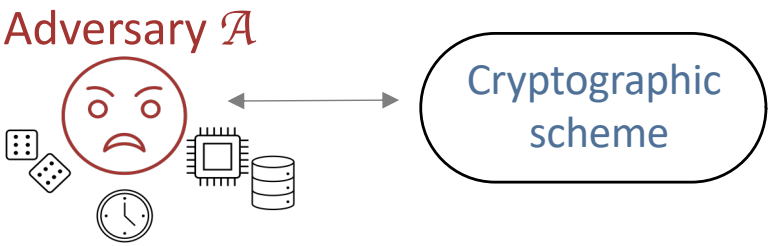
Unconditional vs. Conditional Security -

Unconditional (Information-theoretic)	Conditional (Computational)
... security	
*An adversary with **no restrictions** (**unbounded** computational resources - time, memory) **cannot break** the scheme.*	*An adversary with **computational restrictions** (**bounded** time, memory) **can break** the scheme with **some (negligible) probability**.*

Stands against brute force (+)

Good in theory, poor in practice (−)



(+) Suitable for practice

(−) Weaker than unconditional security

A cryptographic construction satisfies ***computational security*** if any adversary $\mathcal{A}$ that runs the attack in a time $t(n)$ succeeds the attack with probability at most $\varepsilon(n)$; t and ε are functions of a ***computational security parameter*** n.

Statistical Security

A cryptographic construction satisfies $\varepsilon(\lambda)$ ***statistical security*** if any unbounded adversary $\mathcal{A}$ succeeds the attack with probability at most $\varepsilon(\lambda)$; ε is function of a ***statistical security parameter*** λ.

- Introduces a *small* advantage $\varepsilon(\lambda)$ wrt the *a-priory probability* of winning

Statistical and *computational* security are both ***relaxations*** of information-theoretical security.

PPT (Probabilistic Polynomial in Time) Adversary

- $t(n)$ is **polynomial** in n
- $\varepsilon(n)$ is **negligible** in n

Negligibility:

$\forall p(n), \exists n_d$ such that $\forall n \geqslant n_d$ it holds $\varepsilon(n) < 1/p(n)$

$p(n) = n^d$ and d constant

Examples:

✗ $1/2$, $1/n^{100}$

✓ $1/2^n$, $p(n)/2^n$