Non-Interactive Commitment from Non-Transitive Group Actions

Giuseppe D'Alconzo[1], Andrea Flamini[2], and Andrea Gangemi[1,2]

[1] Department of Mathematical Sciences, Politecnico di Torino, Corso Duca degli Abruzzi 24, 10129 Torino, Italy
[2] Department of Mathematics, University of Trento, Povo, 38123 Trento, Italy
giuseppe.dalconzo@polito.it, andrea.flamini@unitn.it, andrea.gangemi@unitn.it

Abstract. Group actions are becoming a viable option for post-quantum cryptography assumptions. Indeed, in recent years some works have shown how to construct primitives from assumptions based on isogenies of elliptic curves, such as CSIDH, on tensors or on code equivalence problems. This paper presents a bit commitment scheme, built on non-transitive group actions, which is shown to be secure in the standard model, under the decisional Group Action Inversion Problem. In particular, the commitment is computationally hiding and perfectly binding, and is obtained from a novel and general framework that exploits the properties of some orbit-invariant functions, together with group actions. Previous constructions depend on an interaction between the sender and the receiver in the commitment phase, which results in an interactive bit commitment. We instead propose the first non-interactive bit commitment based on group actions. Then we show that, when the sender is honest, the constructed commitment enjoys an additional feature, i.e., it is possible to tell whether two commitments were obtained from the same input, without revealing the input. We define the security properties that such a construction must satisfy, and we call this primitive *linkable commitment*. Finally, as an example, an instantiation of the scheme using tensors with coefficients in a finite field is provided. In this case, the invariant function is the computation of the rank of a tensor, and the cryptographic assumption is related to the Tensor Isomorphism problem.

Keywords— *Cryptographic group actions, Non-transitive group actions, Bit commitments, Linkable commitments, Tensors*

1 Introduction

Group Actions in Cryptography. Recent developments in quantum computing make the advent of a quantum machine suitable for cryptanalysis purposes a threat. Many cryptographic algorithms that are used nowadays can no longer be considered secure against a quantum attacker. Primitives relying on the hardness of the Discrete Logarithm or the Factorization problem are broken by the well

known Shor's algorithm [Sho94]. This leads to the birth of the Post-Quantum Cryptography, that aims to find and study protocols based on cryptographic assumptions that appear to be resistant to attacks performed by quantum computers. The most promising ones are based on lattices, multivariate polynomials, hash functions, error correcting codes and isogenies of elliptic curves. However, in order to increase the variety of probably secure assumptions, it is necessary to find new problems with useful features to build new cryptographic protocols. A recent line of study concerns equivalence problems and cryptographic group actions. The most known reference is given by Couveignes in 2006 [Cou06] and was used in the setting of isogeny-based cryptography. Moreover, the explicit use of group actions can be found in the 1991 article of Brassard and Young [BY91]. More recently, the framework has been studied by Grigoriev and Shpilrain, [GS10], Alamati, De Feo, Montgomery and Patranabis [ADMP20] and Ji, Qiao, Feng and Yun [JQSY19], introducing some formal cryptographic assumptions. There are many group actions suitable for post-quantum cryptography, arising from different areas of mathematics and computer science. Some examples can be the class group action of CSIDH [CLM+18], the one induced by the general linear group on various objects [JQSY19; RST22; TDJ+22], the action acting on polynomials [Pat96] or the ones concerning linear codes [BBPS23; RST22]. In the last years, cryptographic group actions have been employed to design many primitives such as sigma protocols and signature schemes (via the GMW scheme for Graph Isomorphism [GMW91]), ring and group signatures [BKP20; BDK+23], key exchanges [CLM+18] and updatable encryption schemes [LR22].

Commitment Schemes. A commitment scheme is a cryptographic protocol between two parties, a sender and a receiver. The sender wants to commit to a value b without revealing it to the other party. To do this, he binds b to a commitment C that is sent to the receiver. In a second moment, the sender wants to reveal b and the receiver must be able to verify that it was the committed value behind C. A commitment must satisfy two security properties: it must not reveal any information about the committed value (hiding property), and the sender cannot reveal a different $b' \neq b$ that opens to the same commitment (binding property).
Commitment schemes are widely used, both as stand-alone protocols and as atomic parts of more involved mechanisms. For example, they are used in Zero-Knowledge proofs [LNS21], digital auctions [OPV09], signature schemes [JLO06], multi-party computation [FPY18], e-voting [DE17] and confidential transactions [PBF+19]. In this work, we will mainly focus on *bit* commitments, where the committed value b can be 1 or 0.

Related works. Bit commitments schemes are a component of many cryptographic algorithms. In 1991, Naor [Nao91] showed how to obtain a bit commitment protocol starting from a pseudorandom generator. Bit committments from group actions are known in literature. In 1991 Brassard and Young [BY91]

present an interactive scheme from certified and uncertified group actions. In 2019 Ji, Qiao, Song and Yun [JQSY19] present, among other construction, two interactive bit commitment schemes relying on cryptographic assumptions on non-abelian group actions.
Finally, another famous commitment, which is however based on a non post-quantum assumption, is the *Pedersen commitment* [Ped01]. This scheme has an interesting property: it can be shown that two commitments are created starting from the same value, without opening the commitments [PBF+19].

Our Contribution. We present a bit commitment scheme that is non-interactive, perfectly binding and computationally hiding in the standard model. This scheme is based on a group action framework that makes use of certain invariant functions. One of the innovative aspects of our proposal is that it concerns *non-transitive* group actions, while known cryptographic applications use transitive actions or they restrict to one orbit. The non-transitivity of the action used in this paper is crucial and necessary, in fact we need to be able to exhibit two elements that are in two different orbits. Such elements are generated with the aid of the new group action framework, in which we endow the group action with a function that is constant inside the orbits. Given the group G acting on the set X via the action $\star$, an *invariant function* $f : X \to T$, with T be a set, has the following property

$$f(g \star x) = f(x), \quad \forall x \in X, g \in G.$$

The key point is that evaluating this function on a randomly chosen element is hard, while for a particular subset of elements, that we call *canonical elements*, it is easy to compute. Also, the fact that the function is constant inside the orbits guarantees that, if we consider two elements with distinct image, they must live in (and generate under the action of G) distinct orbits. This observation is crucial to prove our commitment scheme is perfectly binding. We call *Group Action with Canonical Elements* (GACE) a group action with the above properties. Moreover, the existence of decision problems about whether an element is randomly picked from a specific orbit or not enables us to prove that our commitment scheme is computationally hiding.
The structure of our construction enables an additional property that is shared with the Pedersen commitment. An honest sender generating two commitments of the same value b can prove to the receiver that they are in fact linked to the same message, without revealing it. We call this scheme a *linkable commitment* and we formally define the security properties that enable the adoption of such a primitive in cryptography. However, using some techniques from ring signature schemes [BKP20], we show how to extend this property to the case of a possibly malicious sender in the Random Oracle Model.
This work is organized as follows: Section 2 recaps all the cryptographic tools that will be used in the rest of the paper, while Section 3 introduces the framework that we will use to design a non-interactive commitment scheme starting from cryptographic group actions. In particular, we introduce the concept of

Group Action with Canonical Elements. Section 4 shows how to design a bit commitment starting from canonical elements, and its security is proved under the decisional Group Action Inversion Problem assumption, while in Section 5 we introduce the notion of linkable commitments and we show how our protocol is indeed a linkable one. Section 6 shows an instantiation of the framework with tensors, and finally Section 7 concludes the work and gives some idea for further research.

2 Preliminaries

In the course of this paper, with $\Pr[A]$ we denote the probability of the event A. Let λ denote the security parameter, this means that the parameters of the cryptographic schemes instantiated with security parameter λ are chosen in such a way that the best known attack would break the scheme using at least 2^λ operations. A function $f(\lambda)$ is *negligible* in λ if for every positive integer c there exists a λ_0 such that for each $\lambda > \lambda_0$ we get $f(\lambda) < \frac{1}{\lambda^c}$.
Finally, in the pseudocode "$\leftarrow\!\!\$$" denotes the random sampling, "$\leftarrow$" is a variable assignment and "$=$" is the equality check.

2.1 Group Actions

This section introduces group actions, along with the complexity assumptions that must be made in order to use them in cryptographic protocols. Definitions reported here are mostly taken from [ADMP20]. We point out that through this work we do not need the action to be abelian, contrary to what is required in [Cou06] or [ADMP20]. All the following definitions and constructions are meaningful also in the non-abelian case.

Definition 1. *A group G is said to act on a set X if there is a map $\star : G \times X \to X$ that satisfies the following properties:*

- Identity*: if e is the identity element of the group G, then $e \star x = x$ for every x in X.*
- Compatibility*: given g and h in G and x in X, we have that $(gh) \star x = g \star (h \star x)$.*

In this case, we say that the triple $(G, X, \star)$ is a group action*.*

A group action $(G, X, \star)$ may satisfy some algebraic properties that lead to the definition of classes of group actions, namely the action is *transitive* if for all x_1, x_2 in X there exists an element g in G such that $x_1 = g \star x_2$; moreover, the action is said *free* when the following holds: g is the identity element of G if and only if there is an x in X such that $g \star x = x$. Finally, we say that the action is *regular* if it is both free and transitive.
Note that, if the group action $(G, X, \star)$ is regular and the group G is finite, then for every x in X the map $g \mapsto g \star x$ is a bijection and $|G| = |X|$. Furthermore,

if the group action is regular, then we can define the element $\delta(x, y)$ of G as the unique element for which $x = \delta(x, y) \star y$. If the action is not transitive, instead, then there exist x and y in X such that $\delta(x, y)$ does not exist.

Alamati, De Feo, Montgomery and Patranabis also define the concept of *effective group action*: a formal definition can be found in [ADMP20], here we just report the key points.

Definition 2. *A group action* $(G, X, \star)$ *is* effective *if:*

- *the group* G *is finite and there exists a probabilistic polynomial time* (PPT) *algorithm for executing membership and equality testing, sampling, and for computing the group operation and the inverse of an element;*
- *The set* X *is finite and there exist* PPT *algorithms for computing membership testing and the unique representation of any element in* X*;*
- *There exists an efficient algorithm to compute* $g \star x$*, for each* g *in* G *and* x *in* X*.*

Informally, a group action is said effective if it can be manipulated easily and it can be computed in practical time. An example of non-effective group actions is the set of polynomials in m variables of bounded degree n over a finite field, with the symmetric group $\mathcal{S}_m$, permuting the variables. It can be seen that the unique representation is given by the algebraic normal form, but it cannot be computed in polynomial time in n and m.

In the rest of this work, even when not explicitly written, we will consider effective group actions.

2.2 Cryptographic assumptions on group actions

The presented definition leads to efficient group actions, which can be used to build cryptographic protocols. However, in order to use them in cryptography we need to define some suitable computational assumptions. In [ADMP20] the authors report some computational assumptions on group actions, for instance the following embraces the fact that, given two random elements $x, y \in X$ in the same orbit, then it must be intractable to compute $\delta(x, y)$.

Definition 3. *Let* λ *be a parameter indexing* G *and* X*. Being* $\mathcal{D}_G$ *and* $\mathcal{D}_X$ *two distributions over* G *and* X *respectively, then the group action* $(G, X, \star)$ *is* $(\mathcal{D}_G, \mathcal{D}_X)$-one-way *if for all* PPT *adversaries* $\mathcal{A}$ *there is a negligible function* $\mathtt{negl}(\lambda)$ *such that*

$$\Pr[\mathcal{A}(x, g \star x) \star x = g \star x] \leq \mathtt{negl}(\lambda),$$

where x *is sampled according to* $\mathcal{D}_X$ *and* g *according to* $\mathcal{D}_G$*.*

In this paper, we assume that $\mathcal{D}_G$ and $\mathcal{D}_X$ are the uniform distributions over G and X, and we refer to this assumption as *One-way group action assumption.*

Another assumption that can be used when working with group actions is the *Group Action Pseudo Randomness* (GA-PR) problem, defined in [JQSY19]. It can be seen as a generalisation of the Decisional Diffie-Hellman assumption. An equivalent assumption can be found in [ADMP20], and a group action with this propriety is called *weakly pseudorandom*. For example, in [JQSY19], the authors state that it can be applied to the general linear group action on tensors. Let us now define more formally the problem on which the GA-PR assumption is based.

Definition 4. *Let $\mathcal{G}$ be a group action family such that for a security parameter λ, $\mathcal{G}(1^\lambda)$ returns an effective group action $(G, X, \star)$ with $\log(|G|) = poly(\lambda)$, $\log(|S|) = poly(\lambda)$. Denote the triple as a public parameter $\mathsf{pp} = (G, X, \star)$. Sample $s \leftarrow\!\!\$\ X$ and $g \leftarrow\!\!\$\ G$. The* Group Action Pseudo Randomness *(GA-PR) problem is the following: given (s, t) with $t = g \star s$ or $t \leftarrow\!\!\$\ X$, decide which case t is sampled from.*

To ease the security proofs, we can reformulate the above problem in terms of adversary-challenger game.

Definition 5. *The* group action pseudo random game *(GA-PR) is given in Figure 1. We define the* advantage *of an adversary $\mathcal{A}$ of GA-PR as*

$$\mathsf{Adv}(\mathcal{A}, \textit{GA-PR}) = \left|\Pr[\mathcal{A} \textit{ wins } \text{GA-PR}(\mathsf{pp})] - \frac{1}{2}\right|.$$

The GA-PR assumption states that for all PPT *adversaries $\mathcal{A}$ there is a negligible function* $\mathtt{negl}(\lambda)$*, with λ being the security parameter, such that*

$$\mathsf{Adv}(\mathcal{A}, \textit{GA-PR}) \leq \mathtt{negl}(\lambda),$$

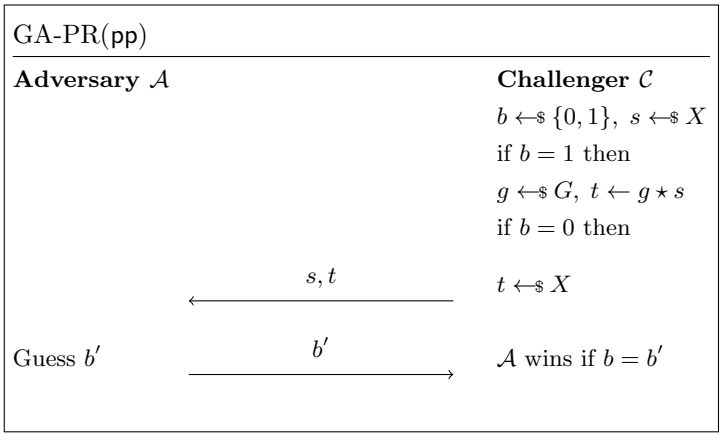

Fig. 1. Group Action Pseudo Random game.

For the bit commitment scheme, we will refer to the GA-PR assumption when the set X consists of only two orbits. We call this new assumption and the relative game 2GA-PR.

We remark that the adversary of the GA-PR game must be able to distinguish whether the challenger has picked the element t uniformly at random inside the orbit of s or inside the set X. However, when t is picked inside X, it is still possible that t is picked inside the orbit of s as well; therefore, even a computationally unbounded adversary would not be able to win the game with probability 1.

In particular, if we consider the 2GA-PR game, and suppose the two orbits have the same cardinality, the event that t is picked uniformly at random inside the set X and t results to be an element in the orbit of s is $\frac{1}{4}$. Therefore, even an adversary with unbounded computational power, who can distinguish whether t lives in the same orbit of s or not, cannot win the game with probability greater than $\frac{3}{4}$.

The observation above motivates the introduction of an assumption which we refer to as *decisional Group Action Inversion Problem* (dGA-IP). The dGA-IP problem, also known as Isomorphism Problem [JQSY19], is the decisional variant of the group action inversion problem presented in [Sto12], applied to the case in which the set X is given by only two orbits. If the restriction on the two orbits is removed, a large number of similar problems can be found in literature [GQ19; GQ21; PR97].

Definition 6. *The* dGA-IP game *is presented in Figure 2, where* pp *is given by the tuple* $(G, X, \star, t_0, t_1)$*, with* t_0 *and* t_1 *elements that lie in distinct orbits under the action of* G*. We define the advantage of an adversary* $\mathcal{A}$ *of dGA-IP as*

$$\mathsf{Adv}(\mathcal{A}, \textit{dGA-IP}) = \left|\Pr[\mathcal{A} \textit{ wins } \textit{dGA-IP}(\mathsf{pp})] - \frac{1}{2}\right|.$$

The dGA-IP assumption *states that for all* PPT *adversaries* $\mathcal{A}$ *there is a negligible function* $\mathtt{negl}(\lambda)$*, with* λ *being the security parameter, such that*

$$\mathsf{Adv}(\mathcal{A}, \textit{dGA-IP}) \leq \mathtt{negl}(\lambda),$$

This game, compared to 2GA-PR, reflects more clearly the fact that it is hard to distinguish whether two elements in X live in the same orbit or not, and an adversary with unbounded computational power would win this game with probability 1.

2.3 Commitment schemes

A commitment scheme is a cryptographic scheme that allows one party to commit to a value m by sending a commitment $\mathtt{com}$, and then to reveal m by opening the commitment at a later point in time.

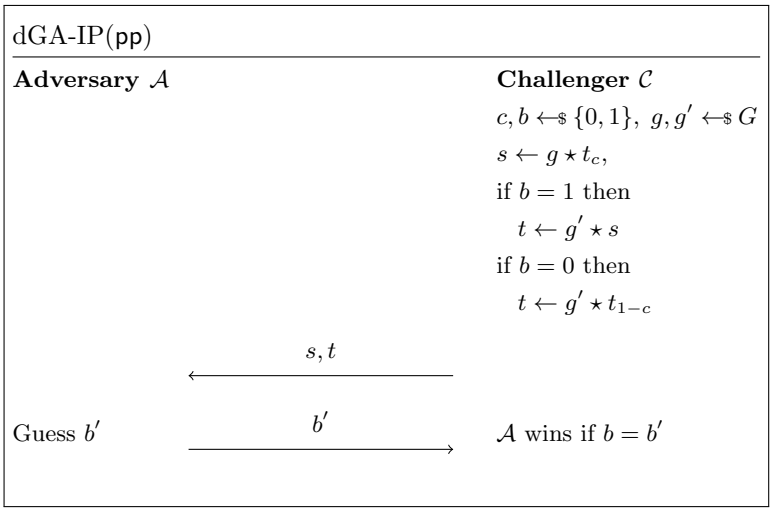

Fig. 2. decisional Group Action Inversion Problem game.

Definition 7. *A* commitment scheme *on a message space $\mathcal{M}$ is a triple of* PPT *algorithms* $(\mathsf{PGen}, \mathsf{Commit}, \mathsf{Open})$ *such that:*

1. $\mathsf{PGen}(1^\lambda)$ *takes as input a security parameter λ in unary and returns public parameters* pp*;*
2. $\mathsf{Commit}(\mathsf{pp}, m)$ *takes as input the public parameters* pp*, a message m in $\mathcal{M}$ and returns the commitment* com *and the* opening material *r;*
3. $\mathsf{Open}(\mathsf{pp}, m, \mathtt{com}, r)$ *takes as input the public parameters* pp*, the message m, the commitment* com *and the opening material r and returns* **accept** *if* com *is the commitment of m or* **reject** *otherwise.*

In the rest of this work we omit the public parameters pp in the inputs of Commit and Open.

To be suitable in cryptography, commitment schemes must satisfy the *hiding* and *binding* properties. Hiding means that com reveals nothing about m and binding means that it is not possible to create a commitment com that can be opened in two different ways. These properties are formally defined.

Definition 8. *Let $\Pi_{\mathsf{Com}} = (\mathsf{PGen}, \mathsf{Commit}, \mathsf{Open})$ be a commitment scheme and let* Hiding(Π_{Com}) *be the hiding game represented in Figure 3. We define the advantage of an adversary $\mathcal{A}$ of* Hiding(Π_{Com}) *as*

$$\mathsf{Adv}(\mathcal{A}, \text{Hiding}(\Pi_{\mathsf{Com}})) = \left|\Pr[\mathcal{A} \textit{ wins } \text{Hiding}(\Pi_{\mathsf{Com}})] - \frac{1}{2}\right|.$$

A commitment scheme Π_{Com} is computationally hiding *if for all* PPT *adversaries $\mathcal{A}$ there is a negligible function* $\mathtt{negl}(\lambda)$*, with λ being the security parameter, such that*

$$\mathsf{Adv}(\mathcal{A}, \text{Hiding}(\Pi_{\mathsf{Com}})) \leq \mathtt{negl}(\lambda),$$

If, for every pair m_0, m_1, the commitments $\mathtt{com}_0$ and $\mathtt{com}_1$ have the same distribution, where $(\mathtt{com}_i, r_i) = \mathsf{Commit}(m_i)$ for $i = 0, 1$, we say that the commitment is perfectly hiding.

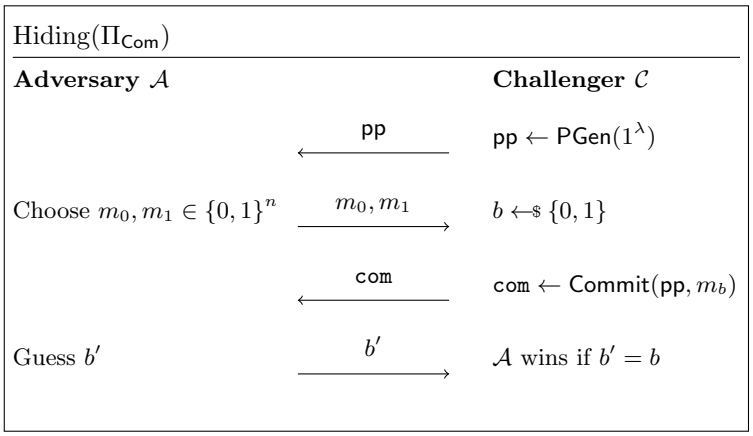

Fig. 3. Hiding game for commitment schemes.

Note that, in the case of a bit commitment, the adversary does not send m_0 and m_1, and the bit chosen by the challenger is the committed bit in $\mathtt{com}$.

Definition 9. *A commitment scheme $\Pi_{\mathsf{Com}} = (\mathsf{PGen}, \mathsf{Commit}, \mathsf{Open})$ is* computationally binding *if for all PPT adversaries $\mathcal{A}$ there is a negligible function $\mathtt{negl}(\lambda)$, with λ being the security parameter, such that*

$$\Pr\left[(\mathtt{com}, m_0, r_0, m_1, r_1) \leftarrow \mathcal{A}(\mathsf{pp}) \;\middle|\; \begin{array}{c} \mathsf{pp} \leftarrow \mathsf{PGen}(1^\lambda), \\ m_0 \neq m_1, \\ \mathsf{Open}(m_0, \mathtt{com}, r_0) = \textbf{accept}, \\ \mathsf{Open}(m_1, \mathtt{com}, r_1) = \textbf{accept} \end{array}\right] \leq \mathtt{negl}(\lambda).$$

If for every adversary $\mathcal{A}$ it holds that $\mathtt{negl}(\lambda) = 0$, we say that the commitment scheme is perfectly binding.

Commitment schemes from Group Actions Previous commitments were known from cryptographic group actions. Brassard and Young [BY91] propose two kind of bit commitments from what they call *certified* and *uncertified* group actions. A certified group action is an action from the group G over the set X such that checking that two elements are in the same orbit is an easy task. On the contrary, the same verification could not be polynomial-time for an uncertified group action. Since the problem of deciding whether two elements of X are in the same orbit is assumed to be hard in this work, we will focus on the latter case.

Given a group action from G on X, the computationally binding and perfectly hiding bit commitment presented in [BY91] is as follows.

- The receiver randomly generates x_0 from X and g from G. Then sets x_1 as $g \star x_0$. He sends to the sender the pair (x_0, x_1) and a proof π that they are in the same orbit.
- The sender wants to commit to the bit b. First, he checks that the proof π is valid, then he picks h from G and sends $\texttt{com} = h \star x_b$ to the receiver, keeping secret h.
- To open the committed bit b, the sender reveals b and h to the receiver, which checks that com is equal to $h \star x_b$.

The first thing to notice is that this is an interactive bit commitment, since the sender needs the receiver's cooperation for the creation of the commitment. Secondly, the communication cost is at least as big as the proof of the statement that x_0 and x_1 are in the same orbit. This is an NP-statement (the witness is given by g) and hence admits an interactive proof (even a non-interactive one, using the Fiat-Shamir heuristic and the Random Oracle Model), but it can be very large in communication.

In [JQSY19], Ji, Qiao, Song and Yun propose two bit commitment protocols. The first is a slight generalization of the protocol from [BY91], using non-abelian group actions. The obtained protocol has the same drawbacks noticed above: it is interactive and has a large communication cost. The second proposal concerns the use of the following pseudorandom function

$$f : X \times G \to X \times X, \quad (x, g) \mapsto (x, g \star x)$$

and, after applying the Blum-Micali amplification [BM19], the authors build an interactive bit commitment scheme using the construction from [Nao91]. In this construction it is needed that $|X| \geq |G|$, and the obtained bit commitment is statistically binding and computationally hiding.

3 Our Framework

The goal of this section is to design a non-interactive commitment scheme using assumptions from cryptographic group actions. We will focus on non-abelian and non-transitive actions. To develop such a commitment scheme, we first analyze the issues arising from an initial construction, then we define a framework that we use to circumvent these problems.

3.1 A first attempt

Based on the non-transitivity of the group action $(G, X, \star)$, we can do a first attempt in building a *non-interactive* bit commitment scheme. We give its description using a trusted third party (TTP), and then we analyze how to remove it.

Given the action $(G, X, \star)$, the TTP chooses and publishes two elements x_0 and x_1 of X laying in different orbits. The sender, to commit a bit b, generates a random g in G and sets as the commitment of b the value $\texttt{com} = g \star x_b$. The opening material is g. In other words, the sender picks a random element in the orbit of x_b. In the opening phase, given b, com and g, the receiver accepts if com is equal to $g \star x_b$ and rejects otherwise. Informally, the hiding propriety is given by the fact that checking whether com is in the orbit of x_0 or x_1 is hard, while the binding propriety follows from the impossibility of going from an orbit to another via the action of G.
In the following we try to remove the TTP and analyze some possible scenarios.

1. **The sender generates and publish x_0 and x_1.** In this case we can see that a malicious sender can generate x_0 and x_1 in the same orbit via $x_1 = h \star x_0$. He commits to $g \star x_0$ and, during the opening phase, he could open to both 0 and 1 using g or gh^{-1}. In this case, the binding property does not hold.
2. **The sender generates and publish x_0, x_1 together with a proof π that they are in different orbits.** Given a proof π that x_0 and x_1 are not in the same orbit, we obtain that the protocol is hiding and binding, under the assumption that deciding whenever two elements share the orbit is hard. In this scenario, the hard task is the generation of the proof π. In fact, the language
$$L = \{(y_0, y_1) \in X \times X \mid y_0 \text{ and } y_1 \text{ are in different orbits}\}$$
is in coNP. Unless we have a computationally unbounded prover [GMW91] (and this is not the case), it means that known techniques fails to generate a short non-interactive proof for L which would enable the design of a non-interactive commitment scheme. Since interactive bit commitments based on group actions are known [BY91; JQSY19], we do not further study this case.
3. **The receiver generates and publish x_0 and x_1.** We are again in the case of interactive bit commitments, and we remand to the known schemes based on group actions.

With such techniques, we have seen that there are some tricky aspects that are hard to deal with. For example, we need to build a proof for a language in coNP, and the absence of a witness (as we are used to, when we work in NP) is the first obstacle. To overcome such difficulties, we introduce a general framework on group actions that ease the design of the non-interactive bit commitment sketched above. The trick is the definition of an invariant function that is constant inside the orbits and is hard to compute for a randomly chosen element. However, we assume that there is a set of representative elements for which the computation of such function is easy. This avoids the need of a proof for the above language L. These concepts will be formalized in the next subsection.

3.2 Group Actions with Canonical Elements

In this section, we introduce the concepts of invariant functions and canonical elements, and we present the cryptographic assumptions linked to them.

Definition 10. *Given a group action $(G, X, \star)$ and a function $f : X \to T$, we say that f is* invariant under the action of G *if $f(g \star x) = f(x)$ for every g in G and every x in X. We say that f is* fully invariant *if $f(x) = f(y)$ if and only if there exists g in G such that $y = g \star x$.*

In the following, we can assume that f is surjective, restricting the set T to the image $f(X)$. To exploit the property of invariant function while keeping the dGA-IP hard, we want the function f to be hard to compute on a large class of elements of X. At the same time, we want to define particular elements of X on which the computation of f is feasible.

Definition 11. *Let $f : X \to T$ be a surjective invariant function for the action $(G, X, \star)$ and let $T' \subset T$. Suppose that there exists a polynomial-computable map*

$$\langle \cdot \rangle : T' \to X, \quad t \mapsto \langle t \rangle$$

such that the function $f \circ \langle \cdot \rangle$ is the identity on the subset T' of T. We call $\langle \cdot \rangle$ the canonical representation of T' in X *and $\langle t \rangle$ the* canonical t-element *(with respect to f and $\langle \cdot \rangle$). If $T' = T$, we say that $\langle \cdot \rangle$ is* complete. *Moreover, we say that $(G, X, \star, f, \langle \cdot \rangle)$ is a* Group Action with Canonical Element *(GACE) if the following hold:*

1. *if $O(z)$ is the orbit of z in X, then for any* PPT *adversary $\mathcal{A}$ there is a negligible function* `negl` *such that*

$$\Pr[\mathcal{A}(x) = f(x)] \leq \frac{1}{|T'|} + negl(|x|),$$

   where x is sampled uniformly random from $\bigsqcup_{t \in T'} O(\langle t \rangle)$;
2. *there is a* PPT *algorithm that for any t in T' computes $f(\langle t \rangle)$.*

In other words, the definition above says that, for every t in T', we have $f(\langle t \rangle) = t$ and the function f is hard to compute in general, but is instead easy to calculate on canonical elements. Moreover, the construction of such $\langle t \rangle$ is a polynomial-time task.

In the following constructions, whenever a random element of X is needed, we pick a random canonical element $\langle t \rangle$, a random g from G and compute $g \star \langle t \rangle$. In this way, instead of using the whole X, we always work with the disjoint union of the orbits of the canonical elements. In other words, the set on which the group G acts becomes

$$X' = \bigsqcup_{t \in T'} O(\langle t \rangle).$$

This implies that the GACE $(G, X', \star, f, \langle \cdot \rangle)$ has a fully invariant function f and the canonical representation $\langle \cdot \rangle$ is complete. Given a fully invariant function f, the problem of determining whether two elements have the same image under f is equivalent to deciding whether they lie in the same orbit (dGA-IP).

4 The Commitment Scheme

4.1 Bit commitment scheme from a GACE

The first application of our framework is a bit commitment scheme. Given a Group Action with Canonical Elements, we design the commitment scheme described in Figure 4, following the attempts shown in Subsection 3.1. The bit commitment is proven secure under both the dGA-IP assumption that we have introduced in this paper and the 2GA-PR assumption; the security proof under the latter assumption can be found in Appendix A.

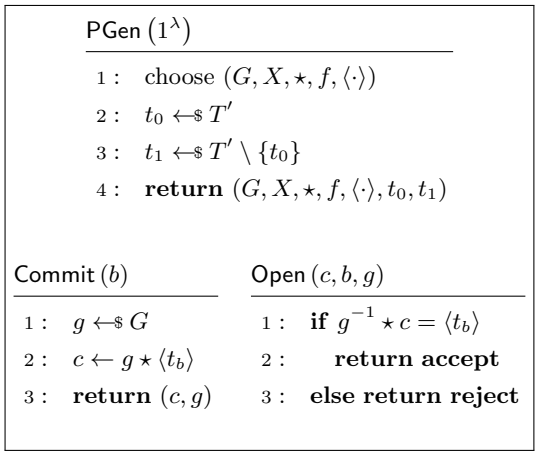

Fig. 4. Bit commitment scheme from a GACE.

Theorem 1. *The bit commitment scheme in Figure 4 is perfectly binding.*

Proof. Without loss of generality, we can assume $m_0 = 0$ and $m_1 = 1$. Suppose there exists an adversary $\mathcal{A}$ that on input $\mathsf{pp} = (G, X, \star, f, \langle\cdot\rangle, t_0, t_1)$ returns the tuple $\mathtt{com}, r_0, r_1$ such that

$$\mathsf{Open}(0, \mathtt{com}, r_0) = \mathsf{Open}(1, \mathtt{com}, r_1) = \textbf{accept}$$

with positive probability. This means that $r_0 \star \langle t_0 \rangle = \mathtt{com} = r_1 \star \langle t_1 \rangle$, and then $r_1^{-1} r_0 \star \langle t_0 \rangle = \langle t_1 \rangle$. Therefore, $\langle t_0 \rangle$ and $\langle t_1 \rangle$ are in the same orbit, but this is a contradiction and such an adversary $\mathcal{A}$ cannot exist.

Theorem 2. *The bit commitment scheme in Figure 4 is computationally hiding under the decisional Group Action Inversion Problem assumption.*

Proof. The dGA-IP assumption states that every adversary of the dGA-IP game have at most negligible advantage. We prove that the existence of an adversary

of the game Hiding(Π_{Com}) with advantage at least $\epsilon(\lambda)$, where $\epsilon(\lambda)$ is a non-negligible function, implies the existence of an adversary $\mathcal{A}$ of the dGA-IP game with advantage $2\epsilon^2(\lambda)$, which is non-negligible.
The proof is divided in 3 parts: firstly, we describe our adversary $\mathcal{A}$ of the dGA-IP game. It will exploit two instances of an adversary of the Hiding(Π_{Com}) game, therefore we must show that it correctly simulates the challenger of such a game. Finally, we quantify a lower bound to the advantage of the adversary $\mathcal{A}$.

1. *Reduction description.*
   The adversary $\mathcal{A}$ of the dGA-IP game (see Figure 5) receives from the challenger two set elements s and t, generated according to the dGA-IP game. $\mathcal{A}$ creates two instances of the adversary of Hiding(Π_{Com}) game having non-negligible advantage, namely $\mathcal{A}_1$ and $\mathcal{A}_2$. Then, the adversary $\mathcal{A}$ provides $\mathcal{A}_1$ with s and $\mathcal{A}_2$ with t separately. The two hiding commitment adversaries $\mathcal{A}_1$ and $\mathcal{A}_2$ return respectively the bits b_0 and b_1 as outputs of their internal routine. Finally, the dGA-IP adversary $\mathcal{A}$ returns to the challenger the bit b' which is set to 1 if $b_0 = b_1$, otherwise it is set to 0.
2. *$\mathcal{A}$ correctly simulates the* Hiding(Π_{Com}) *challenger.*
   We show that $\mathcal{A}$ correctly simulates the challenger of the Hiding(Π_{Com}) game, so that it is possible to quantify the probability of success of the adversaries $\mathcal{A}_1$ and $\mathcal{A}_2$. The elements s and t which $\mathcal{A}$ uses as input to $\mathcal{A}_1$ and $\mathcal{A}_2$ are generated as follows:
   - s is a random element in the orbit generated by $\langle t_c \rangle$, with c chosen uniformly at random in $\{0, 1\}$;
   - when $b = 1$, t is chosen uniformly at random in the same orbit of s (note that $g' \star s = g'g \star \langle t_c \rangle$ is random as long as $g' \leftarrow\!\$\, G$), otherwise, if $b = 0$, t is chosen at random in the orbit of $\langle t_{1-c} \rangle$.

   In particular, the orbit of s is chosen uniformly at random via the selection of c; then, given c, the orbit of t is chosen uniformly at random via b. This guarantees that $\mathcal{A}$ correctly simulates the challenger of the Hiding(Π_{Com}) game, who must choose, in the first step, whether to create a commitment to 0 or to 1. Therefore, the adversaries $\mathcal{A}_1, \mathcal{A}_2$ win their game with probability greater than $\frac{1}{2} + \epsilon(\lambda)$.
3. *Measurement of $\mathcal{A}$'s advantage.*
   Finally, we compute a lower bound to the probability of success of $\mathcal{A}$ that we have described in the dGA-IP game.
   We observe that the adversaries $\mathcal{A}_1$ and $\mathcal{A}_2$ do not interact, so the events that they win their games can be considered independent as long as their inputs are also independent.
   It is possible to show that the selection of the inputs is independent, since the selection process of s and t is performed picking at random the orbit $O(s)$ of s by sampling the bit c, and the orbit $O(t)$ of t by sampling the bit b (actually the bit that determines the orbit of t is interpreted according to the value of s, but this is not relevant as long as the bit b is chosen at random).
   Then, the canonical elements of the sampled orbits are randomized by sampling two random group elements $g, g' \in G$ and computing the action of such

elements (or of the element $g'g$ instead of g', if $b = 1$, which is a random element as long as g' is random) on the canonical elements.
Given that the inputs to $\mathcal{A}_1$ and $\mathcal{A}_2$ are independent and that the two adversaries perform their operations regardless of the existence of each other, the events that $\mathcal{A}_1$ wins its game and $\mathcal{A}_2$ wins its game are independent.
For the sake of brevity, we refer to the event that $\mathcal{A}_1$ wins or loses its game as ($\mathcal{A}_1$ `wins`) or ($\mathcal{A}_1$ `loses`) and we do the same for $\mathcal{A}_2$ and $\mathcal{A}$: the game they are playing will be clear from the context.
Finally, we compute the lower bound of the probability of advantage of $\mathcal{A}$. To do that, we observe that $\mathcal{A}$ wins the game when $b' = b$ and this happens either when both $\mathcal{A}_1$ and $\mathcal{A}_2$ win, or when they both lose.
In fact, when $b = 0$ then $O(t) \neq O(s)$; therefore, $b_0 \neq b_1$ happens if and only if both $\mathcal{A}_1$ and $\mathcal{A}_2$ win or when they both lose. The same holds when $b = 1$. Therefore,

$$
\begin{aligned}
&\Pr[\mathcal{A}\ \texttt{wins}] = \\
&\quad \Pr[(\mathcal{A}_1\ \texttt{wins} \wedge \mathcal{A}_2\ \texttt{wins}) \vee (\mathcal{A}_1\ \texttt{loses} \wedge \mathcal{A}_2\ \texttt{loses})] = \\
&\quad \Pr[(\mathcal{A}_1\ \texttt{wins} \wedge \mathcal{A}_2\ \texttt{wins})] + \Pr[(\mathcal{A}_1\ \texttt{loses} \wedge \mathcal{A}_2\ \texttt{loses})] = \\
&\quad \Pr[(\mathcal{A}_1\ \texttt{wins})] \Pr[(\mathcal{A}_2\ \texttt{wins})] + \Pr[(\mathcal{A}_1\ \texttt{loses})] \Pr[\mathcal{A}_2\ \texttt{loses})] \geq \\
&\quad \left(\frac{1}{2} + \epsilon(\lambda)\right)^2 + \left(\frac{1}{2} - \epsilon(\lambda)\right)^2 = \frac{1}{2} + 2\epsilon(\lambda)^2.
\end{aligned}
$$

Since $\epsilon(\lambda)$ is a non-negligible function, we have defined an adversary $\mathcal{A}$ of the dGA-IP game that has a non-negligible advantage. This contradicts the dGA-IP assumption, therefore the adversary of Hiding(Π_{Com}) with non-negligible advantage does not exist and the commitment scheme Π_{Com} satisfies the hiding property.

The two previous results can be summarized in the following corollary.

Corollary 1. *The bit commitment scheme in Figure 4 is secure under the decisional Group Action Inversion Problem assumption.*

We also have expanded the security analysis of the hiding property of the commitment scheme under to the 2GA-PR assumption requiring that the two orbits O_0 and O_1 used to instantiate the bit commitment have *similar size*, i.e.

$$|\Pr[x \in O_0] - \Pr[x \in O_1]| = \nu(\lambda)$$

for a randomly chosen x in $O_0 \cup O_1$ and a negligible function $\nu(\lambda)$.
We have proved the following theorem.

Theorem 3. *If the bit commitment scheme in Figure 4 is instantiated using two orbits of similar size, it is secure under the 2GA-PR assumption.*

Proof. The commitment scheme satisfies the property of perfect binding, as shown in Theorem 1. The proof of the computationally hiding property can be found in Appendix A.

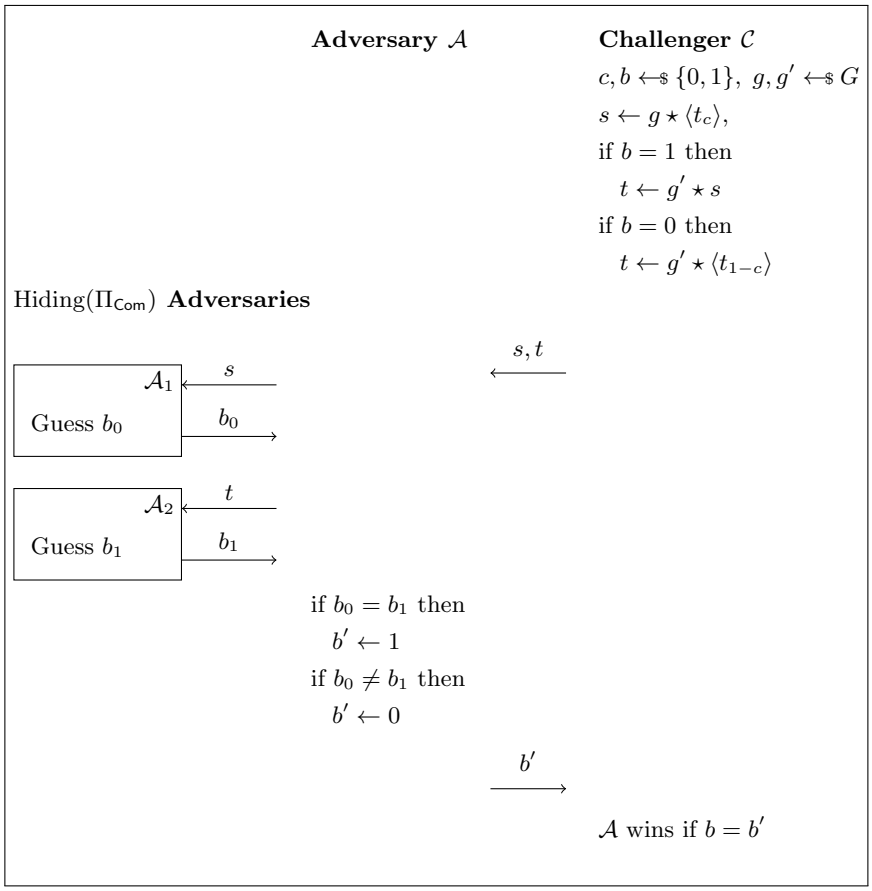

Fig. 5. Reduction from dGA-IP to the hiding game for the bit commitment scheme.

Finally, Appendix B shows that Hiding(Π_{Com}) reduces to dGA-IP, also. This allows us describe the relation between the dGA-IP and 2GA-PR assumptions.

Corollary 2. *The 2GA-PR problem reduces to dGA-IP when it is instantiated with two orbits of similar size.*

We summarize the reductions between the hiding game of the commitment scheme and the two assumptions in Figure 6.

5 Linkable Commitments

The proposed bit commitment has the following additional feature. Given two commitments $\mathtt{com}_0$ and $\mathtt{com}_1$, if we suppose that the sender is honest, there is a way to check if their committed value is the same. Based on this notion, we define the concept of *linkable commitment*. We require that the sender is honest

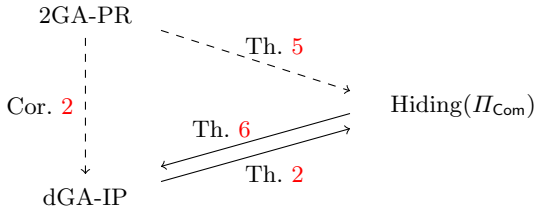

Fig. 6. Reductions between games and problems. "$A \to B$" means that solving B implies solving A. The reductions represented by a dashed line require the extra hypothesis about the similarity of the orbits.

to be assured that the commitments lie either in the orbit of $\langle t_0 \rangle$ or $\langle t_1 \rangle$. To the best of our knowledge, this property has not been formally defined before. However it is well known that, for example, Pedersen commitments enjoy this property which is used, among other things, in the Monero's RingCT protocol [PBF+19].

Definition 12. *Let $\Pi_{\mathsf{Com}} = (\mathsf{PGen}, \mathsf{Commit}, \mathsf{Open})$ be a commitment scheme. Let m_0 and m_1 be two messages and let $(\mathtt{com}_0, r_0) = \mathsf{Commit}(m_0)$ and $(\mathtt{com}_1, r_1) = \mathsf{Commit}(m_1)$. We say that Π_{Com} is* linkable *if there exist the two following* PPT *algorithms:*

1. $\mathsf{LinkMaterial}(r_0, r_1)$*, whose output is a value r_L;*
2. $\mathsf{Link}(\mathtt{com}_0, \mathtt{com}_1, r_L)$*, that returns 1 if $m_0 = m_1$ and 0 otherwise.*

In order to be secure, a linkable bit commitment must satisfy some security properties for these two additional algorithms Link and LinkMaterial as well. First, we want that the linking material r_L does not reveal any information about the committed value. This means that an adversary that has access to two commitments of m and the linking material r_L does not learn anything about m. We call this property *linkable-hiding*. Then, it must not be possible to link two commitments that are obtained starting from two distinct values. A linkable commitment with this property is said *linkable-binding*. Finally, we focus on how the value r_L can be generated. Let m be a message and let $(\mathtt{com}_0, r_0) = \mathsf{Commit}(m)$ and $(\mathtt{com}_1, r_1) = \mathsf{Commit}(m)$. We want that no one can generate a value r_L such that $\mathsf{Link}(\mathtt{com}_0, \mathtt{com}_1, r_L) = 1$ without knowledge of any information regarding the opening materials r_0 and r_1. This property is called *link secrecy*.
We formalize these new properties in the following definition.

Definition 13. *Let* HidingLink(Π_{Com}) *be the game described in Figure 7. We define the advantage of an adversary $\mathcal{A}$ of the game* HidingLink(Π_{Com}) *as*

$$\mathsf{Adv}(\mathcal{A}, \text{HidingLink}(\Pi_{\mathsf{Com}})) = \left| \Pr[\mathcal{A} \textit{ wins } \text{HidingLink}(\Pi_{\mathsf{Com}})] - \frac{1}{2} \right|.$$

Let λ be the security parameter. A linkable bit commitment $\Pi_{\mathsf{Com}} = (\mathsf{PGen}, \mathsf{Commit}, \mathsf{Open}, \mathsf{LinkMaterial}, \mathsf{Link})$ is said

– *computationally* linkable-hiding *if for all* PPT *adversaries* $\mathcal{A}$ *there is a negligible function* $\mathtt{negl}(\lambda)$ *such that*

$$\mathsf{Adv}(\mathcal{A}, \mathrm{HidingLink}(\Pi_{\mathsf{Com}})) \leq \mathtt{negl}(\lambda);$$

– *computationally* linkable-binding *if for all* PPT *adversaries* $\mathcal{A}$ *there is a negligible function* $\mathtt{negl}(\lambda)$ *such that*

$$\Pr\left[(m_0, \mathtt{com}_0, m_1, \mathtt{com}_1, r_L) \leftarrow \mathcal{A}(\mathsf{pp}) \;\middle|\; \begin{array}{c} \mathsf{pp} \leftarrow \mathsf{PGen}(1^\lambda), \\ m_0 \neq m_1, \\ \mathsf{Link}(\mathtt{com}_0, \mathtt{com}_1, r_L) = 1 \end{array}\right] \leq \mathtt{negl}(\lambda);$$

– *computationally* link secret *if for all* PPT *adversaries* $\mathcal{A}$ *there is a negligible function* $\mathtt{negl}(\lambda)$ *such that*

$$\Pr[\mathcal{A} \textit{ wins } \mathrm{LinkSecrecy}(\Pi_{\mathsf{Com}})] \leq \mathtt{negl}(\lambda),$$

where $\mathrm{LinkSecrecy}(\Pi_{\mathsf{Com}})$ *is the linking secrecy game in Figure 8.*

In the above definitions, whenever $\mathtt{negl}(\lambda) = 0$*, we say that the property is* perfect.

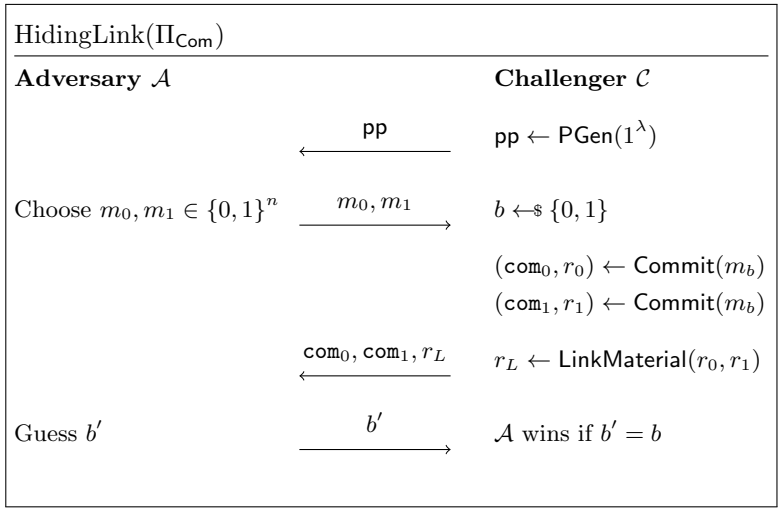

Fig. 7. Linkable-hiding game.

5.1 Linkable bit commitment from GACE

Using the bit commitment shown in Subsection 4.1, we can endow the scheme to obtain a linkable bit commitment. This extension is natural, since the commitments of a chosen message are in the orbit of that message, and showing

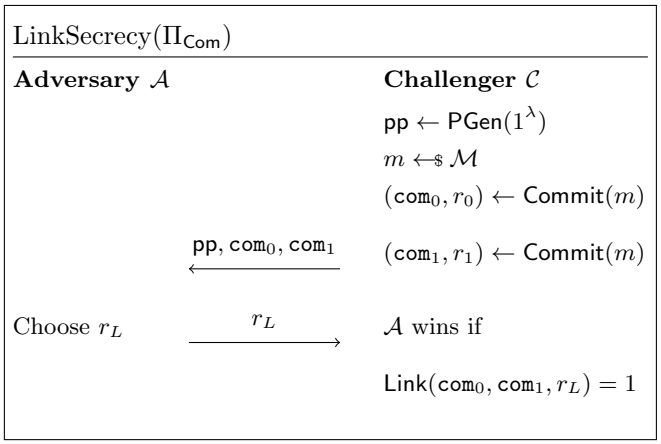

Fig. 8. Link secrecy game.

that they are linked reduces to exhibit a group element which sends one into the other.

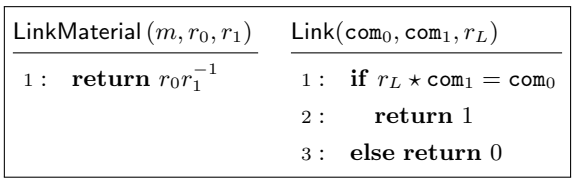

Fig. 9. Algorithm for linking commitment from a GACE.

Theorem 4. *The bit commitment scheme in Figure 4 endowed with the algorithms in Figure 9 is a secure linkable bit commitment scheme under the One-Way Group Action and dGA-IP assumptions.*

Proof. We have already proven in Theorem 1 that the bit commitment in Figure 4 is secure under the dGA-IP assumption. Now, we prove that the linkable commitment scheme is secure, namely it is computationally linkable-hiding, perfectly linkable-binding and computationally link secret.

– **Linkable-hiding**. We show that the Hiding game reduces to the HidingLink game. The idea is to let the adversary of the Hiding(Π_{Com}) game to simulate the HidingLink game challenger by creating a new random commitment (and the linking material) to the same message of the commitment it has received from its challenger. Now we explain it in greater detail.
Let $\mathcal{A}'$ be an adversary that wins the HidingLink game with non-negligible advantage $\epsilon(\lambda)$. We can define an adversary $\mathcal{A}$ for the Hiding game that

wins with a non-negligible advantage. Since we are in the binary case, the challenger $\mathcal{C}$ picks a message b and sends to $\mathcal{A}$ the commitment $\mathtt{com}$ of b. Now $\mathcal{A}$ picks a random element g in G and computes $\mathtt{com}' = g \star \mathtt{com}$, that is a valid and randomly generated commitment to b. $\mathcal{A}$ queries to $\mathcal{A}'$, the adversary of the HidingLink game, the commitments $\mathtt{com}$, $\mathtt{com}'$ and the linking material g. Note that $\mathcal{A}$ correctly simulates the adversary of the HidingLink game since the bit b and $\mathtt{com}$ are chosen at random from $\mathcal{C}$, $\mathtt{com}'$ is chosen at random from $\mathcal{A}$ and the linking material is valid.
$\mathcal{A}'$ returns a bit b' which $\mathcal{A}$ sends to $\mathcal{C}$ as its guess. If $\mathcal{A}'$ correctly guesses the bit committed to in $\mathtt{com}$ and $\mathtt{com}'$ then clearly also $\mathcal{A}$ wins its game. Therefore the advantage of $\mathcal{A}$ is the same of the one of $\mathcal{A}'$ and is non-negligible.
We can conclude that, since the commitment Π_{Com} is computationally hiding under the dGA-IP assumption, it is also computationally linkable-hiding.

- **Perfectly linkable-binding**. Suppose that an adversary returns with positive probability a tuple $(m_0, m_1, \mathtt{com}_0, \mathtt{com}_1, r_L)$ such that $m_0 \neq m_1$ and $\mathsf{Link}(\mathtt{com}_0, \mathtt{com}_1, r_L) = 1$. By construction, there exist two elements g_0 and g_1 in G such that

$$\mathtt{com}_0 = g_0 \star \langle m_0 \rangle \text{ and } \mathtt{com}_1 = g_1 \star \langle m_1 \rangle$$

  From $\mathsf{Link}(\mathtt{com}_0, \mathtt{com}_1, r_L) = 1$ we have that $r_L \star \mathtt{com}_1 = \mathtt{com}_0$, and hence $\mathtt{com}_0$ and $\mathtt{com}_1$ are in the same orbit. Since $m_0 = f(\mathtt{com}_0) = f(\mathtt{com}_1) = m_1$, where f is the invariant function in the GACE, we have a contradiction. Hence, there are no adversaries that can output such a tuple with positive probability.
- **Computationally link secret**. We show that if a PPT adversary $\mathcal{A}$, on input $\mathtt{com}_0$ and $\mathtt{com}_1$ can find r_L such that $\mathsf{Link}(\mathtt{com}_0, \mathtt{com}_1, r_L) = 1$, then it contradicts the One-way group action assumption. Essentially, if $\mathtt{com}_0$ and $\mathtt{com}_1$ are commitments to m_0, then they are in the same orbit of $\langle m_0 \rangle$. Finding an r_L in G such that $\mathsf{Link}(\mathtt{com}_0, \mathtt{com}_1, r_L) = 1$ means finding an element of G sending $\mathtt{com}_1$ to $\mathtt{com}_0$, and this is intractable by hypothesis.

Remark 1. Observe that, if an inadmissible value is committed, for instance an element x that is not in the orbit of $\langle t_0 \rangle$ nor $\langle t_1 \rangle$, then the linkability continues to work. In fact, two commitments of the above x can be linked. Therefore we refer to the above scheme as a *honest sender* linkable commitment. To cover even the case where the sender may commit to an inadmissible value, some techniques from ring signature schemes can be used. Using the framework of Beullens, Katsumata and Pintore [BKP20], a proof of the legitimacy of the commitment can be generated in the random oracle model. In the commit phase, the sender generates $(\mathtt{com}, r)$ from $\mathsf{Commit}(b)$, then attaches to $\mathtt{com}$ a non-interactive proof of the OR-relation

$$\{(\mathtt{com}, g) \mid \mathtt{com} = g \star \langle t_0 \rangle \text{ or } \mathtt{com} = g \star \langle t_1 \rangle\}.$$

We refer to [BKP20] for the details. However, this proof needs many repetitions to achieve a reasonable security level, leading to a huge cost in communication.

6 An Instantiation with Tensors

6.1 3-tensors and group actions

Let n be a positive integer and let $\mathbf{V}$ be the tensor space given by $\mathbb{F}_q^n \otimes \mathbb{F}_q^n \otimes \mathbb{F}_q^n$. Let $\{e_1, \ldots, e_n\}$ be a base of $\mathbb{F}_q^n$, hence an element T of $\mathbf{V}$ can be written as

$$T = \sum_{i,j,k} T(i,j,k) e_i \otimes e_j \otimes e_k, \tag{1}$$

where $T(i,j,k)$ are elements in $\mathbb{F}_q$. A *rank one* (or *decomposable*) tensor is an element of the form $a \otimes b \otimes c$, where a, b, c are in $\mathbb{F}_q^n$. Given a tensor T, its *rank* is the minimal non-negative integer r such that there exist $t_1, \ldots, t_r$ rank one tensors for which $T = \sum_{i=1}^{r} t_i$, and we write $\mathrm{rk}(T) = r$. In general, computing the rank of a tensor is an hard task [Hås89; SŠ18; Shi16].

A group action can be defined on the vector space $\mathbf{V}$ of tensors from the group $G = \mathrm{GL}(n) \times \mathrm{GL}(n) \times \mathrm{GL}(n)$ as follows:

$$\star : G \times \mathbf{V} \to \mathbf{V},$$
$$\left((A,B,C), \sum_{i,j,k} T(i,j,k) e_i \otimes e_j \otimes e_k \right) \mapsto \sum_{i,j,k} T(i,j,k) Ae_i \otimes Be_j \otimes Ce_k.$$

It can be shown that this action does not change the rank of a tensor. However, if it is extended to non-invertible matrices, this property does not hold: for example the zero matrix sends every tensor into the zero tensor.

6.2 GACE and bit commitment from tensors

Given the group action defined above, we want to build a Group Action with Canonical Element. Since the computation of the rank is supposed to be hard, we set $T = \mathbb{N}$ and

$$f : \mathbf{V} \to \mathbb{N},\ T \mapsto \mathrm{rk}(T).$$

In order to define the function $\langle \cdot \rangle$, we need to do some observations. From Eq. (1), we see that the rank of a tensor is at most n^3 and with a simple trick it can be shown that it is at most n^2. Actually, the maximal rank is strictly less that this value. As showed in [How78], the maximal rank attainable by a tensor in $\mathbf{V}$ is between $\frac{1}{3}n^2$ and $\frac{3}{4}n^2$. Moreover, an open problem in this field is to exhibit the explicit construction of a high-rank tensor. Even if there are some results [Blä14; Wei11; AFT11], we are not able to construct a tensor of any given rank. Luckily, there is a set of integers for which we can easily exhibit tensors of a given rank. Let $T' = \{1, \ldots, n\}$ and we can define the function

$$\langle \cdot \rangle : T' \to \mathbf{V},$$
$$r \mapsto \sum_{i=1}^{r} e_i \otimes e_i \otimes e_i.$$

We can see that $f(\langle r \rangle) = r$ for any r in $T' = \{1, \ldots, n\}$, hence the tuple $(G, \mathbf{V}, \star, f, \langle \cdot \rangle)$ is a GACE. In fact, computing the rank of a random tensor of promised rank between 1 and n is hard, while recognize the rank of $\langle r \rangle$ is easy.

The non-interactive bit commitment scheme we present is based on the general one in Figure 4. During the parameter generation phase, we choose $n-1$ and n as elements of T' encoding the bits 0 and 1, respectively.

Concretely, given a security parameter λ, a prime power q, an integer n and the tensor space $\mathbf{V} = \mathbb{F}_q^n \otimes \mathbb{F}_q^n \otimes \mathbb{F}_q^n$, the public parameters are

$$(G, \mathbf{V}, \star, f, \langle \cdot \rangle, n-1, n).$$

Let us analyze the assumptions on this particular group action. The dGA-IP assumption for tensors is related to the Tensor Isomorphism problem [GQ19; GQ21], which is complete for a large class of problems and it is conjectured hard even for a quantum computer. The One-Way assumption on tensors is linked to the computational version of the dGA-IP problem: given two tensors in the same orbit, find the group element that links them. This problem is believed to be hard and it is directly used in various cryptosystem [CNP+22; JQSY19], while other construction use polynomially equivalent problems [TDJ+22]. When we consider just the orbits of rank n and $n-1$, these assumptions seem to remain intractable.

Summarizing, to commit to a bit b, the sender picks a random g in G and obtains the commitment `com` equal to $g \star \langle n-1 \rangle$ if $b = 0$ or $g \star \langle n \rangle$ if $b = 1$. The opening material is given by g. To open the commitment `com`, the sender communicates to the receiver b and g and the latter checks that $g^{-1} \star$ `com` is equal to $\langle n-1 \rangle$ or $\langle n \rangle$. There is one additional check to take care during the opening phase: the receiver must verify the membership of g to G. In fact, if $g = (A, B, C)$ and A, B or C are non-invertible, then g can send a tensor of rank n to a tensor of rank $n-1$, breaking the binding property.
Analogously, a linkable bit commitment can be designed on tensors with the constructions given in Subsection 5.1.

7 Conclusions

In this work, we have presented a framework based on group actions that makes use of invariant functions and canonical elements, namely a Group Action with Canonical Element (GACE). The considered invariant function must be hard to compute on a large class of elements, but at the same time its computation on the canonical elements must be feasible. Then, we showed how to design a bit commitment based on this framework that is proven secure in the standard model. More in detail, breaking the hiding assumption of our commitment scheme means breaking independently both 2GA-PR and dGA-IP. This leads to the first non-interactive bit commitment relying on group actions.
One of the most interesting aspects of our construction is that it requires the

action to be non-transitive. This is somehow novel in the cryptographic group action literature, where previous schemes rely on transitive action or they restrict to a single orbit. Concretely, in our framework we need to exhibit two elements that belong to two different orbits.
Moreover, we introduce the notion of linkable commitment and we prove that our bit commitment can be easily extended to a linkable one. Finally, we show an instantiation of our framework and commitment using tensors on finite fields. In this case, the invariant function is the tensor rank, and the cryptographic assumption is linked to the computational version of the dGA-IP problem.
As a future work, a commitment based on more orbits or new cryptographic schemes starting from a GACE could be investigated. At the same time, it would be interesting to find other GACEs to concretely instantiate the framework.

Acknowledgment

The authors are members of GNSAGA of INdAM. The first and the third authors are members of CrypTO, the group of Cryptography and Number Theory of Politecnico di Torino. The first author acknowledges support from TIM S.p.A. through the PhD scholarship. The second author acknowledges support from Eustema S.p.A. through the PhD scholarship.

References

[ADMP20] N. Alamati, L. De Feo, H. Montgomery, and S. Patranabis, "Cryptographic group actions and applications," in *International Conference on the Theory and Application of Cryptology and Information Security*, Springer, 2020, pp. 411–439 (cit. on pp. 2, 4–6).

[AFT11] B. Alexeev, M. A. Forbes, and J. Tsimerman, "Tensor rank: Some lower and upper bounds," in *2011 IEEE 26th Annual Conference on Computational Complexity*, IEEE, 2011, pp. 283–291 (cit. on p. 21).

[BBPS23] A. Barenghi, J.-F. Biasse, E. Persichetti, and P. Santini, "On the computational hardness of the code equivalence problem in cryptography," *Advances in Mathematics of Communications*, vol. 17, no. 1, pp. 23–55, 2023 (cit. on p. 2).

[BDK+23] W. Beullens, S. Dobson, S. Katsumata, Y.-F. Lai, and F. Pintore, "Group signatures and more from isogenies and lattices: generic, simple, and efficient," *Designs, Codes and Cryptography*, pp. 1–60, 2023 (cit. on p. 2).

[BKP20] W. Beullens, S. Katsumata, and F. Pintore, "Calamari and Falafl: logarithmic (linkable) ring signatures from isogenies and lattices," in *Advances in Cryptology–ASIACRYPT 2020: 26th International Conference on the Theory and Application of Cryptology and Information Security, Daejeon, South Korea, December 7–11, 2020, Proceedings, Part II*, Springer, 2020, pp. 464–492 (cit. on pp. 2, 3, 20).

[Blä14] M. Bläser, "Explicit tensors," *Perspectives in Computational Complexity: The Somenath Biswas Anniversary Volume*, pp. 117–130, 2014 (cit. on p. 21).

[BM19] M. Blum and S. Micali, "How to generate cryptographically strong sequences of pseudo random bits," in *Providing Sound Foundations for Cryptography: On the Work of Shafi Goldwasser and Silvio Micali*, 2019, pp. 227–240 (cit. on p. 10).

[BY91] G. Brassard and M. Yung, "One-way group actions," in *Advances in Cryptology-CRYPTO'90: Proceedings 10*, Springer, 1991, pp. 94–107 (cit. on pp. 2, 9–11).

[CLM+18] W. Castryck, T. Lange, C. Martindale, L. Panny, and J. Renes, "CSIDH: an efficient post-quantum commutative group action," in *Advances in Cryptology–ASIACRYPT 2018: 24th International Conference on the Theory and Application of Cryptology and Information Security, Brisbane, QLD, Australia, December 2–6, 2018, Proceedings, Part III 24*, Springer, 2018, pp. 395–427 (cit. on p. 2).

[CNP+22] T. Chou, R. Niederhagen, E. Persichetti, T. H. Randrianarisoa, K. Reijnders, S. Samardjiska, and M. Trimoska, "Take your MEDS: Digital Signatures from Matrix Code Equivalence," *Cryptology ePrint Archive*, 2022 (cit. on p. 22).

[Cou06] J.-M. Couveignes, "Hard homogeneous spaces," *Cryptology ePrint Archive*, 2006 (cit. on pp. 2, 4).

[DE17] A. Darwish and M. M. El-Gendy, "A new cryptographic voting verifiable scheme for e-voting system based on bit commitment and blind signature," *Int J Swarm Intel Evol Comput*, vol. 6, no. 158, p. 2, 2017 (cit. on p. 2).

[FPY18] T. K. Frederiksen, B. Pinkas, and A. Yanai, "Committed mpc: Maliciously secure multiparty computation from homomorphic commitments," in *Public-Key Cryptography–PKC 2018: 21st IACR International Conference on Practice and Theory of Public-Key Cryptography, Rio de Janeiro, Brazil, March 25-29, 2018, Proceedings, Part I 21*, Springer, 2018, pp. 587–619 (cit. on p. 2).

[GMW91] O. Goldreich, S. Micali, and A. Wigderson, "Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proof systems," *Journal of the ACM (JACM)*, vol. 38, no. 3, pp. 690–728, 1991 (cit. on pp. 2, 11).

[GQ19] J. A. Grochow and Y. Qiao, "Isomorphism problems for tensors, groups, and cubic forms: Completeness and reductions," *arXiv preprint arXiv:1907.00309*, 2019 (cit. on pp. 7, 22).

[GQ21] J. A. Grochow and Y. Qiao, "On the complexity of isomorphism problems for tensors, groups, and polynomials I: Tensor Isomorphism-completeness," in *12th Innovations in Theoretical Computer Science Conference (ITCS 2021)*, Schloss Dagstuhl-Leibniz-Zentrum für Informatik, 2021 (cit. on pp. 7, 22).

[GS10] D. Grigoriev and V. Shpilrain, "Authentication schemes from actions on graphs, groups, or rings," *Annals of Pure and Applied Logic*, vol. 162, no. 3, pp. 194–200, 2010 (cit. on p. 2).

[Hås89] J. Håstad, "Tensor rank is NP-complete," in *International Colloquium on Automata, Languages, and Programming*, Springer, 1989, pp. 451–460 (cit. on p. 21).

[How78] T. D. Howell, "Global properties of tensor rank," *Linear Algebra and its Applications*, vol. 22, pp. 9–23, 1978 (cit. on p. 21).

[JLO06] A. Juels, M. Luby, and R. Ostrovsky, "Security of blind digital signatures," in *Advances in Cryptology—CRYPTO'97: 17th Annual International Cryptology Conference Santa Barbara, California, USA August 17–21, 1997 Proceedings*, Springer, 2006, pp. 150–164 (cit. on p. 2).

[JQSY19] Z. Ji, Y. Qiao, F. Song, and A. Yun, "General linear group action on tensors: A candidate for post-quantum cryptography," in *Theory of Cryptography Conference*, Springer, 2019, pp. 251–281 (cit. on pp. 2, 3, 6, 7, 10, 11, 22).

[LNS21] V. Lyubashevsky, N. K. Nguyen, and G. Seiler, "Shorter lattice-based zero-knowledge proofs via one-time commitments," in *Public-Key Cryptography–PKC 2021: 24th IACR International Conference on Practice and Theory of Public Key Cryptography, Virtual Event, May 10–13, 2021, Proceedings, Part I*, Springer, 2021, pp. 215–241 (cit. on p. 2).

[LR22] A. Leroux and M. Roméas, "Updatable encryption from group actions," *Cryptology ePrint Archive*, 2022 (cit. on p. 2).

[Nao91] M. Naor, "Bit commitment using pseudorandomness," *Journal of cryptology*, vol. 4, pp. 151–158, 1991 (cit. on pp. 2, 10).

[OPV09] R. Ostrovsky, G. Persiano, and I. Visconti, "Simulation-based concurrent non-malleable commitments and decommitments," in *Theory of Cryptography: 6th Theory of Cryptography Conference, TCC 2009, San Francisco, CA, USA, March 15-17, 2009. Proceedings 6*, Springer, 2009, pp. 91–108 (cit. on p. 2).

[Pat96] J. Patarin, "Hidden fields equations (HFE) and isomorphisms of polynomials (IP): Two new families of asymmetric algorithms," in *International Conference on the Theory and Applications of Cryptographic Techniques*, Springer, 1996, pp. 33–48 (cit. on p. 2).

[PBF+19] A. Poelstra, A. Back, M. Friedenbach, G. Maxwell, and P. Wuille, "Confidential assets," in *Financial Cryptography and Data Security: FC 2018 International Workshops, BITCOIN, VOTING, and WTSC, Nieuwpoort, Curaçao, March 2, 2018, Revised Selected Papers 22*, Springer, 2019, pp. 43–63 (cit. on pp. 2, 3, 17).

[Ped01] T. P. Pedersen, "Non-interactive and information-theoretic secure verifiable secret sharing," in *Advances in Cryptology—CRYPTO'91: Proceedings*, Springer, 2001, pp. 129–140 (cit. on p. 3).

[PR97] E. Petrank and R. M. Roth, "Is code equivalence easy to decide?" *IEEE Transactions on Information Theory*, vol. 43, no. 5, pp. 1602–1604, 1997 (cit. on p. 7).

[RST22] K. Reijnders, S. Samardjiska, and M. Trimoska, "Hardness estimates of the Code Equivalence Problem in the Rank Metric," *Cryptology ePrint Archive*, 2022 (cit. on p. 2).

[Shi16] Y. Shitov, "How hard is the tensor rank?" *arXiv preprint arXiv:1611.01559*, 2016 (cit. on p. 21).

[Sho94] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in *Proceedings 35th annual symposium on foundations of computer science*, IEEE, 1994, pp. 124–134 (cit. on p. 2).

[SŠ18] M. Schaefer and D. Štefankovič, "The complexity of tensor rank," *Theory of Computing Systems*, vol. 62, pp. 1161–1174, 2018 (cit. on p. 21).

[Sto12] A. Stolbunov, "Cryptographic schemes based on isogenies," 2012 (cit. on p. 7).

[TDJ+22] G. Tang, D. H. Duong, A. Joux, T. Plantard, Y. Qiao, and W. Susilo, "Practical Post-Quantum Signature Schemes from Isomorphism Problems of Trilinear Forms," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Springer, 2022, pp. 582–612 (cit. on pp. 2, 22).

[Wei11] B. Weitz, "An improvement on ranks of explicit tensors," *arXiv preprint arXiv:1102.0580*, 2011 (cit. on p. 21).

A 2GA-PR reduces to Hiding(Π_{Com})

The reduction used to prove the hiding property under the 2GA-PR assumption is exactly the same given in the proof of Theorem 2, and the main difference between the proof of the hiding property under the dGA-IP assumption and the following is that the outcome of the adversaries of the Hiding(Π_{Com}) game $\mathcal{A}_1$ and $\mathcal{A}_2$ are not independent anymore, but are only conditionally independent once the input values (s and t) are fixed.
In fact, in the 2GA-PR game $\Pr[O(s) = O(t)] = \frac{3}{4}$ which means that the selection of the value of t, input to $\mathcal{A}_2$ depends on the selection of s, given in input to $\mathcal{A}_1$.

Theorem 5. *The bit commitment scheme in Figure 4 instantiated with two orbits of similar size is computationally hiding under the 2GA-PR assumption.*

For simplicity, in the following proof we assume that the cardinality of the two orbits is the same, that is, the probability of picking an element at random inside any orbit is $\frac{1}{2}$. The proof can be easily generalized to the case where the probability of falling into one orbit is negligibly greater than the probability of falling into the other. In other words, the proof holds whenever there exists a negligible function $\nu(\lambda)$ such that, given the two orbits O_0 and O_1,

$$|\Pr[x \in O_0] - \Pr[x \in O_1]| = \nu(\lambda)$$

for a randomly chosen x in $O_0 \cup O_1$. This assumption seems admissible and not too strict for cryptographic purposes.

Proof. We must prove that the hiding property holds for Π_{Com}. We show that, given an adversary of the Hiding(Π_{Com}) game with non-negligible advantage, we can build an adversary of the 2GA-PR game with non-negligible advantage (recall that the advantage of $\mathcal{A}$ is defined as $\mathbf{Adv}(\mathcal{A}, \text{2GA-PR}(\mathtt{pp})) = \Pr[\mathcal{A} \text{ wins 2GA-PR}(\mathtt{pp})] - \frac{1}{2}$).

1. *Reduction description.*
   To define $\mathcal{A}$, we use two independent instances of the same adversary $\mathcal{A}_1, \mathcal{A}_2$ of the hiding game as we did in the proof of Theorem 2; then, we perform the same reduction, as it is presented in Figure 10.
2. *$\mathcal{A}$ correctly simulates the* Hiding(Π_{Com}) *challenger.*
   The adversary $\mathcal{A}$ correctly simulates the challenger of Hiding(Π_{Com}) with respect to the adversaries $\mathcal{A}_1$ and $\mathcal{A}_2$ separately, in fact both s and t are uniformly sampled from the set of commitment to 0 and 1. Therefore, $\mathcal{A}_1$ and $\mathcal{A}_2$ will output the right bit with advantage $\epsilon(\lambda)$.
3. *Measurement of $\mathcal{A}$'s advantage.*
   From now on, when we consider the orbits $O(s)$ and $O(t)$ of s and t respectively, they will assume binary values according to the relation used in the bit commitment scheme Π_{Com}: $O(s) = 1$ if s lives in the orbit of commitments to 1, and $O(s) = 0$ if s lives in the orbit of commitments to 0. The same holds for $O(t)$.
   Before computing the lower bound of the advantage of the adversary $\mathcal{A}$, we state the following remark.

   Remark 2. The outcomes of the games performed by $\mathcal{A}_1$ and $\mathcal{A}_2$ in the reduction of Figure 10 are not independent since the values given as inputs to them are dependent values (note that t is in the same orbit of s with probability $\frac{3}{4}$). However, it is still true that the outcomes of the adversaries $\mathcal{A}_1$ and $\mathcal{A}_2$ are independent if conditioned to fixed input values.

   For the sake of generality, we need to consider the case in which the advantage of the adversaries $\mathcal{A}_1$ and $\mathcal{A}_2$ in playing Hiding(Π_{Com}) game is not uniformly distributed on the possible outputs. That is, it is possible that

$$\Pr[\mathcal{A}_1 \ \mathtt{wins} \mid O(s) = 1] = \frac{1}{2} + \epsilon(\lambda) + \Delta,$$

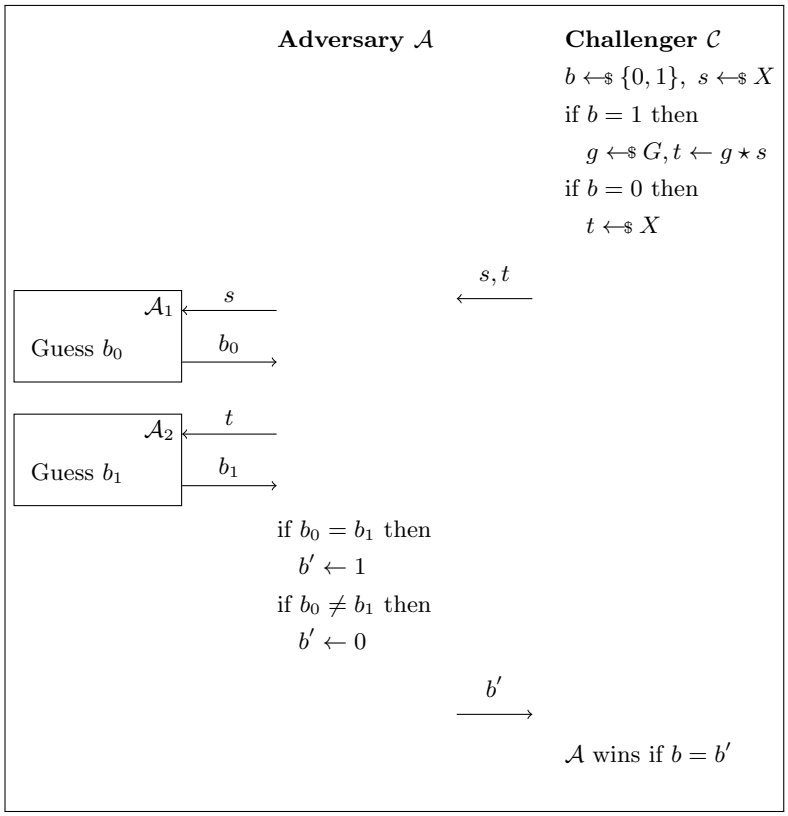

Fig. 10. Reduction from 2GA-PR to the hiding game for the bit commitment scheme.

$$\Pr[\mathcal{A}_1 \ \texttt{wins} \mid O(s) = 0] = \frac{1}{2} + \epsilon(\lambda) - \Delta,$$

with Δ possibly a negative value. The same holds for $\Pr[\mathcal{A}_2 \ \texttt{wins} \mid O(t) = b]$, with $b \in \{0, 1\}$.

Now, we can start with the computation of the lower bound of the advantage of $\mathcal{A}$ in winning the 2GA-PR game.

The probability that $\mathcal{A}$ wins the 2GA-PR game can be computed as follows, partitioning the event in three disjoint events:

$$\begin{aligned}\Pr[\mathcal{A}\ \texttt{wins}] = \Pr[b' = b] = \\ \Pr\Big[\underbrace{(b = 0 \wedge O(s) \neq O(t)) \wedge b' = b}_{\text{Event A}}\Big] + \\ \Pr\Big[\underbrace{(b = 0 \wedge O(s) = O(t)) \wedge b' = b}_{\text{Event B}}\Big] + \\ \Pr\Big[\underbrace{b = 1 \wedge b' = b}_{\text{Event C}}\Big].\end{aligned}$$

We now separately quantify the three probabilities as follows. We recall that according to the event we are considering, the event $b = b'$ can be translated in terms of success of the adversaries $\mathcal{A}_1$ and $\mathcal{A}_2$

- **Event A**: when $b = 0$ and $O(s) \neq O(t)$, then $b = b'$ when both $\mathcal{A}_1$ and $\mathcal{A}_2$ win or when both of them lose. Therefore, it holds that

$$\begin{aligned}\Pr[b = 0 \wedge O(s) \neq O(t) \wedge b' = b] = \\ \Pr[b = 0 \wedge O(s) \neq O(t) \wedge \mathcal{A}_1\ \texttt{wins} \wedge \mathcal{A}_2\ \texttt{wins}] + \\ \Pr[b = 0 \wedge O(s) \neq O(t) \wedge \mathcal{A}_1\ \texttt{loses} \wedge \mathcal{A}_2\ \texttt{loses}].\end{aligned} \tag{2}$$

  We can compute this probability by considering the general case $\Pr[b = 0 \wedge O(s) \neq O(t) \wedge \mathcal{A}_1\ \texttt{outcome} \wedge \mathcal{A}_2\ \texttt{outcome}]$ and then substituting `outcome` with `wins` or `loses` accordingly with the formula above. It holds that

$$\begin{aligned}&\Pr[b = 0 \wedge O(s) \neq O(t) \wedge \mathcal{A}_1\ \texttt{outcome} \wedge \mathcal{A}_2\ \texttt{outcome}] = \\ &\sum_{c=0}^{1} \Pr[b = 0 \wedge O(s) = c \wedge O(t) = 1 - c \wedge \mathcal{A}_1\ \texttt{outcome} \wedge \mathcal{A}_2\ \texttt{outcome}] = \\ &\sum_{c=0}^{1} \Big(\Pr[\mathcal{A}_1\ \texttt{outcome} \wedge \mathcal{A}_2\ \texttt{outcome} \mid b = 0 \wedge O(s) = c \wedge O(t) = 1 - c] \cdot \\ &\qquad \cdot \Pr[b = 0 \wedge O(s) = c \wedge O(t) = 1 - c]\Big).\end{aligned}$$

  Since the outcomes of $\mathcal{A}_1$ and $\mathcal{A}_2$ are independent once their input values are fixed, we have that

$$\begin{aligned}&\Pr[\mathcal{A}_1\ \texttt{outcome} \wedge \mathcal{A}_2\ \texttt{outcome} \mid b = 0 \wedge O(s) = c \wedge O(t) = 1 - c] = \\ &\prod_{i=1}^{2} \Pr[\mathcal{A}_i\ \texttt{outcome} \mid b = 0 \wedge O(s) = c \wedge O(t) = 1 - c],\end{aligned}$$

with $c \in \{0,1\}$.
Since the outcome of $\mathcal{A}_1$ only depends on the value of $O(s)$ and the outcome of $\mathcal{A}_2$ depends only on $O(t)$, then

$$\Pr[\mathcal{A}_1 \ \texttt{outcome} \wedge \mathcal{A}_2 \ \texttt{outcome} \mid b = 0 \wedge O(s) = c \wedge O(t) = 1 - c] = \Pr[\mathcal{A}_1 \ \texttt{outcome} \mid O(s) = c] \Pr[\mathcal{A}_2 \ \texttt{outcome} \mid O(t) = 1 - c]$$

Therefore, since $\Pr\left[b = 0 \wedge O(s) = \bar{b} \wedge O(t) = 1 - \bar{b}\right] = \frac{1}{8}$ with $\bar{b} \in \{0,1\}$ then

$$\Pr[b = 0 \wedge O(s) \neq O(t) \wedge \mathcal{A}_1 \ \texttt{outcome} \wedge \mathcal{A}_2 \ \texttt{outcome}] = \frac{1}{8}\Big(\Pr[\mathcal{A}_1 \ \texttt{outcome} \mid O(s) = 1] \cdot \Pr[\mathcal{A}_2 \ \texttt{outcome} \mid O(t) = 0] + \Pr[\mathcal{A}_1 \ \texttt{outcome} \mid O(s) = 0] \cdot \Pr[\mathcal{A}_2 \ \texttt{outcome} \mid O(t) = 1]\Big).$$

We can finally compute the initial probability given in Eq. (2), by substituting `outcome` with `wins` and `loses` and obtaining

$$\Pr[b = 0 \wedge O(s) \neq O(t) \wedge b' = b] = \frac{1}{8} + \frac{1}{2}\epsilon^2(\lambda) - \frac{1}{2}\Delta^2. \tag{3}$$

– **Event B**: when $b = 0$ and $O(s) = O(t)$, then $b = b'$ when either $\mathcal{A}_1$ wins and $\mathcal{A}_2$ loses or when $\mathcal{A}_1$ loses and $\mathcal{A}_2$ wins. Therefore, it holds that

$$\begin{aligned}\Pr[b = 0 \wedge O(s) = O(t) \wedge b' = b] = \\ \Pr[b = 0 \wedge O(s) = O(t) \wedge \mathcal{A}_1 \ \texttt{wins} \wedge \mathcal{A}_2 \ \texttt{loses}] + \\ \Pr[b = 0 \wedge O(s) = O(t) \wedge \mathcal{A}_1 \ \texttt{loses} \wedge \mathcal{A}_2 \ \texttt{wins}].\end{aligned} \tag{4}$$

Since in this case the input of $\mathcal{A}_1$ and $\mathcal{A}_2$ are in the same orbit, then we can state

$$\begin{aligned}&\Pr[b = 0 \wedge O(s) = O(t) \wedge b' = b] = \\ &2\Pr[b = 0 \wedge O(s) = O(t) \wedge \mathcal{A}_1 \ \texttt{wins} \wedge \mathcal{A}_2 \ \texttt{loses}] = \\ &2\sum_{c=0}^{1} \Pr[b = 0 \wedge O(s) = c \wedge O(t) = c \wedge \mathcal{A}_1 \ \texttt{wins} \wedge \mathcal{A}_2 \ \texttt{loses}].\end{aligned}$$

Using arguments similar to the ones used for **Event A**, that is the conditional independence of the outcomes of the adversaries once the inputs are fixed, the fact that the output of $\mathcal{A}_1$ (resp. $\mathcal{A}_2$) depends only on $O(s)$ (resp. on $O(t)$) and finally that $\Pr[b = 0 \wedge O(s) = c \wedge O(t) = c] = \frac{1}{8}$, for $c \in \{0,1\}$, we can write the Eq. (4) as follows

$$\Pr[b = 0 \wedge O(s) = O(t) \wedge b' = b] = \frac{1}{8} - \frac{1}{2}\epsilon^2(\lambda) - \frac{1}{2}\Delta^2. \tag{5}$$

– **Event C**: when $b = 1$, $O(s) = O(t)$, then $b = b'$ when both $\mathcal{A}_1$ and $\mathcal{A}_2$ win or when both of them lose. Therefore, it holds that

$$\begin{aligned}\Pr[b = 1 \wedge b' = b] = \\ \Pr[b = 1 \wedge \mathcal{A}_1 \ \texttt{wins} \wedge \mathcal{A}_2 \ \texttt{wins}] + \\ \Pr[b = 1 \wedge \mathcal{A}_1 \ \texttt{loses} \wedge \mathcal{A}_2 \ \texttt{loses}].\end{aligned} \tag{6}$$

As in the computation of the probability of **Event A**, we must compute $\Pr[b = 1 \wedge \mathcal{A}_1 \ \texttt{outcome} \wedge \mathcal{A}_2 \ \texttt{outcome}]$. Using similar arguments as before, and noticing that $\Pr[b = 1 \wedge O(s) = c \wedge O(t) = c] = \frac{1}{4}$ with $c \in \{0, 1\}$, it can be shown that

$$\begin{aligned}\Pr[b = 1 \wedge \mathcal{A}_1 \ \texttt{outcome} \wedge \mathcal{A}_2 \ \texttt{outcome}] = \\ \frac{1}{4} \sum_{c=0}^{1} \Pr[\mathcal{A}_1 \ \texttt{outcome} \mid O(s) = c] \Pr[\mathcal{A}_2 \ \texttt{outcome} \mid O(t) = c]\end{aligned}$$

Therefore, substituting `outcome` with `loses` and `wins`, and using the probabilities of success of adversaries $\mathcal{A}_1$ and $\mathcal{A}_2$, from Eq. (6) we obtain

$$\Pr[b = 1 \wedge b' = b] = \frac{1}{4} + \epsilon^2(\lambda) + \Delta^2. \tag{7}$$

Combining the partial results derived analysing **Event A**, **Event B** and **Event C** from Equations (3),(5) and (7) respectively, we obtain the final result

$$\Pr[\mathcal{A} \ \texttt{wins}] = \frac{1}{2} + \epsilon^2(\lambda),$$

which proves that we have built an adversary for the 2GA-PR game which wins with non-negligible advantage. Therefore, an adversary who wins the hiding game with non-negligible advantage does not exist due to the 2GA-PR assumption. This means that the binary commitment scheme we have described results to be perfectly binding and computationally hiding.

B Hiding(Π_{Com}) reduces to dGA-IP

Theorem 6. *The* Hiding(Π_{Com}) *game reduces to dGA-IP game.*

Proof. We show how the existence of an adversary of dGA-IP problem with non-negligible advantage allows the creation of an adversary of the Hiding(Π_{Com}) game with non-negligible advantage.

1. *Reduction description.*
The adversary $\mathcal{A}$ of the Hiding(Π_{Com}) game (see Figure 11) receives from the challenger a commitment c to a randomly generated bit b. $\mathcal{A}$ generates a commitment c' to a random bit b' and sends c, c' to $\mathcal{A}'$, the adversary to the dGA-IP game with non-negligible advantage. $\mathcal{A}$ receives a response b_0 from $\mathcal{A}'$ and returns to the Hiding(Π_{Com}) challenger the bit b' if $b_0 = 1$ (i.e. $\mathcal{A}'$ has guessed that c and c' are in the same orbit), otherwise $\mathcal{A}$ returns $1 - b'$.

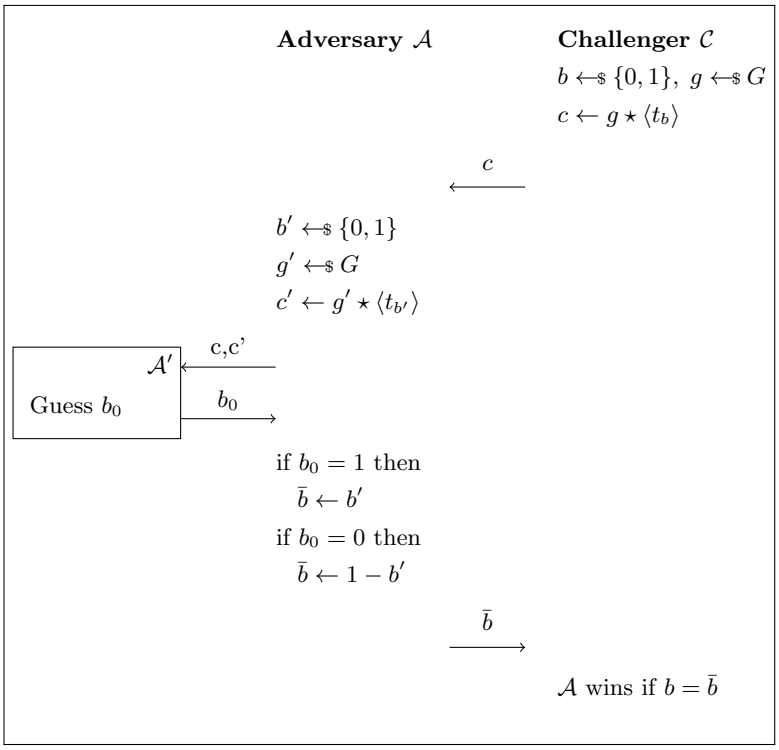

Fig. 11. Reduction from the hiding game for the bit commitment scheme to dGA-IP.

2. *$\mathcal{A}$ correctly simulates the dGA-IP challenger.*
   The adversary $\mathcal{A}$ receives a commitment to a random unknown bit b. Therefore, in order to simulate the dGA-IP challenger, it generates a random bit b' and a commitment to such bit. In this way, $\mathcal{A}$ generates couples of elements in X that live in the same orbit with probability $\frac{1}{2}$ as it does the dGA-IP challenger.
3. *Measurement of $\mathcal{A}$'s advantage.*
   The adversary $\mathcal{A}$ wins exactly with the same probability of $\mathcal{A}'$, since every time $\mathcal{A}'$ guesses the right answer to the dGA-IP game, $\mathcal{A}$ learns the orbit in which the element c lies since it knows the orbit of c'. Therefore, if $\mathcal{A}'$ wins the dGA-IP game with non-negligible advantage, also $\mathcal{A}$ wins the Hiding(Π_{Com}) game with non negligible advantage.