Definition 1 (PPT Decryption Robustness (DROB))**.** *A public key encryption scheme* $\mathsf{PKE} := (\mathsf{Keygen}, \mathsf{Enc}, \mathsf{Dec})$ *satisfies* Decryption Robustness ($\mathsf{DROB\text{-}CCA}$) *if for all efficient adversaries* $\mathcal{A}$ *there exists a negligible* $\mathsf{negl}(\cdot)$ *s.t.*

$$\Pr\left[\mathsf{Exp}^{\mathsf{DROB\text{-}CCA}}_{\mathcal{A},\mathsf{PKE}}(\lambda) = 1\right] \le \mathsf{negl}(\lambda), \text{ where}$$

$$\begin{array}{l} \underline{\mathsf{Exp}^{\mathsf{DROB\text{-}CCA}}_{\mathcal{A},\mathsf{PKE}}(\lambda):} \\ c \leftarrow \mathcal{A}(\lambda) \\ (pk, sk) \leftarrow \mathsf{Keygen}(\lambda) \\ \textbf{return } \mathsf{Dec}(sk, c) \ne \perp \end{array}$$

If PKE satisfies $\mathsf{DROB\text{-}CCA}$, then an adversary cannot create a valid ciphertext without knowing the keypair, specifically, the public key.

Theorem 1. *If* PKE *satisfies* SROB*, then it also satisfies* DROB*.*

Proof. We prove the contrapositive, i.e., we show that if there is an efficient adversary $\mathcal{B}$ against $\mathsf{DROB\text{-}CCA}$, then there is an efficient adversary $\mathcal{A}$ against $\mathsf{SROB\text{-}CCA}$.

The $\mathsf{SROB\text{-}CCA}$ adversary $\mathcal{A}$ receives the security parameter λ and two public keys pk_0, pk_1 corresponding to private keys sk_0, sk_1, respectively. $\mathcal{A}$ runs $c \leftarrow \mathcal{B}(\lambda)$ and submits c to the challenger. We analyze the probability of success for $\mathcal{A}$.

We need to show that $f(\lambda) := \Pr\left[\mathsf{Exp}^{\mathsf{SROB\text{-}CCA}}_{\mathcal{A},\mathsf{PKE}}(\lambda) = 1\right]$ is non-negligible; specifically that

$$\exists d \in \mathbb{N}, \forall n_0 \in \mathbb{N}, \exists \lambda \ge n_0 : f(\lambda) > \frac{1}{\lambda^d}.$$

By assumption, $g(\lambda) := \Pr\left[\mathsf{Exp}^{\mathsf{DROB\text{-}CCA}}_{\mathcal{B},\mathsf{PKE}}(\lambda) = 1\right]$ is non-negligible, i.e., there exists $d_{\mathsf{DROB}} \in \mathbb{N}$ s.t. for any $n_0 \in \mathbb{N}$ there exists $\lambda \ge n_0$ for which $g(\lambda) > \frac{1}{\lambda^{d_{\mathsf{DROB}}}}$. Note that

$$g(\lambda) = \Pr_{\substack{(pk,sk)\sim\mathsf{Keygen}(\lambda) \\ r\sim U_\lambda}}\left[\mathsf{Dec}(sk, \mathcal{B}(\lambda, r)) \ne \perp\right] \implies$$

$$g(\lambda) = \sum_{c \in \mathcal{C}_\lambda} \Pr_{r\sim U_\lambda}\left[\mathcal{B}(\lambda, r) = c\right] \cdot \Pr_{(sk,pk)\sim\mathsf{Keygen}(\lambda)}\left[\mathsf{Dec}(sk, c) \ne \perp\right] > \frac{1}{\lambda^{d_{\mathsf{DROB}}}}.$$

where $\mathcal{C}_\lambda \subseteq \mathcal{C}$ is the set of possible ciphertexts output by $\mathcal{B}(\lambda, \cdot)$ and r denotes the random coins for $\mathcal{B}$. By definition of $\mathcal{A}$ we have

$$f(\lambda) = \Pr\left[\mathsf{Exp}^{\mathsf{SROB\text{-}CCA}}_{\mathcal{A},\mathsf{PKE}}(\lambda) = 1\right] = \Pr_{\substack{(pk_0,sk_0)\sim\mathsf{Keygen}(\lambda) \\ (pk_1,sk_1)\sim\mathsf{Keygen}(\lambda) \\ r\sim U_\lambda}}\left[\mathsf{Dec}(sk_0, \mathcal{B}(\lambda, r)) \ne \perp \wedge \mathsf{Dec}(sk_1, \mathcal{B}(\lambda, r)) \ne \perp\right] \implies$$

$$f(\lambda) = \sum_{c \in \mathcal{C}_\lambda} \Pr_{r\sim U_\lambda}\left[\mathcal{B}(\lambda, r) = c\right] \cdot \Pr_{\substack{(pk_0,sk_0)\sim\mathsf{Keygen}(\lambda) \\ (pk_1,sk_1)\sim\mathsf{Keygen}(\lambda)}}\left[\mathsf{Dec}(sk_0, c) \ne \perp \ \wedge \mathsf{Dec}(sk_1, c) \ne \perp\right].$$

Clearly, for a fixed c, the probabilities that $\mathsf{Dec}(sk_0, c) \ne \perp$ and $\mathsf{Dec}(sk_1, c) \ne \perp$ are independent since sk_0 and sk_1 are independently sampled, therefore

$$f(\lambda) = \sum_{c \in \mathcal{C}_\lambda} \Pr_{r\sim U_\lambda}\left[\mathcal{B}(\lambda, r) = c\right] \cdot \left(\Pr_{(pk,sk)\sim\mathsf{Keygen}(\lambda)}\left[\mathsf{Dec}(sk, c) \ne \perp\right]\right)^2. \tag{1}$$

Jensen's inequality gives us that $\psi(\mathbb{E}[X]) \le \mathbb{E}(\psi(X))$ where ψ is a real convex function and $X : \Omega \to \mathcal{X}$ a random variable. Furthermore, $\mathbb{E}[h(X)] = \sum_{x\in\mathcal{X}} h(x) \Pr[X = x]$ for any $h : \mathcal{X} \to \mathbb{R}$. In our case

$$\psi(x) := x^2$$
$$X := \mathcal{B}(\lambda, \cdot) : U_\lambda \to \mathcal{C}_\lambda \implies \forall c \in \mathcal{C}_\lambda : \Pr[X = c] := \Pr_{r\sim U_\lambda}\left[\mathcal{B}(\lambda, r) = c\right]$$
$$h(c) := \Pr_{(sk,pk)\sim\mathsf{Keygen}(\lambda)}\left[\mathsf{Dec}(sk, c) \ne \perp\right].$$

Therefore, by applying Jensen's inequality to Eq. 1 we get

$$f(\lambda) \geq \left(\sum_{c \in \mathcal{C}_\lambda} \Pr_{r \sim U_\lambda} [\mathcal{B}(\lambda, r) = c] \cdot \Pr_{(sk,pk) \sim \mathsf{Keygen}(\lambda)} [\mathsf{Dec}(sk, c) \neq \perp] \right)^2 = g(\lambda)^2 > \frac{1}{\lambda^{{d_{\mathsf{DROB}}}^2}}.$$

In other words, we have found $d \coloneqq {d_{\mathsf{DROB}}}^2$ which proves that $f(\lambda) = \Pr\left[\mathsf{Exp}^{\mathsf{SROB\text{-}CCA}}_{\mathcal{A},\mathsf{PKE}}(\lambda) = 1\right]$ is non-negligible.

$\square$