Authentication + Anonymity → Ex : Voting

Binding + Blinding → Ex : Auction

↳ Data cannot be changed

↳ Data should not be seen

Compression cannot be 1 : 1 but decompression has to be 1 : 1

More frequent items - compressed, less frequent - expanded, but esoteric, less frequent → It is 1:1 but in use it compresses, some inputs can be smaller than their outputs

Compression without collision

Many to 1 map without collision

Ex : Passwords Hash verification

These are logical impossibilities by definition

First principle of information security : information security is impossible

For passwords, given password x, we want to store $f(x)$ such that given $f(x)$ we cannot know x & $\nexists\ y \ni f(x) \neq f(y)$.

For a fixed password length, by pigeonhole principle, we only need total no. of possible passwords + 1 to brute force.

The 'perfect' password is thus infinite length.

Instead, changing password often → over infinite time, password length is infinite

Destructive Impossibility Interference - Introduce impossibilities that removes constraint

Singleton Bound, Byzantine Agreement, Zero Knowledge Proof

Kinds of impossibilities:

I: Computational Resource Bounds: Modern Internet - Integer Factorization

II: Physical Impossibility

III: Questions with no answers

IV: Practical Impossibility