Cryptographic Protocols

Spring 2017

Part 5

Proofs in NP

„Normal“ Proof

Peggy		Vic
Statement s, Proof p	$\xrightarrow{p}$	verifies proof: $\Psi(s,p) \rightarrow$ accept otherwise $\rightarrow$ reject

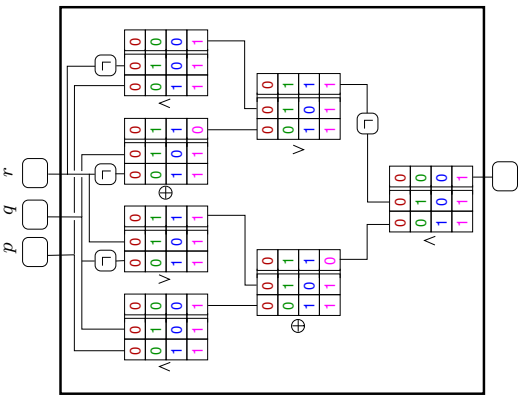
Zero-Knowledge Proof

Peggy		Vic
Statement s, prove „I know p s.t. $\Psi(s,p)$“	$\Longleftrightarrow$	accept/reject

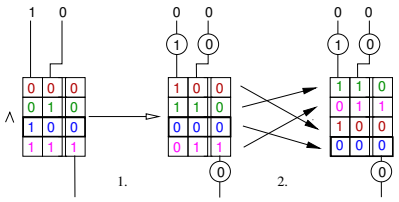
represent $\Psi(s,\cdot)$ as binary circuit $\longrightarrow$ Circuit-SAT

Boolean Circuit for Ψ

$$\Psi \equiv \big((p \wedge q) \oplus (\neg q \vee r)\big) \wedge \neg\big((\neg r \oplus q) \vee (p \vee \neg r)\big)$$



How to Scramble the Truth Tables



1. XOR every wire with a random bit
2. Permute the rows randomly

Scrambled Boolean Circuit for Ψ