Authenticated Hybrid Encryption for Multiple Recipients

Stéphanie Alt

CELAR, Route de Laillé, F-35570 Bruz, France
s.alt@free.fr

January 24, 2006

Abstract. Authenticated encryption schemes used in order to send one message to one recipient have received considerable attention in the last years. We investigate the case of schemes, we call authenticated $\mathtt{1}{\rightarrow}\mathtt{n}$ schemes, that allow one to encrypt efficiently in a public-key setting a message for several, say n, recipients in an authenticated manner. We propose formal security definitions for such schemes that work also for $n = 1$ and which are stronger and/or more general than those currently proposed. We then present a flexible mode of operation that transforms any $\mathtt{1}{\rightarrow}\mathtt{1}$ authenticated encryption scheme working on small messages into a $\mathtt{1}{\rightarrow}\mathtt{n}$ authenticated encryption scheme working on longer messages. We show that it allows the construction of efficient $\mathtt{1}{\rightarrow}\mathtt{n}$ schemes that are proved secure for the strongest security notion.

Keywords: Public key encryption, Authentication, Signcryption, Multicast.

1 Introduction

How to asymmetrically and efficiently encrypt a message for multiple recipients in an authenticated manner? This question takes all its meaning for example in an electronic email context where users are not fixed and not necessarily organized. A sender would like some times to send a message to a unique recipient, and some times extend this action to several, say n, recipients. Repeating the former action n times would lead to a secure but inefficient protocol. Here the efficiency is measured in computational time (including the number of long data treatments), message expansion rate and simplicity of the making use.

MOTIVATIONS. Hybrid encryption is used in practice in order to encrypt a long message. A public key encryption scheme is used to encrypt a key that can then be used to symmetrically encrypt the message. In [27, 28, 9] the authors propose a general framework based on (asymmetric) Key Encapsulation Mechanisms (KEM) and (symmetric) Data Encapsulation Mechanisms (DEM). The KEM does not depend on the message and the key is generated by KEM itself (KEMs are not encryption mechanisms). This well-used framework allows simpler designing and simpler proofs for the confidentiality property of hybrid schemes that can be studied separately for each mechanism. Let's consider Shoup's KEM-DEM model. To encrypt a message m for a recipient B, a sender A first computes $(K, C_0) \leftarrow \texttt{KEM}(pk_B)$ where pk_B is the public key of B and then computes $C_1 = \texttt{DEM}(K, m)$ and sends (C_0, C_1).

The symmetric key K used to encrypt the message m depends on the public key of the recipient. Let's assume now that the sender wants to send the same message m to n recipients $B_1, \ldots, B_n$. The sender would like to have a common symmetric key K to encrypt the (long) message m and then encrypt the (short) key for each recipient. Encapsulation mechanisms are not well-suited to this use. In order to be efficient, a solution is to use an asymmetric encryption scheme ASYM instead of a KEM mechanism. Furthermore techniques of broadcast schemes can be used here to reduce the cost of the sending of the symmetric key. Finally the sender will have to proceed as in Fig.1.

1. choose a random l_K-bit key K where l_K the length of the key used in DEM
2. compute $C_0 = \texttt{DEM}(K, m)$
3. for each recipient (or each public key resulting from the broadcast scheme): compute $C_{1,i} = \texttt{ASYM}(pk_i, K)$
4. send $(C_0, C_{1,1}, \ldots, C_{1,n})$

Fig. 1. Hybrid scheme for multiple recipients

As noticed above, the operation in step 3 can be replaced by any encryption mode that works on small messages and that send one message to n recipients. This mode is not constrained to output n ciphertexts. The public keys used in the encryption mode can be associated to groups of users. In applications where users may be organized, for example with a tree structure, results from broadcast encryption schemes apply. Frameworks of [13, 24, 15] for example can thus be used to efficiently send a message in a confidential but unauthenticated manner to n users.

The rest of the paper consists in authenticating in a secure way the above scheme. We show that another modification of Shoup's KEM-DEM model should be made in order to achieve some appropriate properties.

RELATED WORK. In an asymmetric setting, authenticity is usually provided by signature schemes as defined in [14]. Many proposals such as [17, 30, 4, 16, 23, 12] have been made in order to provide both confidentiality and authenticity but, until recently, without formal security proof. A new primitive for authenticated encryption has also been proposed in [11]. It allows the transformation of an authenticated scheme that sends one small message to one recipient into an authenticated scheme that sends one longer message to one recipient. In the last few years several formal security definitions appeared in the literature and particularly in [1, 3, 2, 23, 10, 12]. However, though security notions for authenticated encryption in the symmetric setting seem to be fixed in [6], in the asymmetric setting the model is not stabilized. Indeed, each of the proposed security models is different from the others and a strong general model is missing. Paradoxically, this general question seems more improved in the very specific area of identity-based cryptography where stronger or more general security definitions are proposed particularly in [22, 7]. In order to send the same message to several recipients, we have currently the choice to use the above mentioned trivial mode which is not efficient, a specific identity-based scheme such as [7, 19], or one of the two proposals given in [21, 31]. The first one composes a signature scheme and an encryption scheme but can only provide a weak authenticity capability. The second one seems to resist the usual adversaries. Nevertheless both were proposed without a formal security model and thus without security proof. It appears that efficient and secure modes of operation that provide both confidentiality and authenticity for multiple recipients are not trivial, particularly when using hybrid encryption, since adversaries considered for such schemes are much stronger than usual adversaries.

CONTRIBUTIONS. We investigate the domain of authenticated schemes, we call authenticated $\mathtt{1}{\rightarrow}\mathtt{n}$ schemes, that send one message to several recipients and that are not constrained to use identity-based nor pairing-based cryptography. We study some criteria in order to construct such schemes, in particular we show that Shoup's KEM-DEM model has to be modified to obtain efficient and secure $\mathtt{1}{\rightarrow}\mathtt{n}$ schemes. We thus survey the current security definitions for authenticated asymmetric ($\mathtt{1}{\rightarrow}\mathtt{1}$) schemes and propose a general and/or stronger one. This definition is then extended in section 3.1 to authenticated $\mathtt{1}{\rightarrow}\mathtt{n}$ schemes and compared to the informal definitions given in [7, 19]. We show that the transformation proposed in [11] can be extended to a $\mathtt{1}{\rightarrow}\mathtt{n}$ authenticated encryption scheme. More generally we propose in section 3.3 a general and flexible mode of operation that transforms any $\mathtt{1}{\rightarrow}\mathtt{1}$ authenticated encryption scheme working on small messages, into a $\mathtt{1}{\rightarrow}\mathtt{n}$ authenticated encryption scheme working on longer messages. We show that it allows the construction of efficient $\mathtt{1}{\rightarrow}\mathtt{n}$ schemes that are proved secure for the strongest security notion thanks to the theorem 3. A particular one, that makes use of a signcryption scheme, is finally compared to Zheng's $\mathtt{1}{\rightarrow}\mathtt{n}$ scheme defined in [31]. In a secondary way, we review the result given in [11] when applied to authenticated encryption. In particular we give, with the theorems 1 and 2, two security results in a public key setting that correct the partial result of [11].

SECURITY ISSUES. Let k be the security parameter. The usual language of polynomial security is used for definitions and main security results. We say that an advantage is negligible if it is smaller than the inverse of any polynomial $p(k)$ for sufficiently large values of k. Nevertheless concrete security statements are also given for each reduction. We thus fix for all players (and adversaries) of the paper a computational model $\mathcal{M}$ (such as a Random Access Machine). In particular, we assume that all players use the same computational resources. We denote by $\mathcal{M}(k)$ the set of machines that are probabilistic and polynomial-time in k.

NOTATIONS. We denote by $x \leftarrow \mathcal{A}()$ the output of a randomized algorithm $\mathcal{A}$, $|x|$ the length in bits of x and $x \leftarrow_r \{0,1\}^l$ a random and uniform choice of x in $\{0,1\}^l$.

2 $\mathtt{1}\longrightarrow\mathtt{1}$ Authenticated encryption schemes

2.1 Definitions

We give in this section definitions for classical authenticated public key encryption schemes used to encrypt one message for one recipient and called $\mathtt{1}\rightarrow\mathtt{1}$ schemes. The difference with usual public key schemes is that the encryption function depends on both the public key of the recipient and the private key of the sender. We also note that, as in usual public key encryption scheme, each user receives a unique private key / public key pair. This choice is made also in [2, 12] and [22, 7]. So the authenticated encryption schemes considered here are not constrained to have two different key generation algorithms, one for senders and one for receivers as in [1, 3, 23, 10].

Definition 1 ($\mathtt{1}\rightarrow\mathtt{1}$ Authenticated encryption) *We define a $\mathtt{1}\rightarrow\mathtt{1}$ authenticated encryption $\mathcal{AE} = (\mathtt{AG}, \mathtt{AK}, \mathtt{AE}, \mathtt{AD})$ by four polynomial-time (in k) algorithms:*

1. *$\mathtt{AG}$ a general randomized setup algorithm that takes as input the security parameter and outputs a global information $\mathcal{I}$;*
2. *$\mathtt{AK}$ a randomized algorithm that takes as input the global information $\mathcal{I}$, and outputs a private key / public key pair (sk, pk);*
3. *$\mathtt{AE}_{sk}$ a randomized encryption algorithm, depending on the secret key sk of the sender, that takes as input the public key of the recipient and a message m, and outputs the public key pk of the sender and a ciphertext;*
4. *$\mathtt{AD}_{sk}$ a decryption algorithm, depending on the secret key sk of the recipient, that takes as input a public key and a ciphertext, and outputs a message m or $\perp$ if the ciphertext is not valid.*

The correctness requirement is that for all key pairs $(sk_A, pk_A), (sk_B, pk_B)$ and for all messages m: $\mathtt{AD}_{sk_B}(\mathtt{AE}_{sk_A}(pk_B, m)) = m$. Furthermore, it is assumed in the following that sk contains pk.

Both privacy and authenticity must be studied for such schemes. Several formal definitions for these properties appear in the literature and particularly in [1, 3, 2, 23, 10, 12] for usual schemes. Nonetheless, the proposed security models are different from each others, depending on the following characteristics. Definitions such as [22, 7] from identity-based cryptography are also considered since they seem more stabilized.

TWO-USER vs MULTI-USER SETTING. The definitions of [1, 3, 23, 10] are given in a two-user setting. These definitions can be useful for a first analysis of the security, but are unfortunately not sufficient to prove the security of a real scheme, always used in a multi-user setting, since some results proved in the former model become wrong in the latter one. The drawback of two-user setting proofs is underlined in [2] where an intuitive technique is given in order to obtain secure schemes in a multi-user setting from secure ones in a two-user setting. However, we choose the multi-user model as done in [12, 22, 7].

ORACLES. When modeling the privacy property (of encryption schemes) or the authenticity property (of signature schemes), some access to oracles are given to the adversary, namely a decryption oracle when attacking the confidentiality, or a signature oracle when attacking the authenticity. This choice is justified by the fact that in an unauthenticated public key encryption scheme only the public key of the recipient is used to compute a ciphertext and only its private key is unknown by the adversary. In the same way, for the signature scheme only the private key of the sender is unknown by the adversary. In an authenticated encryption scheme, the private key of a user is used in both the encryption algorithm and the decryption algorithm, and both the private key of the sender and the public key of the receiver contribute to the computation of a ciphertext. So, an adversary should be given access to both the encryption and the decryption oracles of the users. This is done only in [12, 22, 7]. Besides, in a multi-user setting these oracles must be flexible ones (the terminology comes from [3]), i.e oracles which are not restricted to encrypt (nor decrypt) for a particular user.

Let's consider for example the scheme DHETM of [1] where a ciphertext from A to B is defined by $C = pk_A \parallel C_1 \parallel C_2$ where C_1 is the symmetric encryption of the message m under a key K_1 and C_2 is the result of a MAC function of C_1 under a key K_2, and where $K_1 \parallel K_2 = H(pk_A^{sk_B})$ (where H is a hash function and $pk_A^{sk_B}$ is the static Diffie-Hellman key between A and B). If we consider an adversary who is not given the decryption oracle of A, we can show that the scheme is IND-CCA2 but we cannot say that the only way in practice for an adversary to obtain information on the plaintext is to submit the ciphertext to the decryption algorithm of B because if the adversary has access to the decryption algorithm of A then he would obtain the plaintext. A similar reasoning can be made for the authentication property. A solution for DHETM is to consider a security model as in [1] where the private key used to encrypt is different from the private key used to decrypt, or to break the symmetry of the encryption function in the computation of K_1 and K_2.

OUTSIDER vs INSIDER SECURITY. As opposed to the outsider security, when studying the insider security of a scheme we consider an adversary who can be the sender when attacking the confidentiality or the receiver when attacking the authenticity. In this case we can let the adversary choose his keys as in [1, 2, 12]. Insider security is thus stronger than outsider security but is not necessarily required. It may be interesting in a `1`$\rightarrow$`1` scheme to study for example the consequences of the compromising of the private key of a sender on the indistinguability property, or to study the non-repudiation property of the scheme.

GAMES. The confidentiality of a scheme is in most cases (for the stronger property) modeled by a *find-then-guess* game where the adversary mounts a chosen ciphertext attack, and is only disallowed to submit the received challenge to the decryption oracle of the receiver. We concentrate here on the so-called IND-CCA2 property even if it can be considered as too strong in practice (see for example [2]). For the authenticity, several possibilities exist, when defining the restrictive condition on the forgery returned by the adversary. In some cases, we would like a receiver of a ciphertext to be convinced that a sender A has effectively sent the associated plaintext m, i.e. no adversary is able to construct a valid ciphertext for a new plaintext m that is not submitted to the encryption oracle. This property is denoted here by UF-wPTXT where UF-w stands for weak unforgeability and PTXT stands for plaintext. Since the ciphertext must be produced for a recipient B, we could require in a multi-user setting that (m, pk_B) is not submitted to the oracle. We denote this property by UF-PTXT. In this case the receiver B is convinced that the sender has sent the message m to him. We could also require that the ciphertext returned by the adversary is new, i.e. not returned by the encryption oracle of the sender, or not returned by the encryption oracle of the sender for a request of the type (pk_B, m_i). These properties are denoted by UF-wCTXT and UF-CTXT where CTXT stands for ciphertext.

The following model of security is a generalisation of the definitions of [12, 22, 7] where particular choices are made on the adversaries and on the games. We thus consider an adversary who is given four flexible oracles: $\mathcal{O}_{\mathtt{AE}_A}, \mathcal{O}_{\mathtt{AE}_B}, \mathcal{O}_{\mathtt{AD}_A}, \mathcal{O}_{\mathtt{AD}_B}$, which correspond to the encryption oracles of the sender and the receiver, and the decryption oracles of the sender and the receiver. Such an adversary is denoted by $\mathcal{A}^{\mathcal{O}_{\mathtt{AE}_A}, \mathcal{O}_{\mathtt{AD}_B}, \mathcal{O}_{\mathtt{AE}_B}, \mathcal{O}_{\mathtt{AD}_A}}$.

Definition 2 ($\mathtt{1}\!\rightarrow\!\mathtt{1}$ Outsider security) *An authenticated $\mathtt{1}\!\rightarrow\!\mathtt{1}$ encryption scheme $\mathcal{AE}$ is outsider-secure if:*

1. *$\mathcal{AE}$ is IND-CCA2 i.e. the advantage $Adv^{indcca2}_{\mathcal{AE},\mathcal{A}}(k)$ equals to*

$$2.\Pr[\,\mathcal{I} \leftarrow \mathtt{AG}(1^k), (sk_A, pk_A) \leftarrow \mathtt{AK}(\mathcal{I}), (sk_B, pk_B) \leftarrow \mathtt{AK}(\mathcal{I}), \sigma \leftarrow_r \{0,1\},$$
$$(s, m_0, m_1) \leftarrow \mathcal{A}_1^{\mathcal{O}_{\mathtt{AE}_A}, \mathcal{O}_{\mathtt{AD}_B}, \mathcal{O}_{\mathtt{AE}_B}, \mathcal{O}_{\mathtt{AD}_A}}(\mathcal{I}, pk_B, pk_A), C_\sigma \leftarrow \mathtt{AE}_{sk_A}(pk_B, m_\sigma);$$
$$\mathcal{A}_2^{\mathcal{O}_{\mathtt{AE}_A}, \mathcal{O}_{\mathtt{AD}_B}, \mathcal{O}_{\mathtt{AE}_B}, \mathcal{O}_{\mathtt{AD}_A}}(\mathcal{I}, pk_B, pk_A, s, C_\sigma) = \sigma] - 1$$

   where s is the memory of $\mathcal{A}$ and C_σ is not submitted to $\mathcal{O}_{\mathtt{AD}_B}$, is negligible for all $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2) \in \mathcal{M}(k)$,

2. *$\mathcal{AE}$ is UF-TXT i.e. the advantage $Adv^{uf-txt}_{\mathcal{AE},\mathcal{A}}(k)$ equals to*

$$\Pr[\,\mathcal{I} \leftarrow \mathtt{AG}(1^k), (sk_A, pk_A) \leftarrow \mathtt{AK}(\mathcal{I}), (sk_B, pk_B) \leftarrow \mathtt{AK}(\mathcal{I});$$
$$\mathcal{A}^{\mathcal{O}_{\mathtt{AE}_A}, \mathcal{O}_{\mathtt{AE}_B}, \mathcal{O}_{\mathtt{AD}_A}, \mathcal{O}_{\mathtt{AD}_B}}(\mathcal{I}, pk_B, pk_A) = (pk_A, c) \,/\, \mathtt{AD}_{sk_B}(pk_A, c) = m \neq \perp]$$

   where (pk_A, c) is not a response of $\mathcal{O}_{\mathtt{AE}_A}$ for a request of the form (pk_B, m_i) (for UF-CTXT), or (pk_A, c) is not a response of $\mathcal{O}_{\mathtt{AE}_A}$ (for UF-wCTXT), or (pk_B, m) has not been submitted to $\mathcal{O}_{\mathtt{AE}_A}$ (for UF-PTXT), or m has not been submitted to $\mathcal{O}_{\mathtt{AE}_A}$ (for UF-wPTXT), is negligible for all $\mathcal{A} \in \mathcal{M}(k)$.

For the insider security, we let the adversary choose sk_B when attacking the unforgeability property and sk_A when attacking the IND-CCA2 property. We denote by O-UF the authenticity for outsider adversaries and I-UF the authenticity for insider ones. We denote also the confidentiality property by O-IND-CCA2 for outsider adversaries and I-IND-CCA2 for insider ones.

Finally, we obtain eight properties for the authenticity. We denote them by x-UF-yTXT where $x \in \{O, I\}$ and $y \in \{wP, P, wC, C\}$.

We have clearly for $x \in \{O, I\}$: x-UF-CTXT $\Rightarrow$ x-UF-wCTXT and x-UF-CTXT $\Rightarrow$ x-UF-PTXT $\Rightarrow$ x-UF-wPTXT. The UF-wPTXT property is sufficient in some applications where we do not want to authenticate the recipient, in particular where we would like to be able to forward an authenticated message to other recipients. The only difference between x-UF-CTXT and x-UF-PTXT is on the ability for an adversary to produce a new ciphertext but without changing the message nor the recipient. Nevertheless we keep the x-UF-CTXT property since it is the strongest authentication property. We note also that, in a multi-user setting we have with the current definitions x-UF-wCTXT $\not\Rightarrow$ x-UF-PTXT $\forall x \in \{O, I\}$, since an adversary may submit to $\mathcal{O}_{\mathtt{AE}_A}$ many requests of the form (pk_i, m_i) until the ciphertext decrypts properly under pk_B. Thus, the UF-wCTXT notion will not be used in the following.

2.2 Authentication of a hybrid scheme

COMPOSITION METHODS. A solution to authenticate a hybrid scheme is to use a composition method that combines a signature scheme $\mathcal{S}$ with an encryption scheme $\mathcal{E}$. Encrypt-then-Sign ($\mathcal{E}t\mathcal{S}$) and Sign-then-Encrypt ($\mathcal{S}t\mathcal{E}$) are examples of such schemes. These compositions are shown in [2] secure against insider adversary in a two-user model where the adversary has only access to two oracles. A technique is given to transform these compositions into secure ones in a multi-users setting. Nevertheless, these compositions require two independent key pairs for each users and have a message expansion rate which is not optimal.

AUTHENTICATED `KEM` . In order to avoid the mentioned drawbacks of general composition schemes, one may use one-pass authenticated key exchange protocols as defined in [25]. This solution was first adopted for example in [32, 20, 29]. This technique was also applied to `KEM` mechanisms in [1, 10]. The generated symmetric key depends then on both the key of A and the key of B. It is shown in [10] that this construction may achieve an authentication property against outsider adversary. As noted in the same paper, it does not allow to consider insider security. Indeed since the `KEM` mechanism does not depend on the message, only the symmetric key is authenticated. So, everyone who knows the key (a recipient) can use the authenticated part and the key on another message, i.e. B may construct $C' = (pk_A, C_0, C'_1 = \mathtt{DEM}(K, m'))$. As noted in [2], this is not an issue in several applications for $\mathtt{1}{\rightarrow}\mathtt{1}$ schemes since the recipient is unchanged, in particular if non-repudiation is not required.

SIGNCRYPTION. As shown in [10], a security against insider adversaries may be achieved by considering a construction where the `KEM` part of the hybrid scheme takes as input a public key pk_B and the message m. This leads to a general scheme of the form H-PKE described in Fig.2. The message to encrypt is then, contrary to Shoup's KEM-DEM model, an input of both the asymmetric part and the symmetric part.

$\texttt{H-PKE}_{sk_A}(pk_B, m)$	$\texttt{SC}_{sk_A}(pk_B, m)$
1. $(K, C_0) \leftarrow \texttt{KEM}_{sk_A}(pk_B, m)$	1. Choose a nonce x
2. $C_1 = \texttt{DEM}(K, m)$	2. $K_1, K_2 = H(pk_B^x)$
3. Send (pk_A, C_0, C_1)	3. $\Lambda = \mathcal{H}_{K_1}(m)$
	4. $\Sigma = x/(\Lambda + sk_A) \bmod q$
	5. $C_1 = \texttt{DEM}(K_2, m)$
	6. Send $(pk_A, \Lambda, \Sigma, C_1)$

Fig. 2. H-PKE and SC Functions

Signcryption schemes, introduced in [30], were originally particular cases of H-PKE schemes as defined in Fig.2. They were defined as schemes that "*fulfill both the functions of secure encryption and digital signature but with a cost smaller than that required by signature-then-encryption*", and constitute another way to construct authenticated hybrid schemes. They are computationally very efficient schemes and allow some interesting properties such as the possibility for the signature part to be verifiable directly if the message is given with the public key of the sender [4], non repudiation [23] and so insider security.

A signcryption function depends on the private key sk_A of the sender and takes as input the public key pk_B of a recipient and a message m. We denote by SC a signcryption function that combines a hybrid scheme of the form KEM-DEM and a signature scheme. An example described in Fig.2 is given in [31] where a group of order q is chosen, H is a hash function, $\mathcal{H}_K$ is a keyed hash function under a key K and DEM is the CBC mode of the DES. The KEM part of this scheme can be viewed as the first four steps. The efficiency comes from the fact that the same nonce is used in steps 2 and 4.

2.3 An authenticated 1→1 scheme transformation

Recently, Y. Dodis and J. An proposed in [11] a new primitive that allows one to transform a 1→1 authenticated encryption scheme working on small messages into a 1→1 authenticated encryption scheme working on long messages.

Definition 3 (Concealment) *A concealment scheme is defined by three polynomial-time (in k) algorithms $\mathcal{C} = (\texttt{Setup}, \texttt{Conceal}, \texttt{Open})$, such that:*

1. *$\texttt{Setup}(1^k)$ outputs a public concealment parameter ck possibly empty;*
2. *$\texttt{Conceal}_{ck}(m)$ is randomized and transforms a message m into a pair (h, b);*
3. *$\texttt{Open}_{ck}(h, b)$ is deterministic and outputs m if (h, b) is valid or $\perp$ otherwise;*
4. *correctness: we require that $\texttt{Open}_{ck}(\texttt{Conceal}_{ck}(m)) = m$ for all m and ck;*
5. *non triviality: we require that $|b| \ll |m|$. We denote by $l_b = |b|$.*

Hiding. $\mathcal{C}$ satisfies the hiding property if for all $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2) \in \mathcal{M}(k)$,

$$Adv^{hid}_{\mathcal{C},\mathcal{A}}(k) = 2.\Pr[\ ck \leftarrow \mathtt{Setup}(1^k), (m_0, m_1, s) \leftarrow \mathcal{A}_1(ck), \sigma \leftarrow_r \{0,1\}, \\ (h,b) \leftarrow \mathtt{Conceal}_{ck}(m_\sigma); \mathcal{A}_2(s,h) = \sigma] - 1 < 1/p(k).$$

Binding. $\mathcal{C}$ satisfies the binding property if for all $\mathcal{A} \in \mathcal{M}(k)$,

$$Adv^{bind}_{\mathcal{C},\mathcal{A}}(k) = \Pr[\ ck \leftarrow \mathtt{Setup}(1^k); (b,h,h') \leftarrow \mathcal{A}(ck) \,/\, \mathtt{Open}_{ck}(h,b) \neq \perp \\ \text{and } \mathtt{Open}_{ck}(h',b) \neq \perp] < 1/p(k)$$

even if $\mathtt{Open}_{ck}(h,b) \neq \mathtt{Open}_{ck}(h',b)$.

Relaxed Binding. $\mathcal{C}$ satisfies the relaxed binding property if for all $\mathcal{A} \in \mathcal{M}(k)$,

$$Adv^{r-bind}_{\mathcal{C},\mathcal{A}}(k) = \Pr[\ ck \leftarrow \mathtt{Setup}(1^k), (m,s) \leftarrow \mathcal{A}_1(ck), (h,b) \leftarrow \mathtt{Conceal}_{ck}(m), \\ h' \leftarrow \mathcal{A}_2(s,h,b);\ \mathtt{Open}_{ck}(h',b) \neq \perp] < 1/p(k).$$

We call for short (relaxed) concealment scheme a concealment scheme that is non trivial and that satisfies the hiding and the (relaxed) binding properties. It is shown in [11] that (relaxed) concealment schemes exist iff (universal one way hash function (UOWHF)) collision resistant hash function (CRHF) exist. Furthermore, the following constructions are proposed:

Example 1 (Concealment scheme) *$\mathcal{C}$ is defined by:*

1. $\mathtt{Setup}(1^k) = \emptyset$;
2. $\mathtt{Conceal}(m) = (\mathtt{DEM}(\tau, m), \tau \parallel H(\mathtt{DEM}(\tau, m)))$ *where τ is a nonce, $\mathtt{DEM}$ is a one time encryption scheme (ind-pa), and H is a CRHF;*
3. $\mathtt{Open}(h,b) = \mathtt{DEM}^{-1}(\tau, h)$ *if $b = \tau \parallel t$ and $H(h) = t$, $\perp$ otherwise.*

Authenticated encryption scheme transformation.
Let $\mathcal{AE} = (\mathtt{AG}, \mathtt{AK}, \mathtt{AE}, \mathtt{AD})$ be a $\mathtt{1}{\rightarrow}\mathtt{1}$ authenticated encryption scheme working on small messages and $\mathcal{C} = (\mathtt{Setup}, \mathtt{Conceal}, \mathtt{Open})$ be a concealment scheme. The $\mathtt{1}{\rightarrow}\mathtt{1}$ authenticated encryption scheme working on long messages is defined by $\mathcal{AE}' = (\mathtt{AG}', \mathtt{AK}', \mathtt{AE}', \mathtt{AD}')$ where:

1. $\mathtt{AG}'(1^k)$ outputs $\mathcal{I} = (\mathcal{I}_0, ck)$ where $\mathcal{I}_0 \leftarrow \mathtt{AG}(1^k)$ and $ck \leftarrow \mathtt{Setup}(1^k)$;
2. $\mathtt{AK}'(\mathcal{I})$ outputs (sk, pk) where $(sk, pk) \leftarrow \mathtt{AK}(\mathcal{I}_0)$;
3. $\mathtt{AE}'_{sk_A}(pk_B, m)$ outputs (pk_A, h, c) where $(h,b) \leftarrow \mathtt{Conceal}_{ck}(m)$ and $(pk_A, c) \leftarrow \mathtt{AE}_{sk_A}(pk_B, b)$;
4. $\mathtt{AD}'_{sk_B}(pk_A, h, c)$ outputs $\mathtt{Open}_{ck}(h, \mathtt{AD}_{sk_B}(pk_A, c))$.

Under the hypothesis that $\mathcal{AE}$ is a secure authenticated encryption scheme (IND-CCA2 and UF-CTXT) working on small messages, an equivalence is claimed in [11] between relaxed concealment schemes $\mathcal{C}$ and secure authenticated encryption schemes $\mathcal{AE}'$. A proof is given in a secret key setting (and so for outsider adversary) but a correct proof of the direction "authenticated encryption $\Rightarrow$ relaxed concealment" is missing. This result can be corrected by considering a super-relaxed binding property.

Super-relaxed Binding. $\mathcal{C}$ satisfies the super-relaxed binding property if for all $\mathcal{A} \in \mathcal{M}(k)$,

$$Adv^{sr-bind}_{\mathcal{C},\mathcal{A}}(k) = \Pr[\ ck \leftarrow \mathtt{Setup}(1^k), (m,s) \leftarrow \mathcal{A}_1(ck), (h,b) \leftarrow \mathtt{Conceal}_{ck}(m), \\ h' \leftarrow \mathcal{A}_2(s,h);\ \mathtt{Open}_{ck}(h',b) \neq \perp] < 1/p(k).$$

The existence of super-relaxed concealment schemes can be shown from the existence of concealment schemes that satisfy the hiding property (see appendix A for the proof) with the following example.

Example 2 (Super-relaxed concealment scheme) *$\mathcal{C}$ is defined by:*

1. *$\mathtt{Setup}(1^k) = \emptyset$;*
2. *$\mathtt{Conceal}(m) = (\mathtt{DEM}(\tau, m), \tau \parallel \mathcal{H}_y(\mathtt{DEM}(\tau, m)) \parallel y)$ where τ and y are nonces, $\mathtt{DEM}$ is a one time encryption scheme (ind-pa), and $\mathcal{H}$ is an universal hash function;*
3. *$\mathtt{Open}(h, b) = \mathtt{DEM}^{-1}(\tau, h)$ if $b = \tau \parallel t \parallel y$ and $\mathcal{H}_y(h) = t$, $\perp$ otherwise.*

The theorem 1 shows that a super-relaxed concealment is sufficient (and necessary) to obtain an authenticated encryption scheme secure against outsider adversary.

Theorem 1 *Let $\mathcal{AE}$ be a $\mathtt{1}{\rightarrow}\mathtt{1}$ authenticated encryption scheme for short messages secure against outsider adversary (O-IND-CCA2 and O-UF-CTXT). $\mathcal{C}$ is a super-relaxed concealment scheme iff $\mathcal{AE}'$ is a $\mathtt{1}{\rightarrow}\mathtt{1}$ authenticated encryption scheme secure against outsider adversary (O-IND-CCA2 and O-UF-CTXT).*

In fact, in a public key setting, we can show that a relaxed concealment scheme is equivalent to an authenticated encryption scheme secure against insider adversary.

Theorem 2 *Let $\mathcal{AE}$ be a $\mathtt{1}{\rightarrow}\mathtt{1}$ authenticated encryption scheme for short messages secure against insider adversary (I-IND-CCA2 and I-UF-CTXT). $\mathcal{C}$ is a relaxed concealment scheme iff $\mathcal{AE}'$ is a $\mathtt{1}{\rightarrow}\mathtt{1}$ authenticated encryption scheme secure against insider adversary (I-IND-CCA2 and I-UF-CTXT).*

Concrete security statements are given for these two theorems in Appendix B.1 and B.2.

3 $\mathtt{1}{\rightarrow}\mathtt{n}$ Authenticated encryption schemes

3.1 Definitions

We define in this section authenticated public key encryption schemes used in order to encrypt one message for n recipients and called $\mathtt{1}{\rightarrow}\mathtt{n}$ schemes. We define then security properties for such schemes.

Definition 4 ($\mathtt{1}{\to}\mathtt{n}$ Authenticated encryption) *We define a $\mathtt{1}{\to}\mathtt{n}$ authenticated encryption scheme $\mathcal{AM} = (\mathit{GM}, \mathit{KM}, \mathit{EM}, \mathit{DM})$ by four polynomial-time (in k) algorithms:*

1. *GM a general randomized setup algorithm that takes as input the security parameter and outputs a global information $\mathcal{I}$.*
2. *KM a randomized algorithm that takes as input the global information $\mathcal{I}$, and outputs a private key / public key pair;*
3. *EM_{sk} a randomized encryption mode, depending on the secret key sk of the sender, that takes as input a sequence PK of at most n public keys and a message m and outputs the public key of the sender and a ciphertext C;*
4. *DM_{sk} a decryption mode, depending on the secret key sk of the recipient, that takes as input a public key and a ciphertext C and outputs a message m if C is valid and $\perp$ otherwise.*

The correctness requirement is that for all public key / secret key pairs, for all messages m, any encryption of m under $pk_1, \ldots, pk_n$ decrypts under sk_i (for $i \in \{1, \ldots, n\}$) to the message m. Furthermore, it is supposed in the following that sk contains pk.

As for $\mathtt{1}{\to}\mathtt{1}$ authenticated encryption schemes, indistinguability and authentication properties are required for such schemes. For the first one, we would like (for the outsider security) that no adversary except the sender A and the receivers can obtain information on the plaintext, i.e. can break the IND-CCA2 property. The difficulty to construct a secure $\mathtt{1}{\to}\mathtt{n}$ scheme comes from the authentication property. We would like (again for the outsider security) that for all user B_* (including a receiver), no adversary (outside $\{A, B_*\}$) including a recipient can output a valid ciphertext for B_* apparently from A. To our knowledge, except maybe in the specific area of identity-based cryptography (see Remark 1), no security definition has ever been published for such authenticated $\mathtt{1}{\to}\mathtt{n}$ schemes. We propose to fill this gap with the formalization of the definition 5.

In the next, we denote by $\mathcal{O}_{\mathtt{DM}_{B_i}}$ for $\mathcal{O}_{\mathtt{DM}_{B_1}}, \ldots, \mathcal{O}_{\mathtt{DM}_{B_n}}$ and $\mathcal{O}_{\mathtt{EM}_{B_i}}$ for $\mathcal{O}_{\mathtt{EM}_{B_1}}$, $\ldots, \mathcal{O}_{\mathtt{EM}_{B_n}}$. So the precision "for $i = 1, \ldots, n$" is omitted. We denote also by $C|_i$ the part of C needed to a recipient B_i to decrypt the ciphertext.

Definition 5 ($\mathtt{1}{\to}\mathtt{n}$ Outsider security) *Let $n \geq 1$, and $\{B_1, \ldots, B_n\}$ n recipients of a message m from a sender A. We say that an authenticated $\mathtt{1}{\to}\mathtt{n}$ encryption scheme $\mathcal{AM}$ is outsider-secure if:*

1. *$\mathcal{AM}$ is IND-CCA2 for all adversaries $\mathcal{A}$ outside $\{A, B_1, \ldots, B_n\}$, i.e. the advantage $Adv^{indcca2}_{\mathcal{AM},\mathcal{A}}(k)$ equals to*

$$2.\Pr[\mathcal{I} \leftarrow \mathit{GM}(1^k), (sk_A, pk_A) \leftarrow \mathit{KM}(\mathcal{I}), (sk_{B_i}, pk_{B_i}) \leftarrow \mathit{KM}(\mathcal{I}) \text{ for } i = 1, \ldots, n,$$
$$(s, m_0, m_1) \leftarrow \mathcal{A}_1^{\mathcal{O}_{\mathit{EM}_A}, \mathcal{O}_{\mathit{DM}_A}, \mathcal{O}_{\mathit{EM}_{B_i}}, \mathcal{O}_{\mathit{DM}_{B_i}}}(\mathcal{I}, pk_{B_1}, \ldots, pk_{B_n}, pk_A), \sigma \leftarrow_r \{0,1\};$$
$$\mathcal{A}_2^{\mathcal{O}_{\mathit{EM}_A}, \mathcal{O}_{\mathit{DM}_A}, \mathcal{O}_{\mathit{EM}_{B_i}}, \mathcal{O}_{\mathit{DM}_{B_i}}}(\mathcal{I}, pk_{B_1}, \ldots, pk_{B_n}, pk_A, s, C_\sigma) = \sigma] - 1$$

where $C_\sigma \leftarrow \mathtt{EM}_{sk_A}(\{pk_{B_1},\ldots,pk_{B_n}\},m_\sigma)$ *and for any* $i\in[1,n]$, $C_\sigma|_i$ *is not submitted to the oracle* $\mathcal{O}_{\mathtt{DM}_{B_i}}$, *is negligible for all* $\mathcal{A}=(\mathcal{A}_1,\mathcal{A}_2)\in\mathcal{M}(k)$,

2. $\mathcal{AM}$ *is UF-TXT for all* $B_{i_0}\in\{B_1,\ldots,B_n\}$ *and all adversaries* $\mathcal{A}$ *outside* $\{A,B_{i_0}\}$, *i.e. the advantage* $Adv^{uf-txt}_{\mathcal{AM},\mathcal{A}}(k)$ *equals to*

$$\begin{gathered}\Pr[\mathcal{I}\leftarrow \mathtt{GM}(1^k),(sk_A,pk_A)\leftarrow \mathtt{KM}(\mathcal{I}),(sk_{B_i},pk_{B_i})\leftarrow \mathtt{KM}(\mathcal{I})\ \textit{for}\ i=1,\ldots,n,\\ i_0\leftarrow_r\{1,\ldots,n\};\mathcal{A}^{\mathcal{O}_{\mathtt{EM}_A},\mathcal{O}_{\mathtt{DM}_A},\mathcal{O}_{\mathtt{EM}_{B_{i_0}}},\mathcal{O}_{\mathtt{DM}_{B_{i_0}}}}(\mathcal{I},sk_{B_{i\neq i_0}},pk_A,pk_{B_{i_0}})=C\\ /\,C=(pk_A,c)\ \textit{and}\ \mathtt{DM}_{sk_{B_{i_0}}}(pk_A,c)=m\neq\perp]\end{gathered}$$

where $C|_{i_0}$ *is not given by* $\mathcal{O}_{\mathtt{AE}_A}$ *for a request of the form* (PK_i,m_i) *where* $pk_{B_{i_0}}\in PK_i$ *(for the UF-CTXT property), or* (PK_i,m) *with* $pk_{B_{i_0}}\in PK_i$ *has not been submitted to* $\mathcal{O}_{\mathtt{AE}_A}$ *(for the UF-PTXT property), or* m *has not been submitted to* $\mathcal{O}_{\mathtt{AE}_A}$ *(for the UF-wPTXT property), is negligible for all* $\mathcal{A}\in\mathcal{M}(k)$.

For $n=1$ we have $i_0=1$ and $\{sk_{B_i}, i\neq i_0\}=\emptyset$ as in definition 2. It is also possible to define these properties for insider adversary, where $\mathcal{A}$ chooses sk_A for the indistinguability and $sk_{B_{i_0}}$ for the unforgeability. As for `1`$\longrightarrow$`1` schemes, we denote by x-UF-yTXT where $x\in\{O,I\}$ and $y\in\{wP,P,C\}$ the six interesting different definitions for the unforgeability property of a `1`$\longrightarrow$`n` scheme and x-IND-CCA2 where $x\in\{O,I\}$ the two different definitions for the confidentiality property.

We note that the outsider adversary for the unforgeability properties is much stronger for `1`$\longrightarrow$`n` schemes than for `1`$\longrightarrow$`1` schemes, since he is able to decrypt all $C|_i$ for $i\neq i_0$, and in this way obtain the possible common symmetric key.

Remark 1 *Previous informal security definitions are given in [7, 19] for identity-based* `1`$\longrightarrow$`n` *schemes. The indistinguability is defined in both cases for insider adversary in an equivalent way than here. The unforgeability is defined with two properties in [7]. The first one corresponds to the I-UF-wPTXT property. The second one looks like the O-UF-CTXT property but it is not clear if the (outsider) adversary may be another recipient. In [19] the I-UF-CTXT property is chosen.*

3.2 Authentication of a `1`$\longrightarrow$`n` scheme

An example of authenticated `1`$\longrightarrow$`n` scheme is given in the RFC1421 standard [21], destined to email applications. It uses a hybrid $\mathcal{S}t\mathcal{E}$ composition in order to send a message to several recipients. A common message-encryption key K is asymmetrically encrypted for each recipient by a sender A. These ciphertexts are then attached to the Sign-then-Encrypt message. Thus, only the message is authenticated, and it is easy for a recipient to add a new recipient B' for the same plaintext by only encrypting the key K under B''s public key. B' will believe that A sent him the message. So the scheme can only be UF-wPTXT. As suggested in [2] the identities of the recipients should be signed with the message. Even in this case, the scheme is not I-UF-CTXT since the receiver can now construct a new ciphertext by changing or re-encrypting the symmetric key. But in this case neither the message nor the recipient can change. Nevertheless it shows that in order to obtain the I-UF-PTXT property, the authentication part should depends on the message and the identity of the recipient.

Let's consider now a composition of a one-pass authenticated key exchange protocol and a KEM mechanism. We have seen in section 2.2 that this technique may achieve outsider security but not insider one. Let's suppose now that we apply this technique to the multi-recipients version of the hybrid scheme described in Fig.1, i.e. we make the function ASYM depend on the private key of the sender. As before only the symmetric key would be authenticated. To send a message m to n recipients $B_1, \ldots, B_n$ the user A sends $(C_{0,1}, \ldots, C_{0,n}, C_1 = \mathtt{DEM}(K, m))$ to all users. Then a receiver B_i could re-use the authenticated encrypted key part $C_{0,j}$ of a user B_j on another message, and send a new message to B_j apparently from A with $(C_{0,j}, C'_1 = \mathtt{DEM}(K, m'))$. Thus, this scheme can not achieve outsider security.

These examples show that, in order to obtain the stronger security property, the authentication part should depend on the symmetric key, the message to encrypt and the identity of the recipient. They show furthermore that the consequences of a theoretical attack may be more tragic in practice in a multi-recipient scheme than in a 1→1 scheme.

3.3 A 1⟶n mode of operation

We propose in this section a general mode of operation that transforms any authenticated 1→1 scheme working on small messages into an authenticated 1→n scheme working on long messages. This mode of operation makes use of an authenticated 1→1 scheme $\mathcal{AE} = (\mathtt{AG}, \mathtt{AK}, \mathtt{AE}, \mathtt{AD})$ as defined in section 2.1 and concealment schemes $\mathcal{C} = (\mathtt{Setup}, \mathtt{Conceal}, \mathtt{Open})$ as defined in section 2.3.

We define $\mathcal{AM} = (\mathtt{GM}, \mathtt{KM}, \mathtt{EM}, \mathtt{DM})$ an authenticated 1→n mode of operation for $\mathcal{AE}$ in Fig.3.

Here, we have for $i = 1, \ldots, n$, $C|_i = (pk_A, h, c_i)$. The sender has the choice, depending on the context, to send the global output $(pk_A, h, c_1, \ldots, c_{\#PK})$ to all recipients, or to send only $C|_i$ to each B_i.

Theorem 3 *If $\mathcal{C}$ is a relaxed concealment scheme, and $\mathcal{AE}$ is a secure* 1→1 *authenticated encryption scheme (x-IND-CCA2 and x-UF-yTXT where $x \in \{O, I\}$ and $y \in \{wP, P, C\}$) working on small messages, then the given construction leads to a secure* 1→n *authenticated encryption scheme (x-IND-CCA2 and x-UF-yTXT) working on long messages.*

Due to the power of the considered adversary for 1→n schemes super-relaxed concealments are not sufficient here. The proof of the theorem 3 is presented in appendix B.3. We show in particular that for $x \in \{o, i\}$ and any adversary $\mathcal{A} \in \mathcal{M}(k)$ making $q_d(.)$ decryption-oracles queries and $q_e(.)$ encryption-oracles

1. $\mathtt{GM}$ takes as input the security parameter k, computes:
   (a) $\mathcal{I}_0 \leftarrow \mathtt{AG}(1^k)$
   (b) $ck \leftarrow \mathtt{Setup}(1^k)$
   and outputs $\mathcal{I} = (\mathcal{I}_0, ck)$
2. $\mathtt{KM}$ takes as input $\mathcal{I}$ and computes:
   (a) $(sk, pk) \leftarrow \mathtt{AK}(\mathcal{I})$ for each user
3. Encryption: $\mathtt{EM}_{sk_A}$ takes as input a message m and a set PK of public keys with $\#PK \in \{1, \dots, n\}$ and computes:
   (a) $(h, b) \leftarrow \mathtt{Conceal}_{ck}(m)$
   (b) $(pk_A, c_i) \leftarrow \mathtt{AE}_{sk_A}(pk_{B_i}, b)$ for $pk_{B_i} \in PK$
   and outputs $(pk_A, h, c_1, \dots, c_{\#PK})$
4. Decryption: each owner of sk_{B_i} recovers the message m with $\mathtt{DM}_{sk_{B_i}}$:
   (a) $\mathtt{AD}_{sk_{B_i}}(pk_A, c_i) = b$
   (b) outputs $\mathtt{Open}_{ck}(h, b) = m$ or $\perp$

Fig. 3. Mode of operation $\mathcal{AM}$

queries, there exist $\mathcal{B}, \mathcal{B}', \mathcal{B}'' \in \mathcal{M}(k)^3$ whose running times are essentially the same as that of $\mathcal{A}$ such that for all k

$$Adv_{\mathcal{AM},\mathcal{A}}^{x-indcca2}(k) \leq 2.q_d(k).Adv_{\mathcal{C},\mathcal{B}}^{r-bind}(k) + 2n.Adv_{\mathcal{AE},\mathcal{B}'}^{x-indcca2}(k) + Adv_{\mathcal{C},\mathcal{B}''}^{hid}(k) + \frac{2}{2^{l_b}},$$

where $\mathcal{B}'$ makes at most $n.q_d(k)$ decryption-oracles queries and $n.q_e(k)$ encryption-oracles queries. In the same way, we can show that

$$Adv_{\mathcal{AM},\mathcal{A}}^{x-uf-ctxt}(k) \leq q_e(k).Adv_{\mathcal{C},\mathcal{B}}^{r-bind}(k) + Adv_{\mathcal{AE},\mathcal{B}'}^{x-uf-ctxt}(k),$$

$$Adv_{\mathcal{AM},\mathcal{A}}^{x-uf-(w)ptxt}(k) \leq 2q_e(k).Adv_{\mathcal{C},\mathcal{B}}^{r-bind}(k) + Adv_{\mathcal{AE},\mathcal{B}'}^{x-uf-(w)ptxt}(k),$$

where, in both cases, $\mathcal{B}'$ makes at most $q_d(k)$ decryption-oracles queries and $q_e(k)$ encryption-oracles queries.

3.4 An efficient instantiation

In [31] the author proposes that in order to send a message m to several recipients the scheme described in Fig.4. We denote by $\mathtt{SC}'$ the signcryption scheme used in the mode. $\mathtt{SC}'$ is the $\mathtt{SC}$ function of Fig. 2 where the step 5 is changed. In this construction, the authenticated part depends on both the message m (and the identity of the receiver) and the symmetric key K. It was compared in [31] to the RFC1421 [21] (which is not obsolete) and seems to be more efficient. Nevertheless, it was proposed without proof of security.

We replace in the mode of operation, given in section 3.3, the general authenticated $\mathtt{1}{\rightarrow}\mathtt{1}$ encryption scheme by a signcryption scheme and the general concealment scheme by the example given [11] and described in the example 1.

Zheng's construction.	New construction.
Input : m 1. $K \leftarrow_r \{0,1\}^{l_K}$ 2. $c = \mathtt{DEM}(K, m \parallel \mathcal{H}_K(m))$ 3. $M = m \parallel \mathcal{H}_K(m)$ 4. for each receiver: $(pk_A, h_i, \sigma_i, c_i) = \mathtt{SC}'_{sk_A}(pk_{B_i}, M)$ where $c_i = \mathtt{DEM}(K_2, K)$ Output: $(pk_A, c, h_1, \sigma_1, c_1, \ldots, h_n, \sigma_n, c_n)$	Input : m 1. $K \leftarrow_r \{0,1\}^{l_K}$ 2. $c = \mathtt{DEM}(K, m)$ 3. $M = K \parallel \mathcal{H}(c)$ 4. for each receiver: $(pk_A, h_i, \sigma_i, c_i) = \mathtt{SC}_{sk_A}(pk_{B_i}, M)$ where $c_i = \mathtt{DEM}(K_2, M)$ Output : $(pk_A, c, h_1, \sigma_1, c_1, \ldots, h_n, \sigma_n, c_n)$

Fig. 4. Comparison between two signcryption modes

We obtain for the encryption function $\mathtt{EM}_{sk_A}$ the construction of Fig.4, compared to the construction of Zheng given in [31].

In both cases, the cost is $(n+1)$ computations of a DEM function, 1 computation of a hash function and n computations of signcryption functions. But if we look at the length of data, we see that in the new construction the message to be signed for each receiver is much smaller. This implies only 2 processings of long data instead of $n + 2$.

From the theorem 3 and the security of the concealment scheme proved in [11], we obtain that the new construction is secure in the sense of the definition 5 for all secure SC in the sense of the definition 2.

4 Conclusion and further work

We showed that the concealment primitive has another interesting application in authenticated encryption. It allows us to define a secure and efficient mode of authenticated encryption schemes when used to send a message to several recipients. A further work would be first to prove the currently proposed authenticated $\mathtt{1}\rightarrow\mathtt{1}$ schemes in the security model described in this paper. Next we could see if we can gain in efficiency in the instantiation by choosing an authenticated scheme $\mathcal{AE}$ that is not necessarily secure against insider adversaries (as a signcryption scheme) and which does not use a symmetric encryption scheme since we just need to encrypt a small message. Finally we note that the mode of operation could take as input any authenticated encryption mode that sends one small message to n recipients. In [5] it is shown that many $\mathtt{1}\rightarrow\mathtt{1}$ schemes can be transformed into efficient (unauthenticated) $\mathtt{m}\rightarrow\mathtt{n}$ schemes (for $\mathtt{m} \geq 1$) by re-using the same randomness for the n recipients. In [19] an example is given that shows it is possible to use this technique in an authenticated encryption scheme. A general extension of the results of [5] would thus be very useful for authenticated $\mathtt{1}\rightarrow\mathtt{n}$ schemes.

Acknowledgements. The author would like to thank Yevgeniy Dodis for his contribution on super-relaxed concealment schemes.

References

1. J. H. An. Authenticated encryption in the public-key setting: Security notions and analyses. Cryptology Eprint Archive. http://eprint.iacr.org/2001/079, 2001.
2. J. H. An, Y. Dodis, and T. Rabin. On the security of joint signature and encryption. In *Advances in Cryptology - Eurocrypt'02*, LNCS. Springer-Verlag, 2002.
3. J. Baek, R. Steinfeld, and Y. Zheng. Formal proofs for the security of signcryption. In *Advances in Cryptology–PKC'02*, LNCS. Springer-Verlag, 2002.
4. F. Bao and R. H. Deng. A signcryption scheme with signature directly verifiable by public key. In *Advances in Cryptology—PKC'98*, LNCS. Springer-Verlag, 1998.
5. M. Bellare, A. Boldyreva, and J. Staddon. Multi-recipient encryption schemes: Security notions and randomness re-use. In *Advances in Cryptology - PKC'03*, LNCS. Springer-Verlag, 2003.
6. M. Bellare and C. Namprempre. Authenticated encryption: Relations among notions and analysis of the generic composition paradigm. In *Advances in Cryptology - Asiacrypt'00*, LNCS. Springer-Verlag, 2000.
7. X. Boyen. Multipurpose identity-based signcryption. a swiss army knife for identity-based cryptography. In *Advances in Cryptology - CRYPTO'03*, LNCS. Springer-Verlag, 2003.
8. J. L. Carter and M. N. Wegman. Universal classes of hash functions. *Journal of Computer and System Sciences*, 18, 1978.
9. R. Cramer and V. Shoup. Design and analysis of practical public key encryption schemes secure against adaptative chosen ciphertext attack. Cryptology Eprint Archive. http://eprint.iacr.org/2001/108, 2001.
10. A. Dent. Hybrid cryptography. Cryptology Eprint Archive. http://eprint.iacr.org/2004/210, 2004.
11. Y. Dodis and J. An. Concealment and its applications to authenticated encryption. In *Advances in Cryptology - Eurocrypt'03*, LNCS. Springer-Verlag, 2003.
12. Y. Dodis, M. J. Freedman, S. Jarecki, and S. Walfish. Versatile padding schemes for joint signature and encryption. In *Eleventh ACM Conference on Computer and Communication Security*. ACM, 2004.
13. A. Fiat and M. Naor. Broadcast encryption. In *Advances in Cryptology - Crypto'93*, LNCS. Springer-Verlag, 1993.
14. S. Goldwasser, S. Micali, and R. Rivest. A digital signature scheme secure against adaptative chosen message attacks. *SIAM J. Computing*, 17(2), 1988.
15. D. Halevy and A. Shamir. The lsd broadcast encryption scheme. In *Advances in Cryptology - CRYPTO'02*, LNCS. Springer-Verlag, 2002.
16. W. He and T. Wu. Cryptanalysis and improvement of Petersen-Michels signcryption schemes. IEE Proc. Computers and Digital Techniques, 146(2) : 123–124, 1999.
17. P. Horster, M. Michels, and H. Petersen. Authenticated encryption schemes with low communication costs. Technical Report TR-94-2-R, University of Technology, Chemnitz-Zwickau, 1994. appeared in Electronic Letters, Vol. 30, No. 15, 1994.
18. R. Impagliazzo and M. Luby. One-way functions are essential for complexity-based cryptography. In *FOCS'89*, 1989.
19. B. Libert and J. Quisquater. The exact security of an identity based signature and its applications. Cryptology Eprint Archive. http://eprint.iacr.org/2004/102, 2004.
20. C. H. Lim and P. J. Lee. Another method for attaining security against adaptively chosen ciphertext attacks. In *Advances in Cryptology–Crypto'93*, LNCS. Springer-Verlag, 1994.

21. J. Linn. Privacy enhancement for internet electronic mail: Part 1 : Message encryption and authentification procedures. RFC 1421 IETF, 1993.
22. J. Malone-Lee. Identity-based signcryption. Cryptology Eprint Archive. http://eprint.iacr.org/2002/098, 2002.
23. J. Malone-Lee. Signcryption with non repudiation. Technical Report CSTR–02–004, Department of Computer Science. University of Bristol, 2002.
24. D. Naor, M. Naor, and J. Lotspiech. Revocation and tracing schemes for stateless receivers. In *Advances in Cryptology - Crypto'01*, LNCS. Springer-Verlag, 2001.
25. NIST. Recommendation on key establishment schemes. draft 2.0. Special publication 800-56, 2003.
26. C. Shannon. A mathematical theory of communication. *Bell Systems Technical Journal*, 27, 1948.
27. V. Shoup. Using hash functions as a hedge against chosen ciphertext attack. In *Advances in Cryptology—Eurocrypt'00*, LNCS. Springer-Verlag, 2000.
28. V. Shoup. A proposal for an ISO standard for public key encryption (version 2.1), 2001.
29. Y. Zheng. Improved public key cryptosystems secure against chosen ciphertext attacks. Technical Report tr-94-1, 1994.
30. Y. Zheng. Digital signcryption or how to achieve cost (signature & encryption << cost (signature) + cost (encryption). In *Advances in Cryptology - Crypto'97*, LNCS. Springer-Verlag, 1997.
31. Y. Zheng. Signcryption and its applications in efficient public key solutions. In *Proc. 1st International Information Security Workshop (ISW'97)*, volume 1396 of *LNCS*. Springer-Verlag, 1997.
32. Y. Zheng and J. Seberry. Immunizing public key cryptosystems against chosen ciphertext attacks. *IEEE Journal on Selected Areas in Communications*, 11(5), 1993.

A On super-relaxed concealment

It is known that if two users A and B have a public channel and a secret channel, then if A wants to transmit a message of length k securely to B, A must send k bits over the secret channel or else one-way functions exist (see [26, 18]). Thus, from theorem 1 non-trivial super-relaxed concealments imply one-way functions. Furthermore, consider a Wegman-Carter [8] universal hash function $\mathcal{H}$ from $\{0,1\}^{2\mu(k)} \times \{0,1\}^k$ to $\{0,1\}^{\nu(k)}$. For a fixed $y \in \{0,1\}^{2\mu(k)}$ we view $\mathcal{H}(y,x)$ as a function $\mathcal{H}_y(x)$ of x that maps k bits to $\nu(k)$ bits. This function satisfies : if $Y \leftarrow_r \{0,1\}^{2\mu(k)}$ then for all $x \in \{0,1\}^k, x' \in \{0,1\}^k \setminus \{x\}$, and for all $a, a' \in \{0,1\}^{\nu(k)}$,

$$\Pr_Y[(\mathcal{H}_Y(x) = a) \text{ and } (\mathcal{H}_Y(x') = a')] = 1/2^{2\nu(k)}.$$

This function can be constructed unconditionally. We can indeed define $\mathcal{H}_y(x) = (y_1 x + y_2)_{\{1,\ldots,\nu(k)\}}$ where $y = (y_1, y_2)$, y_i are considered as elements of $GF(2^{\mu(k)})$ and $\mu(k) = \max(\nu(k), k)$. Then, we have the following result.

Lemme 1 *Let $\mathcal{C} = (\texttt{Setup}, \texttt{Conceal}, \texttt{Open})$ be a concealment scheme that satisfies the hiding property. Let $\mathcal{H}$ be an universal hash function as described above with $k = |h|$. Then, the concealment scheme $\mathcal{C}'$ defined by :*

1. $\texttt{Setup}'(1^k) = \texttt{Setup}(1^k) = ck$;
2. $\texttt{Conceal}'_{ck}(m) = (h, b \parallel \mathcal{H}_y(h) \parallel y)$ *where* $y \leftarrow_r \{0,1\}^{2\mu(k)}$ *and* $(h, b) \leftarrow \texttt{Conceal}_{ck}(m)$;
3. $\texttt{Open}'_{ck}(h', b') = \perp$ *if* $\mathcal{H}_y(h') \neq t$ *with* $b' = b \parallel t \parallel y$, *or* $\texttt{Open}_{ck}(h, b)$ *otherwise;*

is a super-relaxed concealment scheme.

Proof. Since $\mathcal{C}$ is hiding, $\mathcal{C}'$ is hiding too. Supposing $\mathcal{C}'$ is not super-relaxed binding, we have an adversary that receives h and outputs h' such that $\mathcal{H}_y(h) = \mathcal{H}_y(h')$ for an $\mathcal{H}_y$ never seen by the adversary. ∎

B Proofs

We use in all proofs the following well-known lemma.

Lemme 2 *Let* E, E' *and* F *be three events defined in some probability distribution such that* $\Pr[E \,\&\, \overline{F}] = \Pr[E' \,\&\, \overline{F}]$. *Then,*

$$|\Pr[E] - \Pr[E']| \leq \Pr[F].$$

B.1 Proof of theorem 1

Definition 6 (Relaxed* binding) *We say that* $\mathcal{C}$ *satisfies the property Relaxed* Binding if the advantage*

$$\begin{aligned} Adv^{r^*-bind}_{\mathcal{C},\mathcal{A}}(k) = \Pr[&\mathcal{I}_0 \leftarrow \texttt{AG}(1^k), (sk_A, pk_A) \leftarrow \texttt{AK}(\mathcal{I}_0), (sk_B, pk_B) \leftarrow \texttt{AK}(\mathcal{I}_0),\\ &ck \leftarrow \texttt{Setup}(1^k); \mathcal{A}_1^{\mathcal{O}_{\texttt{AE}_A}, \mathcal{O}_{\texttt{AE}_B}, \mathcal{O}_{\texttt{AD}_A}, \mathcal{O}_{\texttt{AD}_B}}(\mathcal{I}_0, pk_B, pk_A, ck) = (m, s),\\ &(h, b) \leftarrow \texttt{Conceal}_{ck}(m), c = \texttt{AE}_{sk_A}(pk_B, b);\\ &h' \leftarrow \mathcal{A}_2^{\mathcal{O}_{\texttt{AE}_A}, \mathcal{O}_{\texttt{AE}_B}, \mathcal{O}_{\texttt{AD}_A}, \mathcal{O}_{\texttt{AD}_B}}(s, h, c) \,/\, \texttt{Open}_{ck}(h', b) \neq \perp] \end{aligned}$$

where c *cannot be submitted to* $\mathcal{O}_{\texttt{AD}_B}$, *is negligible for any* $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2) \in \mathcal{M}(k)$.

Lemme 3 *For any adversary* $\mathcal{A} \in \mathcal{M}(k)$ *making* $q_d(.)$ *decryption-oracles queries and* $q_e(.)$ *encryption-oracles queries, there exist* $\mathcal{B}, \mathcal{B}' \in \mathcal{M}(k)^2$ *whose running times are essentially the same as that of* $\mathcal{A}$ *such that for all* k

$$Adv^{r^*-bind}_{\mathcal{C},\mathcal{A}}(k) \leq Adv^{o-indcca2}_{\mathcal{AE},\mathcal{B}}(k) + Adv^{sr-bind}_{\mathcal{C},\mathcal{B}'}(k) + \frac{1}{2^{l_b}}$$

where $\mathcal{B}$ *makes at most* $q_d(k)$ *decryption-oracles queries and* $q_e(k)$ *encryption-oracles queries.*

Proof. Let's fix a security parameter and an adversary $\mathcal{A}$ on the relaxed* binding property. We modify his game by giving him $c = \texttt{AE}_{sk_A}(pk_B, r_1)$ where $r_1 \leftarrow_r \{0,1\}^{l_b} \setminus \{b\}$ instead of $c = \texttt{AE}_{sk_A}(pk_B, b)$. We construct an adversary $\mathcal{B}$ on the O-IND-CCA2 property as follows. $\mathcal{B}^{\mathcal{O}_{\texttt{AE}_A}, \mathcal{O}_{\texttt{AE}_B}, \mathcal{O}_{\texttt{AD}_A}, \mathcal{O}_{\texttt{AD}_B}}(\mathcal{I}_0, pk_A, pk_B)$ chooses ck and runs $\mathcal{A}_1^{\mathcal{O}_{\texttt{AE}_A}, \mathcal{O}_{\texttt{AE}_B}, \mathcal{O}_{\texttt{AD}_A}, \mathcal{O}_{\texttt{AD}_B}}(\mathcal{I}_0, pk_B,\ pk_A, ck)$ who outputs (m, s). Then $\mathcal{B}$

constructs $\texttt{Conceal}_{ck}(m) = (h, b)$, outputs (b, r_1) where $r_1 \leftarrow_r \{0,1\}^{l_b} \setminus \{b\}$ and receives $c^* = \texttt{AE}_{sk_A}(pk_B, b)$ or $\texttt{AE}_{sk_A}(pk_B, r_1)$. Then $\mathcal{B}$ runs $\mathcal{A}_2^{\mathcal{O}_{\texttt{AE}_A}, \mathcal{O}_{\texttt{AE}_B}, \mathcal{O}_{\texttt{AD}_A}, \mathcal{O}_{\texttt{AD}_B}}$ (s, h, c^*) who outputs h'. If $\texttt{Open}_{ck}(b, h') \neq \perp$ $\mathcal{B}$ returns b, else $\mathcal{B}$ returns r_1. $\mathcal{B}$ can simulate oracles for $\mathcal{A}$ with his own oracles. We have $Adv^{o-indcca2}_{\texttt{AE},\mathcal{B}}(k) = |\Pr[\mathcal{B} \rightarrow b/b] - \Pr[\mathcal{B} \rightarrow b/0]| = |\Pr[\mathcal{A}/\text{game } 0] - \Pr[\mathcal{A}/\text{game } 1]|$.

Then, we can show that there exists $\mathcal{B}'$ on the super-relaxed property. $\mathcal{B}'(ck)$ generates $\mathcal{I}_0$ and keys for A and B, and runs $\mathcal{A}_1^{\mathcal{O}_{\texttt{AE}_A}, \mathcal{O}_{\texttt{AE}_B}, \mathcal{O}_{\texttt{AD}_A}, \mathcal{O}_{\texttt{AD}_B}}(\mathcal{I}_0, pk_B, pk_A, ck)$ who outputs (m, s). $\mathcal{B}'$ outputs m and receives h where $(h, b) = \texttt{Conceal}_{ck}(m)$. Then $\mathcal{B}'$ constructs $c = \texttt{AE}_{sk_A}(pk_B, r_1)$ where $r_1 \leftarrow_r \{0,1\}^{l_b}$ and runs $\mathcal{A}_2^{\mathcal{O}_{\texttt{AE}_A}, \mathcal{O}_{\texttt{AE}_B}, \mathcal{O}_{\texttt{AD}_A}, \mathcal{O}_{\texttt{AD}_B}}(s, h, c)$ who outputs h'. $\mathcal{B}'$ outputs h'. Oracles can be simulated with sk_A and sk_B. Since $\Pr[r_1 = b] = 1/2^{l_b}$ we have:
$\Pr[\mathcal{B}'] = \Pr[\mathcal{A}/\text{game } 1] - 1/1^{l_b}$. ∎

Lemme 4 *For any adversary $\mathcal{A} \in \mathcal{M}(k)$ making $q_d(.)$ decryption-oracles queries and $q_e(.)$ encryption-oracles queries, there exist $\mathcal{B}, \mathcal{B}', \mathcal{B}'' \in \mathcal{M}(k)^3$ whose running times are essentially the same as that of $\mathcal{A}$ such that for all k*

$$Adv^{o-indcca2}_{\mathcal{AE}',\mathcal{A}}(k) \leq 2.q_d(k).Adv^{r^*-bind}_{\mathcal{C},\mathcal{B}}(k) + 2.Adv^{o-indcca2}_{\mathcal{AE},\mathcal{B}'}(k) + \frac{2}{2^{l_b}} + Adv^{hid}_{\mathcal{C},\mathcal{B}''}(k)$$

where $\mathcal{B}$ and $\mathcal{B}'$ make at most $q_d(k)$ decryption-oracles queries and $q_e(k)$ encryption-oracles queries.

Proof. Let's fix a security parameter and an adversary $\mathcal{A}$ on the O-IND-CCA2 property of $\mathcal{AE}'$. The game of $\mathcal{A}$ is:

Game 0:
1. $\mathcal{I} \leftarrow \texttt{AG}'(1^k)$,
2. $(sk_A, pk_A) \leftarrow \texttt{AK}'(\mathcal{I})$,
3. $(sk_B, pk_B) \leftarrow \texttt{AK}'(\mathcal{I})$,
4. $\mathcal{A}_1^{\mathcal{O}_{\texttt{AD}'_B}, \mathcal{O}_{\texttt{AE}'_B}, \mathcal{O}_{\texttt{AD}'_A}, \mathcal{O}_{\texttt{AE}'_A}}(\mathcal{I}, pk_B, pk_A) = (s, m_0, m_1)$,
5. $\sigma \leftarrow \{0,1\}$,
6. $\texttt{Conceal}_{ck}(m_\sigma) = (h_\sigma, b_\sigma)$,
7. $c_\sigma = \texttt{AE}_{sk_A}(pk_B, b_\sigma)$,
8. $\mathcal{A}_2^{\mathcal{O}_{\texttt{AD}'_B}, \mathcal{O}_{\texttt{AE}_B}, \mathcal{O}_{\texttt{AD}'_A}, \mathcal{O}_{\texttt{AE}'_A}}(\mathcal{I}, pk_B, pk_A, s, c_\sigma, h_\sigma) = \sigma'$.

Where oracles are defined as real algorithms.

Game 1: We modify the game 0 as follows. When $\mathcal{A}_2$ makes a request to $\mathcal{O}_{\texttt{AD}'_B}$, if $c = c_\sigma$ return $\perp$. The probability to return $\perp$ instead of m is equal to the probability to have $\texttt{Open}_{ck}(h, b_\sigma) \neq \perp$ with $h \neq h_\sigma$. We can in this case construct an adversary $\mathcal{B}$ on the relaxed* binding property. $\mathcal{B}^{\mathcal{O}_{\texttt{AD}_B}, \mathcal{O}_{\texttt{AE}_B}, \mathcal{O}_{\texttt{AD}_A}, \mathcal{O}_{\texttt{AE}_A}}(\mathcal{I}_0, pk_A, pk_B, ck)$ runs $\mathcal{A}_1^{\mathcal{O}_{\texttt{AD}'_B}, \mathcal{O}_{\texttt{AE}'_B}, \mathcal{O}_{\texttt{AD}'_A}, \mathcal{O}_{\texttt{AE}'_A}}(\mathcal{I}, pk_B, pk_A)$ who outputs (s, m_0, m_1), chooses $\sigma \leftarrow \{0,1\}$ and outputs m_σ. Then $\mathcal{B}$ receives (h_σ, c_σ), and runs $\mathcal{A}_2^{\mathcal{O}_{\texttt{AD}'_B}, \mathcal{O}_{\texttt{AE}'_B}, \mathcal{O}_{\texttt{AD}'_A}, \mathcal{O}_{\texttt{AE}'_A}}(\mathcal{I}, pk_B, pk_A, s, c_\sigma, h_\sigma)$ who outputs σ'. $\mathcal{B}$ can simulate oracles for $\mathcal{A}$ with his own oracles except for the request (c_σ, h). So he just has to wait for the request (c_σ, h) and returns h. So we have $|\Pr[\mathcal{A}/\text{Game 0}] - \Pr[\mathcal{A}/\text{Game 1}]| \leq q_d(k). \Pr[\mathcal{B}]$.

Game 2: We replace in game 1 c_σ by $c_\sigma = \mathtt{AE}_{sk_A}(pk_B, r_1)$ where $r_1 \leftarrow_r \{0,1\}^{l_b} \setminus b_\sigma$. We construct an adversary $\mathcal{B}'$ on the O-IND-CCA2 property of $\mathcal{AE}$. First $\mathcal{B}'^{\mathcal{O}_{\mathtt{AD}_B}, \mathcal{O}_{\mathtt{AE}_B}, \mathcal{O}_{\mathtt{AD}_A}, \mathcal{O}_{\mathtt{AE}_A}}(\mathcal{I}_0, pk_B, pk_A)$ generates ck and runs $\mathcal{A}_1^{\mathcal{O}_{\mathtt{AD}'_B}, \mathcal{O}_{\mathtt{AE}'_B}, \mathcal{O}_{\mathtt{AD}'_A}, \mathcal{O}_{\mathtt{AE}'_A}}(\mathcal{I}, pk_B, pk_A)$ who outputs (s, m_0, m_1). Then $\mathcal{B}'$ chooses $\sigma \leftarrow_r \{0,1\}$, constructs $\mathtt{Conceal}_{ck}(m_\sigma) = (h_\sigma, b_\sigma)$ chooses $r_1 \leftarrow_r \{0,1\}^{l_b} \setminus b_\sigma$ and outputs (r_1, b_σ). $\mathcal{B}'$ receives $c^* = \mathtt{AE}_{sk_A}(pk_B, r_1)$ or $c^* = \mathtt{AE}_{sk_A}(pk_B, b_\sigma)$ and runs $\mathcal{A}_2^{\mathcal{O}_{\mathtt{AD}'_B}, \mathcal{O}_{\mathtt{AE}'_B}, \mathcal{O}_{\mathtt{AD}'_A}, \mathcal{O}_{\mathtt{AE}'_A}}$ $(\mathcal{I}, pk_B, pk_A, s, c^*, h_\sigma)$ who outputs σ'. If $\sigma' = \sigma$ then $\mathcal{B}'$ outputs b_σ else $\mathcal{B}'$ outputs r_1. Thanks to the modification made in game 1, $\mathcal{B}'$ can simulate oracles for $\mathcal{A}$ with his own oracles ans we have $|\Pr[\mathcal{A}/\text{Game 1}] - \Pr[\mathcal{A}/\text{Game 2}]| \leq Adv^{o-indcca2}_{\mathcal{AE},\mathcal{B}'}(k)$.

In the last game the only link between (m_0, m_1) and the challenge is given by h_σ. We construct an adversary $\mathcal{B}''$ on the hiding property as follows. $\mathcal{B}''(ck)$ generates $\mathcal{I}_0$, keys for A and B and runs $\mathcal{A}_1^{\mathcal{O}_{\mathtt{AD}'_B}, \mathcal{O}_{\mathtt{AE}'_B}, \mathcal{O}_{\mathtt{AD}'_A}, \mathcal{O}_{\mathtt{AE}'_A}}(\mathcal{I}, pk_B, pk_A)$ who outputs (s, m_0, m_1). $\mathcal{B}''$ outputs (s, m_0, m_1) and receives h_σ where $\sigma \leftarrow_r \{0,1\}$ and $(h_\sigma, b_\sigma) \leftarrow \mathtt{Conceal}(m_\sigma)$. Finally $\mathcal{B}''$ constructs $c^* = \mathtt{AE}_{sk_A}(pk_B, r_1)$ where $r_1 \leftarrow_r \{0,1\}^{l_b}$ and runs $\mathcal{A}_2^{\mathcal{O}_{\mathtt{AD}'_B}, \mathcal{O}_{\mathtt{AE}'_B}, \mathcal{O}_{\mathtt{AD}'_A}, \mathcal{O}_{\mathtt{AE}'_A}}(\mathcal{I}, pk_B, pk_A, s, c^*, h_\sigma)$ who outputs σ', Then, $\mathcal{B}''$ outputs σ'. $\mathcal{B}$ can simulate oracles for $\mathcal{A}$ with sk_A anf sk_B. Since $\Pr[r_1 = b_\sigma] = \frac{1}{2^{l_b}}$ we have $\Pr[\mathcal{A}/\text{game 2}] = \Pr[\mathcal{B}''] + \frac{1}{2^{l_b}}$. ∎

Lemme 5 *For any adversary $\mathcal{A} \in \mathcal{M}(k)$ making $q_d(.)$ decryption-oracles queries and $q_e(.)$ encryption-oracles queries, there exist $\mathcal{B}, \mathcal{B}' \in \mathcal{M}(k)^2$ whose running times are essentially the same as that of $\mathcal{A}$ such that for all k*

$$Adv^{o-uf-ctxt}_{\mathcal{AE}',\mathcal{A}}(k) \leq q_e(k).Adv^{r^*-bind}_{\mathcal{C},\mathcal{B}}(k) + Adv^{o-uf-ctxt}_{\mathcal{AE},\mathcal{B}'}(k)$$

where $\mathcal{B}$ and $\mathcal{B}'$ make at most $q_d(k)$ decryption-oracles queries and $q_e(k)$ encryption-oracles queries.

Proof. Let's fix a security parameter and an adversary $\mathcal{A}$ on the O-UF-CTXT property of $\mathcal{AE}'$ which succeed in the following game.

Game 0:
1. $\mathcal{I} \leftarrow \mathtt{AG}'(1^k)$,
2. $(sk_A, pk_A) \leftarrow \mathtt{AK}'(\mathcal{I})$,
3. $(sk_B, pk_B) \leftarrow \mathtt{AK}'(\mathcal{I})$,
4. $\mathcal{A}^{\mathcal{O}_{\mathtt{AE}'_A}, \mathcal{O}_{\mathtt{AE}'_B}, \mathcal{O}_{\mathtt{AD}'_A}, \mathcal{O}_{\mathtt{AD}'_B}}(\mathcal{I}, pk_B, pk_A) = (c, h)$,
5. $\mathcal{A}$ succeeds if $\mathtt{AD}'_{sk_B}(pk_A, c, h) = m \neq \perp$ and (c, h) is not returned by $\mathcal{O}_{\mathtt{AE}'_A}$ for a request of the type (pk_B, m_i).

Where oracles are defined as real algorithms.

Let's denote by (m_i, pk_i) the ith request to $\mathcal{O}_{\mathtt{AE}'_A}$, and (pk_A, c_i, h_i) the answer. Let E be the event that $(c, pk_B) = (c_i, pk_i)$ for one $i \in [1, q_e]$. We have $\Pr[\mathcal{A}] = \Pr[\mathcal{A}/E]. \Pr[E] + \Pr[\mathcal{A}/\overline{E}]. \Pr[\overline{E}]$ where $\Pr[\mathcal{A}/E] = \Pr[\mathcal{A} \rightarrow (c_i, h)/h \neq h_i$ &

$\mathtt{Open}_{ck}(h, \mathtt{AD}_{sk_B}(pk_A, c_i)) \neq \bot]$. In case where the event E happens, we construct an adversary $\mathcal{B}$ on relaxed* binding as follows. $\mathcal{B}^{\mathcal{O}_{\mathtt{AD}_B}, \mathcal{O}_{\mathtt{AE}_B}, \mathcal{O}_{\mathtt{AD}_A}, \mathcal{O}_{\mathtt{AE}_A}}(\mathcal{I}_0, ck, pk_A, pk_B)$ chooses $i_0 \leftarrow \{1, \ldots q_e\}$ and runs $\mathcal{A}^{\mathcal{O}_{\mathtt{AE}'_A}, \mathcal{O}_{\mathtt{AE}'_B}, \mathcal{O}_{\mathtt{AD}'_A}, \mathcal{O}_{\mathtt{AD}'_B}}(\mathcal{I}, pk_B,\ pk_A)$ who outputs (c, h). The oracle $\mathcal{O}_{\mathtt{AE}'_A}(pk, m_i)$ is simulated as follows. If $i \neq i_0$ then $\mathcal{B}$ proceed as in the real algorithm. Else, $\mathcal{B}$ outputs m_{i_0}, receives (c_{i_0}, h_{i_0}), and return (c_{i_0}, h_{i_0}). $\mathcal{B}$ simulates the other oracles of $\mathcal{A}$ with his own oracles except for the decryption request (c_{i_0}, h_i) to $\mathcal{O}_{\mathtt{AD}'_B}$ where c_{i_0} cannot be submitted to $\mathcal{O}_{\mathtt{AD}_B}$. For this request, if $h = h_{i_0}$ then $\mathcal{B}$ returns m_{i_0}, else $\mathcal{B}$ returns $\bot$. We can suppose that the event to output $\bot$ instead of a message m_i does not happen since we can show that there exists another adversary $\mathcal{A}'$ (better than $\mathcal{A}$) that do not make this request. With probability $1/q_e(k)$, $c = c_{i_0}$ and $\mathcal{B}$ returns h. So $\Pr[\mathcal{B}] = 1/q_e(k). \Pr[\mathcal{A}/E]$.

Then, we construct another adversary $\mathcal{B}'$ on the O-UF-CTXT property of $\mathcal{AE}$. First $\mathcal{B}'^{\mathcal{O}_{\mathtt{AE}_A}, \mathcal{O}_{\mathtt{AE}_B}, \mathcal{O}_{\mathtt{AD}_A}, \mathcal{O}_{\mathtt{AD}_B}}(\mathcal{I}_0, pk_A, pk_B)$ chooses $ck \leftarrow \mathtt{Setup}(1^k)$ and runs $\mathcal{A}^{\mathcal{O}_{\mathtt{AE}'_A}, \mathcal{O}_{\mathtt{AE}'_B}, \mathcal{O}_{\mathtt{AD}'_A}, \mathcal{O}_{\mathtt{AD}'_B}}(\mathcal{I}, pk_B, pk_A)$ who outputs (c, h). Then, $\mathcal{B}'$ outputs c. $\mathcal{O}_{\mathtt{AE}'_A}$, $\mathcal{O}_{\mathtt{AE}'_B}$, $\mathcal{O}_{\mathtt{AD}'_A}, \mathcal{O}_{\mathtt{AD}'_B}$ can be simulated with $\mathcal{O}_{\mathtt{AE}_A}$, $\mathcal{O}_{\mathtt{AE}_B}, \mathcal{O}_{\mathtt{AD}_A}, \mathcal{O}_{\mathtt{AD}_{sk_B}}$ and since we are in the case where the event E does not happen, we have $\Pr[\mathcal{B}'] = \Pr[\mathcal{A}/\overline{E}]$. ∎

Lemme 6 *For any adversary $\mathcal{A} \in \mathcal{M}(k)$, there exists $\mathcal{B} \in \mathcal{M}(k)$ whose running time is essentially the same as that of $\mathcal{A}$ such that for all k*

$$Adv^{hid}_{\mathcal{C},\mathcal{A}}(k) \leq Adv^{o-indcca2}_{\mathcal{AE}',\mathcal{B}}(k)$$

where $\mathcal{B}$ makes no decryption-oracles querie and neither encryption-oracles querie.

Proof. The proof is easy and is left to the reader. ∎

Lemme 7 *For any adversary $\mathcal{A} \in \mathcal{M}(k)$, there exists $\mathcal{B} \in \mathcal{M}(k)$ whose running time is essentially the same as that of $\mathcal{A}$ such that for all k*

$$Adv^{sr-bind}_{\mathcal{C},\mathcal{A}}(k) \leq Adv^{o-uf-ctxt}_{\mathcal{AE}',\mathcal{B}}(k)$$

where $\mathcal{B}$ makes no decryption-oracles querie and 1 encryption-oracles querie.

Proof. Let's fix a security parameter and an adversary $\mathcal{A}$ on the super-relaxed binding property. Then, we construct an adversary $\mathcal{B}$ on the O-UF-CTXT property of $\mathcal{AE}'$ in the following way. $\mathcal{B}^{\mathcal{O}_{\mathtt{AE}'_A}, \mathcal{O}_{\mathtt{AE}'_B}, \mathcal{O}_{\mathtt{AD}'_A}, \mathcal{O}_{\mathtt{AD}'_{sk_B}}}(\mathcal{I}, pk_B, pk_A)$ runs $\mathcal{A}_1(ck)$ who outputs (m, s). Then, $\mathcal{B}$ submits (pk_B, m) to his oracle $\mathcal{O}_{\mathtt{AE}'_A}$ and receives $(c = \mathtt{AE}_{sk_A}(pk_B, b), h)$ with $(h, b) = \mathtt{Conceal}_{ck}(m)$. Then $\mathcal{B}$ runs $\mathcal{A}_2(ck, s, h)$ who returns h'. $\mathcal{B}$ outputs (c, h'). ∎

B.2 Proof of theorem 2

Lemme 8 *For any adversary $\mathcal{A} \in \mathcal{M}(k)$ making $q_d(.)$ decryption-oracles queries and $q_e(.)$ encryption-oracles queries, there exist $\mathcal{B}, \mathcal{B}', \mathcal{B}'' \in \mathcal{M}(k)^3$ whose running times are essentially the same as that of $\mathcal{A}$ such that for all k*

$$Adv^{i-indcca2}_{\mathcal{AE}',\mathcal{A}}(k) \leq 2.q_d(k).Adv^{r-bind}_{\mathcal{C},\mathcal{B}}(k) + 2.Adv^{i-indcca2}_{\mathcal{AE},\mathcal{B}'}(k) + Adv^{hid}_{\mathcal{C},\mathcal{B}''}(k) + \frac{2}{2^{l_b}}$$

where $\mathcal{B}'$ makes at most $q_d(k)$ decryption-oracles queries and $q_e(k)$ encryption-oracles queries.

Proof. Let's fix a security parameter and an adversary $\mathcal{A}$ on the I-IND-CCA2 property of $\mathcal{AE}'$. The game of $\mathcal{A}$ is:

Game 0:

1. $\mathcal{I} \leftarrow \mathtt{AG}'(1^k)$,
2. $(sk_B, pk_B) \leftarrow \mathtt{AK}'(\mathcal{I})$,
3. $\mathcal{A}_1^{\mathcal{O}_{\mathtt{AD}'_B}, \mathcal{O}_{\mathtt{AE}'_B}}(\mathcal{I}, pk_B) = (s, sk_A, m_0, m_1)$,
4. $\sigma \leftarrow \{0,1\}$,
5. $\mathtt{Conceal}_{ck}(m_\sigma) = (h_\sigma, b_\sigma)$,
6. $c_\sigma = \mathtt{AE}_{sk_A}(pk_B, b_\sigma)$,
7. $\mathcal{A}_2^{\mathcal{O}_{\mathtt{AD}'_B}, \mathcal{O}_{\mathtt{AE}'_B}}(\mathcal{I}, pk_B, s, c_\sigma, h_\sigma) = \sigma'$.

Where oracles are defined as real algorithms.

Game 1: We modify the game 0 as follows. When $\mathcal{A}_2$ makes a request to $\mathcal{O}_{\mathtt{AD}'_B}$, if $c = c_\sigma$ then return $\perp$. The probability to return $\perp$ instead of m is equal to the probability to have $\mathtt{Open}_{ck}(h, b_\sigma) \neq \perp$ with $h \neq h_\sigma$. We can in this case construct an adversary $\mathcal{B}$ on the relaxed binding property. $\mathcal{B}(ck)$ generates $\mathcal{I}_0$, keys for B and runs $\mathcal{A}_1^{\mathcal{O}_{\mathtt{AD}'_B}, \mathcal{O}_{\mathtt{AE}'_B}}(\mathcal{I}, pk_B)$ who outputs (s, sk_A, m_0, m_1). Then $\mathcal{B}$ chooses $\sigma \leftarrow \{0,1\}$ and outputs m_σ. $\mathcal{B}$ receives $(b_\sigma, h_\sigma) = \mathtt{Conceal}_{ck}(m_\sigma)$, constructs $c_\sigma = \mathtt{AE}_{sk_A}(pk_B, b_\sigma)$, and runs $\mathcal{A}_2^{\mathcal{O}_{\mathtt{AD}'_B}, \mathcal{O}_{\mathtt{AE}'_B}}(\mathcal{I}, pk_B, s, c_\sigma, h_\sigma)$ who outputs σ'. $\mathcal{B}$ can simulate oracles with sk_B, so he just has to wait for the request (c_σ, h) and returns h. So we have $|\Pr[\mathcal{A}/\text{Game } 0] - \Pr[\mathcal{A}/\text{Game } 1]| \leq q_d(k). \Pr[\mathcal{B}]$.

Game 2: We replace in game 1 c_σ by $c_\sigma = \mathtt{AE}_{sk_A}(pk_B, r_1)$ where $r_1 \leftarrow_r \{0,1\}^{l_b} \setminus b_\sigma$. We construct an adversary $\mathcal{B}'$ on the I-IND-CCA2 of $\mathcal{AE}$. First $\mathcal{B}'^{\mathcal{O}_{\mathtt{AD}_B}, \mathcal{O}_{\mathtt{AE}_B}}(\mathcal{I}_0, pk_B)$ generates ck and runs $\mathcal{A}_1^{\mathcal{O}_{\mathtt{AD}'_B}, \mathcal{O}_{\mathtt{AE}'_B}}(\mathcal{I}, pk_B)$ who outputs (s, sk_A, m_0, m_1). Then $\mathcal{B}'$ constructs $\mathtt{Conceal}_{ck}(m_\sigma) = (h_\sigma, b_\sigma)$ with $\sigma \leftarrow_r \{0,1\}$,, chooses $r_1 \leftarrow_r \{0,1\}^{l_b} \setminus b_\sigma$, and outputs (sk_A, r_1, b_σ). $\mathcal{B}'$ receives $c^* = \mathtt{AE}_{sk_A}(pk_B, r_1)$ or $c^* = \mathtt{AE}_{sk_A}(pk_B, b_\sigma)$ and runs $\mathcal{A}_2^{\mathcal{O}_{\mathtt{AD}'_B}, \mathcal{O}_{\mathtt{AE}'_B}}(\mathcal{I},\ pk_B, s, c^*, h_\sigma)$ who outputs σ'. If $\sigma' = \sigma$, $\mathcal{B}'$ outputs b_σ else $\mathcal{B}'$ outputs r_1. Thanks to the modification made in game 1, $\mathcal{B}'$ can simulate oracles $\mathcal{O}_{\mathtt{AD}'_B}, \mathcal{O}_{\mathtt{AE}'_B}$ with his oracles and we have $|\Pr[\mathcal{A}/\text{Game } 1] - \Pr[\mathcal{A}/\text{Game } 2]| \leq Adv_{\mathcal{AE},\mathcal{B}'}^{i-indcca2}(k)$.

In the last game the only link between (m_0, m_1) and the challenge is given by h_σ. We construct an adversary $\mathcal{B}''$ on the hiding property as follows. $\mathcal{B}''(ck)$ first generates $\mathcal{I}_0$ and keys for B. Then $\mathcal{B}''$ runs $\mathcal{A}_1^{\mathcal{O}_{\mathtt{AD}'_B}, \mathcal{O}_{\mathtt{AE}'_B}}(\mathcal{I}, pk_B)$ who outputs (s, sk_A, m_0, m_1). $\mathcal{B}''$ outputs (s, m_0, m_1) and receives h_σ where $\sigma \leftarrow_r \{0,1\}$ and $(h_\sigma, b_\sigma) \leftarrow \mathtt{Conceal}(m_\sigma)$. Finally $\mathcal{B}''$ constructs $c^* = \mathtt{AE}_{sk_A}(pk_B, r_1)$ where $r_1 \leftarrow_r \{0,1\}^{l_b}$ and runs $\mathcal{A}_2^{\mathcal{O}_{\mathtt{AD}'_B}, \mathcal{O}_{\mathtt{AE}'_B}}(\mathcal{I}, pk_B, s, c^*, h_\sigma)$ who outputs σ'. $\mathcal{B}''$ outputs σ'. $\mathcal{B}''$ can simulate oracles with sk_B. We have $\Pr[r_1 = b_\sigma] = \frac{1}{2^{l_b}}$ and $\Pr[\mathcal{A}/\text{game } 2] = \Pr[\mathcal{B}''] + \frac{1}{2^{l_b}}$. ∎

Lemme 9 *For any adversary $\mathcal{A} \in \mathcal{M}(k)$ making $q_d(.)$ decryption-oracles queries and $q_e(.)$ encryption-oracles queries, there exist $\mathcal{B}, \mathcal{B}' \in \mathcal{M}(k)^2$ whose running times are essentially the same as that of $\mathcal{A}$ such that for all k*

$$Adv^{i-uf-ctxt}_{\mathcal{AE}',\mathcal{A}}(k) \leq q_e(k).Adv^{r-bind}_{\mathcal{C},\mathcal{B}}(k) + Adv^{i-uf-ctxt}_{\mathcal{AE},\mathcal{B}'}(k)$$

where $\mathcal{B}'$ makes at most $q_d(k)$ decryption-oracles queries and $q_e(k)$ encryption-oracles queries.

Proof. Let's fix a security parameter and an adversary $\mathcal{A}$ on the I-UF-CTXT property of $\mathcal{AE}'$. The game of $\mathcal{A}$ is defined by:

Game 0:

1. $\mathcal{I} \leftarrow \mathtt{AG}'(1^k)$,
2. $(sk_A, pk_A) \leftarrow \mathtt{AK}'(\mathcal{I})$,
3. $\mathcal{A}^{\mathcal{O}_{\mathtt{AE}'_A}, \mathcal{O}_{\mathtt{AD}'_A}}(\mathcal{I}, pk_A) = (sk_B, c, h)$,
4. $\mathcal{A}$ succeeds if $\mathtt{AD}'_{sk_B}(pk_A, c, h) = m \neq \perp$ and (c, h) is not returned by $\mathcal{O}_{\mathtt{AE}'_A}$ for a request of the type (pk_B, m_i).

Where oracles are defined as real algorithms.

Let's denote by (m_i, pk_i) the ith request to $\mathcal{O}_{\mathtt{AE}'_A}$, and (pk_A, c_i, h_i) the answer. Let E be the event that $(c, pk_B) = (c_i, pk_i)$ for one $i \in [1, q_e]$. We have $\Pr[A/E] = \Pr[\mathcal{A} \rightarrow (c_i, h)/h \neq h_i \,\&\, \mathtt{Open}_{ck}(h, \mathtt{AE}_{sk_B}(pk_A, c_i)) \neq \perp]$. In case where the event E happens, we construct an adversary $\mathcal{B}$ on relaxed binding. $\mathcal{B}(ck)$ first generates $\mathcal{I}_0$ and keys for A. Then he chooses $i_0 \leftarrow \{1, \ldots q_e\}$ and runs $\mathcal{A}^{\mathcal{O}_{\mathtt{AE}'_A}, \mathcal{O}_{\mathtt{AD}'_A}}$ who returns (sk_B, c, h). The oracle $\mathcal{O}_{\mathtt{AD}'_A}$ is simulated with sk_A as the real algorithm. The oracle $\mathcal{O}_{\mathtt{AE}'_A}(pk, m_i)$ is simulated as follows. If $i \neq i_0$ $\mathcal{B}$ proceed as in the real algorithm. Else $\mathcal{B}$ returns m_{i_0} and receives (h_{i_0}, b_{i_0}). He computes $\mathtt{AE}_{sk_A}(pk, b_{i_0}) = c_{i_0}$ and answers (c_{i_0}, h_{i_0}) to $\mathcal{A}$. With probability $1/q_e$, $c = c_{i_0}$ and $\mathcal{B}$ returns h. So $\Pr[\mathcal{B}] = 1/q_e. \Pr[\mathcal{A}/E]$.

Then, we construct $\mathcal{B}'$ on the I-UF-CTXT property of $\mathcal{AE}$. $\mathcal{B}'^{\mathcal{O}_{\mathtt{AE}_A}, \mathcal{O}_{\mathtt{AD}_A}}(\mathcal{I}_0, pk_A)$ generates ck and runs $\mathcal{A}$ who outputs (sk_B, c, h). Then $\mathcal{B}'$ returns (sk_B, c). $\mathcal{O}_{\mathtt{AE}'_A}$ and $\mathcal{O}_{\mathtt{AD}'_A}$ can be simulated with $\mathcal{O}_{\mathtt{AE}_A}$ and $\mathcal{O}_{\mathtt{AD}_A}$ and since we are in the case where the event E does not happen, we have $\Pr[\mathcal{B}'] = \Pr[\mathcal{A}/\overline{E}]$. ∎

Lemme 10 *For any adversary $\mathcal{A} \in \mathcal{M}(k)$, there exists $\mathcal{B} \in \mathcal{M}(k)$ whose running time is essentially the same as that of $\mathcal{A}$ such that for all k*

$$Adv^{hid}_{\mathcal{C},\mathcal{A}}(k) \leq Adv^{i-indcca2}_{\mathcal{AE}',\mathcal{B}}(k)$$

where $\mathcal{B}$ makes no decryption-oracles querie and neither encryption-oracles querie.

Proof. The proof is easy and is left to the reader. ∎

Lemme 11 *For any adversary $\mathcal{A} \in \mathcal{M}(k)$, there exists $\mathcal{B} \in \mathcal{M}(k)$ whose running time is essentially the same as that of $\mathcal{A}$ such that for all k*

$$Adv_{\mathcal{C},\mathcal{A}}^{r-bind}(k) \leq Adv_{\mathcal{AE}',\mathcal{B}}^{i-uf-ctxt}(k)$$

where $\mathcal{B}$ makes no decryption-oracles querie and 1 encryption-oracles querie.

Proof. Let's fix a security parameter and an adversary $\mathcal{A}$ on the relaxed binding property. We construct an adversary $\mathcal{B}$ on the I-UF-CTXT property of $\mathcal{AE}'$ in the following way. $\mathcal{B}^{\mathcal{O}_{\mathtt{AE}'_A},\mathcal{O}_{\mathtt{AD}'_A}}(\mathcal{I}, pk_A)$ generates keys for B and runs $\mathcal{A}_1(ck)$ who outputs (m, s). $\mathcal{B}$ submit (pk_B, m) to his oracle $\mathcal{O}_{\mathtt{AE}'_A}$ and receives $(c = \mathtt{AE}_{sk_A}(pk_B, b), h)$ with $(h, b) = \mathtt{Conceal}_{ck}(m)$. $\mathcal{B}$ runs $\mathcal{A}_2(ck, s, h, b)$ who outputs h', and returns (sk_B, c, h'). ∎

B.3 Proof of theorem 3

We note that for $n = 1$ we have $\mathcal{AM} = \mathcal{AE}'$ and theorems 2 and 1 give the wanted results. For $n \geq 1$ we first consider outsider adversaries. For insider adversary the proof is roughly the same except $\mathcal{A}$ chooses A's private key for the indistinguability and B_{i_0}'s private key for the unforgeability.

Lemme 12 *For any adversary $\mathcal{A} \in \mathcal{M}(k)$ making $q_d(.)$ decryption-oracles queries and $q_e(.)$ encryption-oracles queries, there exist $\mathcal{B}, \mathcal{B}', \mathcal{B}'' \in \mathcal{M}(k)^3$ whose running times are essentially the same as that of $\mathcal{A}$ such that for all k*

$$Adv_{\mathcal{AM},\mathcal{A}}^{o-indcca2}(k) \leq 2.q_d(k).Adv_{\mathcal{C},\mathcal{B}}^{r-bind}(k) + 2n.Adv_{\mathcal{AE},\mathcal{B}'}^{o-indcca2}(k) + \frac{2}{2^{l_b}} + Adv_{\mathcal{C},\mathcal{B}''}^{hid}(k)$$

where $\mathcal{B}'$ makes at most $n.q_d(k)$ decryption-oracles queries and $n.q_e(k)$ encryption-oracles queries.

Proof. Let's fix a security parameter and an adversary $\mathcal{A}$ for the following game.

Game 0:

1. $\mathcal{I} \leftarrow \mathtt{GM}(1^k)$;
2. $(sk_A, pk_A) \leftarrow \mathtt{KM}(\mathcal{I})$;
3. $(sk_{B_i}, pk_{B_i}) \leftarrow \mathtt{KM}(\mathcal{I})$ for $i = 1, \ldots n$;
4. $\mathcal{A}_1^{\mathcal{O}_{\mathtt{EM}_A},\mathcal{O}_{\mathtt{DM}_A},\mathcal{O}_{\mathtt{EM}_{B_i}},\mathcal{O}_{\mathtt{DM}_{B_i}}}(\mathcal{I}, pk_{B_1}, \ldots, pk_{B_n}, pk_A) = (s, m_0, m_1)$;
5. $\sigma \leftarrow_r \{0, 1\}$;
6. $(h_\sigma, b_\sigma) \leftarrow \mathtt{Conceal}_{ck}(m_\sigma)$;
7. $(pk_A, c_{\sigma,i}) \leftarrow \mathtt{AE}_{sk_A}(pk_{B_i}, b_\sigma)$ for $i = 1, \ldots, n$;
8. $C_\sigma = (pk_A, h_\sigma, c_{\sigma,1}, \ldots, c_{\sigma,n})$;
9. $\mathcal{A}_2^{\mathcal{O}_{\mathtt{EM}_A},\mathcal{O}_{\mathtt{DM}_A},\mathcal{O}_{\mathtt{EM}_{B_i}},\mathcal{O}_{\mathtt{DM}_{B_i}},}(\mathcal{I}, pk_{B_1}, \ldots, pk_{B_n}, pk_A, s, C_\sigma) = \sigma'$;
10. $\mathcal{A}$ succeeds if $\sigma' = \sigma$.

Where oracles are defined as real algorithms. We denote by $(pk, h_j, c_{j,1}, \ldots, c_{j,n})$, where $c_{j,l}$ for $l \neq i$ may be an empty string, the queries to the $\mathcal{O}_{\mathtt{DM}_{B_i}}$ oracles.

Game 1: We modify the game 0 as follows. When $\mathcal{A}_2$ makes a request to $\mathcal{O}_{\mathtt{DM}_{sk_{B_i}}}$: if $(pk_A, c_{j,i}) = (pk_A, c_{\sigma,i})$ then return $\perp$. The probability to return $\perp$ instead of m is equal to the probability to have $\mathtt{Open}_{ck}(h_j, b_\sigma) \neq \perp$ with $h_j \neq h_\sigma$. We construct an adversary $\mathcal{B}$ on the relaxed binding property. $\mathcal{B}(ck)$ first generates $\mathcal{I}_0 \leftarrow \mathtt{AG}(1^k)$ and keys for $A, B_1, \ldots, B_n$, then $\mathcal{B}$ runs $\mathcal{A}_1$ who outputs (s, m_0, m_1). $\mathcal{B}$ choose σ in $\{0,1\}$ and outputs m_σ. Then $\mathcal{B}$ receives (h_σ, b_σ), constructs the ciphertexts $c_{\sigma,i} = \mathtt{AE}_{sk_A}(pk_{B_i}, b_\sigma)$ for $i = 1, \ldots, n$, and runs $\mathcal{A}_2$ with $C_\sigma = (pk_A, h_\sigma, c_{\sigma,1}, \ldots, c_{\sigma,n})$. $\mathcal{B}$ can simulate oracles with the private keys, so he has just to wait for the request $(pk_A, h_j, c_{\sigma,i})$ and outputs h_j. So we have $|\Pr[\mathcal{A}/\text{Game } 0] - \Pr[\mathcal{A}/\text{Game } 1]| \leq q_d(k). \Pr[\mathcal{B}]$.

Game 2: We replace $c_{\sigma,1}$ by $c_{\sigma,1} = \mathtt{AE}_{sk_A}(pk_{B_1}, r_1)$ where $r_1 \leftarrow_r \{0,1\}^{l_b} \setminus b_\sigma$. We construct an adversary $\mathcal{B}'$ on the O-IND-CCA2 property of $\mathcal{AE}$. First $\mathcal{B}'^{\mathcal{O}_{\mathtt{AD}_{B_1}}, \mathcal{O}_{\mathtt{AE}_{B_1}}, \mathcal{O}_{\mathtt{AE}_A}, \mathcal{O}_{\mathtt{AD}_A}}(\mathcal{I}_0, pk_{B_1}, pk_A)$ generates ck and $(sk_{B_i}, pk_{B_i}) \leftarrow \mathtt{KM}(\mathcal{I}_0)$ for $i = 2, \ldots, n$, and runs $\mathcal{A}_1$ who outputs (s, m_0, m_1). Then $\mathcal{B}'$ chooses σ in $\{0,1\}$, constructs $\mathtt{Conceal}_{ck}(m_\sigma) = (h_\sigma, b_\sigma)$ and outputs (r_1, b_σ) with $r_1 \leftarrow_r \{0,1\}^{l_b} \setminus b_\sigma$. Then, $\mathcal{B}'$ receives $c^* = \mathtt{AE}_{sk_A}(pk_{B_1}, r_1)$ or $\mathtt{AE}_{sk_A}(pk_{B_1}, b_\sigma)$, calls $\mathcal{O}_{\mathtt{AE}_{sk_A}}$ with (pk_{B_i}, b_σ) for $i = 2, \ldots, n$ and runs $\mathcal{A}_2$ with $C_\sigma = (pk_A, h_\sigma, c^*,\ c_{\sigma,2}, \ldots, c_{\sigma,n})$ who outputs σ'. If $\sigma' = \sigma$ $\mathcal{B}'$ outputs b_σ else $\mathcal{B}'$ outputs r_1. Thanks to the modification made in game 1, $\mathcal{B}'$ can simulate the oracles for $\mathcal{A}$ with his own oracles and we have $|\Pr[\mathcal{A}/\text{Game } 1] - \Pr[\mathcal{A}/\text{Game } 2]| \leq Adv^{o-indcca2}_{\mathcal{AE},\mathcal{B}'}(k)$.

Games $i = 3, \ldots n+1$: we proceed as in game 2 with $c_{\sigma,(i-1)}$. We obtain: $|\Pr[\mathcal{A}/\text{Game } i-1] - \Pr[\mathcal{A}/\text{Game } i]| \leq Adv^{o-indcca2}_{\mathcal{AE},\mathcal{B}'}(k)$.

In the last game the only link between (m_0, m_1) and the challenge C_σ is given by h_σ. We construct an adversary $\mathcal{B}''$ on hiding property as follows. $\mathcal{B}''(ck)$ first generates $\mathcal{I}_0 \leftarrow \mathtt{AG}(1^k)$ and keys for $A, B_1, \ldots, B_n$. Then, $\mathcal{B}''$ runs $\mathcal{A}_1$ and outputs the same response. $\mathcal{B}''$ receives h_σ where $\sigma \leftarrow_r \{0,1\}$ and $(h_\sigma, b_\sigma) \leftarrow \mathtt{Conceal}(m_\sigma)$. Finally $\mathcal{B}''$ constructs $c_{\sigma,i} = \mathtt{AE}_{sk_A}(pk_{B_i}, r_1)$ for $i = 1, \ldots, n$ where $r_1 \leftarrow_r \{0,1\}^{l_b}$ and runs $\mathcal{A}_2$ with $C_\sigma = (pk_A, h_\sigma, c_{\sigma,1}, \ldots, c_{\sigma,n})$. Finally, $\mathcal{B}''$ outputs the same bit than $\mathcal{A}_2$. $\mathcal{B}''$ can simulate oracles with the private keys. We have $\Pr[r_1 = b_\sigma] = \frac{1}{2^{l_b}}$ and $\Pr[\mathcal{A}/\text{Game } n+1] = \Pr[\mathcal{B}''] + \frac{1}{2^{l_b}}$. ∎

Lemme 13 *For any adversary $\mathcal{A} \in \mathcal{M}(k)$ making $q_d(.)$ decryption-oracles queries and $q_e(.)$ encryption-oracles queries, there exist $\mathcal{B}, \mathcal{B}' \in \mathcal{M}(k)^2$ whose running times are essentially the same as that of $\mathcal{A}$ such that for all k*

$$Adv^{o-uf-ctxt}_{\mathcal{AM},\mathcal{A}}(k) \leq q_e(k).Adv^{r-bind}_{\mathcal{C},\mathcal{B}}(k) + Adv^{o-uf-ctxt}_{\mathcal{AE},\mathcal{B}'}(k)$$

$$Adv^{o-uf-(w)ptxt}_{\mathcal{AM},\mathcal{A}}(k) \leq 2q_e(k).Adv^{r-bind}_{\mathcal{C},\mathcal{B}}(k) + Adv^{o-uf-(w)ptxt}_{\mathcal{AE},\mathcal{B}'}(k)$$

where $\mathcal{B}'$ makes at most $q_d(k)$ decryption-oracles queries and $q_e(k)$ encryption-oracles queries.

Proof. Let's fix a security parameter and an adversary $\mathcal{A}$ for the following game.
Game 0:

1. $\mathcal{I} \leftarrow \texttt{GM}(1^k)$;
2. $(sk_A, pk_A) \leftarrow \texttt{KM}(\mathcal{I})$;
3. $(sk_{B_i}, pk_{B_i}) \leftarrow \texttt{KM}(\mathcal{I})$ for $i = 1, \ldots, n$;
4. $i_0 \leftarrow_r \{1, \ldots, n\}$;
5. $\mathcal{A}^{\mathcal{O}_{\texttt{EM}_A}, \mathcal{O}_{\texttt{DM}_A}, \mathcal{O}_{\texttt{EM}_{B_{i_0}}}, \mathcal{O}_{\texttt{DM}_{B_{i_0}}}}(\mathcal{I}, sk_{B_{i \neq i_0}}, pk_A, pk_{B_{i_0}}) = C$;
6. $\mathcal{A}$ succeeds if $\texttt{DM}_{sk_{B_{i_0}}}(pk_A, C) = m \neq \perp$.

Where oracles are defined as real algorithms.

C is of the form $(h, c_1, \ldots, c_n)$ where c_i for $i \neq i_0$ may be empty strings and (h, c_{i_0}) is not given by $\mathcal{O}_{\texttt{EM}_A}$ for a request of the form (PK_i, m_i) where $pk_{B_{i_0}} \in PK_i$. Let $(pk_A, h_l, c_{l,1}, \ldots, c_{l,n})$ be the l^{th} answer of $\mathcal{O}_{\texttt{EM}_A}$ for $l \in [1, q_e]$ corresponding to a query (PK_l, m_l).

Case 1. Let's suppose that there exists $l \in [0, q_e]$ such that $c_{l,i_0} = c_{i_0}$ and $h \neq h_l$. We can in this case construct an adversary $\mathcal{B}$ on the relaxed binding property. $\mathcal{B}(ck)$ first generates $\mathcal{I}_0 \leftarrow \texttt{AG}(1^k)$ and keys for all users. Then he chooses $l_0 \in [1, q_e]$ and runs $\mathcal{A}$. $\mathcal{B}$ simulates the oracle $\mathcal{O}_{\texttt{EM}_A}$ as follows. For $l \neq l_0$ $\mathcal{B}$ proceed as in the real algorithm with sk_A. For $l = l_0$, $\mathcal{B}$ outputs m_l. Then he receives (h_{l_0}, b_{l_0}), computes $c_{l_0,i} = \texttt{AE}_{sk_A}(pk_{B_i}, b_{l_0})$ for each $pk_{B_i} \in PK_{l_0}$, and answers to $\mathcal{A}$ the concatenation of pk_A, h_{l_0} and all $c_{l_0,i}$. The others oracles are simulated with privates keys as real algorithms. Finally $\mathcal{B}$ outputs h. With probability $1/q_e$ $\mathcal{A}$ outputs C such that $c_{i_0} = c_{l_0,i_0}$, and $\mathcal{B}$ wins, i.e. $\Pr[\mathcal{B}] = 1/q_e. \Pr[\mathcal{A}/E]$.

Case 2. Let's suppose now that $c_{l,i_0} \neq c_{i_0}$ for all $l \in [0, q_e]$, i.e. c_{i_0} is a new $\mathcal{AE}$'s ciphertext from A to B_{i_0}. We can in this case construct an adversary $\mathcal{B}'$ on the O-UF-CTXT property of $\mathcal{AE}$. $\mathcal{B}'^{\mathcal{O}_{\texttt{AD}_{B_{i_0}}}, \mathcal{O}_{\texttt{AE}_{B_{i_0}}}, \mathcal{O}_{\texttt{AE}_A}, \mathcal{O}_{\texttt{AD}_A}}(\mathcal{I}_0, pk_{B_{i_0}}, pk_A)$ constructs keys for B_i for $i \in \{1, \ldots, n\} \setminus i_0$, chooses ck, and runs $\mathcal{A}$. $\mathcal{B}'$ can simulate the oracles for $\mathcal{A}$ with his own oracles. Then, $\mathcal{B}'$ outputs (pk_A, c_{i_0}) and we have $\Pr[\mathcal{B}'] = \Pr[\mathcal{A}/\overline{E}]$.

We can adapt the proof for the O-UF-PTXT property. Let's suppose that in the game 0 that (m, PK) with $pk_{B_{i_0}} \in PK$ has not been submitted to $\mathcal{O}_{\texttt{AE}_A}$. Since schemes must verify the correctness property, (h, c_{i_0}) is not given by $\mathcal{O}_{\texttt{EM}_A}$ for a request of the form (PK_i, m_i) where $pk_{B_{i_0}} \in PK_i$. So, we have just to add some verifications in case 2. Let b be the plaintext corresponding to c_{i_0}. Let's suppose that $(pk_{B_{i_0}}, b)$ has been submitted to $\mathcal{O}_{\texttt{AE}_A}$ by $\mathcal{B}'$, i.e. there exists (PK_l, m_l) in the list of $\mathcal{A}$'s queries to $\mathcal{O}_{\texttt{EM}_A}$ such that $pk_{B_{i_0}} \in PK_l$ and $\texttt{Conceal}(m_l) = (h_l, b_l)$ with $b_l = b$. If $h_l = h$ then $m_l = m$ and (PK, m) with $pk_{B_{i_0}} \in PK$ has been submitted. Else we can construct an adversary $\mathcal{B}'' = \mathcal{B}$ on the relaxed binding property as in case 1. This adaptation works also for the O-UF-wPTXT property. ∎