Quantum computing for cryptographers II

Gates and basic circuits

Tanja Lange
idea and design by Daniel J. Bernstein

Eindhoven University of Technology

SAC – Post-quantum cryptography

NOT gates

NOT_0 gate on 3 qubits:
$(3, 1, 4, 1, 5, 9, 2, 6) \mapsto$
$(1, 3, 1, 4, 9, 5, 6, 2)$.

NOT gates

NOT_0 gate on 3 qubits:
$(3, 1, 4, 1, 5, 9, 2, 6) \mapsto$
$(1, 3, 1, 4, 9, 5, 6, 2)$.

NOT_0 gate on 4 qubits:
$(3,1,4,1,5,9,2,6,5,3,5,8,9,7,9,3) \mapsto$
$(1,3,1,4,9,5,6,2,3,5,8,5,7,9,3,9)$.

NOT gates

NOT_0 gate on 3 qubits:
$(3, 1, 4, 1, 5, 9, 2, 6) \mapsto$
$(1, 3, 1, 4, 9, 5, 6, 2)$.

NOT_0 gate on 4 qubits:
$(3,1,4,1,5,9,2,6,5,3,5,8,9,7,9,3) \mapsto$
$(1,3,1,4,9,5,6,2,3,5,8,5,7,9,3,9)$.

NOT_1 gate on 3 qubits:
$(3, 1, 4, 1, 5, 9, 2, 6) \mapsto$
$(4, 1, 3, 1, 2, 6, 5, 9)$.

NOT gates

NOT_0 gate on 3 qubits:
$(3, 1, 4, 1, 5, 9, 2, 6) \mapsto$
$(1, 3, 1, 4, 9, 5, 6, 2)$.

NOT_0 gate on 4 qubits:
$(3,1,4,1,5,9,2,6,5,3,5,8,9,7,9,3) \mapsto$
$(1,3,1,4,9,5,6,2,3,5,8,5,7,9,3,9)$.

NOT_1 gate on 3 qubits:
$(3, 1, 4, 1, 5, 9, 2, 6) \mapsto$
$(4, 1, 3, 1, 2, 6, 5, 9)$.

NOT_2 gate on 3 qubits:
$(3, 1, 4, 1, 5, 9, 2, 6) \mapsto$
$(5, 9, 2, 6, 3, 1, 4, 1)$.

NOT gates

NOT_0 gate on 3 qubits:
$(3, 1, 4, 1, 5, 9, 2, 6) \mapsto$
$(1, 3, 1, 4, 9, 5, 6, 2)$.

NOT_0 gate on 4 qubits:
$(3,1,4,1,5,9,2,6,5,3,5,8,9,7,9,3) \mapsto$
$(1,3,1,4,9,5,6,2,3,5,8,5,7,9,3,9)$.

NOT_1 gate on 3 qubits:
$(3, 1, 4, 1, 5, 9, 2, 6) \mapsto$
$(4, 1, 3, 1, 2, 6, 5, 9)$.

NOT_2 gate on 3 qubits:
$(3, 1, 4, 1, 5, 9, 2, 6) \mapsto$
$(5, 9, 2, 6, 3, 1, 4, 1)$.

state	measurement
$(1, 0, 0, 0, 0, 0, 0, 0)$	000
$(0, 1, 0, 0, 0, 0, 0, 0)$	001
$(0, 0, 1, 0, 0, 0, 0, 0)$	010
$(0, 0, 0, 1, 0, 0, 0, 0)$	011
$(0, 0, 0, 0, 1, 0, 0, 0)$	100
$(0, 0, 0, 0, 0, 1, 0, 0)$	101
$(0, 0, 0, 0, 0, 0, 1, 0)$	110
$(0, 0, 0, 0, 0, 0, 0, 1)$	111

Operation on quantum state: NOT_0, swapping pairs.
Operation after measurement: flipping bit 0 of result.
Flip: output is not input.

NOT gates

NOT_0 gate on 3 qubits:
$(3,1,4,1,5,9,2,6) \mapsto$
$(1,3,1,4,9,5,6,2)$.

NOT_0 gate on 4 qubits:
$(3,1,4,1,5,9,2,6,5,3,5,8,9,7,9,3) \mapsto$
$(1,3,1,4,9,5,6,2,3,5,8,5,7,9,3,9)$.

NOT_1 gate on 3 qubits:
$(3,1,4,1,5,9,2,6) \mapsto$
$(4,1,3,1,2,6,5,9)$.

NOT_2 gate on 3 qubits:
$(3,1,4,1,5,9,2,6) \mapsto$
$(5,9,2,6,3,1,4,1)$.

state	measurement
$(1,0,0,0,0,0,0,0)$	000
$(0,1,0,0,0,0,0,0)$	001
$(0,0,1,0,0,0,0,0)$	010
$(0,0,0,1,0,0,0,0)$	011
$(0,0,0,0,1,0,0,0)$	100
$(0,0,0,0,0,1,0,0)$	101
$(0,0,0,0,0,0,1,0)$	110
$(0,0,0,0,0,0,0,1)$	111

Operation on quantum state: NOT_0, swapping pairs.
Operation after measurement: flipping bit 0 of result.
Flip: output is not input.

This slide shows the effect of NOT on our representation. This way we can simulate quantum computers to see whether algorithms work.

Controlled-NOT (CNOT) gates

e.g. C_1NOT_0:
$(3, 1, 4, 1, 5, 9, 2, 6) \mapsto$
$(3, 1, 1, 4, 5, 9, 6, 2)$.

Controlled-NOT (CNOT) gates

e.g. C_1NOT_0:
$(3, 1, 4, 1, 5, 9, 2, 6) \mapsto$
$(3, 1, 1, 4, 5, 9, 6, 2)$.

Operation after measurement:
flipping bit 0 *if* bit 1 is set; i.e.,
$(q_2, q_1, q_0) \mapsto (q_2, q_1, q_0 \oplus q_1)$.

Controlled-NOT (CNOT) gates

e.g. C_1NOT_0:
$(3,1,4,1,5,9,2,6) \mapsto$
$(3,1,1,4,5,9,6,2)$.

Operation after measurement:
flipping bit 0 *if* bit 1 is set; i.e.,
$(q_2,q_1,q_0) \mapsto (q_2,q_1,q_0 \oplus q_1)$.

e.g. C_2NOT_0:
$(3,1,4,1,5,9,2,6) \mapsto$
$(3,1,4,1,9,5,6,2)$.

Operation after measurement:
flipping bit 0 *if* bit 2 is set; i.e.,
$(q_2,q_1,q_0) \mapsto (q_2,q_1,q_0 \oplus q_2)$.

Controlled-NOT (CNOT) gates

e.g. C_1NOT_0:
$(3, 1, 4, 1, 5, 9, 2, 6) \mapsto$
$(3, 1, 1, 4, 5, 9, 6, 2)$.

Operation after measurement:
flipping bit 0 *if* bit 1 is set; i.e.,
$(q_2, q_1, q_0) \mapsto (q_2, q_1, q_0 \oplus q_1)$.

e.g. C_2NOT_0:
$(3, 1, 4, 1, 5, 9, 2, 6) \mapsto$
$(3, 1, 4, 1, 9, 5, 6, 2)$.

Operation after measurement:
flipping bit 0 *if* bit 2 is set; i.e.,
$(q_2, q_1, q_0) \mapsto (q_2, q_1, q_0 \oplus q_2)$.

e.g. C_0NOT_2:
$(3, 1, 4, 1, 5, 9, 2, 6) \mapsto$
$(3, 9, 4, 6, 5, 1, 2, 1)$.

Operation after measurement:
flipping bit 2 *if* bit 0 is set; i.e.,
$(q_2, q_1, q_0) \mapsto (q_0 \oplus q_2, q_1, q_0)$.

CNOT is its own inverse, thus it is reversible.

Toffoli gates

Also known as CCNOT gates:
controlled-controlled-NOT gates.

e.g. $C_2C_1NOT_0$: $(3, 1, 4, 1, 5, 9, 2, 6) \mapsto (3, 1, 4, 1, 5, 9, 6, 2)$.

Toffoli gates

Also known as CCNOT gates:
controlled-controlled-NOT gates.

e.g. $C_2C_1NOT_0$: $(3,1,4,1,5,9,2,6) \mapsto (3,1,4,1,5,9,6,2)$.

Operation after measurement:
$(q_2, q_1, q_0) \mapsto (q_2, q_1, q_0 \oplus q_1 q_2)$.

Toffoli gates

Also known as CCNOT gates:
controlled-controlled-NOT gates.

e.g. $C_2C_1NOT_0$: $(3, 1, 4, 1, 5, 9, 2, 6) \mapsto (3, 1, 4, 1, 5, 9, 6, 2)$.

Operation after measurement:
$(q_2, q_1, q_0) \mapsto (q_2, q_1, q_0 \oplus q_1 q_2)$.

e.g. $C_0C_1NOT_2$: $(3, 1, 4, 1, 5, 9, 2, 6) \mapsto (3, 1, 4, 6, 5, 9, 2, 1)$.

Toffoli gates

Also known as CCNOT gates:
controlled-controlled-NOT gates.

e.g. $C_2C_1NOT_0$: $(3,1,4,1,5,9,2,6) \mapsto (3,1,4,1,5,9,6,2)$.

Operation after measurement:
$(q_2, q_1, q_0) \mapsto (q_2, q_1, q_0 \oplus q_1 q_2)$.

e.g. $C_0C_1NOT_2$: $(3,1,4,1,5,9,2,6) \mapsto (3,1,4,6,5,9,2,1)$.

Operation after measurement:
$(q_2, q_1, q_0) \mapsto (q_2 \oplus q_0 q_1, q_1, q_0)$.

Toffoli is its own inverse, thus it is reversible.

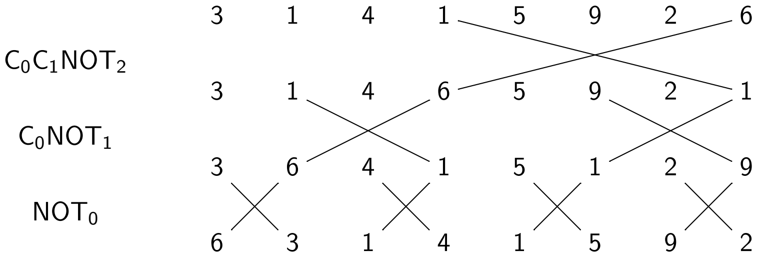
More shuffling

Combine NOT, CNOT, Toffoli to build other permutations.

More shuffling

Combine NOT, CNOT, Toffoli to build other permutations.

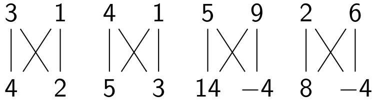
e.g. series of gates to rotate 8 positions by distance 1:



Hadamard gates

Hadamard_0:

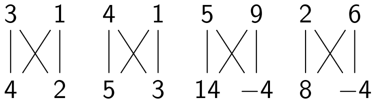
$(a, b) \mapsto (a + b, a - b)$.



Hadamard gates

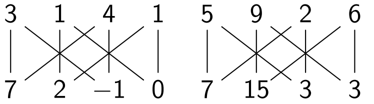
Hadamard$_0$:

$(a, b) \mapsto (a + b, a - b)$.



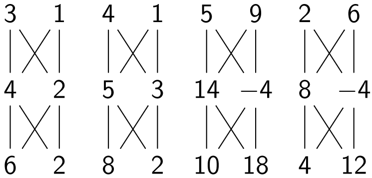
Hadamard$_1$:

$(a, b, c, d) \mapsto$
$(a + c, b + d, a - c, b - d)$.



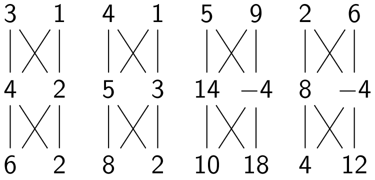
Some uses of Hadamard gates

Hadamard_0, Hadamard_0:



Some uses of Hadamard gates

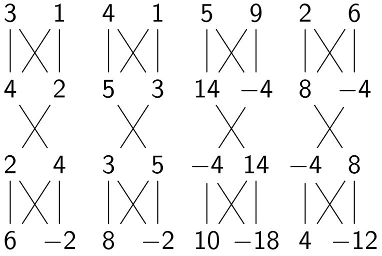
Hadamard$_0$, Hadamard$_0$:



"Multiply each amplitude by 2."

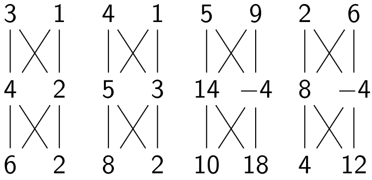
This is not physically observable.
Disappears normally in scaling.
Hadamard is self inverse.

Hadamard$_0$, NOT$_0$, Hadamard$_0$:



Some uses of Hadamard gates

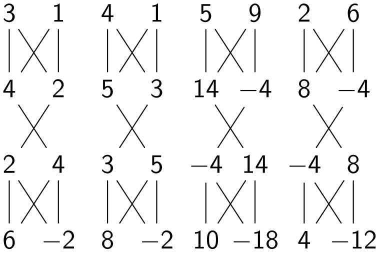
Hadamard$_0$, Hadamard$_0$:



"Multiply each amplitude by 2."

This is not physically observable.
Disappears normally in scaling.
Hadamard is self inverse.

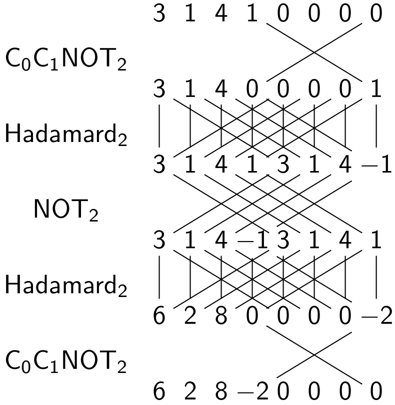
Hadamard$_0$, NOT$_0$, Hadamard$_0$:



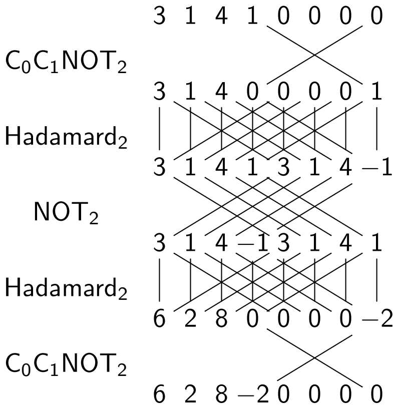
"Multiply each amplitude by 2,
Negate amplitude if q_0 is set."

No effect on measuring *now*.

Getting towards affecting measurements

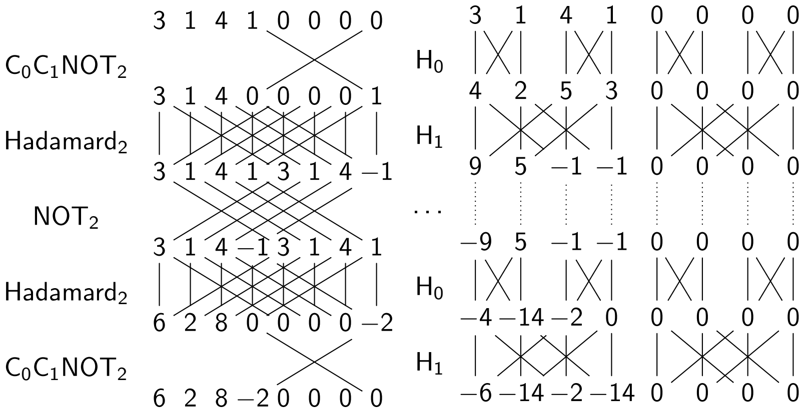


Getting towards affecting measurements



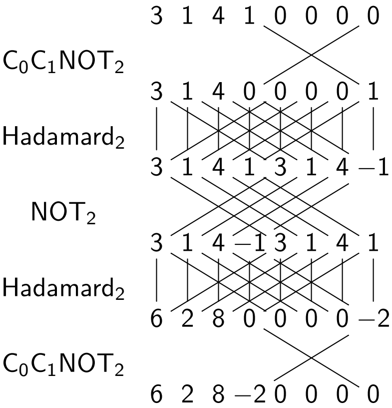
"Negate amplitude if q_0q_1 is set."
Assumes $q_2 = 0$: "ancilla" qubit.
Returns $q_2 = 0$ "clean".

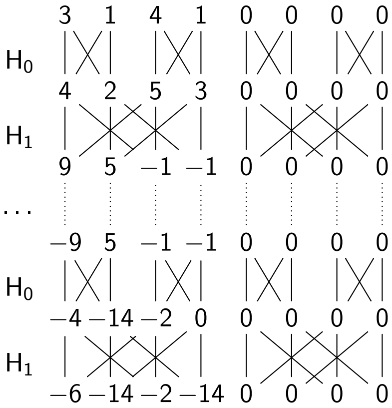
Getting towards affecting measurements



"Negate amplitude if $q_0 q_1$ is set."
Assumes $q_2 = 0$: "ancilla" qubit.
Returns $q_2 = 0$ "clean".

Getting towards affecting measurements





"Negate amplitude if $q_0 q_1$ is set."
Assumes $q_2 = 0$: "ancilla" qubit.
Returns $q_2 = 0$ "clean".

"Negate amplitude around its average."
$(3, 1, 4, 1) \mapsto (1.5, 3.5, 0.5, 3.5)$.
This affects measurements.