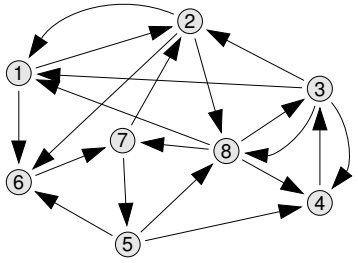
Cryptographic Protocols

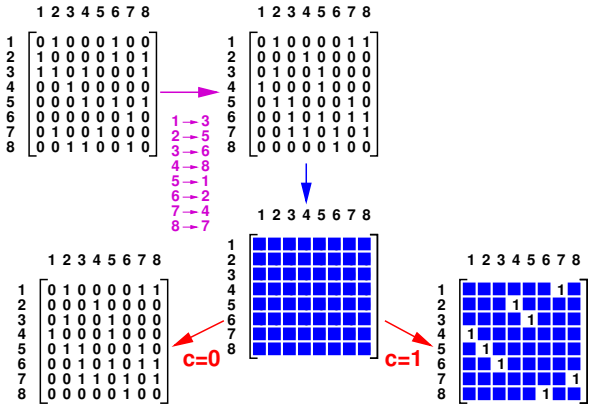
Spring 2018

Part 5

Hamiltonian Cycles



Hamiltonian Cycles — Protocol Idea



Hamiltonian Cycles — One Round of the Protocol

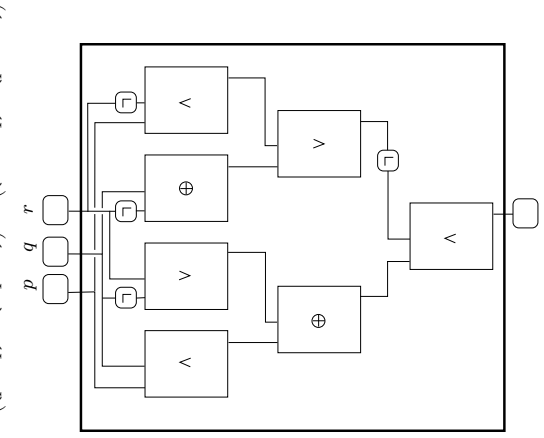
Peggy		Vic
knows HC in $\mathcal{G}$		knows $\mathcal{G}$
π at rand., $\mathcal{H} = \pi\mathcal{G}\pi^{-1}$ Commit $\mathcal{H} \to C_1, .., C_{n^2}$	$\xrightarrow{C_1, .., C_{n^2}}$	
	$\xleftarrow{c}$	$c \in_R \{0, 1\}$
$c = 0$: Decommit $\mathcal{H}$	$\xrightarrow{\pi, d_1, .., d_{n^2}}$	$\mathcal{H}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

Commitment Schemes

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

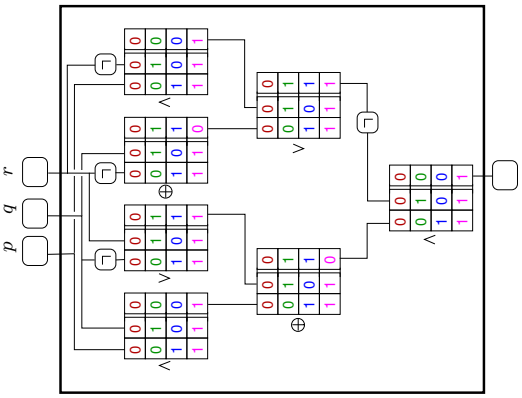
Boolean Circuit for Ψ

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

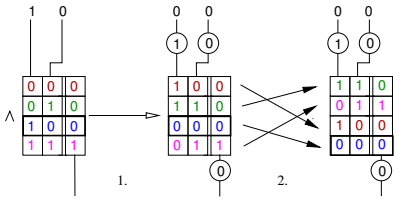


Boolean Circuit for Ψ

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



How to Scramble the Truth Tables



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

Scrambled Boolean Circuit for Ψ