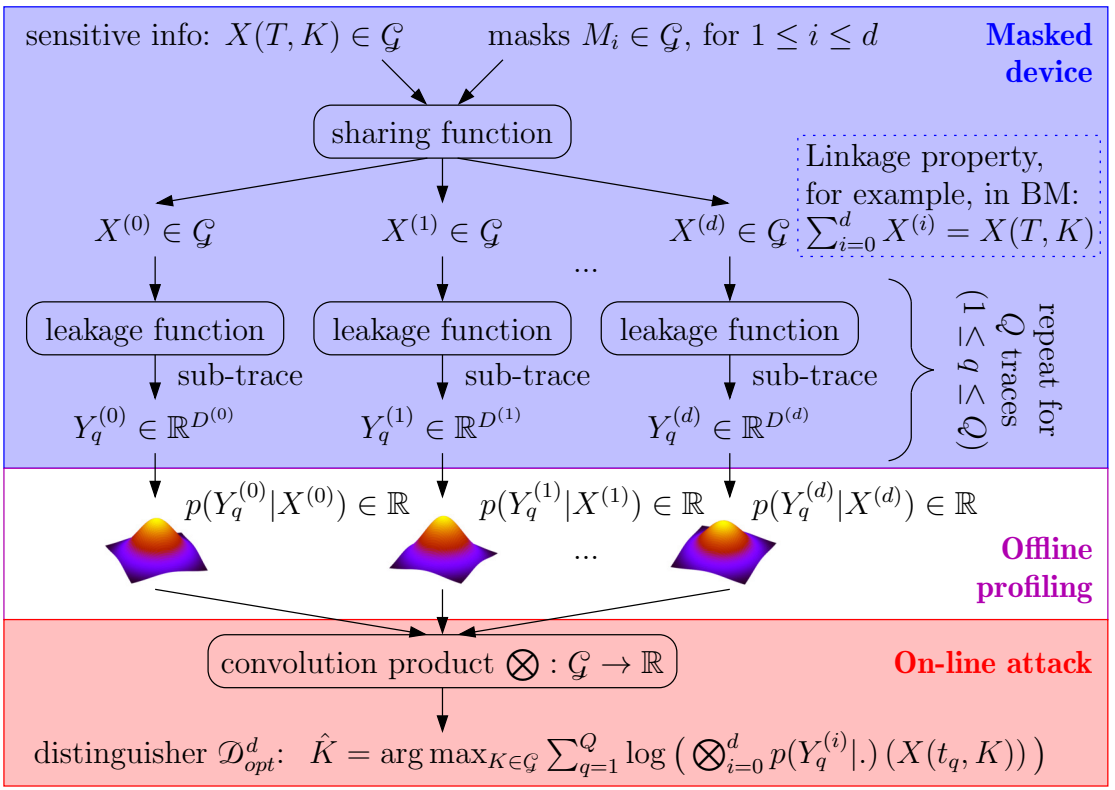
sensitive info: $X(T,K) \in \mathcal{G}$
masks $M_i \in \mathcal{G}$, for $1 \le i \le d$
Masked device
sharing function
Linkage property, for example, in BM: $\sum_{i=0}^{d} X^{(i)} = X(T,K)$
$X^{(0)} \in \mathcal{G}$
$X^{(1)} \in \mathcal{G}$
...
$X^{(d)} \in \mathcal{G}$
leakage function
leakage function
leakage function
sub-trace
sub-trace
sub-trace
$Y_q^{(0)} \in \mathbb{R}^{D^{(0)}}$
$Y_q^{(1)} \in \mathbb{R}^{D^{(1)}}$
$Y_q^{(d)} \in \mathbb{R}^{D^{(d)}}$
repeat for Q traces $(Q \ge q \ge 1)$
$p(Y_q^{(0)}|X^{(0)}) \in \mathbb{R}$
$p(Y_q^{(1)}|X^{(1)}) \in \mathbb{R}$
...
$p(Y_q^{(d)}|X^{(d)}) \in \mathbb{R}$
Offline profiling
convolution product $\bigotimes : \mathcal{G} \to \mathbb{R}$
On-line attack
distinguisher $\mathcal{D}_{opt}^{d}$: $\hat{K} = \arg\max_{K \in \mathcal{G}} \sum_{q=1}^{Q} \log\left(\bigotimes_{i=0}^{d} p(Y_q^{(i)}|.)\,(X(t_q,K)) \right)$