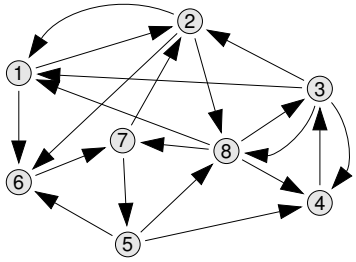
Cryptographic Protocols

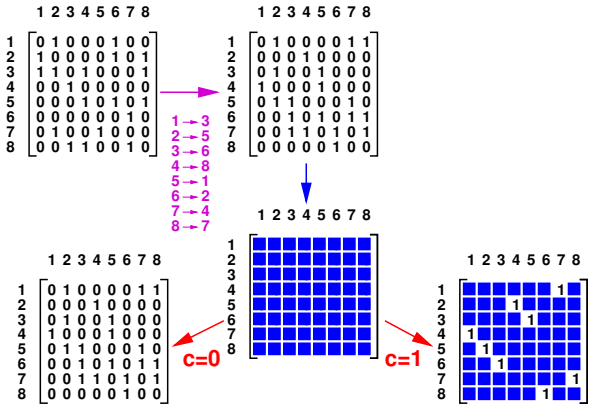
Spring 2020

Part 4

Hamiltonian Cycles



Hamiltonian Cycles — Protocol Idea

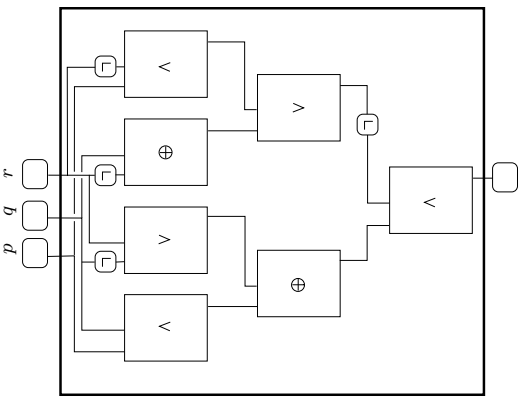


Hamiltonian Cycles — One Round of the Protocol

Peggy		Vic
knows HC in $\mathcal{G}$		knows $\mathcal{G}$
π at rand., $\mathcal{H} = \pi\mathcal{G}\pi^{-1}$ Commit $\mathcal{H} \to C_1, .., C_{n^2}$	$\xrightarrow{C_1, .., C_{n^2}}$	
	$\xleftarrow{c}$	$c \in_R \{0, 1\}$
$c = 0$: Decommit $\mathcal{H}$	$\xrightarrow{\pi, d_1, .., d_{n^2}}$	$\mathcal{H} \stackrel{?}{=} \pi\mathcal{G}\pi^{-1}$
$c = 1$: Decommit HC	$\xrightarrow{d_{I_1}, .., d_{I_n}}$	$d_{I_1}, .., d_{I_n} \stackrel{?}{=}$ HC

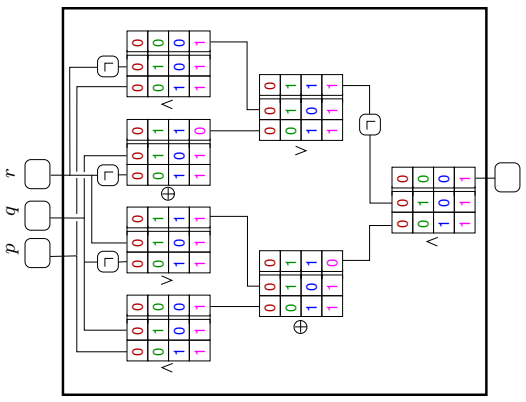
Boolean Circuit for Ψ

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

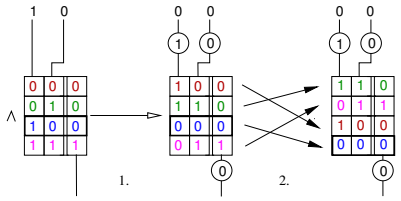


Boolean Circuit for Ψ

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

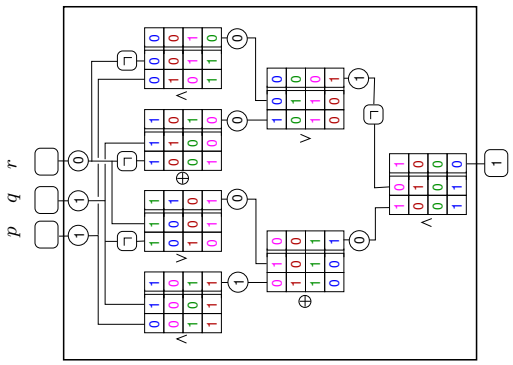


How to Scramble the Truth Tables



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

Scrambled Boolean Circuit for Ψ



Scrambled Boolean Circuit for Ψ