

I dispositivi crittografici possono essere fatti oggetto di attacchi basati sulla vulnerabilità dell'hardware che supporta la loro realizzazione. Tali attacchi (side channel attacks) si basano sull'osservazione di alcuni parametri fisici dei dispositivi al fine di rivelarne i segreti (ad esempio la password). È però possibile contrastare gli attacchi mediante opportune contromisure inserite nei dispositivi stessi.