Public-Key Encryption Schemes with Bounded CCA Security and Optimal Ciphertext Length Based on the CDH and HDH Assumptions

Mayana Pereira[1], Rafael Dowsley[1], Goichiro Hanaoka[2], and Anderson C. A. Nascimento[1]

[1] Department of Electrical Engeneering, University of Brasília
Campus Darcy Ribeiro, 70910-900, Brasília, DF, Brazil
email: mayana@redes.unb.br,rafaeldowsley@redes.unb.br, andclay@ene.unb.br
[2] National Institute of Advanced Industrial Science and Technology (AIST)
1-18-13, Sotokanda, Chyioda-ku, 101-0021, Tokyo, Japan
e-mail: hanaoka-goichiro@aist.go.jp

Abstract. In [5] Cramer et al. proposed a public-key encryption scheme secure against adversaries with a bounded number of decryption queries based on the decisional Diffie-Hellman problem. In this paper, we show that the same result can be obtained based on weaker computational assumptions, namely: the computational Diffie-Hellman and the hashed Diffie-Hellman assumptions.

Keywords: Public-key encryption, bounded chosen ciphertext security, computational Diffie-Hellman assumption, hashed Diffie-Hellman assumption.

1 Introduction

The highest level of security for public-key cryptosystems is indistinguishability against adaptive chosen ciphertext attack (IND-CCA2), proposed by Rackoff and Simon [28] in 1991. The development of cryptosystems with such feature can be viewed as a complex task. Several public-key encryption (PKE) schemes have been proposed with either practical or theoretical purposes. It is possible to obtain IND-CCA2 secure cryptosystems based on many assumptions such as: decisional Diffie-Hellman [7, 8, 26], computational Diffie-Hellman [6, 20], factoring [22], McEliece [13, 12], quadratic residuosity [8] and learning with errors [26, 25].

Currently there are few general paradigms for the elaboration of IND-CCA2 PKE schemes. The first paradigm was proposed by Dwork, Dolev and Naor [11], and is an enhancement of an construction proposed by Naor and Yung [24] (which only achieved non-adaptive IND-CCA security). This scheme is based on non-interactive zero-knowledge techniques. Later Sahai [30] and Lindell [23] made other improvements following the same approach of [11].

Cramer and Shoup [7] proposed the first practical IND-CCA2 scheme without the use of random oracles. They also introduced hash-proof systems, which is an important element used in their construction.

Another remarkable paradigm requires the existence of identity-based encryption (IBE) schemes [3], and was first introduced by Canetti, Halevi and Katz [2].

Recently, a new paradigm was introduced: bounded CCA2 security [5], where the adversary can only make a bounded number of queries to the decryption oracle. In [5] it was proved that there exists a mapping converting chosen plaintext attack (CPA) secure PKE into another one secure under bounded CCA attacks. This weaker version of IND-CCA2 is technically termed IND-q-CCA2, where the polynomial q denotes the limit of the adversary's queries to the decryption oracle and is fixed in advance. Moreover, in [5], the authors proved that in this new setting it is possible to obtain a PKE based on the decisional Diffie-Hellman problem with optimal ciphertext length (just one group element of ciphertext overhead).

1.1 Our Contribution

We improve upon the results presented [5]. Namely, we show that it is possible to obtain an IND-q-CCA2 PKE scheme with optimal ciphertext length (one group element) based on the computational Diffie-Hellman (CDH) assumption. Additionally, we also show a more efficient scheme based on the hashed Diffie-Hellman (HDH) assumption. The ideas behind the proofs are similar to the ones presented in [5], although, in the proof of security of our HDH based scheme, to map the key to the HDH challenge, we make use of a strategy that is not obvious. Furthermore, to the best of our knowledge, no such claims appeared before in the literature.

We also note that recently, Haralambiev et al. [20] proposed an improvement of [19], and obtained a CCA secure PKE based on the CDH assumption without any kind of assumption on the number of queries an adversary performs to the decryption oracle. However, their scheme presents a larger ciphertext length when compared to ours.

An abstract of this work appeared in the Information Security Conference (ISC) 2010 [27].

2 Preliminaries

In this section we present some definitions which were used in the construction of our scheme. We refer the reader to [7], [5], [31], [29], [21], [18] and [4] for more details.

2.1 Notation

If $\mathcal{X}$ is a set then $x \xleftarrow{\$} \mathcal{X}$ denotes the act of choosing an element of $\mathcal{X}$ according to the uniform distribution. We write $w \xleftarrow{\$} \mathcal{A}^{\mathcal{O}}(x, y, ...)$ to indicate that an

(probabilistic) algorithm $\mathcal{A}$ with inputs $x, y, \ldots$ and black-box access to an oracle $\mathcal{O}$ outputs w. We denote by $\Pr[E]$ the probability that the event E occurs. We use λ for the security parameter.

2.2 public-key Encryption

A public-key encryption (PKE) scheme is defined as follows:

Definition 1. *A public-key encryption scheme is a triplet of algorithms* (Gen, Enc, Dec) *such that:*

- Gen is a probabilistic polynomial-time (PPT) key generation algorithm which takes as input a security parameter 1^λ and outputs a public-key pk and a secret key sk. The public-key specifies the message space $\mathcal{M}$ and the ciphertext space $\mathcal{C}$.

- Enc is a PPT encryption algorithm which receives as input a public-key pk and a message $\mathsf{M} \in \mathcal{M}$, and outputs a ciphertext $\mathsf{C} \in \mathcal{C}$.

- Dec is a deterministic polynomial-time decryption algorithm which takes as input a secret key sk and a ciphertext C, and outputs either a message $\mathsf{M} \in \mathcal{M}$ or an error symbol $\perp$.

- (Soundness) For any pair (pk,sk) of keys generated by Gen and any message $\mathsf{M} \in \mathcal{M}$ it holds that Dec(sk,Enc(pk,M))=M with overwhelming probability over the randomness used by Gen and Enc.

Next, we define the notion of IND-q-CCA2 security.

Definition 2. *(IND-q-CCA2 security) For a function q:* $\mathbb{N} \to \mathbb{N}$ *and a two stage adversary* $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ *against PKE we associate the following experiment* $\mathsf{Exp}^{ind-q-cca2}_{\mathcal{A},\mathrm{PKE}}(\lambda)$*:*

$(\mathsf{pk},\mathsf{sk}) \xleftarrow{\$} \mathsf{Gen}(1^\lambda)$
$(\mathsf{M}_0, \mathsf{M}_1, state) \xleftarrow{\$} \mathcal{A}_1^{\mathsf{Dec}(\mathsf{sk},.)}(\mathsf{pk})$ s.t. $|\mathsf{M}_0| = |\mathsf{M}_1|$
$\beta \xleftarrow{\$} \{0,1\}$
$\mathsf{C}^* \xleftarrow{\$} \mathsf{Enc}(\mathsf{pk},\mathsf{M}_\beta)$
$\beta' \xleftarrow{\$} \mathcal{A}_2^{\mathsf{Dec}(\mathsf{sk},.)}(\mathsf{C}^*, state)$
If $\beta = \beta'$ return 1 else return 0

The adversary $\mathcal{A}$ is allowed to ask at most $q(\lambda)$ queries to the decryption oracle Dec. None of the queries of $\mathcal{A}_2$ may contain C^*. We define the advantage of $\mathcal{A}$ in the experiment as

$$\mathsf{Adv}^{ind-q-cca2}_{\mathcal{A},\mathrm{PKE}}(\lambda) = \left| \Pr\left[\mathsf{Exp}^{ind-q-cca2}_{\mathcal{A},\mathrm{PKE}}(\lambda) = 1 \right] - \frac{1}{2} \right|.$$

We say that PKE is *indistinguishable against q-bounded adaptive chosen-ciphertext attack* (IND-q-CCA2) if for all PPT adversaries $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ that makes a polynomial number of oracle queries the advantage of $\mathcal{A}$ in the experiment is a negligible function of λ.

2.3 Number Theoretic Assumptions

In this section we state two of the Diffie-Hellman intractability assumptions: *Computational Diffie-Hellman* and *Hashed Diffie-Hellman*.

Definition 3 (CDH assumption). *Let $\mathbb{G}$ be a group of order p (which depends on the security parameter λ) and g be a generator of $\mathbb{G}$. For all PPT adversaries $\mathcal{A}$, the CDH advantage against $\mathbb{G}$ is defined as*

$$\mathbf{Adv}^{cdh}_{\mathcal{A},\mathbb{G}}(\lambda) = \Pr\left[x, y \xleftarrow{\$} \mathbb{Z}_p \,;\, c \xleftarrow{\$} \mathcal{A}(g, g^x, g^y) \,:\, c = g^{xy} \right].$$

The CDH assumption holds if for every PPT adversary $\mathcal{A}$ the function $\mathbf{Adv}^{cdh}_{\mathcal{A},\mathbb{G}}(\cdot)$ is negligible in λ.

Definition 4 (Hashed-DH Assumption). *Let $\mathbb{G}$ be a group of order p (which depends on the security parameter λ) and g be a generator of $\mathbb{G}$. Let $H\colon\ \mathbb{G} \to \{0,1\}^n$ be a hash function. For a security parameter λ, the sets $\mathcal{D}_\lambda$ and $\mathcal{T}_\lambda$ are defined as:*

$$\mathcal{D}_\lambda := \{(g^x, g^y, H(g^{xy})) \,:\, x, y \in \mathbb{Z}_p, x \neq 0\};$$
$$\mathcal{T}_\lambda := \{(g^x, g^y, r) \,:\, x, y \in \mathbb{Z}_p, x \neq 0, r \in \{0,1\}^n, r \neq H(g^{xy})\}.$$

In this weakening of the DDH assumption, the set $\mathcal{D}_\lambda$ is the set with respect to values of Diffie-Hellman triples. *$\mathcal{T}_\lambda$ is a set with a random element. For $\rho \in \{\mathcal{D}_\lambda, \mathcal{T}_\lambda\}$, let $\mathcal{A}$ be a 0/1-valued PPT adversarial algorithm and let ζ be $\mathcal{A}$'s guess about the triple ρ. The HDH advantage of $\mathcal{A}$ against $\mathbb{G}$ and H is defined as*

$$\mathbf{Adv}^{hdh}_{\mathcal{A},\mathbb{G}}(\lambda) = \left| \Pr\left[\rho \xleftarrow{\$} \mathcal{D}_\lambda \,;\, \zeta \xleftarrow{\$} \mathcal{A}(g, \rho) \,:\, \zeta = 1 \right] - \Pr\left[\rho \xleftarrow{\$} \mathcal{T}_\lambda \,;\, \zeta \xleftarrow{\$} \mathcal{A}(g, \rho) \,:\, \zeta = 1 \right] \right|.$$

The HDH assumption holds for $\mathbb{G}$ and H if for every PPT adversary $\mathcal{A}$ the function $\mathbf{Adv}^{hdh}_{\mathcal{A},\mathbb{G}}(\cdot)$ is negligible in λ.

Throughout this paper we will abbreviate $\epsilon_{cdh} = \mathbf{Adv}^{cdh}_{\mathcal{A},\mathbb{G}}(\lambda)$ and $\epsilon_{hdh} = \mathbf{Adv}^{hdh}_{\mathcal{A},\mathbb{G}}(\lambda)$.

2.4 Goldreich-Levin Hard-Core Function

Let $\mathbb{G}$ be a group of order p and generator g, and $x, y \in \mathbb{Z}_p$. Let $h\colon\ \mathbb{G} \times \{0,1\}^u \to \{0,1\}^v$ denote the Goldreich-Levin hard-core function [16] for g^{xy} (given g^x and g^y), with randomness space $\{0,1\}^u$ and range $\{0,1\}^v$, where $u, v \in \mathbb{Z}$.

Theorem 1. *Suppose that $\mathcal{A}$ is a PPT algorithm such that $\mathcal{A}(g^x, g^y, \mathsf{r}, \mathsf{k})$ distinguishes $\mathsf{k}= h(g^{xy}, r)$ from a uniform string $s \in \{0,1\}^v$ with non-negligible advantage, for random $x, y \in \mathbb{Z}_p$ and random $r \in \{0,1\}^u$. Then there exists a PPT algorithm $\mathcal{B}$ that computes g^{xy} with non-negligible probability given g^x and g^y (for random $x, y \in \mathbb{Z}_p$).*

2.5 Target Collision Resistant Hash Functions

Definition 5 (Target Collision Resistance). *Let* TCR: $\{0,1\}^{n(\lambda)} \to \{0,1\}^\lambda$ *be a family of hash functions. The target collision resistance property is defined using the following experiment executed with a PPT adversary $\mathcal{A}$:*

$$\mathbf{Exp}^{\mathrm{TCR}}_{\mathcal{A},\mathrm{TCR}}(\lambda) : [x \xleftarrow{\$} \{0,1\}^{n(\lambda)}; x' \xleftarrow{\$} \mathcal{A}(1^\lambda, x) \ : \ x \neq x';$$

$$\text{return 1 if } \mathrm{TCR}(x') = \mathrm{TCR}(x), \text{else return 0}].$$

The family of hash functions TCR *is target collision resistant if for every PPT adversary $\mathcal{A}$ it holds that $\mathbf{Exp}^{\mathrm{TCR}}_{\mathcal{A},\mathrm{TCR}}(\cdot)$ is a negligible function of λ.*

Let $\epsilon_{\mathrm{TCR}} = \Pr\left[\mathbf{Exp}^{\mathrm{TCR}}_{\mathcal{A},\mathrm{TCR}}(\lambda) = 1\right]$.

2.6 Strong Pseudorandom Permutation

Let π: $\{0,1\}^\lambda \times \{0,1\}^v \to \{0,1\}^v$ be a family of permutations, and π_k: $\{0,1\}^v \to \{0,1\}^v$ be an instance of π, which is indexed by $k \in \{0,1\}^\lambda$. Let $\mathcal{P}$ be the set of all permutations for bit strings of size v, and $\mathcal{A}$ be a 0/1-valued PPT adversary. Consider the following experiments:

$$\mathbf{Exp}^{sprp}_{\mathcal{A},\pi}(\lambda) : [k \xleftarrow{\$} \{0,1\}^\lambda; \beta \xleftarrow{\$} \mathcal{A}^{\pi_k, \pi_k^{-1}}(1^\lambda) \text{ ; return } \beta]$$
$$\mathbf{Exp}^{ideal}_{\mathcal{A}}(\lambda) : [p \xleftarrow{\$} \mathcal{P}; \beta \xleftarrow{\$} \mathcal{A}^{p, p^{-1}}(1^\lambda) \text{ ; return } \beta]$$

where permutations $\pi_K, \pi_k^{-1}, p, p^{-1}$ are given to $\mathcal{A}$ as black-boxes.

Let

$$\mathbf{Adv}^{sprp}_{\mathcal{A},\pi}(\lambda) = \frac{1}{2}\left|\Pr\left[\mathbf{Exp}^{sprp}_{\mathcal{A},\pi}(\lambda) = 1\right] - \Pr\left[\mathbf{Exp}^{ideal}_{\mathcal{A}}(\lambda) = 1\right]\right|.$$

Definition 6 (Strong Pseudorandom Permutation - SPRP). *A polynomial-time algorithm π: $\{0,1\}^\lambda \times \{0,1\}^v \to \{0,1\}^v$ is said to be a strong pseudorandom permutation if for every PPT $\mathcal{A}$ it holds that $\mathbf{Adv}^{sprp}_{\mathcal{A},\pi}(\cdot)$ is negligible in λ.*

We abbreviate $\epsilon_{sprp} = \mathbf{Adv}^{sprp}_{\mathcal{A},\pi}(\lambda)$.

2.7 Cover Free Families

Let $\mathcal{S}$ be a set, and $\mathcal{F}$ a set of subsets of $\mathcal{S}$. Let d, s, q be positive integers, where $|\mathcal{S}| = d$ and $|\mathcal{F}| = s$. We denote the elements of $\mathcal{F}$ by F_j, for $1 \leq j \leq s$. We say $\mathcal{F}$ is a q-cover-free family, if for any q elements of $\mathcal{F}$, $F_{j_1}, \ldots, F_{j_q} \in \mathcal{F}$, and any other element of $\mathcal{F}$, $F_i \notin \{F_{j_1}, \ldots, F_{j_q}\}$, we have

$$F_i \nsubseteq \bigcup_{k=1}^{q} F_{j_k}.$$

Additionally, we say the family $\mathcal{F}$ is ℓ-uniform if $|F_j| = \ell$ for all $1 \leq j \leq s$.

There is a deterministic polynomial time algorithm that on input s, q returns $\ell, d, \mathcal{F}$ such that the set $\mathcal{F}$ (which has cardinality s) is a ℓ-uniform q-cover-free family over $\{1, \ldots, d\}$, for $\ell = \frac{d}{4q}$ and $d \leq 16q^2 \log s$. For a security parameter λ and a bound on decryption queries $q(\lambda)$, the cover-free family used in our construction has the following parameters: $s(\lambda) = 2^\lambda, d(\lambda) = 16\lambda q^2(\lambda), \ell(\lambda) = 4\lambda q(\lambda)$.

2.8 Hybrid Encryption

Our schemes make use of the hybrid encryption method [9]. Such schemes use public-key encryption techniques to encrypt a random symmetric key K, which is then used to encrypt the actual message using a symmetric encryption scheme. This mechanism is homologous to public-key encryption scheme, but instead of encrypting a message, the encryption algorithm generates a random key and encrypts it.

Key Encapsulation Mechanism A Key Encapsulation Mechanism (KEM) is defined as follows:

Definition 7 (Key Encapsulation Mechanism). *A key encapsulation mechanism is a triplet of algorithms* (KGen, KEnc, KDec) *such that:*

- *KGen is a PPT key generation algorithm which takes as input a security parameter 1^λ and outputs a public-key pk and a secret key sk. The public-key specifies the symmetric-key space $\mathcal{K}$ and the ciphertext space $\mathcal{C}$.*

- *KEnc is a PPT encryption algorithm which receives as input a public-key pk, and outputs (C, K), where $\mathsf{K} \xleftarrow{\$} \mathcal{K}$ is a symmetric key, and $\mathsf{C} \in \mathcal{C}$ is a encapsulated symmetric key (i.e., the ciphertext).*

- *KDec is a deterministic polynomial-time decryption algorithm which takes as input a secret-key sk and a ciphertext C, and outputs a symmetric key $\mathsf{K} \in \mathcal{K}$ or an error symbol $\perp$.*

– *(Soundness) For any pair of public and secret keys generated by* KGen *and any pair* (C, K) *generated by* KEnc *it holds that* $\mathsf{KDec(sk,C)}=\mathsf{K}$ *with overwhelming probability over the randomness used by* KGen *and* KEnc.

Definition 8 (Key Encapsulation Mechanism CCA Security). *To a two stage adversary* $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ *against KEM we associate the following experiment* $\mathbf{Exp}^{kem}_{\mathcal{A},\mathrm{PKE}}(\lambda)$*:* $(\mathsf{pk}, \mathsf{sk}) \xleftarrow{\$} \mathsf{KGen}(1^\lambda)$
$state \xleftarrow{\$} \mathcal{A}_1^{\mathsf{KDec}(\mathsf{sk},\cdot)}(\mathsf{pk})$
$(\mathsf{C}^*, \mathsf{K}^*) \xleftarrow{\$} \mathsf{KEnc}(\mathsf{pk})$
$\beta \xleftarrow{\$} \{0,1\}$
If $\beta = 0$, $\mathsf{K}^\diamond \leftarrow \mathsf{K}^*$*; else* $\mathsf{K}^\diamond \xleftarrow{\$} \mathcal{K}$
$\beta' \xleftarrow{\$} \mathcal{A}_2^{\mathsf{KDec}(\mathsf{sk},\cdot)}(\mathsf{C}^*, \mathsf{K}^\diamond, state)$
If $\beta' = \beta$ *return 1, else return 0.*

The adversary $\mathcal{A}_2$ *is not allowed to query* $\mathsf{KDec}(\mathsf{sk},\cdot)$ *with* $\mathsf{K}^\diamond$*. The advantage of* $\mathcal{A}$ *in the experiment is*

$$\mathbf{Adv}^{kem}_{\mathcal{A},\mathrm{PKE}}(\lambda) = \left| \Pr\left[\mathbf{Exp}^{kem}_{\mathcal{A},\mathrm{PKE}}(\lambda) = 1 \right] - \frac{1}{2} \right|.$$

A KEM is indistinguishable against adaptive chosen-ciphertext attack *if for all PPT adversaries* $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ *the advantage of* $\mathcal{A}$ *in the experiment* $\mathbf{Adv}^{kem}_{\mathcal{A},\mathrm{PKE}}(\cdot)$ *is a negligible function of* λ*. Throughout this paper, we will denote* $\mathbf{Adv}^{kem}_{\mathcal{A},\mathrm{PKE}}(\lambda)$ *as* ϵ_{kem}.

3 IND-q-CCA2 Encryption From CDH

Our first construction yields a IND-q-CCA PKE scheme based on CDH assumption with optimal ciphertext length. The symmetric-key encryption scheme is constructed based on strong pseudorandom permutations, as in [18], in order to obtain the redundancy-free property and security against chosen-ciphertext attacks. Furthermore, we use the randomness established in the encryption phase and a target collision resistant hash function in order to define the index t of the element of the q-cover-free family $\mathcal{F}$ that will be used in the encryption. We use a hardcore function to construct the symmetric key.

It can be assured, due to the property of cover-free families and the unduplicatable set selection, that at least one element of the decryption key set will remain secret, since it will not be required to respond any decryption queries (of course considering the limit of q queries to the decryption oracle).

Construction. We assume the existence of a cyclic group $\mathbb{G}$ of prime-order p where the CDH assumption is believed to hold, i.e., given (g, g^x, g^y) there is no efficient way to compute g^{xy}, for a generator $g \in \mathbb{G}$, and random $x, y \in \mathbb{Z}_p$. Let TCR: $\mathbb{G} \to \{0,1\}^\lambda$ be a target collision resistant hash function, h: $\mathbb{G} \times \{0,1\}^u \to \{0,1\}^k$ be a hard-core function family, and π: $\{0,1\}^k \times \{0,1\}^v \to \{0,1\}^v$ be a

permutation family where the index space is $\{0,1\}^k$. Our scheme from CDH assumption consists of the following algorithms:

$\mathsf{Gen}(1^\lambda)$: Define $s(\lambda) = 2^\lambda$, $d(\lambda) = 16\lambda q^2(\lambda)$, $\ell(\lambda) = 4\lambda q(\lambda)$. For $i = 1, \ldots, d(\lambda)$, compute $X_i = g^{x_i}$ for $x_i \xleftarrow{\$} \mathbb{Z}_p$. Choose $a \xleftarrow{\$} \{0,1\}^u$. Output the public-key $\mathsf{pk} = (X_1, \ldots, X_{d(\lambda)}, a)$ and the secret-key $\mathsf{sk} = (x_1, \ldots, x_{d(\lambda)})$.

$\mathsf{Enc}(\mathsf{pk}, \mathsf{M})$: Compute $r = g^b$ for $b \xleftarrow{\$} \mathbb{Z}_p$. Let $j = \mathrm{TCR}(r)$ and let $F_j = \{j_1, \ldots, j_{\ell(\lambda)}\}$ be the j-th element of $\mathcal{F}$. Set $\tilde{\mathsf{C}} = r$ and compute $\mathsf{K} = (\mathrm{h}(X^b_{j_1}, a) \oplus \ldots \oplus \mathrm{h}(X^b_{j_{\ell(\lambda)}}, a))$. To encrypt the message M, run the symmetric-key encryption to obtain the ciphertext $\psi \leftarrow \pi_{\mathsf{K}}(\mathsf{M})$. Output $\mathsf{C} = (\tilde{\mathsf{C}}, \psi)$.

$\mathsf{Dec}(\mathsf{sk}, \mathsf{C})$: Compute $j = \mathrm{TCR}(\tilde{\mathsf{C}})$ to obtain the subset F_j, and compute the session's symmetric key $\mathsf{K} = (\mathrm{h}(\tilde{\mathsf{C}}^{x_{j_1}}, a) \oplus \ldots \oplus \mathrm{h}(\tilde{\mathsf{C}}^{x_{j_{\ell(\lambda)}}}, a))$. Decrypt $\mathsf{M} \leftarrow \pi^{-1}_{\mathsf{K}}(\psi)$.

Theorem 1 *Assuming that the CDH assumption holds,* TCR *is a target collision resistant hash function, h is a hardcore function, and π is strongly pseudorandom, the above scheme is IND-q-CCA2.*

Proof. We follow the same approach of [5] to prove the above lemma via a game-based proof. We prove that the KEM is IND-q-CCA2 secure and then use the KEM/DEM composition theorem from [9].

Let **Game 0** be the KEM-IND-q-CCA game with adversary $\mathcal{A}$ where the challenge ciphertext is $\tilde{\mathsf{C}}^* = r^* = g^y$ (from the CDH tuple). Let X_0 denote the event that $\mathcal{A}$'s final guess is correct (i.e. X_0 denotes that $\beta = \beta'$). For later games, let X_i $(i > 0)$ be defined analogously. We have:

$$\frac{1}{2}\mathbf{Adv}^{\text{kem-ind-}q\text{-cca2}}_{\mathcal{A},\mathrm{PKE}}(\lambda) = \left|\Pr[\,X_0\,] - \frac{1}{2}\right|$$

Game 1 is identical to **Game 0**, except that the challenge $\tilde{\mathsf{C}}^*$ is initially chosen, and all decapsulation queries with $\mathrm{TCR}(\tilde{\mathsf{C}}) = \mathrm{TCR}(\tilde{\mathsf{C}}^*)$ are rejected.

By reduction on the security of the TCR, one can show that

$$|\Pr[\,X_1\,] - \Pr[\,X_0\,]| \leq \epsilon_{\mathrm{TCR}} + \frac{q}{p}$$

for a suitable adversary $\mathcal{V}$, where ϵ_{TCR} is the probability that $\mathcal{V}$ finds $\mathrm{TCR}(\tilde{\mathsf{C}}) = \mathrm{TCR}(\tilde{\mathsf{C}}^*)$ for $\tilde{\mathsf{C}} \neq \tilde{\mathsf{C}}^*$ and $\frac{q}{p}$ is an upper bound on the probability that $\mathcal{A}_1$ ask the decryption oracle to decrypt $\tilde{\mathsf{C}}^*$.

Game 2 is equivalent to **Game 1**. In this game, we will define

$$Q := \bigcup_{\tilde{\mathsf{C}}^i \neq \tilde{\mathsf{C}}^*} F_{j^i}$$

where $\tilde{\mathsf{C}}^i$ is the i-th decapsulation request of $\mathcal{A}$, $j^i = \mathrm{TCR}(\tilde{\mathsf{C}}^i)$ and F_{j^i} are the sets of PKE key pairs associated with the respective i-th query.

Define $t := min(F_{j^*} \setminus Q)$, for $j^* = \mathrm{TCR}(\tilde{\mathsf{C}}^*)$ (it is always possible since $F_{j^*} \nsubseteq Q$). Additionally choose uniformly and independently $\alpha \in F_{j^*}$. Call ABORT the event that $\alpha \neq t$. Note that

$$\Pr[\,\mathrm{ABORT}|X_2\,] = \frac{\ell - 1}{\ell} = \Pr[\,\mathrm{ABORT}\,]$$

so the events X_2 and ABORT are independent, and in particular, $\Pr[\,X_2\,] = \Pr[\,X_2|\neg\mathrm{ABORT}\,]$. Since we did not actually change anything, $\Pr[\,X_2\,] = \Pr[\,X_1\,]$.

In **Game 3**, we substitute $\mathcal{A}'$s output β' with a random bit whenever ABORT occurs. Obviously, $\Pr[\,X_3|\neg\mathrm{ABORT}\,] = \Pr[\,X_2|\neg\mathrm{ABORT}\,]$ and $\Pr[\,X_3|\mathrm{ABORT}\,] = \frac{1}{2}$.

Since $\Pr[\,\mathrm{ABORT}\,] = \frac{\ell-1}{\ell}$ in Game 3 as well, we can establish that

$$\Pr[\,X_3\,] - \frac{1}{2} = \frac{\Pr[\,X_2\,] - \frac{1}{2}}{\ell}$$

In **Game 4**, we immediately stop the experiment and set ABORT to true (hence immediately taking a random bit for $\mathcal{A}'$s output) as soon as $\mathcal{A}$ asks for a decapsulation where $\tilde{\mathsf{C}} \neq \tilde{\mathsf{C}}^*$ and $\alpha \in F_j$ where $j = \mathrm{TCR}(\tilde{\mathsf{C}})$. Note that already in Game 3, such a query would have implied $t \neq \alpha$ and hence ABORT. Consequently, $\Pr[\,X_4\,] = \Pr[\,X_3\,]$. Note that in this experiment x_α is not necessary to answer the decryption queries.

In **Game 5**, we use g^x (from the CDH tuple) instead of g^{x_α}. Note that the probability distribution of the keys does not change. To answer the challenge query, we receive from the CDH oracle a value z that is equal to either the hardcore function of g^{xy} or a random value in $\{0,1\}^k$. Then we form K^* as

$$\mathrm{h}(X^y_{j_1}, a) \oplus \ldots \oplus z \oplus \ldots \oplus \mathrm{h}(X^y_{j_\ell}, a)$$

Note that $\Pr[\,X_5\,] = \Pr[\,X_4\,]$. Let ϵ' denote the advantage of the adversary in this game. But according to Theorem 1, ϵ' is a negligible function if the CDH assumption holds.

Collecting the probabilities we have that:

$$\mathbf{Adv}^{\text{kem-ind-}q\text{-cca2}}_{\mathrm{PKE},\mathcal{A}}(\lambda) \leq 2 \cdot \epsilon_{\mathrm{tcr}} + \ell \cdot \epsilon' + \frac{2q}{p}.$$

4 IND-q-CCA2 Encryption From HDH

This construction is a variation of the one presented above. It yields in a IND-q-CCA PKE scheme based on HDH assumption also with optimal ciphertext length. In this construction, we equally make use of *key encapsulation* method to construct a key to be used in a symmetric encryption. In this construction, instead of defining the encapsulated key as the product of hardcore functions (similarly to the previous scheme), we define the encapsulated key as the hash of the product of all keys. This makes the scheme more efficient.

CONSTRUCTION. We assume the existence of a cyclic group $\mathbb{G}$ of prime-order p and a hash function $H\colon\ \mathbb{G} \to \{0,1\}^k$ for which the HDH assumption holds. Let TCR: $\mathbb{G} \to \{0,1\}^\lambda$ be a target collision resistant hash function and $\pi\colon\ \{0,1\}^k \times \{0,1\}^v \to \{0,1\}^v$ be a permutation family where the index space is $\{0,1\}^k$ Our scheme from the HDH assumption consists of the following algorithms:

$\mathsf{Gen}(1^\lambda)$: Define $s(\lambda) = 2^\lambda$, $d(\lambda) = 16\lambda q^2(\lambda)$, $\ell(\lambda) = 4\lambda q(\lambda)$. For $i = 1, \ldots, d(\lambda)$, compute $X_i = g^{x_i}$ for $x_i \xleftarrow{\$} \mathbb{Z}_p$. Output the public-key $\mathsf{pk} = (X_1, \ldots, X_{d(\lambda)})$ and the secret-key $\mathsf{sk} = (x_1, \ldots, x_{d(\lambda)})$.

$\mathsf{Enc}(\mathsf{pk}, \mathsf{M})$: Compute $r = g^b$ for $b \xleftarrow{\$} \mathbb{Z}_p$. Let $j = \mathrm{TCR}(r)$ and let $F_j = \{j_1, \ldots, j_{\ell(\lambda)}\}$ be the j-th element of $\mathcal{F}$. Set $\tilde{\mathsf{C}} = r$ and compute $\mathsf{K} = H((\prod_{j_i \in F_j} X_{j_i})^b)$. To encrypt the message M, run the symmetric-key encryption to obtain the ciphertext $\psi \leftarrow \pi_{\mathsf{K}}(\mathsf{M})$. Output $\mathsf{C} = (\tilde{\mathsf{C}}, \psi)$.

$\mathsf{Dec}(\mathsf{sk}, \mathsf{C})$: Compute $j = \mathrm{TCR}(\tilde{\mathsf{C}})$ to obtain the subset F_j, and compute the session's symmetric key $\mathsf{K} = H(\tilde{\mathsf{C}}^{\sum_{j_i \in F_j} x_{j_i}})$. Decrypt $\mathsf{M} \leftarrow \pi_{\mathsf{K}}^{-1}(\psi)$.

Theorem 2 *Assuming that the HDH assumption holds,* TCR *is a target collision resistant hash function, and π is a strongly pseudorandom permutation, the scheme above is IND-q-CCA2.*

Proof. The proof is similar to the previous one.

Let **Game 0** be the KEM-IND-q-CCA game with adversary $\mathcal{A}$ where the challenge $\tilde{\mathsf{C}}^* = r^* = g^y$ (g^y from the HDH tuple). Let X_0 denote the event that $\mathcal{A}$'s final guess is correct (i.e. X_0 denotes that $\beta = \beta'$). For later games, let X_i ($i > 0$) be defined analogously. We have:

$$\frac{1}{2}\mathbf{Adv}^{\text{kem-ind-}q\text{-cca2}}_{\mathcal{A},\mathrm{PKE}}(\lambda) = \left|\Pr[\,X_0\,] - \frac{1}{2}\right|$$

Game 1 is identical to **Game 0**, except that $\tilde{\mathsf{C}}^*$ is initially chosen, and all decapsulation queries with $\mathrm{TCR}(\tilde{\mathsf{C}}) = \mathrm{TCR}(\tilde{\mathsf{C}}^*)$ are rejected.

By reduction on the security of the TCR, one can show that

$$|\Pr[\,X_1\,] - \Pr[\,X_0\,]| \leq \epsilon_{\mathrm{TCR}} + \frac{q}{p}$$

for a suitable adversary $\mathcal{V}$, where ϵ_{TCR} is the probability that $\mathcal{V}$ finds $\mathrm{TCR}(\tilde{\mathsf{C}}) = \mathrm{TCR}(\tilde{\mathsf{C}}^*)$ for $\tilde{\mathsf{C}} \neq \tilde{\mathsf{C}}^*$ and $\frac{q}{p}$ is an upper bound on the probability that $\mathcal{A}_1$ ask the decryption oracle to decrypt $\tilde{\mathsf{C}}^*$.

Game 2 is equivalent to **Game 1**. In this game, we will define

$$Q := \bigcup_{\tilde{\mathsf{C}}^i \neq \tilde{\mathsf{C}}^*} F_{j^i}$$

where $\tilde{\mathsf{C}}^i$ is the i-th decapsulation request of $\mathcal{A}$, $j^i = \mathrm{TCR}(\tilde{\mathsf{C}}^i)$ and F_{j^i} are the sets of PKE key pairs associated with the respective i-th query.

Define $t := min(F_{j^*} \setminus Q)$, for $j^* = \mathrm{TCR}(\tilde{\mathsf{C}}^*)$ (it is always possible since $F_{j^*} \nsubseteq Q$). Additionally choose uniformly and independently $\alpha \in F_{j^*}$. Call ABORT the event that $\alpha \neq t$. Note that

$$\Pr[\,\mathrm{ABORT}|X_2\,] = \frac{\ell - 1}{\ell} = \Pr[\,\mathrm{ABORT}\,]$$

so the events X_2 and ABORT are independent, and in particular, $\Pr[\,X_2\,] = \Pr[\,X_2|\neg\mathrm{ABORT}\,]$. Since we did not actually change anything, $\Pr[\,X_2\,] = \Pr[\,X_1\,]$.

In **Game 3**, we substitute $\mathcal{A}'$s output β' with a random bit whenever ABORT occurs. Obviously, $\Pr[\,X_3|\neg\mathrm{ABORT}\,] = \Pr[\,X_2|\neg\mathrm{ABORT}\,]$ and $\Pr[\,X_3|\mathrm{ABORT}\,] = \frac{1}{2}$.

Since $\Pr[\,\mathrm{ABORT}\,] = \frac{\ell-1}{\ell}$ in Game 3 as well, we can establish that

$$\Pr[\,X_3\,] - \frac{1}{2} = \frac{\Pr[\,X_2\,] - \frac{1}{2}}{\ell}$$

In **Game 4**, we immediately stop the experiment and set ABORT to true (hence immediately taking a random bit for $\mathcal{A}'$s output) as soon as $\mathcal{A}$ asks for a decapsulation where $\tilde{\mathsf{C}} \neq \tilde{\mathsf{C}}^*$ and $\alpha \in F_j$ where $j = \mathrm{TCR}(\tilde{\mathsf{C}})$. Note that already in Game 3, such a query would have implied $t \neq \alpha$ and hence ABORT. Consequently, $\Pr[\,X_4\,] = \Pr[\,X_3\,]$. Note that in this experiment x_α is not necessary to answer the decryption queries.

In **Game 5**, we modify X_α to

$$g^x * (\prod_{i \in F_{t^*} \setminus \alpha} g^{x_i})^{-1}$$

where g^x is from the HDH tuple. Note that the probability distribution of the keys does not change, so $\Pr[\,X_5\,] = \Pr[\,X_4\,]$. In this game if $\beta = 0$, $\mathsf{K}^\diamond = H(g^{xy})$ and if $\beta = 1$, $\mathsf{K}^\diamond$ is random.

Collecting the probabilities we have that:

$$\mathbf{Adv}^{\text{kem-ind-}q\text{-cca2}}_{\mathrm{PKE},\mathcal{A}}(\lambda) \leq 2 \cdot \epsilon_{\mathrm{tcr}} + \ell \cdot \epsilon_{hdh} + \frac{2q}{p}.$$

5 Expanding the Encapsulated Key in the CDH Scheme

The IND-q-CCA KEM scheme based on the CDH assumption proposed in section 3 results in a small symmetric key. In this section we show how to expand the key without increasing the size of the ciphertext overhead. A symmetric key of size kn is obtained by generating n groups of secret/public-keys.

Construction. As in section 3, we assume the existence of a cyclic group $\mathbb{G}$ of prime-order p where the CDH assumption is believed to hold. Let TCR: $\mathbb{G} \to \{0,1\}^\lambda$ be a target collision resistant hash function, h: $\mathbb{G} \times \{0,1\}^u \to \{0,1\}^k$ be a

hard-core function family, and π: $\{0,1\}^{kn} \times \{0,1\}^v \to \{0,1\}^v$ be a permutation family where the index space is $\{0,1\}^{kn}$. Our modified scheme from the CDH assumption works as follows:

$\mathsf{Gen}(1^\lambda)$: Define $s(\lambda) = 2^\lambda$, $d(\lambda) = 16\lambda q^2(\lambda)$, $\ell(\lambda) = 4\lambda q(\lambda)$. For $i = 1, \ldots, d(\lambda)$ and $m = 1, \ldots, n$, compute $X_{m,i} = g^{x_{m,i}}$ for $x_{m,i} \xleftarrow{\$} \mathbb{Z}_p$. Choose $a \xleftarrow{\$} \{0,1\}^u$. Let $\mathsf{pk}_m = (X_{m,1}, \ldots, X_{m,d(\lambda)})$ and $\mathsf{sk}_m = (x_{m,1}, \ldots, x_{m,d(\lambda)})$. The public-key is $\mathsf{pk} = \{\mathsf{pk}_1, \ldots, \mathsf{pk}_n, a\}$, and the secret key is $\mathsf{sk} = \{\mathsf{sk}_1, \ldots, \mathsf{sk}_n\}$.

$\mathsf{Enc}(\mathsf{pk}, \mathsf{M})$: Compute $r = g^b$ for $b \xleftarrow{\$} \mathbb{Z}_p$. Let $j = \mathrm{TCR}(r)$ and let $F_j = \{j_1, \ldots, j_{\ell(\lambda)}\}$ be the j-th element of $\mathcal{F}$. Set $\tilde{\mathsf{C}} = r$ and compute $\mathsf{K}_m = (\mathrm{h}(X^b_{m,j_1}, a) \oplus \ldots \oplus \mathrm{h}(X^b_{m,j_{\ell(\lambda)}}, a))$ for $m = 1, \ldots, n$. Define $\mathsf{K} = \mathsf{K}_1 || \mathsf{K}_2 || \ldots || \mathsf{K}_n$. To encrypt the message M, run the symmetric-key encryption to obtain the ciphertext $\psi \leftarrow \pi_{\mathsf{K}}(\mathsf{M})$. Output $\mathsf{C} = (\tilde{\mathsf{C}}, \psi)$.

$\mathsf{Dec}(\mathsf{sk}, \mathsf{C})$: Compute $j = \mathrm{TCR}(\tilde{\mathsf{C}})$ to obtain the subset F_j, compute $\mathsf{K}_m = (\mathrm{h}(\tilde{\mathsf{C}}^{x_{m,j_1}}, a) \oplus \ldots \oplus \mathrm{h}(\tilde{\mathsf{C}}^{x_{m,j_{\ell(\lambda)}}}, a))$ and $\mathsf{K} = \mathsf{K}_1 || \mathsf{K}_2 || \ldots || \mathsf{K}_n$. Decrypt $\mathsf{M} \leftarrow \pi^{-1}_{\mathsf{K}}(\psi)$.

Theorem 3 *Assuming that the CDH assumption holds,* TCR *is a target collision resistant hash function, h is a hardcore function, and π is strongly pseudorandom, the above scheme is IND-q-CCA2.*

Proof. In addition to the approach used in previous sections, we use an hybrid argument to prove the security of the above scheme.

Let **Game 0** be the KEM-IND-q-CCA game with adversary $\mathcal{A}$ where the challenge ciphertext is $\tilde{\mathsf{C}}^* = r^* = g^y$ (from the CDH tuple). Let X_0 denote the event that $\mathcal{A}$'s final guess is correct (i.e. X_0 denotes that $\beta = \beta'$). For later games, let X_i $(i > 0)$ be defined analogously. We have:

$$\frac{1}{2}\mathbf{Adv}^{\text{kem-ind-}q\text{-cca2}}_{\mathcal{A},\mathrm{PKE}}(\lambda) = \left|\Pr[\, X_0 \,] - \frac{1}{2}\right|$$

Game 1 is identical to **Game 0**, except that the challenge $\tilde{\mathsf{C}}^*$ is initially chosen, and all decapsulation queries with $\mathrm{TCR}(\tilde{\mathsf{C}}) = \mathrm{TCR}(\tilde{\mathsf{C}}^*)$ are rejected.

By reduction on the security of the TCR, one can show that

$$|\Pr[\, X_1 \,] - \Pr[\, X_0 \,]| \leq \epsilon_{\mathrm{TCR}} + \frac{q}{p}$$

for a suitable adversary $\mathcal{V}$, where ϵ_{TCR} is the probability that $\mathcal{V}$ finds $\mathrm{TCR}(\tilde{\mathsf{C}}) = \mathrm{TCR}(\tilde{\mathsf{C}}^*)$ for $\tilde{\mathsf{C}} \neq \tilde{\mathsf{C}}^*$ and $\frac{q}{p}$ is an upper bound on the probability that $\mathcal{A}_1$ ask the decryption oracle to decrypt $\tilde{\mathsf{C}}^*$.

Game 2 is equivalent to **Game 1**. In this game, we will define

$$Q := \bigcup_{\tilde{\mathsf{C}}^i \neq \tilde{\mathsf{C}}^*} F_{j^i}$$

where $\tilde{\mathsf{C}}^i$ is the i-th decapsulation request of $\mathcal{A}$, $j^i = \mathrm{TCR}(\tilde{\mathsf{C}}^i)$ and F_{j^i} are the sets of PKE key pairs associated with the respective i-th query.

Define $t := min(F_{j^*} \setminus Q)$, for $j^* = \mathrm{TCR}(\tilde{\mathsf{C}}^*)$ (it is always possible since $F_{j^*} \nsubseteq Q$). Additionally choose uniformly and independently $\alpha \in F_{j^*}$. Call ABORT the event that $\alpha \neq t$. Note that

$$\Pr[\,\mathrm{ABORT}|X_2\,] = \frac{\ell - 1}{\ell} = \Pr[\,\mathrm{ABORT}\,]$$

so the events X_2 and ABORT are independent, and in particular, $\Pr[\,X_2\,] = \Pr[\,X_2|\neg\mathrm{ABORT}\,]$. Since we did not actually change anything, $\Pr[\,X_2\,] = \Pr[\,X_1\,]$.

In **Game 3**, we substitute $\mathcal{A}'$s output β' with a random bit whenever ABORT occurs. Obviously, $\Pr[\,X_3|\neg\mathrm{ABORT}\,] = \Pr[\,X_2|\neg\mathrm{ABORT}\,]$ and $\Pr[\,X_3|\mathrm{ABORT}\,] = \frac{1}{2}$.

Since $\Pr[\,\mathrm{ABORT}\,] = \frac{\ell-1}{\ell}$ in Game 3 as well, we can establish that

$$\Pr[\,X_3\,] - \frac{1}{2} = \frac{\Pr[\,X_2\,] - \frac{1}{2}}{\ell}$$

In **Game 4**, we immediately stop the experiment and set ABORT to true (hence immediately taking a random bit for $\mathcal{A}'$s output) as soon as $\mathcal{A}$ asks for a decapsulation where $\tilde{\mathsf{C}} \neq \tilde{\mathsf{C}}^*$ and $\alpha \in F_j$ where $j = \mathrm{TCR}(\tilde{\mathsf{C}})$. Note that already in Game 3, such a query would have implied $t \neq \alpha$ and hence ABORT. Consequently, $\Pr[\,X_4\,] = \Pr[\,X_3\,]$. Note that in this experiment x_α is not necessary to answer the decryption queries.

In the following games, we demonstrate, by a standard hybrid argument, that any PPT adversary has a negligible advantage in distinguishing a real key from a random string of same size.

We start the exposition of the hybrid argument constructing the key as described in the protocol, i.e., a well formed key. On each upcoming game, we replace a component of the key with a random element of the same size, so the difference of adjacent games will be of only one key component. In the last game, we will have a completely random key.

In **Game 5**, the challenge key is formed as:

$$\mathsf{K} = \mathsf{K}_1||\mathsf{K}_2||\ldots||\mathsf{K}_n$$

Since it consists in a well formed key, $\Pr[\,X_5\,] = \Pr[\,X_4\,]$.

In **Game 6**, the challenge key will be constructed in the following way:

$$\mathsf{K} = \mathsf{K}_1||\mathsf{K}_2||\ldots||\mathsf{K}_{n-1}||rnd^1$$

where rnd^1 is a random element from $\{0,1\}^k$.

The last component K_n in **Game 5** is formed as

$$\mathsf{K}_n = \mathrm{h}(X^y_{n,j_1}, a) \oplus \ldots \oplus \mathrm{h}((g^{x_{n,\alpha}})^y, a) \oplus \ldots \oplus \mathrm{h}(X^y_{n,j_{\ell(\lambda)}}, a)$$

We can see that distinguishing K_n from a random element of $\{0,1\}^k$ implies in distinguishing $\mathrm{h}((g^{x_{k,\alpha}})^y, a)$ from a random element of $\{0,1\}^k$.

From theorem 1, an adversary that distinguishes $\mathrm{h}((g^{x_{k,\alpha}})^y, a)$ from a random element of $\{0,1\}^k$, solves the CDH problem. Therefore, if the CDH assumption holds, $\Pr[X_6] - \Pr[X_5] \leq \epsilon''$, where ϵ'' is a negligible function.

In **Game 5+i**, for $2 \leq i \leq n$, the challenge key is formed as the following:

$$\mathsf{K} = \mathsf{K}_1 || \mathsf{K}_2 || \ldots || \mathsf{K}_{n-i} || rnd^i$$

where rnd^i is a random element from $\{0,1\}^{ki}$.

From theorem 1, we have that, if the CDH assumption holds, $\Pr[X_{5+i}] - \Pr[X_{5+i-1}] \leq \epsilon''$, where ϵ'' is a negligible function.

We also have that

$$\Pr[X_{5+n}] = \frac{1}{2}$$

since in **Game 5+n** the key is completely random.

Collecting the probabilities we have that:

$$\mathbf{Adv}^{\text{kem-ind-}q\text{-cca2}}_{\text{PKE},\mathcal{A}}(\lambda) \leq 2 \cdot \epsilon_{\text{tcr}} + \ell \cdot \lambda \cdot \epsilon'' + \frac{2q}{p}.$$

References

1. Mihir Bellare and Thomas Ristenpart. Simulation without the artificial abort: Simplified proof and improved concrete security for waters' ibe scheme. *Advances in Cryptology – EUROCRYPT '09*, 2009.
2. Dan Boneh, Ran Canetti, Shai Halevi, and Jonathan Katz. Chosen-ciphertext security from identity-based encryption. *SIAM J. Comput.*, 36(5):1301–1328, 2006.
3. Dan Boneh and Matthew K. Franklin. Identity-based encryption from the weil pairing. In *CRYPTO '01: Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology*, pages 213–229, London, UK, 2001. Springer-Verlag.
4. David Cash, Eike Kiltz, and Victor Shoup. The twin diffie-hellman problem and applications. *Journal of Cryptology*, 22(4):470–504, 2009.
5. Ronald Cramer, Goichiro Hanaoka, Dennis Hofheinz, Hideki Imai, Eike Kiltz, Rafael Pass, Abhi Shelat, and Vinod Vaikuntanathan. Bounded cca2-secure encryption. *Advances in Cryptology – ASIACRYPT 2007*, 4833/2008:502–518, 2007.
6. Ronald Cramer, Dennis Hofheinz, and Eike Kiltz. A twist on the naor-yung paradigm and its application to efficient cca-secure encryption from hard search problems. In Daniele Micciancio, editor, *TCC*, volume 5978 of *Lecture Notes in Computer Science*, pages 146–164. Springer, 2010.
7. Ronald Cramer and Victor Shoup. A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. *CRYPTO '98*, 1462 of LNCS(13-25), 1998.
8. 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*, volume 2332 of *Lecture Notes in Computer Science*, pages 45–64. Springer, 2002.

9. 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.
10. Alexander W. Dent. A brief history of provably-secure public-key encryption. In *AFRICACRYPT*, pages 357–370, 2008.
11. Danny Dolev, Cynthia Dwork, and Moni Naor. Non-malleable cryptography. *In Proc. 23rd ACM Symp. on Theory of Computing, pages 542–552*, 1991.
12. Nico Döttling, Rafael Dowsley, Jörn Müller-Quade, and Anderson C. A. Nascimento. A cca2 secure variant of the mceliece cryptosystem. *IEEE Transactions on Information Theory*, 58(10):6672–6680, 2012.
13. Rafael Dowsley, Jörn Müller-Quade, and Anderson C. A. Nascimento. A cca2 secure public key encryption scheme based on the mceliece assumptions in the standard model. In Marc Fischlin, editor, *CT-RSA*, volume 5473 of *Lecture Notes in Computer Science*, pages 240–251. Springer, 2009.
14. Oded Goldreich. *Foundations of Cryptography: Basic Tools*, volume 1. Cambridge University Press, 2001.
15. Oded Goldreich. *Foundations of Cryptography: Basic Applications*, volume 2. Cambridge University Press, 2004.
16. Oded Goldreich and Leonid A. Levin. A hard-core predicate for all one-way functions. In *In Proceedings of the Twenty First Annual ACM Symposium on Theory of Computing*, pages 25–32, 1989.
17. Oded Goldreich, Noam Nisan, and Avi Wigderson. On yao's xor-lemma. *Technical Report TR95-050, Electronic Colloquium on Computational Complexity*, 1995.
18. Goichiro Hanaoka and Hideki Imai. A generic construction of cca-secure cryptosystems without nizkp for a bounded number of decryption queries. *Cryptology ePrint Archive, Report 2006/408*, 2006.
19. Goichiro Hanaoka and Kaoru Kurosawa. Efficient chosen ciphertext secure public key encryption under the computational diffie-hellman assumption. In *ASIACRYPT '08: Proceedings of the 14th International Conference on the Theory and Application of Cryptology and Information Security*, pages 308–325, Berlin, Heidelberg, 2008. Springer-Verlag.
20. Kristiyan Haralambiev, Tibor Jager, Eike Kiltz, and Victor Shoup. Simple and efficient public-key encryption from computational diffie-hellman in the standard model. *13th International Conference on Practice and Theory in Public Key Cryptography (PKC)*, 2010.
21. D. Hofheinz and E. Kiltz. Secure hybrid encryption from weakened key encapsulation. *CRYPTO 2007*, pages 553–571.
22. Dennis Hofheinz and Eike Kiltz. Practical chosen ciphertext secure encryption from factoring. In Antoine Joux, editor, *EUROCRYPT*, volume 5479 of *Lecture Notes in Computer Science*, pages 313–332. Springer, 2009.
23. Yehuda Lindell. A simpler construction of cca2-secure public-key encryption under general assumptions. *Journal of Cryptology*, 19(3)(359-377), 2006.
24. Moni Naor and M. Yung. Public-key cryptosystems provably secure against chosen ciphertext attacks. *STOC 90*, 1990.
25. Chris Peikert. Public-key cryptosystems from the worst-case shortest vector problem: extended abstract. In Michael Mitzenmacher, editor, *STOC*, pages 333–342. ACM, 2009.
26. Chris Peikert and Brent Waters. Lossy trapdoor functions and their applications. In Cynthia Dwork, editor, *STOC*, pages 187–196. ACM, 2008.

27. Mayana Pereira, Rafael Dowsley, Goichiro Hanaoka, and Anderson C. A. Nascimento. Public key encryption schemes with bounded cca security and optimal ciphertext length based on the cdh assumption. In Mike Burmester, Gene Tsudik, Spyros S. Magliveras, and Ivana Ilic, editors, *ISC*, volume 6531 of *Lecture Notes in Computer Science*, pages 299–306. Springer, 2010.
28. C. Rackoff and D. Simon. Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack. *Advances in Cryptology – Crypto '91*, 576 of Lecture Notes in Computer Science:434–444, 1991.
29. Alon Rosen and Gil Segev. Chosen-ciphertext security via correlated products. *TCC*, (419-436), 2009.
30. Amit Sahai. Non-malleable non-interactive zero knowledge and adaptive chosen-ciphertext security. *FOCS '99*, pages 543–553, 1999.
31. Victor Shoup. Sequences of games: a tool for taming complexity in security proofs. *Cryptology ePrint Archive, Report 2004/332*, 2004.