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

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 [2] a public key encryption scheme was proposed against adversaries with a bounded number of decryption queries based on the decisional Diffie-Helman Problems. In this paper, we show that the same result can be easily obtained based on weaker computational assumption, namely: the computational Diffie-Helman assumption.

Keywords Bounded chosen ciphertext secure public key encryption, computational Diffie-Hellman assumption.

1 Introduction

The highest level of security known to public key cryptosystems is indistinguishability against adaptive chosen ciphertext attack (IND-CCA2), proposed by Rackoff and Simon [11] in 1991.

Currently there are a few paradigms for the elaboration of IND-CCA2 PKE schemes. The first paradigm was proposed by Dwork, Dolev and Naor [5], and is an enhancement of an construction proposed by Naor and Yung [10] (which only achieved the non-adptive IND-CCA). This scheme is based on non-interactive zero knowledge techniques. Cramer and Shoup [3] 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.

Recently, a new paradigm was introduced for obtaining IND-CCA2 PKE schemes: bounded CCA2 security [2]. In [2] it was proved that there exists a mapping converting chosen plaintext attack (CPA) secure PKE into another one secure under adaptive chosen ciphertext attacks for a bounded number of access to the decryption oracle. This weaker version of IND-CCA2 is technically termed IND-q-CCA2, where the polynomial q denotes the number of the adversary's queries to the decryption oracle. Additionally, the polynomial q is fixed in advance, in the key-generation phase. Moreover, in [2], 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.

1.1 Our Contribution

We improve upon the results presented [2]. Namely, we show that it is possible to obtain a IND-q-CCA2 PKE scheme with optimal ciphertext length (one group element) based on the Computational Diffie-Hellman (CDH) assumption.

We also note that [1], [7] and [8] obtain CCA secure PKE based on the CDH assumption without any kind of assumption on the number of queries an adversary performs to decryption oracle. However, these schemes present larger ciphertext length when compared to ours.

2 Preliminaries

In this section we present some definitions which were used in the construction of our scheme. We refer the reader to [3], [2], [9] and [1] for more detailed explanations of these definitions.

Throughout this paper it will be used the subsequent notations. If $\mathcal{X}$ is a set then $\mathrm{x} \xleftarrow{\$} \mathcal{X}$ denotes the experiment of choosing an element of $\mathcal{X}$ according to the uniform distribution. If $\mathcal{A}$ is an algorithm, $x \leftarrow \mathcal{A}$ denotes that the output of $\mathcal{A}$ is x. We write $w \leftarrow \mathcal{A}^{\mathcal{O}}(x, y, ...)$ to indicate an algorithm $\mathcal{A}$ with inputs $x, y, \ldots$ and black-box access to an oracle $\mathcal{O}$. We denote by $\Pr[E]$ the probability that the event E occurs.

2.1 Public Key Encryption

A Public Key Encryption Scheme (PKE) 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 ($p.p.t$) key generation algorithm which takes as input a security parameter 1^k 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 *p.p.t.* 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 of public and private 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 $q(k) : \mathbb{N} \to \mathbb{N}$ and a two stage adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$, against PKE we associate the following experiment $\mathsf{Exp}^{ind-q-cca2}_{\mathcal{A},\mathrm{PKE}}(k)$:*

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

The adversary $\mathcal{A}$ is allowed to ask at most $q(k)$ queries to the decryption oracle Dec in each run of the experiment. None of the queries of $\mathcal{A}_2$ may contain C^*. We define the advantage of $\mathcal{A}$ in the experiment as $\mathsf{Adv}^{ind-q-cca2}_{\mathcal{A},\mathrm{PKE}}(k) = |\Pr[\mathsf{Exp}^{ind-q-cca2}_{\mathcal{A},\mathrm{PKE}}(k) = 1] - \frac{1}{2}|$. We say that PKE is *indistinguishable against q-bounded adaptive chosen-ciphertext attack* (IND-q-CCA2) if for all *p.p.t.* 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 k.

2.2 Number Theoretic Assumptions

In this section we state a Diffie-Hellman intractability assumption: *Computational Diffie-Helman.*

Definition 3. *(CDH assumption) Let $\mathbb{G}$ be a group of order p and generator g. For all* p.p.t. *adversaries $\mathcal{A}$, we define its CDH advantage against $\mathbb{G}$ at a security paramerer k as* $\mathbf{Adv}^{cdh}_{\mathcal{A},\mathbb{G}}(k) = \Pr[c = g^{xy} : x, y \xleftarrow{\$} \mathbb{Z}_p; c \leftarrow \mathcal{A}(1^k, g^x, g^y)]$.

We say that the CDH assumption holds for $\mathbb{G}$ if for every polynomial-time adversary $\mathcal{A}$ the function $\mathbf{Adv}^{cdh}_{\mathcal{A},\mathbb{G}}$ is negligible in k. Throughout this paper we will denote $\epsilon_{cdh} = \mathbf{Adv}^{cdh}_{\mathcal{A},\mathbb{G}}(k)$.

2.3 Goldreich-Levin Hard-Core Function

Let $\mathbb{G}$ be a group of order p and generator g, and $x, y \in \mathbb{Z}_p$. We denote by h: $\mathbb{G} \times \{0,1\}^u \to \{0,1\}^v$ the Goldreich-Levin hard-core function [6] for g^{xy} (given g^x and g^y), with randomness space $\{0,1\}^u$ and range $\{0,1\}^v$, where $u, v \in \mathbb{Z}$.

The following theorem is from [1, Theorem 9].

Theorem 1. *Suppose that $\mathcal{A}$ is a* p.p.t. *algorithm such that $\mathcal{A}(g^x, g^y, r, k)$ distinguishes $k = h(g^{xy}, r)$ 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* p.p.t. *algorithm $\mathcal{B}$ that computes g^{xy} with non-negligible probability given g^x and g^y, for random $x, y \in \mathbb{Z}_p$.*

2.4 Target Collision Resistant Hash Functions

Let $\mathbb{G}$ be a group, and k the security parameter. We denote by TCR: $\{0,1\}^{\ell} \rightarrow \{0,1\}^{n}$ the Target collision resistant hash function. Consider the following experiment, where $\mathcal{A}$ is an adversarial algorithm.
$\mathbf{Exp}^{tcr}_{\mathcal{A},\pi}(k) : [x \xleftarrow{\$} \{0,1\}^{\ell}; x' \leftarrow \mathcal{A}(k,x), x \neq x'; \text{return 1 if TCR}(x') = \text{TCR}(x),$ else return 0]. We define $\epsilon_{tcr} = \Pr[\mathbf{Exp}^{tcr}_{\mathcal{A},\pi}(k) = 1]$.

Definition 4. *(Target Collision Resistant Hash Function) A polynomial-time algorithm* TCR:$\{0,1\}^{\ell} \rightarrow \{0,1\}^{n}$ *is said to be a target collision resistant hash function if for every* p.p.t. $\mathcal{A}$ *it holds that* ϵ_{tcr} *is negligible.*

2.5 Strong Pseudo-Random Permutation

Let π: $\{0,1\}^{k} \times \{0,1\}^{*} \rightarrow \{0,1\}^{*}$ be a family of permutations, and π_k: $\{0,1\}^{*} \rightarrow \{0,1\}^{*}$ be an instance of π, which is indexed by $k \in \{0,1\}^{k}$. Let $\mathcal{P}$ be the set of all permutations for bit strings of size *, and $\mathcal{A}$ be an adversary. Then, consider the following experiments: $\mathbf{Exp}^{sprp}_{\mathcal{A},\pi}(k) : [k \xleftarrow{\$} \{0,1\}^{k}; \beta \leftarrow \mathcal{A}^{\pi_K, \pi_k^{-1}}; return\ \beta]$ and $\mathbf{Exp}^{ideal}_{\mathcal{A},\pi}(k) : [perm \xleftarrow{\$} \mathcal{P}; \beta \leftarrow \mathcal{A}^{perm, perm^{-1}}; return\ \beta]$, where permutations $\pi_K, \pi_k^{-1}, perm, perm^{-1}$ are given to $\mathcal{A}$ as black boxes, and $\mathcal{A}$ can observe only their outputs which correspond to $\mathcal{A}$'s inputs.
We define $\epsilon_{sprp} = \frac{1}{2}|\Pr[\ \mathbf{Exp}^{sprp}_{\mathcal{A},\pi}(k) = 1] - \Pr[\ \mathbf{Exp}^{ideal}_{\mathcal{A},\pi}(k) = 1]|$.

Definition 5. *(Strong Pseudorandom Permutation - SPRP) A polynomial-time algorithm* π_k*:* $\{0,1\}^{*} \rightarrow \{0,1\}^{*}$ *is said to be a strong pseudorandom permutation if for every* p.p.t. $\mathcal{A}$ *it holds that* ϵ_{sprp} *is negligible.*

2.6 Cover Free Families

Let S be a set, and $\mathcal{F}$ a set of subsets of S. Let d, s, q be positive integers, where $|\text{S}| = d$ and $|\mathcal{F}| = s$. We say $\mathcal{F}$ is a q-cover-free family, if for any q subsets of S, $\mathcal{F}_1, \ldots, \mathcal{F}_q \in \mathcal{F}$, and any other subset of S, $\mathcal{F}_i \notin \{\mathcal{F}_1, \ldots, \mathcal{F}_q\}$, we have $\bigcup_{j=1}^{q} \mathcal{F}_j \not\supseteq \mathcal{F}_i$. Additionally, we say the family $\mathcal{F}$ is ℓ-uniform if the cardinality of every element in the family is ℓ.

Furthermore, we point out the existence of a deterministic polynomial time algorithm that on input s, q returns $\ell, d, \mathcal{F}$. 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 $d \leq 16q^2 \log s$. The cover-free family used in our construction has the following parameters (for a security parameter k): $s(k) = 2^k, d(k) = 16kq^2(k), \ell(k) = 4kq(k)$.

2.7 Hybrid Encryption

Our model make use of a method of hybrid encryption [4]. Such schemes uses public-key encryption techniques to encrypt a random key K. The encrypted key $\overline{\mathsf{K}}$ is then used to encrypt a actual message using a symmetric encryption scheme.

Definition 6. *A key encapsulation mechanism is a triplet of algorithms* (KGen, KEnc, KDec) *such that:*

- KGen is a probabilistic polynomial-time (*p.p.t*) key generation algorithm which takes as input a security parameter 1^k and outputs a public key pk and a secret key sk. The public key specifies the key space $\mathcal{K}$ and the symmetric key space $\overline{\mathcal{K}}$.
- KEnc is a (possibly) *p.p.t.* encryption algorithm which receives as input a public key pk, and outputs (K ,$\overline{\mathsf{K}}$), where $\mathsf{K} \in \mathcal{K}$ is a key, and $\overline{\mathsf{K}} \in \overline{\mathcal{K}}$ is a encapsulated symmetric key.
- KDec is a deterministic polynomial-time decryption algorithm which takes as input a secret key sk and a key K, and outputs a encapsulated symmetric key $\overline{\mathsf{K}} \in \overline{\mathcal{K}}$ or an error symbol $\perp$.
- (Soundness) For any pair of public and private keys generated by KGen and any pair (K ,$\overline{\mathsf{K}}$) generated by KEnc it holds that KDec(sk,K)=$\overline{\mathsf{K}}$ with overwhelming probability over the randomness used by KGen and KEnc.

Definition 7. *(Key Encapsulation Mechanism Adaptive Chosen Ciphertext Security) To a two stage adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$, against KEM we associate the following experiment* $\mathbf{Exp}^{kem}_{\mathcal{A},\mathrm{PKE}}(k)$*:*

$(\mathsf{pk}, \mathsf{sk}) \xleftarrow{\$} \mathsf{KGen}(1^k)$
$state \leftarrow \mathcal{A}_1^{\mathsf{KDec}(\mathsf{sk},.)}(\mathsf{pk})$
$(\mathsf{K}^*, \overline{\mathsf{K}}^*) \leftarrow \mathsf{KEnc}(\mathsf{pk})$
$\beta \xleftarrow{\$} \{0,1\}$
If $\beta = 0$, $\overline{\mathsf{K}}^\diamond \leftarrow \overline{\mathsf{K}}^*$, else $\overline{\mathsf{K}}^\diamond \xleftarrow{\$} \overline{\mathcal{K}}$
$\beta' \leftarrow \mathcal{A}_2^{\mathsf{KDec}(\mathsf{sk},\cdot)}(\mathsf{K}^*, \overline{\mathsf{K}}^\diamond, state, \mathsf{pk})$
If $\beta' = \beta$ return 1, else return 0.

The adversary $\mathcal{A}_2$ is not allowed to query KDec(sk,.) with $\overline{\mathsf{K}}^\diamond$. We define the advantage of $\mathcal{A}$ in the experiment as $\mathbf{Adv}^{kem}_{\mathcal{A},\mathrm{PKE}}(\mathrm{k}) = |\Pr[\mathbf{Exp}^{kem}_{\mathcal{A},\mathrm{PKE}}(\mathrm{k}) = 1] - \frac{1}{2}|$. We say a KEM used in a PKE is *indistinguishable against adaptive chosen-ciphertext attack* (IND-CCA2) if for all *p.p.t.* adversaries $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ the advantage of $\mathcal{A}$ in the experiment is a negligible function of k. Throughout this paper, we will denote $\mathbf{Adv}^{kem}_{\mathcal{A},\mathrm{PKE}}(\mathrm{k})$ as ϵ_{kem}.

3 IND-*q*-CCA2 Encryption From CDH

Our construction yields a IND-q-CCA PKE scheme based on CDH assumption with optimal ciphertext length. To achieve a scheme with such features, we make use of hybrid encryption techniques.The symmetric-key encryption scheme is constructed based on strong pseudorandom permutations, as in [2], to obtain redundancy-free property and security against chosen-ciphertext attacks.

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 calculate g^{xy}, for random $g \in \mathbb{G}$, and random x, $y \in \mathbb{Z}_p$. Let TCR:

$\{0,1\}^{\ell} \rightarrow \{0,1\}^{n}$ be a target collision resistant hash function , $\pi : \{0,1\}^{k} \times \{0,1\}^{v} \rightarrow \{0,1\}^{v}$ be a permutation family where the index space is $\{0,1\}^{k}$, and h: $\mathbb{G}\times\ \{0,1\}^{u} \rightarrow \{0,1\}^{v}$ be a hard-core function family.Our scheme from CDH assumption consists of the following algorithms:

$\mathsf{Gen}(1^k)$: Define $s(k) = 2^k, d(k) = 16kq^2(k), \ell(k) = 4kq(k)$. Run KGen. For $i = 1,\ldots,d(k)$ and $m = 1,\ldots,k$, computes $X_{mi} = g^{x_{mi}}$ for $x_{mi} \xleftarrow{\$} \mathbb{Z}_p$. Choose $a \xleftarrow{\$} \{0,1\}^u$. Outputs $\mathsf{pk}_m = (X_{m1},\ldots,X_{md(k)})$ and $\mathsf{sk}_m = (x_{m1},\ldots,x_{md(k)})$. The public key is $\mathsf{pk} = \{\mathsf{pk}_1,\ldots,\mathsf{pk}_k, a\}$, and the secret key is $\mathsf{sk} = \{\mathsf{sk}_1,\ldots,\mathsf{sk}_k\}$.

$\mathsf{Enc}(\mathsf{pk}, \mathsf{M})$: Run KEnc. KEnc computes $\mathrm{r} = g^b$ for $b \xleftarrow{\$} \mathbb{Z}_p$ $j = \mathrm{TCR}(\mathrm{r})$ where $\mathcal{F}_j = \{j_1,\ldots,j_{\ell(k)}\}$ is the q-CFF subset associated to value j(which will define the set of the session's public/private keys). Sets K= r and calculates $\overline{\mathsf{K}}_m = (\mathrm{h}(X^b_{mj_1}, a) \oplus \ldots \oplus \mathrm{h}(X^b_{mj_{\ell(k)}}, a))$ for $m = 1,\ldots,k$, where $\oplus$ is the XOR bitwise. Define $\overline{\mathsf{K}} = \overline{\mathsf{K}}_1||\overline{\mathsf{K}}_2||\ldots||\overline{\mathsf{K}}_k$. To encrypt message M, run symmetric-key encryption to obtain the ciphertext $\psi \leftarrow \pi_{\overline{\mathsf{K}}}(\mathsf{M})$. Output C=(K, ψ).

$\mathsf{Dec}(\mathsf{sk}, \mathsf{C})$: Run KDec. KDec computes $j = \mathrm{TCR}(\mathsf{K})$ to obtain the subset $\mathcal{F}_j$, and compute $\overline{\mathsf{K}}_m = (\mathrm{h}(\mathsf{K}^{x_{mj_1}}, a) \oplus \ldots \oplus \mathrm{h}(\mathsf{K}^{x_{mj_{\ell(k)}}}, a))$. Set $\overline{\mathsf{K}} = \overline{\mathsf{K}}_1||\overline{\mathsf{K}}_2||\ldots||\overline{\mathsf{K}}_k$. Decrypt ψ to $\mathsf{M} \leftarrow \pi^{-1}_{\overline{\mathsf{K}}}(\psi)$.

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

We follow the same approach of [2] to prove the above theorem via a game-based proof. We prove that the KEM is IND-q-CCA2 secure and then use the KEM/DEM composition theorem from [4]. Let **Game 0** be the KEM-IND-q-CCA game with adversary $\mathcal{A}$ where $\mathsf{K}^* = r^* = g^y$ for $y \xleftarrow{\$} \mathbb{Z}_p$ and $\mathcal{A}$'s output of the game, β, is a random bit. Let X_0 denotes that $\beta = \beta'$. For later games, let X_i ($i > 0$) be defined analogously. We have: $\frac{1}{2}\mathbf{Adv}^{\text{KEM-IND-}q\text{-CCA}}_{\text{PKE},\mathcal{A}}(k) = |\Pr[X_0] - \frac{1}{2}|$.

Game 1 is identical to **Game 0**, except that the key K^* is initially chosen, and all decapsulation queries with $\mathrm{TCR}(\mathsf{K}) = \mathrm{TCR}(\mathsf{K}^*)$ are rejected. By reduction on the security of the TCR, one can show that $|\Pr[X_1] - \Pr[X_0]| \leq \epsilon_{tcr} + \frac{q(k)}{p}$, for a suitable adversary $\mathcal{V}$, where ϵ_{tcr} is the probability that $\mathcal{V}$ finds $\mathrm{TCR}(\mathsf{K}) = \mathrm{TCR}(\mathsf{K}^*)$ for $\mathsf{K} \neq \mathsf{K}^*$ and $\frac{q(k)}{p}$ is an upper bound on the probability that $\mathcal{A}_1$ ask the decryption oracle to decrypt K^*.

Game 2 is equivalent to **Game 1**. In this game, we will define$Q := \bigcup_{\mathsf{K}^i \neq \mathsf{K}^*} \mathcal{F}_{j^i}$, where K^i is the i-th decapsulation request of $\mathcal{A}$, $j^i = \mathrm{TCR}(\mathsf{K}^i)$ and $\mathcal{F}_{j^i}$ are the sets of PKE key pairs associated with the respective i-th query. Define $t := \min(\mathcal{F}_{j^*} \backslash Q)$, for $j^* = \mathrm{TCR}(\mathsf{K}^*)$ (it is always possible since $\mathcal{F}_{j^*} \nsubseteq Q$). Additionally we choose uniformly and independently $\alpha \in \mathcal{F}_{j^*}$. Call ABORT the event that $\alpha \neq t$. Note that $\Pr[\text{ABORT}|X_2] = \frac{\ell-1}{\ell} = \Pr[\text{ABORT}]$, so the events X_2 and ABORT are independent, and in particular, $\Pr[X_2] = \Pr[X_1]$.

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

$\frac{1}{2}$. Since Pr[ABORT] = $(\ell - 1)/\ell$ 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 as soon as $\mathcal{A}$ asks for a decapsulation where $\mathsf{K} \neq \mathsf{K}^*$ and $\alpha \in \mathcal{F}_j$ ($j = \mathrm{TCR}(\mathsf{K})$). Consequently, $\Pr[X_4]$=$\Pr[X_3]$.

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

In **Game 5**, the challenge key is formed as: $\overline{\mathsf{K}} = \overline{\mathsf{K}}_1||\overline{\mathsf{K}}_2||\ldots||\overline{\mathsf{K}}_k$. 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: $\overline{\mathsf{K}} = \overline{\mathsf{K}}_1||\overline{\mathsf{K}}_2||\ldots||\overline{\mathsf{K}}_{k-1}||rnd^1$, where rnd^1 is a random element from $\{0,1\}^v$. The last component $\overline{\mathsf{K}}_k$ in **Game 5** is formed as $\overline{\mathsf{K}}_k = \mathrm{h}(X^y_{kj_1}, a) \oplus \ldots \oplus \mathrm{h}((g^{x_{k\alpha}})^y, a) \oplus \ldots \oplus \mathrm{h}(X^y_{kj_\ell}, a)$. We can see that distinguishing $\overline{\mathsf{K}}_k$ from a random element of $\{0,1\}^v$ implies in distinguishing $\mathrm{h}((g^{x_{k\alpha}})^y, a)$ from a random element of $\{0,1\}^v$. From **Theorem 2.5**, an adversary that distinguishes $\mathrm{h}((g^{x_{k\alpha}})^y, a)$ from a random element of $\{0,1\}^v$, solves the CDH problem. Therefore, if the CDH assumption holds, $\Pr[X_6]$ - $\Pr[X_5] \leq \epsilon''$, where ϵ'' is negligible.

In **Game 5+n**, for $2 \leq n \leq k$, the challenge key is formed as the following: $\overline{\mathsf{K}} = \overline{\mathsf{K}}_1||\overline{\mathsf{K}}_2||\ldots||\overline{\mathsf{K}}_{k-n}||rnd^n$, where rnd^n is a random element from $\{0,1\}^{nv}$. From **Theorem 2.5**, $\Pr[X_{5+n}]$ - $\Pr[X_{5+n-1}] \leq \epsilon''$, where ϵ'' is negligible. In particular, $\Pr[X_{5+k}] = \frac{1}{2}$, since in **Game 5+$k$** the key is completely random. Collecting the probabilities we have that:$\mathbf{Adv}^{\text{KEM-IND-}q\text{-CCA}}_{\text{PKE},\mathcal{A}}(k) \leq 2 \cdot \epsilon_{tcr} + \ell(k) \cdot k \cdot \epsilon'' + \frac{2q(k)}{p}$.

References

1. D. Cash, E. Kiltz, and V. Shoup. The twin diffie-hellman problem and applications. *Journal of Cryptology*, 22(4):470–504, 2009.
2. R. Cramer, G. Hanaoka, D. Hofheinz, H. Imai, E. Kiltz, R. Pass, A. Shelat, and V. Vaikuntanathan. Bounded cca2-secure encryption. *ASIACRYPT '07*.
3. R. Cramer and V. Shoup. A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. *CRYPTO '98*, 1462 of LNCS(13-25).
4. R. Cramer and V. 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.
5. D. Dolev, C. Dwork, and M. Naor. Non-malleable cryptography. *STOC '91*.
6. O. Goldreich and L. Levint. A hard-core predicate for all one-way functions. In *STOC '89*.
7. G. Hanaoka and K. Kurosawa. Efficient chosen ciphertext secure public key encryption under the computational diffie-hellman assumption. In *ASIACRYPT '08*.
8. K. Haralambiev, T. Jager, E. Kiltz, and V. Shoup. Simple and efficient public-key encryption from computational diffie-hellman in the standard model. *PKC '10*.
9. D. Hofheinz and E. Kiltz. Secure hybrid encryption from weakened key encapsulation. *CRYPTO '07*.
10. M. Naor and M. Yung. Public-key cryptosystems provably secure against chosen ciphertext attacks. *STOC '90*.
11. C. Rackoff and D. Simon. Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack. *Crypto '91*.