Hash functions

ian.mcloughlin@gmit.ie

Definition (Functions)**.** *A function from a set A to a set B is a set f of ordered pairs with the first element from A and the second from B, such that each element from A is the first element in a tuple exactly once. We write $f : A \to B$.*

A computer is a generic electronic circuit, capable of mimicking other circuits. Lots of circuits of purpose-built, pre-designed to perform some individual function. For example, a light circuit for a room is designed to turn on and off lights, and nothing else. A light switch is a device that allows a human to change the input to a light bulb. The input can be a high voltage, in which case the light will be on, or a low voltage in which case the light will be off. The light switch switches between these two inputs to the light bulb.

When we talk about computers we typically call on and off 0 and 1, but the physical reality is the same — the computer is typically using different voltages for 0's and 1's. Where a light bulb might only essentially have one wire which can take on two different voltages, computer circuits might have tens, millions, or even billions of wires that can each take on two different voltages. The Central Processing Unit (CPU), a crucial device in your computer, might use a sixty-four wire circuit. In how many different ways can sixty-four on-off switches be