Introduction
27 January 2016


Definition 2 (Zero-Knowledge Proof). A proof for some statement $X$ that does not provide any information other than “$X$ is true.”

Definition 3 (Binary String). Or 0-1 string. A string of 0/1 strings of any length, e.g. 0011011101.

Definition 4 (Set). A collection of objects with no order and no repetition, written as a list between curly braces. For example, \{Red, Brown, Green\}

Definition 5 (Subset). A set $B$ is a subset of $A$ if every element in $B$ is also an element in $A$. $A$ is a subset of itself, and the empty set (written $\varnothing$) is a subset of $A$.

Theorem 1. A set containing $n$ objects has $2^n$ subsets.