The CCA2-Security of Hybrid Damgård's ElGamal

Eike Kiltz[1] Krzysztof Pietrzak[2] Martijn Stam[3] Moti Yung[4]

Abstract

We consider a hybrid version of Damgård's ElGamal public-key encryption scheme that incorporates the use of a symmetric cipher and a hash function for key-derivation. We prove that under appropriate choice of the hash function this scheme is IND-CCA2 secure under the Decisional Diffie-Hellman assumption in the standard model. Our results can be generalized to universal hash proof systems where our main technical contribution can be viewed as an efficient generic transformation from 1-universal to 2-universal hash proof systems.

Keywords: Chosen-ciphertext security, hybrid encryption, hash proof systems, ElGamal

1 Introduction

In 1991, Damgård [6] proposed a new public-key encryption scheme and proved it secure against lunchtime attacks [17] (CCA1 secure) under the *knowledge of exponent* assumption.[1] His scheme can be viewed as a "double-base" variant of the original ElGamal encryption scheme [8] and therefore it is often denoted as *Damgård's ElGamal* in the literature. In this paper we revisit Damgård's ElGamal, incorporating the knowledge about the design and analysis of public-key encryption schemes gained since its original publication in 1991. Since Damgård's original proposal is trivially malleable (and hence not IND-CCA2 secure), we consider a modern hybrid [5] variant of it (called hybrid Damgård's ElGamal) which incorporates the use of a strongly secure symmetric cipher and a hash function as key-derivation function.

The main result of this paper is as follows. We prove hybrid Damgård's ElGamal secure against chosen-ciphertext attack [19] (IND-CCA2) if the following properties hold:

1. the standard Decisional Diffie-Hellman (DDH) is hard;
2. the symmetric cipher is secure in the sense of authenticated encryption (e.g., an encrypt-then-mac based cipher);
3. the hash function is a 4-wise independent hash function with a sufficiently small image compared to the order of the group.

Our security analysis is in the standard model and does not make use of idealized models such as the random oracle model [2]. To the best of our knowledge this is the first IND-CCA2 security proof of hybrid Damgård's ElGamal under standard security assumptions.

We stress that the motivation for modifying Damgård's original ElGamal scheme [6] and all our security claims rely on techniques from Cramer and Shoup's breakthrough paradigm of

[1] CWI Amsterdam, The Netherlands. Email: kiltz@cwi.nl. URL: http://www.cwi.nl/∼kiltz.

[2] CWI Amsterdam, The Netherlands. Email: pietrzak@cwi.nl. URL: www.cwi.nl/∼pietrzak.

[3] EPFL, Switzerland. Email: martijn.stam@epfl.ch. URL: people.epfl.ch/martijn.stam.

[4] Google Inc. Email: moti@cs.columbia.edu. URL: www1.cs.columbia.edu/∼moti/.

[1] This assumption basically states that given two group elements (g_1, g_2) with unknown discrete logarithm $\omega = \log_{g_1}(g_2)$, the *only way* to efficiently compute (g_1^x, g_2^x) is to *know* the exponent x.

universal hash proof systems [3, 4, 5] and its more recent extensions [14, 9, 12], all of which were only published several years after Damgård's original article. In fact, universal hash proof systems provide a framework for the theoretical explanation of our results: Hybrid Damgård's ElGamal instantiated with a strongly secure cipher (and no hash function) can be viewed as the Kurosawa-Desmedt paradigm [14] instantiated with the DDH-based 1-universal hash proof system from [4]. Hence, this scheme can be proved IND-CCA1 (lunchtime) secure but it is still not IND-CCA2 secure. At the core of our IND-CCA2 construction lies the application of a 4-wise independent hash function to provide an efficient conversion from 1-universal to 2-universal hash proof system. For this result we need a generalization of the leftover hash lemma [11] that may be of independent interest. Only the application of the 4-wise independent hash function makes the hash proof system 2-universal which in turn makes it possible to prove the scheme's IND-CCA2 security.

We prove that this is also true in general: a 4-wise independent hash function with sufficiently small image can be used to upgrade a 1-universal hash proof system to a 2-universal one. Our transformation based on 4-wise independent hash function improves the one from Cramer and Shoup [4] which incorporates a linear overhead. As a direct application of this we obtain a number of new and efficient IND-CCA2 secure hybrid encryption schemes from known 1-universal hash proof systems with a hard subset membership problem such as Paillier's DCR assumption, the quadratic residue assumption [4], and the class of n-Linear assumptions [12].

1.1 Related work

Due to its efficiency, Damgård's original scheme has attracted a handful of investigations; these resulted in the following statements we discuss now:

- Damgård himself proved it IND-CCA1 secure under an assumption that is today known as the "knowledge of exponent" assumption. However, this assumption is very strong and has often been critized in the literature. In particular, it is not efficiently falsifiable according to the classification of Naor [16].
- Gjøsteen [10] proved Damgård's ElGamal IND-CCA1 secure under some *interactive* version of the DDH assumption, where the adversary is given oracle access to some (restricted) DDH oracle.
- Recently, and independent of this work, Wu and Stinson [22], and at the same time Lipmaa [15] improve on the above two results. However, their security results are much weaker than ours: they only prove IND-CCA1 security of Damgård's ElGamal, still requiring security assumption that are either interactive or of "knowledge of exponent" type.

We stress that the above security results are about the original Damgård's ElGamal scheme without any modification.

2 Preliminaries

2.1 Notation

If x is a string, then $|x|$ denotes its length, while if S is a set then $|S|$ denotes its size. If $k \in \mathbb{N}$ then 1^k denotes the string of k ones. If S is a set then $s \overset{\$}{\leftarrow} S$ denotes the operation of picking an element s of S uniformly at random. We write $\mathsf{A}(x, y, \ldots)$ to indicate that A is an algorithm with inputs $x, y, \ldots$ and by $z \overset{\$}{\leftarrow} \mathsf{A}(x, y, \ldots)$ we denote the operation of running A with inputs $(x, y, \ldots)$ and letting z be the output. Unless denoted otherwise, logarithms over the reals are base 2.

2.2 Public-Key Encryption

A *public key encryption* scheme $\mathsf{PKE} = (\mathsf{Kg}, \mathsf{Enc}, \mathsf{Dec})$ with message space $\mathit{MsgSp}(k)$ consists of three polynomial time algorithms (PTAs), of which the first two, Kg and Enc, are probabilistic and the last one, Dec, is deterministic. Public/secret keys for security parameter $k \in \mathbb{N}$ are generated using $(pk, sk) \overset{\$}{\leftarrow} \mathsf{Kg}(1^k)$. Given such a key pair, a message $m \in \mathit{MsgSp}(k)$ is encrypted by $C \overset{\$}{\leftarrow} \mathsf{Enc}(pk, m)$; a ciphertext is decrypted by $m \overset{\$}{\leftarrow} \mathsf{Dec}(sk, C)$, where possibly Dec outputs $\perp$ to denote an invalid ciphertext. For consistency, we require that for all $k \in \mathbb{N}$, all messages $m \in \mathit{MsgSp}(k)$, it must hold that $\Pr[\mathsf{Dec}(sk, \mathsf{Enc}(pk, m)) = m] = 1$ where the probability is taken over the above randomized algorithms and $(pk, sk) \overset{\$}{\leftarrow} \mathsf{Kg}(1^k)$.

The security we require for PKE is $\mathsf{IND\text{-}CCA2}$ security [19, 7]. To an adversary $\mathsf{A} = (\mathsf{A}_1, \mathsf{A}_2)$ we associate the following experiment $\mathbf{Exp}^{\mathrm{cca2}}_{\mathsf{PKE},\mathsf{A}}(k)$.

```
Experiment $\mathbf{Exp}^{\mathrm{cca2}}_{\mathsf{PKE},\mathsf{A}}(k)$
  $(pk, sk) \overset{\$}{\leftarrow} \mathsf{Kg}(1^k)$
  $(m_0, m_1, St) \overset{\$}{\leftarrow} \mathsf{A}_1^{\mathsf{Dec}(sk,\cdot)}(pk)$ s.t. $|m_0| = |m_1|$
  $b \overset{\$}{\leftarrow} \{0, 1\}$ ; $C^* \overset{\$}{\leftarrow} \mathsf{Enc}(pk, m_b)$
  $b' \overset{\$}{\leftarrow} \mathsf{A}_2^{\mathsf{Dec}(sk,\cdot)}(C^*, St)$
  If $b = b'$ return 1 else return 0
```

The adversary A_2 is restricted not to query $\mathsf{Dec}(sk, \cdot)$ with C^*. We define the advantage of A in the experiment as

$$\mathbf{Adv}^{\mathrm{cca2}}_{\mathsf{PKE},\mathsf{A}}(k) \overset{\mathrm{def}}{=} \left| \Pr[\mathbf{Exp}^{\mathrm{cca2}}_{\mathsf{PKE},\mathsf{A}}(k) = 1] - \frac{1}{2} \right| .$$

PKE scheme PKE is said to be indistinguishable against chosen-ciphertext attacks ($\mathsf{IND\text{-}CCA2}$ secure in short) if the advantage function $\mathbf{Adv}^{\mathrm{cca2}}_{\mathsf{PKE},\mathsf{A}}(k)$ is a negligible function in k for all adversaries $\mathsf{A} = (\mathsf{A}_1, \mathsf{A}_2)$ with probabilistic PTA A_1, A_2.

For integers k, t, Q we also define $\mathbf{Adv}^{\mathrm{cca2}}_{\mathsf{PKE},t,Q}(k) = \max_{\mathsf{A}} \mathbf{Adv}^{\mathrm{cca2}}_{\mathsf{PKE},\mathsf{A}}(k)$, where the maximum is over all A that run in time at most t while making at most Q decryption queries.

We also mention the weaker security notion of *indistinguishability against lunch-time attacks* ($\mathsf{IND\text{-}CCA1}$ security), which is defined as $\mathsf{IND\text{-}CCA2}$ security with the restriction that the adversary is not allowed to make decryption queries after having seen the challenge ciphertext. The corresponding advantage term $\mathbf{Adv}^{\mathrm{cca1}}_{\mathsf{PKE},t,Q}(k)$ is defined analogously.

2.3 Symmetric Encryption

A symmetric encryption scheme $\mathsf{SE} = (\mathsf{E}, \mathsf{D})$ is specified by its encryption algorithm E (encrypting $m \in \mathit{MsgSp}(k)$ with keys $K \in \mathcal{K}(k)$) and decryption algorithm D (returning $m \in \mathit{MsgSp}(k)$ or $\perp$). Here we restrict ourselves to deterministic algorithms E and D.

The most common notion of security for symmetric encryption is that of ciphertext indistinguishability, which requires that all efficient adversaries fail to distinguish between the encryptions of two messages of their choice. Another common security requirement is *ciphertext authenticity*. Ciphertext authenticity requires that no efficient adversary can produce a new valid ciphertext under some key when given one encryption of a message of his choice under the same key. A symmetric encryption scheme which satisfies *both* requirements simultaneously is called secure in the sense of authenticated encryption ($\mathsf{AE\text{-}OT}$ secure). Note that $\mathsf{AE\text{-}OT}$ security is a stronger notion than chosen-ciphertext security. The above requirements are formalized as follows:

Ciphertext Indistinguishability. Let $\mathsf{SE} = (\mathsf{E}, \mathsf{D})$ be a symmetric encryption scheme, and let $\mathsf{A} = (\mathsf{A}_1, \mathsf{A}_2)$ be an adversary. The advantage of A in breaking the ciphertext indistinguishability security of SE is:

$$\mathbf{Adv}^{\text{ind-ot}}_{\mathsf{SE},\mathsf{A}}(k) \overset{\text{def}}{=} \left| \Pr\left[b = b' : \begin{array}{c} K^* \xleftarrow{\$} \mathcal{K}(k)\ ;\ (m_0, m_1, St) \xleftarrow{\$} \mathsf{A}_1(1^k)\ ; \\ b \xleftarrow{\$} \{0,1\}\ ;\ \psi^* \xleftarrow{\$} \mathsf{E}_{K^*}(m_b)\ ;\ b' \xleftarrow{\$} \mathsf{A}_2(1^k, St, \psi^*) \end{array} \right] - 1/2 \right|$$

The symmetric encryption scheme SE is one-time secure in the sense of *indistinguishability* ($\mathsf{IND\text{-}OT}$) if i for every adversary A with probabilistic PTA A_1 and A_2, the advantage $\mathbf{Adv}^{\text{ind-ot}}_{\mathsf{SE},A}(\cdot)$ is negligible.

Ciphertext Integrity. This captures the property that no efficient adversary can produce a new valid ciphertext after seeing the encryption of a single message. Let $\mathsf{SE} = (\mathsf{E}, \mathsf{D})$ be a symmetric encryption scheme, and let $\mathsf{A} = (\mathsf{A}_1, \mathsf{A}_2)$ be an algorithm.

$$\mathbf{Adv}^{\text{int-ot}}_{\mathsf{SE},\mathsf{A}}(k) \overset{\text{def}}{=} \Pr\left[\psi \neq \psi^* \wedge \mathsf{D}_{K^*}(\psi) \neq \perp : \begin{array}{c} K^* \xleftarrow{\$} \mathcal{K}(k)\ ;\ (m, St) \xleftarrow{\$} \mathsf{A}_1(1^k)\ ; \\ \psi^* \leftarrow \mathsf{E}_{K^*}(m)\ ;\ \psi \xleftarrow{\$} \mathsf{A}_2(1^k, St, \psi^*) \end{array} \right]$$

The symmetric encryption scheme SE is one-time secure in the sense of *ciphertext integrity* ($\mathsf{INT\text{-}OT}$) if for every adversary A with probabilistic PTA A_1 and A_2, the advantage $\mathbf{Adv}^{\text{int-ot}}_{\mathsf{SE},\mathsf{A}}(\cdot)$ is negligible.

We also define weak ciphertext integrity ($\mathsf{WINT\text{-}OT}$) where in the above security experiment the adversary (in the second stage) never sees the ciphertext ψ^*. The corresponding advantage function is denoted as $\mathbf{Adv}^{\text{wint-ot}}_{\mathsf{SE},\mathsf{A}}$.

A symmetric encryption scheme is secure in the sense of *one-time authenticated encryption* ($\mathsf{AE\text{-}OT}$) iff it is $\mathsf{IND\text{-}OT}$ and $\mathsf{INT\text{-}OT}$ secure. For the notion of *weak one-time authenticated encryption* ($\mathsf{WAE\text{-}OT}$) we only require it to be $\mathsf{IND\text{-}OT}$ and $\mathsf{WINT\text{-}OT}$ secure.

In Appendix A we recall (following the encrypt-then-mac approach [1, 5]) how to build a symmetric scheme secure in the sense of $\mathsf{AE\text{-}OT}$, respectively $\mathsf{WAE\text{-}OT}$, from the following basic primitives:

- a (computationally secure) one-time symmetric encryption scheme with binary k-bit keys (such as AES or padding with a PRNG);
- a (computationally secure) MAC (existentially unforgeable) with k-bit keys;
- and a (computationally secure) key-derivation function (pseudorandom).

2.4 Hardness assumptions

A group scheme $\mathcal{GS}$ [5] specifies a sequence $(\mathcal{GR}_k)_{k\in\mathbb{N}}$ of group descriptions. For every value of a security parameter $k \in \mathbb{N}$, the pair $\mathcal{GR}_k = (\mathbb{G}_k, p_k)$ specifies a cyclic (multiplicative) group $\mathbb{G}_k$ of prime order p_k. Henceforth, for notational convenience, we tend to drop the index k. We assume the existence of an efficient sampling algorithm $x \xleftarrow{\$} \mathbb{G}$ and an efficient membership algorithm. We define the ddh-advantage of an adversary B as

$$\mathbf{Adv}^{\text{ddh}}_{\mathcal{GS},\mathsf{B}}(k) \overset{\text{def}}{=} \left| \Pr[\mathsf{B}(g_1, g_2, g_1^r, g_2^r) = 1] - \Pr[\mathsf{B}(g_1, g_2, g_1^r, g_2^{\tilde{r}}) = 1] \right|,$$

where $g_1,\ g_2 \xleftarrow{\$} \mathbb{G}$, $r \xleftarrow{\$} \mathbb{Z}_p$, $\tilde{r} \xleftarrow{\$} \mathbb{Z}_p \setminus \{r\}$. We say that the DDH problem is hard in $\mathcal{GS}$ if the advantage function $\mathbf{Adv}^{\text{ddh}}_{\mathcal{GS},\mathsf{B}}(k)$ is a negligible function in k for all probabilistic PTA B.

2.5 Extractors

Here we review a few concepts related to probability distributions and extracting uniform bits from weak random sources. The *statistical distance* between two random variables X and Y having a common domain D is $\mathsf{SD}(X, Y) = \frac{1}{2}\sum_{x \in D} |\Pr[X = x] - \Pr[Y = x]|$. The *min-entropy* of a random variable A is defined as $H_\infty(A) = -\log(\max_{a \in D} \Pr[A = a])$.

Let $\mathcal{HS}$ be a family of hash functions $\mathcal{H} : \mathcal{X} \rightarrow \mathcal{Y}$. With $|\mathcal{HS}|$ we denote the number of functions in this family and when sampling from $\mathcal{HS}$ we assume a uniform distribution. Let $k > 1$ be an integer, the hash-family $\mathcal{HS}$ is k-wise independent if for any sequence of distinct elements $x_1, \ldots, x_k \in \mathcal{X}$ the random variables $\mathcal{H}(x_1), \ldots, \mathcal{H}(x_k)$, where $\mathcal{H} \overset{\$}{\leftarrow} \mathcal{HS}$, are uniform random.[2]

We will now prove a generalization of the leftover hash lemma [11]. Recall that the leftover hash lemma states that for a 2-wise independent hash function $\mathcal{H}$ and a random variable X with min-entropy slightly larger than the range of $\mathcal{H}$, the random variable $(\mathcal{H}, \mathcal{H}(X))$ is close to uniformly random. We show that if $\mathcal{H}$ is 4-wise independent, then $(\mathcal{H}, \mathcal{H}(X), \mathcal{H}(\tilde{X}))$ is close to uniformly random, where $X, \tilde{X}$ can be dependent (but of course we have to require $X \neq \tilde{X}$).

Lemma 2.1 Let $(X, \tilde{X}) \in \mathcal{X} \times \mathcal{X}$ be two random variables (having joint distribution) where $H_\infty(X) \geq \kappa, H_\infty(\tilde{X}) \geq \kappa$ and $\Pr[X = \tilde{X}] = 0$. Let $\mathcal{HS}$ be a family of 4-wise independent hash functions with domain $\mathcal{X}$ and image $\{0,1\}^\ell$. Then for $\mathcal{H} \overset{\$}{\leftarrow} \mathcal{HS}$ and $U_{2\ell} \overset{\$}{\leftarrow} \{0,1\}^{2\ell}$

$$\mathsf{SD}((\mathcal{H}, \mathcal{H}(X), \mathcal{H}(\tilde{X})), (\mathcal{H}, U_{2\ell})) \leq 2^{\ell - \kappa/2}$$

so in particular (for $0 < \epsilon < 1$)

$$\mathsf{SD}((\mathcal{H}, \mathcal{H}(X), \mathcal{H}(\tilde{X})), (\mathcal{H}, U_{2\ell})) \leq \epsilon$$

as long as $2^{\ell - \kappa/2} \leq \epsilon$ or, equivalently, $\kappa \geq 2\ell + 2\log 1/\epsilon$.

Proof: Let $d = \log|\mathcal{HS}|$. For a random variable Y and Y' an independent copy of Y, we denote with $Col(Y) = \Pr[Y = Y']$ the collision probability of Y, in particular

$$\begin{aligned}
Col(\mathcal{H}, \mathcal{H}(X), \mathcal{H}(\tilde{X})) &= \Pr_{\mathcal{H},(X,\tilde{X}),\mathcal{H}',(X',\tilde{X}')}[(\mathcal{H}, \mathcal{H}(X), \mathcal{H}(\tilde{X})) = (\mathcal{H}', \mathcal{H}'(X'), \mathcal{H}'(\tilde{X}'))] \\
&= \Pr_{\mathcal{H},\mathcal{H}'}[\mathcal{H} = \mathcal{H}'] \cdot \Pr_{\mathcal{H},(X,\tilde{X}),\mathcal{H}',(X',\tilde{X}')}[(\mathcal{H}(X), \mathcal{H}(\tilde{X})) = (\mathcal{H}'(X'), \mathcal{H}'(\tilde{X}')) | \mathcal{H} = \mathcal{H}'] \\
&= \underbrace{\Pr_{\mathcal{H},\mathcal{H}'}[\mathcal{H} = \mathcal{H}'] \cdot}_{=2^{-d}} \Pr_{\mathcal{H},(X,\tilde{X}),(X',\tilde{X}')}[(\mathcal{H}(X), \mathcal{H}(\tilde{X})) = (\mathcal{H}(X'), \mathcal{H}(\tilde{X}'))] \qquad (1)
\end{aligned}$$

We define the event E, which holds if $X, \tilde{X}, X', \tilde{X}'$ are pairwise different.

$$\begin{aligned}
\Pr_{(X,\tilde{X}),(X',\tilde{X}')}[\neg \mathrm{E}] &= \Pr_{(X,\tilde{X}),(X',\tilde{X}')}[X = X' \vee X = \tilde{X}' \vee \tilde{X} = X' \vee \tilde{X} = \tilde{X}'] \\
&\leq 4 \cdot 2^{-\kappa} = 2^{-\kappa+2}
\end{aligned}$$

[2] A simple construction of a k-wise independent hash function $\mathbb{Z}_p \rightarrow \mathbb{Z}_p$ is the following: to sample a function, sample k elements $c_0, \ldots, c_{k-1} \overset{\$}{\leftarrow} \mathbb{Z}_p^k$, and define $h_{c_0,\ldots,c_{k-1}}(X) = c_0 + c_1 X + c_2 X^2 + \ldots + c_{k-1} X^{k-1} \bmod p$.

Where in the first step we used that $X \neq \tilde{X}, X' \neq \tilde{X}'$ by assumption, and in the second step we use the union bound and also our assumption that the min entropy of X and $\tilde{X}$ is at least κ (and thus e.g. $\Pr[X = X'] \leq 2^{-\kappa}$). With this we can write (1) as

$$\begin{aligned} Col(\mathcal{H}, \mathcal{H}(X), \mathcal{H}(\tilde{X})) &\leq 2^{-d} \cdot (\Pr[(\mathcal{H}(X), \mathcal{H}(\tilde{X})) = (\mathcal{H}(X'), \mathcal{H}(\tilde{X}'))|\mathrm{E}] + \Pr[\neg\mathrm{E}]) & (2) \\ &\leq 2^{-d}(2^{-2\ell} + 2^{-\kappa+2}) & (3) \end{aligned}$$

where in the second step we used that $\mathcal{H}$ is 4-wise independent. Let Y be a random variable with support $\mathcal{Y}$ and U be uniform over $\mathcal{Y}$, then

$$\|Y - U\|_2^2 = Col(Y) - |\mathcal{Y}|^{-1}$$

in particular

$$\begin{aligned} \|(\mathcal{H}, \mathcal{H}(X), \mathcal{H}(\tilde{X})) - (\mathcal{H}, U_{2\ell})\|_2^2 &= Col(\mathcal{H}, \mathcal{H}(X), \mathcal{H}(\tilde{X})) - 2^{-d-2\ell} \\ &\leq 2^{-d}(2^{-2\ell} + 2^{-\kappa+2}) - 2^{-d-2\ell} = 2^{-d-\kappa+2} \end{aligned}$$

Using that $\|Y\|_1 \leq \sqrt{|\mathcal{Y}|}\|Y\|_2$ for any random variable Y with support $\mathcal{Y}$, we obtain

$$\begin{aligned} \mathsf{SD}((\mathcal{H}, \mathcal{H}(X), \mathcal{H}(\tilde{X})), (\mathcal{H}, U_{2\ell})) &= \frac{1}{2}\|(\mathcal{H}, \mathcal{H}(X), \mathcal{H}(\tilde{X})) - (\mathcal{H}, U_{2\ell})\|_1 \\ &\leq \frac{1}{2}\sqrt{2^{d+2\ell}}\|(\mathcal{H}, \mathcal{H}(X), \mathcal{H}(\tilde{X})) - (\mathcal{H}, U_{2\ell})\|_2 \\ &\leq \frac{1}{2}\sqrt{2^{d+2\ell}}\sqrt{2^{-d-\kappa+2}} = 2^{\ell-\kappa/2} . \end{aligned}$$

This concludes the proof. ▌

We note that if $\Pr[X = \tilde{X}] = \epsilon_c > 0$, this introduces an additional term of at most ϵ_c to the statistical difference above. Moreover, the statement also holds when auxiliary information Z about X and $\tilde{X}$ leaks, as long as $H_\infty(X|Z) \geq k$ and $H_\infty(\tilde{X}|Z) \geq k$ (and $\mathcal{H}$ is independent of $(X, \tilde{X}, Z)$).

3 Damgård's ElGamal and its variants

3.1 Hybrid Damgård's ElGamal

We now propose a hybrid version of Damgård's original encryption scheme that incorporates the use of a strongly secure symmetric cipher. We need a special hash function that serves as a bridge between the group scheme and the symmetric cipher. We assume that, for a security parameter k, the symmetric cipher takes keys from $\{0,1\}^{\ell(k)}$. We therefore need a family of hash functions $\mathcal{HS}$ with $\mathcal{H} : \mathbb{G} \to \{0,1\}^{\ell(k)}$. As a minimal security requirement we assume that $\mathcal{HS}$ is pseudorandom, i.e., that uniform input gets mapped to (computationally) uniform output. (See Appendix A for a formal definition.)

Let $\mathcal{GS}$ be a group scheme where $\mathcal{GR}_k$ specifies $(\mathbb{G}, p)$ and a generator $g_1 \in \mathbb{G}$, let $\mathcal{H}$ be a family of hash functions with $\mathcal{H} : \mathbb{G} \to \{0,1\}^\ell$, and let $\mathsf{SE} = (\mathsf{E}, \mathsf{D})$ be a symmetric encryption scheme with keyspace $\{0,1\}^\ell$. Hybrid Damgård's ElGamal $\mathsf{HD\mathring{A}G} = (\mathsf{Kg}, \mathsf{Enc}, \mathsf{Dec})$ is defined as follows.

PKE scheme $\mathsf{HD\AA G} = (\mathsf{Kg}, \mathsf{Enc}, \mathsf{Dec})$

$\mathsf{Kg}(1^k)$	$\mathsf{Enc}(pk, m)$	$\mathsf{Dec}(sk, C)$
$\omega, x \stackrel{\$}{\leftarrow} \mathbb{Z}_p$; $g_2 \leftarrow g_1^{\omega}$; $X \leftarrow g_1^x$	$r \stackrel{\$}{\leftarrow} \mathbb{Z}_p^*$; $c_1 \leftarrow g_1^r$; $c_2 \leftarrow g_2^r$	Parse C as (c_1, c_2, ψ)
Pick random key κ for $\mathcal{H}$	$K \leftarrow \mathcal{H}_\kappa(X^r) \in \{0,1\}^\ell$	if $c_1^{\omega} \neq c_2$ return $\bot$
$pk \leftarrow (g_2, X, \kappa)$; $sk \leftarrow (x, \omega)$	$\psi \leftarrow \mathsf{E}_K(m)$	$K \leftarrow \mathcal{H}_\kappa(c_1^x)$
Return (sk, pk)	Return $C = (c_1, c_2, \psi)$	Return $\{m, \bot\} \leftarrow \mathsf{D}_K(\psi)$

Damgård's original scheme [6] is a special case of $\mathsf{HD\AA G}$ where $\mathcal{H}$ is the identity function and SE is "any easy to invert group operation" [6], for example the one-time pad with $\mathsf{E}_K(m) = K \oplus m$. In his paper, Damgård proved $\mathsf{IND\text{-}CCA1}$ security of his scheme under the DDH assumption and the *knowledge of exponent* assumption in $\mathcal{GS}$.[3]

3.2 Equivalent description of the scheme

In $\mathsf{HD\AA G}$, invalid ciphertexts of the form $c_1^{\omega} \neq c_2$ are reject explicitly. Similar to [5], we now give a variant of this scheme called "implicit rejection Hybrid Damgård's ElGamal", $\mathsf{HD\AA G_{IR}} = (\mathsf{Kg}, \mathsf{Enc}, \mathsf{Dec})$, in which such invalid ciphertexts only get rejected implicitly using the security properties of the symmetric cipher SE. In this variant we assume that $\mathcal{GR}_k$ specifies $(\mathbb{G}, p)$ and two independent generators $g_1, g_2 \in \mathbb{G}$.

PKE scheme $\mathsf{HD\AA G_{IR}} = (\mathsf{Kg}, \mathsf{Enc}, \mathsf{Dec})$

$\mathsf{Kg}(1^k)$	$\mathsf{Enc}(pk, m)$	$\mathsf{Dec}(sk, C)$
$x_1, x_2 \stackrel{\$}{\leftarrow} \mathbb{Z}_p$; $X \leftarrow g_1^{x_1} g_2^{x_2}$	$r \stackrel{\$}{\leftarrow} \mathbb{Z}_p^*$; $c_1 \leftarrow g_1^r$; $c_2 \leftarrow g_2^r$	Parse C as (c_1, c_2, ψ)
Pick random key κ for $\mathcal{H}$	$K \leftarrow \mathcal{H}_\kappa(X^r) \in \{0,1\}^\ell$	$K \leftarrow \mathcal{H}_\kappa(c_1^{x_1} c_2^{x_2})$
$pk \leftarrow (X, \kappa)$; $sk \leftarrow (x_1, x_2)$	$\psi \leftarrow \mathsf{E}_K(m)$	Return $\{m, \bot\} \leftarrow \mathsf{D}_K(\psi)$
Return (sk, pk)	Return $C = (c_1, c_2, \psi)$	

Theorem 3.1 Let SE be a symmetric encryption scheme that is secure in the sense of $\mathsf{INT\text{-}OT}$ and let $\mathcal{HS}$ be a family of pseudorandom hash functions. Then $\mathsf{HD\AA G}$ is $\mathsf{IND\text{-}CCA2}$ secure if and only if $\mathsf{HD\AA G_{IR}}$ is $\mathsf{IND\text{-}CCA2}$ secure. In particular, for integers t, Q,

$$|\mathbf{Adv}^{\mathrm{cca2}}_{\mathsf{HD\AA G},t,Q}(k) - \mathbf{Adv}^{\mathrm{cca2}}_{\mathsf{HD\AA G_{IR}},t,Q}(k)| \leq Q \cdot (\mathbf{Adv}^{\mathrm{int\text{-}ot}}_{\mathsf{SE},t}(k) + \mathbf{Adv}^{\mathrm{pr}}_{\mathcal{HS},t}(k)) .$$

Theorem 3.1 can be easily proved with the methods of the proof of Theorem 4.1, where Lemma 4.2 is the main technical tool.

We remark that a similar theorem can be proved concerning $\mathsf{IND\text{-}CCA1}$ security, given that SE is $\mathsf{WINT\text{-}OT}$ secure.

4 Security of Hybrid Damgård's ElGamal

4.1 $\mathsf{IND\text{-}CCA2}$ Security

We prove $\mathsf{IND\text{-}CCA2}$ security of Hybrid Damgård's ElGamal where

- $\mathcal{GS}$ is a group scheme where $\mathcal{GR}_k$ specifies $(\mathbb{G}, p)$ and the DDH assumption holds
- $\mathcal{HS}$ is a family $\mathcal{H}_k : \mathbb{G} \to \{0,1\}^{\ell(k)}$ of 4-wise independent hash functions with $\log_2(p) \geq 4\ell(k)$

[3] To be more precise, Damgård only formally proved one-way ($\mathsf{OW\text{-}CCA1}$) security of his scheme, provided that the original ElGamal scheme is $\mathsf{OW\text{-}CPA}$ secure. But he also remarks that his proof can be reformulated to prove $\mathsf{IND\text{-}CCA1}$ security, provided that ElGamal itself is $\mathsf{IND\text{-}CPA}$ secure. $\mathsf{IND\text{-}CPA}$ security of ElGamal under the DDH assumption was only formally proved later in [20].

- $\mathsf{SE} = (\mathsf{E}, \mathsf{D})$ is a $\mathsf{AE\text{-}OT}$ secure symmetric encryption scheme with key-space $\{0,1\}^{\ell(k)}$.

Theorem 4.1 Let $\mathcal{GS} = (\mathbb{G}, p)$ be a group scheme where the DDH problem is hard, let $\mathcal{H}$ be a family of 4-wise independent hash functions from $\mathbb{G}$ to $\{0,1\}^{\ell(k)}$ with $\log_2 p \geq 4\ell(k)$, and let SE be a symmetric encryption that is secure in the sense of $\mathsf{AE\text{-}OT}$. Then $\mathsf{HD\mathring{A}G_{IR}}$ is secure in the sense of $\mathsf{IND\text{-}CCA2}$. In particular,

$$\mathbf{Adv}^{\mathrm{cca2}}_{\mathsf{HD\mathring{A}G_{IR}},t,Q}(k) \leq \mathbf{Adv}^{\mathrm{ddh}}_{\mathcal{GS},t}(k) + 2Q \cdot \mathbf{Adv}^{\mathrm{int\text{-}ot}}_{\mathsf{SE},t}(k) + \mathbf{Adv}^{\mathrm{ind\text{-}ot}}_{\mathsf{SE},t}(k) + \frac{Q+1}{2^{\ell(k)}} .$$

$\mathsf{IND\text{-}CCA2}$ security of the "explicit-rejection" version $\mathsf{HD\mathring{A}G}$ follows by Theorem 3.1. We remark that even though we cannot prove the KEM part of the above scheme $\mathsf{IND\text{-}CCA2}$ secure, it can be proved "IND-CCCA" secure. The latter notion was defined in [12] and proved sufficient to yield $\mathsf{IND\text{-}CCA2}$ secure encryption when combined with a $\mathsf{AE\text{-}OT}$ secure cipher.

Efficiency. A particular advantage of $\mathsf{HD\mathring{A}G}$ is its efficiency. Compared to the reference scheme by Kurosawa and Desmedt [14] and its more recently proposed variants with improved efficiency [9, 12] it saves one standard exponentiation in encryption and its key-sizes are smaller. Furthermore, it does not use any kind of (target) collision resistant hash function which can be quite expensive to implement from the DDH assumption. Decryption and ciphertext expansion are the same. On the other hand, in terms of concrete security, Theorem 4.1 requires the image $\{0,1\}^\ell$ of $\mathcal{H}$ to be sufficiently small, i.e., $\ell \leq \frac{1}{4}\log_2 p$. Consequently, for a symmetric cipher with $\ell = k = 80$ bits keys we are forced to use groups of order $\log_2 p \geq 4k = 320$ bits. For some specific groups such as elliptic curves this can be a drawback since there one typically works with groups of order $\log p = 2k = 160$ bits. However, for many other practical groups such as prime sub-groups of $\mathbb{Z}_q^*$ one usually takes a group of order between 768 and 1024 bits in which case the requirement $\log_2 p \geq 4k$ can be easily fulfilled. In the latter case Hybrid Damgård's ElGamal seems to be an attractive alternative to the scheme by Kurosawa and Desmedt.

Proof of Theorem 4.1: Let A be an adversary on the $\mathsf{IND\text{-}CCA2}$ security of the PKE $\mathsf{HD\mathring{A}G_{IR}}$. We will consider a sequence of games, Game 1, Game 2, ..., each game involving A. Let X_i be the event that in Game i, it holds that $b = b'$, i.e., that the adversary succeeds.

Game 1. The PKE $\mathsf{IND\text{-}CCA2}$ game with random $b \in \{0,1\}$, i.e., we have

$$|\Pr[X_1] - 1/2| = \mathbf{Adv}^{\mathrm{cca2}}_{\mathsf{HD\mathring{A}G_{IR}},\mathsf{A}}(k) .$$

Let us introduce some notation. Let $C^* = (c_1^*, c_2^*, \psi^*) = (g_1^r, g_2^r, \mathsf{E}_{K^*}(m_b))$ be the challenge ciphertext, where $K^* = \mathcal{H}(A^*)$ is the challenge key and $A^* = X^r$ is the algebraic challenge key. A ciphertext $C = (c_1, c_2, \psi) \in \mathbb{G} \times \mathbb{G} \times \{0,1\}^*$ is said to have an invalid KEM part if $\log_{g_1} c_1 \neq \log_{g_2} c_2$.

Game 2. Change the generation of the challenge key as follows. Instead of computing $\mathcal{H}(X^r)$ compute $K^* \leftarrow \mathcal{H}((c_1^*)^{x_1}(c_2^*)^{x_2})$. Since $X^r = (c_1^*)^{x_1}(c_2^*)^{x_2}$ this does not change the view of the adversary, hence

$$\Pr[X_2] = \Pr[X_1] .$$

Game 3. Change the generation of the challenge ciphertext as follows. Instead of computing c_1^* and c_2^* based on the same exponent r, use different exponents for each of them: $c_1^* = g_1^{r_1^*}$

and $c_2^* = g_2^{r_2^*}$, where $r_1^* \xleftarrow{\$} \mathbb{Z}_p$ and $r_2^* \xleftarrow{\$} \mathbb{Z}_p \setminus \{r_1^*\}$. Essentially this means that the challenge ciphertext is no longer valid. However, the DDH assumption will ensure this will go unnoticed by adversary A.

Indeed, given any adversary, we can turn him into a DDH-solver as follows. Given a quadruple (g_1, g_2, h_1, h_2) we want to determine whether it is a DDH-tuple or arbitrary. Run the adversary with challenge ciphertext $(c_1^*, c_2^*, \psi^*) = (h_1, h_2, \mathcal{H}(h_1^{x_1} h_2^{x_2}))$, simulating the rest of the experiment as before (using x_1, x_2). Output whatever A outputs. If the given quadruple is DDH, we are running Game 2 and output 1 with probability $\Pr[X_2]$. If the given quadruple is arbitrary, we are running Game 3 and output 1 with probability $\Pr[X_3]$. Hence

$$|\Pr[X_3] - \Pr[X_2]| \le \mathbf{Adv}^{\mathrm{ddh}}_{\mathcal{GS},t}(k) .$$

Game 4. Now we are done with the DDH assumption. Key generation now computes g_2 as $g_2 = g_1^{\omega}$, for uniform $\omega \in \mathbb{Z}_p^*$. A query (c_1, c_2, ψ) adversary A makes to the decryption oracle is now processed in the following way:
Case 1: If $(c_1, c_2) = (c_1^*, c_2^*)$ then use K^* to compute $\{m, \perp\} \leftarrow \mathsf{D}_{K^*}(\psi)$.
Case 2: If $(c_1, c_2) \neq (c_1^*, c_2^*)$ then the simulator checks whether the ciphertext is valid by using its trapdoor ω. If $c_2 = c_1^{\omega}$ the adversary proceeds as normal. If the check fails (and the ciphertext is invalid), the adversary outputs $\perp$.

The proof of the following key lemma will be given later.

Lemma 4.2 $|\Pr[X_4] - \Pr[X_3]| \le Q \cdot (\mathbf{Adv}^{\mathsf{wint\text{-}ot}}_{\mathsf{SE},t}(k) + \frac{1}{2^\ell})$.

Game 5. Replace the symmetric key K^* used to create the challenge ciphertext with a random key K^*, uniformly independently chosen from $\{0,1\}^\ell$. Linear algebra shows that this essentially is simply a change of random variables and therefore

$$|\Pr[X_5] - \Pr[X_4]| \le 2^{-\ell}. \tag{4}$$

More precisely, in the proof of Lemma 4.2 we showed that given X, the random variable A^* in Game 4 is uniformly distributed over $\mathbb{G}$, independent of A's view. Again, Lemma 2.1 gives us $\mathsf{SD}((\mathcal{H}, \mathcal{H}(A^*)), (\mathcal{H}, U_\ell)) \le 2^{-\ell}$ since $\log_2 p \ge \ell + 2\log(1/2^{-\ell}) = 3\ell$. This proves Equation (4).

The next (last) two games are standard since at this point A essentially plays a symmetric chosen-ciphertext game with the challenger.

Game 6. Reject all decryption queries of the form $(c_1^*, c_2^*, *)$. Since ψ^* was generated using a random key K^* that only leaks to A through ψ^*, integrity of SE implies

$$|\Pr[X_6] - \Pr[X_5]| \;\le\; Q \cdot \mathbf{Adv}^{\mathsf{int\text{-}ot}}_{\mathsf{SE},\mathsf{B}_{dem}}(k)$$

for a suitable adversary B_{dem} against the $\mathsf{INT\text{-}OT}$ security of SE. We remark that here we really need the stronger notion of $\mathsf{INT\text{-}OT}$ security since A sees one encryption ψ^* under K^*.

Finally, Game 6 models one-time security of the symmetric scheme, and we have

$$|\Pr[X_6] - 1/2| \le \mathbf{Adv}^{\mathsf{ind\text{-}ot}}_{\mathsf{SE},t}(k) .$$

Collecting the probabilities proves the theorem. ▮

It leaves to prove Lemma 4.2.

Proof: For $j \in \{1, \ldots, Q\}$, let E_j denote the event that in Game 4, adversary A submits as j-th decryption query a ciphertext (c_1, c_2, ψ) that gets rejected, but would *not* have been rejected in Game 3; all earlier queries where treated identically in Game 4 and 3. Let $E := E_1 \vee \ldots \vee E_Q$. Games 3 and 4 proceed identical unless a decryption query gets treated differently. We can remark that all decryption queries that get rejected in Game 3 will also get rejected in Game 4 and that for all decryption queries that are not rejected in Game 4, the answers in both games will coincide. Consequently,

$$|\Pr[X_3] - \Pr[X_4] \leq \Pr[E_1] + \ldots + \Pr[E_Q] = \Pr[E]. \tag{5}$$

Now consider events $\hat{E}_j$, where for $j \in \{1, \ldots, Q\}$, event $\hat{E}_j$ denotes that the j-th decryption query in Game 4 gets rejected, but $\mathsf{D}_{K'} \neq \perp$ under an independently uniformly chosen symmetric key $K' \overset{\$}{\leftarrow} \{0,1\}^\ell$ (and all earlier queries were treated identically in Games 4 and 3). By the integrity property of SE, we have for $j \in \{1, \ldots, Q\}$,

$$\Pr[\hat{E}_j] \leq \mathbf{Adv}^{\mathsf{wint\text{-}ot}}_{\mathsf{SE},\mathsf{B}_{dem}}(k),$$

for a suitable adversary B_{dem} against $\mathsf{WINT\text{-}OT}$ security of the symmetric encryption scheme. We now claim that

$$\text{for all } j: \quad |\Pr[\hat{E}_j] - \Pr[E_j]| \leq 2^{-\ell}\ . \tag{6}$$

This implies

$$\Pr[E_1] + \ldots + \Pr[E_Q] \leq \Pr[\hat{E}_1] + \ldots + \Pr[\hat{E}_Q] + \frac{Q}{2^\ell} \leq Q \cdot (\mathbf{Adv}^{\mathsf{wint\text{-}ot}}_{\mathsf{SE},t}(k) + \frac{1}{2^\ell}).$$

Combining this with (5) completes the proof of Lemma 4.2.

It leaves to prove Equation (6). Fix a security parameter k and $j \in \{1, \ldots, Q(k)\}$. Let (c_1, c_2, ψ) be the ciphertext of the j-th decryption query in Game 3. Without loss of generalization we assume that all decryption queries are made after seeing the challenge ciphertext.

Let $r_1 := \log_{g_1} c_1$, and $r_2 := \log_{g_2} c_2$. Write furthermore $\omega = \log_{g_1} g_2$, and $x = \log_{g_1} X = x_1 + \omega x_2$. Then (c_1, c_2) is a valid KEM part iff $r_1 = r_2$ or, alternatively, if $c_1^\omega = c_2$. Furthermore, if (c_1, c_2) is valid, then E_j and $\hat{E}_j$ cannot be fulfilled by definition.

Let $A = c_1^{x_1} c_2^{x_2}$ be the virtual algebraic key and $K = \mathcal{H}(A)$ be the virtual symmetric key used to determine whether $\mathsf{D}_K(\psi) = \perp$ or not (according to the rules of Game 4). We claim that under the condition that (c_1, c_2, ψ) has an invalid KEM part, K is, just as the key K' of event $\hat{E}_j$, uniformly distributed and *independent* of ψ. To this end we compute the average min-entropy of A, conditioned on the view of the adversary.

Consider the random variables $X = g_1^{x_1} g_2^{x_2} = g_1^{x_1 + \omega x_2}$, $A = c_1^{x_1} c_2^{x_2} = g_1^{x_1 r_1 + \omega x_2 r_2}$ with $r_1 \neq r_2$, and $A^* = (c_1^*)^{x_1} (c_2^*)^{x_2} = g_1^{x_1 r_1^* + \omega x_2 r_2^*}$ with $r_1^* \neq r_2^*$.

Claim: $H_\infty(A|X) = \log p$ and $H_\infty(A^*|X) = \log p$.

To prove the claim we show that given X, A still looks like a uniform random element from $\mathbb{G}$. By $r_1 \neq r_2$, the equation $\log_{g_1}(A) = x_1 r_1 + \omega x_2 r_2$ is linearly independent from $\log_{g_1}(X) = x_1 + \omega x_2$. Therefore, $H_\infty(A|X) = \log p$. The same argument also shows $H_\infty(A^*|X) = \log p$ which concludes the proof of the claim.

Now we can apply Lemma 2.1 to induce

$$\mathsf{SD}((X, \mathcal{H}, K = \mathcal{H}(A), K^* = \mathcal{H}(A^*)), (X, K = \mathcal{H}(A), \mathcal{H}, K') \leq 2^{-\ell}$$

since $4\ell = \log p \geq 2\ell + 2\log(1/2^{-\ell}) = 4\ell$. ▌

4.2 IND-CCA1 security

In this section we consider the security properties of Hybrid Damgård's ElGamal where

- $\mathcal{GS}$ is a group scheme where $\mathcal{GR}_k$ specifies $(\mathbb{G}, p)$ and the DDH assumption holds;
- $\mathcal{HS}$ is the identity function;
- $\mathsf{SE} = (\mathsf{E}, \mathsf{D})$ is a WAE-OT secure symmetric encryption scheme with key-space $\mathbb{G}$.

Theorem 4.3 Let $\mathcal{GS} = (\mathbb{G}, p)$ be a group scheme where the DDH problem is hard, let $\mathcal{H}$ be a secure key-derivation function, and let SE be a symmetric encryption that is secure in the sense of WAE-OT. Then $\mathsf{HD\mathring{A}G_{IR}}$ is secure in the sense of IND-CCA1. In particular,

$$\mathbf{Adv}^{\mathrm{cca1}_{\circ}}_{\mathsf{HD\mathring{A}G_{IR}},t,Q}(k) \leq \mathbf{Adv}^{\mathrm{ddh}}_{\mathcal{GS},t}(k) + Q \cdot \mathbf{Adv}^{\mathrm{wint\text{-}ot}}_{\mathsf{SE},t}(k) + \mathbf{Adv}^{\mathrm{ind\text{-}ot}}_{\mathsf{SE},t}(k)$$

We only sketch the proof of Theorem 4.3 since it is essentially the same as the one of Theorem 4.1. However, now we do not need the strong extractor properties of the 4-wise independent hash function anymore. Indeed, given $X = g_1^{x_1} g_2^{x_2}$ any single invalid decryption query yields an algebraic key $A = c_1^{x_1} c_2^{x_2}$ which is uniformly distributed. By using a hybrid argument one can show that all those queries will be rejected by the strong integrity properties of the symmetric cipher. This shows that all decryption queries with an invalid KEM part will get rejected during the IND-CCA1 experiment. Finally, using the same argument as in the proof of Theorem 4.1 one can then show that the challenge key K^* (computed from the invalid KEM part (c_1^*, c_2^*)) is uniformly random.

On the other hand, we remark that the scheme is, in general, not IND-CCA2 secure anymore. In fact, there exists symmetric encryption schemes that are secure in the sense of AE-OT (constructed using the encrypt-then-mac paradigm, see Appendix A) but that are "malleable" with respect to the symmetric key: That is, given $\psi^* = \mathsf{E}_{K^*}(m)$, it is possible to compute (with high probability) a $\psi = \mathsf{E}_K(m)$, where $K = g \cdot K^* \in \mathbb{G}$. Note that this does not contradict the security definition since AE-OT only guarantees security with respect to a uniform key K^*. The schemes usually loose all their security properties once the key can be altered. If such a symmetric scheme is deployed a decryption query $(c_1^* \cdot g, c_2^* \cdot g, \psi)$ reveals the message m contained in the challenge ciphertext (c_1^*, c_2^*, ψ^*).

In terms of efficiency, the scheme discussed in this subsection seems to be the most efficient schemes based on a standard number-theoretic security assumotion.

5 Hybrid encryption from Hash Proof Systems

In [4] Cramer and Shoup showed that their original scheme in [5] was a special instance of a generic framework based on hash proof systems (HPS). In this section we will show how our security results of the last section can be re-phrased in terms of HPS. As our main technical result we show an efficient transformation from a 1-universal to a 2-universal HPS. Combining the latter with an AE-OT secure symmetric cipher gives an IND-CCA2 secure public-key encryption scheme. This result can be readily applied to all known 1-universal hash proof systems with a hard subset membership problem (e.g., from Paillier, QR [4] and n-Linear [12]) to obtain a number of alternative $\mathsf{IND\text{-}CCA2}$ secure encryption schemes. We remark that in [4], Cramer and Shoup also propose a generic transformation from 1-universal to 2-universal HPSs but their construction involves a significant overhead: the key of their transformed 2-universal HPS has linearly many keys of the original 1-universal HPS.

5.1 Hash proof systems

Let $\mathcal{C}, \mathcal{K}$ be sets and $\mathcal{V} \subset \mathcal{C}$ a language. Let $\Lambda_{sk} : \mathcal{C} \to \mathcal{K}$ be a hash function indexed with $sk \in \mathcal{S}$, where $\mathcal{S}$ is a set. A hash function Λ_{sk} is *projective* if there exists a projection $\mu : \mathcal{S} \to \mathcal{P}$ such that $\mu(sk) \in \mathcal{P}$ defines the action of Λ_{sk} over the subset $\mathcal{V}$. That is, for every $C \in \mathcal{V}$, the value $K = \Lambda_{sk}(C)$ is uniquely determined by $\mu(sk)$ and C. In contrast, nothing is guaranteed for $C \in \mathcal{C} \setminus \mathcal{V}$, and it may not be possible to compute $\Lambda_{sk}(C)$ from $\mu(sk)$ and C. More precisely, we define 1- and 2-universal as follows.

1-universal. The projective hash function is ϵ-almost 1-*universal* if for all $C \in \mathcal{C} \setminus \mathcal{V}$,

$$\mathsf{SD}((pk, \Lambda_{sk}(C)), (pk, K)) \leq \epsilon \tag{7}$$

where in the above $pk = \mu(sk)$ for $sk \xleftarrow{\$} \mathcal{S}$ and $K \xleftarrow{\$} \mathcal{K}$.

2-universal. The projective hash function is ϵ-almost 2-*universal* if for all $C, C^* \in \mathcal{C} \setminus \mathcal{V}$ with $C \neq C^*$,

$$\mathsf{SD}((pk, \Lambda_{sk}(C^*), \Lambda_{sk}(C)), (pk, \Lambda_{sk}(C^*), K)) \leq \epsilon \tag{8}$$

where in the above $pk = \mu(sk)$ for $sk \xleftarrow{\$} \mathcal{S}$ and $K \xleftarrow{\$} \mathcal{K}$.

A hash proof system $\mathsf{HPS} = (\mathsf{Param}, \mathsf{Pub}, \mathsf{Priv})$ consists of three algorithms. The randomized algorithm $\mathsf{Param}(1^k)$ generates instances of $params = (group, \mathcal{K}, \mathcal{C}, \mathcal{V}, \mathcal{P}, \mathcal{S}, \Lambda_{(\cdot)} : \mathcal{C} \to \mathcal{K}, \mu : \mathcal{S} \to \mathcal{P})$, where *group* may contain some additional structural parameters. The deterministic public evaluation algorithm Pub inputs the projection key $pk = \mu(sk)$, $C \in \mathcal{V}$ and a witness w of the fact that $C \in \mathcal{V}$ and returns $K = \Lambda_{sk}(C)$. The deterministic private evaluation algorithm inputs $sk \in \mathcal{S}$ and returns $\Lambda_{sk}(C)$, without knowing a witness. We further assume there are efficient algorithms given for sampling $sk \in \mathcal{S}$ and sampling $C \in \mathcal{V}$ uniformly together with a witness w.

As computational problem we require that the *subset membership problem* is hard in HPS which means that the two elements C_0 and C_1 are computationally indistinguishable, for random $C_0 \in \mathcal{V}$ and random $C_1 \in \mathcal{C} \setminus \mathcal{V}$. This is captured by defining the advantage function $\mathbf{Adv}^{\mathrm{sm}}_{\mathsf{HPS},\mathsf{A}}(k)$ of an adversary A as

$$\mathbf{Adv}^{\mathrm{sm}}_{\mathsf{HPS},\mathsf{A}}(k) \stackrel{\text{def}}{=} \left| \Pr[\mathsf{A}(\mathcal{C}, \mathcal{V}, C_1) = 1] - \Pr[\mathsf{A}(\mathcal{C}, \mathcal{V}, C_0) = 1] \right| .$$

where $\mathcal{C}$ is taken from the output of $\mathsf{Param}(1^k)$, $C_1 \xleftarrow{\$} \mathcal{C}$ and $C_0 \xleftarrow{\$} \mathcal{C} \setminus \mathcal{V}$.

5.2 Hybrid encryption from HPS

Using the above notion of a hash proof system, Kurosawa and Desmedt [14] proposed the following hybrid encryption scheme which improved the schemes from [4]. The system parameters of the scheme consist of $params \xleftarrow{\$} \mathsf{Param}(1^k)$.

$\mathsf{Kg}(k)$**.** Choose random $sk \xleftarrow{\$} \mathcal{S}$ and define $pk = \mu(sk) \in \mathcal{P}$. Return (pk, sk).

$\mathsf{Enc}(pk, m)$. Pick $C \xleftarrow{\$} \mathcal{V}$ together with its witness ω that $C \in \mathcal{V}$. The session key $K = \Lambda_{sk}(C) \in \mathcal{K}$ is computed as $K \leftarrow \mathsf{Pub}(pk, C, \omega)$. The symmetric ciphertext is $\psi \leftarrow \mathsf{E}_K(m)$. Return the ciphertext (C, ψ).

$\mathsf{Dec}(sk, C)$. Reconstruct the key $K = \Lambda_{sk}(C)$ as $K \leftarrow \mathsf{Priv}(sk, C)$ and return $\{m, \perp\} \leftarrow \mathsf{D}_K(\psi)$.

The following was proved in [14, 9, 12].

Theorem 5.1 Assume HPS is ϵ-almost 2-universal with hard subset membership problem, $\epsilon = \epsilon(k)$ is negligible and SE is AE-OT secure. Then the encryption scheme is secure in the sense of IND-CCA2.

The analogue "lite version" for 1-universal HPS can be stated as follows.

Theorem 5.2 Assume HPS is ϵ-almost 1-universal with hard subset membership problem, $\epsilon = \epsilon(k)$ is negligible and SE is WAE-OT secure. Then the encryption scheme is secure in the sense of IND-CCA1.

5.3 From 1-universal to 2-universal HPS

Given HPS and a family of hash functions $\mathcal{HS}$ with $\mathcal{H} : \mathcal{K} \to \{0,1\}^\ell$ we define the hashed variant of it, $\mathsf{HPS}^{\mathcal{HS}}$, such that for all $C \in \mathcal{C}$, $\Lambda_{sk}^{\mathcal{HS}}(C) := \mathcal{H}_\kappa(\Lambda_{sk}(C))$. Therefore we formally have that $\Lambda_{sk}^{\mathcal{HS}} : \mathcal{C} \to \{0,1\}^\ell$. We also need to add the choice of hash $\mathcal{H} \in \mathcal{HS}$ to the index of the overall hash in $\mathsf{HPS}^{\mathcal{HS}}$. To this end define the projection $\mu^{\mathcal{HS}} : \mathcal{S} \times \mathcal{HS} \to \mathcal{P} \times \mathcal{HS}$ by $\mu(sk, \mathcal{H}) = (pk, \mathcal{H})$. Note that $\mathcal{C}$ and $\mathcal{V}$ are the same for $\mathsf{HPS}^{\mathcal{HS}}$ and HPS.

Theorem 5.3 Assume HPS is ϵ_1-almost 1-universal and $\mathcal{H}$ is a family of 4-wise independent hash functions $\mathcal{K} \to \{0,1\}^\ell$, let $\kappa = \log(|\mathcal{K}|)$ and $\epsilon_c = \max_{C,C^* \in \mathcal{C}\setminus\mathcal{V}, C \neq C^*}(\Pr_{sk}[\Lambda_{sk}(C) = \Lambda_{sk}(C^*)]$. Then $\mathsf{HPS}^{\mathcal{HS}}$ is ϵ_2-almost 2-universal for $\epsilon_2 \geq 2^{\frac{\ell-\kappa}{2}} + 2^{\frac{2\ell-\kappa}{2}} + 3\epsilon_1 + \epsilon_c$.

Proof of Theorem 5.3: Let us consider, for all $C, C^* \in \mathcal{C} \setminus \mathcal{V}$ with $C \neq C^*$, the statistical distance relevant for 2-universality for $\mathsf{HPS}^{\mathcal{HS}}$ and let Y be the random variable $(pk, \mathcal{H}, U_{2\ell})$ where $pk = \mu(sk)$ for $sk \xleftarrow{\$} \mathcal{S}$, $\mathcal{H} \xleftarrow{\$} \mathcal{HS}$ and $U_{2\ell} \xleftarrow{\$} \{0,1\}^{2\ell}$. Then we can use the triangle inequality to get

$$\begin{aligned}&\mathsf{SD}((pk, \mathcal{H}, \mathcal{H}(\Lambda_{sk}(C^*)), \mathcal{H}(\Lambda_{sk}(C))), (pk, \mathcal{H}, \mathcal{H}(\Lambda_{sk}(C^*)), U_\ell)) \\ &\quad \leq \mathsf{SD}((pk, \mathcal{H}, \mathcal{H}(\Lambda_{sk}(C^*)), \mathcal{H}(\Lambda_{sk}(C))), Y)) + \mathsf{SD}(Y, (pk, \mathcal{H}, \mathcal{H}(\Lambda_{sk}(C^*)), U_\ell)) \qquad (9)\end{aligned}$$

where as before $pk = \mu(sk)$ for $sk \xleftarrow{\$} \mathcal{S}$, $\mathcal{H} \xleftarrow{\$} \mathcal{HS}$ and $U_\ell \xleftarrow{\$} \{0,1\}^\ell$. We can upper bound the second term of (9), using again the triangle inequality in the first step, as

$$\begin{aligned}&\mathsf{SD}(Y, (pk, \mathcal{H}, \mathcal{H}(\Lambda_{sk}(C^*)), U_\ell)) \\ \leq\ & \mathsf{SD}(Y, (pk, \mathcal{H}, \mathcal{H}(K), U_\ell)) + \mathsf{SD}((pk, \mathcal{H}, \mathcal{H}(K), U_\ell), (pk, \mathcal{H}, \mathcal{H}(\Lambda_{sk}(C^*))), U_\ell) \\ \leq\ & \mathsf{SD}(Y, (pk, \mathcal{H}, \mathcal{H}(K), U_\ell)) + \mathsf{SD}((pk, K), (pk, \Lambda_{sk}(C^*))) \\ \leq\ & 2^{\frac{\ell-\kappa}{2}} + \epsilon_1 \,.\end{aligned}$$

In the last step we used the (standard) leftover hash-lemma and ϵ_1-almost universality of the HPS (cf. eq.(7)) which states that for any $C \in \mathcal{C} \setminus \mathcal{V}$

$$\mathsf{SD}((pk, K), (pk, \Lambda_{sk}(C))) = \mathsf{SD}(K, \Lambda_{sk}(C)|pk) \leq \epsilon_1 \,.$$

By the above, for $C \in \mathcal{C} \setminus \mathcal{V}$ we can define an event E_C, such that $H_\infty(\Lambda_{sk}(C)|pk, E_C) = H_\infty(K|pk) = k$ where $\Pr[\neg E_C] \leq \epsilon_1$. Further, let E_{Col} denote the event $[\Lambda_{sk}(C) \neq \Lambda_{sk}(C^*)]$, by assumption $\Pr_{sk}[\neg E_{Col}] \leq \epsilon_c$.

We now bound the first term of (9) as

$$\begin{aligned}
& \mathsf{SD}((pk, \mathcal{H}, \mathcal{H}(\Lambda_{sk}(C^*)), \mathcal{H}(\Lambda_{sk}(C))), Y) \\
\leq\ & \mathsf{SD}((pk, \mathcal{H}, \mathcal{H}(\Lambda_{sk}(C^*)), \mathcal{H}(\Lambda_{sk}(C))), Y | E_C \wedge E_{C^*} \wedge E_{Col}) + \Pr_{sk}[\neg E_C \vee \neg E_{C^*} \vee \neg E_{Col}] \\
\leq\ & 2^{\frac{2\ell - \kappa}{2}} + 2\epsilon_1 + \epsilon_c
\end{aligned}$$

where in the last step we used Lemma 2.1. ▌

5.4 A 1-universal HPS from the DDH assumption

We recall a 1-universal HPS from [4] whose hard subset membership problem is based on the DDH assumption. Let $\mathcal{GS}$ be a group scheme where $\mathcal{GR}_k$ specifies $(\mathbb{G}, p)$. Let $group = (\mathcal{GR}, g_1, g_2)$, where g_1, g_2 are independent generators of $\mathbb{G}$. Define $\mathcal{C} = \mathbb{G}^2$ and $\mathcal{V} = \{(g_1^r, g_2^r) \subset \mathbb{G}^2 : r \in \mathbb{Z}_p\}$ The value $r \in \mathbb{Z}_p$ is a witness of $C \in \mathcal{V}$. Let $\mathcal{S} = \mathbb{Z}_p^2$, $\mathcal{P} = \mathbb{G}$, and $\mathcal{K} = \mathbb{G}$. For $sk = (x_1, x_2) \in \mathbb{Z}^2$, define $\mu(sk) = X = g_1^{x_1} g_2^{x_2}$. This defines the output of $\mathsf{Param}(1^k)$. For $C = (c_1, c_2) \in \mathcal{C}$ define

$$\Lambda_{sk}(C) := c_1^{x_1} c_2^{x_2} \ . \tag{10}$$

This defines $\mathsf{Priv}(sk, C)$. Given $pk = \mu(sk)$, $C \in \mathcal{V}$ and a witness $r \in \mathbb{Z}_p$ such that $C = (c_1, c_2) = (g_1^r, g_2^r)$ public evaluation $\mathsf{Pub}(pk, C, r)$ computes $K = \Lambda_{sk}(C)$ as

$$K = X^r \ .$$

Correctness follows by Equation (10) and the definition of μ. This completes the description of HPS. Clearly, under the DDH assumption, the subset membership problem is hard in HPS. Using the techniques from the proof of Theorem 4.1, (perfect) 1-universality of the HPS is easy to verify. See also [4]. Since $\epsilon_c = 1/p$, Theorems 5.3 and 5.1 reproduce (a slightly less tight version of) Theorem 4.1.

Acknowledgements

We thank Ronald Cramer for interesting discussions.

References

[1] Mihir Bellare and Chanathip Namprempre. Authenticated encryption: Relations among notions and analysis of the generic composition paradigm. In Tatsuaki Okamoto, editor, *ASIACRYPT 2000*, volume 1976 of *LNCS*, pages 531–545. Springer-Verlag, Berlin, Germany, December 2000. (Cited on page 4, 16, 17.)

[2] Mihir Bellare and Phillip Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In V. Ashby, editor, *ACM CCS 93*, pages 62–73. ACM Press, November 1993. (Cited on page 1.)

[3] Ronald Cramer and Victor Shoup. A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. In Hugo Krawczyk, editor, *CRYPTO'98*, volume 1462 of *LNCS*, pages 13–25. Springer-Verlag, Berlin, Germany, August 1998. (Cited on page 2.)

[4] Ronald Cramer and Victor Shoup. Universal hash proofs and a paradigm for adaptive chosen ciphertext secure public-key encryption. In Lars R. Knudsen, editor, *EUROCRYPT 2002*, volume 2332 of *LNCS*, pages 45–64. Springer-Verlag, Berlin, Germany, April / May 2002. (Cited on page 2, 11, 12, 14.)

[5] Ronald Cramer and Victor Shoup. Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack. *SIAM Journal on Computing*, 33(1):167–226, 2003. (Cited on page 1, 2, 4, 7, 11, 16, 17.)

[6] Ivan Damgård. Towards practical public key systems secure against chosen ciphertext attacks. In Joan Feigenbaum, editor, *CRYPTO'91*, volume 576 of *LNCS*, pages 445–456. Springer-Verlag, Berlin, Germany, August 1992. (Cited on page 1, 7.)

[7] Danny Dolev, Cynthia Dwork, and Moni Naor. Nonmalleable cryptography. *SIAM Journal on Computing*, 30(2):391–437, 2000. (Cited on page 3.)

[8] Taher ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. In G. R. Blakley and David Chaum, editors, *CRYPTO'84*, volume 196 of *LNCS*, pages 10–18. Springer-Verlag, Berlin, Germany, August 1985. (Cited on page 1.)

[9] Rosario Gennaro and Victor Shoup. A note on an encryption scheme of kurosawa and desmedt. Cryptology ePrint Archive, Report 2004/194, 2004. `http://eprint.iacr.org/`. (Cited on page 2, 8, 13.)

[10] Kristian Gjøsteen. A new security proof for damgård's ElGamal. In David Pointcheval, editor, *CT-RSA 2006*, volume 3860 of *LNCS*, pages 150–158. Springer-Verlag, Berlin, Germany, February 2006. (Cited on page 2.)

[11] Johan Håstad, Russell Impagliazzo, Leonid A. Levin, and Michael Luby. A pseudorandom generator from any one-way function. *SIAM Journal on Computing*, 28(4):1364–1396, 1999. (Cited on page 2, 5.)

[12] Dennis Hofheinz and Eike Kiltz. Secure hybrid encryption from weakened key encapsulation. In Alfred Menezes, editor, *CRYPTO 2007*, volume 4622 of *LNCS*, pages 553–571. Springer-Verlag, Berlin, Germany, August 2007. (Cited on page 2, 8, 12, 13.)

[13] Jonathan Katz and Moti Yung. Unforgeable encryption and chosen ciphertext secure modes of operation. In Bruce Schneier, editor, *FSE 2000*, volume 1978 of *LNCS*, pages 284–299. Springer-Verlag, Berlin, Germany, April 2000. (Cited on page 17.)

[14] Kaoru Kurosawa and Yvo Desmedt. A new paradigm of hybrid encryption scheme. In Matthew Franklin, editor, *CRYPTO 2004*, volume 3152 of *LNCS*, pages 426–442. Springer-Verlag, Berlin, Germany, August 2004. (Cited on page 2, 8, 12, 13.)

[15] Helger Lipmaa. On CCA1-Security of Elgamal and Damgård cryptosystems. Cryptology ePrint Archive, Report 2008/234, 2008. `http://eprint.iacr.org/`. (Cited on page 2.)

[16] Moni Naor. On cryptographic assumptions and challenges (invited talk). In Dan Boneh, editor, *CRYPTO 2003*, volume 2729 of *LNCS*, pages 96–109. Springer-Verlag, Berlin, Germany, August 2003. (Cited on page 2.)

[17] Moni Naor and Moti Yung. Public-key cryptosystems provably secure against chosen ciphertext attacks. In *22nd ACM STOC*. ACM Press, May 1990. (Cited on page 1.)

[18] Duong Hieu Phan and David Pointcheval. About the security of ciphers (semantic security and pseudo-random permutations). In Helena Handschuh and Anwar Hasan, editors, *SAC 2004*, volume 3357 of *LNCS*, pages 182–197. Springer-Verlag, Berlin, Germany, August 2004. (Cited on page 17.)

[19] Charles Rackoff and Daniel R. Simon. Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack. In Joan Feigenbaum, editor, *CRYPTO'91*, volume 576 of *LNCS*, pages 433–444. Springer-Verlag, Berlin, Germany, August 1992. (Cited on page 1, 3.)

[20] Yiannis Tsiounis and Moti Yung. On the security of ElGamal based encryption. In Hideki Imai and Yuliang Zheng, editors, *PKC'98*, volume 1431 of *LNCS*, pages 117–134. Springer-Verlag, Berlin, Germany, February 1998. (Cited on page 7.)

[21] Mark N. Wegman and Larry Carter. New hash functions and their use in authentication and set equality. *Journal of Computer and System Sciences*, 22:265–279, 1981. (Cited on page 17.)

[22] J. Wu and D.R. Stinson. On the security of the elgamal encryption scheme and damgard's variant. Cryptology ePrint Archive, Report 2008/200, 2008. `http://eprint.iacr.org/`. (Cited on page 2.)

A Construction of authenticated encryption schemes

We recall details of the encrypt-then-mac approach [1, 5] for constructing authenticated symmetric encryption.

A.1 Building blocks

Key Derivation Functions. A key-derivation function KDF is a family of functions $\mathsf{KDF}_k : \{0,1\}^\ell \to \{0,1\}^{2k}$. We assume its output on a random input is computationally indistinguishable from a random $2k$-bit string (pseudorandomness), captured by defining the pr-advantage of an adversary B_{kdf} as

$$\mathbf{Adv}^{\text{pr}}_{\mathsf{KDF},\mathsf{B}_{\text{kdf}}}(k) = |\Pr[\mathsf{B}_{\text{kdf}}(\mathsf{KDF}(K)) = 1] - \Pr[\mathsf{B}_{\text{kdf}}(X) = 1]|,$$

where $K \xleftarrow{\$} \{0,1\}^\ell$ and $X \xleftarrow{\$} \{0,1\}^{2k}$.

Message Authentication Codes. A message authentication code $\mathsf{MAC} = (\mathsf{Tag}, \mathsf{Vfy})$ with keys $mk \in \{0,1\}^k$ consists of a tag algorithm $\mathsf{Tag}_{mk}(m)$ and a verification algorithm $\mathsf{Vfy}_{mk}(\tau)$. For consistency we require that for all messages M, we have $\Pr[\mathsf{Vfy}_{mk}(M, \mathsf{Tag}_{mk}(M)) \neq \perp] = 1$, where the probability is taken over the choice of coins of all the algorithms in the expression above.

MAC needs to be *strongly unforgeable against one-time attacks* ($\mathsf{SUF\text{-}OT}$) captured by defining the suf-ot-advantage of an adversary B_{mac} as

$$\mathbf{Adv}^{\text{suf-ot}}_{\mathsf{MAC},\mathsf{B}_{mac}}(k) = \Pr[\mathsf{Vfy}_{mk}(m^*,\tau^*) \neq \perp \ : \ mk \xleftarrow{\$} \{0,1\}^k \ ; \ (M^*,\tau^*) \xleftarrow{\$} \mathsf{B}_{mac}^{\mathsf{Tag}_{mk}(\cdot)}(1^k)] \ .$$

Above, oracle $\mathsf{Tag}_{mk}(\cdot)$ returns $\tau \leftarrow \mathsf{Tag}_{mk}(m)$ and A may only make one single query to oracle $\mathsf{Tag}_{mk}(\cdot)$. The target pair (m^*,τ^*) must be different from the pair (m,τ) obtained from $\mathsf{Tag}_{mk}(\cdot)$ (strong unforgeability).

We remark that efficient MACs satisfying the above definition can be constructed without any computational assumption (and secure against unbounded adversaries) using, e.g., almost strongly-universal hash families [21].

A.2 Construction of $\mathsf{AE\text{-}OT}$ and $\mathsf{WAE\text{-}OT}$ secure ciphers

Let $\mathsf{OTP} = (\tilde{\mathsf{E}},\tilde{\mathsf{D}})$ be a symmetric encryption that inputs keys from $\{0,1\}^k$, let KDF a key-derivation function that outputs bitstrings of length $2k$, and let MAC be a MAC scheme with keys $mk \in \{0,1\}^k$. Using the "Encrypt-then-MAC" paradigm we can construct $\mathsf{SE} = (\mathsf{E},\mathsf{D})$ that inputs keys $K \in \{0,1\}^\ell$ as follows.

```
$\mathsf{E}_K(m)$
    $(mk||dk) \leftarrow \mathsf{KDF}(K)$, where $mk, dk \in \{0,1\}^k$
    $\psi' \leftarrow \tilde{\mathsf{E}}_{dk}(m)$
    $\tau \leftarrow \mathsf{Tag}_{mk}(\psi')$
    Return $\psi = (\psi',\tau)$

$\mathsf{D}_K(\psi = (\psi',\tau))$
    $(mk||dk) \leftarrow \mathsf{KDF}(K)$
    If $\mathsf{Vfy}_{mk}(\psi',\tau) = \perp$ return $\perp$
    $M \leftarrow \tilde{\mathsf{D}}_{dk}(\psi')$
    Return $M$
```

Typically, a MAC tag (from a computationally secure MAC) has k bits, so the above construction generates ciphertexts of size $d(k) = |m| + k$. The following lemma [5, 13, 1] guarantees the AE scheme is one-time secure.

Lemma A.1 Assume OTP is $\mathsf{IND\text{-}OT}$, KDF is pseudorandom, and MAC is $\mathsf{SUF\text{-}OT}$. Then SE is $\mathsf{AE\text{-}OT}$. In particlar, we have

$$\mathbf{Adv}^{\text{ind-ot}}_{\mathsf{SE},t}(k) \leq \mathbf{Adv}^{\text{pr}}_{\mathsf{KDF},t}(k) + \mathbf{Adv}^{\text{ind-ot}}_{\mathsf{OTP},t}(k), \quad \mathbf{Adv}^{\text{int-ot}}_{\mathsf{SE},t}(k) \leq \mathbf{Adv}^{\text{pr}}_{\mathsf{KDF},t}(k) + \mathbf{Adv}^{\text{suf-ot}}_{\mathsf{MAC},t}(k) \ .$$

We remark that for authenticated encryption is a strictly stronger security notion than chosen-ciphertext security (using a separation example from [1]), whereas the latter is already sufficient for the KEM/DEM composition theorem [5] (i.e., a $\mathsf{IND\text{-}CCA2}$ secure KEM plus chosen-ciphertext secure symmetric encryption implies $\mathsf{IND\text{-}CCA2}$ secure PKE). On the other hand, there exists redundancy-free chosen-ciphertext secure symmetric encryption [18] (with $d(k) = |m|$) whereas redundancy-free authenticated encryption do not exist.

If we only require $\mathsf{WAE\text{-}OT}$ security, we can construct $\mathsf{SE} = (\mathsf{E},\mathsf{D})$ without a MAC as follows.

```
$\mathsf{E}_K(m)$
    $(mk||dk) \leftarrow \mathsf{KDF}(K)$, where $mk, dk \in \{0,1\}^k$
    $\psi' \leftarrow \tilde{\mathsf{E}}_{dk}(m)$
    Return $\psi = (\psi', mk)$

$\mathsf{D}_K(\psi = (\psi', mk'))$
    $(mk||dk) \leftarrow \mathsf{KDF}(K)$
    If $mk \neq mk'$ return $\perp$
    Returm $m \leftarrow \tilde{\mathsf{D}}_{dk}(\psi')$
```

Lemma A.2 Assume OTP is $\mathsf{IND\text{-}OT}$ and KDF is pseudorandom. Then SE is $\mathsf{WAE\text{-}OT}$. In particlar, we have

$$\mathbf{Adv}^{\text{ind-ot}}_{\mathsf{SE},t}(k) \leq \mathbf{Adv}^{\text{pr}}_{\mathsf{KDF},t}(k) + \mathbf{Adv}^{\text{ind-ot}}_{\mathsf{OTP},t}(k), \quad \mathbf{Adv}^{\text{int-ot}}_{\mathsf{SE},t}(k) \leq \mathbf{Adv}^{\text{pr}}_{\mathsf{KDF},t}(k) \ .$$