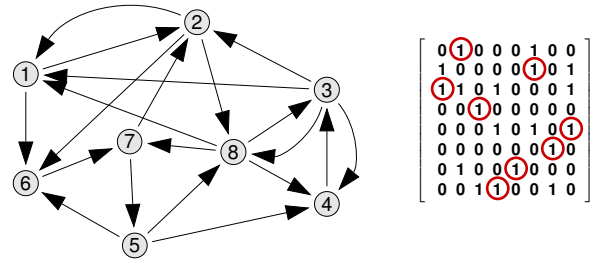


Cryptographic Protocols

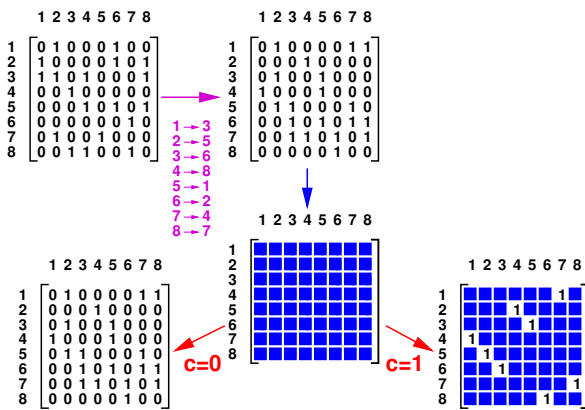
Spring 2019

Part 5

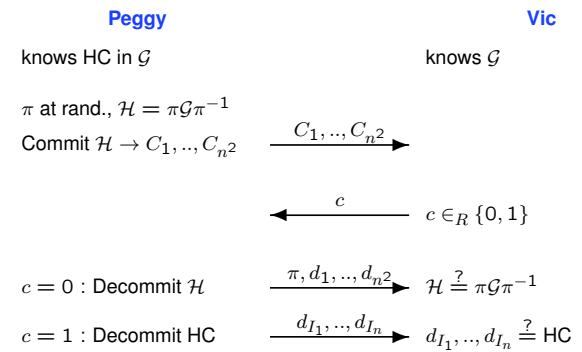
Hamiltonian Cycles



Hamiltonian Cycles — Protocol Idea



Hamiltonian Cycles — One Round of the Protocol

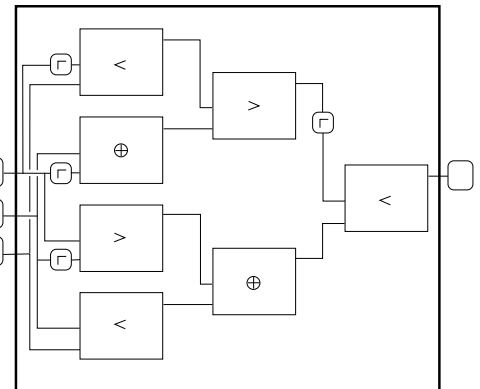


Commitment Schemes

Name	Setup	Value	Commit	Type	Comments
GI	G_0, G_1 $G_1 = \sigma G_0 \sigma^{-1}$	$x \in \{0, 1\}$	$B = \pi G_x \pi^{-1}$	H	Trapdoor: σ
DL	$ H = q$ $H = \langle h \rangle$	$x \in \mathbb{Z}_q$	$b = h^x$	B	OR: $\text{LSB}(x)$
Pedersen	$ H = q$ $H = \langle g \rangle = \langle h \rangle$	$x \in \mathbb{Z}_q$	$b = g^x h^r$	H	Trapdoor $\text{DL}_{g,h}$
QR B	$m = pq$, $t \in \text{QNR}$, $(\frac{t}{m}) = 1$	$x \in \{0, 1\}$	$b = r^2 t^x$	B	
QR H	$m = pq$, $t \in \text{QR}$	$x \in \{0, 1\}$	$b = r^2 t^x$	H	Trapdoor \sqrt{t}

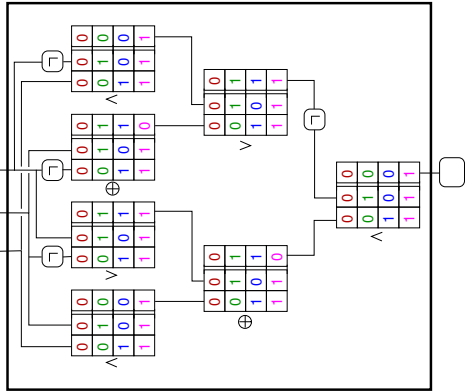
Boolean Circuit for Ψ

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

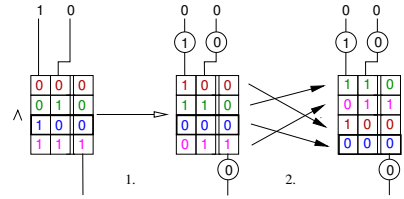


Boolean Circuit for ψ

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



How to Scramble the Truth Tables



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

Scrambled Boolean Circuit for ψ

