Appendix : IND-CPA games

A scheme E is said to be IND-CPA secure if no attacker can win the following games with probability more than $0.5+\varepsilon(\lambda)$, where $\varepsilon(\lambda)$ is a negligible function of the security paramater λ (usually, λ is the size of the key).

IND-CPA game without diversification

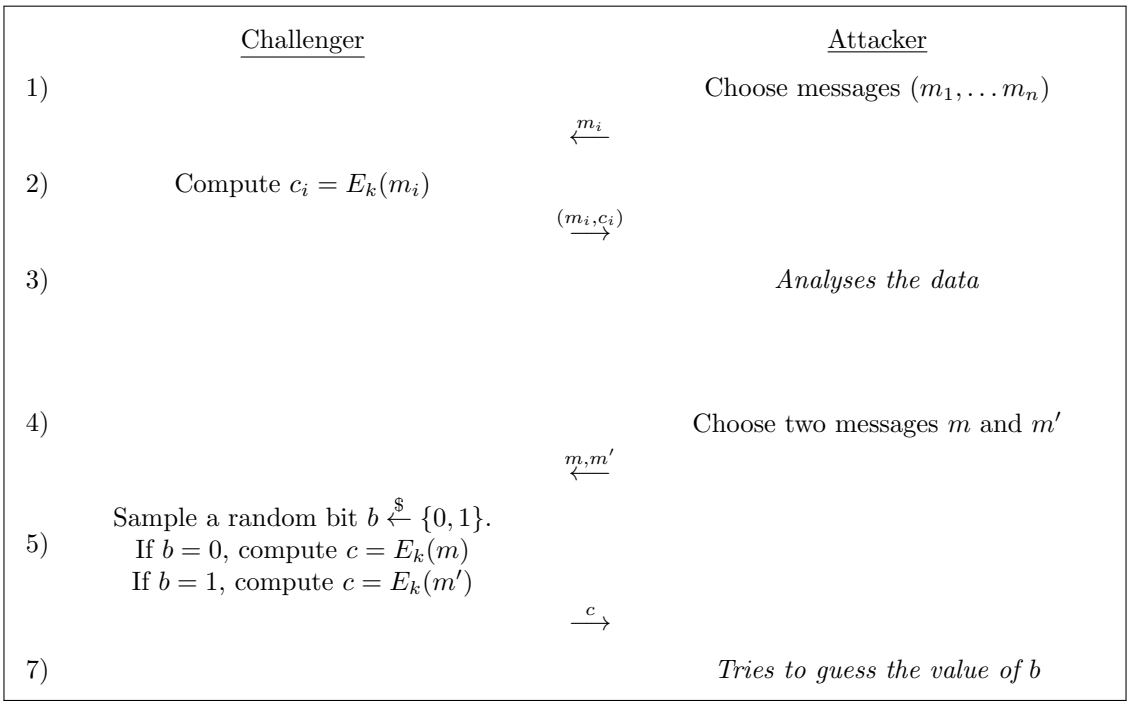

FIGURE 1 – The IND-CPA game without diversification

The attacker must respect some constraints when choosing their messages :

1. The number of queries must be of polynomial size (with regard to the security parameter λ).
2. The messages m and m' cannot be among the queried messages.

IND-CPA game with diversification

Now, our scheme E has three inputs : the key k, the message m and a diversifier d. The IND-CPA game becomes :

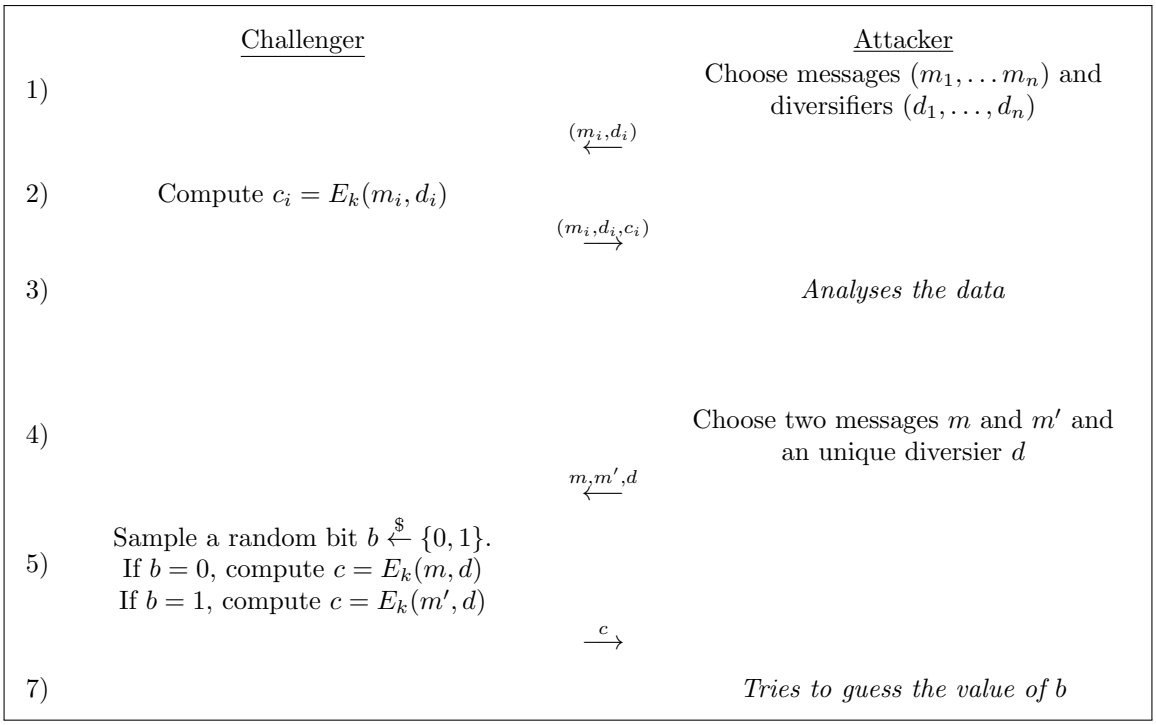

FIGURE 2 – The IND-CPA game with diversification

The attacker must respect some constraints when choosing their messages and diversifiers :

1. The number of queries must be of polynomial size (with regard to the security parameter λ).
2. The messages m and m' can be anything.
3. The diversifier d must be a nonce : it cannot be equal to any d_i chosen during the query phase.