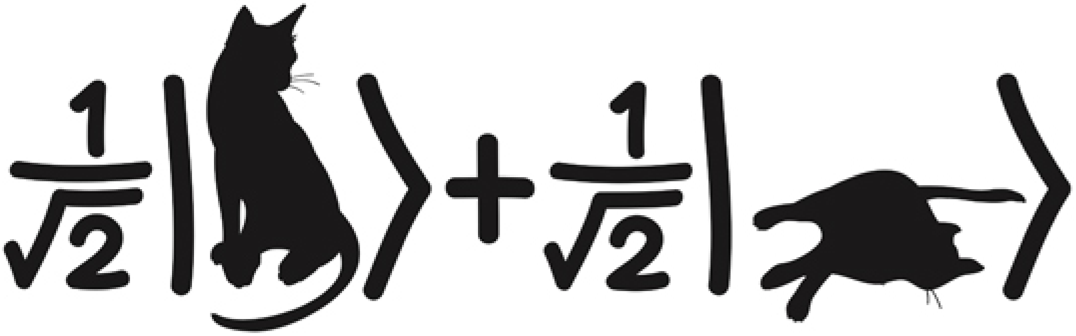
Using Simon’s algorithm



Ahmed Alharbi

13 Aug 2017

Contents

- Dirac’s Notation
- Gates and {partial}-measurement
- Simon’s Algorithm
- Three attacks
- Remarks & Further readings

Dirac's notation

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \alpha|0\rangle + \beta|1\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$$

$$|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \alpha^2 + \beta^2 = 1,\ \alpha, \beta \in \mathbb{C}$$

Dirac's notation

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad \alpha|0\rangle + \beta|1\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$$

$$|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \quad \alpha^2 + \beta^2 = 1, \ \alpha, \beta \in \mathbb{C}$$

$$\langle 0| = \begin{bmatrix} 0 & 1 \end{bmatrix} \quad \overline{\alpha}\langle 0| + \overline{\beta}\langle 1| = \begin{bmatrix} \overline{\alpha} & \overline{\beta} \end{bmatrix}$$

$$\langle 1| = \begin{bmatrix} 1 & 0 \end{bmatrix} \quad \alpha^2 + \beta^2 = 1, \ \alpha, \beta \in \mathbb{C}$$

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad \alpha|0\rangle + \beta|1\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$$

$$|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \quad \alpha^2 + \beta^2 = 1,\ \alpha, \beta \in \mathbb{C}$$

$$\langle 0| = \begin{bmatrix} 0 & 1 \end{bmatrix} \quad \overline{\alpha}\langle 0| + \overline{\beta}\langle 1| = \begin{bmatrix} \overline{\alpha} & \overline{\beta} \end{bmatrix}$$

$$\langle 1| = \begin{bmatrix} 1 & 0 \end{bmatrix} \quad \alpha^2 + \beta^2 = 1,\ \alpha, \beta \in \mathbb{C}$$

- Tensor product

$$|x\rangle \otimes |y\rangle = \begin{pmatrix} x_0 \begin{bmatrix} y_0 \\ y \end{bmatrix} \\ x_1 \begin{bmatrix} y_0 \\ y_1 \end{bmatrix} \end{pmatrix} = \begin{bmatrix} x_0 y_0 \\ x_0 y_1 \\ x_1 y_0 \\ x_1 y_1 \end{bmatrix}$$

Dirac's notation

$$|1\rangle \otimes |0\rangle \otimes |1\rangle \otimes = |101\rangle$$

Dirac's notation

$$|1\rangle \otimes |0\rangle \otimes |1\rangle \otimes = |101\rangle \equiv \begin{bmatrix} 0 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

Dirac's notation

$$|1\rangle \otimes |0\rangle \otimes |1\rangle \otimes = |101\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1_{5+1} \\ 0 \\ 0 \end{bmatrix}$$

Gates

- We are allowed to use unitary transformation *i.e*

$$U \cdot U^\dagger = \mathbb{I}$$

Gates

- We are allowed to use unitary transformation *i.e*

$$U \cdot U^\dagger = \mathbb{I}$$

- Example: Hadamard's gate
  - $H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$
  -
  - $H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$
  - in a compact format:
  - $H|x\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + (-1)^x|1\rangle\right)$
  - Or in matrix form:

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

$H|0\rangle$ $H|1\rangle$

Dirac's Notation

- Given a state $|\psi\rangle = \sum \alpha_i |i\rangle$ probability of getting $|i\rangle$ after measurement is $|\alpha_i|^2$

Gates: evaluating a function

- Suppose we have a function $f : \{0,1\}^n \to \{0,1\}^m$
- How do we construct a unitary that evaluates *f*?

Gates: evaluating a function

- Suppose we have a function $f : \{0,1\}^n \to \{0,1\}^m$
- How do we construct a unitary that evaluates *f?*
- *Solution: define* U_f *as following:*

$$U_f|x\rangle|y\rangle = |x\rangle|y \oplus x\rangle$$

- Is U_f unitary?

Gates: evaluating a function

- Suppose we have a function $f : \{0,1\}^n \rightarrow \{0,1\}^m$
- How do we construct a unitary that evaluates *f?*
- *Solution: define* U_f *as following:*

$$U_f|x\rangle|y\rangle = |x\rangle|y \oplus x\rangle$$

- Is U_f unitary?
- *Yes! Proof idea* U_f *we is a permutation matrix*

Gates

- What is the value of $H^{\bigotimes n}\left|x_n x_{n-1} \ldots x_1\right\rangle$?

- What is the value of $H^{\otimes n}|x_n x_{n-1} \ldots x_1\rangle$?

$$
\begin{aligned}
&H^{\otimes n}|x_n x_{n-1} \ldots x_1\rangle \\
&= \left(\frac{1}{\sqrt{2}}|0\rangle + (-1)^{x_n}\frac{1}{\sqrt{2}}|1\rangle\right)\left(\frac{1}{\sqrt{2}}|0\rangle + (-1)^{x_{n-1}}\frac{1}{\sqrt{2}}|1\rangle\right)\ldots\left(\frac{1}{\sqrt{2}}|0\rangle + (-1)^{x_1}\frac{1}{\sqrt{2}}|1\rangle\right) \\
&= \frac{1}{\sqrt{2^n}}\left(|0\rangle + (-1)^{x_n}|1\rangle\right)\left(|0\rangle + (-1)^{x_{n-1}}|1\rangle\right)\ldots\left(|0\rangle + (-1)^{x_1}|1\rangle\right) \\
&= \frac{1}{\sqrt{2^n}}\sum_{y\in\{0,1\}^n}(-1)^{x\cdot y}|y\rangle
\end{aligned}
$$

Gates

- *Superposition is extremely useful*

$$
\begin{aligned}
U_f H^{\otimes n} |00\ldots 0\rangle |00\ldots 0\rangle &= U_f \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle |00\ldots 0\rangle \\
&= \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} U_f |x\rangle |00\ldots 0\rangle
\end{aligned}
$$

Gates

- *Superposition is extremely useful*

$$\begin{aligned} U_f H^{\otimes n}|00\ldots0\rangle|00\ldots0\rangle &= U_f \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle|00\ldots0\rangle \\ &= \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} U_f|x\rangle|00\ldots0\rangle \\ &= \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle|f(x)\rangle \end{aligned}$$

Contents

Simon's algorithm

Simon's problem:

Let $f : \{0,1\}^n \to \{0,1\}^n \text{s.t} f(x \oplus s) = f(x)$ find s

Simon's algorithm

Simon's problem:

Let $f : \{0,1\}^n \to \{0,1\}^n \text{s.t} f(x \oplus s) = f(x)$ find s

Theorem [Simon 1995]:

There exists a quantum algorithm that returns S with high probability using O(n) queries.

Simon's algorithm: description

$$U_f H^{\otimes n} |00\ldots0\rangle|00\ldots0\rangle = U_f \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle|00\ldots0\rangle$$

Simon's algorithm: description

$$
\begin{aligned}
U_f H^{\otimes n}|00\ldots0\rangle|00\ldots0\rangle &= U_f \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle|00\ldots0\rangle \\
&= \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} U_f|x\rangle|00\ldots0\rangle \\
&= \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle|f(x)\rangle
\end{aligned}
$$

Simon's algorithm: description

$$
\begin{aligned}
U_f H^{\otimes n}|00\ldots0\rangle|00\ldots0\rangle &= U_f \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle|00\ldots0\rangle \\
&= \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} U_f|x\rangle|00\ldots0\rangle \\
&= \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle|f(x)\rangle \\
&= \frac{1}{\sqrt{2^n}} \sum_{x} \left(|x\rangle + |x\oplus s\rangle\right)|f(x)\rangle
\end{aligned}
$$

Simon's algorithm: description

$$
\begin{aligned}
U_f H^{\otimes n}|00\ldots 0\rangle|00\ldots 0\rangle &= U_f \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle|00\ldots 0\rangle \\
&= \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} U_f|x\rangle|00\ldots 0\rangle \\
&= \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle|f(x)\rangle \\
&= \frac{1}{\sqrt{2^n}} \sum_{x} \left(|x\rangle + |x\oplus s\rangle\right)|f(x)\rangle
\end{aligned}
$$

- Apply Hadamard on the first register

Simon's algorithm: description

$$H^{\otimes n} \frac{1}{\sqrt{2^n}} \sum_x \left(|x\rangle + |x \oplus s\rangle \right) |f(x)\rangle$$

$$= \frac{1}{\sqrt{2^n}} \sum_y \Big((-1)^{y \cdot x} |y\rangle + (-1)^{y \cdot (x \oplus s)} |y\rangle \Big) |f(x)\rangle$$

$$= \frac{1}{\sqrt{2^n}} \sum_y (-1)^{y \cdot x} \left(1 + (-1)^{y \cdot s} \right) |y\rangle |f(x)\rangle$$

Simon's algorithm: description

$$H^{\otimes n} \frac{1}{\sqrt{2^n}} \sum_x \left(|x\rangle + |x \oplus s\rangle\right) |f(x)\rangle$$

$$= \frac{1}{\sqrt{2^n}} \sum_y \Big((-1)^{y \cdot x} |y\rangle + (-1)^{y \cdot (x \oplus s)} |y\rangle \Big) |f(x)\rangle$$

$$= \frac{1}{\sqrt{2^n}} \sum_y (-1)^{y \cdot x} \left(1 + (-1)^{y \cdot s} \right) |y\rangle |f(x)\rangle$$

- The crucial observation is that when $y.s = 1 \ mod \ 2$ then the probability of observing $|y\rangle|f(x)\rangle$ is 0

- In other words, after measurement we will get y such that $y.s = 0 \bmod 2$
- *More precisely,*
- $y_n s_n \oplus y_{n-1} s_{n-1} \oplus \ldots \oplus y_1 s_1 = 0 \bmod 2$
- Finally, run the above procedures cn times to collect enough linear equations then use Gauss elimination to find S

Analysis of Simon

- After collection m independent equations, the probability of getting new independent equation is $\frac{2^n - 2^m}{2^n}$

Analysis of Simon

- After collection m independent equations, the probability of getting new independent equation is $\frac{2^n - 2^m}{2^n}$
- Thus, the success probability after m queries $\prod_m \frac{2^n - 2^m}{2^n} = \prod_m \left(1 - \frac{2^m}{2^n}\right)$

Analysis of Simon's

- After collection m independent equations, the probability of getting new independent equation is $\frac{2^n - 2^m}{2^n}$
-
- Thus, the success probability after m queries $\prod_{m=1}^{k} \frac{2^n - 2^m}{2^n} = \prod_{m=1}^{k} \left(1 - \frac{2^m}{2^n}\right)$
- A direct bound $\prod_{m=1}^{k} \left(1 - \frac{2^m}{2^n}\right) \geq 1 - \sum \frac{1}{2^m}$

Analysis of Simon's

- After collection m independent equations, the probability of getting new independent equation is $\frac{2^n - 2^m}{2^n}$
-
- Thus, the success probability after m queries $\prod_{m=1}^{k} \frac{2^n - 2^m}{2^n} = \prod_{m=1}^{k} \left(1 - \frac{2^m}{2^n}\right)$
- A direct bound $\prod_{m=1}^{k} \left(1 - \frac{2^m}{2^n}\right) \geq 1 - \sum \frac{1}{2^m}$
- After n-1 experiments $\prod_{m=1}^{n-1} \left(1 - \frac{2^m}{2^n}\right) \geq 1 - \sum_{m=2}^{n} \frac{1}{2^m} = \frac{1}{2} - \frac{1}{2^n}$

Analysis of Simon's

- After collection m independent equations, the probability of getting new independent equation is $\frac{2^n - 2^m}{2^n}$
-
- Thus, the success probability after m queries $\prod_{m=1}^{k} \frac{2^n - 2^m}{2^n} = \prod_{m=1}^{k} \left(1 - \frac{2^m}{2^n}\right)$
- A direct bound $\prod_{m=1}^{k} \left(1 - \frac{2^m}{2^n}\right) \geq 1 - \sum \frac{1}{2^m}$
- After n-1 experiments $\prod_{m=1}^{n-1} \left(1 - \frac{2^m}{2^n}\right) \geq 1 - \sum_{m=2}^{n} \frac{1}{2^m} = \frac{1}{2} - \frac{1}{2^n}$
- After $\mathrm{c(n}$-$1)$ experiments

$$\left(1 - \frac{1}{2}\right)^{2c} \leq e^{-c}$$

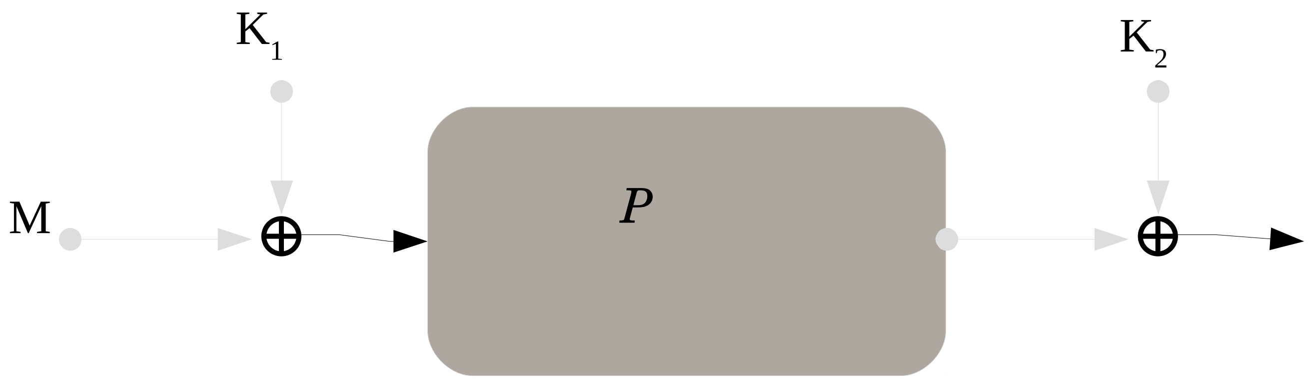
Digression: Hidden Subgroup Problem

- Simon's algorithm is a special of HSP over $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2$

Contents

Key Retrieval

Even-Mansour

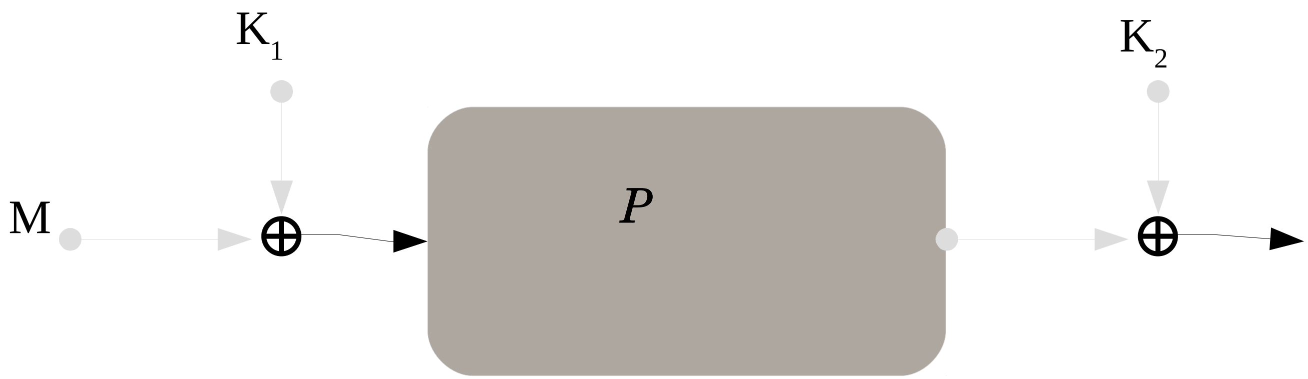


Classical Even-Mansour

$$E_{k_1,k_2} : \{0,1\}^n \rightarrow \{0,1\}^n, \text{ s.t } E_{k_1,k_2}(x) = P(x \oplus k_1) \oplus k_2$$

Classical security $O\left(2^{\frac{n}{2}}\right)$

Even-Mansour



Classical Even-Mansour

$$E_{k_1,k_2} : \{0,1\}^n \to \{0,1\}^n, \text{ s.t } E_{k_1,k_2}(x) = P(x \oplus k_1) \oplus k_2$$

Classical security $O\left(2^{\frac{n}{2}}\right)$

Quantum Even-Mansour

$$U_{E_{k_1,k_2}}|x\rangle|00\ldots0\rangle = |x\rangle|P(x \oplus k_1) \oplus k_2\rangle$$

Quantum security $O\left(n\right)$

Attack

- Define $f(x) = P(x \oplus k_1) \oplus P(x) \oplus k_2$

- Notice that:

$$f(x) = P(x \oplus k_1) \oplus P(x) \oplus k_2$$
$$f(x \oplus k_1) = P(x) \oplus P(x \oplus k_1) \oplus k_2$$

Attack

- Define $f(x) = P(x \oplus k_1) \oplus P(x) \oplus k_2$

- Notice that:

$$f(x) = P(x \oplus k_1) \oplus P(x) \oplus k_2$$
$$f(x \oplus k_1) = P(x) \oplus P(x \oplus k_1) \oplus k_2$$

- Our quantum version of f is

$$U_f = U_P U_{E_{k_1,k_2}} \text{ where } U_P|x\rangle|y\rangle = |x\rangle|P(x) \oplus y\rangle$$

Attack

- Define $f(x) = P(x \oplus k_1) \oplus P(x) \oplus k_2$

- Notice that:

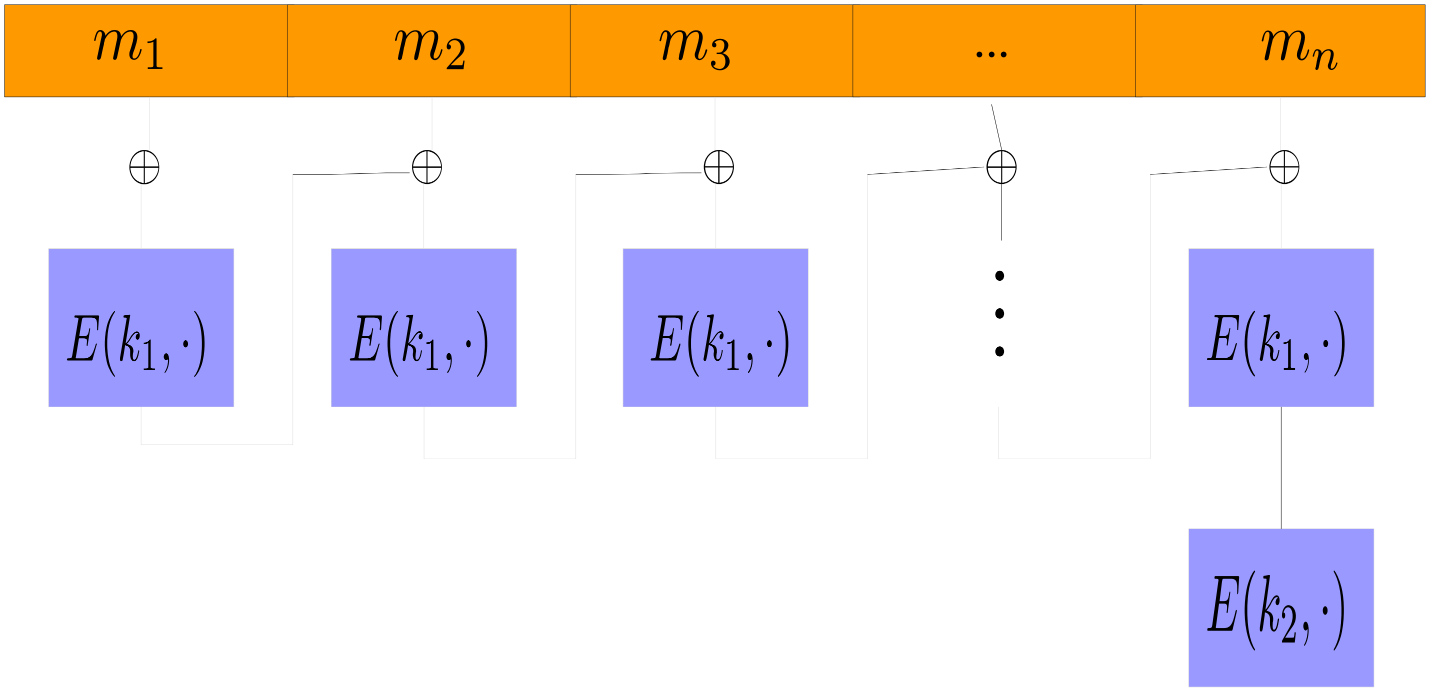
$$f(x) = P(x \oplus k_1) \oplus P(x) \oplus k_2$$
$$f(x \oplus s) = P(x) \oplus P(x \oplus k_1) \oplus \oplus k_2$$

- Our quantum version of *f* is

$$U_f = U_P U_{E_{k_1,k_2}} \text{ where } U_P|x\rangle|y\rangle = |x\rangle|P(x) \oplus y\rangle$$

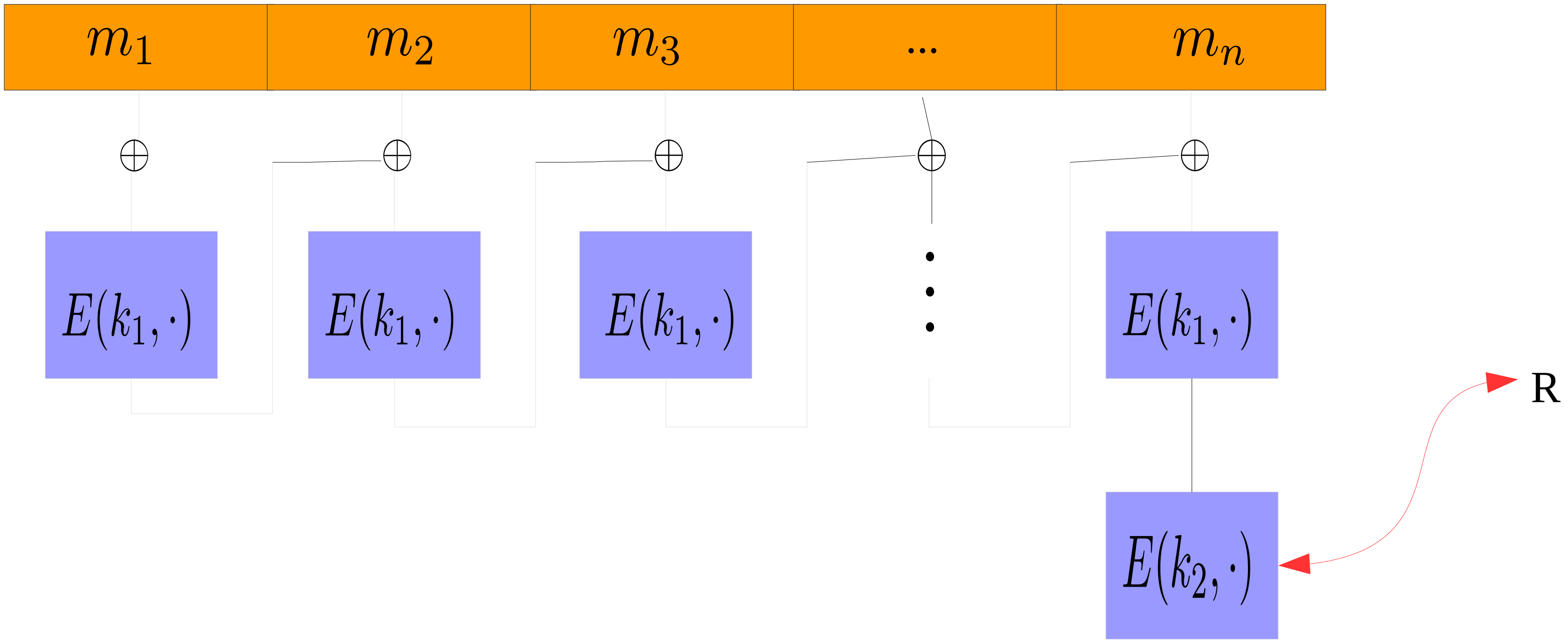
- *Notice that P is known*
- Run Simon's algorithm to get k_1 then simple xor gives us k_2

Forgery Attack



CBC-MAC

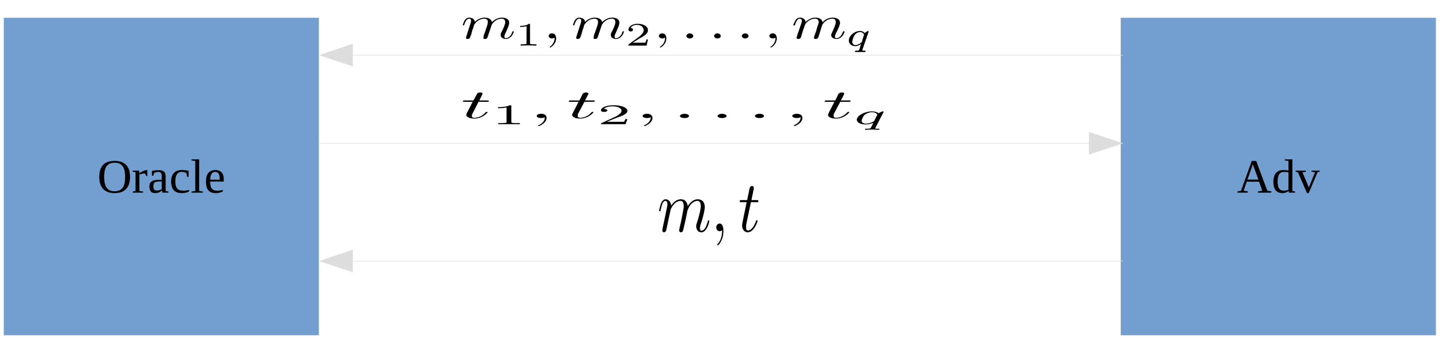
$$x_0 = 0, x_i = E_{k_1}(x_{i-1} \oplus m_i), CBCMAC(M) = E_{k_2}(x_n)$$



CBC-MAC

$$x_0 = 0, x_i = E_{k_1}(x_{i-1} \oplus m_i), CBCMAC(M) = E_{k_2 \oplus R}(x_n)$$

Security definition (informal)



- An adversary query q messages.
- After receiving q tags, if the adversary produces a message *m* with a valid tag t then the message authentication is considered insecure.

Simon's function

- For arbitrary messages m_0, m_1 define f as following:

$$f : \{0,1\} \times \{0,1\}^n \to \{0,1\}^n$$

$$\begin{aligned} CBCMAC(m_b||x) &= E_{k_1}\left(E_{k_1}\left(x \oplus E_{k_1}\left(m_b\right)\right)\right) \\ &= F\left(x \oplus E_{k_1}\left(m_b\right)\right) \end{aligned}$$

Simon's function

- For arbitrary messages m_0, m_1 define f as following:

$$f : \{0,1\} \times \{0,1\}^n \to \{0,1\}^n$$

$$\begin{aligned} CBCMAC(m_b||x) &= E_{k_1}\left(E_{k_1}\left(x \oplus E_{k_1}\left(m_b\right)\right)\right) \\ &= F\left(x \oplus E_{k_1}\left(m_b\right)\right) \end{aligned}$$

Then

$$f\left(b||x\right) = f\left(b'||x'\right) \Leftrightarrow \begin{cases} x = x' & \text{if } b = b' \\ x = x' \oplus E_{k_1}(m_0) \oplus E_{k_1}(m_1) & \text{if } b \neq b' \end{cases}$$

Simon's function

- For arbitrary messages m_0, m_1 define f as following:

$$f : \{0,1\} \times \{0,1\}^n \to \{0,1\}^n$$

$$\begin{aligned} CBCMAC(m_b||x) &= E_{k_1}\left(E_{k_1}\left(x \oplus E_{k_1}\left(m_b\right)\right)\right) \\ &= F\left(x \oplus E_{k_1}\left(m_b\right)\right) \end{aligned}$$

Then

$$f\left(b||x\right) = f\left(b'||x'\right) \Leftrightarrow \begin{cases} x = x' & \text{if } b = b' \\ x = x' \oplus E_{k_1}(m_0) \oplus E_{k_1}(m_1) & \text{if } b \neq b' \end{cases}$$

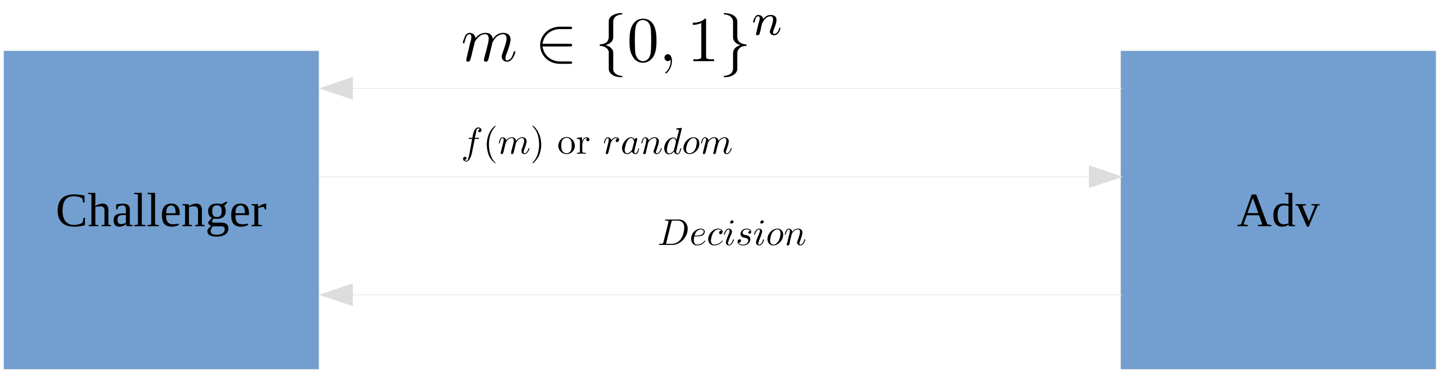
Given a tag t of x' then $x' \oplus E_{k_1}(m_0) \oplus E_{k_1}(m_1)$is a valid message of the same tag

Forgery attack

- Use Simon's algorithm which needs q message to find the period of f and save the values.
-

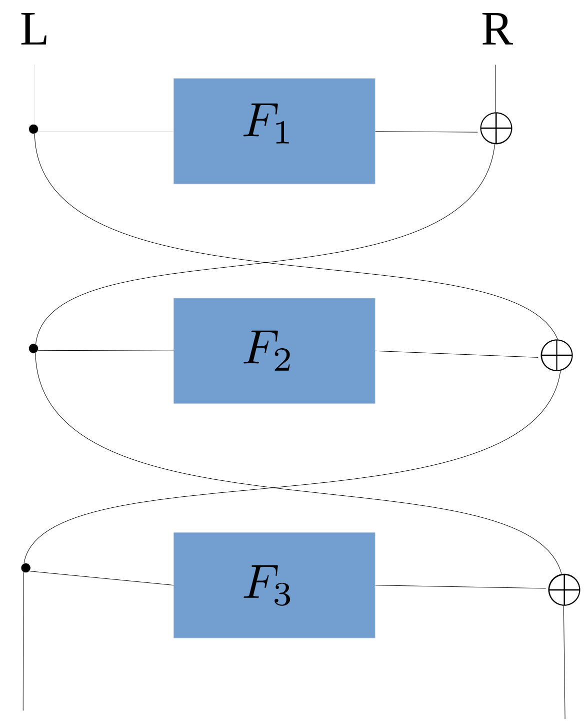
Quantum Distinguisher

Security notion



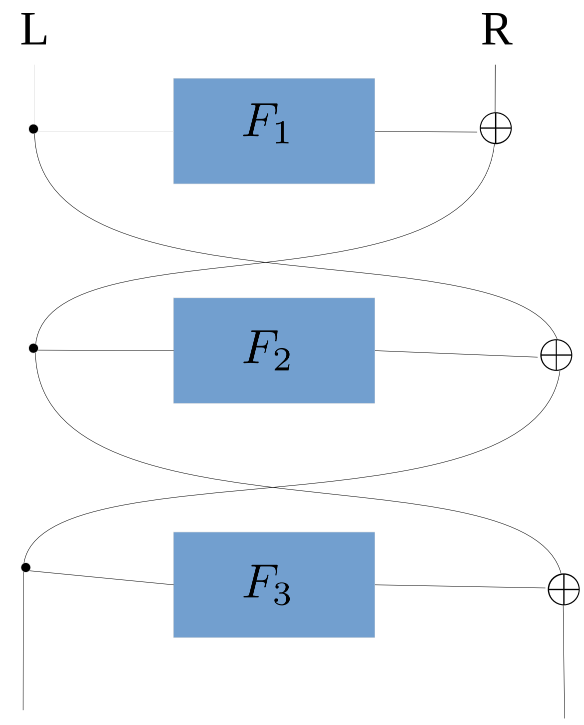
- Pseudo-random function *f* is secure if there is does not exist an efficient algorithm that can distinguish with non-negligible probability between *f's* output and a random string.

3-Feistel network



- 3-Feistel network is secure PRP given that all F_i are secure PRP

Quantum distinguisher: 3-Feistel network



- 3-Feistel network is secure PRP given that all F_i are secure Random Permutations
- By examining the right output, we see that its structure is similar to CBC-MAC (Exercise) .
- If the result of running Simon's algorithm is non-zero then it is not a random function.
- PRP is secure classically does not imply it is secure qunatumly

Contents

- Dirac’s Notation
- Gates and {partial}-measurement
- Simon’s Algorithm
- Three attacks
- Remarks & Further readings

Success probability of Simon's algorithm

- How about approximate Simon's promise?

Success probability of Simon's algorithm

- How about approximate Simon's promise?
  - Simon's algorithm works! See "Breaking Symmetric Microsystems Using Quantum Period Finding" published in Crypto 2016

Success probability of Simon’s algorithm

- How about approximate Simon’s promise?
  - Simon’s algorithm works! See “Breaking Symmetric Microsystems Using Quantum Period Finding” published in Crypto 2016
- More attacks
  - “Superposition Attacks on Cryptographic Protocols”
  - “Post-Quantum Security of the CBC, CFB, OFB, CTR, and XTS Modes of Operation”
  - “Breaking Symmetric Cryptosystems Using Quantum Period Finding”
  - “Quantum Key-Recovery on full AEZ” 8 Aug 2017

Success probability of Simon’s algorithm

- How about approximate Simon’s promise?
  - Simon’s algorithm works! See “Breaking Symmetric Microsystems Using Quantum Period Finding” published in Crypto 2016
- More attacks(Chronologically ordered:
  - “Superposition Attacks on Cryptographic Protocols”
  - “Post-Quantum Security of the CBC, CFB, OFB, CTR, and XTS Modes of Operation”
  - “Breaking Symmetric Cryptosystems Using Quantum Period Finding”
  - “Quantum Key-Recovery on full AEZ” 8 Aug 2017
- Constructing secure ciphers under superposition attacks
  - “Quantum-Secure Message Authentication Codes”
  - "Secure Signatures and Chosen Ciphertext Security in a Quantum Computing World"
  - Replace $\underbrace{\mathbb{Z}_2 \times \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2}_{n}$ with $\mathbb{Z}_n$ as proposed in:
    - “Quantum-Secure Symmetric-Key Cryptography Based on Hidden Shifts"

5.4 Perspectives

The main challenge of my ERC project QUASYModo is to redesign symmetric cryptography for the post-quantum world. The final objective is to construct and recommend symmetric primitives secure in the post-quantum world, as well as the tools needed to properly evaluate them. I will continue to work on this toolbox, and when it is ready, I will use it to: 1) analyze existing cryptosystems/primitives, and 2) design new ones for which we will gain confidence in the post-quantum world.

Some other short-term aims are: improvements on linear cryptanalysis using QFT seem possible, try to find better algorithms for solving the same problem as Kupderberg when having several parallel modular additions, providing a quantized version of improved slide attacks, and study the effect of a smaller than the key state for quantum adversaries (starting for instance quantizing sweet-32). I also plan to start working on the design of a block cipher with an internal state size of 256 bits.

From MÉMOIRE D’HABILITATION À DIRIGER DES RECHERCHES, Université Pierre et Marie Curie, Paris 6 by María Naya-Plasencia, Inria de Paris

Thank you