties of the group $\mathbb{Z}_{n^2}^*$ we can write $u_1^2 = g_1^{r_1} h^{t_1}$ and $u_2^2 = g_2^{r_2} h^{t_2}$. Finally let $v^2 = g_1^r h^t$. Based on these we know the following regarding the values $x_{1i}, x_{2i}, y_{1i}, y_{2i}$.

$$\begin{pmatrix} 1 & w & 0 & 0 \\ 0 & 0 & 1 & w \\ r_1 & wr_2 & r_1\mathsf{h} & wr_2\mathsf{h} \end{pmatrix} \cdot \begin{bmatrix} x_{1i} \\ x_{2i} \\ y_{1i} \\ y_{2i} \end{bmatrix} \equiv_{p'q'} \begin{bmatrix} \log_{g_1} c_i \\ \log_{g_1} d_i \\ r \end{bmatrix}$$

where the first two equations are provided by the public-key information and the third equation is suggested by the j-th decryption query. Note that the above matrix has a minor with determinant that is equal to $w(r_2 - r_1)$ over $\mathbb{Z}_{p'q'}$. Observe that up to the j-th query of the adversary no more information is provided by the game to the adversary regarding the values $x_{1i}, x_{2i}, y_{1i}, y_{2i} \bmod p'q'$.

Now we consider two cases, either $u_1^{2nw} = u_2^{2n}$ and $u_1^{2w} \neq u_2^2$ or $u_1^{2nw} \neq u_2^{2n}$ (one of these two cases must be true given that $u_1^{2w} \neq u_2^2$). In the second case it follows immediately that $r_2 \neq r_1$ and as result the determinant $w(r_2 - r_1)$ is non-zero conditioning on $w \in \mathbb{Z}_{p'q'}^*$ which is an overwhelming probability event. Still it may be the case that $r_2 - r_1 \bmod p'q'$ is a zero divisor in $\mathbb{Z}_{p'q'}$. In this case it must be that $\alpha = u_1^{2nw} u^{-2n}$ is an element of $\mathcal{X}_{n^2}$ for which it holds that its order is either p' or q'. Based on this fact we can factor n by computing $\gcd(\alpha - 1, n)$. Based on the above we conclude that the determinant $w(r_2 - r_1) \in \mathbb{Z}_{p'q'}^*$ and thus the likelihood of the above system being satisfied by $x_{1i}, x_{2i}, y_{1i}, y_{2i}$ is negligible.

Suppose on the other hand that, $u_1^{2nw} = u_2^{2n}$ and $u_1^w \neq u_2$. The above argument cannot be extended in this case since we have that $r_2 = r_1$. However we know that it holds $s_1 \neq ws_2$ and $v^2 = u_1^{x_{1i}+y_{1i}\mathsf{h}} u_2^{x_{2i}+y_{2i}\mathsf{h}}$. From this we obtain the equation $s = (x_{1i} + y_{1i}\mathsf{h})s_1 + w(x_{2i} + y_{2i}\mathsf{h})s_2$ in $\mathbb{Z}_n$. Observe that up to this moment the adversary's view is completely independent of the values

$x_{1i}, y_{1i}, x_{2i}, y_{2i} \bmod n$ (based on Chinese remaindering). It follows that the probability that this equation is satisfied is negligible (due to $s_1 \neq ws_2$ the values s_1, s_2 cannot be both zero).

Using the above we conclude that the event R_j will happen with negligible probability and as a result it also holds that $\mathbf{Prob}[\mathsf{R}]$ is negligible. Composing the above facts together we have that $|\mathbf{Prob}[\mathsf{S}_0] - \mathbf{Prob}[\mathsf{S}_1]|$ is negligible under the assumption that factoring is hard.

Game G_2. We make the following change to the previous game.

9. $e^* \leftarrow (u_1^*)^{z_{1b}}(u_2^*)^{z_{2b}} h^m$; $b \xleftarrow{\mathtt{r}} \{0,1\}$
10. $v^* \leftarrow ||(u_1^*)^{x_{1b}+\mathsf{h}^* y_{1b}}(u_2^*)^{x_{2b}+\mathsf{h}^* y_{2b}}||$; $\mathsf{h}^* \leftarrow \mathcal{H}(u_1^*, u_2^*, e^*, L)$.

It is easy to see that the above modification is purely conceptual and does not affect the view of the adversary in any way. It follows easily, $\mathbf{Prob}[\mathsf{S}_2] = \mathbf{Prob}[\mathsf{S}_1]$.

Game G_3. We make the following change to the previous game.

8. $u_1^* \leftarrow g_1^{r_1^*}$; $u_2^* \leftarrow g_2^{r_2^*}$; $r_1^*, r_2^* \leftarrow_R [\frac{n}{4}]$.

Regarding the above modification to game G_2 It is easy to see that $|\mathbf{Prob}[\mathsf{S}_3] - \mathbf{Prob}[\mathsf{S}_2]| \leq \mathsf{Adv}_{\mathsf{DDH}_{\mathsf{SQNR}}}(\nu)$.

Game G_4. Next we make the following modifications in the way the decryption oracles operate in the `GUESS` and `FIND` stages:

`if` $u_2^2 = u_1^{2w}$ `and` $v^2 = u_1^{2(x_{1i}+wx_{2i}+(y_{1i}+wy_{2i})\mathsf{h})}$ `and` $v = ||v||$ `then` $\mathsf{L}(e^2 \cdot (u_1^2)^{-z_{1i}-wz_{2i}})$ `else` $\perp$

`if` $u_2^2 = u_1^{2w}$ `and` $v^2 = u_1^{2(x_{1i}+wx_{2i}+(y_{1i}+wy_{2i})\mathsf{h})}$ `and` $v = ||v||$ `and` $\langle \psi, L\rangle \neq \langle \psi^*, L^*\rangle$ `then` $\mathsf{L}(e^2 \cdot (u_1^2)^{-z_{1i}-wz_{2i}})$ `else` $\perp$

) Let R be the event that the adversary produces a ciphertext ψ directed to one of the two decryption oracles and a label L that is answered differently in game G_3 and in game G_4. Let us concentrate first on the `FIND` stage. First suppose that the ciphertext ψ with context L pass the decryption test of G_4. This means that they satisfy $u_2^2 = u_1^{2w}$ and $v^2 = u_1^{2(x_{1i}+wx_{wi}+(y_{1i}+wy_{wi})\mathsf{h})}$ where $\psi = \langle u_1, u_2, e, v\rangle$. From this we obtain that $v^2 = u_1^{2(x_{1i}+y_{1i}\mathsf{h})} u_2^{2(x_{2i}+y_{2i}\mathsf{h})}$ i.e.,the ciphertext should also pass the decryption test of game G_3. Given that decryption itself is identical in the two games we have that the two oracles behave in identical fashion. Note that the same holds true even in the `GUESS` stage.

We conclude that if R happens it must be that the ciphertext ψ and label L gets rejected in the decryption test of game G_4 and passes the decryption test of game G_3 (so that the answers of the two oracles is different). It follows that either $u_2^2 \neq u_1^{2w}$ or $v^2 \neq u_1^{2(x_{1i}+wx_{2i}+(y_{1i}+wy_{2i})\mathsf{h})}$. Note that it must be that $u_2^2 \neq u_1^{2w}$ (otherwise, if $u_2^2 = u_1^{2w}$ given that the decryption same of G_3 passes it will also be the case for the decryption test of G_4). We conclude that the event R happens whenever $u_2^2 \neq u_1^{2w}$ and the ciphertext passes the decryption test of game G_3.

We split the event R so that R_1 means that the first time the adversary produces a ciphertext that triggers R is in the `FIND` stage similarly for R_4 for the `GUESS` stage. We will first consider R_1. We split the event R_1 in the number of queries of the adversary and we consider the event that it happens for the first time in the j-th query. We have that in his j-th query the adversary for some $i \in \{1,2\}$, for the first time produces $\langle u_1, u_2, v, e, L\rangle$ so that $u_2^2 \neq u_1^{2w}$ and $v^2 = u_1^{2(x_{1i}+y_{1i}\mathsf{h})} u_2^{2(x_{2i}+y_{2i}\mathsf{h})}$). Suppose that $u_1^2 = g_1^{r_1} h^{s_1}$ and $u_2^2 = g_2^{r_2} h^{s_2}$. Also let $v^2 = g_1^r h^s$. We obtain the following system of equations in $\mathbb{Z}_{p'q'}$ that represents the view of the adversary with respect to the values $x_{1i}, x_{2i}, y_{1i}, y_{2i}$.

$$\begin{pmatrix} 1 & w & 0 & 0 \\ 0 & 0 & 1 & w \\ r_1 & wr_2 & r_1\mathsf{h} & wr_2\mathsf{h} \end{pmatrix} \cdot \begin{bmatrix} x_{1i} \\ x_{2i} \\ y_{1i} \\ y_{2i} \end{bmatrix} \equiv_{p'q'} \begin{bmatrix} \log_{g_1} c_i \\ \log_{g_1} d_i \\ r \end{bmatrix}$$

the first two equations are given by the public-key of the system whereas the last equation corresponds to the ciphertext that was produced by the adversary. Observe that the above system has a 3x3 matrix with determinant $w(r_2 - r_1)$.

Now we consider two cases, either $u_1^{2nw} = u_2^{2n}$ and $u_1^{2w} \neq u_2^2$ or $u_1^{2nw} \neq u_2^{2n}$. In the second case it follows immediately that $r_2 \neq r_1$ and as a result the determinant $w(r_2 - r_1)$ is non-zero conditioning on $w \in \mathbb{Z}^*_{p'q'}$ which is an overwhelming probability event. Still it may be the case that $r_2 - r_1 \bmod p'q'$ is a zero divisor. In this case it must be that $\alpha = u_1^{2nw}u^{-2n}$ is an element of $\mathcal{X}_{n^2}$ for which it holds that its order is either p' or q'. Based on this fact we can factor n by computing $\gcd(\alpha - 1, n)$. Based on the above we conclude that the determinant $w(r_2 - r_1) \in \mathbb{Z}^*_{p'q'}$ and thus the likelihood of the above system being satisfied is negligible.

Suppose on the other hand that, $u_1^{2nw} = u_2^{2n}$ and $u_1^{2w} \neq u_2^2$. As before the above argument cannot be extended in this case since we have that $r_2 = r_1$. Nevertheless now, we know that it holds $s_1 \neq ws_2$ and $v^2 = u_1^{2(x_{1i}+y_{1i}\mathsf{h})}u_2^{2(x_{2i}+y_{2i}\mathsf{h})}$. From this we obtain the equation $s = (x_{1i}+y_{1i}\mathsf{h})s_1 + w(x_{2i}+y_{2i}\mathsf{h})s_2$ in $\mathbb{Z}_n$. Observe that up to this moment the adversary's view is completely independent of the values $x_{1i}, y_{1i}, x_{2i}, y_{2i} \bmod n$ (based on Chinese remaindering). It follows that the probability that this equation is satisfied is negligible (given that $s_1 \neq ws_2$ not both s_1, s_2 can be simultaneously zero). This completes the argument that the probability of the event R_1 is negligible (under the assumption that factoring is hard).

We turn now to the event R_4 which is the event that the adversary is producing the query to the decryption oracle after he has received the challenge. We will only consider the case that the challenge ciphertext is consistent with the oracle targetted as it is the most complex one; the other case can be dealt with in a very similar way. We will further split the event R_4 in three sub-cases, (i) that $u_1^{2nw} = u_2^{2n}$ and $\mathsf{h} \neq \mathsf{h}^*$, (ii) $u_1^{2nw} \neq u_2^{2n}$ and $\mathsf{h} \neq \mathsf{h}^*$, and (iii) $\mathsf{h} = \mathsf{h}^*$.

Within $\mathbb{Z}^*_{p'q'}$ the following system of equations is defined from the view of the adversary:

$$\begin{pmatrix} 1 & w & 0 & 0 \\ 0 & 0 & 1 & w \\ r_1^* & wr_2^* & r_1^*\mathsf{h}^* & wr_2^*\mathsf{h}^* \\ r_1 & wr_2 & r_1\mathsf{h} & wr_2\mathsf{h} \end{pmatrix} \cdot \begin{bmatrix} x_{1i} \\ x_{2i} \\ y_{1i} \\ y_{2i} \end{bmatrix} \equiv_{p'q'} \begin{bmatrix} \log_{g_1} c_i \\ \log_{g_1} d_i \\ r^* \\ r \end{bmatrix}$$

where r^* comes from $(v^*)^2 = g_1^{r^*}h^{s^*}$ and r comes from $v^2 = g_1^r h^s$. The integer determinant of this system is equal to $w^2(r_1 - r_2)(r_1^* - r_2^*)(\mathsf{h} - \mathsf{h}^*)$. Below we will condition on $w^2(r_1^* - r_2^*) \in \mathbb{Z}^*_{p'q'}$ as it is an overwhelming probability event. Considering now the case (i) we have that $r_2 \neq r_1$ and $\mathsf{h} \neq \mathsf{h}^*$. Under the assumption that factoring is hard we obtain as before that the determinant is an element of $\mathbb{Z}^*_{p'q'}$ and thus the probability that the adversary has in satisfying the system is negligible. Suppose now case (ii) happens. In this case we cannot use the system above as it holds $r_2 = r_1$. Nevertheless we have that $s_2 \neq ws_1$ and that the equation $s = (x_{1i} + y_{1i}\mathsf{h})s_1 + w(x_{2i} + y_{2i}\mathsf{h})s_2$ is satisfied in $\mathbb{Z}_n$. The adversary has no prior information about the values $x_{1i}, x_{2i}, y_{1i}, y_{2i}$ (not even from the challenge ciphertext since the u_1^*, u_2^* values belong to $\mathcal{X}_{n^2}$) and as a result we have that the adversary has negligible success probability in satisfying this equation. Finally we consider, case (iii), $\mathsf{h} = \mathsf{h}^*$. We know regarding the submitted ciphertext $\psi = \langle u_1, u_2, e, v, L\rangle$ that it holds $\langle u_1, u_2, e, v, L\rangle \neq \langle u_1^*, u_2^*, e^*, v^*, L^*\rangle$ since in the opposite case the ciphertext would have been rejected. Consider now two cases (iiia) $\langle u_1, u_2, e, L\rangle = \langle u_1^*, u_2^*, e^*, L^*\rangle$ and $v \neq v^*$ and (iiib) $\langle u_1, u_2, e, L\rangle \neq \langle u_1^*, u_2^*, e^*, L^*\rangle$.

Case (iiib) it follows easily that the probability it happens will be bounded by the advantage of finding collisions in the given UOWH family. Regarding case (iiia) we observe that $u_1 = u_1^* \in \mathcal{X}_{n^2}$ and $u_2 = u_2^* \in \mathcal{X}_{n^2}$. Moreover we know that $(v^*)^2 = (u_1^*)^{2(x_{1i}+y_{1i}\mathsf{h})}(u_2^*)^{2(x_{2i}+y_{2i}\mathsf{h})}$ by definition. Since the ciphertext ψ passes the test of game G_3 it also holds that $v^2 = (u_1)^{2(x_{1i}+y_{1i}\mathsf{h})}(u_2)^{2(x_{2i}+y_{2i}\mathsf{h})}$, i.e., $(v^*)^2 = v^2$. In addition we have that $v = ||v||$ and $v^* = ||v^*||$. From this we obtain the fact that v, v^* are two elements of $\mathbb{Z}_{n^2}^*$ that satisfy $v \neq v^*$ but $v \neq \pm v^*$ and $v^2 = (v^*)^2$. It follows that we can factor n by computing $\gcd(n, v - v^*)$ and as a result case (iiia) is a negligible probability event based on factoring.

Game G_5. We modify the parameter selection so that the factorization of n is known. We modify the decryption oracles as follows:

`if` $u_1^2 \in \mathcal{X}_{n^2}$ `and` $u_2^2 = u_1^{2w}$ `and` $v^2 = u_1^{2(x_{1i}+wx_{2i}+(y_{1i}+wy_{2i})\mathsf{h})}$ `and` $v = ||v||$ `then` $\mathsf{L}(e^2 \cdot (u_1^2)^{-z_{1i}-wz_{2i}})$ `else` $\perp$

`if` $u_1^2 \in \mathcal{X}_{n^2}$ `and` $u_2^2 = u_1^{2w}$ `and` $v^2 = u_1^{2(x_{1i}+wx_{2i}+(y_{1i}+wy_{2i})\mathsf{h})}$ `and` $v = ||v||$ `and` $\langle \psi, L\rangle \neq \langle \psi^*, L^*\rangle$ `then` $\mathsf{L}(e^2 \cdot (u_1^2)^{-z_{1i}-wz_{2i}})$ `else` $\perp$

Note that the test $u_1^2 \in \mathcal{X}_{n^2}$ is possible since the factorization of n is known. Consider R the event that the adversary produces a ciphertext for which it passes the test of game G_4 but it is rejected by game G_5 (it cannot be the other way around). Let us suppose that $u_1^2 = g_1^{r_1} h^{s_1}$. In the `FIND` stage of the adversary the equation that must be satisfied by the query ciphertext is as follows:

$$\tilde{s} \equiv_n s_1(x_{1i} + wx_{2i} + (y_{1i} + wy_{2i})\mathsf{h})$$

where $v^2 = g^{\tilde{r}} h^{\tilde{s}}$. Since it holds that $s_1 \neq 0$ then observe that up to this point the values $x_{1i}, x_{2i}, y_{1i}, y_{2i}$ in $\mathbb{Z}_n$ are independent of the adversary's view and as a result the probability that a ciphertext submitted by the adversary satisfies the equation is negligible. The result is the same for the `GUESS` stage of the adversary as the challenge ciphertext does not provide any information about the values of $x_{1i}, x_{2i}, y_{1i}, y_{2i}$ in $\mathbb{Z}_n$.

Game G_6. We modify the computation of the challenge as follows:

9. $e^* \leftarrow g_1^{r'} h^m$; $b \xleftarrow{\mathtt{r}} \{0,1\}, r' \xleftarrow{\mathtt{r}} [\frac{n}{4}]$.

Observe that in game G_5 the value e^* is calculated as $g_1^{r_1^* z_{1b} + w r_2^* z_{2b}} h^m$ whereas in G_6 it is calculated as $g_1^{r'} h^m$. Considering the setting of game G_5 regarding the values z_{1b}, z_{2b} the adversary knows the following equations:

$$\begin{pmatrix} 1 & w \\ r_1^* & wr_2^* \end{pmatrix} \cdot \begin{bmatrix} z_{1b} \\ z_{2b} \end{bmatrix} \equiv_{p'q'} \begin{bmatrix} \log_{g_1} y_b \\ r' \end{bmatrix}$$

Conditioning on $w(r_1^* - r_2^*) \in \mathbb{Z}_{p'q'}^*$ (which is an overwhelming probability event) it follows that te determinant of the matrix is invertible and thus any choice of r' can be accommodated by z_1, z_2; it follows that the probability distributions of e^* in games G_5 and game G_6 are statistically indistinguishable. It should be stressed that the adversary has no other information about z_{1b}, z_{2b} in $\mathbb{Z}_{p'q'}^*$ as his decryption oracles depend on z_{1b}, z_{2b} used only through $z_{1b} + wz_{2b} \bmod p'q' = \log_{g_1} y_b$.

Game G_7. We modify further the calculation of the challenge as follows:

10. $v^* \leftarrow ||g_1^{r''}||$; $r'' \leftarrow_R \mathbb{Z}_q$.

The adversary knows the following regarding the values $x_{1b}, x_{2b}, y_{1b}, y_{2b}$:

$$\begin{pmatrix} 1 & w & 0 & 0 \\ 0 & 0 & 1 & w \\ r_1^* & wr_2^* & r_1^*\mathsf{h}^* & wr_2^*\mathsf{h}^* \end{pmatrix} \cdot \begin{bmatrix} x_{1b} \\ x_{2b} \\ y_{1b} \\ y_{2b} \end{bmatrix} \equiv_{p'q'} \begin{bmatrix} \log_{g_1} c_b \\ \log_{g_1} d_b \\ r'' \end{bmatrix}$$

The above system has a 3x3 matrix with integer determinant $w(r_2^* - r_1^*)$ which belongs to $\mathbb{Z}_{p'q'}^*$ with overwhelming probability. Any choice of r'' can be accommodated by the system and as a result the statistical distance between game G_6 and game G_7 is negligible. Note that no other information is revealed to the adversary regarding the values $x_{1b}, x_{2b}, y_{1b}, y_{2b}$ beyond $\log_{g_1} c_b$ and $\log_{g_1} d_b$.

Observe that the probability of the event $(b = b^*)$ in game G_7 is clearly $1/2$ since no information about b is shared with the adversary in any phase of the game. ■

4.2 Proof of Public-Key Validity

We will employ the public-key encryption scheme above to build the public-key $\mathsf{database}$ of the GE scheme. When a user joins the group he will be allowed to generate a public-key and he will be required to show that the public-key is valid. For our new cryptosystem the language of valid public-keys is $\mathcal{L}_{pk}^{\mathsf{param}} = \{\langle c, d, y\rangle \mid c, d, y \in \mathcal{X}_{n^2}\}$ where $\mathsf{param} = \langle n, g_1, g_2, \mathcal{H}\rangle$. It follows that joining will require three instances of a proof of language membership to the subgroup $\mathcal{X}_{n^2}$ of $\mathbb{Z}_{n^2}^*$. The validity of an element y can be performed by executing the following steps where $k_0, k_1 \in \mathbb{N}$ are parameters that affect the soundness and zero-knowledge properties of the proof of language membership below:

1. [User:] Select $t \xleftarrow{r} \{0,1\}^{k_0}$ and transmit $a \leftarrow g^t \bmod n^2$.

2. [GM:] Select $c \xleftarrow{r} \{0,1\}^{k_1}$ and transmit c.

3. [User:] Compute $s \leftarrow t - cz \in \mathbb{Z}$ and transmit s.

4. [GM:] Verify $a^2 \equiv_{n^2} (g_1^2)^s y^{2c}$.

It is easy to verify that given any prover that produces a value y and then executes the proof above, it must be the case that $y^2 \in \mathcal{X}_{n^2}$ with probability $1 - 2^{-k_1}$. Note that this still allows for a slight misbehavior on the part of the user as he can multiply y with an element of order 2 inside $\mathbb{Z}_{n^2}^*$; while it is easy to add an additional step in the above proof to avoid this slight misbehavior we will not do so as we will show the security properties of our GE scheme without such guarantee.

4.3 Construction of GE of Discrete-logarithms

We proceed to the description of the GE scheme $\mathtt{SETUP}, \mathtt{JOIN}, \langle \mathcal{G}_{\mathsf{dl}}, \mathcal{R}_{\mathsf{dl}}, \mathsf{sample}_{\mathsf{dl}}\rangle, \mathtt{ENC}, \mathtt{DEC}, \mathtt{OPEN}, \langle \mathcal{P}, \mathcal{V}, \mathsf{recon}\rangle$. First recall that from the discrete-logarithm relation, $\mathcal{G}_{\mathsf{dl}}$ given 1^ν samples a description of a cyclic group of ν-bits order and a generator γ of that group; $\mathcal{R}_{\mathsf{dl}}$ contains pairs of the form (x, w) where $x = \gamma^w$. Finally $\mathsf{sample}_{\mathsf{dl}}$ on input $\mathsf{pk}_{\mathcal{R}} = \langle \mathrm{desc}(G), \gamma\rangle$ selects a witness w and returns the pair $(x = \gamma^w, w)$.

Parameter Selection. The procedure $\mathtt{SETUP}$ selects the following parameters:

∘ Integer values k_0, k_1.

∘ A safe composite n of ℓ_n bits and generators $g, \breve{g}, g_1, g_2$ of the group $\mathcal{X}_{n^2}$.

∘ The description of a hash function $\mathcal{H}$ drawn at random from a UOWH family.

∘ A prime number Q of the form $\lambda \cdot n^2 + 1$ and F, H generators of the order n^2 subgroup of $\mathbb{Z}_Q^*$.

∘ A safe composite $\hat{n}$ of ℓ_N bits and two generators $\hat{g}, \hat{y}$ of the group $\mathcal{X}_{\hat{n}^2}$.

We stress that the above parameters are part of the trusted setup of the system (also referred to as the common reference string, and no participant of the system, including the GM, OA, or any user will know any private information about these values).

$\mathtt{SETUP}_{\mathsf{OA}}$. The procedure selects $\mathsf{x}_1, \mathsf{x}_2, \mathsf{y}_1, \mathsf{y}_2, \mathsf{z} \leftarrow_R [\frac{n^2}{4}]$ and set $\mathsf{pk}_{\mathsf{OA}} = \langle \breve{y}, \breve{c}, \breve{d} \rangle = \langle g^{\mathsf{z}}, g^{\mathsf{x}_1} \breve{g}^{\mathsf{x}_2}, g^{\mathsf{y}_1} \breve{g}^{\mathsf{y}_2} \rangle$.

$\mathtt{SETUP}_{\mathsf{GM}}$. The GM will employ a digital signature $\langle \mathcal{G}_{\mathsf{s}}, \mathcal{S}, \mathcal{V}_{\mathsf{s}} \rangle$ that must satisfy adaptive chosen message security and be suitable for engaging in proofs of knowledge of signed messages when the signature is committed. In our design will employ the signature of Camenisch and Lysyanskaya [CL02] as the underlying digital signature scheme (hence referred to as CL-signature). The choice of the digital signature is not unique to our design and other signature schemes can be employed as well. The key-generation procedure $\mathcal{G}_{\mathsf{s}}$ (that will be used by GM in $\mathtt{SETUP}_{\mathsf{GM}}$) samples a pair $\langle \mathsf{sk}_{\mathsf{GM}}, \mathsf{pk}_{\mathsf{GM}} \rangle$ where $\mathsf{pk}_{\mathsf{GM}} = \langle A_0, A_1, A_2, G, Y_1, Y_2, Y_3, N \rangle$ with N a safe composite of ℓ_N bits and $A_0, A_1, A_2, G, Y_1, Y_2, Y_3 \in \mathbb{Z}_N^*$ are random quadratic residues in $\mathcal{Q}_N$. The signing key $\mathsf{sk}_{\mathsf{GM}}$ is the factorization of N. In addition to ℓ_N we have the parameters ℓ_m where $[0, 2^{\ell_m})$ will be the message space for the signature such that $n^2 < 2^{\ell_m}$ (this is because we want to use the signature to sign public-keys of the encryption scheme).

$\mathtt{JOIN}$. The prospective group member submits c, d, y as generated by the encryption system $\langle \mathcal{G}_{\mathsf{e}}, \mathcal{E}, \mathcal{D} \rangle$ given in the beginning of the section. In particular, recall that $\langle c, d, y \rangle$ is defined as $c \leftarrow g_1^{x_1} g_2^{x_2} \bmod n^2, d \leftarrow g_1^{y_1} g_2^{y_2} \bmod n^2$, $y \leftarrow g_1^{z}$ and $x_1, x_2, y_1, y_2, z \leftarrow_R [\frac{n^2}{4}]$. The secret key of the user is set to the values x_1, x_2, y_1, y_2, z. The user engages with the GM in a proof of membership for the validity of c, d, y. Upon acceptance the GM will use the signing procedure $\mathcal{S}$ for CL-signatures that is as follows: given the message $M \in \{c, d, y\}$, the GM will sample $R \leftarrow [0, 2^{\ell_N + \ell_m + \ell})$ where ℓ is a security parameter and a random prime $E > 2^{\ell_m + 1}$ of length $\ell_m + 2$ bits; then it will compute $A = (A_0 A_1^M A_2^R)^{1/E} (\mathrm{mod} N)$ (recall that the factorization of N is the signing key). Finally the signature to M is the triple $\langle A, E, R \rangle$. It follows that each recipient will accumulate three signatures for his public-key $\langle y, c, d \rangle$ that will be denoted by $\langle A_{\mathsf{a}}, E_{\mathsf{a}}, R_{\mathsf{a}} \rangle$ for $\mathsf{a} \in \{\mathsf{y}, \mathsf{c}, \mathsf{d}\}$.

Finally, the GM will enter $\langle c, d, y \rangle$ into the public $\mathtt{database}$ followed by the three signatures. Note that the GM should not allow a user to enter into $\mathsf{database}$ a key $\langle c, d, y \rangle$ such that there is some $\langle c_i, d_i, y_i \rangle$ in the database already for which it holds that $c^2 = c_i^2$, or $d^2 = d_i^2$ or $y^2 = y_i^2$. Note that the verification algorithm $\mathcal{V}_{\mathsf{s}}$ given a message M and a signature $\langle A, E, R \rangle$ on it, checks whether it holds that $A^E = A_0 A_1^M A_2^R \bmod N$ and verifies all the range constraints on M, E, R as stated above.

$\mathtt{ENC}$, $\mathtt{DEC}$ and recon. Following our modular design methodology of section 3 the GE encryption function consists of the encryption of the witness w under a recipient's public-key $\langle c, d, y \rangle$ and a sequence of commitments to the public-key used and commitments to the certificate of this public-key. More specifically when Alice wants to encrypt her witness w for her public-value $x = \gamma^w$ under label L she computes the following:

1. Commitment to Certificate of Public-key. The commitment to the certificate of the public-key of the recipient that Alice selected is formed as follows: for each one of the three certificates $\langle A_{\mathsf{a}}, E_{\mathsf{a}}, R_{\mathsf{a}} \rangle$ for $\mathsf{a} \in \{\mathsf{y}, \mathsf{c}, \mathsf{d}\}$ the following values are computed $\tilde{B}_{\mathsf{a}} = G^{u_{\mathsf{a}}} \bmod N$, $\tilde{A}_{\mathsf{a}} = Y_1^{u_{\mathsf{a}}} A_{\mathsf{a}} \bmod N$, $\tilde{E}_{\mathsf{a}} = Y_2^{u_{\mathsf{a}}} G^{E_{\mathsf{a}}} \bmod N$, $\tilde{R}_{\mathsf{a}} = Y_3^{u_{\mathsf{a}}} G^{R_{\mathsf{a}}} \bmod N$ for $\mathsf{a} \in \{\mathsf{y}, \mathsf{c}, \mathsf{d}\}$.

2. Bridge Commitments. The "bridge commitments" will assist in the efficient proof of ciphertext validity. In particular Alice includes the commitments $\hat{E}_{\mathsf{a}} = \hat{g}^{E_{\mathsf{a}}} (l_{\mathsf{a},1})^{\hat{n}} \bmod \hat{n}^2$, $\hat{R}_{\mathsf{a}} = \hat{g}^{R_{\mathsf{a}}} (l_{\mathsf{a},2})^{\hat{n}} \bmod \hat{n}^2$ for $\mathsf{a} \in \{\mathsf{y}, \mathsf{c}, \mathsf{d}\}$ and $l_{\mathsf{a},j} \xleftarrow{\mathtt{r}} \mathbb{Z}_n$ where $\mathsf{a} \in \{\mathsf{y}, \mathsf{c}, \mathsf{d}\}$ and $j = 1, 2$. Moreover she includes the commitments $\tilde{y} = H_{\mathsf{y}}^{u'} F^y \bmod Q, \tilde{c} = H_{\mathsf{c}}^{u'} F^c \bmod Q, \tilde{d} = H_{\mathsf{d}}^{u'} F^d \bmod Q$.

3. Encryption of the recipient's public-key. Encryption of the public-key that Alice selected is formed as three ciphertexts: $\langle f_{\mathsf{c}}, \breve{f}_{\mathsf{c}}, \dot{f}_{\mathsf{c}}, \ddot{f}_{\mathsf{c}} \rangle$, $\langle f_{\mathsf{d}}, \breve{f}_{\mathsf{d}}, \dot{f}_{\mathsf{d}}, \ddot{f}_{\mathsf{d}} \rangle$, $\langle f_{\mathsf{y}}, \breve{f}_{\mathsf{y}}, \dot{f}_{\mathsf{y}}, \ddot{f}_{\mathsf{y}} \rangle$, where each is selected as $\langle g^{u_{\mathsf{a}}}, \breve{g}^{u_{\mathsf{a}}}, \breve{y}^{u_{\mathsf{a}}} a, \breve{c}^{u_{\mathsf{a}}} \breve{d}^{u_{\mathsf{a}} \mathcal{H}(L'_{\mathsf{a}})} \rangle$ where $u_{\mathsf{a}} \xleftarrow{\mathtt{r}} [\frac{n}{4}]$, $\mathsf{a} \in \{\mathsf{y}, \mathsf{c}, \mathsf{d}\}$, $a \in \{y, c, d\}$ and $L'_{\mathsf{a}} = \langle f_{\mathsf{a}}, \breve{f}_{\mathsf{a}}, \dot{f}_{\mathsf{a}}, \ddot{f}_{\mathsf{a}}, L \rangle$.

4. Encryption of the witness. The encryption of witness w is as follows: $\langle u_1, u_2, e, v\rangle \leftarrow \langle g_1^r, g_2^r, y^r h^w, ||c^r d^{r\mathcal{H}(u_1,u_2,e,L'_{\mathsf{c}},L'_{\mathsf{d}},L'_{\mathsf{y}})}||\rangle$.

`DEC` is the decryption process as defined in the beginning of the section for the new encryption scheme. recon is simply the identity function.

`OPEN`. The opening procedure applies to the three ciphertext excluding the witness ciphertext (item 4, above). In particular, it returns $\langle c, d, y\rangle = \langle f_{\mathsf{c}} \dot{f}_{\mathsf{c}}^{-\mathsf{z}}, \dot{f}_{\mathsf{d}} f_{\mathsf{d}}^{-\mathsf{z}}, \dot{f}_{\mathsf{y}} f_{\mathsf{y}}^{-\mathsf{z}}\rangle$ or $\perp$ depending on the outcome of the ciphertext validity tests $f_{\mathsf{a}}^{\mathsf{x}_1+\mathsf{y}_1} \breve{f}_{\mathsf{a}}^{(\mathsf{x}_2+\mathsf{y}_2)\mathcal{H}(L')} \stackrel{?}{=} \ddot{f}_{\mathsf{a}}$ for $\mathsf{a} \in \{\mathsf{y}, \mathsf{c}, \mathsf{d}\}$. The owner of the public-key is identified by comparing $\langle c^2, d^2, y^2\rangle$ to all entries $\langle c_i^2, d_i^2, y_i^2\rangle$ that are inside the database $\mathsf{database}$.

The proof of validity $\langle \mathcal{P}, \mathcal{V}\rangle$. This protocol will be constructed as an AND composition of four sub-protocols and are presented in section 4.4. These protocols belong to a class of efficient proofs for discrete log relations that are very common in the design of cryptographic primitives and their concrete and efficient instantiation has become quite standard in the literature. An exception perhaps is protocol # 2 which is a more complex protocol and is related to the "double-decker" proof of knowledge for discrete-logarithms [Sta96, CS97]. This protocol is the least efficient as it requires parallel repetition for decreasing the knowledge-error. Still, we stress that the overall communication is independent of the size of the group and well within practical limits.

4.4 The $\langle \mathcal{P}, \mathcal{V}\rangle$ construction

Protocol #1. This proof of knowledge will establish that $\langle u_1, u_2, e, v\rangle$ is a valid ciphertext encrypting a witness w for which it holds that $w = \log_\gamma x$ (recall that x and γ are public-values) under a public-key that is committed into the three ciphertexts $\langle f_{\mathsf{a}}, \breve{f}_{\mathsf{a}}, \dot{f}_{\mathsf{a}}, \ddot{f}_{\mathsf{a}}\rangle$ for $\mathsf{a} \in \{\mathsf{c}, \mathsf{d}, \mathsf{y}\}$. At the same time we prove that the public-key ciphertxts $\langle f_{\mathsf{a}}, \breve{f}_{\mathsf{a}}, \dot{f}_{\mathsf{a}}, \ddot{f}_{\mathsf{a}}\rangle$ have the valid format and thus they decrypt properly to the values they commit. Using the notation introduced in [CS97] we can describe this protocol as:

$$\mathsf{PK}\Big(w, r, u_{\mathsf{a}}, \pi_{\mathsf{a}} : (u_1^2 = g_1^{2r}) \wedge (u_2^2 = g_2^{2r}) \wedge_{\mathsf{a}} (f_{\mathsf{a}}^2 = g^{2u_{\mathsf{a}}}) \wedge_{\mathsf{a}} (\breve{f}_{\mathsf{a}}^2 = \breve{g}^{2u_{\mathsf{a}}}) \wedge (f_{\mathsf{a}}^{2r} = g^{2\pi_{\mathsf{a}}}) \wedge$$

$$\wedge (e^2 \breve{y}^{2\pi} = h^{2w} \dot{f}_{\mathsf{y}}^{2r}) \wedge (v^2 \breve{y}^{2\pi_{\mathsf{c}}} \breve{y}^{2\pi_{\mathsf{d}}} = (\dot{f}_{\mathsf{c}} \dot{f}_{\mathsf{d}}^{\mathsf{h}})^{2r}) \wedge_{\mathsf{a}} (\ddot{f}_{\mathsf{a}}^2 = (\breve{c}\breve{d}^{\mathsf{h}'})^{2u_{\mathsf{a}}}) \wedge (x = \gamma^w)\Big)$$

where h and h' are the two hashes of encryptions and commitments that are employed for the encryption of the witness and the encryption of the public-key respectively (these values are publicly computable) and a ranges in $\{\mathsf{c}, \mathsf{d}, \mathsf{y}\}$.

Protocol #2. This will ensure that the value committed into $(f_{\mathsf{a}}, \dot{f}_{\mathsf{a}})$ where $\mathsf{a} \in \{\mathsf{c}, \mathsf{d}, \mathsf{y}\}$ is *also* committed into $\tilde{\mathsf{a}}$ (note that $\tilde{\mathsf{a}}$ is a Pedersen commitment to a, whereas $(f_{\mathsf{a}}, \dot{f}_{\mathsf{a}})$ can be viewed as a regular ElGamal ciphertext encrypting a inside $\mathcal{X}_{n^2}$). A protocol achieving this is as follows:

Blinding phase. The prover selects, $B_1 = g^{\omega_1} \bmod n^2$ and $B_2 = H_{\mathsf{a}}^{\omega_2} F^{((g_{\mathsf{a}})^{-\omega_1} \bmod n^2)}$ where $\omega_1 \leftarrow_R [\frac{n}{4}]$ and $\omega_2 \leftarrow_R \mathbb{Z}_{n^2}$. The prover submits B_1, B_2 to the verifier.

Challenge selection. The verifier selects $c \leftarrow_R \{0, 1\}$ and submits c to the prover.

Response. The prover responds by $\sigma_1 = \omega_1 - cu$ (in $\mathbb{Z}$) and $\sigma_2 = \omega_2 - cz_2 \dot{f}_{\mathsf{a}}^{-1}(g_{\mathsf{a}})^{-\sigma_1} \bmod n^2$.

Verification. The verifier checks the relations $B_1 \stackrel{?}{=} g^{\sigma_1} f_{\mathsf{a}}^c$ and $B_2 \stackrel{?}{=} H_{\mathsf{a}}^{\sigma_2} (F^{(g_{\mathsf{a}})^{-\sigma_1}})^{1-c} (\tilde{\mathsf{a}}^{\dot{f}_{\mathsf{a}}^{-1}(g_{\mathsf{a}})^{-\sigma_1}})^c$.

To check the completeness of the above, recall that $B_2 = H_{\mathsf{a}}^{\omega_2} F^{(\dot{f}_{\mathsf{a}})^{-\omega_1}}$; now observe that if $c = 1$ and $\tilde{a}$ and $(f_{\mathsf{a}}, \dot{f}_{\mathsf{a}})$ are well-formed we have that $H_{\mathsf{a}}^{\sigma_2} \cdot \tilde{\mathsf{a}}^{\dot{f}_{\mathsf{a}}^{-1}(g_{\mathsf{a}})^{-\sigma_1}} = H_{\mathsf{a}}^{\sigma_2 + u' \dot{f}_{\mathsf{a}}^{-1}(g_{\mathsf{a}})^{-\sigma_1}} F^{\mathsf{a} \dot{f}_{\mathsf{a}}^{-1}(g_{\mathsf{a}})^{-\sigma_1}} = H_{\mathsf{a}}^{\omega_1} F^{\mathsf{a}\mathsf{a}^{-1}(g_{\mathsf{a}})^{-u-\sigma_1}} = H_{\mathsf{a}}^{\omega_1} F^{(\dot{f}_{\mathsf{a}})^{-u-\omega_1+u}} = B_2$. The case $c = 0$ is straightforward.

Observe that the above proof ensures with probability $1/2$ that the encryption $(f_{\mathsf{a}}, \dot{f}_{\mathsf{a}})$ is consistent with the commitment $\tilde{\mathsf{a}}$. In the AND composition we will (essentially) run this proof k_1 times in parallel (where k_1 is the length of the challenge selected by $\mathcal{V}$).

Protocol #3. The values $\tilde{B}_{\mathsf{a}}, \tilde{A}_{\mathsf{a}}, \tilde{E}_{\mathsf{a}}, \tilde{R}_{\mathsf{a}}$ for $\mathsf{a} \in \{\mathsf{c}, \mathsf{d}, \mathsf{y}\}$ constitute a commitment to a *valid* CL-certificate $\langle A_{\mathsf{a}}, E_{\mathsf{a}}, R_{\mathsf{a}} \rangle$ of the value $a \in \{y, c, d\}$ that is committed into $\tilde{\mathsf{a}}$.

$$\mathsf{PK}\Big(u, u', a, R, E, \pi : (\tilde{B}_{\mathsf{a}} = G^u) \wedge (\tilde{E}_{\mathsf{a}} = Y_2^u G^E) \wedge (\tilde{R}_{\mathsf{a}} = Y_3^u G^R) \wedge (\tilde{\mathsf{a}} = H_{\mathsf{a}}^{u'} F^a) \wedge$$

$$\wedge (\tilde{B}_{\mathsf{a}}^E = G^{\pi}) \wedge (A_{\mathsf{a}}^E = A_0 A_1^y A_2^R Y_1^{\pi})\Big)$$

Protocol #4. The Paillier ciphertexts $\hat{E}_{\mathsf{a}}, \hat{R}_{\mathsf{a}}$ for $\mathsf{a} \in \{\mathsf{c}, \mathsf{d}, \mathsf{y}\}$ hide the same values with the Pedersen commitments $\tilde{E}_{\mathsf{a}}$ and $\tilde{R}_{\mathsf{a}}$ for $\mathsf{a} \in \{\mathsf{c}, \mathsf{d}, \mathsf{y}\}$. This requires a proof of knowledge between a Paillier ciphertext $\hat{c} = \hat{g}^m l^{\hat{n}}$ and a Pedersen commitment $C = Y^u G^m$. The protocol proceeds as follows: the prover computes $c' = g^{m'} l_0^{\hat{n}}$ and $C' = Y^{u'} G^{m'}$ and transmits c', C' to the verifier. The verifier responds by a random challenge $d \in \{0,1\}^{k_1}$ and the prover computes the answer $s = u' - du$, $t = m' - dm$ and $l_1 = l_0 l^{-d}$ and transmits s, t, l_1. The verifier accepts provided that $g^t (\hat{c})^d l_1^{\hat{n}} = c'$ $Y^s G^t C^d = C'$.

Based on the above, the theorem below follows as a corollary of theorem 3.1:

Theorem 4.6 *The* GE *scheme for discrete-logarithms defined above satisfies (i)* Correctness*; (ii)* Anonymity *and (iii)* Security*, both properties under the* $\mathsf{DDH}_{\mathsf{SQNR}}$*,* DDH *over* $\mathcal{Q}_N$*,* DCR *and the collision resistance of the* UOWH *family; (iv)* Soundness*, under the Strong-RSA and the DLOG assumptions.*

Proof. The proof of the theorem is an application of theorem 3.1. In particular we observe the following:
(1). The public-key encryption scheme that is employed by the users satisfies CCA2-key privacy based on theorem 4.5 assuming the $\mathsf{DDH}_{\mathsf{SQNR}}$ assumption (note that we can also design a UOWH function family so that its target collision resistance is also based on $\mathsf{DDH}_{\mathsf{SQNR}}$. Next, note that the encryption scheme employed by the OA satisfies CCA2-security assuming the DDH assumption over the subgroup of quadratic residues $\mathcal{Q}_n$ as well as the factoring assumption; this follows from the fact that the scheme employed by the OA is simply a Cramer-Shoup [CS98] variant over the $\mathbb{Z}_n^*$ group that was investigated by [Luc02]. The commitment scheme we employ to hide the certificate and the public-key satisfies the hiding property under the DDH assumption over $\mathcal{Q}_N$ and the DCR assumption. Regarding the zero-knowledge property observe that the protocol $\langle \mathcal{P}_{pk}, \mathcal{V}_{pk} \rangle$ as well as the protocols presented in section 4.4 satisfy the honest-verifier zero-knowledge (HVZK) property. To turn them into zero-knowledge proofs in various adversarial settings a number of techniques exist, e.g., [Dam00b, GMY03] as well as heuristics [FS86]. For example, using an equivocal commitment (cf. [Dam00b]) we can obtain easily turn all the protocols into concurrent zero-knowledge proofs of knowledge in the common reference string model. The above suggest that the GE scheme satisfies the anonymity property.
(2). The public-key encryption scheme that is employed by the users satisfies CCA2-security based on theorem 4.2 assuming the DCR assumption as well as target collision resistance of the underlying UOWH function family (which in turn can follow from $\mathsf{DDH}_{\mathsf{SQNR}}$ as in case 1). Arguing in the same way as in case 1 we also conclude that the commitment employed for hiding the certificate and the public-key is hiding under the DDH and DCR assumptions over $\mathcal{Q}_N$ as well as the employed protocols are zero-knowledge.
(3). The employed digital signature scheme satisfies adaptive chosen message security based on the Strong-RSA assumption (following [CL02]). Moreover the employed commitment scheme is binding based on the DLOG assumption respectively over $\mathcal{Q}_N$ and the $\langle F \rangle$ subgroup of $\mathbb{Z}_Q^*$. The commitment used for the certificate is extractable by using the the factorization of $\hat{n}$ as the trapdoor as well as the discrete-logarithms of Y_1, Y_2, Y_3 base G within $\mathbb{Z}_N^*$. Finally the soundness of the zero-knowledge

proofs of knowledge of $\langle \mathcal{P}_{pk}, \mathcal{V}_{pk} \rangle$ and $\langle \mathcal{P}, \mathcal{V} \rangle$ can be argued under the Strong-RSA assumption in a similar way as in [FO97, DF02] ■

Length of proof and interaction. The total communication cost for a full $\langle \mathcal{P}, \mathcal{V} \rangle$ interaction is about 70Kbytes if one wants to achieve a knowledge error of 2^{-50}. The GE ciphertext itself is of length 10 Paillier ciphertexts, which for a choice of 1024-bits for the RSA key amounts to 2.5 Kbytes.

4.5 Cascaded Group Encryptions

In the cascaded group encryption setting, instead of a single opening authority, we have a structured group of opening authorities; to open a cascaded group encryption, the opening authorities need to apply in sequence their keys to the cascaded ciphertext following the order selected by the sender; each opening authority will reveal the identity of the next opening authority and can forward the ciphertext to her. The very last opening authority will obtain the identity of Alice's recipient Bob.

In our GE construction above the public-key of the opening authority is $\langle g, \breve{g}, \breve{c}, \breve{d}, \breve{y} \rangle$ and the public-key of the recipient is $\langle g_1, g_2, c, d, y \rangle$ (with g_1, g_2 shared across recipients). In the cascaded encryption setting, each opening authority A will have a key of the form $\langle g, \breve{g}, \breve{c}_A, \breve{d}_A, \breve{y}_A \rangle$ (i.e., all of them will share the same $g, \breve{g}$). Using a similar technique as in our basic construction above, Alice can choose a sequence of opening authorities $A_1, \ldots, A_v$ and will employ the public-key of A_i to encrypt the public-key of A_{i+1} for $i = 1, \ldots, v-1$; finally she will perform a group encryption of her witness under Bob's public-key using the public-key of A_v as the last opening authority.

In order for the above construction to work we need the following: First, the encryption used by opening authorities must satisfy CCA2-key-privacy; given that the encryption used by opening authorities is a Cramer-Shoup [CS98] variant over $\mathcal{X}_{n^2}$, the result will follow from the $\mathsf{DDH}_{\mathsf{SQNR}}$ using similar reasoning as in the proof of theorem 4.5. Second, Alice will need to convince the verifier that the public-key she employs for each opening authority is a certified one; this can be done by requiring all opening authorities to be members of a PKI (or disjoint PKI's if preferred) and Alice will be committing to their certificates as well as proving that they are correct in exactly the same way we demonstrated above where she proves that her recipient's public-key is certified. Thus, the construction methodology we developed for GE is sufficient for efficiently cascading the construction; we omit further details.

References

[ACHdM05] G. Ateniese, J. Camenisch, S. Hohenberger, and B. de Medeiros. Practical group signatures without random oracles. Cryptology ePrint Archive, Report 2005/385, 2005. `http://eprint.iacr.org/`.

[ACJT00] Giuseppe Ateniese, Jan Camenisch, Marc Joye, and Gene Tsudik. A practical and provably secure coalition-resistant group signature scheme. In Mihir Bellare, editor, *Advances in Cryptology – CRYPTO ' 2000*, volume 1880 of *Lecture Notes in Computer Science*. International Association for Cryptologic Research, Springer, 2000.

[AT99] G. Ateniese and G. Tsudik. Some open issues and new directions in group signatures. In Matthew Franklin, editor, *Financial cryptography: Third International Conference, FC '99, Anguilla, British West Indies, February 22–25, 1999: proceedings*, volume 1648 of *Lecture Notes in Computer Science*, pages 196–211. Springer-Verlag, 1999.

[BBDP01] Mihir Bellare, Alexandra Boldyreva, Anand Desai, and David Pointcheval. Key-privacy in public-key encryption. In Colin Boyd, editor, *ASIACRYPT*, volume 2248 of *Lecture Notes in Computer Science*, pages 566–582. Springer, 2001.

[BBS04] Dan Boneh, Xavier Boyen, and Hovav Shacham. Short group signatures. In Matt Franklin, editor, *Advances in Cryptology – CRYPTO 2004*, volume 3152 of *Lecture Notes in Computer Science*, pages 41–55. Springer, 2004.

[Bon98] Dan Boneh. The decision diffie-hellman problem. In *the Third Algorithmic Number Theory Symposium*, volume 1423 of *Lecture Notes in Computer Science*, pages 48–63. Springer-Verlag, 1998.

[BSZ05] Mihir Bellare, Haixia Shi, and Chong Zhang. Foundations of group signatures: The case of dynamic groups. In Alfred Menezes, editor, *CT-RSA*, volume 3376 of *Lecture Notes in Computer Science*, pages 136–153. Springer, 2005.

[BW06] Xavier Boyen and Brent Waters. Compact group signatures without random oracles. In Serge Vaudenay, editor, *EUROCRYPT*, volume 4004 of *Lecture Notes in Computer Science*, pages 427–444. Springer, 2006.

[Cam97] Jan Camenisch. Efficient and generalized group signatures. In Walter Fumy, editor, *Advances in Cryptology - EUROCRYPT '97, International Conference on the Theory and Application of Cryptographic Techniques*, Lecture Notes in Computer Science, pages 465–479. International Association for Cryptologic Research, Springer, 1997.

[CD00] Jan Camenisch and Ivan Damgård. Verifiable encryption, group encryption, and their applications to separable group signatures and signature sharing schemes. In Tatsuaki Okamoto, editor, *ASIACRYPT*, volume 1976 of *Lecture Notes in Computer Science*, pages 331–345. Springer, 2000.

[CL01a] Jan Camenisch and Anna Lysyanskaya. An efficient system for non-transferable anonymous credentials with optional anonymity revocation. In Birgit Pfitzmann, editor, *EUROCRYPT*, volume 2045 of *Lecture Notes in Computer Science*, pages 93–118. Springer, 2001.

[CL01b] Jan Camenisch and Anna Lysyanskaya. An identity escrow scheme with appointed verifiers. In Joe Kilian, editor, *Advances in Cryptology – CRYPTO ' 2001*, volume 2139 of *Lecture Notes in Computer Science*, pages 388–407. International Association for Cryptologic Research, Springer-Verlag, Berlin Germany, 2001.

[CL02] Jan Camenisch and Anna Lysyanskaya. A signature scheme with efficient protocols. In *International Conference on Security in Communication Networks – SCN*, volume 2576 of *Lecture Notes in Computer Science*, pages 268–289. Springer Verlag, 2002.

[CL04] Jan Camenisch and Anna Lysyanskaya. Signature schemes and anonymous credentials from bilinear maps. In Matthew K. Franklin, editor, *CRYPTO*, volume 3152 of *Lecture Notes in Computer Science*, pages 56–72. Springer, 2004.

[CM98] Jan Camenisch and Markus Michels. A group signature scheme with improved efficiency. In Kazuo Ohta and Dingyi Pei, editors, *ASIACRYPT: Advances in Cryptology – ASIACRYPT: International Conference on the Theory and Application of Cryptology*, volume 1514 of *Lecture Notes in Computer Science*, pages 160–174. International Association for Cryptologic Research, Springer-Verlag, 1998.

[CM99] Jan Camenisch and Markus Michels. Separability and efficiency for generic group signature schemes (extended abstract). In Michael j. Wiener, editor, *19th International Advances in Cryptology Conference – CRYPTO '99*, volume 1666 of *Lecture Notes in Computer Science*, pages 413–430. Springer, 1999.

[CP94] L. Chen and T. P. Pedersen. New group signature schemes (extended abstract). In Alfredo De Santis, editor, *Advances in Cryptology—EUROCRYPT 94*, volume 950 of *Lecture Notes in Computer Science*, pages 171–181. Springer-Verlag, 1995, 9–12 May 1994.

[CS97] Jan Camenisch and Markus Stadler. Efficient group signature schemes for large groups. In Burton S. Kaliski Jr., editor, *Advances in Cryptology – CRYPTO ' 1997*, volume 1294 of *Lecture Notes in Computer Science*, pages 410–424. International Association for Cryptologic Research, Springer, 1997.

[CS98] Ronald Cramer and Victor Shoup. A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. In Hugo Krawczyk, editor, *CRYPTO 1998*, pages 13–25. Springer-Verlag, 1998. Lecture Notes in Computer Science No. 1462.

[CS03] Jan Camenisch and Victor Shoup. Practical verifiable encryption and decryption of discrete logarithms. In *CRYPTO 2003*. Springer-Verlag, 2003.

[CvH91] D. Chaum and E. van Heyst. Group signatures. In D. W. Davies, editor, *Advances in Cryptology, EUROCRYPT 1991 (Lecture Notes in Computer Science 547)*, pages 257–265. Springer-Verlag, April 1991. Brighton, U.K.

[Dam00a] Ivan Damgård. Efficient concurrent zero-knowledge in the auxiliary string model. In *EUROCRYPT*, pages 418–430, 2000.

[Dam00b] Ivan Damgård. Efficient concurrent zero-knowledge in the auxiliary string model. In *EUROCRYPT*, pages 418–430, 2000.

[DDN91] Danny Dolev, Cynthia Dwork, and Moni Naor. Non-malleable cryptography (extended abstract). In *Proceedings of the Twenty Third Annual ACM Symposium on Theory of Computing*, pages 542–552, New Orleans, Louisiana, 6–8May 1991.

[Des87] Yvo Desmedt. Society and group oriented cryptography: A new concept. In Carl Pomerance, editor, *CRYPTO*, volume 293 of *Lecture Notes in Computer Science*, pages 120–127. Springer, 1987.

[DF02] Ivan Damgård and Eiichiro Fujisaki. A statistically-hiding integer commitment scheme based on groups with hidden order. In *ASIACRYPT: Advances in Cryptology – ASIACRYPT: International Conference on the Theory and Application of Cryptology*, Lecture Notes in Computer Science, pages 125–142. Springer-Verlag, 2002.

[FO97] Eiichiro Fujisaki and Tatsuaki Okamoto. Statistical zero knowledge protocols to prove modular polynomial relations. In Burton S. Kaliski, Jr., editor, *Advances in Cryptology – CRYPTO ' 97*, volume 1294 of *Lecture Notes in Computer Science*, pages 16–30. International Association for Cryptologic Research, Springer-Verlag, Berlin Germany, 1997.

[FS86] Amos Fiat and Adi Shamir. How to Prove Yourself: Practical Solutions to Identification and Signature Problems. In *Proceedings of CRYPTO'86*, volume 263 of *Lecture Notes in Computer Science*, pages 186–194. Springer Verlag, 1986.

[GIL+90] Oded Goldreich, Russell Impagliazzo, Leonid A. Levin, Ramarathnam Venkatesan, and David Zuckerman. Security preserving amplification of hardness. In *FOCS*, volume I, pages 318–326. IEEE, 1990.

[GL03] Rosario Gennaro and Yehuda Lindell. A framework for password-based authenticated key exchange. In Eli Biham, editor, *Advances in Cryptology – EUROCRYPT 2003*, volume 2656 of *Lecture Notes in Computer Science*, Warsaw, Poland, 2003. Springer.

[GMR84] Shafi Goldwasser, Silvio Micali, and Ronald L. Rivest. A "paradoxical" solution to the signature problem (extended abstract). In *25th Annual Symposium on Foundations of Computer Science*, pages 441–448, Singer Island, Florida, 24–26October 1984. IEEE.

[GMW91] Oded Goldreich, Silvio Micali, and Avi Wigderson. Proofs that yield nothing but their validity or all languages in np have zero-knowledge proof systems. *J. ACM*, 38(3):691–729, 1991.

[GMY03] Juan A. Garay, Philip D. MacKenzie, and Ke Yang. Strengthening zero-knowledge protocols using signatures. In Eli Biham, editor, *EUROCRYPT*, volume 2656 of *Lecture Notes in Computer Science*, pages 177–194. Springer, 2003.

[Gol04] Oded Goldreich. *The Foundations of Cryptography - Volume 1*. Cambridge University Press, 2004.

[Gro06] Jens Groth. Simulation-sound nizk proofs for a practical language and constant size group signatures. In Xuejia Lai and Kefei Chen, editors, *ASIACRYPT*, volume 4284 of *Lecture Notes in Computer Science*, pages 444–459. Springer, 2006.

[Hal05] Shai Halevi. Sufficient condition for key privacy. Cryptology ePrint Archive, Report 2005/005, 2005. `http://eprint.iacr.org/`.

[KP98] Joe Kilian and Erez Petrank. Identity escrow. In Hugo Krawczyk, editor, *Advances in Cryptology – CRYPTO 1998*, volume 1462 of *Lecture Notes in Computer Science*, pages 169–185. International Association for Cryptologic Research, Springer, 1998.

[KY03] Aggelos Kiayias and Moti Yung. Extracting group signatures from traitor tracing schemes. In Eli Biham, editor, *Advances in Cryptology – EUROCRYPT 2003*, volume 2656 of *Lecture Notes in Computer Science*, pages 630–648, Warsaw, Poland, 2003. Springer.

[KY05] Aggelos Kiayias and Moti Yung. Group signatures with efficient concurrent join. In Ronald Cramer, editor, *EUROCRYPT*, volume 3494 of *Lecture Notes in Computer Science*, pages 198–214. Springer, 2005.

[KY06] Aggelos Kiayias and Moti Yung. Secure scalable group signature with dynamic joins and separable authorities. *Int. J. Security and Networks*, 1(1/2):24–45, 2006.

[Luc02] Stefan Lucks. A variant of the cramer-shoup cryptosystem for groups of unknown order. In Yuliang Zheng, editor, *ASIACRYPT*, volume 2501 of *Lecture Notes in Computer Science*, pages 27–45. Springer, 2002.

[NY89] Moni Naor and Moti Yung. Universal one-way hash functions and their cryptographic applications. In *STOC*, pages 33–43. ACM, 1989.

[Pai99] Pascal Paillier. Public-key cryptosystems based on composite degree residuosity classes. In *Advances in cryptology—EUROCRYPT 1999*, volume 1592 of *Lecture Notes in Computer Science*, pages 223–238, 1999.

[Rom90] John Rompel. One-way functions are necessary and sufficient for secure signatures. In *STOC*, pages 387–394. ACM, 1990.

[RS92] Charles Rackoff and Daniel R. Simon. Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack. In Joan Feigenbaum, editor, *Advances in Cryptology – CRYPTO ' 91*, volume 576 of *Lecture Notes in Computer Science*, pages 433–444. International Association for Cryptologic Research, Springer-Verlag, Berlin Germany, 1992.

[Sta96] Markus Stadler. Publicly verifiable secret sharing. In Ueli Maurer, editor, *Advances in Cryptology – EUROCRYPT ' 96*, volume 1070 of *Lecture Notes in Computer Science*, pages 190–199. International Association for Cryptologic Research, Springer, 1996.

[TW05] Mårten Trolin and Douglas Wikström. Hierarchical group signatures. In Luís Caires, Giuseppe F. Italiano, Luís Monteiro, Catuscia Palamidessi, and Moti Yung, editors, *ICALP*, volume 3580 of *Lecture Notes in Computer Science*, pages 446–458. Springer, 2005.

[Yao82] Andrew C. Yao. Theory and applications of trapdoor functions (extended abstract). In *23rd Annual Symposium on Foundations of Computer Science*, pages 80–91, Chicago, Illinois, 3–5November 1982. IEEE.