Homomorphic Trapdoor Commitments to Group Elements

Jens Groth

University College London
j.groth@ucl.ac.uk

Abstract

We present homomorphic trapdoor commitments to group elements. In contrast, previous homomorphic trapdoor commitment schemes only allow the messages to be exponents. Our commitment schemes are length-reducing, we can make a short commitment to many group elements at once, and they are perfectly hiding and computationally binding.

The commitment schemes are based on groups with a bilinear map. We can commit to elements from a base group, whereas the commitments belong to the target group. We present two constructions based on simple computational intractability assumptions, which we call respectively the double pairing assumption and the simultaneous triple pairing assumption. While the assumptions are new, we demonstrate that they are implied by well-known assumptions; respectively the decision Diffie-Hellman assumption and the decision linear assumption.

Our constructions also have applications in the context of committing to exponents. Variants of the Pedersen commitment scheme make it possible to commit to many exponents at once; however, this comes at the cost of a public key that grows linearly in the number of committed exponents. We propose homomorphic trapdoor commitment schemes for multiple exponents with constant size commitments and sub-linear size public keys.

Keywords: Homomorphic trapdoor commitment, bilinear groups, double pairing assumption, simultaneous triple pairing assumption.

1 Introduction

A non-interactive commitment scheme makes it possible to create a *commitment* c to a secret message m. The commitment *hides* the message, but we may later disclose m and demonstrate that c was a commitment to m by revealing the randomness r used when creating it. Revealing the message and the randomness is called *opening* the commitment. It is essential that once a commitment is made, it is *binding*. Binding means that it is infeasible to find two openings of the same commitment to two different messages.

In this paper, we are interested in public-key commitments with some useful features. First, we want the commitment scheme to have a *trapdoor* property. In normal operation the commitment scheme is binding, however, if we know a secret trapdoor tk associated with the public commitment key ck, then it is possible to create commitments that can be opened to any message. We note that the trapdoor property implies that the commitment hides the message. Second, we want the commitment scheme to be *homomorphic*. Homomorphic means that messages and commitments belong to abelian groups and if we multiply two commitments, we get a new commitment that contains the product of the two messages. Third, we want the commitment scheme to be length reducing, *i.e.*, the commitment is shorter than the message.

Related work. There are many examples of homomorphic commitments. Homomorphic cryptosystems such as ElGamal [ElG85], Okamoto-Uchiyama [OU98], Paillier [Pai99], BGN [BGN05] or Linear

Encryption [BBS04] can be seen as homomorphic commitment schemes that are perfectly binding and computationally hiding. Commitments based on homomorphic encryption can be converted into computationally binding and perfectly hiding homomorphic commitments, see for instance the mixed commitments of Damgård and Nielsen [DN02] and the commitment schemes used by Groth, Ostrovsky and Sahai [GOS06], Boyen and Waters [BW06], Groth [Gro06] and Groth and Sahai [GS08]. Even in the perfectly hiding versions of these commitment schemes the size of a commitment is larger than the size of a message though. This length-increase follows from the fact that the underlying building block is a cryptosystem and a ciphertext must be large enough to include the message.

There are also direct constructions of homomorphic trapdoor commitment schemes such as Guillou and Quisquater commitments [GQ88] and Pedersen commitments [Ped91]. Pedersen commitments are one of the most used commitment schemes in the field of cryptography. The public key consists of two group elements g, h belonging to a group of prime order p and we commit to a message $m \in \mathbb{Z}_p$ by computing $c = g^m h^t$, where $t \in \mathbb{Z}_p$ is a randomly chosen randomizer. Pedersen commitments are perfectly hiding with a trapdoor and if the discrete logarithm problem is hard they are computationally binding. There are many variants of the Pedersen commitment scheme. Fujisaki and Okamoto [FO97] and Damgård and Fujisaki [DF02] for instance suggest a variant where the messages can be arbitrary integers.

There is an important generalization of the Pedersen commitment scheme that makes it possible to commit to many messages at once. The public key consists of $m+1$ group elements $\gamma_1, \ldots, \gamma_m, h$ and we compute a commitment to $(m_1, \ldots, m_m)$ as $c = h^t \prod_{i=1}^m \gamma_i^{m_i}$. This commitment scheme is length-reducing since we only use one group element to commit to m messages, a feature that has been found useful in contexts such as mix-nets/voting, digital credentials, blind signatures and zero-knowledge proofs [FS01, Nef01, Bra00, KZ06, Lip03].

Common for all the homomorphic trapdoor commitment schemes[1] we mentioned above is that they are homomorphic with respect to *addition* in a ring or a field. However, in public-key cryptography it is common to work over groups that are not rings or fields and often it is useful to commit to group elements from such groups. Of course, if we know the discrete logarithms of the group elements we want to commit to, we can use the Pedersen commitment scheme to commit to the discrete logarithms. In general, we cannot expect to know the discrete logarithms of the group elements that we want to commit to though, leaving us with the open problem of constructing homomorphic trapdoor commitments to group elements.

Our contribution. The contribution of this paper is the construction of homomorphic trapdoor commitment schemes for group elements. The commitment schemes are perfectly hiding, perfectly trapdoor and computationally binding. We stress that we can commit to arbitrary group elements and trapdoor-open to arbitrary group elements, even if we do not know the discrete logarithms of these group elements. Moreover, the commitment schemes have the additional advantage of being length-reducing; we can commit to multiple group elements with one short commitment.

Our constructions are based on bilinear groups. These are groups G_1, G_2, G_T with a bilinear map $e : G_1 \times G_2 \to G_T$. Messages and randomizers are elements from G_2, whereas the commitments will consist of a few group elements in G_T. An advantage of our commitment schemes is that the constructions are very simple. In one construction, the public key consists of $n+1$ group elements $(g_r, g_1, \ldots, g_n)$ from G_1 and we commit to $m_1, \ldots, m_n \in G_2$ by choosing $r \in G_2$ at random and computing the commitment

$$c = e(g_r, r) \prod_{i=1}^{n} e(g_i, m_i).$$

[1]Boyen and Waters [BW06], Groth [Gro06] and Groth and Sahai [GS08] use homomorphic commitments to group elements, but they do not have a *trapdoor* property that makes it possible to open them to arbitrary group elements. Moreover, those commitments suffer from being length-increasing.

In the other construction, the public key consists of $2n + 4$ group elements $(g_r, h_r, g_s, h_s, g_1, h_1, \ldots, g_n, h_n)$ from G_1 and the commitment consists of picking r, s at random from G_2 and computing the commitment (c, d) as

$$c = e(g_r, r)e(g_s, s)\prod_{i=1}^{n} e(g_i, m_i) \quad \text{and} \quad d = e(h_r, r)e(h_s, s)\prod_{i=1}^{n} e(h_i, m_i).$$

The commitment schemes are computationally binding assuming the double pairing assumption respectively the simultaneous triple pairing assumption hold. The double pairing assumption says that given a random couple (g_r, g_t) from G_1 it is computationally infeasible to find non-trivial group elements $r, t \in G_2$ so

$$e(g_r, r)e(g_t, t) = 1.$$

The simultaneous triple pairing assumption says that given two random triples (g_r, g_s, g_t) and (h_r, h_s, h_t) from G_1 it is computationally infeasible to find non-trivial group elements $r, s, t \in G_2$ so

$$e(g_r, r)e(g_s, s)e(g_t, t) = 1 \quad \text{and} \quad e(h_r, r)e(h_s, s)e(h_t, t) = 1.$$

We will show that the decision Diffie-Hellman assumption in G_1 implies the double pairing assumption and perhaps surprisingly that the decision linear assumption [BBS04] in G_1 implies the simultaneous triple pairing assumption.

We remark that the roles of G_1 and G_2 can be reversed giving us commitments to group elements in G_1. Since the constructions and the assumptions would be identical after reversing the roles of G_1 and G_2, we will without loss of generality only consider the case of committing to group elements in G_2.

Applications. As an example of the usage of our commitment schemes, we consider in Section 5 the case of committing to Pedersen commitments. Pedersen commitments, allow the commitment to multiple values $m_1, \ldots, m_m \in \mathbb{Z}_p$ as $h^t \prod_{i=1}^{m} \gamma_i^{m_i}$. A Pedersen commitment is itself just a group element, and we can therefore use our commitment schemes to commit to multiple Pedersen commitments. Since our commitment schemes are homomorphic and the Pedersen commitment scheme is homomorphic, their combination is also homomorphic. We get a homomorphic trapdoor commitment scheme to mn elements from $\mathbb{Z}_p$. In contrast with the Pedersen commitment scheme, however, the public key of our scheme is only $O(m + n)$ group elements. Moreover, we propose an honest verifier zero-knowledge argument of knowledge of the committed values with a communication complexity $O(m + n)$ group and field elements, which improves on the communication complexity of mn field elements for the most practical honest verifier zero-knowledge arguments of knowledge for the Pedersen commitment scheme to mn field elements.

Such an efficient homomorphic trapdoor commitment scheme may in turn be a useful component in constructing more advanced zero-knowledge arguments. One can for instance reduce the communication complexity of Groth's [Gro09] sub-linear size zero-knowledge argument for circuit satisfiability from $O(|C|^{\frac{1}{2}})$ group elements to $O(|C|^{\frac{1}{3}})$ group elements, although the details of the construction are beyond the scope of this paper.

2 Definitions

Notation. Algorithms in our commitment schemes take a security parameter k as input written in unary. For simplicity we will sometimes omit writing the security parameter explicitly, assuming k can be deduced from the other inputs. All our algorithms will be probabilistic polynomial time algorithms. We write $y = A(x; r)$, when A on input x and randomness r outputs y. We write $y \leftarrow A(x)$, for the process of picking randomness r at random and setting $y = A(x; r)$. We also write $y \leftarrow S$ for sampling y uniformly at random from the set S. When defining security, we assume that there is an adversary attacking our schemes. The adversary is modeled as a non-uniform polynomial time stateful algorithm. By stateful, we mean that we do not need to give it the same input twice, it remembers from the last invocation what its state was. This makes the notation a little simpler, since we do not need to explicitly write out the transfer of state from one invocation to the next. Given two functions $f, g : \mathbb{N} \rightarrow [0; 1]$ we write $f(k) \approx g(k)$ when there is negligible difference, *i.e.*, $|f(k) - g(k)| = k^{-\omega(1)}$.

2.1 Commitments

A commitment scheme is a protocol between Alice and Bob that allows Alice to commit to a secret message m. Later Alice may open the commitment and reveal to Bob that she committed to m. Commitment schemes must be binding and hiding. Binding means that Alice cannot change her mind; a commitment can only be opened to one message m. Hiding means that Bob does not learn which message Alice committed to.

In this paper, we will focus on non-interactive commitment schemes. In a non-interactive commitment scheme, Alice computes the commitment herself and sends it to Bob. The opening process is also non-interactive, it simply consists of Alice sending the message and the randomness she used when creating the commitment to Bob. Bob can now run the commitment protocol himself to check that indeed this was the message Alice had committed to.

A non-interactive commitment scheme consists of three polynomial time algorithms $(\mathcal{G}, K, \mathrm{com})$. $\mathcal{G}$ is a probabilistic setup algorithm that takes as input the security parameter k and outputs some setup information gk. The setup information gk can for instance describe a finite group over which we are working, but it could also just be the security parameter written in unary so there is no loss of generality in including a setup algorithm. We include an explicit algorithm for the setup because when designing cryptographic protocols we often need the commitment scheme to work with an existing finite group. K is a probabilistic algorithm that takes as input the setup gk and generates a public commitment key ck and a trapdoor key tk. The commitment key ck specifies a message space $\mathcal{M}_{ck}$, a randomizer space $\mathcal{R}_{ck}$ and a commitment space $\mathcal{C}_{ck}$. We assume it is easy to verify membership of the message space, randomizer space and the commitment space and it is possible to sample randomizers uniformly at random from $\mathcal{R}_{ck}$. The algorithm com takes as input the commitment key ck, a message m from the message space, a randomizer r from the randomizer space and outputs a commitment c in the commitment space.

We are interested in constructing homomorphic trapdoor commitments. By homomorphic, we mean that $\mathcal{M}_{ck}, \mathcal{R}_{ck}, \mathcal{C}_{ck}$ are groups with the property that if we multiply two commitments, then we get a commitment to the product of the messages. By trapdoor we mean that given the secret trapdoor key generated by the key generator, it is possible to open a commitment to any message. For this purpose, we have two additional probabilistic polynomial time algorithms Tcom and Topen. Tcom takes the trapdoor tk as input and outputs an equivocal commitment c and an equivocation key ek. Topen on input ek, c and a message $m \in \mathcal{M}_{ck}$ creates an opening $r \in \mathcal{R}_{ck}$ of the commitment, so $c = \mathrm{com}_{ck}(m; r)$.

Definition 1 (Homomorphic trapdoor commitment scheme) *A homomorphic trapdoor commitment scheme consists of a quintuple of algorithms* $(\mathcal{G}, K, \mathrm{com}, \mathrm{Tcom}, \mathrm{Topen})$ *as described above, such that* $(\mathcal{G}, K, \mathrm{com})$ *is hiding and binding and homomorphic and* $(\mathcal{G}, K, \mathrm{com}, \mathrm{Tcom}, \mathrm{Topen})$ *has a perfect trapdoor property as defined below.*

Definition 2 (Perfect hiding) *The triple* $(\mathcal{G}, K, \mathrm{com})$ *is perfectly hiding if for all stateful adversaries* $\mathcal{A}$ *we have*

$$\begin{aligned} & \Pr\left[gk \leftarrow \mathcal{G}(1^k); (ck, tk) \leftarrow K(gk); (m_0, m_1) \leftarrow \mathcal{A}(gk, ck); c \leftarrow \mathrm{com}_{ck}(m_0) : \mathcal{A}(c) = 1\right] \\ = \; & \Pr\left[gk \leftarrow \mathcal{G}(1^k); (ck, tk) \leftarrow K(gk); (m_0, m_1) \leftarrow \mathcal{A}(gk, ck); c \leftarrow \mathrm{com}_{ck}(m_1) : \mathcal{A}(c) = 1\right], \end{aligned}$$

where we require that $\mathcal{A}$ outputs m_0, m_1 that belong to $\mathcal{M}_{ck}$.

Definition 3 (Computational binding) *The triple $(\mathcal{G}, K, \mathrm{com})$ is computationally binding if for all non-uniform polynomial time stateful adversaries $\mathcal{A}$ we have*

$$\Pr\Big[gk \leftarrow \mathcal{G}(1^k); (ck, tk) \leftarrow K(gk); (m_0, m_1, r_0, r_1) \leftarrow \mathcal{A}(gk, ck) : \\ m_0 \neq m_1 \quad \wedge \quad \mathrm{com}_{ck}(m_0; r_0) = \mathrm{com}_{ck}(m_1; r_1)\Big] \approx 0,$$

where we require that $\mathcal{A}$ outputs $m_0, m_1 \in \mathcal{M}_{ck}$ and $r_0, r_1 \in \mathcal{R}_{ck}$.

Definition 4 (Perfect trapdoor) *The quintuple $(\mathcal{G}, K, \mathrm{com}, \mathrm{Tcom}, \mathrm{Topen})$ is perfectly trapdoor if for all stateful adversaries $\mathcal{A}$ we have*

$$\begin{aligned} & \Pr\Big[gk \leftarrow \mathcal{G}(1^k); (ck, tk) \leftarrow K(gk); m \leftarrow \mathcal{A}(gk, ck); r \leftarrow \mathcal{R}_{ck}; c = \mathrm{com}_{ck}(m; r) : \mathcal{A}(c, r) = 1\Big] \\ = \; & \Pr\Big[gk \leftarrow \mathcal{G}(1^k); (ck, tk) \leftarrow K(gk); m \leftarrow \mathcal{A}(gk, ck); (c, ek) \leftarrow \mathrm{Tcom}_{ck}(tk); \\ & \qquad r \leftarrow \mathrm{Topen}_{ek}(c, m) : \mathcal{A}(c, r) = 1\Big], \end{aligned}$$

where $\mathcal{A}$ outputs $m \in \mathcal{M}_{ck}$.

We note that the perfect trapdoor property implies that the commitment scheme is perfectly hiding, since a commitment is perfectly indistinguishable from an equivocal commitment that can be opened to any message.

Definition 5 (Homomorphic) *The commitment scheme $(\mathcal{G}, K, \mathrm{com})$ is homomorphic if K always outputs ck describing groups $\mathcal{M}_{ck}, \mathcal{R}_{ck}, \mathcal{C}_{ck}$, which we will write multiplicatively, such that for all $m, m' \in \mathcal{M}_{ck}, r, r' \in \mathcal{C}_{ck}$ we have*

$$\mathrm{com}_{ck}(m; r)\mathrm{com}_{ck}(m; r') = \mathrm{com}_{ck}(mm'; rr').$$

3 Foundations

Bilinear groups. Let $\mathcal{G}$ be a probabilistic polynomial time algorithm that generates $(p, G_1, G_2, G_T, e) \leftarrow \mathcal{G}(1^k)$ such that

- p is a k-bit prime
- G_1, G_2, G_T are cyclic groups of order p
- $e : G_1 \times G_2 \rightarrow G_T$ is a non-degenerate bilinear map so
  - $e(\gamma_1, \gamma_2)$ generates G_T if γ_1, γ_2 generate G_1 and G_2
  - $\forall \gamma_1 \in G_1, \gamma_2 \in G_2, a, b \in \mathbb{Z}_p$ we have $e(\gamma_1^a, \gamma_2^b) = e(\gamma_1, \gamma_2)^{ab}$
- Group operations, evaluation of the bilinear map, sampling of generators and membership of G_1, G_2, G_T are all efficiently computable.

Double pairing assumption. The security of our first commitment scheme will be based on the double pairing assumption.[2] The double pairing problem is given random elements $g_r, g_t \in G_1$ to find a non-trivial couple $(r, t) \in G_2^2$ such that $e(g_r, r)e(g_t, t) = 1$.

[2]The double pairing assumption was also proposed independently by Abe, Haralambiev and Ohkubo [AHO10].

Definition 6 *We say the double pairing assumption holds for the bilinear group generator $\mathcal{G}$ if for all non-uniform polynomial time adversaries $\mathcal{A}$ we have*

$$\Pr\Big[gk = (p, G_1, G_2, G_T, e) \leftarrow \mathcal{G}(1^k); g_r, g_t \leftarrow G_1; (r, t) \leftarrow \mathcal{A}(gk, g_r, g_t) :$$
$$(r, t) \in G_2^2 \setminus \{(1, 1)\} \quad \wedge \quad e(g_r, r)e(g_t, t) = 1\Big] \approx 0.$$

One could also consider the reverse double pairing assumption, where $g_r, g_t \in G_2$. The double pairing assumption is used for commitments to elements in G_2, whereas the reverse double pairing assumption would be used for commitments to elements in G_1. We will without loss of generality only describe commitments to group elements in G_2 in the paper.

SIMULTANEOUS TRIPLE PAIRING ASSUMPTION. The security of our second commitment scheme will be based on the simultaneous triple pairing assumption. The simultaneous triple pairing problem is given random elements $g_r, h_r, g_s, h_s, g_t, h_t \in G_1$ to find a non-trivial triple $(r, s, t) \in G_2^3$ such that $e(g_r, r)e(g_s, s)e(g_t, t) = 1$ and $e(h_r, r)e(h_s, s)e(h_t, t) = 1$.

Definition 7 (Simultaneous triple pairing assumption) *We say the simultaneous triple pairing assumption holds for the bilinear group generator $\mathcal{G}$ if for all non-uniform polynomial time adversaries $\mathcal{A}$ we have*

$$\Pr\Big[gk = (p, G_1, G_2, G_T, e) \leftarrow \mathcal{G}(1^k); g_r, h_r, g_s, h_s, g_t, h_t \leftarrow G_1;$$
$$(r, s, t) \leftarrow \mathcal{A}(gk, g_r, h_r, g_s, h_s, g_t, h_t) : (r, s, t) \in G_2^3 \setminus \{(1, 1, 1)\}$$
$$\wedge \quad e(g_r, r)e(g_s, s)e(g_t, t) = 1 \quad \wedge \quad e(h_r, r)e(h_s, s)e(h_t, t) = 1\Big] \approx 0.$$

The simultaneous triple pairing assumption is used to build commitments to group elements in G_2. We could also define a reverse simultaneous triple pairing assumption, which would give us commitments to group elements in G_1. We will without loss of generality only describe commitments to group elements in G_2 in the paper.

COMPARISON. The double pairing assumption is the simplest of the two assumptions and leads to the most efficient commitment scheme. It is a stronger assumption than the simultaneous triple pairing assumption though as the following theorem shows.

Theorem 8 *If the double pairing assumption holds for $\mathcal{G}$, then the simultaneous triple pairing assumption holds for $\mathcal{G}$.*

Proof. We will show that if $\mathcal{A}$ has probability $\epsilon(k)$ of breaking the simultaneous triple pairing assumption for $\mathcal{G}$, then there is an algorithm $\mathcal{B}$ that breaks the double pairing assumption for $\mathcal{G}$ with at least $\epsilon(k) - 1/p$ chance.

Let (gk, g_r, g_t) be a random double pairing challenge given to $\mathcal{B}$. If $g_r = 1$ or $g_t = 1$, it is trivial to find a solution to the double pairing problem. If $g_r \neq 1$ and $g_t \neq 1$, the double pairing adversary $\mathcal{B}$ selects $\rho_r, \tau_r, \rho_s, \tau_s, \rho_t, \tau_t \leftarrow \mathbb{Z}_p$ and computes $h_r = g_r^{\rho_r} g_t^{\tau_r}, h_s = g_r^{\rho_s} g_t^{\tau_s}, h_t = g_r^{\rho_t} g_t^{\tau_t}$. It also selects $\hat{g}_r, \hat{g}_s, \hat{g}_t \leftarrow G_1$ at random.

The double pairing adversary $\mathcal{B}$ runs $\mathcal{A}$ on $(gk, \hat{g}_r, \hat{g}_s, \hat{g}_t, h_r, h_s, h_t)$ and with at least $\epsilon(k)$ probability it gets a non-trivial solution $(\hat{r}, \hat{s}, \hat{t})$ to the simultaneous triple pairing problem. The solution satisfies $e(h_r, \hat{r})e(h_s, \hat{s})e(h_t, \hat{t}) = 1$ (it will not be needed in the proof that the solution also satisfies $e(\hat{g}_r, \hat{r})e(\hat{g}_s, \hat{s})e(\hat{g}_t, \hat{t}) = 1$).

We deduce $e(g_r, \hat{r}^{\rho_r}\hat{s}^{\rho_s}\hat{t}^{\rho_t})e(g_t, \hat{r}^{\tau_r}\hat{s}^{\tau_s}\hat{t}^{\tau_t}) = 1$. No matter what the ρ_r, ρ_s, ρ_t values are, the random choice of τ_r, τ_s, τ_t makes h_r, h_s, h_t be random group elements. This means $\mathcal{A}$ has no information whatsoever about ρ_r, ρ_s, ρ_t and hence there is probability $1/p$ for $\hat{r}^{\rho_r}\hat{s}^{\rho_s}\hat{t}^{\rho_t} = 1$. With at least $\epsilon(k) - 1/p$ probability $(\hat{r}^{\rho_r}\hat{s}^{\rho_s}\hat{t}^{\rho_t}, \hat{r}^{\tau_r}\hat{s}^{\tau_s}\hat{t}^{\tau_t})$ is a solution to the double pairing problem. □

There are some types of bilinear groups the double pairing assumption cannot be true. Galbraith, Paterson and Smart [GPS08] classify bilinear groups into three types:

Type 1: $G_1 = G_2$.

Type 2: There is no efficiently computable homomorphism $\psi : G_1 \to G_2$.

Type 3: There are no efficiently computable homomorphisms in either direction between G_1 and G_2.

The double pairing assumption can only hold when there is no efficiently computable non-trivial homomorphism $\psi : G_1 \to G_2$, since otherwise $r = \psi(g_t)$ and $t = \psi(g_r)$ would be a solution to the double pairing problem. This means the double pairing assumption does not hold in bilinear groups of Type 1 and the reverse double pairing assumption does not hold in bilinear groups of Type 1 or Type 2. In contrast, the simultaneous triple pairing assumption and the reverse simultaneous triple pairing assumption are plausible in all types of bilinear groups.

3.1 Security Analysis of the Double Pairing Assumption

The double pairing assumption is a new assumption. To gain confidence in the double pairing assumption, we will now show that it is implied by the decision Diffie-Hellman assumption in G_1.

Definition 9 (Decision Diffie-Hellman assumption) *The decision Diffie-Hellman assumption holds in G_1 for $\mathcal{G}$ if for all non-uniform polynomial time adversaries $\mathcal{A}$ we have*

$$\begin{aligned} & \Pr\Big[gk = (p, G_1, G_2, G_T, e) \leftarrow \mathcal{G}(1^k)\ ;\ g_r, g_t \leftarrow G_1;\ \rho \leftarrow \mathbb{Z}_p\ : \mathcal{A}(gk, g_r, g_t, g_r^\rho, g_t^\rho) = 1\Big] \\ \approx\ & \Pr\Big[gk = (p, G_1, G_2, G_T, e) \leftarrow \mathcal{G}(1^k)\ ;\ g_r, g_t \leftarrow G_1;\ \rho, \tau \leftarrow \mathbb{Z}_p\ : \mathcal{A}(gk, g_r, g_t, g_r^\rho, g_t^\tau) = 1\Big]. \end{aligned}$$

Theorem 10 *If the decision Diffie-Hellman assumption holds in G_1 for $\mathcal{G}$, then the double pairing assumption holds for $\mathcal{G}$.*

Proof. We will show that an adversary $\mathcal{A}$ that breaks the double pairing assumption with probability $\epsilon(k)$ can be used to build a decision Diffie-Hellman adversary $\mathcal{B}$ that has advantage $\epsilon(k) - 3/p$ in breaking the decision Diffie-Hellman problem.

Given a Diffie-Hellman challenge $(gk, g_r, g_t, g_r^\rho, g_t^\tau)$, where τ may be random or may be equal to ρ, $\mathcal{B}$ gives the challenge (gk, g_r, g_t) to $\mathcal{A}$. $\mathcal{A}$ outputs a pair (r, t) in response. $\mathcal{B}$ outputs 1 if (r, t) is a non-trivial pair so $e(g_r, r)e(g_t, t) = 1$ and $e(g_r^\rho, r)e(g_t^\tau, t) = 1$, otherwise $\mathcal{B}$ outputs 0.

Let us look at the first distribution $(gk, g_r, g_t, g_r^\rho, g_t^\rho)$. There is $\epsilon(k)$ chance for $\mathcal{A}$ outputting a non-trivial pair so $e(g_r, r)e(g_t, t) = 1$, in which case we will also have $e(g_r^\rho, r)e(g_t^\rho, t) = 1$. So here $\mathcal{B}$ has probability $\epsilon(k)$ of outputting 1.

Let us now look at the second distribution $(gk, g_r, g_t, g_r^\rho, g_t^\tau)$. There is less than $3/p$ chance of $g_r = 1, g_t = 1$ or $\rho = \tau$. In case $g_r \neq 1, g_t \neq 1$ and $\rho \neq \tau$, there is no non-trivial couple r, t such that $e(g_r, r)e(g_t, t) = 1$ and $e(g_r^\rho, r)e(g_t^\tau, t) = 1$. □

3.2 Security Analysis of the Simultaneous Triple Pairing Assumption

To gain confidence in the simultaneous triple pairing assumption, we will show that it follows from the decision linear assumption [BBS04]. The decision linear problem is to decide whether a tuple $(g_1, g_2, g_3, g_1^\rho, g_2^\sigma, g_3^\tau)$ has $\tau = \rho + \sigma$ or τ is random.

Definition 11 (Decision linear assumption) *The decision linear assumption holds in G_1 for $\mathcal{G}$ if* *for all non-uniform polynomial time adversaries $\mathcal{A}$ we have:*

$$\Pr\Big[gk = (p, G_1, G_2, G_T, e) \leftarrow \mathcal{G}(1^k)\ ;\ g_1, g_2, g_3 \leftarrow G_1;\ \rho, \sigma \leftarrow \mathbb{Z}_p\ :$$
$$\mathcal{A}(gk, g_1, g_2, g_3, g_1^\rho, g_2^\sigma, g_3^{\rho+\sigma}) = 1\Big]$$
$$\approx\ \Pr\Big[gk = (p, G_1, G_2, G_T, e) \leftarrow \mathcal{G}(1^k)\ ;\ g_1, g_2, g_3 \leftarrow G_1;\ \rho, \sigma, \tau \leftarrow \mathbb{Z}_p\ :$$
$$\mathcal{A}(gk, g_1, g_2, g_3, g_1^\rho, g_2^\sigma, g_3^\tau) = 1\Big].$$

Theorem 12 *If the decision linear assumption holds in G_1 for $\mathcal{G}$, then the simultaneous triple pairing assumption holds for $\mathcal{G}$.*

Proof. We will show how to convert an adversary $\mathcal{A}$ that breaks the simultaneous triple pairing assumption with probability $\epsilon(k)$ into an adversary $\mathcal{B}$ that has advantage $\epsilon(k) - 11/p$ against the decision linear assumption.

On a decision linear challenge $(gk, g_1, g_2, g_3, h_1, h_2, h_3)$, $\mathcal{B}$ picks $\alpha, \beta \leftarrow \mathbb{Z}_p$ at random, sets

$$g_r = g_1\ ,\ h_r = h_1\ ,\ g_s = g_2\ ,\ h_s = h_2\ ,\ g_t = g_3^2 g_1^\alpha g_2^\beta\ ,\ h_t = h_3 h_1^\alpha h_2^\beta$$

and runs $(r, s, t) \leftarrow \mathcal{A}(gk, g_r, h_r, g_s, h_s, g_t, h_t)$. $\mathcal{B}$ returns 1 if (r, s, t) is a non-trivial solution to

$$\begin{array}{cccc} & e(g_r, r)e(g_s, s)e(g_t, t) = 1 & \wedge & e(h_r, r)e(h_s, s)e(h_t, t) = 1 \\ \wedge & e(g_1, rt^\alpha)e(g_3, t) = 1 & \wedge & e(g_2, st^\beta)e(g_3, t) = 1, \end{array}$$

and else it returns 0.

Let us now analyze the success probability of $\mathcal{B}$. It is given a challenge $(gk, g_1, g_2, g_3, g_1^\rho, g_2^\sigma, g_3^\tau)$, where $\tau = \rho + \sigma$ or τ is random. By the choice of $(g_r, g_s, g_t, h_r, h_s, h_t)$ a solution (r, s, t) to the simultaneous triple pairing problem $e(g_r, r)e(g_s, s)e(g_t, t) = 1 \wedge e(h_r, r)e(h_s, s)e(h_t, t) = 1$ also satisfies

$$\begin{array}{cc} & \Big(e(g_1, rt^\alpha)e(g_3, t)\Big)\Big(e(g_2, st^\beta)e(g_3, t)\Big) = 1 \\ \wedge & \Big(e(g_1, rt^\alpha)e(g_3, t)\Big)^\rho\Big(e(g_2, st^\beta)e(g_3, t)\Big)^\sigma = e(g_3, t^{\rho+\sigma-\tau}). \end{array}$$

Let us first analyze the case of τ being random. If $g_3 \neq 1, \tau \neq \rho + \sigma$, then a simultaneous triple pairing solution (r, s, t) that also satisfies $e(g_1, rt^\alpha)e(g_3, t) = 1\ \wedge\ e(g_2, st^\beta)e(g_3, t) = 1$ would by the latter equation given above have $t = 1$. If $g_1 \neq 1, g_2 \neq 1, \rho \neq \sigma$ the two equations above then imply $r = 1$ and $s = 1$, leading us to conclude that (r, s, t) is trivial. Since the chance of $g_1 = 1 \vee g_2 = 1 \vee g_3 \vee \rho = \sigma \vee \tau = \rho + \sigma$ is less than $5/p$, there is less than $5/p$ chance of outputting 1 when τ is chosen at random.

Let us now analyze the case $\tau = \rho + \sigma$. The simultaneous triple pairing problem given to $\mathcal{A}$ is of the form $(gk, g_1, g_2, g_3^2 g_1^\alpha g_2^\beta, g_1^\rho, g_2^\sigma, g_3^\tau g_1^{\rho\alpha}, g_2^{\sigma\beta})$. Assuming $g_1 \neq 1, g_2 \neq 1, \rho \neq \sigma$ this corresponds to a standard triple pairing challenge conditioned on $g_1 \neq 1, g_2 \neq 1, h_1 \neq h_2$. So there is at least probability $\epsilon(k) - 3/p$ chance that $\mathcal{A}$ outputs a non-trivial solution (r, s, t) so $e(g_r, r)e(g_s, s)e(g_t, t) = 1$ and $e(h_r, r)e(h_s, s)e(h_t, t) = 1$. Since $\tau = \rho + \sigma$ and $\rho \neq \sigma$, the two equations above tell us that such a solution (r, s, t) also satisfies $e(g_1, rt^\alpha)e(g_3, t) = 1$ and $e(g_2, st^\beta)e(g_3, t) = 1$. Since there is probability at most $3/p$ for $g_1 = 1 \vee g_2 = 1 \vee \rho = \sigma$, we conclude that $\mathcal{B}$ has probability at least $\epsilon(k) - 6/p$ for outputting 1 when $\tau = \rho + \sigma$. $\square$

4 Homomorphic Trapdoor Commitments to Group Elements

We will now present the homomorphic trapdoor commitment schemes. The setup algorithm generates a bilinear group (p, G_1, G_2, G_T, e) and the commitment schemes can commit to n group elements from G_2.

4.1 Commitments based on the Double Pairing Assumption

We have message space $\mathcal{M}_{ck} = G_2^n$, randomizer space $\mathcal{R}_{ck} = G_2$ and commitment space $\mathcal{C}_{ck} = G_T$, where each of them are interpreted as a group using entry-wise multiplication.

Setup: On input 1^k return $gk = (p, G_1, G_2, G_T, e) \leftarrow \mathcal{G}(1^k)$.

Key generator: On input gk pick at random $g_r \leftarrow G_1 \setminus \{1\}$ and $x_1, \ldots, x_n \leftarrow \mathbb{Z}_p$ and define $g_1 = g_r^{x_1}, \cdots, g_n = g_r^{x_n}$. The commitment key is $ck = (gk, g_r, g_1, \ldots, g_n)$ and the trapdoor key is $tk = (gk, g_r, x_1, \ldots, x_n)$.

Commitment: Using commitment key ck on input message $(m_1, \ldots, m_n) \in G_2^n$ pick randomizer $r \leftarrow G_2$. The commitment is given by

$$c = e(g_r, r) \prod_{i=1}^{n} e(g_i, m_i).$$

Trapdoor commitment: Using commitment key ck and trapdoor key tk generate an equivocal commitment $c \in G_T$ by picking $r \leftarrow G_2$ and computing $c = e(g_r, r)$ The corresponding equivocation key is $ek = (tk, r)$.

Trapdoor opening: On an equivocal commitment $c \in G_T$ to a message $(m_1, \ldots, m_n) \in G_2^n$ using the equivocation key ek, compute and return the trapdoor opening $r' = r \prod_{i=1}^{n} m_i^{-x_i}$.

Theorem 13 $(\mathcal{G}, K, \mathrm{com}, \mathrm{Tcom}, \mathrm{Topen})$ *described above is homomorphic, perfectly trapdoor, and assuming the double pairing assumption holds for $\mathcal{G}$ the commitment scheme is computationally binding.*

Proof. Given a commitment key $ck = (gk, g_r, g_1, \ldots, g_n)$ it is straightforward to check the homomorphic property. For all $(m_1, \ldots, m_n), (m'_1, \ldots, m'_n) \in G_2^n$ and all $r, r' \in G_2$ we have

$$e(g_r, r) \prod_{i=1}^{n} e(g_i, m_i) \cdot e(g_r, r') \prod_{i=1}^{n} e(g_i, m'_i) = e(g_r, rr') \prod_{i=1}^{n} e(g_i, m_i m'_i).$$

Next, we will prove that the commitment scheme has the perfect trapdoor property. By construction, $g_r \neq 1$ so both real commitments and trapdoor commitments are distributed uniformly at random in G_T, because of their $e(g_r, r)$ factor where r is chosen randomly from G_2. The fact that $g_r \neq 1$ also implies that for any commitment c and set of messages $(m_1, \ldots, m_n) \in G_2^n$ there is a unique randomizer $r \in G_2$ so $c = e(g_r, r) \prod_{i=1}^{n} e(g_i, m_i)$. To conclude the proof for the perfect trapdoor property, we therefore just need to show that the trapdoor opening algorithm gives the correct opening r' of the commitment. This follows from

$$e(g_r, r') \prod_{i=1}^{n} e(g_i, m_i) = e(g_r, r \prod_{i=1}^{n} m_i^{-x_i}) \prod_{i=1}^{n} e(g_r^{x_i}, m_i) = e(g_r, r) = c.$$

Finally, we will prove that the commitment scheme is computationally binding if the double pairing assumption holds for $\mathcal{G}$. We will show that if $\mathcal{A}$ has probability $\epsilon(k)$ of breaking the binding property, then there is an algorithm $\mathcal{B}$ that breaks the double pairing assumption with at least $\epsilon(k) - 3/p$ chance.

Let (gk, g_r, g_t) be a random double pairing challenge given to $\mathcal{B}$. If $g_r = 1$ or $g_t = 1$, it is trivial to break the double pairing assumption. If $g_r \neq 1, g_t \neq 1$ the double pairing adversary $\mathcal{B}$ selects $\rho_1, \tau_1, \ldots, \rho_n, \tau_n \leftarrow \mathbb{Z}_p$ and computes $g_1 = g_r^{\rho_1} g_t^{\tau_1}, \ldots, g_n = g_r^{\rho_n} g_t^{\tau_n}$. It runs $\mathcal{A}$ on $(gk, g_r, g_1, \ldots, g_n)$ and with $\epsilon(k)$ probability it gets two different openings to the same commitment. If the openings are $m_1, \ldots, m_n, r$ and $m'_1, \ldots, m'_n, r'$, we have by the homomorphic property of the commitment scheme that $e(g_r, r^{-1}r')\prod_{i=1}^n e(g_i, m_i^{-1}m_i') = 1$. Defining $\mu_1 = m_1^{-1}m_1', \ldots, \mu_n = m_n^{-1}m_n'$ this means we have $e(g_r, r^{-1}r')\prod_{i=1}^n e(g_i, \mu_i) = 1$ where at least one $\mu_i \neq 1$. This implies

$$e(g_r, r^{-1}r')\prod_{i=1}^n e(g_r^{\rho_i}g_t^{\tau_i}, \mu_i) = e(g_r, r^{-1}r'\prod_{i=1}^n \mu_i^{\rho_i})e(g_t, \prod_{i=1}^n \mu_i^{\tau_i}) = 1.$$

This breaks the double pairing assumption unless $r^{-1}r'\prod_{i=1}^n \mu_i^{\rho_i} = 1$ and $\prod_{i=1}^n \mu_i^{\tau_i} = 1$ at the same time. However, since the ρ_i's are perfectly hidden by the τ_i's, we have no more than $1/p$ chance of the latter equality holding when there is some $\mu_i \neq 1$. □

4.2 Commitments based on the Simultaneous Triple Pairing Assumption

We have message space $\mathcal{M}_{ck} = G_2^n$, randomizer space $\mathcal{R}_{ck} = G_2^2$ and commitment space $\mathcal{C}_{ck} = G_T^2$, where each of them are interpreted as a group using entry-wise multiplication.

Setup: On input 1^k return $gk = (p, G_1, G_2, G_T, e) \leftarrow \mathcal{G}(1^k)$.

Key generator: On input gk pick at random $g \leftarrow G_1 \setminus \{1\}$ and $x_r, y_r, x_s, y_s, x_1, y_1, \ldots, x_n, y_n \leftarrow \mathbb{Z}_p$ such that $x_r y_s \neq x_s y_r$ and define

$$g_r = g^{x_r} \quad h_r = g^{y_r} \quad g_s = g^{x_s} \quad h_s = g^{y_s} \quad g_1 = g^{x_1} \quad h_1 = g^{y_1} \cdots g_n = g^{x_n} \quad h_n = g^{y_n}.$$

The commitment key is $ck = (gk, g_r, h_r, g_s, h_s, g_1, h_1, \ldots, g_n, h_n)$ and the trapdoor key is $tk = (gk, g, x_r, x_s, y_r, y_s, x_1, y_1, \ldots, x_n, y_n)$.

Commitment: Using commitment key ck on input message $(m_1, \ldots, m_n) \in G_2^n$ pick randomizer $(r, s) \leftarrow G_2^2$. The commitment is $(c, d) \in G_T^2$ given by

$$c = e(g_r, r)e(g_s, s)\prod_{i=1}^n e(g_i, m_i) \quad \text{and} \quad d = e(h_r, r)e(h_s, s)\prod_{i=1}^n e(h_i, m_i).$$

Trapdoor commitment: Using commitment key ck and trapdoor key tk, generate an equivocal commitment $(c, d) \in G_T^2$ by picking $(r, s) \leftarrow G_2^2$ and computing

$$c = e(g_r, r)e(g_s, s) \quad \text{and} \quad d = e(h_r, r)e(h_s, s).$$

The corresponding equivocation key is $ek = (tk, r, s)$.

Trapdoor opening: To trapdoor open an equivocal commitment $(c, d) \in G_T^2$ to a message $(m_1, \ldots, m_n) \in G_2^n$ using the equivocation key ek, compute

$$a = r^{x_r}s^{x_s}\prod_{i=1}^n m_i^{-x_i} \quad \text{and} \quad b = r^{y_r}s^{y_s}\prod_{i=1}^n m_i^{-y_i}.$$

Since $x_r y_s \neq x_s y_r$ we can compute

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} x_r & x_s \\ y_r & y_s \end{pmatrix}^{-1}.$$

Compute

$$r' = a^{\alpha}b^{\beta} \quad \text{and} \quad s' = a^{\gamma}b^{\delta}.$$

Return the opening (r', s') of (c, d) to message $(m_1, \ldots, m_n)$.

Theorem 14 $(\mathcal{G}, K, \mathrm{com}, \mathrm{Tcom}, \mathrm{Topen})$ *described above is a homomorphic trapdoor commitment scheme to n group elements. It has the perfect trapdoor property and assuming the simultaneous triple pairing assumption holds for $\mathcal{G}$ the commitment scheme is computationally binding.*

Proof. Given a commitment key $ck = (gk, g_r, h_r, g_s, h_s, g_1, h_1, \ldots, g_n, h_n)$ it is straightforward to check the homomorphic property. For all $(m_1, \ldots, m_n), (m_1', \ldots, m_n') \in G_2^n$ and all $(r, s), (r', s') \in G_2^2$ we have

$$\begin{aligned} e(g_r, r)e(g_s, s)\prod_{i=1}^n e(g_i, m_i) \cdot e(g_r, r')e(g_s, s')\prod_{i=1}^n e(g_i, m_i') &= e(g_r, rr')e(g_s, ss')\prod_{i=1}^n e(g_i, m_i m_i') \\ e(h_r, r)e(h_s, s)\prod_{i=1}^n e(h_i, m_i) \cdot e(h_r, r')e(h_s, s')\prod_{i=1}^n e(h_i, m_i') &= e(h_r, rr')e(h_s, ss')\prod_{i=1}^n e(h_i, m_i m_i') \end{aligned}$$

Next, we will prove that the commitment scheme has the perfect trapdoor property. By construction, $x_r y_s \neq x_s y_r$ so (x_r, y_r) and (x_s, y_s) are linearly independent in $\mathbb{Z}_p^2$. We can deduce from this that both real commitments and trapdoor commitments are distributed uniformly at random in G_T^2, because of their $e(g_r, r)e(g_s, s)$ and $e(h_r, r)e(h_s, s)$ factors where r, s are chosen randomly from G_2. The linear independence of (x_r, y_r) and (x_s, y_s) also implies that for any pair $(c, d) \in G_T^2$ and a set of messages $(m_1, \ldots, m_n) \in G_2^n$ there is a unique randomizer $(r, s) \in G_2^2$ so

$$c = e(g_r, r)e(g_s, s)\prod_{i=1}^n e(g_i, m_i) \quad \wedge \quad d = e(h_r, r)e(h_s, s)\prod_{i=1}^n e(h_i, m_i).$$

To conclude the proof for the perfect trapdoor property, we therefore just need to show that the trapdoor opening algorithm gives the correct opening (r', s') of the commitment. Since

$$\begin{pmatrix} x_r & x_s \\ y_r & y_s \end{pmatrix}\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

we have

$$\begin{aligned} e(g_r, r')e(g_s, s') &= e(g^{x_r}, a^\alpha b^\beta)e(g^{x_s}, a^\gamma b^\delta) = e(g, a^{x_r\alpha + x_s\gamma})e(g, b^{x_r\beta + x_s\delta}) = e(g, a) \\ e(h_r, r')e(h_s, s') &= e(g^{y_r}, a^\alpha b^\beta)e(g^{y_s}, a^\gamma b^\delta) = e(g, a^{y_r\alpha + y_s\gamma})e(g, b^{y_r\beta + y_s\delta}) = e(g, b). \end{aligned}$$

By plugging in $a = r^{x_r} s^{x_s} \prod_{i=1}^n m_i^{-x_i}$ and $b = r^{y_r} s^{y_s} \prod_{i=1}^n m_i^{-y_i}$ we get

$$\begin{aligned} e(g_r, r')e(g_s, s')\prod_{i=1}^n e(g_i, m_i) &= e(g, r^{x_r} s^{x_s})\prod_{i=1}^n e(g, m_i^{x_i - x_i}) = e(g_r, r)e(g_s, s) = c \\ e(h_r, r')e(h_s, s')\prod_{i=1}^n e(h_i, m_i) &= e(g, r^{y_r} s^{y_s})\prod_{i=1}^n e(g, m_i^{y_i - y_i}) = e(h_r, r)e(h_s, s) = d, \end{aligned}$$

as we wanted.

Finally, we will prove that the commitment scheme is computationally binding if the simultaneous triple pairing assumption holds for $\mathcal{G}$. More precisely, we will show that if $\mathcal{A}$ has probability $\epsilon(k)$ of breaking the binding property, then there is an algorithm $\mathcal{B}$ that breaks the simultaneous triple pairing assumption with at least $\epsilon(k) - 3/p$ chance.

Let $(gk, g_r, g_s, g_t, h_r, h_s, h_t)$ be a random simultaneous triple pairing challenge for $\mathcal{B}$. Fix some $g \neq 1$ and let $x_r = \log_g(g_r), x_s = \log_g(g_s), y_r = \log_g(h_r), y_s = \log_g(h_s)$. We pick at random $\rho_1, \sigma_1, \tau_1, \ldots, \rho_n, \sigma_n, \tau_n \leftarrow \mathbb{Z}_p$ and define $g_1, h_1, \ldots, g_n, h_n$ by

$$g_i = g_r^{\rho_i} g_s^{\sigma_i} g_t^{\tau_i} \qquad\qquad h_i = h_r^{\rho_i} h_s^{\sigma_i} h_t^{\tau_i}.$$

If (x_r, y_r) and (x_s, y_s) are linearly independent in $\mathbb{Z}_p^2$ all these group elements are randomly distributed in G_1. This means $ck = (gk, g_r, h_r, g_s, h_s, g_1, h_1, \ldots, g_n, h_n)$ has the same distribution as commitment keys generated by K.

$\mathcal{B}$ gives this ck to $\mathcal{A}$ and in case $x_r y_s \neq x_s y_r$ it has $\epsilon(k)$ probability of getting two different messages $(m_1, \ldots, m_n), (m'_1, \ldots, m'_n)$ and randomizers $(r, s), (r', s')$ so

$$\mathrm{com}_{ck}(m_1, \ldots, m_n; r, s) = \mathrm{com}_{ck}(m'_1, \ldots, m'_n; r', s').$$

Define $\mu_1 = m'_1 m_1^{-1}, \ldots, \mu_n = m'_n m_n^{-1}$ and $r'' = r' r^{-1}, s'' = s' s^{-1}$. By the homomorphic property of the commitment scheme we have $\mathrm{com}_{ck}(\mu_1, \ldots, \mu_n; r'', s'') = (1, 1)$. This gives us

$$\begin{aligned} e(g_r, r'')e(g_s, s'')\prod_{i=1}^n e(g_i, \mu_i) = e(g_r, r''\prod_{i=1}^n \mu_i^{\rho_i})e(g_s, s''\prod_{i=1}^n \mu_i^{\sigma_i})e(g_t, \prod_{i=1}^n \mu_i^{\tau_i}) &= 1 \\ e(h_r, r'')e(h_s, s'')\prod_{i=1}^n e(h_i, \mu_i) = e(h_r, r''\prod_{i=1}^n \mu_i^{\rho_i})e(h_s, s''\prod_{i=1}^n \mu_i^{\sigma_i})e(h_t, \prod_{i=1}^n \mu_i^{\tau_i}) &= 1. \end{aligned}$$

Since $(m_1, \ldots, m_n)$ and $(m'_1, \ldots, m'_n)$ are different, there is at least one $\mu_i \neq 1$. Recall $g_i = g_r^{\rho_i} g_s^{\sigma_i} g_t^{\tau_i}$ and $h_i = h_r^{\rho_i} h_s^{\sigma_i} h_t^{\tau_i}$ for random $\rho_i, \sigma_i, \tau_i \leftarrow \mathbb{Z}_p$. With (x_r, y_r) and (x_s, y_s) linearly independent in $\mathbb{Z}_p^2$ there is for any τ'_i a unique pair $(\rho'_i, \sigma'_i) \in \mathbb{Z}_p^2$ that would yield g_i, h_i. This means from $\mathcal{A}$'s perspective τ_i is a perfectly hidden random value in $\mathbb{Z}_p$. The probability that $\prod_{i=1}^n \mu_i^{\tau_i} = 1$ is therefore at most $1/p$.

Conditioned on $x_r y_s \neq x_s y_r$ the adversary $\mathcal{B}$ breaks the simultaneous triple pairing problem with probability $\epsilon(k) - 1/p$. There is less than $2/p$ chance for the discrete logarithms satisfying $x_r y_s = x_s y_r$. We conclude that $\mathcal{B}$ has more than $\epsilon(k) - 3/p$ chance of $(r'' \prod_{i=1}^n \mu_i^{\rho_i}, s'' \prod_{i=1}^n \mu_i^{\sigma_i}, \prod_{i=1}^n \mu_i^{\tau_i})$ being a non-trivial solution to the simultaneous triple pairing problem. $\square$

5 Committing to Commitments

Recall the Pedersen commitment to multiple elements from $\mathbb{Z}_p$. The public key consists of $\gamma_1, \ldots, \gamma_m, h$ and we commit to $m_1, \ldots, m_m \in \mathbb{Z}_p$ by computing $c = h^t \prod_{i=1}^m \gamma_i^{m_i}$ for $t \leftarrow \mathbb{Z}_p$. Since Pedersen commitments are group elements, we can use one of our commitment schemes to commit to multiple Pedersen commitments. Each Pedersen commitment can hold m elements from $\mathbb{Z}_p$ so we get a commitment to mn elements from $\mathbb{Z}_p$. Since our commitment scheme is homomorphic with respect to multiplication in G_2 and the Pedersen commitments are homomorphic with respect to addition in $\mathbb{Z}_p$, the combined commitment scheme is homomorphic with respect to addition in $\mathbb{Z}_p$. Moreover, since our commitment schemes is a perfectly hiding trapdoor commitment scheme, the combined commitment scheme is also a perfectly hiding trapdoor commitment scheme. The binding property relies on the discrete logarithm assumption in G_2 and either the double pairing assumption or the simultaneous triple pairing assumption.

We will now give the full protocol for the combined commitment scheme[3], where $(\mathcal{G}, K, \mathrm{com}, \mathrm{Tcom}, \mathrm{Topen})$ is one of our commitment schemes for n elements in G_2.

Setup: On input 1^k return $gk = (p, G_1, G_2, G_T, e) \leftarrow \mathcal{G}(1^k)$.

Key generator: On input gk pick at random $\gamma_1, \ldots, \gamma_m, h \leftarrow G_2 \setminus \{1\}$ and $(ck, tk) \leftarrow K(gk)$. The commitment key is $(ck, \gamma_1, \ldots, \gamma_m, h)$ and the trapdoor key is tk.

[3]The commitment scheme can be simplified by omitting the h component in the Pedersen commitment scheme, since we only need the binding property of the Pedersen commitment scheme. The trapdoor property will follow from the trapdoor property of our commitment scheme, even if the simplified Pedersen commitment scheme is not hiding. For conceptual simplicity we have opted for maintaining the unmodified Pedersen commitments in our description, which may also be useful in some cases as the full Pedersen commitment scheme provides an alternative trapdoor.

Commitment: On message $(m_{11},\dots,m_{mn})\in\mathbb{Z}_p^{mn}$ pick $r\leftarrow\mathcal{R}_{ck}$ and $t_1,\dots,t_n\leftarrow\mathbb{Z}_p$ and compute

$$c=\mathrm{com}_{ck}(c_1,\dots,c_n;r)\quad\text{ where }\quad c_j=h^{t_j}\prod_{i=1}^m\gamma_i^{m_{ij}}.$$

Trapdoor commitment: Generate an equivocal commitment $(c,ek)\leftarrow\mathrm{Tcom}_{ck}(tk)$.

Trapdoor opening: To trapdoor open the equivocal commitment c to a message $(m_{11},\dots,m_{mn})\in\mathbb{Z}_p^{mn}$ pick $t_1,\dots,t_n\leftarrow\mathbb{Z}_p$ and using the equivocation key ek generate $r'=\mathrm{Topen}_{ek}(c,c_1,\dots,c_n)$, where $c_j=h^{t_j}\prod_{i=1}^m\gamma_i^{m_{ij}}$.

The public key consists of $n+1$ group elements in G_1 and $m+1$ group elements in G_2 if we base it on the double pairing assumption, and the public key consists of $2n+4$ group elements in G_1 and $m+1$ group elements in G_2 if we base it on the simultaneous triple pairing assumption. This means that unlike the Pedersen commitment scheme the combined commitment scheme enjoys having both a sub-linear size public key and constant size commitments. The following theorem shows that the combined commitment scheme is secure.

Theorem 15 *The combined commitment scheme is homomorphic, perfect trapdoor, and computationally binding assuming the discrete logarithm problem is hard in G_2 and assuming $(\mathcal{G},K,\mathrm{com})$ is computationally binding.*

Proof. Let us first show that the combined commitment scheme is homomorphic, since both the underlying commitment schemes are homomorphic. We have for all choices of $r,t_1,\dots,t_n,m_{11},\dots,m_{mn}$ and $r',t_1',\dots,t_n',m_{11}',\dots,m_{mn}'$ that

$$\begin{aligned}
&\mathrm{com}_{ck}(h^{t_1}\prod_{i=1}^m\gamma_i^{m_{i1}},\dots,h^{t_n}\prod_{i=1}^m\gamma_i^{m_{in}};r)\cdot\mathrm{com}_{ck}(h^{t_1'}\prod_{i=1}^m\gamma_i^{m_{i1'}},\dots,h^{t_n'}\prod_{i=1}^m\gamma_i^{m_{in}'};r')\\
=\;&\mathrm{com}_{ck}(h^{t_1}\prod_{i=1}^m\gamma_i^{m_{i1}}\cdot h^{t_1'}\prod_{i=1}^m\gamma_i^{m_{i1'}},\dots,h^{t_n}\prod_{i=1}^m\gamma_i^{m_{in}}\cdot h^{t_n'}\prod_{i=1}^m\gamma_i^{m_{in}'};r\cdot r')\\
=\;&\mathrm{com}_{ck}(h^{t_1+t_1'}\prod_{i=1}^m\gamma_i^{m_{i1}+m_{ij}'},\dots,h^{t_n+t_n'}\prod_{i=1}^m\gamma_i^{m_{in}+m_{in}'};rr'),
\end{aligned}$$

which is a commitment to $m_{11}+m_{11}',\dots,m_{mn}+m_{mn}'$ using randomness $rr',t_1+t_1',\dots,t_n+t_n'$.

To see that a trapdoor opening is perfectly indistinguishable from a real opening, observe first that both in real commitments and in trapdoor openings we have Pedersen commitments $c_1,\dots,c_j$ where $c_j=h^{t_j}\prod_{i=1}^m\gamma_i^{m_{ij}}$ for random t_j. The perfect trapdoor property of our commitment schemes therefore gives us that the combined commitment scheme has identical probability distributions of real openings and trapdoor openings.

To see that the combined commitment scheme is binding, consider an adversary that produces two different openings of the same commitment. If the two openings lead to two different sets of Pedersen commitments $c_1,\dots,c_n$ then it is a breach of the binding property of $(\mathcal{G},K,\mathrm{com})$. If on the other hand both openings lead to the same Pedersen commitments $c_1,\dots,c_n$, then there must be at least one of the Pedersen commitments that has been opened in two different ways leading to a breach of the binding property of the Pedersen commitment scheme. Since the Pedersen commitment scheme is binding if the discrete logarithm assumption holds in G_2, we conclude that the discrete logarithm assumption in G_2 and the binding property of $(\mathcal{G},K,\mathrm{com})$ implies the binding property of the combined commitment scheme. □

Honest Verifier Zero-Knowledge Argument of Knowledge. While reducing the key size for homomorphic commitments is interesting in its own right, another concern that comes up in practice is that they have large openings that grow linearly in the number of committed values. We will now show that the combined commitment scheme has an efficient 3-move honest verifier zero-knowledge argument of knowledge, which in some applications means that we do not have to reveal the entire opening. This stands in contrast to the standard Pedersen commitment to multiple messages, where all known practical zero-knowledge arguments of knowledge have a size that grows linearly in the number of field elements we have committed to. It is possible to give similar types of efficient honest verifier zero-knowledge arguments for statements such as all the committed values being 0 or the committed values having a particular sum.

Let $\gamma_1, \ldots, \gamma_m, h$ be the commitment key for a Pedersen commitment to m exponents and let ck be a commitment key for one of our commitments scheme. The statement is a commitment $c \in \mathcal{C}_{ck}$ and the prover wants to give an argument of knowledge of the contents of c. The prover's private input consists of $r \in \mathcal{R}_{ck}$ and $m_{11}, \ldots, m_{mn} \in \mathbb{Z}_p$ so $c = \mathrm{com}_{ck}(c_1, \ldots, c_n; r)$, where $c_j = h^{t_j} \prod_{i=1}^m \gamma_i^{m_{ij}}$. The argument runs as follows.

1. The prover sends $c' = \mathrm{com}_{ck}(c'_1, \ldots, c'_n; r')$ and $c_d = h^t \prod_{i=1}^m \gamma_i^{d_i}$ to the verifier, where $r' \leftarrow \mathcal{R}_{ck}$ with $c_j = h^{t_j}$ for $t'_1, \ldots, t'_n \leftarrow \mathbb{Z}_p$ and $t, d_1, \ldots, d_m \leftarrow \mathbb{Z}_p$.

2. The verifier sends the prover random challenges $e, e_1, \ldots, e_n \leftarrow \mathbb{Z}_p$.

3. The prover answers with $r'' = r^e r', c''_1 = c_1^e c'_1, \ldots, c''_n = c_n^e c'_n$ and $t' = e \sum_{j=1}^n e_j t_j + \sum_{j=1}^n e_j t'_j + t, m_1 = d_1 + e \sum_{j=1}^n e_j m_{1j}, \ldots, m_m = d_m + e \sum_{j=1}^n e_j m_{mj}$.

4. The verifier accepts if $c^e c' = \mathrm{com}_{ck}(c''_1, \ldots, c''_n; r'')$ and $c_d \prod_{j=1}^n (c''_j)^{e_j} = h^{t'} \prod_{i=1}^m \gamma_i^{m_i}$.

The complexity of this argument is roughly n or $2n$ pairings (depending on the commitment scheme), $m + n$ exponentiations and mn multiplications for the prover, and n or $2n$ pairings (depending on the commitment scheme) and $n + m$ exponentiations for the verifier. The communication is roughly $2n + m$ group and field elements. In other words, it is in all aspects significantly shorter and faster than the process of committing, opening, and verifying the opening of the commitment. The following theorem shows that it is an honest verifier zero-knowledge argument of knowledge of the contents of the commitment c.

Theorem 16 *The protocol given above is a 3-move honest verifier zero-knowledge argument of knowledge of the contents of the commitment c.*

Proof. The protocol clearly has 3 moves and it can be verified directly that it has perfect completeness.

We will now show that the protocol has perfect special honest verifier zero-knowledge. By this we mean that given a challenge $e, e_1, \ldots, e_n$ it is possible to perfectly simulate the entire argument. The simulation works as follows, the simulator picks random commitments $c''_1, \ldots, c''_n$ and randomizer r'' and computes $c' = c^{-e}\mathrm{com}_{ck}(c''_1, \ldots, c''_n; r'')$. It also picks $m_1, \ldots, m_n$ and t' at random and computes $c_d = h^{t'} \prod_{i=1}^m \gamma_i^{m_i} \prod_{j=1}^n (c''_j)^{-e_j}$. The simulated argument is $(c_d, c', e, e_1, \ldots, e_n, r'', c''_1, \ldots, c''_n, t', m_1, \ldots, m_m)$.

To see this is a perfect simulation when the challenge is $e, e_1, \ldots, e_n$, observe that both in a real argument and in a simulated argument the values $r'', c''_1, \ldots, c''_n$ and $t', m_1, \ldots, m_m$ are uniformly random. Conditioned on these values, both c' and c_d can be determined uniquely. Real arguments and simulated arguments are therefore identically distributed.

Finally, we will show that the protocol is an argument of knowledge. Consider an adversary $\mathcal{A}$ that has probability of $\epsilon(k)$ of making an acceptable argument, we will show that there is an expected polynomial time black-box witness-extended emulator $\mathcal{B}$ that has success-probability $\epsilon(k) - \mathrm{negligible}(k)$ of answering a random challenge $e, e_1, \ldots, e_n$ and at the same time outputting an opening of the commitment.

$\mathcal{B}$ runs $\mathcal{A}$ using a random challenges $e, e_1, \dots, e_n$. If $\mathcal{A}$ fails to produce an acceptable argument, we are done. However, with probability $\epsilon(k)$ it does produce an accepting argument on the challenge, and $\mathcal{B}$ needs to extract an opening of the commitment. $\mathcal{B}$ rewinds $\mathcal{A}$ to the point where it has sent the initial message and selects new random challenges $e, e_1, \dots, e_n$ (it is possible, although unlikely, that the same challenge will repeat) until it has $2n+1$ acceptable arguments with the same initial message c_d, c'. Since $\mathcal{A}$ has probability $\epsilon(k)$ chance of making an accepting argument in the first place, and collecting $2n+1$ acceptable arguments will take an average of $\frac{2n+1}{\epsilon(k)}$ rewinds, we get that on average $\mathcal{B}$ uses $2n+1$ runs of $\mathcal{A}$.

Let us now look at accepting challenges collected by $\mathcal{B}$. Since $\mathcal{B}$ runs an expected $2n+1$ runs of $\mathcal{A}$, which is expected polynomial time, there is an overwhelming probability that two of the accepting arguments use different challenges. With two different challenges $e \neq \hat{e}$ we get two equations $c^e c' = \mathrm{com}_{ck}(c''_1, \dots, c''_n; r'')$ and $c^{\hat{e}} c' = \mathrm{com}_{ck}(\hat{c_1}'', \dots, \hat{c_n}''; \hat{r}'')$. From this we can compute an opening of c and then compute an opening of c'. By the binding property of the commitment scheme, these openings will be used by $\mathcal{A}$ in all the accepting arguments when answering the challenges.

Consider now the second part of the verification. All the accepting arguments satisfy

$$c_d \prod_{j=1}^{n} (c''_j)^{e_j} = c_d \prod_{j=1}^{n} (c_j^e c'_j)^{e_j} = c_d^1 \prod_{j=1}^{n} c_j^{ee_j} \prod_{j=1}^{n} (c'_j)^{e_j} = h^{t'} \prod_{i=1}^{m} \gamma_i^{m_i}.$$

With overwhelming probability the $2n+1$ challenge vectors $(1, ee_1, \dots, ee_n, e_1, \dots, e_n)$ are linearly independent. The $2n+1$ equations given by the accepting arguments then make it possible to extract openings of all the commitments $c_1, \dots, c_n$. We conclude that the probability is negligible for $\mathcal{A}$ making a valid argument, yet $\mathcal{B}$ not being able to extract an opening of c. □

References

[AHO10] Masayuki Abe, Kristiyan Haralambiev, and Miyako Ohkubo. Signing on elements in bilinear groups for modular protocol design. Cryptology ePrint Archive, Report 2010/133, 2010.

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

[BGN05] Dan Boneh, Eu-Jin Goh, and Kobbi Nissim. Evaluating 2-DNF formulas on ciphertexts. In *TCC*, volume 3378 of *Lecture Notes in Computer Science*, pages 325–341, 2005.

[Bra00] Stefan Brands. *Rethinking Public Key Infrastructures and Digital Certificates; Building in Privacy.* MIT Press, 2000.

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

[DF02] Ivan Damgård and Eiichiro Fujisaki. A statistically-hiding integer commitment scheme based on groups with hidden order. In *ASIACRYPT*, volume 2501 of *Lecture Notes in Computer Science*, pages 125–142, 2002.

[DN02] Ivan Damgård and Jesper Buus Nielsen. Perfect hiding and perfect binding universally composable commitment schemes with constant expansion factor. In *CRYPTO*, volume 2442 of *Lecture Notes in Computer Science*, pages 581–596, 2002. Full paper available at `http://www.brics.dk/RS/01/41/index.html`.

[ElG85] Taher ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, 31(4):469–472, 1985.

[FO97] Eiichiro Fujisaki and Tatsuaki Okamoto. Statistical zero knowledge protocols to prove modular polynomial relations. In *CRYPTO*, volume 1294 of *Lecture Notes in Computer Science*, pages 16–30, 1997.

[FS01] Jun Furukawa and Kazue Sako. An efficient scheme for proving a shuffle. In *CRYPTO*, volume 2139 of *Lecture Notes in Computer Science*, pages 368–387, 2001.

[GOS06] Jens Groth, Rafail Ostrovsky, and Amit Sahai. Non-interactive zaps and new techniques for NIZK. In *CRYPTO*, volume 4117 of *Lecture Notes in Computer Science*, pages 97–111, 2006.

[GPS08] Steven D. Galbraith, Kenneth G. Paterson, and Nigel P. Smart. Pairings for cryptographers. *Discrete Applied Mathematics*, 156(16):3113–3121, 2008.

[GQ88] Louis C. Guillou and Jean-Jacques Quisquater. A practical zero-knowledge protocol fitted to security microprocessor minimizing both trasmission and memory. In *EUROCRYPT*, volume 330 of *Lecture Notes in Computer Science*, pages 123–128, 1988.

[Gro06] Jens Groth. Simulation-sound NIZK proofs for a practical language and constant size group signatures. In *ASIACRYPT*, volume 4248 of *Lecture Notes in Computer Science*, pages 444–459, 2006. Full paper available at `http://www.brics.dk/~jg/NIZKGroupSignFull.pdf`.

[Gro09] Jens Groth. Linear algebra with sub-linear zero-knowledge arguments. In *CRYPTO*, volume 5677 of *Lecture Notes in Computer Science*, pages 192–208, 2009.

[GS08] Jens Groth and Amit Sahai. Efficient non-interactive proof systems for bilinear groups. In *EUROCRYPT*, volume 4965 of *Lecture Notes in Computer Science*, pages 415–432, 2008. Full paper available at `http://eprint.iacr.org/2007/155`.

[KZ06] Aggelos Kiayias and Hong-Sheng Zhou. Concurrent blind signatures without random oracles. In *SCN*, volume 4116 of *Lecture Notes in Computer Science*, pages 49–62, 2006.

[Lip03] Helger Lipmaa. On diophantine complexity and statistical zero-knowledge arguments. In *ASIACRYPT*, volume 2894 of *Lecture Notes in Computer Science*, pages 398–415, 2003.

[Nef01] C. Andrew Neff. A verifiable secret shuffle and its application to e-voting. In *ACM CCS*, pages 116–125, 2001.

[OU98] Tatsuaki Okamoto and Shigenori Uchiyama. A new public-key cryptosystem as secure as factoring. In *EUROCRYPT*, volume 1403 of *Lecture Notes in Computer Science*, pages 308–318, 1998.

[Pai99] Pascal Paillier. Public-key cryptosystems based on composite residuosity classes. In *EUROCRYPT*, volume 1592 of *Lecture Notes in Computer Science*, pages 223–239, 1999.

[Ped91] Torben P. Pedersen. Non-interactive and information-theoretic secure verifiable secret sharing. In *CRYPTO*, volume 576 of *Lecture Notes in Computer Science*, pages 129–140, 1991.