Non-interactive and Re-usable Universally Composable String Commitments with Adaptive Security

Marc Fischlin[1], Benoît Libert[2], and Mark Manulis[1]

[1] TU Darmstadt & CASED, Germany
[2] Université catholique de Louvain, ICTEAM Institute, Belgium

Abstract. We present the first provably secure constructions of universally composable (UC) commitments (in pairing-friendly groups) that simultaneously combine the key properties of being *non-interactive*, supporting commitments to *strings* (instead of bits only), and offering *re-usability of the common reference string* for multiple commitments. Our schemes are also *adaptively secure* assuming reliable erasures.

1 Introduction

UC-security. Cryptographic protocols being proven secure in the Universal Composability (UC) framework [6] bring several fundamental benefits compared to protocols for which only stand-alone proofs of security exist. A widely recognized advantage is that executions of UC-secure protocols remain secure in arbitrary, possibly malicious environments — essentially what one should expect from security protocols deployed in the real world. UC protocols do not receive much attention from practitioners, who in addition to security take many other factors into account such as efficiency and robustness, especially when it comes to protocols that require network communication. In this work we focus of universally composable commitment schemes [8] that are useful for various distributed applications.

UC commitments and their properties. In general commitment schemes are cryptographic protocols that proceed in two phases: In the *commit phase* the sender computes a commitment c to some message m and communicates c to the receiver; in the *open phase* the sender discloses the message m together with some proof d to provide assurance that m was indeed used in the commit phase. Typically, commitment schemes serve as building blocks in higher level applications, which is why striving for UC-security of these schemes is worthwhile. It is known that UC commitments imply key exchange and more general forms of secure two- and multi-party computation [9,12]. Unfortunately, security of commitment schemes under universal composition cannot be obtained without additional setup assumptions. A detailed explanation of the underlying simulation problem and work-around has been given in the seminal work by Canetti and Fischlin [8], who also showed that the UC-security of commitments

D.H. Lee and X. Wang (Eds.): ASIACRYPT 2011, LNCS 7073, pp. 468–485, 2011.

prevents their malleability, which is critical to many anticipated applications of these schemes. Since [8], one of the most basic and widely used setup assumptions is the Common Reference String (CRS) model, which is also used in our work. Note that alternative constructions of UC commitments appeal to stronger setup assumptions like random oracles [18] or hardware tokens [19]. In addition to setup assumptions prior work has identified several key properties, based on which UC commitment schemes are often compared. These properties (which we list below) may serve as "quality criteria" for UC commitments since they shed light on the security and potential practicality of the schemes.

Efficiency. Several factors contribute to the overall efficiency of a UC commitment scheme. In particular, its *communication complexity* measures the total amount of bits (often in dependency on the security parameter) that are transmitted between the sender and the receiver during the both phases of the protocol. These costs also include the actual *commitment length*, *i.e.*, number of bits that receiver would have to store until the open phase. The *computational complexity* of a commitment schemes indicates the total amount of work performed by participants and is often given in form of costly public-key operations (e.g. modular exponentiations). Earlier UC commitments, e.g. [8,9], were *bit commitments* and required ℓ executions of the basic protocol to commit to an ℓ-bit string. This results usually in a commitment length of $\Omega(\ell \cdot \lambda)$, whereas the length should ideally be $O(\lambda)$ only.[1] Modern UC schemes, such as [13,12,5,22,20], are more efficient in that they can be used to commit to ℓ-bit strings directly without incurring an expansion factor proportional to the security parameter. Another efficiency indicator of UC commitments in the CRS model is the *length of the CRS*, which should ideally remain independent of the number of possible users. Note that this latter property is satisfied by many UC schemes today, e.g. [12,5,22,20].

CRS re-usability. UC commitments in the CRS model assume trusted generation of the CRS parameters. Of practical relevance is the question of whether these parameters are re-usable across polynomially many executions of the commitment protocol or whether they need to be set up for each new commit phase. Clearly, re-usability of CRS parameters is desirable in practice, where setting up these parameters anew for each commitment operation may not always be possible. Note that CRS re-usability is provided by many existing UC schemes, e.g. [13,12,5,20], though the CRS length in [13] is not constant.

Interaction. Another important property of a UC commitment scheme is whether its phases require interaction between the sender and the receiver. Ideally, UC commitment should be *non-interactive*, meaning that each phase should

[1] Due to the so-called extraction property of UC commitments [8] a commitment needs to somewhat contain the entire message, stipulating that the commitment itself is at least as large as the message. Hence, demanding a length $O(\lambda)$ usually requires $\ell \leq \lambda$.

contain at most one message sent by the sender towards the silent receiver. Such property is, for example, inherent to many regular (non-UC) commitments, e.g. [26]. Interactivity may increase the communication complexity by several factors, since in addition to the actual commitment length the amount of bits communicated during the interactive phases would have to be counted as well. For example, the two most recent interactive commitments by Lindell [20] have commitment lengths of only 4 resp. 6 group elements, while their total communication complexity amounts to 14 resp. 19 group elements (we remark that for concrete choices of parameters [20] still remains very efficient in this respect).

The actual advantage of non-interactive UC commitments from the practical point of view is resistance to denial of service attacks: Within an interactive phase (commit or open) parties maintain a state between the communication rounds. It is thus possible for an adversary (malicious sender/receiver or man-in-the-middle), by sending incorrectly formed messages during the interaction rounds, to lure parties into wasting their (computational) resources — something which does not happen in the non-interactive case. Note that, even if no adversary is present, interaction between the sender and the receiver may still be endangered by faults. Earlier UC bit commitments [8,9] were non-interactive. However, in the more desirable case of UC string commitments, the only known non-interactive scheme is due to Nishimaki *et al.* [22]. However, [22] does not allow CRS re-usability, which arguably diminishes the advantage gained through its non-interactivity. Other existing UC string commitments, e.g. [13,12,5,20], are all interactive, either in the commit or in the open phase.

UC commitments that have acceptably low computation and communication costs, allow CRS re-usability, and do not require any interaction between the sender and the receiver would already be ideal from the practical point of view. In addition to these properties there are further desirable properties which should also be assessed concerning their impact on their relevance in practice.

Adaptive security. A typical question asked about UC-secure protocols is whether security is proven against static or adaptive adversaries. A *static* adversary can corrupt protocol participants at the outset of the protocol only. In case of UC commitments such corruptions would be allowed only prior to the execution of the commit phase, even before the CRS is generated. Since commitments always have two phases with the open phase being executed after the commit phase, it appears unrealistic to exclude corruptions between the two phases. Hence, *adaptive* UC-security, where the adversary can corrupt participants at any point in time, revealing all their secrets (including randomness being used), appears of higher practical relevance. We observe that some of known UC commitments are adaptively secure, e.g. [8,9,12,5,20].

Secure erasures. Another property inherent to the UC-security of commitment schemes is whether they rely on the additional assumption that secrets can be securely erased. This assumption is often used in combination with adaptive security where secrets used in the commit phase that are no longer needed for the open phase are erased to allow simulation in case of later corruptions. Al-

though secure erasures could be realized in practice, it is still desirable for a UC commitment scheme to avoid them. We observe that most adaptively secure UC commitments require secure erasures, the only exception (in addition to less efficient bit commitments from [8,9]) where adaptivity is achieved without erasures is the interactive string commitment by Damgård and Groth [12].

Hardness assumptions. Last but not least, in addition to an inevitable setup assumption (e.g. CRS) and possible reliance on secure erasures, UC-security of commitments is typically based on further hardness assumptions. These are either general assumptions such as existence of trapdoor permutations as in [8,9] or more concrete number-theoretic assumptions, which are more likely to give rise to efficient schemes. For example, UC commitments by Damgård and Nielsen [13] rely on p-subgroup [23] or Decision Composite Residuosity (DCR) assumption [25]. The DCR assumption has also been used in the UC commitments by Damgård and Groth [12] (together with Strong RSA (SRSA) assumption), by Camenisch and Shoup [5], and by Nishimaki *et al.* [22]. The recent UC commitments by Lindell [20] rely on the more established Decision Diffie-Hellman (DDH) assumption, which has also been used in one of the bit commitment schemes by Canetti and Fischlin [8] and in a particular instantiation of Nishimaki *et al.*'s scheme [22] with El-Gamal based matrix encryption of Peikert and Waters [27] (those communication complexity is asymptotically comparable to that of a bit commitment scheme though).

The current state of affairs is that *none* of the existing CRS-based UC-secure string commitment schemes fulfills all of the above mentioned "quality criteria".

1.1 Our Results and Comparison to Prior Work

Results. We propose the first UC-secure string commitment schemes in the (standard) CRS model with the so far unique combination of key properties: Our schemes have constant costs (*i.e.*, independent of the message length and the number of participants) for communication, computation, and CRS length. They offer re-usability of the CRS for polynomially many executions. Both schemes are completely non-interactive (*i.e.*, the commitment and opening phases both consist of a single message from the sender to the receiver). We prove their UC-security under adaptive corruptions (with erasures) using the well-known Decision Linear (DLIN) assumption [3]. As demonstrated in Table 1, such UC string commitments were not known to exist before. In particular, their ability to commit to strings with re-usable CRS in combination with non-interactivity and adaptive security seems so far unique.[2]

Our schemes are also the first UC-secure commitments designed for pairing-friendly groups. The main ingredients of our schemes are Groth-Sahai proofs [16]

[2] Zhu [30] claims to have a non-interactive, UC-secure string commitment without erasures for re-usable common reference strings; we were unable to verify the proof of the scheme, though. In fact, the encryption-based scheme does not seem to satisfy the usual equivocality property of such commitments.

Table 1. Comparison of UC commitment schemes in the CRS model

UC commitment schemes		comm. complexity in sec.par.(bits)	CRS re-usable	non-inter. phases	without erasures	adaptive security	hardness assumptions
CF01 (1)	[8]	$O(\ell \cdot \lambda)$	—	✓	✓	✓	TDP
CF01 (2)	[8]	$O(\ell \cdot \lambda)$	✓	✓	—	✓	CFP + CCA PKE
CF01 (3)	[8]	$O(\ell \cdot \lambda)$	✓	✓	✓	✓	DDH + UOWHF
CLOS02	[9]	$O(\ell \cdot \lambda)$	✓	✓	✓	✓	TDP
DN02 (1)	[13]	$18 \cdot \lambda$ (13824)	✓	—	✓	✓	p-subgroup
DN02 (2)	[13]	$24 \cdot \lambda$ (18432)	✓	—	✓	✓	DCR
DG03	[12]	$16 \cdot \lambda$ (12288)	✓	—	✓	✓	DCR + SRSA
CS03	[5]	$94 \cdot \lambda$ (72192)	✓	—	—	✓	DCR + CRHF
NFT09	[22]	$21 \cdot \lambda$ (16128)	—	✓	—	✓	DCR + sEUF-OT
NFT09	[22]	$O(\ell \cdot \lambda)$	—	✓	—	✓	DDH + sEUF-OT
Lin11 (1)	[20]	$14 \cdot \lambda$ (3584)	✓	—	✓	—	DDH + CRHF
Lin11 (2)	[20]	$19 \cdot \lambda$ (4864)	✓	—	—	✓	DDH + CRHF
Scheme I		$21 \cdot \lambda$ (5376)	✓	✓	—	✓	DLIN + CRHF
Scheme II		$40 \cdot \lambda$ (10240)	✓	✓	—	✓	DLIN + CRHF

Complexity costs: ℓ - length of committed messages, λ - security parameter, (bits) - total number of communicated bits (based on λ)
In DN02, DG03, CS03, and DCR-based NFT09, λ is the length of the prime factor of N (RSA modulus). We use $\lambda = 768$ bits.
In Lin11 λ is the length of the prime group order. We use $\lambda = 256$ bits.
In our schemes λ is the length of the prime group order of the input group. We use $\lambda = 256$ bits (cf. [24] for parameter choice).
Hardness assumptions: TDP - trapdoor permutations, CFP - claw-free permutations, UOWHF - universal one-way hash functions, CRHF - collision-resistant hash functions, DDH - Decision Diffie-Hellman, DCR - Decision Composite Residuosity, SRSA - Strong RSA, sEUF-OT - strongly unforgeable one-times signature, DLIN - Decision Linear.

and Cramer-Shoup encryption (under DLIN assumption [3]). Although pairing operations are traditionally costlier in comparison to modular exponentiations in the RSA or Discrete Logarithm settings, constant costs incurred by our schemes seem still to be sufficient for practical purposes. As demonstrated in Table 1, the total communication costs of our schemes, when instantiated with appropriate security parameters, are lower than in all previous DCR-based constructions. For our first scheme, the costs are only slightly higher than for the recent (interactive) UC commitments by Lindell [20]. The entire communication complexity amounts to 21 group elements for our first scheme and 40 elements for our second scheme. Yet our schemes have opposite trade-offs regarding the two phases: Our first scheme outputs commitments containing only 5 group elements and transmits 16 elements in the open phase. In contrast, our second scheme requires 37 group elements to commit and only 3 elements to open.

Techniques. Our first scheme is inspired by the UC commitment scheme of Lindell [20], where the committer encrypts the message in the commit phase using the DDH-based Cramer-Shoup encryption scheme, and in the open phase, simply reveals the committed message and gives an interactive Sigma proof that the message is indeed the one encrypted in the ciphertext. Using non-interactive Groth-Sahai proofs we show that this interaction can be safely removed while

preserving UC security and without losing much of the efficiency. We thus use the DLIN assumption instead of DDH. Observe that DLIN assumption is often referred to as a natural counterpart of the DDH assumption in bilinear groups where the latter does not hold. More surprisingly, when transforming Lindell's scheme, we also obtain security against adaptive corruptions essentially for free. That is, the basic scheme in [20] — which is the starting point for our first construction — is only secure against static corruptions. Lindell then provides additional means to derive a variant which withstands adaptive corruptions. In [20], there is no way to prove the basic scheme adaptively secure (even with reliable erasures) because the committer needs to store the randomness used to encrypt in order to give the interactive zero-knowledge proof in the opening phase, and thus cannot erase it after having committed. Having to present this randomness in case of adaptive corruption, however, inhibits the necessary equivocality property of commitments [8], the ability to adapt simulated commitments appropriately. In our case, the committer can compute the *non-interactive* proof already in the commitment phase and present it together with the message in the decommitment phase. By this, the committer only needs to store the proof and can erase any randomness from the commitment phase, buying us security against adaptive corruptions (with erasures).

At this point, we notice that Groth-Sahai proofs are widely used in many cryptographic constructions for reducing the amount of interaction. Interestingly, their applicability to the setting of UC commitments was not explored so far. We thus show that their techniques are powerful enough to allow construction of UC commitments with, up till now, unique properties. We demonstrate this not only with our first scheme, based on the Lindell's commitments (while using the DLIN assumption instead of DDH), but also with our second scheme, which builds upon Camenisch-Shoup commitments [5] with the difference that we work in a discrete logarithm setting instead of relying on the composite residuosity assumption as in [5].

We obtain our second scheme using pairing-based trapdoor commitments to group elements [10,15] in combination with Groth-Sahai proofs and DLIN-based Cramer-Shoup encryption. This scheme can be viewed as the UC secure non-interactive (pairing-based) version of the scheme from [5] with the following tweak: We use trapdoor commitments to group elements prior to the encryption scheme. Unlike [5], where a Pedersen commitment [26] to message M with randomness r is computed and followed by a verifiable encryption of (M, r), we trapdoor-commit to M (viewed as group element) and then encrypt only M. Yet, we can still extract an opening of the trapdoor commitment when the need arises in the security proof (due to the properties of Groth-Sahai commitments). The resulting scheme is somewhat more efficient in communication than if the full opening of the trapdoor commitment is encrypted as in the original construction [5]. We also notice that description of the UC commitment scheme in [5] was limited to the presentation of main ideas but a concrete specification and the eventual analysis of security were left open. With our pairing-based construction and the above mentioned tweak, we not only remove interaction in this scheme

and significantly improve its communication complexity but essentially develop the initial ideas from [5] to a full-fledged specification and the corresponding proof of security.

Organization. We recall the basic building blocks that we need in Section 2. Section 3 then presents our non-interactive (adaptively) UC-secure string commitment scheme with re-usable CRS together with the detailed proof of security.

2 Preliminaries

2.1 Complexity Assumptions

In the paper, we use groups $(\mathbb{G}, \mathbb{G}_T)$ of prime order p with a generator $g \in \mathbb{G}$ and endowed with a mapping $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ such that $e(g^a, g^b) = e(g, g)^{ab}$ for all $a, b \in \mathbb{Z}_p$ and $e(g, h) \neq 1_{\mathbb{G}_T}$ whenever $g, h \neq 1_{\mathbb{G}}$. We occasionally consider the Cartesian product of groups as vector spaces where component-wise multiplication $(A, B, C) \cdot (X, Y, Z) = (AX, BY, CZ)$ is the vector addition and component-wise exponentiation $(A, B, C)^x = (A^x, B^x, C^x)$ is the scalar multiplication. In these groups, we rely on the following assumption.

Definition 1 ([3]). *The* **Decision Linear Problem** *(DLIN) in* $\mathbb{G}$ *consists in distinguishing the distribution* $D_1 = \{(g, g^a, g^b, g^{ac}, g^{bd}, g^{c+d}) | a, b, c, d \xleftarrow{R} \mathbb{Z}_p^*\}$ *from the distribution* $D_2 = \{(g, g^a, g^b, g^{ac}, g^{bd}, g^z) | a, b, c, d, z \xleftarrow{R} \mathbb{Z}_p^*\}$.

2.2 Groth-Sahai Proof Systems

In the following notations, for equal-dimension vectors $\boldsymbol{A}$ and $\boldsymbol{B}$ containing group elements, $\boldsymbol{A} \cdot \boldsymbol{B}$ stands for their component-wise product.

When based on the DLIN assumption, the Groth-Sahai (GS) proof systems [16] use a common reference string comprising vectors $\boldsymbol{g_1}, \boldsymbol{g_2}, \boldsymbol{g_3} \in \mathbb{G}^3$, where $\boldsymbol{g_1} = (g_1, 1, g)$, $\boldsymbol{g_2} = (1, g_2, g)$ for some $g_1, g_2 \in \mathbb{G}$. To commit to $X \in \mathbb{G}$, one sets $\boldsymbol{C} = (1, 1, X) \cdot \boldsymbol{g_1}^r \cdot \boldsymbol{g_2}^s \cdot \boldsymbol{g_3}^t$ with $r, s, t \xleftarrow{R} \mathbb{Z}_p^*$. When proofs should be perfectly sound, $\boldsymbol{g_3}$ is set as $\boldsymbol{g_3} = \boldsymbol{g_1}^{\xi_1} \cdot \boldsymbol{g_2}^{\xi_2}$ with $\xi_1, \xi_2 \xleftarrow{R} \mathbb{Z}_p^*$. Commitments $\boldsymbol{C} = (g_1^{r+\xi_1 t}, g_2^{s+\xi_2 t}, X \cdot g^{r+s+t(\xi_1+\xi_2)})$ are then Boneh-Boyen-Shacham (BBS) ciphertexts [3] that can be decrypted using $\alpha_1 = \log_g(g_1)$, $\alpha_2 = \log_g(g_2)$. In the witness indistinguishability (WI) setting, vectors $\boldsymbol{g_1}, \boldsymbol{g_2}, \boldsymbol{g_3}$ are linearly independent and $\boldsymbol{C}$ is a perfectly hiding commitment. Under the DLIN assumption, the two kinds of CRS are indistinguishable.

To commit to an exponent $x \in \mathbb{Z}_p$, one computes $\boldsymbol{C} = \boldsymbol{\varphi}^x \cdot \boldsymbol{g_1}^r \cdot \boldsymbol{g_2}^s$, with $r, s \xleftarrow{R} \mathbb{Z}_p^*$, using a CRS comprising vectors $\boldsymbol{\varphi}, \boldsymbol{g_1}, \boldsymbol{g_2}$. In the soundness setting $\boldsymbol{\varphi}, \boldsymbol{g_1}, \boldsymbol{g_2}$ are linearly independent vectors (typically, one chooses $\boldsymbol{\varphi} = \boldsymbol{g_3} \cdot (1, 1, g)$ where $\boldsymbol{g_3} = \boldsymbol{g_1}^{\xi_1} \cdot \boldsymbol{g_2}^{\xi_2}$) whereas, in the WI setting, choosing $\boldsymbol{\varphi} = \boldsymbol{g_1}^{\xi_1} \cdot \boldsymbol{g_2}^{\xi_2}$ gives a perfectly hiding commitment since $\boldsymbol{C}$ is always a BBS encryption of $1_{\mathbb{G}}$. On a perfectly sound CRS (where $\boldsymbol{g_3} = \boldsymbol{g_1}^{\xi_1} \cdot \boldsymbol{g_2}^{\xi_2}$ and $\boldsymbol{\varphi} = \boldsymbol{g_3} \cdot (1, 1, g)$), commitments to exponents are not fully extractable since the trapdoor (α_1, α_2) only allows recovering g^x from $\boldsymbol{C} = \boldsymbol{\varphi}^x \cdot \boldsymbol{g_1}^r \cdot \boldsymbol{g_2}^s$. To prove that committed variables satisfy a

set of relations, the Groth-Sahai techniques require one commitment per variable and one proof element (made of a constant number of group elements) per relation. Such proofs are available for pairing-product relations, which are of the type

$$\prod_{i=1}^{n} e(\mathcal{A}_i, \mathcal{X}_i) \cdot \prod_{i=1}^{n} \cdot \prod_{j=1}^{n} e(\mathcal{X}_i, \mathcal{X}_j)^{a_{ij}} = t_T, \tag{1}$$

for variables $\mathcal{X}_1, \ldots, \mathcal{X}_n \in \mathbb{G}$ and constants $t_T \in \mathbb{G}_T$, $\mathcal{A}_1, \ldots, \mathcal{A}_n \in \mathbb{G}$, $a_{ij} \in \mathbb{G}$, for $i, j \in \{1, \ldots, n\}$. Efficient proofs also exist for multi-exponentiation equations

$$\prod_{i=1}^{m} \mathcal{A}_i^{y_i} \cdot \prod_{j=1}^{n} \mathcal{X}_j^{b_j} \cdot \prod_{i=1}^{m} \cdot \prod_{j=1}^{n} \mathcal{X}_j^{y_i \gamma_{ij}} = T, \tag{2}$$

for variables $\mathcal{X}_1, \ldots, \mathcal{X}_n \in \mathbb{G}$, $y_1, \ldots, y_m \in \mathbb{Z}_p$ and constants $T, \mathcal{A}_1, \ldots, \mathcal{A}_m \in \mathbb{G}$, $b_1, \ldots, b_n \in \mathbb{Z}_p$ and $\gamma_{ij} \in \mathbb{G}$, for $i \in \{1, \ldots, m\}, j \in \{1, \ldots, n\}$.

Multi-exponentiation equations admit zero-knowledge proofs at no additional cost. On a simulated CRS (prepared for the WI setting), the trapdoor (ξ_1, ξ_2) makes it possible to simulate proofs without knowing witnesses, and simulated proofs are perfectly indistinguishable from real proofs. As for pairing-product equations, NIZK proofs are often possible (this is typically the case when the target element t_T has a special form) but usually come at some expense.

In both cases, proofs for quadratic equations (namely, when at least one of the coefficients a_{ij} and γ_{ij} is non-zero in (1) and (2), respectively) cost 9 group elements. Linear pairing-product equations (when $a_{ij} = 0$ for all i, j in (1)) take 3 group elements each. Linear multi-exponentiation equations of the type $\prod_{j=1}^{n} \mathcal{X}_j^{b_j} = T$ (resp. $\prod_{i=1}^{m} \mathcal{A}_i^{y_i} = T$) demand 3 (resp. 2) group elements.

2.3 Cramer-Shoup Encryption Based on DLIN Assumption

This section recalls a variant of the Cramer-Shoup encryption scheme [11] based on the DLIN assumption and suggested in [28,17]. The scheme offers IND-CCA2 security for encryption schemes with labels [29]. If we assume public generators g_1, g_2, g that are parts of public parameters (*i.e.*, a common reference string), the receiver's public key is made of

$$\begin{array}{lll} X_1 = g_1^{x_1} g^{x} & X_3 = g_1^{x_3} g^{y} & X_5 = g_1^{x_5} g^{z} \\ X_2 = g_2^{x_2} g^{x} & X_4 = g_2^{x_4} g^{y} & X_6 = g_2^{x_6} g^{z}. \end{array}$$

To encrypt $m \in \mathbb{G}$ under the label L, the sender picks $r, s \xleftarrow{R} \mathbb{Z}_p^*$ and computes

$$\psi_{\mathsf{CS}} = \big(U_1, U_2, U_3, U_4, U_5\big) = \Big(g_1^r,\ g_2^s,\ g^{r+s},\ m \cdot X_5^r X_6^s,\ (X_1 X_3^{\alpha})^r \cdot (X_2 X_4^{\alpha})^s\Big),$$

Functionality $\mathcal{F}_{\text{MCOM}}$

$\mathcal{F}_{\text{MCOM}}$ is parameterized by a message space $\mathcal{M}$ interacts with parties $P_1, \ldots, P_n$ and adversary $\mathcal{S}$ as follows.

- Upon receiving $(\texttt{commit}, sid, cid, P_i, P_j, M)$ from P_i, where $M \in \mathcal{M}$, record (sid, cid, P_i, P_j, M) and send a publicly delayed $(\texttt{receipt}, sid, cid, P_i, P_j)$ to P_j. Ignore any subsequent $(\texttt{commit}, sid, cid, P_i, P_j, *)$ messages.
- Upon receiving $(\texttt{open}, sid, cid, P_i, P_j)$ from P_i, if some tuple (cid, P_i, P_j, M) was previously recorded then send a publicly delayed $(\texttt{open}, sid, cid, P_i, P_j, M)$ to P_j. Otherwise halt.
- Upon receiving $(\texttt{corrupt-committer}, sid, cid)$ from the adversary, check if there is already an entry (sid, cid, P_i, P_j, M) and, if so, send M to the adversary. If the adversary provides some M' and $(\texttt{receipt}, sid, cid, P_i, P_j)$ has not yet been written on P_j's output tape, then change the record to (sid, cid, P_i, P_j, M').

Fig. 1. Functionality $\mathcal{F}_{\text{MCOM}}$ for Multiple Commitments

where $\alpha = H(U_1, U_2, U_3, U_4, L) \in \mathbb{Z}_p$ is a collision-resistant[3] hash function. Given a pair (ψ_{CS}, L), the receiver computes α. If $U_5 \neq U_1^{x_1+\alpha x_3} U_2^{x_2+\alpha x_4} U_3^{x+\alpha y}$ then the receiver outputs $\perp$; otherwise he outputs $m = U_4/(U_1^{x_5} U_2^{x_6} U_3^{z})$.

2.4 Ideal Functionality for Multiple Commitments

The ideal commitment functionality $\mathcal{F}_{\text{MCOM}}$ described in Figure 1 is the one defined by Canetti and Fischlin [8] but, as in [18], we consider publicly delayed messages, where the message is delivered to the corresponding party only upon confirmation by the adversary (who sees the message first). Note that the functionality now takes another unique "commitment identifier" *cid*, which may be used if a sender commits to the same receiver multiple times within a session. We assume that the combination of *sid*, *cid* is globally unique.

3 Scheme I: A Tweak on Lindell's Scheme

Our first construction builds on Lindell's first interactive UC-secure commitment scheme from [5], which is only known to be secure against static corruptions in its original variant. We show how to utilize Groth-Sahai proofs so as to completely remove interaction, while still guaranteeing UC security (in the adaptive sense) and preserving all other valuable properties of the scheme.

[3] The security proofs of the original Cramer-Shoup encryption scheme [11] and its variants based on the DLIN assumption [17,28] only require a universal one-way hash function [21]. As mentioned in [4], for example, collision-resistance is needed when the scheme is extended so as to support labels.

CRS-Gen(λ)**:** choose bilinear groups $(\mathbb{G}, \mathbb{G}_T)$ of order $p > 2^\lambda$, $g \xleftarrow{R} \mathbb{G}$ and $g_1 = g^{\alpha_1}$, $g_2 = g^{\alpha_2}$, with $\alpha_1, \alpha_2 \xleftarrow{R} \mathbb{Z}_p^*$. Define vectors $\boldsymbol{g_1} = (g_1, 1, g)$, $\boldsymbol{g_2} = (1, g_2, g)$ and $\boldsymbol{g_3} = \boldsymbol{g_1}^{\xi_1} \cdot \boldsymbol{g_2}^{\xi_2}$ with $\xi_1, \xi_2 \xleftarrow{R} \mathbb{Z}_p^*$, which form a Groth-Sahai CRS $\mathbf{g} = (\boldsymbol{g_1}, \boldsymbol{g_2}, \boldsymbol{g_3})$ for the perfect soundness setting. Then, choose a collision-resistant hash function $H : \{0,1\}^* \to \mathbb{Z}_p$ and generate a public key $\mathsf{pk} = (X_1, \ldots, X_6)$ for the linear Cramer-Shoup encryption scheme. The CRS consists of $\mathsf{crs} = \{\lambda, \mathbb{G}, \mathbb{G}_T, g, \mathbf{g}, H, \mathsf{pk}\}$.

Commit$(\mathsf{crs}, M, sid, cid, P_i, P_j)$**:** to commit to message $M \in \mathbb{G}$ for party P_j upon receiving a command $(\mathtt{commit}, sid, cid, P_i, P_j, M)$, party P_i parses crs as $\{\lambda, \mathbb{G}, \mathbb{G}_T, g, \mathbf{g}, \mathbf{f}, \mathsf{pk}\}$, respectively, first fetches crs from $\mathcal{F}_{\mathrm{CRS}}$ if not done already, and then conducts the following steps.

1. Choose random exponents $r, s \xleftarrow{R} \mathbb{Z}_p$ and compute a Cramer-Shoup encryption $\psi_{\mathsf{CS}} = (U_1, U_2, U_3, U_4, U_5)$ of $M \in \mathbb{G}$ under the label $L = P_i||sid||cid$ and the public key $\mathsf{pk} \in \mathbb{G}^6$ as in Section 2.3.
2. Generate a NIZK proof $\pi_{val\text{-}enc}$ that $\psi_{\mathsf{CS}} = (U_1, U_2, U_3, U_4, U_5)$ is a valid encryption of $M \in \mathbb{G}$. This requires to commit to exponents r, s and prove that these exponents satisfy the multi-exponentiation equations

$$\begin{aligned} U_1 &= g_1^r, & U_2 &= g_2^s, & U_3 &= g^{r+s}, \\ U_4/M &= X_5^r X_6^s, & U_5 &= (X_1 X_3^\alpha)^r \cdot (X_2 X_4^\alpha)^s \end{aligned} \tag{3}$$

   (which only takes 5 times 2 elements as base elements are all public). Including commitments com_r and com_s to exponents r and s, the proof $\pi_{val\text{-}enc}$ demands 16 group elements overall.
3. P_i erases (r, s) after the generation of $\pi_{val\text{-}enc}$ but retains the state information $D_M = \pi_{val\text{-}enc}$.

The commitment $\sigma = \psi_{\mathsf{CS}}$ comprises 5 group elements. Upon receiving $(\mathtt{Com}, sid, cid, \sigma)$ from P_i, party P_j verifies that $\sigma = \psi_{\mathsf{CS}}$ can be parsed as an element of $\mathbb{G}^5$. If yes, P_j outputs $(\mathtt{receipt}, sid, cid, P_i, P_j)$. Otherwise, P_j ignores the message.

Open$\big(\mathsf{crs}, M, D_M, sid, cid, P_i, P_j\big)$**:** when receiving a command $(\mathtt{open}, sid, cid, P_i, P_j, M)$, party P_i reveals M and his state information $D_M = \pi_{val\text{-}enc}$ to P_j.

Verify$\big(\mathsf{crs}, (\mathtt{Com}, sid, cid, \sigma), M, D_M, sid, cid, P_i, P_j\big)$**:** P_j verifies the proof $\pi_{val\text{-}enc}$ and ignores the opening if verification fails. If both proofs verify, P_j outputs $(\mathtt{open}, sid, cid, P_i, P_j, M)$ iff cid has not been used with this committer previously. Otherwise, P_j also ignores the message.

Theorem 1. *The above commitment scheme securely realizes* $\mathcal{F}_{\mathrm{MCOM}}$ *in the* CRS *model against adaptive corruptions (assuming reliable erasure), provided that (i) the DLIN assumption holds in* $\mathbb{G}$*; (ii)* H *is collision-resistant.*

Proof. We construct an ideal-world adversary $\mathcal{S}$ that runs a black-box simulation of the real-world adversary $\mathcal{A}$ by simulating the protocol execution and relaying messages between $\mathcal{A}$ and the environment $\mathcal{Z}$. The ideal-world adversary $\mathcal{S}$ proceeds as follows in experiment IDEAL.

1. $\mathcal{S}$ sets up crs by choosing $\mathbf{g} = (\boldsymbol{g_1}, \boldsymbol{g_2}, \boldsymbol{g_3})$ as a Groth-Sahai CRS for the perfect WI setting (namely, $\boldsymbol{g_3} = \boldsymbol{g_1}^{\xi_1} \cdot \boldsymbol{g_2}^{\xi_2} \cdot (1, 1, g)^{-1}$ for some $\xi_1, \xi_2 \xleftarrow{R} \mathbb{Z}_p^*$). Also, $\mathcal{S}$ generates a public key $\mathsf{pk} = (X_1, \ldots, X_6)$ as specified by the linear Cramer-Shoup encryption scheme.
2. When the environment $\mathcal{Z}$ requires some uncorrupted party P_i to commit to a message and send $(\mathtt{Commit}, sid, cid, P_i, P_j, M)$ to the functionality, the simulator $\mathcal{S}$ is notified that a commitment operation took place but does not know the committed message M. Therefore, $\mathcal{S}$ chooses a fake random message $R \xleftarrow{R} \mathbb{G}$ and computes a linear Cramer-Shoup encryption ψ_{CS} of $R \in \mathbb{G}$ using random exponents $r, s \xleftarrow{R} \mathbb{Z}_p$. The adversary $\mathcal{A}$ is then given $(\mathtt{Com}, sid, cid, \sigma)$ with $\sigma = \psi_{\mathsf{CS}}$ and, when $\tilde{P}_j$ eventually obtains $(\mathtt{Com}, sid, cid, \sigma)$ and outputs $(\mathtt{Receipt}, sid, cid, P_i, P_j)$, the simulator $\mathcal{S}$ allows $\mathcal{F}_{\mathrm{MCOM}}$ to proceed with the delivery of message $(\mathtt{Commit}, sid, cid, P_i, P_j)$ to P_j.
3. If $\mathcal{Z}$ requires some uncorrupted party P_i to open a previously generated commitment $\sigma = \psi_{\mathsf{CS}}$ to some message $M \in \mathbb{G}$, $\mathcal{S}$ learns M from $\mathcal{F}_{\mathrm{MCOM}}$ and, using the trapdoor $\xi_1, \xi_2 \in (\mathbb{Z}_p)^2$ of the simulated Groth-Sahai CRS, generates a simulated proof $\pi_{val\text{-}enc}$ that equations (3) are satisfied for the message M obtained from $\mathcal{F}_{\mathrm{MCOM}}$. The internal state of $\tilde{P}_i$ is modified to be $D_M = \pi_{val\text{-}enc}$, which is also given to $\mathcal{A}$ as the real-world de-commitment. Before allowing $\mathcal{F}_{\mathrm{MCOM}}$ to deliver the message $(\mathtt{Open}, sid, cid, P_i, P_j, M)$ to P_j, algorithm $\mathcal{S}$ waits for $\tilde{P}_j$ to acknowledge the opening in the simulation.
4. When the simulated adversary $\mathcal{A}$ delivers a commitment $(\mathtt{Com}, sid^*, cid^*, \sigma^*)$ for party $\tilde{P}_i$ to party $\tilde{P}_j$ and the latter still has not received a commitment with subsession ID cid^* from $\tilde{P}_i$, $\mathcal{S}$ proceeds as follows. If $\tilde{P}_i$ (and thus P_i as well) is uncorrupted, $\mathcal{S}$ notifies $\mathcal{F}_{\mathrm{MCOM}}$ that the commitment (sid^*, cid^*) can be delivered. The $\mathtt{Receipt}$ message returned by $\mathcal{F}_{\mathrm{MCOM}}$ is delivered to the dummy P_j as soon as the simulated $\tilde{P}_j$ outputs his own $\mathtt{Receipt}$ message. If $\tilde{P}_i$ is a corrupted party, then σ^* has to be extracted. Namely, $\mathcal{S}$ parses σ^* as ψ^*_{CS}. If $\psi^*_{\mathsf{CS}} \notin \mathbb{G}^5$, $\mathcal{S}$ simply ignores the commitment. Otherwise, it uses the private key sk corresponding to pk to decrypt ψ^*_{CS}. If ψ^*_{CS} turns out to be an invalid Cramer-Shoup ciphertext, the commitment is ignored. Otherwise, $\mathcal{S}$ obtains the plaintext $M \in \mathbb{G}$ and sends $(\mathtt{Commit}, sid^*, cid^*, P_i, P_j, M)$ to $\mathcal{F}_{\mathrm{MCOM}}$, which causes $\mathcal{F}_{\mathrm{MCOM}}$ to prepare a $\mathtt{Receipt}$ message for P_j. The latter is delivered by $\mathcal{S}$ as soon as $\tilde{P}_j$ produces his own output.
5. If $\mathcal{A}$ gets a simulated corrupted party $\tilde{P}_i$ to correctly open a commitment $(\mathtt{Com}, sid^*, cid^*, \sigma^*)$ to message M^*, the ideal-world adversary $\mathcal{S}$ compares M^* to the message M that was previously extracted from σ^* and aborts if $M \neq M^*$. Otherwise, $\mathcal{S}$ sends $(\mathtt{Open}, sid, cid, P_i, P_j, M)$ on behalf of P_i to $\mathcal{F}_{\mathrm{MCOM}}$. If $\mathcal{A}$ provides an incorrect opening, $\mathcal{S}$ simply ignores this opening.
6. If the simulated $\mathcal{A}$ decides to corrupt some party $\tilde{P}_i$, $\mathcal{S}$ corrupts the corresponding party P_i in the ideal world and obtains all his internal information. It also modifies all de-commitment information about the unopened commitments generated by $\tilde{P}_i$ so as to make it match the received de-commitment information of P_i. (Note that P_i is supposed to reliably delete the exponents

and to store only the group elements for decommitments.) This modified internal information is given to $\mathcal{A}$. For each commitment intended for P_j but for which P_j did not receive $(\texttt{Commit}, sid, cid, P_i, P_j)$, the newly corrupted $\tilde{P}_i$ is allowed to decide what the committed message will eventually be. A new message $M \in \mathbb{G}$ is thus supplied by $\mathcal{A}$ and $\mathcal{S}$ informs $\mathcal{F}_{\text{MCOM}}$ that M supersedes the message chosen by P_i before his corruption.

To show that the output of the environment $\mathcal{Z}$ in the ideal world is indistinguishable from its output in the real world, we consider several hybrid experiments involving hybrid adversaries $\mathcal{S}_i$.

$\mathsf{HYB}^1_{\mathcal{S}_1,\mathcal{Z}}$: is identical to the real experiment with two differences. The first one is that the simulator $\mathcal{S}_1$ generates the CRS by choosing $\mathbf{g} = (\boldsymbol{g_1}, \boldsymbol{g_2}, \boldsymbol{g_3})$ for the WI setting (namely, $\boldsymbol{g_3}$ is chosen as $\boldsymbol{g_3} = \boldsymbol{g_1}^{\xi_1} \cdot \boldsymbol{g_2}^{\xi_2} \cdot (1, 1, g)^{-1}$) instead of the perfect soundness setting. The other difference is that honest parties generate commitments by computing ψ_{CS} as an encryption of a random group element $R \in \mathbb{G}$ instead of the real message M. The NIZK proof $\pi_{val\text{-}enc}$ is then simulated using the trapdoor (ξ_1, ξ_2) of the Groth-Sahai CRS $(\boldsymbol{g_1}, \boldsymbol{g_2}, \boldsymbol{g_3})$. Experiment $\mathsf{HYB}^1_{\mathcal{S}_1,\mathcal{Z}}$ proceeds almost identically to the ideal-world experiment: the only difference is that $\mathcal{S}_1$ does not extract messages that corrupted parties commit to and never has to abort.

We first observe that the output of the environment $\mathcal{Z}$ in $\mathsf{HYB}^1_{\mathcal{S}_1,\mathcal{Z}}$ is negligibly close to its output in the real experiment REAL if the linear Cramer-Shoup encryption scheme is IND-CPA and if the two types of Groth-Sahai reference strings are indistinguishable.

Claim. If the DLIN assumption holds in $\mathbb{G}$, the output of $\mathcal{Z}$ in REAL is negligibly different from its output in $\mathsf{HYB}^1_{\mathcal{S}_1,\mathcal{Z}}$.

Proof. The proof proceeds using two intermediate hybrid experiments HYB_0 and HYB'_0 between REAL and $\mathsf{HYB}^1_{\mathcal{S}_1,\mathcal{Z}}$. In HYB_0, the perfectly sound CRS $\mathbf{g} = (\boldsymbol{g_1}, \boldsymbol{g_2}, \boldsymbol{g_3})$, where $\boldsymbol{g}_3 = \boldsymbol{g_1}^{\xi_1} \cdot \boldsymbol{g_2}^{\xi_2}$, is replaced by a fake CRS, where $\boldsymbol{g}_3 = \boldsymbol{g_1}^{\xi_1} \cdot \boldsymbol{g_2}^{\xi_2} \cdot (1, 1, g)^{-1}$. It is clear that, under the DLIN assumption, this modification cannot affect $\mathcal{Z}$'s view.

Then, HYB'_0 is like HYB_0 with the difference that NIZK proofs $\pi_{val\text{-}enc}$ (which are generated when $\mathcal{S}_1$ has to open honestly generated commitments) are simulated using the trapdoor (ξ_1, ξ_2). Observe that proofs $\pi_{val\text{-}enc}$ are simulated proofs for true statements in HYB'_0. Since these proofs have the same distribution as real proofs on a fake CRS, $\mathcal{Z}$'s view is identical in HYB_0 and HYB'_0.

We now turn to the indistinguishability of HYB'_0 and $\mathsf{HYB}^1_{\mathcal{S}_1,\mathcal{Z}}$ and rely on the semantic security of the Cramer-Shoup cryptosystem, which is equivalent to the DLIN assumption. Namely, if there exist an environment $\mathcal{Z}$ and an adversary $\mathcal{A}$ for which the two experiments are distinguishable, there is an IND-CPA adversary $\mathcal{D}_{CPA}$ (in the sense of the left-or-right definition of [2]) against the linear Cramer-Shoup scheme. This adversary takes in an encryption key pk and proceeds as follows. (We merely provide a sketch here.) It uses a Groth-Sahai CRS $\mathbf{g} = (\boldsymbol{g_1}, \boldsymbol{g_2}, \boldsymbol{g_3})$ for the WI setting and the challenge Cramer-Shoup public key

pk is used to complete the generation of crs. It then simulates adversary $\mathcal{A}$ with the left-or-right oracle and the simulation trapdoor (ξ_1, ξ_2) to simulate a NIZK proof. Algorithm $\mathcal{D}_{CPA}$ eventually outputs what the environment outputs. If the secret bit of the encryption oracle is $b = 0$, $\mathcal{D}_{CPA}$ is running experiment HYB'_0 whereas, if $b = 1$, it is running $\mathsf{HYB}^1_{\mathcal{S}_1,\mathcal{Z}}$. The same argument as in [8, Theorem 8] shows that experiments REAL and $\mathsf{HYB}^1_{\mathcal{S}_1,\mathcal{Z}}$ are indistinguishable. □

We observe that the only situation where experiments IDEAL and $\mathsf{HYB}^1_{\mathcal{S}_1,\mathcal{Z}}$ depart from each other is when, during the ideal experiment IDEAL, $\mathcal{S}$ gives a message M to $\mathcal{F}_{\text{MCOM}}$ when a corrupted party $\tilde{P}_i$ comes up with a commitment and, later on, $\tilde{P}_i$ opens that commitment to $M^* \neq M$. We are thus left with the task of bounding the probability of the latter event, which we call Fail, in IDEAL. To this end, we will actually rule out the possibility of such a mismatch in an experiment IDEAL/GENUINE where $\mathcal{A}$'s view is nearly the same as in the ideal experiment. We then argue that, if Fail occurs with non-negligible probability during IDEAL, the same holds in IDEAL/GENUINE.

Experiment IDEAL/GENUINE is defined as being identical to IDEAL with two differences: (1) when honest parties generate commitments, the simulator $\mathcal{S}$ "magically" knows which message is being committed to and computes ψ_{CS} and the corresponding opening $\pi_{val\text{-}enc}$ according to the specification of the scheme; (2) $\mathcal{S}$ configures the Groth-Sahai CRS $\mathbf{g} = (\boldsymbol{g_1}, \boldsymbol{g_2}, \boldsymbol{g_3})$ for the perfect soundness setting (namely, with $\boldsymbol{g_3} = \boldsymbol{g_1}^{\xi_1} \cdot \boldsymbol{g_2}^{\xi_2}$, for some random $\xi_1, \xi_2 \in \mathbb{Z}_p$).

In IDEAL/GENUINE, event Fail occurs if, on behalf of a corrupted player, the adversary $\mathcal{A}$ comes up with a commitment $\sigma^* = \psi^*_{\mathsf{CS}}$ for which ψ^*_{CS} decrypts to M but $\mathcal{A}$ subsequently produces a convincing opening $\pi^*_{val\text{-}enc}$ proving that ψ^*_{CS} opens to $M^* \neq M$. As in IDEAL, $\mathcal{S}$ aborts if Fail occurs during IDEAL/GENUINE. As will be argued later on, the probability of Fail is actually zero in IDEAL/GENUINE.

Claim. If the DLIN assumption holds and if H is collision-resistant, the probability that event Fail occurs in IDEAL is negligibly close to its probability of occurring in experiment IDEAL/GENUINE.

Proof. To prove the statement, we define experiments $\text{IDEAL/GENUINE}^{(1)}$ and $\text{IDEAL/GENUINE}^{(2)}$.

- $\text{IDEAL/GENUINE}^{(1)}$: is identical to IDEAL except that $\mathcal{S}$ knows which messages honest dummy parties commit to and computes ψ_{CS} as an encryption of the committed message M. On the other hand, NIZK proofs $\pi_{val\text{-}enc}$ are still simulated when these commitments have to be opened.
- $\text{IDEAL/GENUINE}^{(2)}$: is as $\text{IDEAL/GENUINE}^{(1)}$ but, when the simulator $\mathcal{S}$ has to open honest parties' commitments, NIZK proofs $\pi_{val\text{-}enc}$ are calculated using the real witnesses instead of the simulation trapdoor (ξ_1, ξ_2).
- IDEAL/GENUINE: is the same as $\text{IDEAL/GENUINE}^{(2)}$ with the difference that $\mathbf{g} = (\boldsymbol{g_1}, \boldsymbol{g_2}, \boldsymbol{g_3})$ is defined to be a perfectly sound Groth-Sahai CRS.

Experiments $\mathsf{IDEAL/GENUINE}^{(1)}$ and $\mathsf{IDEAL/GENUINE}^{(2)}$ provide the adversary and $\mathcal{Z}$ with identical views since, in the WI setting, simulated proofs are distributed as real proofs. Also, it is straightforward that $\mathsf{IDEAL/GENUINE}$ and $\mathsf{IDEAL/GENUINE}^{(2)}$ are indistinguishable under the DLIN assumption.

It remains to prove indistinguishability of IDEAL and $\mathsf{IDEAL/GENUINE}^{(1)}$. To this end, we show that, if there exist an environment $\mathcal{Z}$ and an adversary $\mathcal{A}$ such that Fail occurs with noticeably different probabilities in the two experiments, there is a chosen-ciphertext adversary $\mathcal{D}_{CCA}$ against the linear Cramer-Shoup encryption scheme. Our adversary $\mathcal{D}_{CCA}$ takes as input a public key pk for the encryption scheme and is granted access to a decryption oracle. It then proceeds similar to $\mathcal{D}_{CPA}$ but this time uses its decryption oracle to extract messages from adversarial commitments (we omit a formal description here for space reasons). We observe that, if the challenger's bit is $b = 1$, $\mathcal{D}_{CCA}$ proceeds in such a way that $\mathcal{A}$'s view is exactly as in experiment IDEAL. If $b = 0$, $\mathcal{D}_{CCA}$ is running experiment $\mathsf{IDEAL/GENUINE}^{(1)}$. Hence, as long as the linear Cramer-Shoup system is chosen-ciphertext secure, $\mathcal{D}_{CCA}$'s output probabilities in both experiments must be negligibly far apart.

In experiment $\mathsf{IDEAL/GENUINE}$, it is easy to see that event Fail cannot occur whatsoever. Indeed, it would require the adversary to produce a valid proof for a false statement, which is precluded by the perfect soundness of Groth-Sahai proofs in the soundness setting. □

4 Scheme II: A Tweak on the Camenisch-Shoup Scheme

4.1 Trapdoor Commitments to Group Elements

We need a trapdoor commitment scheme, suggested in [10], that allows committing to elements of a pairing-friendly group $\mathbb{G}$. To simplify our security analysis, we need commitments to consist of elements of the same group $\mathbb{G}$. We note that Groth's trapdoor commitment to group elements [15,1] could be used as well. However, our construction would then require to include NIZK proofs for pairing-product equations in each UC commitment, which would eventually result in longer commitment strings.

Such a trapdoor commitment can be obtained by modifying the opening phase of perfectly hiding Groth-Sahai commitments so as to enable trapdoor openings. This commitment uses a commitment key describing a prime order group $\mathbb{G}$ and $g \in \mathbb{G}$. The commitment key consists of vectors $(\boldsymbol{f_1}, \boldsymbol{f_2}, \boldsymbol{f_3})$ chosen as $\boldsymbol{f_1} = (f_1, 1, g)$, $\boldsymbol{f_2} = (1, f_2, g)$ and $\boldsymbol{f_3} = \boldsymbol{f_1}^{\chi_1} \cdot \boldsymbol{f_2}^{\chi_2} \cdot (1, 1, g)^{\chi_3}$, with $f_1, f_2 \xleftarrow{R} \mathbb{G}$, $\chi_1, \chi_2, \chi_3 \xleftarrow{R} \mathbb{Z}_p^*$. To commit to $X \in \mathbb{G}$, the sender picks $\theta_1, \theta_2, \theta_3 \xleftarrow{R} \mathbb{Z}_p^*$ and sets $\boldsymbol{C}_X = (1, 1, X) \cdot \boldsymbol{f_1}^{\theta_1} \cdot \boldsymbol{f_2}^{\theta_2} \cdot \boldsymbol{f_3}^{\theta_3}$, which, if $\boldsymbol{f_3}$ is parsed as $(f_{3,1}, f_{3,2}, f_{3,3})$, can be written $\boldsymbol{C}_X = (f_1^{\theta_1} \cdot f_{3,1}^{\theta_3}, f_2^{\theta_2} \cdot f_{3,2}^{\theta_3}, X \cdot g^{\theta_1+\theta_2} \cdot f_{3,3}^{\theta_3})$. To open $\boldsymbol{C}_X = (C_1, C_2, C_3)$, the sender reveals $(D_1, D_2, D_3) = (g^{\theta_1}, g^{\theta_2}, g^{\theta_3})$ and X. The receiver is convinced

that the committed value was X by checking that

$$\begin{cases} e(C_1, g) = e(f_1, D_1) \cdot e(f_{3,1}, D_3) \\ e(C_2, g) = e(f_2, D_2) \cdot e(f_{3,2}, D_3) \\ e(C_3, g) = e(X \cdot D_1 \cdot D_2, g) \cdot e(f_{3,3}, D_3). \end{cases}$$

If a sender can come up with distinct openings of $\boldsymbol{C}_X$, we can easily construct a distinguisher for the DLIN assumption (and even break a computational assumption that implies DLIN), as noted in [10].

Using the trapdoor (χ_1, χ_2, χ_3), the sender can equivocate commitments when $\chi_3 \neq 0$. Given a commitment $\boldsymbol{C}_X$ and its opening $(X, (D_1, D_2, D_3))$, one can trapdoor open $\boldsymbol{C}_X$ to any other $X' \in \mathbb{G}$ (without knowing $\log_g(X')$) by computing $D_1' = D_1 \cdot (X'/X)^{\chi_1/\chi_3}$, $D_2' = D_2 \cdot (X'/X)^{\chi_2/\chi_3}$ and $D_3' = (X/X')^{1/\chi_3} \cdot D_3$. The scheme is thus a trapdoor commitment whenever $\chi_3 \neq 0$. When $\chi_3 = 0$, the commitment is perfectly binding and even extractable with knowledge of discrete logarithms of the commitment key since X can be computed from (C_1, C_2, C_3) using $\beta_1 = \log_g(f_1)$, $\beta_2 = \log_g(f_2)$.

4.2 Construction

Our second construction builds upon the Camenisch-Shoup interactive UC-secure commitments [5]. The latter requires the committer to trapdoor-commit to the message m using some randomness r with the Pedersen trapdoor commitment [26] before encrypting m using a CCA2-secure encryption scheme supporting labels. In the committing phase, the sender then provides an interactive proof that the ciphertext ψ encrypts the plaintext which is committed to. To remove interaction from this construction, we use the Groth-Sahai techniques and combine them with the trapdoor commitment to group elements recalled in Section 4.1. The proof itself relies on a common reference string.

CRS-Gen(λ)**:** choose bilinear groups $(\mathbb{G}, \mathbb{G}_T)$ of order $p > 2^\lambda$ with $g \xleftarrow{R} \mathbb{G}$ and compute $g_1 = g^{\alpha_1}$, $g_2 = g^{\alpha_2}$, $f_1 = g^{\beta_1}$, $f_2 = g^{\beta_2}$ with $\alpha_1, \alpha_2, \beta_1, \beta_2 \xleftarrow{R} \mathbb{Z}_p^*$. Define vectors $\boldsymbol{g_1} = (g_1, 1, g)$, $\boldsymbol{g_2} = (1, g_2, g)$ and $\boldsymbol{g_3} = \boldsymbol{g_1}^{\xi_1} \cdot \boldsymbol{g_2}^{\xi_2}$ with $\xi_1, \xi_2 \xleftarrow{R} \mathbb{Z}_p^*$, which form a Groth-Sahai CRS $\mathbf{g} = (\boldsymbol{g_1}, \boldsymbol{g_2}, \boldsymbol{g_3})$ for the perfect soundness setting. Then, define vectors $\boldsymbol{f_1} = (f_1, 1, g)$, $\boldsymbol{f_2} = (1, f_2, g)$ and $\boldsymbol{f_3} = \boldsymbol{f_1}^{\chi_1} \cdot \boldsymbol{f_2}^{\chi_2} \cdot (1, 1, g)^{\chi_3}$ with $\chi_1, \chi_2, \chi_3 \xleftarrow{R} \mathbb{Z}_p^*$, which form a public key $\mathbf{f} = (\boldsymbol{f_1}, \boldsymbol{f_2}, \boldsymbol{f_3})$ for the trapdoor commitment to group elements. Finally, choose a collision-resistant hash function $H : \{0,1\}^* \to \mathbb{Z}_p$ and generate a public key $\mathsf{pk} = (X_1, \ldots, X_6)$ for the linear Cramer-Shoup encryption scheme. The CRS consists of $\mathsf{crs} = \{\lambda, \mathbb{G}, \mathbb{G}_T, g, \mathbf{g}, \mathbf{f}, H, \mathsf{pk}\}$.

Commit$(\mathsf{crs}, M, sid, cid, P_i, P_j)$**:** to commit to message $M \in \mathbb{G}$ for party P_j upon receiving a command $(\texttt{commit}, sid, cid, P_i, P_j, M)$, party P_i parses crs as $\{\lambda, \mathbb{G}, \mathbb{G}_T, g, \mathbf{g}, \mathbf{f}, \mathsf{pk}\}$, respectively, first fetches crs from $\mathcal{F}_{\text{CRS}}$ if not done already, and then conducts the following steps.

1. Using vectors $\mathbf{f} = (\boldsymbol{f_1}, \boldsymbol{f_2}, \boldsymbol{f_3})$ as $\boldsymbol{f_1} = (f_1, 1, g)$, $\boldsymbol{f_2} = (1, f_2, g)$ and $\boldsymbol{f_3} = (f_{3,1}, f_{3,2}, f_{3,3})$, pick $\theta_1, \theta_2, \theta_3 \xleftarrow{R} \mathbb{Z}_p^*$ and compute a commitment to $M \in \mathbb{G}$ as
$$com_M = (c_{M,1}, c_{M,2}, c_{M,3}) = \big(f_1^{\theta_1} \cdot f_{3,1}^{\theta_3},\ f_2^{\theta_2} \cdot f_{3,2}^{\theta_3},\ M \cdot g^{\theta_1+\theta_2} \cdot f_{3,3}^{\theta_3}\big).$$
2. Choose exponents $r, s \xleftarrow{R} \mathbb{Z}_p^*$ and compute a Cramer-Shoup encryption $\psi_{\mathsf{CS}} = (U_1, U_2, U_3, U_4, U_5)$ of $M \in \mathbb{G}$ under the label $L = P_i||sid||cid$ and the public key $\mathsf{pk} \in \mathbb{G}^6$ as in Section 2.3.
3. Generate a NIZK proof $\pi_{val\text{-}enc}$ that $\psi_{\mathsf{CS}} = (U_1, U_2, U_3, U_4, U_5)$ is a valid Cramer-Shoup encryption. This requires to commit to encryption exponents r, s and prove that these satisfy $U_1 = g_1^r$, $U_2 = g_2^s$, $U_3 = g^{r+s}$ and $U_5 = (X_1 X_3^{\alpha})^r \cdot (X_2 X_4^{\alpha})^s$ (which only takes 4 times 2 elements as base elements are all public). Including commitments com_r and com_s to exponents r and s, the proof $\pi_{val\text{-}enc}$ demands 14 group elements overall.
4. Generate a NIZK proof $\pi_{eq\text{-}com}$ that ψ_{CS} encrypts the same group element $M \in \mathbb{G}$ as the one that was committed to in com_M. In other words, prove that committed exponents $(r, s, \theta_1, \theta_2, \theta_3)$ satisfy
$$\Big(\frac{U_1}{c_{M,1}}, \frac{U_2}{c_{M,2}}, \frac{U_4}{c_{M,3}}\Big) = \big(g_1^r \cdot f_1^{-\theta_1} \cdot f_{3,1}^{-\theta_3},\ g_2^s \cdot f_2^{-\theta_2} \cdot f_{3,2}^{-\theta_3},\ g^{-\theta_1-\theta_2} \cdot f_{3,3}^{-\theta_3} \cdot X_5^r \cdot X_6^s\big). \tag{4}$$
Commitments to r, s are already part of $\pi_{val\text{-}enc}$. Committing to $\theta_1, \theta_2, \theta_3$ takes 9 elements. Proving (4) requires 6 elements as each relation is linear. Hence, $\pi_{eq\text{-}com}$ requires 15 group elements and P_i erases $(r, s, \theta_1, \theta_2, \theta_3)$ after its generation but retains the information $D_M = (g^{\theta_1}, g^{\theta_2}, g^{\theta_3})$.

The entire commitment $\sigma = (com_M, \psi_{\mathsf{CS}}, \pi_{val\text{-}enc}, \pi_{eq\text{-}com})$ takes 37 group elements. Upon receiving a commitment $(\mathtt{Com}, sid, cid, \sigma)$ from P_i, party P_j verifies the proofs $\pi_{val\text{-}enc}, \pi_{eq\text{-}com}$ in σ and, if correct, outputs $(\mathtt{receipt}, sid, cid, P_i, P_j)$; for invalid proofs P_j ignores the message.

Open$(\mathsf{crs}, M, D_M, sid, cid, P_i, P_j)$**:** when receiving $(\mathtt{open}, sid, cid, P_i, P_j, M)$, P_i reveals M and $D_M = (D_1, D_2, D_3) = (g^{\theta_1}, g^{\theta_2}, g^{\theta_3})$ to P_j.

Verify$(\mathsf{crs}, (\mathtt{Com}, sid, cid, \sigma), M, D_M, sid, cid, P_i, P_j)$**:** P_j verifies proofs $\pi_{val\text{-}enc}$, $\pi_{eq\text{-}com}$ (or recalls the previous check in the commitment phase) and ignores the opening if verification fails. If both proofs verify, P_j outputs $(\mathtt{open}, sid, cid, P_i, P_j, M)$ iff cid has not been used with this committer previously and the opening $D_M = (D_1, D_2, D_3)$ of com_M passes the verification test (as described in section 4.1). Otherwise, P_j also ignores the message.

4.3 Security

Theorem 2. *The above commitment scheme securely realizes $\mathcal{F}_{\text{MCOM}}$ in the* CRS *model against adaptive corruptions (assuming reliable erasure), provided that (i) the DLIN assumption holds in $\mathbb{G}$; (ii) the hash function H is collision-resistant.* (The proof appears in the full version of the paper).

5 Conclusion

In this paper we gave new constructions of efficient UC-secure commitment schemes in the CRS model, simultaneously supporting many useful properties: their commitment/opening phases are both non-interactive and they allow committing to strings rather than single bits while re-using the common reference string for an unbounded (but polynomial) number of commitments. Such UC secure commitments have not been known to exist so far. The only missing property, left as an open problem of our work, is to find new ways for eliminating the reliance on erasures (without introducing new assumptions, such as deployment of tamper-proof hardware that can be used in practice to avoid erasures, or using weaker adversary models that prevent adversarial access to ephemeral secrets).

Acknowledgments. Marc Fischlin was supported by grants Fi 940/2-1 and Fi 940/3-1 of the German Research Foundation (DFG). Benoît Libert acknowledges the Belgian Fund for Scientific Research (F.R.S.-F.N.R.S) for his "Chargé de recherches" fellowship and the BCRYPT Interuniversity Attraction Pole. Mark Manulis was supported by the DFG grant MA 4957. This work was also supported by CASED (`www.cased.de`).

References

1. Abe, M., Fuchsbauer, G., Groth, J., Haralambiev, K., Ohkubo, M.: Structure-Preserving Signatures and Commitments to Group Elements. In: Rabin, T. (ed.) CRYPTO 2010. LNCS, vol. 6223, pp. 209–236. Springer, Heidelberg (2010)
2. Bellare, M., Desai, A., Jokipii, E., Rogaway, P.: A Concrete Security Treatment of Symmetric Encryption. In: FOCS 1997, pp. 394–403 (1997)
3. Boneh, D., Boyen, X., Shacham, H.: Short Group Signatures. In: Franklin, M. (ed.) CRYPTO 2004. LNCS, vol. 3152, pp. 41–55. Springer, Heidelberg (2004)
4. Camenisch, J., Chandran, N., Shoup, V.: A Public Key Encryption Scheme Secure Against Key Dependent Chosen Plaintext and Adaptive Chosen Ciphertext Attacks. In: Joux, A. (ed.) EUROCRYPT 2009. LNCS, vol. 5479, pp. 351–368. Springer, Heidelberg (2009)
5. Camenisch, J., Shoup, V.: Practical Verifiable Encryption and Decryption of Discrete Logarithms. In: Boneh, D. (ed.) CRYPTO 2003. LNCS, vol. 2729, pp. 126–144. Springer, Heidelberg (2003)
6. Canetti, R.: Universally Composable Security: A New Paradigm for Cryptographic Protocols. In: FOCS 2001, pp. 136–145 (2001)
7. Canetti, R., Dodis, Y., Pass, R., Walfish, S.: Universally Composable Security with Global Setup. In: Vadhan, S.P. (ed.) TCC 2007. LNCS, vol. 4392, pp. 61–85. Springer, Heidelberg (2007)
8. Canetti, R., Fischlin, M.: Universally Composable Commitments. In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 19–40. Springer, Heidelberg (2001)
9. Canetti, R., Lindell, Y., Ostrovsky, R., Sahai, A.: Universally composable two-party and multi-party secure computation. In: STOC 2002, pp. 494–503 (2002)
10. Cathalo, J., Libert, B., Yung, M.: Group Encryption: Non-Interactive Realization in the Standard Model. In: Matsui, M. (ed.) ASIACRYPT 2009. LNCS, vol. 5912, pp. 179–196. Springer, Heidelberg (2009)
11. Cramer, R., Shoup, V.: A Practical Public Key Cryptosystem Provably Secure Against Adaptive Chosen Ciphertext Attack. In: Krawczyk, H. (ed.) CRYPTO 1998. LNCS, vol. 1462, pp. 13–25. Springer, Heidelberg (1998)

12. Damgård, I., Groth, J.: Non-interactive and reusable non-malleable commitment schemes. In: STOC 2003, pp. 426–437 (2003)
13. Damgård, I., Nielsen, J.B.: Perfect Hiding and Perfect Binding Universally Composable Commitment Schemes with Constant Expansion Factor. In: Yung, M. (ed.) CRYPTO 2002. LNCS, vol. 2442, pp. 581–596. Springer, Heidelberg (2002)
14. Dolev, D., Dwork, C., Naor, M.: Non-malleable cryptography. In: STOC 1991, pp. 542–552. ACM Press (1991)
15. Groth, J.: Homomorphic trapdoor commitments to group elements. Cryptology ePrint Archive: Report 2009/007 (2009)
16. Groth, J., Sahai, A.: Efficient Non-Interactive Proof Systems for Bilinear Groups. In: Smart, N.P. (ed.) EUROCRYPT 2008. LNCS, vol. 4965, pp. 415–432. Springer, Heidelberg (2008)
17. Hofheinz, D., Kiltz, E.: Secure Hybrid Encryption from Weakened Key Encapsulation. In: Menezes, A. (ed.) CRYPTO 2007. LNCS, vol. 4622, pp. 553–571. Springer, Heidelberg (2007)
18. Hofheinz, D., Müller-Quade, J.: Universally Composable Commitments Using Random Oracles. In: Naor, M. (ed.) TCC 2004. LNCS, vol. 2951, pp. 58–76. Springer, Heidelberg (2004)
19. Katz, J.: Universally Composable Multi-party Computation Using Tamper-Proof Hardware. In: Naor, M. (ed.) EUROCRYPT 2007. LNCS, vol. 4515, pp. 115–128. Springer, Heidelberg (2007)
20. Lindell, Y.: Highly-Efficient Universally-Composable Commitments Based on the DDH Assumption. In: Paterson, K.G. (ed.) EUROCRYPT 2011. LNCS, vol. 6632, pp. 446–466. Springer, Heidelberg (2011)
21. Naor, M., Yung, M.: Universal one-way hash functions and their cryptographic applications. In: STOC 1989, pp. 33–43 (1989)
22. Nishimaki, R., Fujisaki, E., Tanaka, K.: Efficient Non-interactive Universally Composable String-Commitment Schemes. In: Pieprzyk, J., Zhang, F. (eds.) ProvSec 2009. LNCS, vol. 5848, pp. 3–18. Springer, Heidelberg (2009)
23. Okamoto, T., Uchiyama, S.: A New Public-Key Cryptosystem as Secure as Factoring. In: Nyberg, K. (ed.) EUROCRYPT 1998. LNCS, vol. 1403, pp. 308–318. Springer, Heidelberg (1998)
24. Page, D., Smart, N.P., Vercauteren, F.: A comparison of MNT curves and supersingular curves. Appl. Algebra Eng., Commun. Comput. 17(5), 379–392 (2006)
25. Paillier, P.: Public-Key Cryptosystems Based on Composite Degree Residuosity Classes. In: Stern, J. (ed.) EUROCRYPT 1999. LNCS, vol. 1592, pp. 223–238. Springer, Heidelberg (1999)
26. Pedersen, T.: Non-Interactive and Information-Theoretic Secure Verifiable Secret Sharing. In: Feigenbaum, J. (ed.) CRYPTO 1991. LNCS, vol. 576, pp. 129–140. Springer, Heidelberg (1992)
27. Peikert, C., Waters, B.: Lossy Trapdoor Functions and Their Applications. In: STOC 2008, pp. 187–196 (2008)
28. Shacham, H.: A Cramer-Shoup encryption scheme from the linear assumption and from progressively weaker linear variants. Cryptology ePrint Archive: Report 2007/074 (2007)
29. Shoup, V.: A proposal for the ISO standard for public-key encryption (version 2.1) (2001) (manuscript), `http://shoup.net/`
30. Zhu, H.: New Constructions for Reusable, Non-erasure and Universally Composable Commitments. In: Bao, F., Li, H., Wang, G. (eds.) ISPEC 2009. LNCS, vol. 5451, pp. 102–111. Springer, Heidelberg (2009)