A New Security Notion for PKC in the Standard Model: Weaker, Simpler, and Still Realizing Secure Channels

Wasilij Beskorovajnov[1], Roland Gröll[1], Jörn Müller-Quade[1,2,3],
Astrid Ottenhues[2,3], and Rebecca Schwerdt[2,3](✉)

[1] FZI Research Center for Information Technology, Karlsruhe, Germany
{beskorovajnov,groell}@fzi.de
[2] Karlsruhe Institute of Technology (KIT), Karlsruhe, Germany
[3] KASTEL Security Research Labs, Karlsruhe, Germany
{mueller-quade,ottenhues,schwerdt}@kit.edu

Abstract. Encryption satisfying CCA2 security is commonly known to be unnecessarily strong for realizing secure channels. Moreover, CCA2 constructions in the standard model are far from being competitive practical alternatives to constructions via random oracle. A promising research area to alleviate this problem are weaker security notions—like IND-RCCA secure encryption or IND-atag-wCCA secure tag-based encryption—which are still able to facilitate secure message transfer (SMT) via authenticated channels.

In this paper we introduce the concept of sender-binding encryption (SBE), unifying prior approaches of SMT construction in the universal composability (UC) model. We furthermore develop the corresponding non-trivial security notion of IND-SB-CPA and formally prove that it suffices for realizing SMT in conjunction with authenticated channels. Our notion is the weakest so far in the sense that it generically implies the weakest prior notions—RCCA and atag-wCCA—without additional assumptions, while the reverse is not true. A direct consequence is that IND-stag-wCCA, which is strictly weaker than IND-atag-wCCA but stronger than our IND-SB-CPA, can be used to construct a secure channel.

Finally, we give an efficient IND-SB-CPA secure construction in the standard model from IND-CPA secure double receiver encryption (DRE) based on McEliece. This shows that IND-SB-CPA security yields simpler and more efficient constructions in the standard model than the weakest prior notions, i.e., IND-atag-wCCA and IND-stag-wCCA.

Keywords: Secure message transfer · Authenticated channel · Tag-based encryption · IND-CPA · IND-CCA2 · CCA2 Relaxations · Universal composability · McEliece

G. Hanaoka et al. (Eds.): PKC 2022, LNCS 13178, pp. 316–344, 2022.
https://doi.org/10.1007/978-3-030-97131-1_11

1 Introduction

The construction of secure channels is one of the main goals of cryptography. Among the milestones that have been reached to this end are public-key cryptosystems by Diffie and Hellman [18], semantic security by Goldwasser and Micali [22] (today referred to as chosen plaintext attack (CPA)), and the stronger adaptive chosen ciphertext attack (CCA2) by Rackoff and Simon [29].

Nowadays, CCA2 secure public key encryption (PKE) is a cornerstone of many protocols realizing secure channels for our daily life applications. One of the most typical applications is the encryption of e-mails. This is usually realized by implementations of either the S/MIME [32] or OpenPGP [7] standard. Both standards utilize a public key infrastructure (PKI) and digital signatures to realize authenticated channels. Hence we see that widespread applications of secure message transfer (SMT) integrally use authenticated channels and a PKI in addition to encryption. secure message transfer (SMT) is an abstraction of authenticated and encrypted communication in the universal composability (UC) model. How secure message transfer (SMT) can be utilized in practical real world scenarios can be seen for example in [30].

It is widely known that CCA2 is unnecessarily strong to construct SMT when authenticated channels are already present [11]. In addition many concrete CCA2 constructions either lack efficiency to be considered practical constructions or were only proven secure within the random oracle model (ROM), which has inherent problems, e.g., that some constructions which can be proven secure in the ROM are insecure with any implementation of the random oracle [10]. We would like to point out that we do not question the usefulness of the ROM despite its shortcomings. However, we consider the exploration of alternatives just as important and therefore focus on constructions proven secure in the standard model in this work. Hence the following question arises:

> *What is the weakest security definition in order to establish a secure channel in the standard model if we assume existing authenticated channels?*

In an attempt to answer this question we find a non-trivial relaxation of the weakest prior notions of replayable chosen ciphertext attack (RCCA) from [11] and adaptive-tag weakly chosen ciphertext attack (atag-wCCA) from [26], which were both shown to be weaker than CCA2 and used to construct secure channels. While this work does not provide an ultimate answer to this question—i.e., we do not prove that our definition, labeled indistinguishability under senderbinding chosen plaintext attack (IND-SB-CPA), is the weakest possible and hence necessary—we show IND-SB-CPA to be sufficient in the sense that any encryption protocol satisfying this security can be used directly to UC-realize SMT using authenticated channels.

Although this is an interesting theoretic result, we argue that for more relevancy the previous question needs to be accompanied by the following:

> *Can weaker security notions lead to simpler and more efficient constructions of a secure channel in the standard model?*

In the current state of affairs, tag-based encryption (TBE) is an attractive choice for constructing efficient CCA2 secure PKE in the standard model as already the weakest established TBE security notion, indistinguishability under selective-tag weakly chosen ciphertext attack (IND-stag-wCCA), was shown by Kiltz [23] to yield a transformation to CCA2 secure PKE by adding one-time signatures for example. We show that IND-stag-wCCA secure TBE does not actually require prior transformation to CCA2 secure PKE in order to construct secure channels: By deriving the new concept of sender-binding encryption (SBE) from TBE we are able to construct secure channels directly from IND-stag-wCCA secure encryption. The intuition behind SBE is to tie ciphertexts not only to the receiver as with classic PKE notions, but to the sending/encrypting party as well.

Somewhat surprisingly, via IND-SB-CPA secure SBE we are also able to construct secure channels from double receiver encryption (DRE) which only satisfies CPA security and soundness. CPA secure DRE was initially introduced by Diament et al. [17] to facilitate message transmission from one sender to two different receivers and allows for interesting applications such as security puzzles for denial of service countermeasures. Subsequently, Chow et al. [14] introduced the property of soundness for DRE, and proved it to be crucial for some applications such as plaintext awareness (PA). Our DRE-based protocol allows for a much simpler and more efficient encryption than IND-stag-wCCA secure TBE for constructing secure channels and hence allows us to answer the second question in the positive.

One caveat of the construction via DRE is that we require an extended PKI that realizes the *key registration with knowledge (KRK)* functionality. This guarantees that users of the PKI have knowledge of their private keys. While this is not a common functionality of PKIs in use today, there are first protocol drafts like OTRv4[1] which utilize deniable authenticated key exchange protocols that rely on the KRK functionality. In this case those are DAKEZ and XZDH due to Unger and Goldberg [33].

As discussed in the next section the two questions we raise have partially been considered in prior works. In this paper we make considerable headway towards answering both of them.

1.1 Related Work

In this section we firstly analyze the current scientific landscape of security notions for SMT construction with authenticated channels. We then discuss the most promising prior constructions to efficiently achieve these security notions.

A PKE satisfying CCA2 security was already shown by Canetti in [9] to realize SMT in the UC framework by communicating confidentially over authenticated channels. On the other hand CCA2 was also shown by Canetti et al. [11] to be unnecessarily strong for this purpose. Hence relaxations of CCA2 came into focus. Among these relaxations is indistinguishability under replayable

[1] https://github.com/otrv4/otrv4/blob/master/otrv4.md.

chosen ciphertext attack (IND-RCCA), introduced by Canetti, Krawczyk and Nielsen in [11] where they show that IND-RCCA suffices to UC-realize SMT using authenticated channels. IND-RCCA differs from CCA2 in the characteristic that the ability to generate ciphertexts, which decrypt to the same plaintext as the test ciphertext, does not help the adversary to win the game. We provide the formal notions of IND-RCCA in Appendix B.1 of the full version of this paper [3]. Recently, Badertscher et al. [1] examined IND-RCCA and variations of it using the constructive cryptography framework to construct a confidential channel—a strictly weaker notion than SMT. They concluded that IND-RCCA is not sufficient to realize confidential channels when using the authenticated channel for public key transfer only. They introduce a stronger security definition to solve this problem whereas we, like the original IND-RCCA paper, assume authentication for every message transfer.

Another direction to achieve weaker security definitions is that of TBE which was introduced by MacKenzie, Reiter and Yang [26]. They introduced the notion of tag-based non-malleability, which is nowadays known as indistinguishability under adaptive-tag weakly chosen ciphertext attack (IND-atag-wCCA) security for TBE. The authors show that an IND-atag-wCCA secure TBE scheme is also sufficient to realize SMT when provided with authenticated channels. A relaxation, IND-stag-wCCA, has been shown to facilitate CCA2 constructions with the additional usage of a one-time signature scheme [5] or a message authentication code combined with a commitment scheme [6]. Both constructions are originally meant for identity based encryption (IBE), but Kiltz showed in [23] how to adapt these for the TBE setting. So far IND-stag-wCCA secure TBE has not been shown, however, to directly facilitate SMT.

Let us now look at how efficiently these security notions can be achieved without employing the ROM. The most efficient general construction paradigms nowadays are the lossy trapdoor functions by Peikert and Waters [28], the correlated products by Rosen and Segev [31] and the very similar k-repetition by Döttling et al. [19][2], the Cramer-Shoup-like constructions [15] and the adaptive trapdoor functions [25]. More efficient constructions of SMT can be built upon TBE. The—to the best of our knowledge—most efficient code-based TBE schemes nowadays are due to Kiltz [23], Kiltz, Masny and Pietrzak [24], Cheng et al. [13] and Yu et al. [34]. In their schemes, the notion of IND-stag-wCCA security for TBE is required, which can be used to construct CCA2 schemes by adding one-time signatures or message authentication codes and commitments as mentioned above.

Regarding both of our research questions we see that although some progress was made in previous works there is still a lot of room for improvement. In the following section we highlight this paper's contribution towards closing this gap.

[2] In spite of being a generic paradigm this work was applied only to McEliece so far.

1.2 Our Contribution

In this paper we develop the new security notion of IND-SB-CPA, which is the weakest so far to UC-realize SMT in conjunction with authenticated channels. We also give a concrete efficient construction of an IND-SB-CPA secure SBE scheme in the standard model. An overview of this five-part contribution is illustrated in Fig. 1. The five contribution parts correspond to the Sects. 2 to 6:

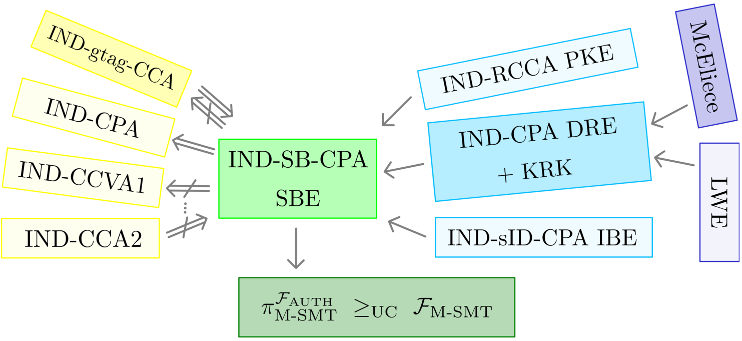

Fig. 1. Overview of our contribution

- In Sect. 2 we firstly provide the unifying definition of SBE, capturing all prior ways to construct SMT from authenticated channels and some form of encryption. A direct consequence is that all of the TBE notions, reformulated as SBE, directly construct SMT from authenticated channels. We then go on to develop the new game-based security notion of IND-SB-CPA. This is explicitly tailored to be as weak as possible while still only requiring authenticated channels to facilitate SMT. We achieve this by binding ciphertexts to sending parties.
- Section 3 presents a generic transformation from an indistinguishability under chosen plaintext attack (IND-CPA) secure DRE scheme with key registration to an IND-SB-CPA secure SBE scheme. To the extent of our knowledge it was not previously known how CPA secure DRE could be used to realize SMT. Appendix E of the full version of this paper [3] presents further generic transformations based on IND-RCCA secure PKE and indistinguishability under selective identity chosen plaintext attack (IND-sID-CPA) secure IBE.
- In Sect. 4 we construct an IND-CPA secure and sound DRE scheme from a McEliece variant. In conjunction with Sect. 3 this can be used to implement SMT in a more efficient and simpler way than known so far. To the extent of our knowledge we are the first to construct a McEliece-based DRE with soundness. Moreover, we show an improvement of a factor 5 regarding the size of the public key, which is mostly due to the avoidance of relying solely

on the (low-noise) learning parity with noise (LPN) assumption. Additionally, we provide another (2-repetition) McEliece construction and one from LWE-based binding encryption in Appendix F of the full version of this paper [3]. All our constructions are proven secure in the standard model.

- In Sect. 5 we finally construct a protocol which combines IND-SB-CPA security with authenticated channels. This protocol is subsequently proven to UC-realize SMT under static corruption by a malicious adversary.
- Section 6 highlights the theoretical relation between IND-SB-CPA and TBE security notions—in particular that the new notion of IND-SB-CPA is implied by the weakest known TBE security. Appendix G.2 of the full version of this paper [3] expands on this theoretic classification by comparing IND-SB-CPA to classic PKE indistinguishability notions from CPA to CCA2.

1.3 Preliminaries

Firstly, let us note that all notations and abbreviations we use can be looked up in Appendix A. We talk about different *game-based security notions* for various types of encryption schemes throughout this paper. While we would expect the reader to be familiar with the standard definitions of IND-CPA/-CCA2 etc., we provide formal definitions of all notions for your convenience in Appendix B of the full version of this paper [3]—in particular the more involved ones pertaining, e.g., to DRE, TBE and IBE schemes including security, correctness and soundness definitions.

In this work we use DRE as a building block for our construction. DRE encrypts a plaintext to two ciphertexts using two different public keys with the guarantee, that these ciphertexts decrypt to the same plaintext. Formally a DRE scheme consists of three probabilistic polynomial time (PPT) algorithms $(\texttt{gen}, \texttt{enc}, \texttt{dec})$ and the function $\texttt{f}_{\text{Key}}$, which checks if the key pair (sk, pk) is well-formed.

$$\begin{aligned}
\texttt{gen}: &\quad 1^\lambda \mapsto (sk, pk)\\
\texttt{enc}: &\quad (pk_1, pk_2, m) \mapsto c\\
\texttt{dec}: &\quad (sk_i, pk_1, pk_2, c) \mapsto m \text{ where } i \in \{1, 2\}\\
\texttt{f}_{\text{Key}}: &\quad (sk, pk) \mapsto \begin{cases} \mathsf{true} \\ \mathsf{false}. \end{cases}
\end{aligned}$$

TBE extends public key encryption by adding a tag to the encryption and decryption algorithms. This tag contains additional information and is a simple string. Formally a TBE scheme with message space $\mathbf{M}$ and tag space $\mathbf{T}$ consists of three PPT algorithms $(\texttt{gen}, \texttt{enc}, \texttt{dec})$.

$$\begin{aligned}
\texttt{gen}: &\quad (1^\lambda) \mapsto (sk, pk)\\
\texttt{enc}: &\quad (pk, t, m) \mapsto c\\
\texttt{dec}: &\quad (sk, t, c) \mapsto m \in \mathbf{M} \cup \{\perp\}
\end{aligned}$$

The weakest security notion of TBE so far is IND-stag-wCCA introduced by Kiltz [23]. This and further definitions of TBE security can be found in the full version of this paper [3]. The TBE notion IND-gtag-wCCA—which we start from to develop our notion of IND-SB-CPA security—is explicitly given in Sect. 2.

For readers who are not intimately familiar with the concept of *simulation-based security* or *universal composability* we also briefly recap the ideal/real-paradigm as well as UC in Appendix C of the full version of this paper [3]. More detailed explanations can be found, for instance, in [8,9]. As there have been conflicting definitions, we explicitly state formal definitions for the *ideal functionalities* of $\mathcal{F}_{\text{AUTH}}$, $\mathcal{F}_{\text{M-SMT}}$ and $\mathcal{F}_{\text{KRK}}$. For $\mathcal{F}_{\text{AUTH}}$ and $\mathcal{F}_{\text{M-SMT}}$ these can be found in Sect. 5 and additionally with further discussion in Appendix D of the full version of this paper [3]. The definition for $\mathcal{F}_{\text{KRK}}$ can be found in Appendix D of the full version as well.

2 IND-SB-CPA Security

SMT is commonly realized by combining an IND-CCA2 secure PKE or an IND-atag-wCCA secure TBE scheme with authenticated channels. As highlighted in Sect. 1, however, both of those security notions seem to be unnecessarily strong and restrictive for this application. In this observation we are hardly the first (cp. Sect. 1.1) as there are previous efforts to relax security notions with the aim to facilitate SMT—like the RCCA relaxation of CCA2 and efforts to use IND-stag-wCCA secure TBE.

In this section we introduce the concept of SBE and our new security notion of IND-SB-CPA. It is even weaker than the IND-atag-wCCA relaxation IND-stag-wCCA but still captures the security needed for secure message transfer via authenticated channels. Although the term SBE has not previously been defined, all prior realizations of SMT via authenticated channels (based on CCA2, RCCA, atag-wCCA or selective-tag weakly chosen ciphertext attack (stag-wCCA)) work by constructing an SBE scheme from the underlying encryption scheme. We therefore regard this as a long overdue unifying definition which is central for the topic of SMT construction.

Definition 1 (Sender-binding encryption (SBE)). *The interface of an SBE scheme is given by a set of three PPT algorithms* $(\texttt{gen}, \texttt{enc}, \texttt{dec})$*:*

$$\begin{aligned} \texttt{gen}: &\quad 1^\lambda \mapsto (sk, pk) \\ \texttt{enc}: &\quad (pk, S, m) \mapsto c \\ \texttt{dec}: &\quad (sk, S, c) \mapsto m. \end{aligned}$$

We expect an SBE scheme to fulfill the notion of correctness, i.e. that whenever $(sk, pk) \leftarrow \texttt{gen}(1^\lambda)$*, then*

$$m = \texttt{dec}(sk, S, \texttt{enc}(pk, S, m)).$$

Some remarks are in order about this use case definition of SBE.

In addition to the inputs present in any common PKE scheme, encryption and decryption algorithms use the encrypting party's ID S[3] as well. The ID of a party represents the identification information used within the system. This might be the public key itself, the party's actual name, their e-mail address etc. This does not only bind a ciphertext to the receiving party who holds the secret key and is able to decrypt the ciphertext—as any PKE scheme does—but also to the party who created the encryption.

However, binding a ciphertext to the ID of a sending/encrypting party alone does not yet yield obvious benefits. Even if a specific party ID is specified by the protocol, party IDs are public knowledge and malicious parties can insert any ID they want. SBE starts to unfold its benefit when used in conjunction with IDs that are associated with authenticated channels. This channel reliably indicates the true sender S of a message. Checking this against the sender ID bound to the received ciphertext prevents (honest sender) replay attacks, i.e., that this message was just copied from another (unwitting) sender. The terminology "sender-binding" stems from the example application of SMT via authenticated channels where this is taken to be the encrypting/sending party. Of course there might be other use cases for SBE where the encrypting party does not constitute a "sender". But throughout this paper (whenever we talk about SBE) we use R and "receiver" to denote the party owning the keys $(sk_R, pk_R) := (sk, pk)$, and S and the term "sender" for the party whose ID is input on encryption and decryption.

Given the definition of an SBE scheme we still need to arrive at a meaningful corresponding security notion. The intuitive way to construct an SBE scheme is to use a TBE scheme where the tag space $\mathbf{T}$ is chosen to be the set of party IDs $\mathbf{P}$. Even a TBE scheme with arbitrary tag space $\mathbf{T}$ can easily be used for

```
$\mathsf{Exp}^{\text{IND-gtag-wCCA}}_{\text{TBE},\mathcal{A}}$

(1) $t^* \overset{R}{\leftarrow} \mathbf{T}$
    $(sk, pk) \leftarrow \mathtt{gen}(1^\lambda)$
(2) $(st, m_0, m_1) \leftarrow \mathcal{A}^{\mathtt{dec}(sk,\cdot,\cdot)^a}(t^*, pk)$
(3) $b \overset{R}{\leftarrow} \{0,1\}$
    $c^* \leftarrow \mathtt{enc}(pk, t^*, m_b)$
(4) $b^* \leftarrow \mathcal{A}^{\mathtt{dec}(sk,\cdot,\cdot)^a}(st, c^*)$
(5) Return 1 if $b = b^*$, else return 0

[a] Decryption outputs $\perp$ for tags $t^* \in \{S, R\}$.
```

Fig. 2. The IND-gtag-wCCA TBE game.

[3] For the encryption mechanism we will sometimes omit the explicit input of the ID S if it is clear from the context which party S is conducting the encryption.

SBE as long as the tag space is as least as large as the set $\mathbf{P}$ of participating parties. To do so a public and injective function $\mathbf{P} \hookrightarrow \mathbf{T}$ is chosen to translate party IDs into tags. Hence to develop a security notion for SBE we start from the TBE notion indistinguishability under given-tag weakly chosen ciphertext attack (IND-gtag-wCCA). This is an intuitive weakening of the previously considered IND-stag-wCCA, with the only difference being that the adversary is not allowed to choose the challenge tag but is instead given a random tag by the challenger:

Definition 2 (IND-gtag-wCCA). *A TBE scheme* $(\mathtt{gen}, \mathtt{enc}, \mathtt{dec})$ *satisfies IND-gtag-wCCA security, if and only if for any PPT adversary* $\mathcal{A}_{gtag\text{-}CCA}$ *the advantage to win the IND-gtag-wCCA game shown in Fig. 2 is negligible in* λ.

Using party IDs as tags in TBE provides a special meaning to these tags. It is this additional meaning which induces the changes we make to IND-gtag-wCCA to arrive at our new notion of IND-SB-CPA for SBE: We now additionally have a connection between tags and key pairs, as any party ID (tag) is associated to the key pair of this party. Hence there is another ID/tag R corresponding to the key pair $(sk_R, pk_R) = (sk, pk)$ and another key pair (sk_S, pk_S) corresponding to the party $S = t^*$. As we are aiming towards the weakest possible notion from which to construct SMT we let both of those be chosen by the challenger instead of giving the adversary any more power. Depending on the underlying encryption scheme it is possible that keys may not be generated independently of the ID (think, e.g., of IBE schemes) or that public keys are used as IDs themselves. Hence we assume the challenger to randomly generate/draw keys and IDs in

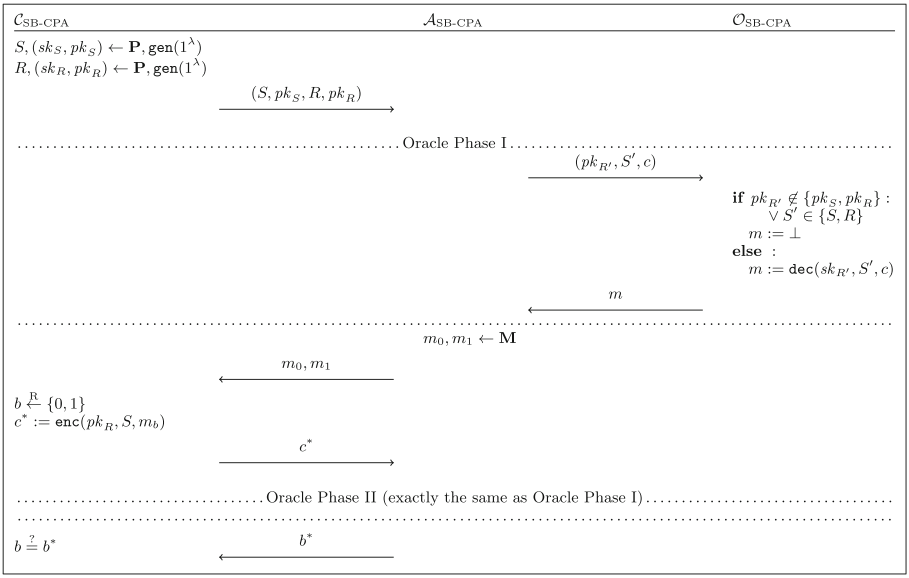
$\mathcal{C}_{\text{SB-CPA}}$
$\mathcal{A}_{\text{SB-CPA}}$
$\mathcal{O}_{\text{SB-CPA}}$
$S, (sk_S, pk_S) \leftarrow \mathbf{P}, \mathtt{gen}(1^\lambda)$
$R, (sk_R, pk_R) \leftarrow \mathbf{P}, \mathtt{gen}(1^\lambda)$
(S, pk_S, R, pk_R)
Oracle Phase I
$(pk_{R'}, S', c)$
if $pk_{R'} \notin \{pk_S, pk_R\}$:
$\vee\, S' \in \{S, R\}$
$m := \perp$
else :
$m := \mathtt{dec}(sk_{R'}, S', c)$
m
$m_0, m_1 \leftarrow \mathbf{M}$
m_0, m_1
$b \overset{R}{\leftarrow} \{0,1\}$
$c^* := \mathtt{enc}(pk_R, S, m_b)$
c^*
Oracle Phase II (exactly the same as Oracle Phase I)
$b \overset{?}{=} b^*$
b^*

Fig. 3. The IND-SB-CPA game for SBE

a consistent fashion. With the additional key pair (sk_S, pk_S) we also need to define how much decryption power the adversary gets for these keys in the two oracle phases. We choose this intuitively to be symmetric with the challenge keys (sk_R, pk_R). Because this gives a weaker notion and is still enough for SMT we restrict decryption not only for the challenge tag S but for R as well. All in all this adjustment of IND-gtag-wCCA to SBE yields the following definition:

Definition 3 (IND-SB-CPA). *An SBE scheme* $(\mathtt{gen}, \mathtt{enc}, \mathtt{dec})$ *satisfies IND-SB-CPA security, if and only if for any PPT adversary* $\mathcal{A}_{SB\text{-}CPA}$ *the advantage to win the IND-SB-CPA game shown in Fig. 3 is negligible in* λ.

Within this context of SBE, the new security notion of IND-SB-CPA has a very straight forward intuition: If it was possible to alter a ciphertext $c \leftarrow \mathtt{enc}(pk, S, m)$ to some c' which successfully decrypted under another sender ID S' (i.e. $\mathtt{dec}(sk_R, S', c') \neq \bot$), replay attacks would be possible. Let us look at this in a bit more detail. From Fig. 3 we see that the adversary is provided with perfect knowledge (via oracle or its own power) about any ciphertext which involves any other party than just S and R. About communication between S and R, on the other hand, the adversary learns nothing—with the natural exception that encryption only requires public knowledge and can therefore be conducted by the adversary as well. A directed version—where the adversary can additionally decrypt messages from R to S (but not from S to R)—would also naturally suggest itself. But as mentioned before our choice of a symmetric version is strictly weaker as well as sufficient for SMT construction. Having no decryption possibilities for the channel (S to R) along which the challenge ciphertext is sent justifies classifying IND-SB-CPA as some form of CPA security. For more thoughts on these classifications see Appendix G.3 of the full version of this paper [3].

We thoroughly investigate the relationships between IND-SB-CPA and other game-based notions in Sect. 6 and Appendix G.2 of the full version of this paper [3]. In the next section we show that IND-SB-CPA is not merely of academic interest by giving a generic example construction for IND-SB-CPA secure SBE via DRE.

3 Transformation from DRE to SBE

In this section we generically construct an IND-SB-CPA secure SBE scheme from DRE. Further generic constructions as well as more involved discussions of this DRE construction—particular about the use of KRK—can be found in the full version of this paper [3].

Originally meant to encrypt a message to two receivers, we use DRE in such a way, that one of those ciphertexts is encrypted using the public key of the sender. This, together with the usage of PKIs using KRK results in an encryption where the sender is aware of the plaintext. Without KRK there is no guarantee that the sender has knowledge of the private key corresponding to his public key, so this awareness could not be guaranteed. A possible realization of the KRK functionality is that the PKI demands a zero-knowledge proof of knowledge about the secret key when registering the public key. While this is a possibly expensive operation it only needs to be done once while registering.

We require the underlying DRE scheme to be sound, IND-CPA secure and compatible with the key registration functionality $\mathcal{F}_{\mathrm{KRK}}$. For the definition of DRE, its soundness, and the definition of $\mathcal{F}_{\mathrm{KRK}}$ we refer the reader to Appendices B.4 and D of the full version of this paper [3] respectively. This transformation will broaden our intuitive understanding of the new notion as well as provide a background for the concrete DRE construction we discuss in Sect. 4. We furthermore use the transformation in Sect. 6 to show that IND-SB-CPA does not in fact imply IND-gtag-wCCA but is a strictly weaker security notion.

Although DRE was initially devised to facilitate message transmission from one sender to two different receivers, choosing one of the receivers to be the sender itself provides a way to bind the ciphertext to the sender and to achieve an IND-SB-CPA secure SBE scheme.

One small caveat of using DRE is the need for key registration with knowledge: If we can not make sure the sender knows a key pair, ciphertexts encrypted under this key will not establish a reliable connection between ciphertext and sender. Hence we employ the ideal functionality $\mathcal{F}_{\mathrm{KRK}}$. To do so, however, we need to make sure the underlying DRE scheme is compatible:

Remark 1. Throughout this section we will assume DRE schemes to permit efficiently computable boolean functions $\mathtt{f}_{\mathrm{Key}}$. On input of a (possible) key pair (sk, pk) this function decides whether the keys "belong together", i.e., whether they could have been output by the encryption scheme's key generation algorithm or might just be an unrelated pair of values:

$$\mathtt{f}_{\mathrm{Key}} : (sk, pk) \mapsto \begin{cases} \mathsf{true}, & (sk, pk) \leftarrow \mathtt{gen}(1^\lambda) \\ \mathsf{false}, & \text{else.} \end{cases}$$

This is necessary for the scheme to be used in conjunction with the registration functionality $\mathcal{F}_{\mathrm{KRK}}$. In Appendix D of the full version of this paper [3] we discuss $\mathcal{F}_{\mathrm{KRK}}$ a bit more and also see that we can easily dispose of the need for a function $\mathtt{f}_{\mathrm{Key}}$ if we are happy for the registration functionality to (partially) generate the keys for the registering parties.

Let $(\mathtt{gen}, \mathtt{enc}, \mathtt{dec})$ be an IND-CPA secure DRE scheme which admits a function $\mathtt{f}_{\mathrm{Key}}$. We define a new encryption scheme $(\mathtt{Gen}, \mathtt{Enc}, \mathtt{Dec})$:

$\texttt{Gen}(1^\lambda)$ executed by party P:
- $(sk, pk) \leftarrow \texttt{gen}(1^\lambda)$.
- Register (sk, pk) with $\mathcal{F}_{\text{KRK}}^{\mathbf{f}_{\text{Key}}}$.

$\hookrightarrow$ Return $(SK, PK) := ((sk, pk), P)$.

$\texttt{Enc}(PK_R, S, m) = \texttt{Enc}(R, S, m)$ executed by party S:
- Retrieve pk_R and pk_S from $\mathcal{F}_{\text{KRK}}^{\mathbf{f}_{\text{Key}}}$.

$\hookrightarrow$ Return $c \leftarrow \texttt{enc}(pk_R, pk_S, m)$.

$\texttt{Dec}(SK_R, S, c) = \texttt{Dec}((sk_R, pk_R), S, c)$ executed by party R:
- Retrieve pk_S from $\mathcal{F}_{\text{KRK}}^{\mathbf{f}_{\text{Key}}}$.

$\hookrightarrow$ Return $m := \texttt{dec}(sk_R, pk_R, pk_S, c)$.

Let us give some intuition about the construction before we move on to formalities. Choosing one of the receivers for DRE to be the sender itself and having them encrypt a message under its own key might seem counterintuitive at first, but has one crucial benefit: It guarantees to the other (actual) receiver that even if the sender might not have constructed the ciphertext themselves but rather copied it from somewhere else, they have knowledge about the plaintext since they are able to decrypt as well. This is guaranteed by the registration with $\mathcal{F}_{\text{KRK}}^{\mathbf{f}_{\text{Key}}}$ in conjunction with the soundness property of the underlying DRE scheme. In addition to showing that this construction does in fact satisfy IND-SB-CPA security, we provide a discussion in Appendix E of the full version of this paper [3] on what properties exactly we need from DRE and how this is related to registration-based plaintext awareness (RPA).

Lemma 1. *In the $\mathcal{F}_{KRK}^{\mathbf{f}_{Key}}$ hybrid model* $(\texttt{Gen}, \texttt{Enc}, \texttt{Dec})$ *is an IND-SB-CPA secure SBE scheme.*

Proof. Assuming that $(\texttt{gen}, \texttt{enc}, \texttt{dec})$ is a sound DRE scheme with key function $\mathtt{f}_{\text{Key}}$ and assuming we have an adversary $\mathcal{A}_{\text{SB-CPA}}$ who has non-negligible success probability in winning the IND-SB-CPA game with respect to $(\texttt{Gen}, \texttt{Enc}, \texttt{Dec})$, we construct an adversary $\mathcal{A}_{\text{DRE-CPA}}$ with non-negligible success probability in winning the DRE IND-CPA game with respect to $(\texttt{gen}, \texttt{enc}, \texttt{dec})$. Note that in this case, $\mathcal{A}_{\text{DRE-CPA}}$ not only fields $\mathcal{A}_{\text{SB-CPA}}$'s queries to $\mathcal{O}_{\text{SB-CPA}}$ but also plays the role of $\mathcal{F}_{\text{KRK}}^{\mathbf{f}_{\text{Key}}}$ and has therefore access to registered keys. In the reduction shown in Fig. 4 we do not explicitly state this, but all interactions with $\mathcal{F}_{\text{KRK}}^{\mathbf{f}_{\text{Key}}}$ are handled exactly as the functionality itself would. The only exceptions are that an instantaneous $\texttt{ok}$ is assumed whenever the functionality would ask the adversary for some permission and that in the first phase the adversary $\mathcal{A}_{\text{DRE-CPA}}$ itself "registers" the keys pk_S and pk_R for S and R respectively without providing corresponding secret keys.

Since $\mathcal{A}_{\text{DRE-CPA}}$ has access to the internal state of $\mathcal{F}_{\text{KRK}}^{\mathbf{f}_{\text{Key}}}$, they can look up the keys $(sk_{S'}, pk_{S'})$ for any oracle query (R', S', c). If no such keys have been registered, decryption of the ciphertext would result in $\perp$. If keys have been registered, they can be used to correctly decrypt the ciphertext as the soundness

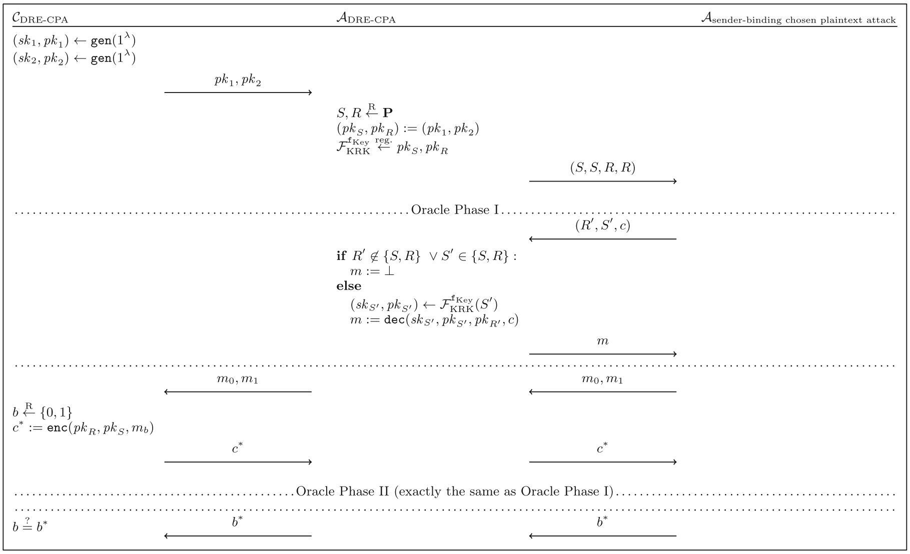
$\mathcal{C}_{\text{DRE-CPA}}$
$\mathcal{A}_{\text{DRE-CPA}}$
$\mathcal{A}_{\text{sender-binding chosen plaintext attack}}$
$(sk_1, pk_1) \leftarrow \texttt{gen}(1^\lambda)$
$(sk_2, pk_2) \leftarrow \texttt{gen}(1^\lambda)$
pk_1, pk_2
$S, R \overset{R}{\leftarrow} \mathbf{P}$
$(pk_S, pk_R) := (pk_1, pk_2)$
$\mathcal{F}_{\text{KRK}}^{\mathbf{f}_{\text{Key}}} \overset{\text{reg.}}{\leftarrow} pk_S, pk_R$
(S, S, R, R)
Oracle Phase I
(R', S', c)
if $R' \notin \{S, R\} \vee S' \in \{S, R\}$:
$m := \bot$
else
$(sk_{S'}, pk_{S'}) \leftarrow \mathcal{F}_{\text{KRK}}^{\mathbf{f}_{\text{Key}}}(S')$
$m := \texttt{dec}(sk_{S'}, pk_{S'}, pk_{R'}, c)$
m
m_0, m_1
m_0, m_1
$b \overset{R}{\leftarrow} \{0, 1\}$
$c^* := \texttt{enc}(pk_R, pk_S, m_b)$
c^*
c^*
Oracle Phase II (exactly the same as Oracle Phase I)
$b \overset{?}{=} b^*$
b^*
b^*

Fig. 4. Reduction for DRE construction

of DRE (see Appendix B.4 of the full version of this paper [3] for definition) guarantees

$$\texttt{dec}(sk_{S'}, pk_{S'}, pk_{R'}, c) = \texttt{dec}(sk_{R'}, pk_{R'}, pk_{S'}, c).$$

Hence it is no problem for $\mathcal{A}_{\text{DRE-CPA}}$ to respond with correct decryptions exactly as $\mathcal{O}_{\text{SB-CPA}}$ would. This gives $\mathcal{A}_{\text{DRE-CPA}}$ the same non-negligible success probability as $\mathcal{A}_{\text{SB-CPA}}$. □

This newfound utility for IND-CPA secure DRE schemes provides the motivational background for the next section, which in turn shows the relevance of our theoretical construction for the efficient construction of SMT in the standard model.

4 Efficient DRE Construction from McEliece and LPN

In this section we present an efficient way to construct an IND-CPA secure and sound DRE scheme from the McEliece and LPN assumptions and discuss how our construction improves the state of the art of SMT realizations in the standard model based on the McEliece and LPN assumptions. Moreover, to the extent of our knowledge we are the first to construct a DRE based on these assumptions. More details on our construction as well as further constructions via 2-repetition McEliece and learning with errors (LWE)-based binding encryption can be found in Appendix F of the full version of this paper [3].

Construction. Our DRE scheme can be seen as an augmentation of a construction from Kiltz et al. [24]. In this the authors propose a creative construction of a low-noise LPN-based TBE scheme, which they show to be IND-stag-wCCA secure. In the appendix of [24] the authors introduce a simplified variant of their IND-stag-wCCA secure construction, which is only IND-CPA secure. We use this simplified variant as a basis for our own construction. In order to establish the soundness property we add a second encryption of the randomness and exploit the randomness recovery to perform the consistency check. Moreover, we change the trapdoor mechanism to the one from the McEliece cryptosystem over Goppa codes. Hence we define our DRE scheme $(\texttt{gen}, \texttt{enc}, \texttt{dec})$ as follows:

`gen` Generate the McEliece secret key $sk := (\mathsf{S}, \mathsf{G}', \mathsf{P})$ and corresponding public key $pk := (\mathsf{G}, \mathsf{C})$ where $\mathsf{G} := \mathsf{S}\mathsf{G}'\mathsf{P}$ and C is a random binary matrix.

`enc` Sample a fresh random vector s, fresh error vectors $\mathsf{e}, \mathsf{e}_R, \mathsf{e}_S$ and encrypt s for both sender S and receiver R, i.e., $\mathsf{c}_S := \mathsf{s} \cdot \mathsf{G}_S \oplus \mathsf{e}_S$ and $\mathsf{c}_R := \mathsf{s} \cdot \mathsf{G}_R \oplus \mathsf{e}_R$. Mask the encoded message m with the noisy product $\mathsf{s} \cdot \mathsf{C}_S \oplus \mathsf{e}$, i.e. $\mathsf{c}' = \mathsf{s} \cdot \mathsf{C}_S \oplus \mathsf{e} \oplus Encode(m)$ and output $c := (\mathsf{c}_R, \mathsf{c}_S, \mathsf{c}')$ as the ciphertext.

`dec` The receiver recovers the randomness s from c_R with textbook McEliece decryption, verifies the hamming weight $wgt(\mathsf{s} \cdot \mathsf{G}_S \oplus \mathsf{c}_S) < t$ and unmasks $Encode(m) \oplus \mathsf{e} = \mathsf{c}' \oplus \mathsf{s} \cdot \mathsf{C}_S$. Finally, the receiver decodes and outputs the message m.

For the encoding and decoding we propose to use a suitable Goppa code, which is fixed for all parties. More details can be found in Appendix F of the full version of this paper [3].

Theorem 1. *The DRE scheme* $(\texttt{gen}, \texttt{enc}, \texttt{dec})$ *is IND-CPA secure, given that both the McEliece indistinguishability assumption and the learning parity with noise decisional problem (LPNDP) hold. In particular, let $\mathcal{A}$ be an IND-CPA adversary against the cryptosystem. Then there is a distinguisher $\mathcal{B}$ for Goppa codes and a distinguisher $\mathcal{D}$ for the LPNDP, such that for all $\lambda \in \mathbb{N}$*

$$\mathsf{Adv}_{\mathcal{A}}^{CPA}(\lambda) \leq \mathsf{Adv}_{\mathcal{D}}^{LPNDP_{\theta}(3n,l)}(\lambda) + 2 \times \mathsf{Adv}_{\mathcal{B}_R, G_R}^{IND}(\lambda).$$

Theorem 2. *The DRE scheme* $(\texttt{gen}, \texttt{enc}, \texttt{dec})$ *satisfies DRE soundness.*

The proofs and formal definitions of assumptions and experiments can be found in Appendix F of the full version of this paper [3] as well. Note also, that this DRE scheme admits an efficiently computable function $\mathtt{f}_{\text{Key}}$ as required for the use with $\mathcal{F}_{\text{KRK}}$ (cp. Sect. 3):

$$\mathtt{f}_{\text{Key}} : ((\mathsf{S}, \mathsf{P}, \mathsf{G}'), (\mathsf{G}, \mathsf{C})) \mapsto \begin{cases} \mathsf{true}, & \mathsf{G} = \mathsf{S}\mathsf{G}'\mathsf{P} \\ \mathsf{false}, & \text{else.} \end{cases}$$

In conjunction with Theorems 1 and 2 our DRE scheme satisfies all requirements for the generic transformation to IND-SB-CPA given in Sect. 3. Hence we can use it to efficiently achieve SMT if combined with authenticated channels.

Discussion. Considering that one of the third round finalists of the post-quantum cryptography (PQC) standardization by the NIST[4] is a McEliece variant based on Goppa codes we expect this mechanism to have significantly better parameters than cryptosystems that are based solely on the (low noise) LPN assumption. We argue, however, that our construction may as well be realized with the sole (low noise) LPN assumption or the Niederreiter cryptosystem [27]. Also, a similar augmentation of the randomness recovering variant of the dual Regev [21] cryptosystem may yield a very similar construction of DRE based on LWE. Currently, the Niederreiter cryptosystem seems the most promising as it was already shown in [20] that the trapdoor function is one-way under k-correlated input. The tightness loss is expected to be a factor of 3 regarding the number of LPNDP samples and a factor of 2 regarding the indistinguishability assumption. Therefore, we expect our construction of DRE to have roughly the same parameters as their single receiver IND-CPA counterparts without the soundness. An algebraic comparison of the public keys and the ciphertext from our work and the current state of the art in [24] and [34] can be found in Table 1.

Table 1. Comparison of public keys and ciphertext between [24,34] and this work.

Construction	Public Key	Ciphertext
Kiltz et al. [24]	$(A, B_0, B_1, C) \in (\mathbb{Z}_2^{m \times n'})^3 \times \mathbb{Z}_2^{l' \times n'}$	$(c, c_0, c_1, c_2) \in (\mathbb{Z}_2^{m})^3 \times \mathbb{Z}_2^{l'}$
Yu et al. [34]	$(A, B_0, B_1, C) \in \mathbb{Z}_2^{\overline{n} \times \overline{n}} \times (\mathbb{Z}_2^{q \times \overline{n}})^2 \times \mathbb{Z}_2^{\overline{l} \times \overline{n}}$	$(c, c_0, c_1, c_2) \in (\mathbb{Z}_2^{\overline{n}}) \times (\mathbb{Z}_2^{q})^2 \times \mathbb{Z}_2^{\overline{l}}$
This Work	$(G, C) \in \mathbb{Z}_2^{l \times n} \times \mathbb{Z}_2^{l \times n}$	$(c_R, c_S, c') \in (\mathbb{Z}_2^{n})^3$

At this point some remarks are necessary to understand the comparisons more thoroughly. For the sake of simplicity we will give rough estimations of the respective public key sizes. Kiltz et al. [24] require for their dimensions that $m \geq 2n'$ and $l' \geq m$, where n' is the dimension of the low-noise LPN secret. Current estimations suggest that cryptosystems based on low-noise LPN to have rather large dimensions, e.g., [16] suggest for 80 bits of security $n' = 9000$ when the noise is $\mu = 0.0044$. Therefore, setting $n' = 9000$ leads to the smallest possible $m = 18000$ and $l' = 18000$ and results in a public key size of roughly 77 megabyte.

Yu et al. [34] improved the construction of [24] in such a way that it may be based on constant noise LPN assuming sub-exponential hardness. Current estimations of concrete constant noise LPN hardness suggest much smaller dimensions than in the low-noise variant, e.g., [4] suggest for 80 bits of security $\overline{n} = 1280$ and noise level of $\mu = 0.05$, which meets the restriction from [34] that $\mu \leq 0.1$. The crucial parameter is, however, the choice of an $\alpha > 0$ as this parameter controls the dimension $q = O(\overline{n}^{6 \cdot \alpha + 1})$, which means that minimizing α will minimize the size of the public key. In order to estimate α as small as possible we take the formula $\beta = \frac{1}{2} - \frac{1}{\overline{n}^{3 \cdot \alpha}}$, which controls the number $\beta \cdot q$ of bit flipping errors that a suitable error correcting code will correct. For the

[4] National Institute of Standards and Technology.

sake of simplicity we set $\alpha = 0.04$, which is almost the minimal possible α for an $\overline{n} = 1280$, and get approximately $q = 7127$. Finally, fixing the remaining dimension $\overline{l} = \overline{n}$ we get a public key size of roughly 2.5 megabyte, which is a substantial improvement compared to [24].

For classic McEliece constructions Bernstein et al. [2] suggests for 80 bits of security to utilize $[1632, 1269]$ Goppa codes. Setting $n = 1632$ and $l = 1269$ in this work leads to a public key size of roughly 505 kilobyte, which is roughly factor 5 smaller than previous works.

We would like to point out that constructions from [24] and [34] are not directly comparable to our construction because we rely on the additional indistinguishability assumption of Goppa codes from random linear codes. However, all three constructions are code-based and implement a secure channel such that (rough) estimations of concrete sizes regarding the same security level may help to understand the improvement.

5 Realizing $\mathcal{F}_{\text{M-SMT}}$ from IND-SB-CPA and $\mathcal{F}_{\text{AUTH}}$

In this section we show that IND-SB-CPA secure SBE suffices in conjunction with authenticated channels to realize SMT. We prove this in the universal composability (UC) model of Canetti [9] (which is explained in more detail in Appendix C of the full version of this paper [3]) using *static corruptions* only. This means that the adversary chooses which parties to corrupt at the start of the protocol execution and not adaptively as the computation proceeds. We provide the formal definitions of the UC functionalities $\mathcal{F}_{\text{AUTH}}$ for authenticated channels and $\mathcal{F}_{\text{M-SMT}}$ for SMT to clarify which exact definitions we use. The latter deals with multiple receivers, multiple senders *and* multiple messages rather than working with a multi-session extension (cp. [12]) of a functionality $\mathcal{F}_{\text{SMT}}$ which only transmits a single message. Note that this is just a technical difference but essentially equivalent to the base of many arisen different definitions for SMT over the past. For more detailed discussions on these ideal functionalities see Appendix D of the full version of this paper [3].

$\mathcal{F}_{\text{AUTH}}$

Provides:
Single-receiver single-message single-sender authenticated message transfer with constant message size.
Behaviour:

- Upon invocation with input $(\texttt{send}, sid, R, m)$ from some party S, send backdoor message $(\texttt{send}, sid, S, R, m)$ to the adversary $\mathcal{A}$.
- Upon receiving $(\texttt{send ok}, sid)$ from adversary $\mathcal{A}$: If not yet generated output, then output $(\texttt{sent}, sid, S, R, m)$ to R.
- Ignore all further inputs.

$\mathcal{F}_{\textbf{M-SMT}}$

Provides:
Multi-receiver multi-message multi-sender secure message transfer with constant message size.
State:
Function $p_{\text{Msg}} : \mathbf{SID} \times \mathbf{MID} \to \mathbf{M} \times \mathbf{P}^2$ of pending messages.
Behaviour:

- Upon receiving $(\texttt{send}, sid, R, m)$ from some party S, draw fresh mid, send $(\texttt{send}, sid, mid, S, R)$ to the adversary $\mathcal{A}$ and append $(sid, mid) \mapsto (m, S, R)$ to p_{Msg}.
- Upon receiving $(\texttt{send ok}, sid, mid)$ from the adversary, look up $(m, S, R) := p_{\text{Msg}}(sid, mid)$. If it exists, output $(\texttt{sent}, sid, S, m)$ to R.

We will proceed towards the goal of realizing SMT in three stages: Firstly, we define a candidate protocol $\pi_{\text{M-SMT}}^{\mathcal{F}_{\text{AUTH}}}$ in the $\mathcal{F}_{\text{AUTH}}$-hybrid model which utilizes an IND-SB-CPA secure SBE scheme. Secondly, we construct a simulator $\mathcal{S}_{\text{M-SMT}}$ aiming to provide indistinguishability between the candidate protocol and the SMT functionality $\mathcal{F}_{\text{M-SMT}}$. The last step is formally proving that in the $\mathcal{F}_{\text{AUTH}}$-hybrid model indistinguishability from $\mathcal{F}_{\text{M-SMT}}$ is actually achieved by $\pi_{\text{M-SMT}}^{\mathcal{F}_{\text{AUTH}}}$ in conjunction with $\mathcal{S}_{\text{M-SMT}}$.

Protocol $\boldsymbol{\pi_{\text{M-SMT}}^{\mathcal{F}_{\text{AUTH}}}}$ Let $(\texttt{gen}, \texttt{enc}, \texttt{dec})$ be an IND-SB-CPA secure SBE scheme. From this we define a secure message transfer protocol $\pi_{\text{M-SMT}}^{\mathcal{F}_{\text{AUTH}}}$ as follows: Whenever a party S wants to securely transmit a message m to some party R, they essentially send the encryption $c \leftarrow \texttt{enc}(pk_R, S, m)$ over an authenticated channel to R. When a party R receives a ciphertext c over an authenticated channel from some party S, they decrypt it via $m := \texttt{dec}(sk_R, S, c)$. Although this general principle is very simple, many details—e.g. regarding key generation—need to be taken into account. The formal definition looks as follows:

$\pi_{\textbf{M-SMT}}^{\mathcal{F}_{\textbf{AUTH}}}$

Realizes:
Multi-receiver multi-message multi-sender secure message transfer with constant message size.

Parameters:
- IND-SB-CPA secure SBE scheme $(\texttt{gen}, \texttt{enc}, \texttt{dec})$ with message size l and ciphertext length l'.
- Functionality $\mathcal{F}_{\text{AUTH}}$.

State of Party P:

- Function $p_{\mathrm{Cred}} : \mathbf{SID} \rightarrow \mathbf{SK} \times \mathbf{PK}$ of own credentials.
- Function $p_{\mathrm{Pk}} : \mathbf{SID} \times \mathbf{P} \rightarrow \mathbf{PK}$ of known public keys.
- Function $p_{\mathrm{Send}} : \mathbf{SID} \times \mathbf{P} \rightarrow \mathbf{M}^*$ of pending messages.

Behaviour of Party P:

\\\\ Being asked to initialize

- Upon receiving output $(\texttt{sent}, \mathit{sid}_{\mathrm{AUTH}}, S, P, (\texttt{init}, \mathit{sid}))$ from $\mathcal{F}_{\mathrm{AUTH}}$, if there is no entry $p_{\mathrm{Cred}}(\mathit{sid})$ yet:
  (1) $(\mathit{sk}, \mathit{pk}) \leftarrow \texttt{gen}(1^\lambda)$.
  (2) Append $\mathit{sid} \mapsto (\mathit{sk}, \mathit{pk})$ to p_{Cred}.
  (3) For each party $P' \neq P$: Draw fresh $\mathit{sid}'_{\mathrm{AUTH}}$ and call $\mathcal{F}_{\mathrm{AUTH}}$ with input $(\texttt{send}, \mathit{sid}'_{\mathrm{AUTH}}, P', (\texttt{inited}, \mathit{sid}, \mathit{pk}))$.

\\\\ Receiving keys and sending stored messages

- Upon receiving output $(\texttt{sent}, \mathit{sid}_{\mathrm{AUTH}}, P', P, (\texttt{inited}, \mathit{sid}, \mathit{pk}_{P'}))$ from $\mathcal{F}_{\mathrm{AUTH}}$, if there is no entry $p_{\mathrm{Pk}}(\mathit{sid}, P')$ yet:
  (1) Append $(\mathit{sid}, P') \mapsto \mathit{pk}_{P'}$ to p_{Pk}.
  (2) For any $m \in p_{\mathrm{Send}}(\mathit{sid}, P')$:
    (1) Remove m from $p_{\mathrm{Send}}(\mathit{sid}, P')$.
    (2) $c \leftarrow \texttt{enc}(\mathit{pk}_{P'}, P, m)$.
    (3) Draw fresh $\mathit{sid}_{\mathrm{AUTH}}$.
    (4) Call $\mathcal{F}_{\mathrm{AUTH}}$ with input $(\texttt{send}, \mathit{sid}_{\mathrm{AUTH}}, P', (\mathit{sid}, c))$.

\\\\ Sending messages

- Upon receiving input $(\texttt{send}, \mathit{sid}, R, m)$ with $m \in \{0,1\}^l$ from environment $\mathcal{Z}$:
  ◦ If $R = P$ report output $(\texttt{sent}, \mathit{sid}, P, m)$ to the environment.
  ◦ Else if no entry $p_{\mathrm{Pk}}(\mathit{sid}, R)$ exists yet:
    (1) Append m to $p_{\mathrm{Send}}(\mathit{sid}, R)$.
    (2) Draw fresh $\mathit{sid}_{\mathrm{AUTH}}$.
    (3) Call $\mathcal{F}_{\mathrm{AUTH}}$ with input $(\texttt{send}, \mathit{sid}_{\mathrm{AUTH}}, R, (\texttt{init}, \mathit{sid}))$.
  ◦ Else:
    (1) $\mathit{pk}_R := p_{\mathrm{Pk}}(\mathit{sid}, R)$.
    (2) $c \leftarrow \texttt{enc}(\mathit{pk}_R, P, m)$.
    (3) Draw fresh $\mathit{sid}_{\mathrm{AUTH}}$.
    (4) Call $\mathcal{F}_{\mathrm{AUTH}}$ with input $(\texttt{send}, \mathit{sid}_{\mathrm{AUTH}}, R, (\mathit{sid}, c))$.

\\\\ Receiving messages

- Upon receiving output $(\texttt{sent}, \mathit{sid}_{\mathrm{AUTH}}, S, R, (\mathit{sid}, c))$ from $\mathcal{F}_{\mathrm{AUTH}}$:
  (1) Look up $\mathit{pk}_S := p_{\mathrm{Pk}}(\mathit{sid}, S)$. If this does not exist, abort.
  (2) $m \leftarrow \texttt{dec}(\mathit{sk}, S, c)$.
  (3) Report output $(\texttt{sent}, \mathit{sid}, S, m)$ to the environment $\mathcal{Z}$.

Simulator $\boldsymbol{\mathcal{S}}_{\textbf{M-SMT}}$. According to the real/ideal paradigm explained in Appendix C of the full version of this paper [3], our protocol $\pi^{\mathcal{F}_{\mathrm{AUTH}}}_{\mathrm{M\text{-}SMT}}$ realizes secure message transfer if and only if for any (dummy) adversary $\mathcal{A}$ interacting with the real protocol, there exists a simulator $\mathcal{S}$ interacting with the ideal functionality $\mathcal{F}_{\text{M-SMT}}$ such that no environment $\mathcal{Z}$ can distinguish between executions in the real and ideal world. We now construct such a simulator $\mathcal{S}_{\text{M-SMT}}$ which we will later show to achieve indistinguishability for $\pi_{\text{M-SMT}}^{\mathcal{F}_{\text{AUTH}}}$ and $\mathcal{F}_{\text{M-SMT}}$.

The main idea of the simulator $\mathcal{S}_{\text{M-SMT}}$ is that it simulates the protocol behaviour of all parties and the hybrid functionality $\mathcal{F}_{\text{AUTH}}$ in its head. It takes inputs to and reports messages and outputs from these in-the-head parties to $\mathcal{Z}$ on the one hand and uses them on the other hand to interface with the ideal functionality $\mathcal{F}_{\text{M-SMT}}$. The only case in which the simulator does not have sufficient knowledge to perfectly simulate the protocol in their head is when an honest party S sends a message m to another honest party R: The simulator has no way of knowing the actual message m. In this case $\mathcal{S}_{\text{M-SMT}}$ reports an encryption $c \leftarrow \texttt{enc}(pk_R, S, 0)$ of zero to have been send instead.

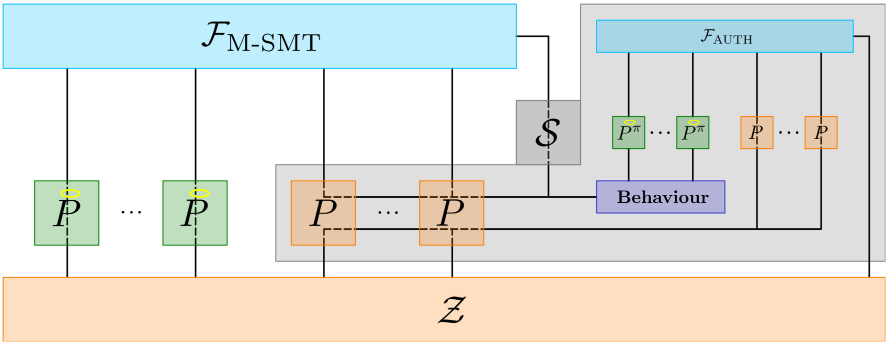

Fig. 5. Overview of Simulator $\mathcal{S}$

The overall construction of $\mathcal{S}_{\text{M-SMT}}$ is shown in Fig. 5. Again there are some more details to keep track of (especially regarding the box labeled "Behaviour" in Fig. 5) so we provide a more formal definition as well:

$\mathcal{S}_{\text{M-SMT}}$

Realizes:
Multi-receiver multi-message multi-sender secure message transfer with constant message size.

Parameters:

- Security parameter λ.
- IND-SB-CPA secure SBE scheme $(\texttt{gen}, \texttt{enc}, \texttt{dec})$.

In-the-head Parties:

- Functionality $\mathcal{F}_{\text{AUTH}}$. This functionality communicates in-the-head with all honest in-the-head parties as well as with the environment $\mathcal{Z}$ as adversary.
- Copies of honest parties running the protocol $\pi^{\mathcal{F}_{\text{AUTH}}}_{\text{M-SMT}}$, which we will denote as P^{π}. These parties communicate in-the-head with the in-the-head functionality $\mathcal{F}_{\text{AUTH}}$. Their interface to the environment is played by the simulator (defined in "Behaviour" below).
- Dummy corrupted parties. Whenever the simulator is asked by the environment to call the functionality $\mathcal{F}_{\text{AUTH}}$ in the name of a corrupted party, this in-the-head dummy calls the in-the-head functionality correspondingly and reports all outputs back to the environment $\mathcal{Z}$.

State:

- Everything the in-the-head parties store in their states.

Behaviour:

\\ Self-communication

- Upon receiving $(\texttt{send}, \mathit{sid}, \mathit{mid}, P, P)$ from $\mathcal{F}_{\text{M-SMT}}$ to $\mathcal{A}$ for honest party P, call $\mathcal{F}_{\text{M-SMT}}$ with input $(\texttt{send ok}, \mathit{sid}, \mathit{mid})$.

\\ Message from honest to honest party

- Upon receiving $(\texttt{send}, \mathit{sid}, \mathit{mid}, S, R)$ from $\mathcal{F}_{\text{M-SMT}}$ to $\mathcal{A}$ for honest parties $S \neq R$:
  - Start in-the-head party S^{π} with input $(\texttt{send}, \mathit{sid}, R, 0)$ from the environment $\mathcal{Z}$.
  - If in-the-head party R^{π} at some point reports output $(\texttt{sent}, \mathit{sid}, S, 0)$, call $\mathcal{F}_{\text{M-SMT}}$ with input $(\texttt{send ok}, \mathit{sid}, \mathit{mid})$.[5]

\\ Message from honest to corrupted party

- Upon receiving $(\texttt{send}, \mathit{sid}, \mathit{mid}, S, R)$ from $\mathcal{F}_{\text{M-SMT}}$ to $\mathcal{A}$ for honest party S and corrupted party R:
  1. Call $\mathcal{F}_{\text{M-SMT}}$ with input $(\texttt{send ok}, \mathit{sid}, \mathit{mid})$.
  2. Receive output $(\texttt{sent}, \mathit{sid}, S, m)$ from $\mathcal{F}_{\text{M-SMT}}$ to R.
  3. Start in-the-head party S^{π} with input $(\texttt{send}, \mathit{sid}, R, m)$ from the environment $\mathcal{Z}$.

\\ Message from corrupted to honest party

- Upon in-the-head honest party R^{π} reporting output $(\texttt{sent}, \mathit{sid}, S, m)$ for corrupted party S:
  1. Call $\mathcal{F}_{\text{M-SMT}}$ with input $(\texttt{send}, \mathit{sid}, R, m)$ in the name of S.
  2. Receive output $(\texttt{send}, \mathit{sid}, \mathit{mid}, S, R)$ from $\mathcal{F}_{\text{M-SMT}}$ to $\mathcal{A}$.
  3. Call $\mathcal{F}_{\text{M-SMT}}$ with input $(\texttt{send ok}, \mathit{sid}, \mathit{mid})$.

[5] At this point we assume the simulator to track the protocol executions in their head so they know which *mid* to use. For readability purposes we refrained from introducing notation to explicitly store this.

Security Theorem and Proof. The last thing left to do is to prove that under static corruption the simulator $\mathcal{S}_{\text{M-SMT}}$ does in fact achieve indistinguishability between $\pi_{\text{M-SMT}}^{\mathcal{F}_{\text{AUTH}}}$ and $\mathcal{F}_{\text{M-SMT}}$ in the $\mathcal{F}_{\text{AUTH}}$-hybrid model. To do so we will reduce this indistinguishability to the IND-SB-CPA security of the underlying SBE scheme. I.e. assuming there is an environment $\mathcal{Z}$ which can efficiently distinguish a real execution of $\pi_{\text{M-SMT}}^{\mathcal{F}_{\text{AUTH}}}$ from an ideal experiment with $\mathcal{F}_{\text{M-SMT}}$ and $\mathcal{S}_{\text{M-SMT}}$ (with non-negligible probability) we construct an adversary $\mathcal{A}_{\text{SB-CPA}}$ who can win the IND-SB-CPA game with non-negligible probability.

To achieve this let us first take a closer look at what a successfully distinguishing environment needs to do:

Remark 2. From the definition of the simulator $\mathcal{S}_{\text{M-SMT}}$ we immediately see that if an environment $\mathcal{Z}$ is able to distinguish executions of $\mathcal{F}_{\text{M-SMT}}$ and $\pi_{\text{M-SMT}}^{\mathcal{F}_{\text{AUTH}}}$, it can only do so by messages between honest parties $S \neq R$. In this case the simulator prompts its in-the-head sender S^{π} to send a message 0 to R instead of the actual message m (which the simulator does not know). The environment will therefore receive from $\mathcal{F}_{\text{AUTH}}$ (played by $\mathcal{S}_{\text{M-SMT}}$) a message

$$\Big(\texttt{send}, sid_{\text{AUTH}}, S, R, \big(sid, \texttt{enc}(pk_R, S, 0)\big)\Big)$$

in the ideal execution, while it receives in the protocol execution the message

$$\Big(\texttt{send}, sid_{\text{AUTH}}, S, R, \big(sid, \texttt{enc}(pk_R, S, m)\big)\Big).$$

In all other cases the simulator can perfectly mimic the protocol execution by playing the relevant parties and functionalities in its head.[6]

Let us restrict the distinguishing possibilities even more by introducing a sequence of hybrid games and showing that we only need to consider distinguishability of two consecutive hybrids:

Definition 4 (Hybrids H_k). *Let $k \in \mathbb{N}_0$ be a natural number. The hybrid H_k represents the execution set-up where almost all interactions are handled as in the real world execution of $\pi_{M\text{-}SMT}^{\mathcal{F}_{AUTH}}$. Note that Remark 2 guarantees that these are the same as in the ideal world, apart from encryptions of messages between honest parties. Now the only difference between an execution of $\pi_{M\text{-}SMT}^{\mathcal{F}_{AUTH}}$ and H_k is the following: For the first k messages m_i ($i \leq k$) between two honest parties $R_i \neq S_i$, the output from $\mathcal{F}_{AUTH}$ to the environment $\mathcal{Z}$*

$$\Big(\texttt{send}, sid_{AUTH}, S_i, R_i, \big(sid, \texttt{enc}(pk_{R_i}, S_i, 0)\big)\Big)$$

contains an encryption of zeros—as it would in the ideal execution with simulator $\mathcal{S}_{M\text{-}SMT}$—instead of an encryption of the real message m_i.
Note that H_0 is equal to the real world execution of $\pi_{M\text{-}SMT}^{\mathcal{F}_{AUTH}}$ and H_∞ (where encryptions of zeros are used for all messages m_i, $i \in \mathbb{N}$) is equal to the ideal world execution of $\mathcal{F}_{M\text{-}SMT}$ with $\mathcal{S}_{M\text{-}SMT}$.

[6] Please convince yourself from the definition of the simulator $\mathcal{S}_{\text{M-SMT}}$ that it has all the knowledge required for simulation and that activations/outputs of $\mathcal{F}_{\text{M-SMT}}$ will actually occur at the right times.

Lemma 2. *Let there be an environment $\mathcal{Z}$ which distinguishes real and ideal world. Then there is a $\kappa \in \mathbb{N}$ and an environment $\mathcal{Z}_\kappa$ which distinguishes hybrids $H_{\kappa-1}$ and H_κ.*

Proof. By definition $\mathcal{Z}$ distinguishes executions in hybrids H_0 and H_∞. Since $\mathcal{Z}$ is PPT, there is a polynomial $p_\mathcal{Z}$ which bounds its runtime, i.e. $\mathcal{Z}$ takes at most $p_\mathcal{Z}(\lambda)$ steps. In particular $\mathcal{Z}$ can request no more than $p_\mathcal{Z}(\lambda)$ messages to be sent between honest parties, and hence executions of $\mathcal{Z}$ in H_∞ and H_k are the same for all $k > p_\mathcal{Z}(\lambda)$. Hence by transitivity of indistinguishability (here we require the chain from H_0 to H_∞ to actually be finite by the argument before), there is an $\kappa \in \mathbb{N}$ such that H_κ and $H_{\kappa-1}$ are not indistinguishable. □

With this preparatory work, we are finally ready to prove that our protocol $\pi^{\mathcal{F}_{\text{AUTH}}}_{\text{M-SMT}}$ does in fact realize secure message transfer:

Theorem 3. *Under static corruption, $\pi^{\mathcal{F}_{AUTH}}_{M\text{-}SMT}$ is a UC-realization of $\mathcal{F}_{M\text{-}SMT}$ in the $\mathcal{F}_{AUTH}$-hybrid model, if the underlying SBE scheme satisfies IND-SB-CPA security. I.e.*

$$\pi^{\mathcal{F}_{AUTH}}_{M\text{-}SMT} \geq_{UC} \mathcal{F}_{M\text{-}SMT}.$$

Proof. Assume there is an environment $\mathcal{Z}$ which distinguishes between executions of $\pi^{\mathcal{F}_{\text{AUTH}}}_{\text{M-SMT}}$ and $\mathcal{F}_{\text{M-SMT}}$. By Lemma 2 there is a $\kappa \in \mathbb{N}$ such that $\mathcal{Z}$ distinguishes hybrids $H_{\kappa-1}$ and H_κ with non-negligible probability. We now construct and adversary $\mathcal{A}_{\text{SB-CPA}}$ from $\mathcal{Z}$ which has non-negligible probability to win the IND-SB-CPA game. First $\mathcal{A}_{\text{SB-CPA}}$ receives (S, pk_S, R, pk_R) from $\mathcal{C}_{\text{SB-CPA}}$. Then it starts $\mathcal{Z}$ in it's head, playing all other parties. Again by Remark 2, $\mathcal{Z}$ needs to register at least two honest parties (and send a message between them) to distinguish. For the two honest parties R and S (randomly chosen by the challenger), $\mathcal{A}_{\text{SB-CPA}}$ does not generate fresh credentials as the honest parties would do, but rather uses pk_S and pk_R from $\mathcal{C}_{\text{SB-CPA}}$.

It is no problem that $\mathcal{A}_{\text{SB-CPA}}$ does not know sk_R, sk_S. The only case they are used is when a corrupted party sends a message to R or S, i.e. when one of them receives output $(\texttt{sent}, sid_{\text{AUTH}}, P, R/S, (sid, c))$ for some corrupted party P from the functionality $\mathcal{F}_{\text{AUTH}}$. In this case $\mathcal{A}_{\text{SB-CPA}}$ promts the oracle $\mathcal{O}_{\text{SB-CPA}}$ with input (pk_S, P, c). Note that it is $P \notin \{S, R\}$. Hence $\mathcal{O}_{\text{SB-CPA}}$ by definition responds with the decryption $m := \texttt{dec}(sk_{S/R}, P, c)$ and $\mathcal{A}_{\text{SB-CPA}}$ can let the simulator call $\mathcal{F}_{\text{M-SMT}}$ with input $(\texttt{send}, sid, S/R, m)$ in the name of P as usual.

For the first $\kappa - 1$ messages which are sent between two honest parties, we report encryptions of 0 instead, when $\mathcal{Z}$ asks the adversary to see the content of the communication channel. When $\mathcal{Z}$ asks for the κ-th message m_κ to be sent, $\mathcal{A}_{\text{SB-CPA}}$ does the following:

- If m_κ is not a message from S to R, give up.
- If m_κ is to be sent from S to R, hand messages 0 and m_κ to $\mathcal{C}_{\text{SB-CPA}}$ and receive challenge c^*. Report c^* as communication channel content to $\mathcal{Z}$.

From now on, when a message m is sent between two honest parties, always report an encryption of m as channel content instead of 0 as before. When $\mathcal{Z}$

stops and reports it has run in the hybrid H_{κ}, report bit $b = 0$ to $\mathcal{C}_{\text{SB-CPA}}$, if $\mathcal{Z}$ decides on $H_{\kappa-1}$, report $b = 1$. □

6 Relation Between IND-SB-CPA and TBE Notions

We have presented the new notion of IND-SB-CPA for SBE in Sect. 2, given some intuition on what this notion implies and broadened the intuitive understanding by a generic example construction in Sect. 3. What is still missing from the picture is a formal classification of how this notion directly relates to other security notions. To fill this gap we firstly examine the connection between IND-SB-CPA and TBE security notions in this section.

In Appendix G.2 of the full version of this paper [3] we also look at the implications between IND-SB-CPA and classical PKE IND notions ranging from CPA to CCA2.

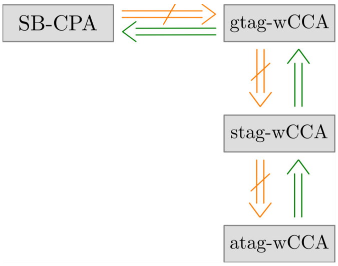

Fig. 6. Relationship to TBE notions

First note that although the notion of IND-gtag-wCCA has not been defined prior to this work it is an obvious relaxation of IND-stag-wCCA security—which was the weakest TBE notion considered so far. The proofs for the (non-)implications between IND-gtag-wCCA and IND-stag-wCCA can be found in Appendix G.1 of the full version of this paper [3].

In this section we concentrate on the relationship between IND-SB-CPA and IND-gtag-wCCA. To compare the two notions we assume the tag space $\mathbf{T}$ considered for IND-gtag-wCCA to be equal to a set $\mathbf{P}$ of party IDs. Of course a bijection between the two is sufficient as well, but we compare the notions for tag and ID spaces of the same size. An overview is shown in Fig. 6.

Lemma 3. *IND-SB-CPA* $\Leftarrow$ *IND-gtag-wCCA.*

Proof. Let $(\texttt{gen}, \texttt{enc}, \texttt{dec})$ be a TBE scheme. Under assumption of an efficient adversary $\mathcal{A}_{\text{SB-CPA}}$ with non-negligible probability to win the IND-SB-CPA security game, we will construct an efficient adversary $\mathcal{A}_{\text{gtag-wCCA}}$ who has the same success probability in the IND-gtag-wCCA game. An overview of the construction can be found in Fig. 7.

After being handed an ID S as the challenge tag and a public key pk, the adversary $\mathcal{A}_{\text{gtag-wCCA}}$ determines an ID R matching the public key $pk = pk_R$ and generates a key pair (sk_S, pk_S) matching the ID S. Depending on the specific scheme, these might, e.g., involve some key registration or be completely independent of one another. The IDs and public keys (S, pk_S, R, pk_R) are handed on to $\mathcal{A}_{\text{SB-CPA}}$. Any valid oracle queries $(pk_{R'}, S', c)$ from $\mathcal{A}_{\text{SB-CPA}}$ (i.e., those with $S' \notin \{S, R\}$ and $pk_{R'} \in \{pk_S, pk_R\}$) are answered in one of two ways: If pk'_R is equal to the challenge key pk_R, the query (S', c) is forwarded to $\mathcal{A}_{\text{gtag-wCCA}}$'s

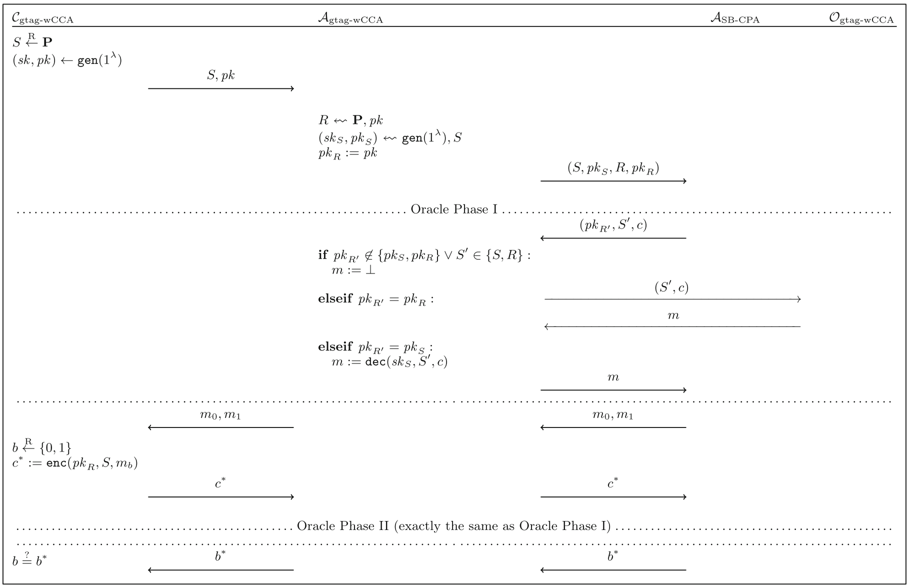
$\mathcal{C}_{\text{gtag-wCCA}}$
$\mathcal{A}_{\text{gtag-wCCA}}$
$\mathcal{A}_{\text{SB-CPA}}$
$\mathcal{O}_{\text{gtag-wCCA}}$
$S \overset{R}{\leftarrow} \mathbf{P}$
$(sk, pk) \leftarrow \texttt{gen}(1^\lambda)$
S, pk
$R \leftsquigarrow \mathbf{P}, pk$
$(sk_S, pk_S) \leftsquigarrow \texttt{gen}(1^\lambda), S$
$pk_R := pk$
(S, pk_S, R, pk_R)
Oracle Phase I
$(pk_{R'}, S', c)$
if $pk_{R'} \notin \{pk_S, pk_R\} \vee S' \in \{S, R\}$:
$m := \perp$
elseif $pk_{R'} = pk_R$:
(S', c)
m
elseif $pk_{R'} = pk_S$:
$m := \texttt{dec}(sk_S, S', c)$
m
m_0, m_1
m_0, m_1
$b \overset{R}{\leftarrow} \{0, 1\}$
$c^* := \texttt{enc}(pk_R, S, m_b)$
c^*
c^*
Oracle Phase II (exactly the same as Oracle Phase I)
$b \overset{?}{=} b^*$
b^*
b^*

Fig. 7. Reduction for IND-SB-CPA $\Leftarrow$ IND-gtag-wCCA

own oracle $\mathcal{O}_{\text{gtag-wCCA}}$. Otherwise, $\mathcal{A}_{\text{gtag-wCCA}}$ uses it's secret key sk_S to perform the decryption itself. In both cases the challenge is answered exactly like an oracle $\mathcal{O}_{\text{SB-CPA}}$ would. After forwarding the messages m_0, m_1 and the challenge ciphertext c^* between $\mathcal{A}_{\text{SB-CPA}}$ and $\mathcal{C}_{\text{gtag-wCCA}}$, the oracle phase is repeated exactly as before. Finally, the bit b^* which $\mathcal{A}_{\text{SB-CPA}}$ outputs is forwarded as well. If the adversary $\mathcal{A}_{\text{SB-CPA}}$ wins, so will $\mathcal{A}_{\text{gtag-wCCA}}$. □

Lemma 4. *IND-SB-CPA $\not\Rightarrow$ IND-gtag-wCCA.*

Proof. Let us consider the DRE-based example $(\texttt{Gen}, \texttt{Enc}, \texttt{Dec})$ from Sect. 3 again. In Lemma 1 we have already shown that this scheme is IND-SB-CPA secure. To prove our current claim it remains to be shown that $(\texttt{Gen}, \texttt{Enc}, \texttt{Dec})$ does not satisfy IND-gtag-wCCA security. We do so by constructing an efficient adversary $\mathcal{A}_{\text{gtag-wCCA}}$ which has non-negligible probability of winning the IND-gtag-wCCA security game. Firstly the challenger $\mathcal{C}_{\text{gtag-wCCA}}$ chooses a random party ID $S \in \mathbf{P}$, generates the challenge key pair (SK_R, PK_R) and registers it for some party R. On input of S, PK_R, the adversary $\mathcal{A}_{\text{gtag-wCCA}}$ generates a fresh key pair (SK_S, PK_S), and register this key pair with $\mathcal{F}_{\text{KRK}}$ in the name of S. Now the adversary chooses random messages $m_0 \neq m_1$ for the challenge and receives $c^* = \texttt{Enc}(PK_R, S, m_b)$. Due to DRE soundness the adversary can now decrypt the challenge as $m_b = \texttt{Dec}(SK_S, R, c^*)$ and win the IND-gtag-wCCA game with probability one. □

Although this proof is instructing for the intuitive understanding of SBE schemes since it relies on the fact that there is a connection between tags and party keys, it also relies on the party whose ID is randomly chosen as the challenge tag to be corruptible by the adversary. I.e. the adversary needs to be able to register keys for this party. Due to this caveat let us give a second proof of the lemma:

Proof (Alternative version). Let $(\mathtt{gen}, \mathtt{enc}, \mathtt{dec})$ be an IND-SB-CPA secure SBE scheme. We use this to construct an SBE/TBE scheme $(\mathtt{Gen}, \mathtt{Enc}, \mathtt{Dec})$ which is still IND-SB-CPA secure but does not satisfy IND-gtag-wCCA security:

$$\mathtt{Gen} := \mathtt{gen}$$

$$\mathtt{Enc} := \mathtt{enc}$$

$$\mathtt{Dec}(sk, S, c) := \begin{cases} \mathtt{dec}(sk, S, c) || sk & , sk = sk_S \\ \mathtt{dec}(sk, S, c) || 0 \cdots 0 & , \text{ else.} \end{cases}$$

It is obvious that this modified scheme does still satisfy IND-SB-CPA security, as we have $(\mathtt{Gen}, \mathtt{Enc}) = (\mathtt{gen}, \mathtt{enc})$ everywhere and $\mathtt{Dec} = \mathtt{dec}$ on the domain where $\mathcal{O}_{\text{SB-CPA}}$ answers queries. It is not, however, IND-gtag-wCCA secure, as any adversary can query $\mathcal{O}_{\text{gtag-wCCA}}$ with input (R, c) where R is the party ID corresponding to challenge key pk_R and c is an arbitrary ciphertext. The oracle will hand back sk_R which can be used to decrypt the challenge ciphertext c^* and win the security game every time. □

7 Conclusion

In this work we have introduced the concept of sender-binding encryption and developed the corresponding new security notion of IND-SB-CPA. We showed IND-SB-CPA security to be sufficient for UC-realizing secure message transfer (SMT) when combined with authenticated channels. Furthermore the direct implication from Sect. 6 and generic transformations from Appendix E of the full version of this paper [3] show that it is currently the weakest known notion with this property. Additionally we provided a generic transformation for IND-SB-CPA via IND-CPA secure double receiver encryption (DRE) in conjunction with key registration with knowledge. In particular this construction from DRE yields an efficient practical instantiation based on McEliece in the standard model.

For future work we see several directions to further this line of research. Although we know IND-SB-CPA to be weaker than prior notions which realize SMT via authenticated channels, it remains to be shown whether it constitutes the weakest possible notion to do so. It is also far from obvious that our current practical constructions are the most efficient to satisfy IND-SB-CPA security. More effort in this direction might prove fruitful as well.

Acknowledgments. We thank Björn Kaidel for fruitful initial discussions. We thank the PKC 2022 anonymous reviewers for their valuable feedback. The work presented in this paper has been funded by the German Federal Ministry of Education and Research (BMBF) under the project “PQC4MED” (ID 16KIS1044) and by KASTEL Security Research Labs.

A Notations and Abbreviations

This section can be used to look up all notations and abbreviations employed throughout this paper.

A.1 Notations

$\overset{R}{\leftarrow}$	Uniformly randomly drawn from
$\hookrightarrow$	Output
$\geq_{\mathrm{UC}}$	Securely UC-realizes
$\perp$	Invalid/failed
$\mathcal{A}$	Adversary
Adv	Advantage
aux	Auxiliary input/output
b	Bit from $\{0, 1\}$
$\mathcal{C}$	Challenger
c	Ciphertext
c^*	Challenge ciphertext
$\boldsymbol{c}$	Vectors
`dec`/`Dec`	Decryption algorithm
$\mathcal{E}$	Encryption scheme
`enc`/`Enc`	Encryption algorithm
Exp	Experiment
`ext`	Key extraction algorithm
$\mathcal{F}$	Ideal functionality
$\mathtt{f}_{\mathrm{ID}}/\mathtt{F}_{\mathrm{ID}}$	ID function
$\mathtt{f}_{\mathrm{Key}}/\mathtt{F}_{\mathrm{Key}}$	Boolean key function
$\mathtt{f}_{\mathbf{PK}}$	Key function $sk \mapsto pk$
$\boldsymbol{G}$	Matrices
`gen`/`Gen`	Key generation algorithm
goal	Goal of the adversary
id/ID	Protocol party ID
$\mathbf{ID}$	Set of all IDs
`init`	Asking to initialize
`inited`	Initialization done
k	Binary key length
λ	Security parameter
l	Message length
l'	Ciphertext length
m	Message
$\mathbf{M}$	Message space
`message`	$\mathcal{F}$ message variable
mid	Message ID
$\mathbf{MID}$	Set of all message IDs
mpk	IBE master public key
msk	IBE master secret key
n	Security parameter for McEliece
$\mathcal{O}$	Oracle
π	Protocol
$\pi^{\mathcal{F}_{\mathrm{AUTH}}}_{\text{M-SMT}}$	M-SMT protocol
P	Party
$\mathbf{P}$	Set of all parties
$\mathbb{P}$	Probability
pk/PK	Public key
$\mathbf{PK}$	Set of all public keys
pow	Power of the adversary
pr	Boolean prefix function
R	Receiver
$\mathbf{R}$	Set of all registered parties
`receiver`	Message *receiver*
`register`	Asking to be registered
`register ok`	Registration allowed
`registered`	Registration done
`retrieve`	Asking to retrieve credentials
`retrieve ok`	Retrieval allowed
`retrieved`	Retrieval done
$resp$	Oracle response
S	Sender
$\mathcal{S}$	Simulator
$\mathcal{S}_{\text{M-SMT}}$	Simulator for $\pi^{\mathcal{F}_{\mathrm{AUTH}}}_{\text{M-SMT}}$
scp	Scope of adversary's power
`send`	Asking to send message
`send ok`	Transmission allowed
`sent`	Message sent
set	Setting of security game
sid	Session ID
$\mathbf{SID}$	Set of all session IDs
sk/SK	Secret key
$\mathbf{SK}$	Set of all secret keys
`stray`	Message *stray*
$test$	Special response of $\mathcal{O}_{\mathrm{RCCA}}$
usk	User secret key
$\mathcal{Z}$	Environment

A.2 Abbreviations

CCA2 adaptive chosen ciphertext attack

CPA chosen plaintext attack

DAKEZ Deniable authenticated key exchange with zero-knowledge

DRE double receiver encryption

IBE identity based encryption

IF ideal functionality

IND indistinguishability

IND-CCA2 indistinguishability under adaptive chosen ciphertext attack

IND-CPA indistinguishability under chosen plaintext attack

IND-gtag-wCCA indistinguishability under given-tag weakly chosen ciphertext attack

gtag-wCCA given-tag weakly chosen ciphertext attack

IND-stag-wCCA indistinguishability under selective-tag weakly chosen ciphertext attack

stag-wCCA selective-tag weakly chosen ciphertext attack

IND-RCCA indistinguishability under replayable chosen ciphertext attack

IND-sID-CPA indistinguishability under selective identity chosen plaintext attack

IND-SB-CPA indistinguishability under sender-binding chosen plaintext attack

IND-atag-wCCA indistinguishability under adaptive-tag weakly chosen ciphertext attack

atag-wCCA adaptive-tag weakly chosen ciphertext attack

KRK key registration with knowledge

LPN learning parity with noise

LPNDP learning parity with noise decisional problem

LWE learning with errors

M-SMT multiple secure message transfer

OTR Off-the-Record

PA plaintext awareness

PKE public key encryption

PKI public key infrastructure

PPT probabilistic polynomial time

PQC post-quantum cryptography

RCCA replayable chosen ciphertext attack

ROM random oracle model

RPA registration-based plaintext awareness

SBE sender-binding encryption

SMT secure message transfer

TBE tag-based encryption

UC universal composability

XZDH Extended Zero-knowledge Diffie-Hellman

References

1. Badertscher, C., Maurer, U., Portmann, C., Rito, G.: Revisiting (R)CCA security and replay protection. IACR Cryptol, pp. 177 (2020). ePrint Arch. 2020. https://eprint.iacr.org/2020/177
2. Bernstein, D.J., Lange, T., Peters, C.: Attacking and defending the McEliece cryptosystem. In: Buchmann, J., Ding, J. (eds.) PQCrypto 2008. LNCS, vol. 5299, pp. 31–46. Springer, Heidelberg (2008). https://doi.org/10.1007/978-3-540-88403-3_3
3. Beskorovajnov, W., Groll, R., Muller-Quade, J., Ottenhues, A., Schwerdt, R.: A new security notion for PKC in the standard model: weaker, simpler, and still realizing secure channels, cryptology. ePrint Archive, Report 2021/1649 (2021). https://ia.cr/2021/1649

4. Bogos, S., Tramer, F., Vaudenay, S.: On solving LPN using BKW and variants. IACR Cryptol. ePrint Arch. (2015). http://eprint.iacr.org/2015/049
5. Boneh, D., Canetti, R., Halevi, S., Katz, J.: Chosen-ciphertext security from identity-based encryption. SIAM J. Comput. **36**(5), 1301–1328 (2007)
6. Boneh, D., Katz, J.: Improved efficiency for CCA-secure cryptosystems built using identity-based encryption. In: Menezes, A. (ed.) CT-RSA 2005. LNCS, vol. 3376, pp. 87–103. Springer, Heidelberg (2005). https://doi.org/10.1007/978-3-540-30574-3_8
7. Callas, J., Donnerhacke, L., Finney, H., Shaw, D., Thayer, R.: OpenPGP Message Format. RFC 4880, pp. 1–90 (2007). https://doi.org/10.17487/RFC4880
8. Canetti, R.: Security and Composition of Multi-party Cryptographic Protocols, Cryptology ePrint Archive, Report 1998/018 (1998). https://eprint.iacr.org/1998/018
9. Canetti, R.: Universally composable security: a new paradigm for cryptographic protocols. In: 42nd FOCS, pp. 136–145. IEEE Computer Society Press (2001). https://doi.org/10.1109/SFCS.2001.959888
10. Canetti, R., Goldreich, O., Halevi, S.: The Random Oracle Methodology, Revisited, Cryptology ePrint Archive, Report 1998/011 (1998). https://eprint.iacr.org/1998/011
11. Canetti, R., Krawczyk, H., Nielsen, J.B.: Relaxing chosen-ciphertext security. In: Boneh, D. (ed.) CRYPTO 2003. LNCS, vol. 2729, pp. 565–582. Springer, Heidelberg (2003). https://doi.org/10.1007/978-3-540-45146-4_33
12. Canetti, R., Rabin, T.: Universal composition with joint state. In: Boneh, D. (ed.) CRYPTO 2003. LNCS, vol. 2729, pp. 265–281. Springer, Heidelberg (2003). https://doi.org/10.1007/978-3-540-45146-4_16
13. Cheng, H., Li, X., Qian, H., Yan, D.: Simpler CCA secure PKE from LPN problem without double-trapdoor. In: Naccache, D., Xu, S., Qing, S., Samarati, P., Blanc, G., Lu, R., Zhang, Z., Meddahi, A. (eds.) ICICS 2018. LNCS, vol. 11149, pp. 756–766. Springer, Cham (2018). https://doi.org/10.1007/978-3-030-01950-1_46
14. Chow, S.S.M., Franklin, M.K., Zhang, H.: Practical dual-receiver encryption - soundness, complete non-malleability, and applications. In: Benaloh, J. (ed.) CT-RSA 2014. LNCS, pp. 85–105. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3319-04852-9
15. Cramer, R., Shoup, V.: Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack. SIAM J. Comput. **33**(1), 167–226 (2003)
16. Damgard, I., Park, S.: Is Public-Key Encryption Based on LPN Practical? IACR Cryptol. ePrint Arch. (2012). http://eprint.iacr.org/2012/699
17. Diament, T., Lee, H.K., Keromytis, A.D., Yung, M.: The dual receiver cryptosystem and its applications. In: Atluri, V., Pfitzmann, B., McDaniel, P. (eds.) ACM CCS 2004, pp. 330–343. ACM Press (2004). https://doi.org/10.1145/1030083
18. Diffie, W., Hellman, M.E.: New directions in cryptography. IEEE Trans. Inf. Theory **22**(6), 644–654 (1976)
19. Dottling, N., Dowsley, R., Mxiller-Quade, J., Nascimento, A.C.A.: A CCA2 Secure Variant of the McEliece Cryptosystem, Cryptology ePrint Archive, Report 2008/468 (2008). https://eprint.iacr.org/2008/468
20. Freeman, D.M., Goldreich, O., Kiltz, E., Rosen, A., Segev, G.: More constructions of lossy and correlation-secure trapdoor functions. In: Nguyen, P.Q., Pointcheval, D. (eds.) PKC 2010. LNCS, vol. 6056, pp. 279–295. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-13013-7_17

21. Gentry, C., Peikert, C., Vaikuntanathan, V.: Trapdoors for hard lattices and new cryptographic constructions. In: Ladner, R.E., Dwork, C. (eds.) 40th ACM STOC, pp. 197–206. ACM Press (2008). https://doi.org/10.1145/1374376.1374407
22. Goldwasser, S., Micali, S.: Probabilistic encryption. J. Comput. Syst. Sci. **28**(2), 270–299 (1984)
23. Kiltz, E.: Chosen-ciphertext security from tag-based encryption. In: Halevi, S., Rabin, T. (eds.) TCC 2006. LNCS, vol. 3876, pp. 581–600. Springer, Heidelberg (2006). https://doi.org/10.1007/11681878_30
24. Kiltz, E., Masny, D., Pietrzak, K.: Simple chosen-ciphertext security from low-noise LPN. In: Krawczyk, H. (ed.) PKC 2014. LNCS, vol. 8383, pp. 1–18. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-642-54631-0_1
25. Kiltz, E., Mohassel, P., O'Neill, A.: Adaptive trapdoor functions and chosen-ciphertext security. In: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 673–692. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-13190-5_34
26. MacKenzie, P.D., Reiter, M.K., Yang, K.: Alternatives to non-malleability: definitions, constructions, and applications (extended ebstract). In: Naor, M. (ed.) TCC 2004. LNCS, pp. 171–190. Springer, Heidelberg (2004). https://doi.org/10.1007/9783-540-24638-1
27. Nojima, R., Imai, H., Kobara, K., Morozov, K.: Semantic security for the McEliece cryptosystem without random oracles. Des. Codes Cryptogr. **49**(1–3), 289–305 (2008). https://doi.org/10.1007/sl0623-008-9175-9
28. Peikert, C, Waters, B.: Lossy trapdoor functions and their applications. In: Ladner, R.E., Dwork, C. (eds.) 40th ACM STOC, pp. 187–196. ACM Press (2008). https://doi.org/10.1145/1374376.1374406
29. Rackoff, O., Simon, D.R.: Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack. In: Feigenbaum, J. (ed.) CRYPTO'91. LNCS, pp. 433–444. Springer, Heidelberg (1992). https://doi.org/10.1007/3-540-46766-l_35
30. Rill, J.: Towards Applying Cryptographic Security Models to Real-World Systems. Karlsruhe Institute of Technology, Germany (2020)
31. Rosen, A., Segev, G.: Chosen-ciphertext security via correlated products. In: Reingold, O. (ed.) TCC 2009. LNCS, vol. 5444, pp. 419–436. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-00457-5_25
32. Schaad, J., Ramsdell, B., Turner, S.: Secure/multipurpose internet mail extensions (S/MIME) version 4.0 message specification. RFC 8551, pp. 1–63 (2019). https://doi.org/10.17487/RFC8551
33. Unger, N., Goldberg, I.: Improved strongly deniable authenticated key exchanges for secure messaging. PoPETs **2018**(1), 21–66 (2018)
34. YU, Y., Zhang, J.: Cryptography with auxiliary input and trapdoor from constant-noise LPN. In: Robshaw, M., Katz, J. (eds.) CRYPTO 2016. LNCS, vol. 9814, pp. 214–243. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-53018-4_9