Cryptographic Protocols

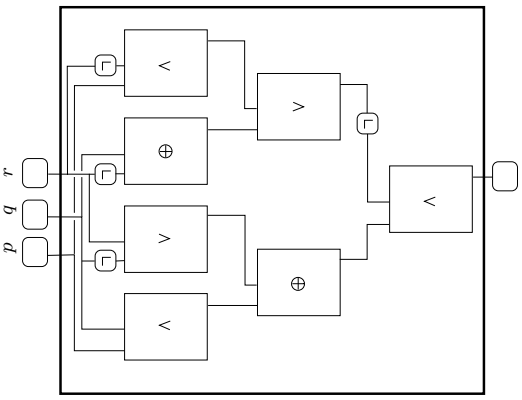
Spring 2021

Part 6

						4		
2					1		5	
4	3		7	5		1		2
				7			6	
	5	3				2	4	
	4			1				
3		1		8	2		7	4
	2		9					5
		8						

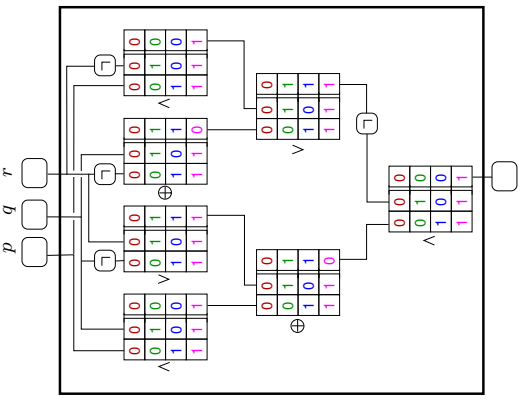
Boolean Circuit for Ψ

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



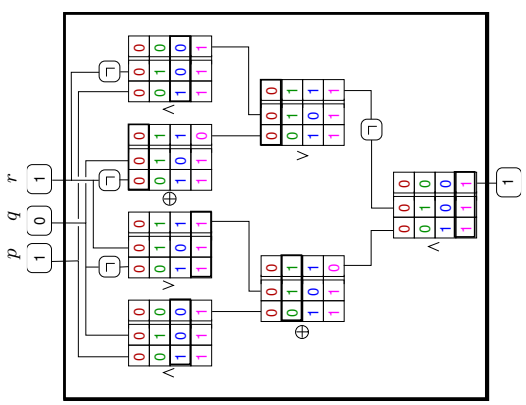
Boolean Circuit for Ψ

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

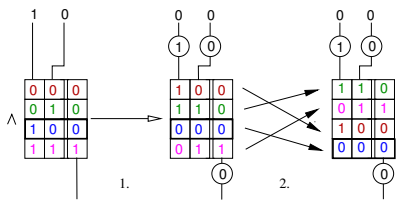


Boolean Circuit for Ψ

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

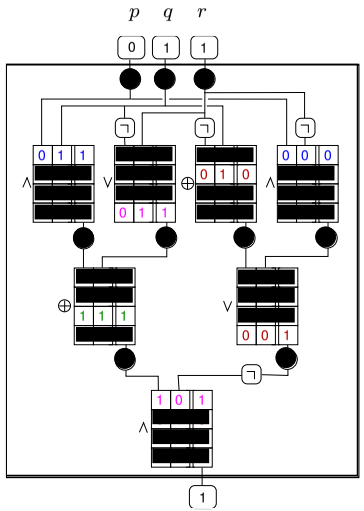


How to Scramble the Truth Tables

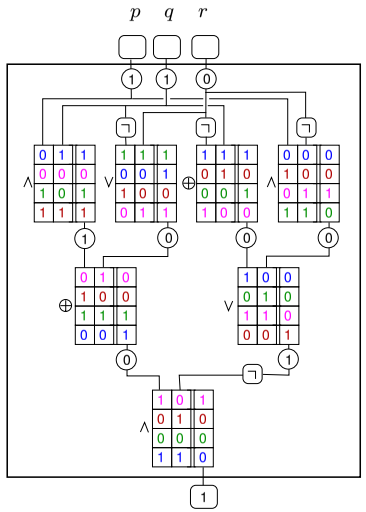


1. XOR every wire with a random bit
2. Permute the rows randomly

Scrambled Boolean Circuit for Ψ



Scrambled Boolean Circuit for Ψ



Scrambled Boolean Circuit for Ψ