

Definition of the zero knowledge proof refuted

© Copyright 2017 by Colin James III All rights reserved.

From: en.wikipedia.org/wiki/Zero-knowledge_proof

"A formal definition of zero-knowledge has to use some computational model, the most common one being that of a Turing machine. Let P, V, and S be Turing machines. An interactive proof system with (P,V) for a language L is zero-knowledge if for any probabilistic polynomial time (PPT) verifier V-hat there exists an expected PPT simulator S such that

$$\forall x \in L, z \in \{0,1\}^*, \text{View}_{V\text{-hat}} [P(x) \leftrightarrow V\text{-hat}(x,z)] = S(x,z). \quad (1.1)$$

We assume the apparatus of the Meth8 modal logic model checker implementing variant system VL4. Meth8 allows to mix four logical values with four analytical values. The designated *proof* value is T.

Definition	Axiom	Symbol	Name	Meaning	2-tuple	Ordinal
1	p=p	T	Tautology	proof	11	3
2	p@p	F	Contradiction	absurdum	00	0
3	%p>#p	N	Non-contingency	truth	01	1
4	%p<#p	C	Contingency	falsity	10	2

LET: ~ Not; + Or; & And; \ Not and; > Imply; < ∈ Not imply; = ↔ Equivalent to;
 @ Not equivalent to; # all; % some; (p@p) 00, zero; (p=p) 11, one;
 q p s u v x z L P S V-hat View x z

Results are the repeating proof table(s) of 16-values in row major horizontally.

We render Eq. 1.10 as:

$$(((\#x < q) \& (z < ((p @ p) + (p = p)))) \& ((v \& u) \& ((p \& x) = (u \& (x \& z)))))) = (s \& (x \& z)) ; \quad (1.2)$$

TTTT TTTT TTTT TTTT, TTTT TTTT FFFF FFFF

Eq. 1.2 means the formal definition of the zero-knowledge proof as rendered is *not* tautologous.

What follows is the assumption that in **NP** all problems and all languages have zero-knowledge proofs is mistaken. What also follows is that one-way functions do not exist.