An extended abstract of this paper appears in Advances in Cryptology – EUROCRYPT '09, Lecture Notes in Computer Science Vol. ????, A. Joux ed., Springer-Verlag, 2009. This is the full version.

A New Randomness Extraction Paradigm for Hybrid Encryption

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

February 9, 2009

Abstract

We present a new approach to the design of IND-CCA2 secure hybrid encryption schemes in the standard model. Our approach provides an efficient generic transformation from 1-universal to 2-universal hash proof systems. The transformation involves a randomness extractor based on a 4-wise independent hash function as the key derivation function. Our methodology can be instantiated with efficient schemes based on standard intractability assumptions such as Decisional Diffie-Hellman, Quadratic Residuosity, and Paillier's Decisional Composite Residuosity. Interestingly, our framework also allows to prove IND-CCA2 security of a hybrid version of 1991's Damgård's ElGamal public-key encryption scheme under the DDH assumption.

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

1 Introduction

Chosen-Ciphertext Security. Indistinguishability against chosen-ciphertext attack (IND-CCA2 security) is by now the accepted standard security definition for public-key encryption schemes. It started with the development of security under lunchtime attacks (also called IND-CCA1) by Naor and Yung [20], who also gave a proof of feasibility using inefficient non-interactive zero-knowledge techniques. This was extended to the more involved systems with IND-CCA2 security in their full generality [22, 9].

Known practical constructions. Efficient designs in the standard model were first presented in the breakthrough works of Cramer and Shoup [2, 3, 4, 24]. At the heart of their design methodology is the notion of *hash proof systems* (HPSs), generalizing the initial system based on the decisional Diffie-Hellman (DDH) problem. Moreover, they are the first to formalize the notion of "Hybrid Encryption," where a public key cryptosystem is used to encapsulate the (session) key of a symmetric cipher which is subsequently used to conceal the data. This is also known as the KEM-DEM approach, after its two constituent parts (the KEM for key encapsulation mechanism, the DEM for data encapsulation mechanism); it is the most efficient way to employ a public key cryptosystem (and encrypting general strings rather than group elements).

Kurosawa and Desmedt [17] later improved upon the original work of Cramer and Shoup with a new paradigm. Whereas Cramer and Shoup [4] require both the KEM and the DEM IND-CCA2 secure, Kurosawa and Desmedt show that with a stronger requirement on the DEM (i.e., one-time authenticated encryption), the requirement on the KEM becomes weaker and can be satisfied with any strongly 2-universal hash proof system. (Cramer and Shoup need both a 2-universal and a smooth hash proof system.)

[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. and Columbia University Email: moti@cs.columbia.edu. URL: www1.cs.columbia.edu/∼moti/.

MAIN RESULT. The main result of this work is a new paradigm for constructing IND-CCA2 secure hybrid encryption schemes, based on the Kurosawa-Desmedt paradigm. At its core is a surprisingly clean and efficient new method employing *randomness extraction* (as part of the key derivation) to transform a universal$_1$ hash proof system (that only assures IND-CCA1 security) into a universal$_2$ hash proof system. In fact, our method also works for a more general class of hash proof systems which we denote "κ-entropic" hash proof systems. From that point on we follow the Kurosawa-Desmedt paradigm: the combination of a universal$_2$ HPS with a one-time authenticated encryption scheme (as DEM) will provide an IND-CCA2 secure hybrid encryption scheme. The efficient transformation enables the design of new and efficient IND-CCA2 secure hybrid encryption schemes based on various hard subset membership problem, such as the DDH assumption, Paillier's Decisional Composite Residuosity (DCR) assumption [21], the family of Linear assumptions [14, 23] that generalizes DDH, and the Quadratic Residuosity (QR) assumption.

For the new transformation to work we require a sufficiently compressing 4-wise independent hash function (made part of the public key); we also need a generalization of the leftover hash lemma [13] that may be of independent interest.

APPLICATIONS. One application of our method is centered around Damgård's public-key scheme [5] (from 1991) which he proved IND-CCA1 secure under the rather strong *knowledge of exponent* assumption.[1] This scheme can be viewed as a "double-base" variant of the original ElGamal encryption scheme [10] and consequently it is often referred to as *Damgård's ElGamal* in the literature. We first view the scheme as a hybrid encryption scheme (as advocated in [24, 4]), applying our methodology of randomness extraction in the KEM's symmetric key derivation before the authenticated encryption (as DEM). The resulting scheme is a hybrid Damgård's ElGamal which is IND-CCA2 secure, under the standard DDH assumption. We furthermore propose a couple of variants of our basic hybrid scheme that offer certain efficiency tradeoffs. Compared to Cramer and Shoup's original scheme [2] and the improved scheme given by Kurosawa-Desmedt [17], our scheme crucially removes the dependence on the hard to construct target collision hash functions (UOWHF), using an easy-to-instantiate 4-wise independent hash function instead. Furthermore, the IND-CCA2 security of hybrid Damgård's ElGamal can be directly explained through our randomness extraction paradigm when applying it to the DDH-based universal$_1$ hash proof system. In contrast, due to the dependence on the target colission resistant hash function, the efficient schemes from [2, 17] cannot be directly explained through Cramer and Shoup's hash proof system framework [3] and therefore all require separate proofs.

Another application of our method is given by a κ-entropic HPS from the QR assumption which is a variant of a HPS by Cramer and Shoup [3]. The resulting IND-CCA2 secure encryption scheme has very compact ciphertexts which only consist of one single element in $\mathbb{Z}_N^*$ plus the symmetric part. Like the scheme by Cramer and Shoup, the number of exponentiations in $\mathbb{Z}_N$ (for encryption and decryption) is linear in the security parameter. Hofheinz and Kiltz [15] give an IND-CCA2 secure encryption scheme based on the factoring assumption that is much more efficient than ours but has slightly larger ciphertexts.

RELATED WORK. Cramer and Shoup [3] already proposed a generic transformation from universal$_1$ to universal$_2$ HPSs. Unfortunately their construction involves a significant overhead: the key of their transformed universal$_2$ HPS has linearly many keys of the original universal$_1$ HPS. We further remark that the notion of randomness extraction has had numerous applications in complexity and cryptography, and in particular in extracting random keys at the final step of key exchange protocols. Indeed, Cramer and Shoup [3] already proposed using a pairwise independent hash function to turn a universal$_1$ HPS into a universal$_2$ HPS. Our novel usage is within the context of hybrid encryption as a tool that shifts the integrity checking at decryption time solely to the DEM portion. In stark contrast to the generic transformations by Cramer and Shoup ours is practical.

Various previous proofs of variants of Damgård's original scheme have been suggested after Damgård himself proved it IND-CCA1 secure under the strong "knowledge of exponent" assumption (an assumption that has often been criticized in the literature; e.g., it is not efficiently falsifiable according to the classification of Naor [19]). More recent works are by Gjøsteen [12] who showed the scheme IND-CCA1 secure under some *interactive* version of the DDH assumption, where the adversary is given oracle access to some (restricted) DDH oracle. Also, Wu and Stinson [26], and at the same time Lipmaa [18] improve

[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.

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 assumptions that are either interactive or of "knowledge of exponent" type. Desmedt and Hieu [8] recently showed a hybrid variant that is IND-CCA2 secure, yet under an even stronger assumption than Damgård's. Finally, and concurrently with our work, Desmedt et al. [7] recently showed a hybrid variant IND-CCA1 secure under the DDH assumption and a weaker KDF than ours.

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 $s \leftarrow_R S$ 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 $z \leftarrow_R \mathsf{A}(x, y, \ldots)$ we denote the operation of running A with inputs $(x, y, \ldots)$ and letting z be the output. We write $\lg x$ for logarithms over the reals with base 2. The *statistical distance* between two random variables X and Y having a common domain $\mathcal{X}$ is $\Delta[X, Y] = \frac{1}{2}\sum_{x\in\mathcal{X}} |\Pr[X = x] - \Pr[Y = x]|$. We also define the conditional statistical distance as $\Delta_E[X, Y] = \frac{1}{2}\sum_{x\in\mathcal{X}} |\Pr[X = x \mid E] - \Pr[Y = x \mid E]|$. The *min-entropy* of a random variable X is defined as $H_\infty(X) = -\lg(\max_{x\in\mathcal{X}} \Pr[X = x])$.

2.2 Public-Key Encryption

A *public key encryption* scheme $\mathsf{PKE} = (\mathsf{Kg}, \mathsf{Enc}, \mathsf{Dec})$ with message space $\mathcal{M}(k)$ 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 $(pk, sk) \leftarrow_R \mathsf{Kg}(1^k)$. Given such a key pair, a message $m \in \mathcal{M}(k)$ is encrypted by $C \leftarrow_R \mathsf{Enc}(pk, m)$; a ciphertext is decrypted by $m \leftarrow_R \mathsf{Dec}(sk, C)$, where possibly Dec outputs $\perp$ to denote an invalid ciphertext. For consistency, we require that for all $k \in \mathbb{N}$, all messages $m \in \mathcal{M}(k)$, 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 $(pk, sk) \leftarrow_R \mathsf{Kg}(1^k)$.

The security we require for PKE is IND-CCA2 security [22, 9]. We define the advantage of an adversary $\mathsf{A} = (\mathsf{A}_1, \mathsf{A}_2)$ as

$$\mathsf{Adv}^{\mathrm{cca2}}_{\mathsf{PKE},\mathsf{A}}(k) \stackrel{\mathrm{def}}{=} \left| \Pr\left[b = b' \;:\; \begin{array}{l} (pk, sk) \leftarrow_R \mathsf{Kg}(1^k) \\ (m_0, m_1, St) \leftarrow_R \mathsf{A}_1^{\mathsf{Dec}(sk,\cdot)}(pk) \\ b \leftarrow_R \{0, 1\};\ C^* \leftarrow_R \mathsf{Enc}(pk, m_b) \\ b' \leftarrow_R \mathsf{A}_2^{\mathsf{Dec}(sk,\cdot)}(C^*, St) \end{array} \right] - \frac{1}{2} \right| .$$

The adversary A_2 is restricted not to query $\mathsf{Dec}(sk, \cdot)$ with C^*. PKE scheme PKE is said to be indistinguishable against chosen-ciphertext attacks (IND-CCA2 secure in short) if the advantage function $\mathsf{Adv}^{\mathrm{cca2}}_{\mathsf{PKE},\mathsf{A}}(k)$ 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 $\mathsf{Adv}^{\mathrm{cca2}}_{\mathsf{PKE},t,Q}(k) = \max_{\mathsf{A}} \mathsf{Adv}^{\mathrm{cca2}}_{\mathsf{PKE},\mathsf{A}}(k)$, 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* (IND-CCA1 security), which is defined as IND-CCA2 security with the restriction that the adversary is not allowed to make decryption queries after having seen the challenge ciphertext.

2.3 Hash Proof Systems

Smooth Projective Hashing. We recall the notion of hash proof systems as introduced by Cramer and Shoup [3]. Let $\mathcal{C}, \mathcal{K}$ be sets and $\mathcal{V} \subset \mathcal{C}$ a language. In the context of public-key encryption (and viewing a hash proof system as a key encapsulation mechanism (KEM) [4] with "special algebraic properties") one may think of $\mathcal{C}$ as the set of all *ciphertexts*, $\mathcal{V} \subset \mathcal{C}$ as the set of all *valid (consistent) ciphertexts*, and $\mathcal{K}$ as the set of all *symmetric keys*. Let $\Lambda_{sk} : \mathcal{C} \to \mathcal{K}$ be a hash function indexed with $sk \in \mathcal{SK}$, where $\mathcal{SK}$ is a set. A hash function Λ_{sk} is *projective* if there exists a projection $\mu : \mathcal{SK} \to \mathcal{PK}$ such that $\mu(sk) \in \mathcal{PK}$

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, following [14] we define universal$_1$ and universal$_2$ as follows.

universal$_1$. The projective hash function is ϵ_1-*almost universal$_1$* if for all $C \in \mathcal{C} \setminus \mathcal{V}$,

$$\Delta\left[(pk, \Lambda_{sk}(C)\,,\,(pk, K)\right] \leq \epsilon_1 \tag{1}$$

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

universal$_2$. The projective hash function is ϵ_2-*almost universal$_2$* if for all $C, C^* \in \mathcal{C} \setminus \mathcal{V}$ with $C \neq C^*$,

$$\Delta\left[(pk, \Lambda_{sk}(C^*), \Lambda_{sk}(C)\,,\,(pk, \Lambda_{sk}(C^*), K)\right] \leq \epsilon_2 \tag{2}$$

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

We introduce the following relaxation of the universal$_1$ property which only requires that for all $C \in \mathcal{C} \setminus \mathcal{V}$, given $pk = \mu(sk)$, $\Lambda_{sk}(C)$ has high min entropy.

κ-entropic. The projective hash function is ϵ_1-*almost κ-entropic* if for all $C \in \mathcal{C} \setminus \mathcal{V}$,

$$\Pr\left[\, H_\infty(\Lambda_{sk}(C) \mid pk) \geq \kappa \,\right] \geq 1 - \epsilon_1 \tag{3}$$

where in the above $pk = \mu(sk)$ for $sk \leftarrow_R \mathcal{SK}$.

From the above definitions, we get the following simple lemma.

Lemma 2.1 Every ϵ_1-almost universal$_1$ projective hash function is ϵ_1-almost κ-entropic, for $\kappa = \lg(|\mathcal{K}|)$.

Collision probability. To a projective hash function we also associate the collision probability, δ, defined as

$$\delta = \max_{C, C^* \in \mathcal{C} \setminus \mathcal{V}, C \neq C^*} \left(\Pr_{sk}\left[\,\Lambda_{sk}(C) = \Lambda_{sk}(C^*)\,\right]\right). \tag{4}$$

Hash Proof System. A hash proof system $\mathsf{HPS} = (\mathsf{Param}, \mathsf{Pub}, \mathsf{Priv})$ consists of three algorithms. The randomized algorithm $\mathsf{Param}(1^k)$ generates parametrized instances of $params = (group, \mathcal{K}, \mathcal{C}, \mathcal{V}, \mathcal{PK}, \mathcal{SK}, \Lambda_{(\cdot)} : \mathcal{C} \to \mathcal{K}, \mu : \mathcal{SK} \to \mathcal{PK})$, 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 r of the fact that $C \in \mathcal{V}$ and returns $K = \Lambda_{sk}(C)$. The deterministic private evaluation algorithm Priv inputs $sk \in \mathcal{SK}$ and returns $\Lambda_{sk}(C)$, without knowing a witness. We further assume that μ is efficiently computable and that there are efficient algorithms given for sampling $sk \in \mathcal{SK}$, sampling $C \in \mathcal{V}$ uniformly (or negligibly close to) together with a witness r, sampling $C \in \mathcal{C}$ uniformly, and for checking membership in $\mathcal{C}$.

We say that a hash proof system is universal$_1$ (resp., κ-entropic, universal$_2$) if for all possible outcomes of $\mathsf{Param}(1^k)$ the underlying projective hash function is $\epsilon_1(k)$-almost universal$_1$ (resp., $\epsilon_1(k)$-almost entropic, $\epsilon_2(k)$-almost universal$_2$) for negligible $\epsilon_1(k)$ (resp., $\epsilon_2(k)$). Furthermore, we say that a hash proof system is perfectly universal$_1$ (resp., κ-entropic, universal$_2$) if $\epsilon_1(k) = 0$ (resp., $\epsilon_2(k)$).

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

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

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

Hash Proof Systems with Trapdoor. Following [17], we also require that the subset membership problem can be efficiently solved with a master trapdoor. More formally, we assume that the hash proof

system HPS additionally contains two algorithms Param' and Decide. The alternative parameter generator $\mathsf{Param}'(1^k)$ generates output indistinguishable from the one of $\mathsf{Param}(1^k)$ and additionally returns a trapdoor ω. The subset membership deciding algorithm $\mathsf{Decide}(params, \omega, x)$ returns 1 if $x \in \mathcal{V}$, and 0, otherwise. All known hash proof systems actually have such a trapdoor.

2.4 Symmetric Encryption

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

The most common notion of security for symmetric encryption is that of (one-time) ciphertext indistinguishability ($\mathsf{IND\text{-}OT}$), 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*. (One-time) ciphertext integrity ($\mathsf{INT\text{-}OT}$) 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. Formal definitions and constructions are provided in the full version [16]. There we also recall how to build a symmetric scheme with k-bit keys secure in the sense of $\mathsf{AE\text{-}OT}$ from a (computationally secure) one-time symmetric encryption scheme, a (computationally secure) MAC, and a (computationally secure) key-derivation function.

3 Randomness Extraction

In this section we review a few concepts related to probability distributions and extracting uniform bits from weak random sources. As a technical tool for our new paradigm, we will prove the following generalization of the leftover hash lemma [13]: if H is 4-wise independent, then $(\mathsf{H}, \mathsf{H}(X), \mathsf{H}(\tilde{X}))$ is close to uniformly random, where $X, \tilde{X}$ can be dependent (but of course we have to require $X \neq \tilde{X}$).

Let $\mathcal{H}$ be a family of hash functions $\mathsf{H} : \mathcal{X} \to \mathcal{Y}$. With $|\mathcal{H}|$ we denote the number of functions in this family and when sampling from $\mathcal{H}$ we assume a uniform distribution. Let $k > 1$ be an integer, the hash-family $\mathcal{H}$ is k-wise independent if for any sequence of distinct elements $x_1, \ldots, x_k \in \mathcal{X}$ the random variables $\mathsf{H}(x_1), \ldots, \mathsf{H}(x_k)$, where $\mathsf{H} \leftarrow_R \mathcal{H}$, are uniform random. We refer to [6] for a simple and efficient construction of a compressing k-wise independent hash function.

Recall that the leftover hash lemma states that for a 2-wise independent hash function H and a random variable X with min-entropy exceeding the bitlength of H's range, the random variable $(\mathsf{H}, \mathsf{H}(X))$ is close to uniformly random [13].

Lemma 3.1 Let $X \in \mathcal{X}$ be a random variable where $H_\infty(X) \geq \kappa$. Let $\mathcal{H}$ be a family of pairwise independent hash functions with domain $\mathcal{X}$ and image $\{0,1\}^\ell$. Then for $\mathsf{H} \leftarrow_R \mathcal{H}$ and $U_\ell \leftarrow_R \{0,1\}^\ell$, $\Delta\left[(\mathsf{H}, \mathsf{H}(X)), (\mathsf{H}, U_\ell)\right] \leq 2^{(\ell-\kappa)/2}$.

We will now prove a generalization of the leftover hash lemma that states that even when the hash function is evaluated in two distinct points, the two outputs jointly still look uniformly random. To make this work, we need a 4-wise independent hash function and, as before, sufficient min-entropy in the input distribution. We do note that, unsurprisingly, the loss of entropy compared to Lemma 3.1 is higher, as expressed in the bound on the statistical distance (or alternatively, in the bound on the min-entropy required in the input distribution).

Lemma 3.2 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 $\Pr[X = \tilde{X}] \leq \delta$. Let $\mathcal{H}$ be a family of 4-wise independent hash functions with domain $\mathcal{X}$ and image $\{0,1\}^\ell$. Then for $\mathsf{H} \leftarrow_R \mathcal{H}$ and $U_{2\ell} \leftarrow_R \{0,1\}^{2\ell}$,

$$\Delta\left[(\mathsf{H}, \mathsf{H}(X), \mathsf{H}(\tilde{X})), (\mathsf{H}, U_{2\ell})\right] \leq \sqrt{1+\delta} \cdot 2^{\ell-\kappa/2} + \delta \,.$$

Proof: We will first prove the lemma for $\delta = 0$, and at the end show how the general case $\delta > 0$ can be reduced to it. Let $d = \lg |\mathcal{H}|$. For a random variable Y and Y' an independent copy of Y, we denote with $\mathsf{Col}[Y] = \Pr[Y = Y']$ the collision probability of Y. In particular,

$$\begin{aligned}
&\mathsf{Col}[(\mathsf{H}, \mathsf{H}(X), \mathsf{H}(\tilde{X}))] \\
&= \Pr_{\mathsf{H},(X,\tilde{X}),\mathsf{H}',(X',\tilde{X}')}[(\mathsf{H}, \mathsf{H}(X), \mathsf{H}(\tilde{X})) = (\mathsf{H}', \mathsf{H}'(X'), \mathsf{H}'(\tilde{X}'))] \\
&= \Pr_{\mathsf{H},\mathsf{H}'}[\mathsf{H} = \mathsf{H}'] \cdot \Pr_{\mathsf{H},(X,\tilde{X}),\mathsf{H}',(X',\tilde{X}')}[(\mathsf{H}(X), \mathsf{H}(\tilde{X})) = (\mathsf{H}'(X'), \mathsf{H}'(\tilde{X}')) \mid \mathsf{H} = \mathsf{H}'] \\
&= \underbrace{\Pr_{\mathsf{H},\mathsf{H}'}[\mathsf{H} = \mathsf{H}']}_{=2^{-d}} \cdot \Pr_{\mathsf{H},(X,\tilde{X}),(X',\tilde{X}')}[(\mathsf{H}(X), \mathsf{H}(\tilde{X})) = (\mathsf{H}(X'), \mathsf{H}(\tilde{X}'))] \,. \qquad (5)
\end{aligned}$$

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

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

Where in the first step we used that $\delta = 0$, and thus $X \neq \tilde{X}, X' \neq \tilde{X}'$. 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 (5) as

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

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

$$\|Y - U\|_2^2 = \mathsf{Col}[Y] - |\mathcal{Y}|^{-1} \,.$$

In particular,

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

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

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

This concludes the proof of (3.2) for $\delta = 0$. Now consider $X, \tilde{X}$ as in the statement of the lemma where $\Pr[X = \tilde{X}] \leq \delta$ for some $\delta > 0$. Let π denote any permutation over $\mathcal{X}$ without a fixpoint, i.e., $\pi(x) \neq x$ for all $x \in \mathcal{X}$. Let $(Y, \tilde{Y})$ be sampled as follows: first sample $(X, \tilde{X})$, if $X \neq \tilde{X}$ let $(Y, \tilde{Y}) = (X, \tilde{X})$, otherwise sample $Y \leftarrow_R \mathcal{X}$ uniformly at random and set $\tilde{Y} := \pi(Y)$. By definition $\Pr[Y = \tilde{Y}] = 0$, and as $(Y, \tilde{Y})$ has the same distribution as $(X, \tilde{X})$ except with probability δ, $\Delta\left[(X, \tilde{X}) \,,\, (Y, \tilde{Y})\right] \leq \delta$. Moreover, using that $\max_{x \in \mathcal{X}} \Pr[X = x] \leq 2^{-\kappa}$

$$\max_{x \in \mathcal{X}} \Pr[Y = x] \leq 2^{-\kappa} + \delta/|\mathcal{X}| \leq (1 + \delta)2^{-\kappa} \,.$$

Thus $H_\infty(Y) \geq \kappa - \lg(1+\delta)$, and similarly $H_\infty(\tilde{Y}) \geq \kappa - \lg(1+\delta)$. We can now apply the lemma for the special case $\delta = 0$ (which we proved) and get

$$\Delta\left[(\mathsf{H}, \mathsf{H}(Y), \mathsf{H}(\tilde{Y}))\,,\,(\mathsf{H}, U_{2\ell})\right] \leq 2^{\ell-(\kappa-\lg(1+\delta))/2} = \sqrt{1+\delta}\cdot 2^{\ell-\kappa/2}\,.$$

The lemma now follows as

$$\begin{aligned}
&\Delta\left[(\mathsf{H}, \mathsf{H}(X), \mathsf{H}(\tilde{X}))\,,\,(\mathsf{H}, U_{2\ell})\right] \\
&\quad\leq\quad \Delta\left[(\mathsf{H}, \mathsf{H}(Y), \mathsf{H}(\tilde{Y}))\,,\,(\mathsf{H}, U_{2\ell})\right] + \Delta\left[(X, \tilde{X})\,,\,(Y, \tilde{Y})\right] \\
&\quad\leq\quad \sqrt{1+\delta}\cdot 2^{\ell-\kappa/2} + \delta\,.
\end{aligned}$$

∎

4 Hybrid Encryption from Randomness Extraction

In this section we revisit the general construction of hybrid encryption from universal$_2$ hash proof systems. As our main technical result we show an efficient transformation from a κ-entropic to a universal$_2$ HPS, so in particular also from a universal$_1$ to a universal$_2$ HPS. Combining the latter universal$_2$ HPS with an AE-OT secure symmetric cipher gives an IND-CCA2 secure hybrid encryption scheme. This result can be readily applied to all known hash proof systems with a hard subset membership problem that are universal$_1$ (e.g., from Paillier's DCR, the DDH/n-Linear [14, 23] assumptions) or κ-entropic (e.g., from the QR [3] assumption) to obtain a number of new IND-CCA2 secure hybrid encryption schemes. More concretely, in Section 5 we will discuss the consequences for DDH-based schemes and in Section 6 for QR-based schemes.

4.1 Hybrid Encryption from HPSs

Recall the notion of a hash proof system from Section 2.3. Kurosawa and Desmedt [17] proposed the following hybrid encryption scheme which improved the schemes from Cramer and Shoup [3].

Let $\mathsf{HPS} = (\mathsf{Param}, \mathsf{Pub}, \mathsf{Priv})$ be a hash proof system and let $\mathsf{SE} = (\mathsf{E}, \mathsf{D})$ be an AE-OT secure symmetric encryption scheme whose key-space $\mathcal{K}_{\mathsf{SE}}$ matches the key-space $\mathcal{K}$ of the HPS.[2] The system parameters of the scheme consist of $params \leftarrow_R \mathsf{Param}(1^k)$.

$\mathsf{Kg}(k)$**.** Choose random $sk \leftarrow_R \mathcal{SK}$ and define $pk = \mu(sk) \in \mathcal{PK}$. Return (pk, sk).

$\mathsf{Enc}(pk, m)$**.** Pick $C \leftarrow_R \mathcal{V}$ together with its witness r that $C \in \mathcal{V}$. The session key $K = \Lambda_{sk}(C) \in \mathcal{K}$ is computed as $K \leftarrow \mathsf{Pub}(pk, C, r)$. 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 $\{m, \perp\} \leftarrow \mathsf{D}_K(\psi)$.

Note that the trapdoor property of the HPS is not used in the actual scheme: it is only needed in the proof. However, as an alternative the trapdoor can be added to the secret key.[3] This allows explicit rejection of invalid ciphertexts during decryption. The security of this explicit-rejection variant is identical to that of the scheme above.

The following was proved in [17, 11, 14].

Theorem 4.1 Assume HPS is (ϵ_2) universal$_2$ with hard subset membership problem (with trapdoor), and SE is AE-OT secure. Then the encryption scheme is secure in the sense of IND-CCA2. In particular,

$$\mathsf{Adv}^{\mathrm{cca2}}_{\mathsf{PKE},t,Q}(k) \leq \mathsf{Adv}^{\mathrm{sm}}_{\mathsf{HPS},t}(k) + 2Q\cdot\mathsf{Adv}^{\mathrm{int\text{-}ot}}_{\mathsf{SE},t}(k) + \mathsf{Adv}^{\mathrm{ind\text{-}ot}}_{\mathsf{SE},t}(k) + Q\cdot\epsilon_2\,.$$

[2] The requirement that $\mathcal{K}_{\mathsf{SE}} = \mathcal{K}$ is not a real restriction since once can always apply a key-derivation function $\mathsf{KDF} : \mathcal{K} \to \mathcal{K}_{\mathsf{SE}}$.

[3] Strictly speaking the algorithm to sample elements in $\mathcal{V}$ (with witness) should then be regarded as part of the public key instead of simply a system parameter.

We remark that even though in general the KEM part of the above scheme cannot be proved IND-CCA2 secure [1], it can be proved "IND-CCCA" secure. The latter notion was defined in [14] and proved sufficient to yield IND-CCA2 secure encryption when combined with an AE-OT secure cipher. We also remark that the security bound in the above theorem implicitly requires that the image of $\Lambda_{sk}(\cdot)$ restricted to $\mathcal{V}$ is sufficiently large (say, contains at least 2^k elements). This is since otherwise the key-space of the symmetric scheme is too small and the two advantages functions $\mathsf{Adv}^{\text{int-ot}}_{\mathsf{SE},t}(k)$ and $\mathsf{Adv}^{\text{ind-ot}}_{\mathsf{SE},t}(k)$ cannot be negligible.

There is also an analogue "lite version" for universal$_1$ HPS, giving IND-CCA1 only (and using a slightly weaker asymmetric primitive). It can be stated as follows.

Theorem 4.2 Assume HPS is universal$_1$ with hard subset membership problem and SE is WAE-OT secure. Then the encryption scheme is secure in the sense of IND-CCA1.

We note that if the HPS is only κ-entropic then we can use the standard Leftover Hash Lemma (Lemma 3.1) to obtain a universal$_1$ HPS.

4.2 A generic transformation from κ-entropic to universal$_2$ HPSs

We propose the following transformation. Given a projective hash function $\Lambda_{sk} : \mathcal{C} \to \mathcal{K}$ with projection $\mu : \mathcal{SK} \to \mathcal{PK}$ and a family of hash functions $\mathcal{H}$ with $\mathsf{H} : \mathcal{K} \to \{0,1\}^\ell$. Then we define the hashed variant of it as:

$$\Lambda^{\mathcal{H}}_{sk} : \mathcal{C} \to \{0,1\}^\ell, \quad \Lambda^{\mathcal{H}}_{sk}(C) := \mathsf{H}(\Lambda_{sk}(C)) \ .$$

We also define $\mathcal{PK}^{\mathcal{H}} = \mathcal{PK} \times \mathcal{H}$ and $\mathcal{SK}^{\mathcal{H}} = \mathcal{SK} \times \mathcal{H}$, such that the hashed projection is given by $\mu^{\mathcal{H}} : \mathcal{SK}^{\mathcal{H}} \to \mathcal{PK}^{\mathcal{H}}$, $\mu^{\mathcal{H}}(sk, \mathsf{H}) = (pk, \mathsf{H})$. This also induces a transformation from a hash proof system HPS into $\mathsf{HPS}^{\mathcal{H}}$, where the above transformation is applied to the projective hash function. Note that $\mathcal{C}$ and $\mathcal{V}$ are the same for HPS and $\mathsf{HPS}^{\mathcal{H}}$ (so that in particular the trapdoor property for the language $\mathcal{V}$ is inherited).

We are now ready to state our main theorem. To simplify the bounds, we will henceforth assume that $\delta \leq \frac{1}{2}$ and $\ell \geq 6$.

Theorem 4.3 Assume HPS is ϵ_1-almost κ-entropic with collision probability $\delta \leq 1/2$ and $\mathcal{H}$ is a family of 4-wise independent hash functions with $\mathsf{H} : \mathcal{K} \to \{0,1\}^\ell$ and $\ell \geq 6$. Then $\mathsf{HPS}^{\mathcal{H}}$ is ϵ_2-almost universal$_2$ for

$$\epsilon_2 = 2^{\ell - \frac{\kappa-1}{2}} + 3\epsilon_1 + \delta \ .$$

Proof: Let us consider, for all $C, C^* \in \mathcal{C} \setminus \mathcal{V}$ with $C \neq C^*$, the statistical distance relevant for universal$_2$ for HPS and let Y be the following random variable

$$Y := (pk, \mathsf{H}, U_{2\ell}) \ ,$$

where $pk = \mu(sk)$ for $sk \leftarrow_R \mathcal{SK}$, $\mathsf{H} \leftarrow_R \mathcal{H}$ and $U_{2\ell} \leftarrow_R \{0,1\}^{2\ell}$. Then we can use the triangle inequality to get

$$\begin{aligned} &\Delta\left[(pk, \mathsf{H}, \mathsf{H}(\Lambda_{sk}(C^*)), \mathsf{H}(\Lambda_{sk}(C)) \ , \ (pk, \mathsf{H}, \mathsf{H}(\Lambda_{sk}(C^*)), U_\ell)\right] \\ &\leq \Delta\left[(pk, \mathsf{H}, \mathsf{H}(\Lambda_{sk}(C^*)), \mathsf{H}(\Lambda_{sk}(C))) \ , \ Y\right] + \Delta\left[Y \ , \ (pk, \mathsf{H}, \mathsf{H}(\Lambda_{sk}(C^*)), U_\ell)\right] \end{aligned} \tag{6}$$

where as before $pk = \mu(sk)$ for $sk \leftarrow_R \mathcal{SK}$, $\mathsf{H} \leftarrow_R \mathcal{H}$ and $U_\ell \leftarrow_R \{0,1\}^\ell$. In the latter probability space, let E_{C^*} be the event that $H_\infty(\Lambda_{sk}(C^*) \mid pk) \geq \kappa$. We can upper bound the second term of (6), using again the triangle inequality in the first step, as

$$\begin{aligned} \Delta\left[Y \ , \ (pk, \mathsf{H}, \mathsf{H}(\Lambda_{sk}(C^*)), U_\ell)\right] &\leq \Delta_{E_{C^*}}\left[Y \ , \ (pk, \mathsf{H}, \mathsf{H}(\Lambda_{sk}(C^*)), U_\ell)\right] + \Pr_{sk}[\neg E_{C^*}] \\ &\leq 2^{\frac{\ell-\kappa}{2}} + \epsilon_1 \ . \end{aligned} \tag{7}$$

In the last step we used the (standard) leftover hash-lemma (Lemma 3.1). Let E_C be the event that $H_\infty(\Lambda_{sk}(C)) \mid pk) \geq \kappa$. Similarly, we now bound the first term of (6) as

$$\begin{aligned}
&\Delta\left[(pk, \mathsf{H}, \mathsf{H}(\Lambda_{sk}(C^*)), \mathsf{H}(\Lambda_{sk}(C)))\,,\, Y\right] \\
&\quad\leq\quad \Delta_{E_C \wedge E_{C^*}}\left[(pk, \mathsf{H}, \mathsf{H}(\Lambda_{sk}(C^*)), \mathsf{H}(\Lambda_{sk}(C)))\,,\, Y\right] + \Pr_{sk}[\neg E_C \vee \neg E_{C^*}] \\
&\quad\leq\quad \sqrt{1+\delta} \cdot 2^{\ell - \frac{\kappa}{2}} + \delta + 2\epsilon_1\,,
\end{aligned}$$

where in the last step we used Lemma 3.2. Combining this with (7) and using $\delta \leq 1/2$ and $\ell \geq 6$ we obtain the required bound on ϵ_2. ∎

4.3 Hybrid Encryption from κ-entropic HPSs

Putting the pieces from the last two sections together we get a new IND-CCA2 secure hybrid encryption scheme from any κ-entropic hash proof system. Let $\mathsf{HPS} = (\mathsf{Param}, \mathsf{Pub}, \mathsf{Priv})$ be a hash proof system, let $\mathcal{H}$ be a family of hash functions with $\mathsf{H} : \mathcal{K} \to \{0,1\}^\ell$ and let $\mathsf{SE} = (\mathsf{E}, \mathsf{D})$ be an AE-OT secure symmetric encryption scheme with key-space $\mathcal{K}_{\mathsf{SE}} = \{0,1\}^\ell$. The system parameters of the scheme consist of $params \leftarrow_R \mathsf{Param}(1^k)$.

$\mathsf{Kg}(k)$**.** Choose random $sk \leftarrow_R \mathcal{SK}$ and define $pk = \mu(sk) \in \mathcal{PK}$. Pick a random hash function $\mathsf{H} \leftarrow_R \mathcal{H}$. The public-key is (H, pk), the secret-key is (H, sk).

$\mathsf{Enc}(pk, m)$**.** Pick $C \leftarrow_R \mathcal{V}$ together with its witness r that $C \in \mathcal{V}$. The session key $K = \mathsf{H}(\Lambda_{sk}(C)) \in \{0,1\}^\ell$ is computed as $K \leftarrow \mathsf{H}(\mathsf{Pub}(pk, C, r))$. The symmetric ciphertext is $\psi \leftarrow \mathsf{E}_K(m)$. Return the ciphertext (C, ψ).

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

Combining Theorems 4.1 and 4.3 gives us the following corollary.

Corollary 4.4 Assume HPS is (ϵ_1-almost) κ-entropic with hard subset membership problem and with collision probability $\delta(k)$, that $\mathcal{H}$ is a family of 4-wise independent hash functions with $\mathsf{H} : \mathcal{K} \to \{0,1\}^{\ell(k)}$, and that SE is AE-OT secure. If $2^{\ell(k) - \kappa(k)/2}$ and $\delta(k)$ are negligible, then the encryption scheme above is secure in the sense of IND-CCA2. In particular,

$$\mathsf{Adv}^{\mathrm{cca2}}_{\mathsf{PKE},t,Q}(k) \leq \mathsf{Adv}^{\mathrm{sm}}_{\mathsf{HPS},t}(k) + 2Q \cdot \mathsf{Adv}^{\text{int-ot}}_{\mathsf{SE},t}(k) + \mathsf{Adv}^{\text{ind-ot}}_{\mathsf{SE},t}(k) + Q \cdot (2^{\ell - \frac{\kappa-1}{2}} + 3\epsilon_1 + \delta).$$

5 Instantiations from the DDH Assumption

In this section we discuss two practical instantiations of our randomness extraction framework whose security is based on the DDH assumption.

5.1 The Decisional Diffie-Hellman (DDH) Assumption

A group scheme $\mathcal{GS}$ [4] 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 $x \leftarrow_R \mathbb{G}$ and an efficient membership algorithm. We define the ddh-advantage of an adversary B as

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

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

5.2 Variant 1: the Scheme HE_1

THE UNIVERSAL$_1$ HASH PROOF SYSTEM. We recall a universal$_1$ HPS by Cramer and Shoup [3], whose hard subset membership problem is based on the DDH assumption. Let $\mathcal{GS}$ be a group scheme where $\mathcal{GR}_k$ specifies $(\mathbb{G}, p)$ and let g_1, g_2 be two 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 $C \in \mathcal{V}$. The trapdoor generator Param picks a uniform trapdoor $\omega \in \mathbb{Z}_p$ and computes $g_2 = g_1^\omega$. Note that using trapdoor ω, algorithm Decide can efficiently perform subset membership tests for $C = (c_1, c_2) \in \mathcal{C}$ by checking whether $c_1^\omega = c_2$.

Let $\mathcal{SK} = \mathbb{Z}_p^2$, $\mathcal{PK} = \mathbb{G}$, and $\mathcal{K} = \mathbb{G}$. For $sk = (x_1, x_2) \in \mathbb{Z}_p^2$, 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

$$\Lambda_{sk}(C) := c_1^{x_1} c_2^{x_2} \ . \tag{8}$$

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

$$K = X^r \ .$$

Correctness follows by (8) and the definition of μ. This completes the description of HPS. Clearly, under the DDH assumption, the subset membership problem is hard in HPS. Moreover, this HPS is known to be (perfect) universal$_1$ [3].

Lemma 5.1 The above HPS is perfect universal$_1$ (so $\epsilon_1 = 0$) with collision probability $\delta = 1/p$.

Proof: To show that the HPS is universal$_1$, it suffices to show that given the public key X and any pair $(C, K) \in (\mathcal{C} \setminus \mathcal{V}) \times \mathcal{K}$, there exists exactly one secret key sk such that $\mu(sk) = X$ and $\Lambda_{sk}(C) = K$. Let $\omega \in \mathbb{Z}_p^*$ be such that $g_2 = g_1^\omega$, write $C = (g_1^r, g_2^s)$ for $r \neq s$ and consider a possible secret key $sk = (x_1, x_2) \in \mathbb{Z}_p^2$. Then we simultaneously need that $\mu(sk) = g_1^{x_1 + \omega x_2} = X = g^x$ (for some $x \in \mathbb{Z}_p$) and $\Lambda_{sk}(C) = g_1^{r x_1 + s\omega x_2} = K = g_1^y$ (for some $y \in \mathbb{Z}_p$). Then, using linear algebra, x_1 and x_2 follow uniquely from r, s, x, y and ω provided that the relevant determinant $(s - r)\omega \neq 0$. This is guaranteed here since $r \neq s$ and $\omega \neq 0$.

To verify the bound on the collision probability δ it suffices —due to symmetry— to determine for any distinct pair $(C, C^*) \in (\mathcal{C} \setminus \mathcal{V})^2$ the probability $\Pr_{sk}[\Lambda_{sk}(C) = \Lambda_{sk}(C^*)]$. In other words, for $(r, s) \neq (r', s')$ (with $r \neq s$ and $r' \neq s'$, but that is irrelevant here) we have that

$$\begin{aligned}
\delta &= \Pr_{x_1, x_2 \leftarrow_R \mathbb{Z}_p}[g_1^{r x_1 + x_2 \omega s} = g_1^{r' x_1 + x_2 \omega s'}] \\
&= \Pr_{x_1, x_2 \leftarrow_R \mathbb{Z}_p}[r x_1 + x_2 \omega s = r' x_1 + x_2 \omega s'] \\
&= 1/p \ .
\end{aligned}$$

(For the last step, use that if $r \neq r'$ for any x_2 only one x_1 will "work"; if $r = r'$ then necessarily $s \neq s'$ and for any x_1 there is a unique x_2 to satisfy the equation.) ∎

THE HYBRID ENCRYPTION SCHEME HE_1. We apply the transformation from Section 4.3 to the above HPS and obtain an hybrid encryption scheme which is depicted in Figure 1.

Theorem 5.2 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 $\lg p \geq 4\ell(k)$, and let SE be a symmetric encryption scheme with key-space $\mathcal{K}_{\mathsf{SE}} = \{0,1\}^{\ell(k)}$. that is secure in the sense of $\mathsf{AE\text{-}OT}$. Then HE_1 is secure in the sense of $\mathsf{IND\text{-}CCA2}$. In particular,

$$\mathsf{Adv}^{\mathrm{cca2}}_{\mathsf{HE}_1, t, Q}(k) \leq \mathsf{Adv}^{\mathrm{ddh}}_{\mathcal{GS}, t}(k) + 2Q \cdot \mathsf{Adv}^{\mathrm{int\text{-}ot}}_{\mathsf{SE}, t}(k) + \mathsf{Adv}^{\mathrm{ind\text{-}ot}}_{\mathsf{SE}, t}(k) + Q \cdot 2^{-\ell(k)+1} \ .$$

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

Figure 1: Hybrid encryption scheme $\mathsf{HE}_1 = (\mathsf{Kg}, \mathsf{Enc}, \mathsf{Dec})$ obtained by applying our randomness extraction framework to the HPS from Section 5.2.

$\mathsf{Kg}(1^k)$	$\mathsf{Enc}(pk, m)$	$\mathsf{Dec}(sk, C)$
$\omega, x \leftarrow_R \mathbb{Z}_p$	$r \leftarrow_R \mathbb{Z}_p^*$	Parse C as (c_1, c_2, ψ)
$g_2 \leftarrow g_1^\omega$; $X \leftarrow g_1^x$	$c_1 \leftarrow g_1^r$; $c_2 \leftarrow g_2^r$	if $c_1^\omega \neq c_2$ return $\perp$
Pick $\mathsf{H} \leftarrow_R \mathcal{H}$	$K \leftarrow \mathsf{H}(X^r)$	$K \leftarrow \mathsf{H}(c_1^x)$
$pk \leftarrow (g_2, X, \mathsf{H})$; $sk \leftarrow (x, \omega)$	$\psi \leftarrow \mathsf{E}_K(m)$	Return $\{m, \perp\} \leftarrow \mathsf{D}_K(\psi)$
Return (sk, pk)	Return $C = (c_1, c_2, \psi)$	

Figure 2: Hybrid encryption scheme $\mathsf{HE}_1^{\mathsf{er}} = (\mathsf{Kg}, \mathsf{Enc}, \mathsf{Dec})$. A variant of HE_1 with explicit rejection.

Proof: By Lemma 5.1 the HPS is (perfectly) universal$_1$ and therefore (by Lemma 2.1) it is also (perfectly) κ-entropic with $\kappa = \lg(|\mathcal{K}|) = \lg p \geq 4\ell(k)$. It leaves to bound the loss due to the κ-entropic to universal$_2$ HPS transformation from Corollary 4.4:

$$(1+\delta)2^{\ell - \frac{\kappa}{2}} + 2^{\frac{\ell-\kappa}{2}} + 3\epsilon_1 + \delta \leq 2^{-\ell+1}$$

where we used that $|\mathcal{K}| = |\mathbb{G}| = p \geq 2^{4\ell}$ and (by Lemma 5.1) $\epsilon_1 = 0$ and $\delta = 1/p$. ∎

We remark that in terms of concrete security, Theorem 5.2 requires the image $\{0,1\}^{\ell(k)}$ of H to be sufficiently small, i.e., $\ell(k) \leq \frac{1}{4}\lg p$. For a symmetric cipher with $\ell(k) = k = 80$ bits keys we are forced to use groups of order $\lg p = 4k = 320$ bits. For some specific groups such as elliptic curves this can be a drawback since there one typically works with groups of order $\lg p = 2k = 160$ bits.

Relation to Damgård's ElGamal. In HE_1, invalid ciphertexts of the form $c_1^\omega \neq c_2$ are rejected implicitly by authenticity properties of the symmetric cipher. Similar to [4], a variant of this scheme, $\mathsf{HE}_1^{\mathsf{er}} = (\mathsf{Kg}, \mathsf{Enc}, \mathsf{Dec})$, in which such invalid ciphertexts get explicitly rejected is given in Figure 2. The scheme is slightly simplified compared to a direct explicit version that adds the trapdoor to the secret key; the simplification can be justified using the techniques of Lemma 5.1.

We remark that, interestingly, Damgård's encryption scheme [5] (also known as Damgård's ElGamal) is a special case of $\mathsf{HE}_1^{\mathsf{er}}$ from Figure 2 where the hash function H is the identity function (or an easy-to-invert, canonical embedding of the group into, say, the set of bitstrings) and SE is "any easy to invert group operation" [5], for example the one-time pad with $\mathsf{E}_K(m) = K \oplus m$. In his paper, Damgård proved IND-CCA1 security of his scheme under the DDH assumption and the *knowledge of exponent* assumption in $\mathcal{GS}$.[4] Our schemes $\mathsf{HE}_1^{\mathsf{er}}$ and HE_1 can therefore be viewed as hybrid versions of Damgård's ElGamal scheme, that can be proved IND-CCA2 secure under the DDH assumption.

5.3 Variant 2: the Scheme HE_2

The universal$_1$ hash proof system. We now give an alternative (and new) universal$_1$ hash proof system from the DDH assumption. Keep $\mathcal{C}$ and $\mathcal{V}$ as in Section 5.2. Define $\mathcal{SK} = \mathbb{Z}_p^4$, $\mathcal{PK} = \mathbb{G}^2$, and

[4] To be more precise, Damgård only formally proved one-way (OW-CCA1) security of his scheme, provided that the original ElGamal scheme is OW-CPA secure. But he also remarks that his proof can be reformulated to prove IND-CCA1 security, provided that ElGamal itself is IND-CPA secure. IND-CPA security of ElGamal under the DDH assumption was only formally proved later [25].

$\mathsf{Kg}(1^k)$	$\mathsf{Enc}(pk, m)$	$\mathsf{Dec}(sk, C)$
$x_1, x_2, \hat{x}_1, \hat{x}_2 \leftarrow_R \mathbb{Z}_p$	$r \leftarrow_R \mathbb{Z}_p^*$	Parse C as (c_1, c_2, ψ)
$X \leftarrow g_1^{x_1} g_2^{x_2}$; $\hat{X} \leftarrow g_1^{\hat{x}_1} g_2^{\hat{x}_2}$	$c_1 \leftarrow g_1^r$; $c_2 \leftarrow g_2^r$	$K \leftarrow \mathsf{H}(c_1^{x_1} c_2^{x_2}, c_1^{\hat{x}_1} c_2^{\hat{x}_2})$
Pick $\mathsf{H} \leftarrow_R \mathcal{H}$	$K \leftarrow \mathsf{H}(X^r, \hat{X}^r)$	Return $\{m, \perp\} \leftarrow \mathsf{D}_K(\psi)$
$pk \leftarrow (X, \hat{X}, \mathsf{H})$	$\psi \leftarrow \mathsf{E}_K(m)$	
$sk \leftarrow (x_1, x_2, \hat{x}_1, \hat{x}_2)$	Return $C = (c_1, c_2, \psi)$	
Return (sk, pk)		

Figure 3: Hybrid encryption scheme $\mathsf{HE}_2 = (\mathsf{Kg}, \mathsf{Enc}, \mathsf{Dec})$ obtained by applying our randomness extraction framework to the HPS from Section 5.3.

$\mathcal{K} = \mathbb{G}^2$. For $sk = (x_1, x_2, \hat{x}_1, \hat{x}_2) \in \mathbb{Z}^4$, define $\mu(sk) = (X, \hat{X}) = (g_1^{x_1} g_2^{x_2}, g_1^{\hat{x}_1} g_2^{\hat{x}_2})$. For $C = (c_1, c_2) \in \mathcal{C}$ define

$$\Lambda_{sk}(C) := (c_1^{x_1} c_2^{x_2}, c_1^{\hat{x}_1} c_2^{\hat{x}_2}) \ .$$

This also 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

$$K = (X^r, \hat{X}^r) \ .$$

Similar to Lemma 5.1 we can prove the following.

Lemma 5.3 The above HPS is perfect universal$_1$ with collision probability $\delta = 1/p^2$.

The scheme HE_2. For our second hybrid encryption scheme HE_2 we make the same assumption as for HE_1, with the difference that $\mathcal{H}$ is now a family $\mathsf{H}_k : \mathbb{G}^2 \to \{0,1\}^{\ell(k)}$ of 4-wise independent hash functions with $\lg p \geq 2\ell(k)$. The resulting hybrid encryption scheme obtained by applying Corollary 4.4 (in conjuction with Lemma 5.3) is depicted in Figure 3.

Theorem 5.4 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 $\mathbb{G}^2$ to $\{0,1\}^{\ell(k)}$ with $\lg p \geq 2\ell(k)$, and let SE be a symmetric encryption scheme with key-space $\mathcal{K}_{\mathsf{SE}} = \{0,1\}^{\ell(k)}$ that is secure in the sense of $\mathsf{AE\text{-}OT}$. Then HE_2 is secure in the sense of $\mathsf{IND\text{-}CCA2}$. In particular,

$$\mathsf{Adv}^{\mathrm{cca2}}_{\mathsf{HE}_2,t,Q}(k) \leq \mathsf{Adv}^{\mathrm{ddh}}_{\mathcal{GS},t}(k) + 2Q \cdot \mathsf{Adv}^{\text{int-ot}}_{\mathsf{SE},t}(k) + \mathsf{Adv}^{\text{ind-ot}}_{\mathsf{SE},t}(k) + Q \cdot 2^{-\ell(k)+1} \ .$$

Note that HE_2 now only has the restriction $\lg p \geq 2\ell(k)$ which fits nicely with the typical choice of $\ell(k) = k$ and $\lg p = 2k$. So one is free to use any cryptographic group, in particular also elliptic curve groups.

Similar to $\mathsf{HE}_1^{\mathsf{er}}$, the variant $\mathsf{HE}_2^{\mathsf{er}}$ with explicit rejection can again be proven equivalent. In the explicit rejection variant, $\mathsf{HE}_2^{\mathsf{er}}$, the public-key contains the group elements $g_2 = g_1^{\omega}$, $X = g_1^x$, and $\hat{X} = g_1^{\hat{x}}$), and decryption first checks if $c_1^{\omega} = c_2$ and then computes $K = \mathsf{H}(c_1^x, c_1^{\hat{x}})$.

Relation to a scheme by Kurosawa and Desmedt. We remark that, interestingly, the scheme HE_2 is quite similar to the one by Kurosawa and Desmedt [17]. The only difference is that encryption in the latter defines the key as $K = X^{rt} \cdot \hat{X}^r \in \mathbb{G}$, where $t = \mathsf{T}(c_1, c_2)$ is the output of a (keyed) target collision-resistant hash function $\mathsf{T} : \mathbb{G} \times \mathbb{G} \to \mathbb{Z}_p$.

5.4 Efficiency Considerations

In this section we compare the efficiency of $\mathsf{HE}_1/\mathsf{HE}_2$ and their explicit rejection variants $\mathsf{HE}_1^{\mathsf{er}}/\mathsf{HE}_2^{\mathsf{er}}$ with the reference scheme KD by Kurosawa and Desmedt [17] and its variants [11, 14].

The drawback of HE_1 is that, in terms of concrete security, Theorem 5.2 requires the image $\{0,1\}^{\ell}$ of H to be sufficiently small, i.e., $\ell \leq \frac{1}{4} \lg p$. Consequently, for a symmetric cipher with $\ell = k = 80$ bits keys we are forced to use groups of order $\lg p \geq 4k = 320$ bits. For some specific groups such as elliptic curves this can be a drawback since there one typically works with groups of order $\lg p = 2k = 160$ bits. However,

Scheme	Assumption	Encryption	Decryption	Ciphertext	Key-size		Restriction
		#[multi/sequential,single]-exp		Size	Public	Secret	on $p = \|\mathbb{G}\|$
KD	DDH & TCR	$[1,2]$+tcr	$[1,0]$+tcr	$2\|\mathbb{G}\|+\|\psi\|$	$4\|\mathbb{G}\|+\|\mathsf{T}\|$	$4\|\mathbb{Z}_p\|$	$\lg p \geq 2\ell(k)$
$\mathsf{HE}_1^{\mathsf{er}}$	DDH	$[0,3]$+4wh	$[1,0]$+4wh	$2\|\mathbb{G}\|+\|\psi\|$	$3\|\mathbb{G}\|+\|\mathsf{H}\|$	$2\|\mathbb{Z}_p\|$	$\lg p \geq 4\ell(k)$
$\mathsf{HE}_2^{\mathsf{er}}$	DDH	$[0,4]$+4wh	$[1,0]$+4wh	$2\|\mathbb{G}\|+\|\psi\|$	$4\|\mathbb{G}\|+\|\mathsf{H}\|$	$4\|\mathbb{Z}_p\|$	$\lg p \geq 2\ell(k)$

Table 1: Efficiency comparison for known $\mathsf{CCA2}$-secure encryption schemes from the DDH assumption. All "symmetric" operations concerning the authenticated encryption scheme are ignored. The symbols "tcr" and "4wh" denote one application of a target collision-resistant hash function and 4-wise independent hash function, respectively.

for other more traditional groups such as prime subgroups of $\mathbb{Z}_q^*$ one sometimes takes a subgroup of order already satisfying the requirement $\lg p \geq 4k$. The scheme HE_2 overcomes this restriction at the cost of an additional exponentiation in the encryption algorithm.

Table 1 summarizes the efficiency of the schemes KD [17], $\mathsf{HE}_1^{\mathsf{er}}$, and $\mathsf{HE}_2^{\mathsf{er}}$. (A comparison of the explicit rejection variants seems more meaningful.) It is clear that when groups of similar size are used, our new scheme $\mathsf{HE}_1^{\mathsf{er}}$ will be the most efficient. But, as detailed above, typically $\mathsf{HE}_1^{\mathsf{er}}$ will have to work in a larger (sub)group. Even when underlying operations such as multiplication and squaring remain the same, the increased exponent length will make this scheme noticeably slower than the other two options.

6 Instantiations from the Quadaratic Residuosity Assumption

Quadratic residuosity assumption. Let $b = b(k) : \mathbb{N} \to \mathbb{N}^{>0}$ be a function. Let $N = pq$ be an RSA modulus consisting of distinct safe primes of bit-length $b/2$, i.e., $p = 2P + 1$ and $q = 2Q + 1$ for two primes P, Q. Let $\mathbb{J}_N$ denote the (cyclic) subgroup of elements in $\mathbb{Z}_N^*$ with Jacobi symbol 1, and let $\mathbb{QR}_N$ denote the unique (cyclic) subgroup of $\mathbb{Z}_N^*$ of order PQ (so in particular $\mathbb{QR}_N \subset \mathbb{J}_N$) which is the group of all squares modulo N. We assume the existence of an RSA instance generator RSAgen that generates the above elements, together with a random generator $g \in \mathbb{QR}_N$. The quadratic residuosity (QR) assumption states that distinguishing a random element from $\mathbb{QR}_N$ from a random element from $\mathbb{J}_N$ is computationally infeasible.

The hash proof system. Define $\mathcal{C} = \mathbb{J}_N$ and $\mathcal{V} = \mathbb{QR}_N = \{g^r \ : \ r \in \mathbb{Z}_{PQ}\}$. The value $r \in \mathbb{Z}$ is a witness of $C \in \mathcal{V}$. (Note that it is possible to sample an almost uniform element from $\mathcal{V}$ together with a witness by first picking $r \in \mathbb{Z}_{\lfloor N/4 \rfloor}$ and defining $C = g^r$.) Define $\mathcal{SK} = \mathbb{Z}_{2PQ}^n$, $\mathcal{PK} = \mathbb{QR}_N^n$, and $\mathcal{K} = \mathbb{J}_N^n$. For $sk = (x_1, \ldots, x_n) \in \mathbb{Z}_{2PQ}^n$, define $\mu(sk) = (X_1, \ldots, X_n) = (g^{x_1}, \ldots, g^{x_n})$.

For $C \in \mathcal{C}$ define

$$\Lambda_{sk}(C) := (C^{x_1}, \ldots, C^{x_n}) \ .$$

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

$$K = (X_1^r, \ldots, X_n^r) \ .$$

This completes the description of HPS. Under the QR assumption, the subset membership problem is hard in HPS. (The statistical difference between the uniform distribution over $\mathbb{QR}_N$ and the proposed way of sampling above, is at most $2^{-b/2}$, causing only a small extra term between the QR advantage and the HPS membership advantage.)

Consider a pair (X_i, x_i), where x_i is from sk and X_i is from pk and note that X_i does not reveal whether $0 \leq x_i < PQ$ or $PQ \leq x_i < 2PQ$. Therefore, for $C \in \mathcal{C} \setminus \mathcal{V}$, given $pk = \mu(sk)$, each of the C^{x_i} contains exactly one bit of min entropy such that $H_\infty((C^{x_1}, \ldots, C^{x_n}) \mid pk) = n$. Therefore:

Lemma 6.1 The hash proof system is n-entropic with collision probability $\delta = 2^{-n}$.

The encryption scheme. Let $\mathsf{H} : \mathbb{J}_N^n \to \{0,1\}^k$ be a 4-wise independent hash function and let SE be a symmetric cipher with key-space $\{0,1\}^k$, i.e., we set $\ell(k) = k$. For the encryption scheme obtained by

$\mathsf{Kg}(1^k)$	$\mathsf{Enc}(pk, m)$	$\mathsf{Dec}(sk, C)$
$(N, P, Q, g) \leftarrow_R \mathsf{RSAgen}(1^k)$	$r \leftarrow_R \mathbb{Z}_{\lfloor N/4 \rfloor}$	Parse C as (c, ψ)
For $i = 1$ to $n := 4k + 1$ do	$c \leftarrow g^r$	$K \leftarrow \mathsf{H}(c^{x_1}, \ldots, c^{x_n})$
$x_i \leftarrow_R \mathbb{Z}_{2PQ}$; $X_i \leftarrow g^{x_i}$	$K \leftarrow \mathsf{H}(X_1^r, \ldots, X_n^r)$	Return
Pick $\mathsf{H} \leftarrow_R \mathcal{H}$	$\psi \leftarrow \mathsf{E}_K(m)$	$\{m, \perp\} \leftarrow \mathsf{D}_K(\psi)$
$pk \leftarrow (N, g, (X_i), \mathsf{H})$; $sk \leftarrow ((x_i))$	Return $C = (c, \psi)$	
Return (sk, pk)		

Figure 4: Hybrid encryption scheme $\mathsf{HE}_3 = (\mathsf{Kg}, \mathsf{Enc}, \mathsf{Dec})$ obtained by applying our randomness extraction framework to the HPS from Section 6.

applying Corollary 4.4 (which is depicted in Figure 4) we choose the parameter $n = n(k) = 4k + 1$ such that $k - (n-1)/2 = -k$ so we can bound ϵ_2 by $2^{-k} + 2^{-n}$ using Theorem 4.3.

Theorem 6.2 Assume the QR assumption holds, let $\mathcal{H}$ be a family of 4-wise independent hash functions from $\mathbb{J}_N^{n(k)}$ to $\{0,1\}^k$ with $n(k) \geq 4k+1$, and let SE be a symmetric encryption that is secure in the sense of AE-OT. Then the encryption scheme from Figure 4 is IND-CCA2 secure. In particular,

$$\mathsf{Adv}^{\mathrm{cca2}}_{\mathsf{PKE},t,Q}(k) \leq 2^{-b/2} + \mathsf{Adv}^{\mathrm{qr}}_{\mathcal{GS},t}(k) + 2Q \cdot \mathsf{Adv}^{\text{int-ot}}_{\mathsf{SE},t}(k) + \mathsf{Adv}^{\text{ind-ot}}_{\mathsf{SE},t}(k) + Q2^{-k+1} \ .$$

The scheme has very compact ciphertexts but encryption/decryption are quite expensive since they require $n = 4k + 1$ exponentiations in $\mathbb{Z}_N^*$. (Note that decryption can be sped up considerably compared to encryption by using CRT and multi-exponentiation techniques.)

Acknowledgements

We thank Ronald Cramer for interesting discussions. We are furthermore grateful to Victor Shoup for pointing out the scheme from Section 5.3. We thank Kenny Paterson, Steven Galbraith and James Birkett for useful feedback, prompting the comparison in Section 5.4.

References

[1] Seung Geol Choi, Javier Herranz, Dennis Hofheinz, Jung Yeon Hwang, Eike Kiltz, Dong Hoon Lee, and Moti Yung. The Kurosawa-Desmedt key encapsulation is not chosen-ciphertext secure. *Information Processing Letters*, pages ???–???, 2009. (Cited on page 8.)

[2] 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 1, 2.)

[3] 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 1, 2, 3, 7, 10.)

[4] 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, 3, 9, 11.)

[5] 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 2, 11.)

[6] Ivan Damgård, Oded Goldreich, Tatsuaki Okamoto, and Avi Wigderson. Honest verifier vs dishonest verifier in public cain zero-knowledge proofs. In Don Coppersmith, editor, *CRYPTO'95*, volume 963 of *LNCS*, pages 325–338. Springer-Verlag, Berlin, Germany, August 1995. (Cited on page 5.)

[7] Yvo Desmedt, Helger Lipmaa, and Duong Hieu Phan. Hybrid Damgård is CCA1-secure under the DDH assumption. In *CANS 2008*, volume 5339 of *LNCS*, pages 18–30. Springer-Verlag, 2008. (Cited on page 3.)

[8] Yvo Desmedt and Duong Hieu Phan. A CCA secure hybrid Damgårds ElGamal encryption. In *ProvSec 2008*, volume 5324 of *LNCS*, pages 68–82. Springer-Verlag, 2008. (Cited on page 3.)

[9] Danny Dolev, Cynthia Dwork, and Moni Naor. Nonmalleable cryptography. *SIAM Journal on Computing*, 30(2):391–437, 2000. (Cited on page 1, 3.)

[10] 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 2.)

[11] 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 7, 12.)

[12] 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.)

[13] 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.)

[14] 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, 4, 7, 8, 12.)

[15] Dennis Hofheinz and Eike Kiltz. Practical chosen ciphertext secure encryption from factoring. In *EUROCRYPT 2009*, volume ???? of *LNCS*, pages ??? – ???, 2009. (Cited on page 2.)

[16] Eike Kiltz, Krzysztof Pietrzak, Martijn Stam, and Moti Yung. A new randomness extraction paradigm for hybrid encryption. Cryptology ePrint Archive, Report 2008/304, 2008. `http://eprint.iacr.org/`. (Cited on page 5.)

[17] 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 1, 2, 4, 7, 12, 13.)

[18] 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.)

[19] 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.)

[20] 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.)

[21] Pascal Paillier. Public-key cryptosystems based on composite degree residuosity classes. In Jacques Stern, editor, *EUROCRYPT'99*, volume 1592 of *LNCS*, pages 223–238. Springer-Verlag, Berlin, Germany, May 1999. (Cited on page 2.)

[22] 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.)

[23] Hovav Shacham. A cramer-shoup encryption scheme from the linear assumption and from progressively weaker linear variants. Cryptology ePrint Archive, Report 2007/074, 2007. `http://eprint.iacr.org/`. (Cited on page 2, 7.)

[24] Victor Shoup. Using hash functions as a hedge against chosen ciphertext attack. In Bart Preneel, editor, *EUROCRYPT 2000*, volume 1807 of *LNCS*, pages 275–288. Springer-Verlag, Berlin, Germany, May 2000. (Cited on page 1, 2.)

[25] 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 11.)

[26] 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.)