2.9.1 Leakage Models

Classical leakage models come from the fact that, in CMOS technology (which is used to realise the majority of existing integrated circuits), peaks of power consumption are observable when the output of the gates transition from either a "0" to "1" or a "1" to "0" logic state. For an internal variable Z, examples of classical leakage models $L(Z)$ are the following deterministic functions of Z:

- *mono-bit model*: the value of one bit of Z,
- *Hamming weight model*: the Hamming weight $\mathrm{HW}(Z)$,
- *Hamming distance model*: the Hamming distance between Z and another intermediate variable Z', defined as $\mathrm{HD}(Z, Z') = \mathrm{HW}(Z \oplus Z')$, supposing *e.g.* that one of the two variable overwrites the other into the same logic states (thus, the number of switched bits is counted),
- *linear model*: a linear combination of the bits of Z, supposing that some states influence the power consumption more than others,
- *identity model*: the value of Z itself.

When a leakage model is considered, it is understand that the variable $\vec{X}$ is a noised observation of $L(Z)$. The noise distribution is a critical component of the attack efficiency. Thus, some efforts to better specify the form of the noise in such a model have been done in the SCA literature, leading to perform analysis with some *noisy leakage models*. The most classical noisy leakage model is the one introduced by [Cha+99], where noise is assumed as an addend of the deterministic function $L(Z)$, is assumed to follow a Gaussian distribution, and is quantified by its standard deviation. A more general model was proposed in [PR13], where noise is quantified as a statistical distance, called *bias*, between the distribution of Z and the conditional distribution of Z given $\vec{X}$. In this thesis we do not need to consider a precise description of the noise. Despite the fact that some of the proposed techniques present optimality features in presence of Gaussian hypothesis, we will not endorse the Gaussian model. The unique assumption that is done is the following, that we believe be a common point of many models in literature. The first-order moments of the conditional variables $\vec{X} \mid Z = s$ are different for at least two different values of s. When a (deterministic) leakage model $L(Z)$ is considered, it is understood that it coincides with such first moments, *i.e.* $L(s) = \mathbb{E}[\vec{X} \mid Z = s]$. In general it is meant that the noise has no impact over the first-order moments of the acquisition, but only eventually over the quality of their estimations.