Term Paper

Breaking Symmetric Cryptosystems using Quantum Period Finding.

Authors: Marc Kaplan, Gaetan Leurent, Anthony Leverrier and Maria Naya-Plasencia

---

Siva Kumar
CVS 2016

Simon's problem:

Given a Boolean function $f: \{0,1\}^n \longrightarrow \{0,1\}^n$ and the promise that there exists $s \in \{0,1\}^n$ such that for any $(x,y) \in \{0,1\}^n \times \{0,1\}^n$,

$f(x) = f(y) \iff x \oplus y \in \{0, s\}$, the goal is to find s.

This problem can be ~~solved~~ Solved classically by searching for collisions.

Classical ~~Algo~~ optimal algorithm:

queries f-oracle $\Theta(2^{n/2})$ many times

Let the queries be $\{x_1, \ldots x_{2^{n/2}}$

and the ~~xx~~ corresponding responses be $f(x_1) \ldots f(x_{2^{n/2}})$

Where $x_1, \ldots, x_{2^n}$ are chosen

randomly

Then by Birthday paradox

there exists i, j s.t

$x_j \neq x_j$ and $f(x_i) = f(x_j)$

with high probability.

So by the promise, $s = x_i \oplus x_j$

Quantum algorithm (Simon's algorithm).

Note:

$$H^{\otimes n} |x\rangle = \frac{1}{\sqrt{2^n}} \sum_{s \in \{0,1\}^n} (-1)^{x \cdot s} |s\rangle$$

Step 1) Starting with $2n$-qubit state $|0\rangle|0\rangle$,

One applies Hadamard transformation $H^{\otimes n}$

to the first register to obtain the

quantum superposition.

$$\frac{1}{\sqrt{2^n}} \sum_x (-1)^{0 \cdot x} |x\rangle |y\rangle = \frac{1}{\sqrt{2^n}} \sum_x (-1)^0 |x\rangle |0\rangle$$

Step 2)

$$= \frac{1}{\sqrt{2^n}} \sum_x |x\rangle |0\rangle$$

Step 2> A quantum query to the function f maps ~~maps~~ quantum state U_f.

maps this state to $\frac{1}{\sqrt{2^n}} \sum_x |x\rangle |f(x)\rangle$.

Step 3> Measuring the second register in the computational basis yields a value $f(z)$ and collapses the first register to the state

$$\frac{1}{\sqrt{2}} \left(|z\rangle + |z \oplus s\rangle \right).$$

Step 4> Applying again the Hadamard transform $H^{\otimes n}$ to the first register gives:

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

Step 5> The vectors y such that $y \cdot s = 1$ have amplitude 0. Therefore, measuring the state in the computational basis yields a random vector y s.t $y \cdot s = 0$.

By repeating the above ~~#~~ ~~Step~~ subroutine $O(n)$ times one obtains $(n-1)$ independent vectors orthogonal to s, with high probability. And s can be recovered successfully.

In Cryptanalysis we might not be able to construct a function f which satisfies the Simon's promise perfectly.

One might not be able to obtain full rank ~~matrix~~ of system of linear equations after $O(n)$ queries.

Def:

Let

$$f : \{0,1\}^n \longrightarrow \{0,1\}^n \text{ s.t}$$

$$f(x \oplus s) = f(x) \quad \forall x, \text{ for some } s \in \{0,1\}^n$$

$$\varepsilon(f,s) = \max_{b \in \{0,1\}^n - \{0,s\}} \Pr_x [f(x) = f(x \oplus b)].$$

This $\varepsilon(f,s)$ quantifies how far function f is from satisfying the Simon's promise.

Ex:

For a random function f, $\varepsilon(f,s) = O\left(\frac{n}{2^n}\right)$

On the other hand if f is ~~Constant~~ constant

$$\varepsilon(f,s) = 1.$$

Theorem: (Simon's algorithm with approximate promise).

If $\varepsilon(f,s) \leq p_0 < 1$, then Simon's algorithm returns s with cn queries, with probability at least $1 - \left(2\left(\frac{1+p_0}{2}\right)^c\right)^n$

In particular choosing $c \geq \frac{3}{1-p_0}$

ensures that error decreases exponentially with n.

Theorem: (Simon's algorithm without promise).

After cn steps of Simon's algorithm, if t is orthogonal to all vectors y_i returned by each step of the algorithm, then $\Pr[f(n \oplus t) = f(t)] \geq p_0$ with probability at least $1 - \left(2\left(\frac{1+p_0}{2}\right)^c\right)^n$.

Attack Strategy:

1) Start with an encryption oracle

$$E_k : \{0,1\}^n \longrightarrow \{0,1\}^n$$

2) Then exhibit a new function f that satisfies Simon's promise with two additional properties:

(a) Superposition of queries are allowed to quantum oracle access to E_k.

(b) Knowledge of the string s, should be sufficient to break the cipher.

3) Fix a pair of messages x_0, x_1 & $x_0 \neq x_1$, and make $f = E_k(x_0) \oplus E_k(x_1)$.

The input of f will be injected into the state with difference s, so that $f(x) = f(x \oplus s)$.

In this paper f is of the form either $f^{(1)}$ or $f^{(2)}$.

$$f^{(1)}: x \longmapsto P\left(\tilde{E}(x) \oplus \tilde{E}(x \oplus s)\right)$$

$$f^{(2)}: bx \longmapsto \begin{cases} \tilde{E}(x) & \text{if } b=0 \\ \tilde{E}(x \oplus s) & \text{if } b=1. \end{cases}$$

Three round Feistel scheme:

The Feistel scheme is a classical construction to build a random permutation out of random function & random permutation.

Luby and Rackoff proved that three round Feistel scheme is secure as pseudo-random permutation.

Pseudo random function: It is a family of keyed function.

$$F: \{0,1\}^k \times \{0,1\}^m \longrightarrow \{0,1\}^n.$$

F is family of keyed function.

We say that F is a PRF

if. for all adversaries A, if A is not able to ~~to~~ differentiate between F_k and U in poly time.

where $U : \{0,1\}^m \longrightarrow \{0,1\}^n$ is a random function.

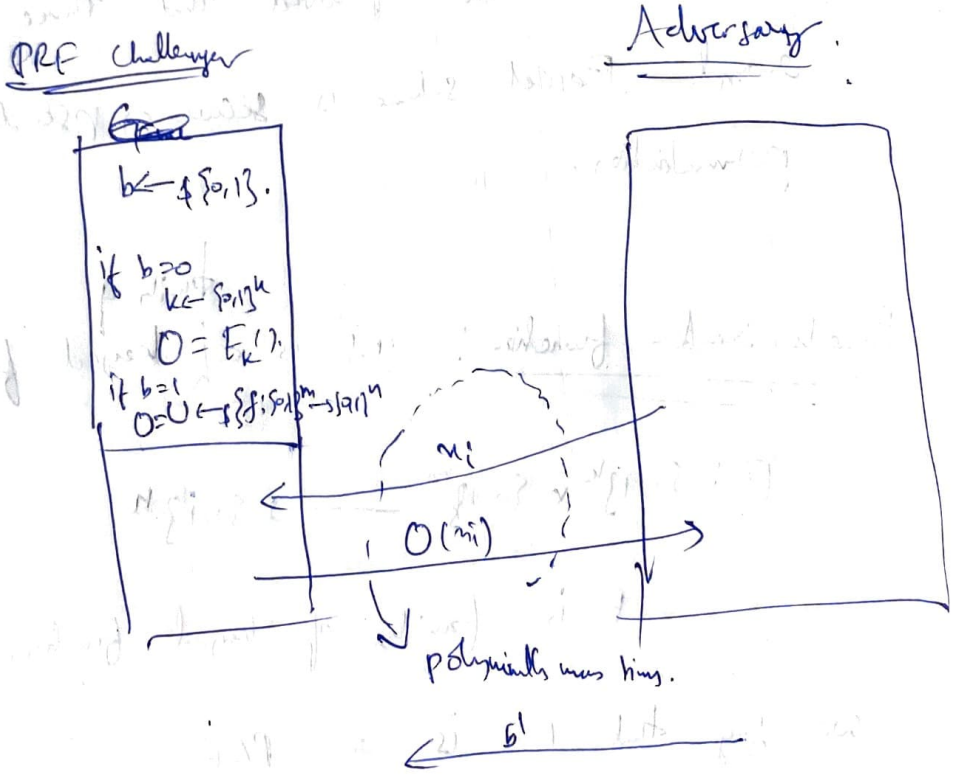
i.e,

~~PRF adv [A]~~

$$PRF\ adv[A, F] = 2\left|Pr[A \text{ succeeds}] - \frac{1}{2}\right| < \varepsilon(n).$$

negligible.

PRF game:



A succeeds if $b' = b$.

Now we will construct a polynomial distinguisher using Simon's algorithm in Quantum setup.

Let R_1, R_L & R_R be any random functions.

$$E : \{0,1\}^k \times \{0,1\}^n \times \{0,1\}^n \longrightarrow \{0,1\}^n \times \{0,1\}^n.$$

$$E(x_L, x_R) = (y_L, y_R).$$

$$(u_0, v_0) = (x_L, x_R),$$

$$(u_i, v_i) = (v_{i-1} \oplus R_i(u_{i-1}), u_{i-1}) \quad \forall\ i = 1, 2, 3,$$

$$(y_L, y_R) = (u_3, v_3).$$

Let $\alpha_0 \neq \alpha_1$,

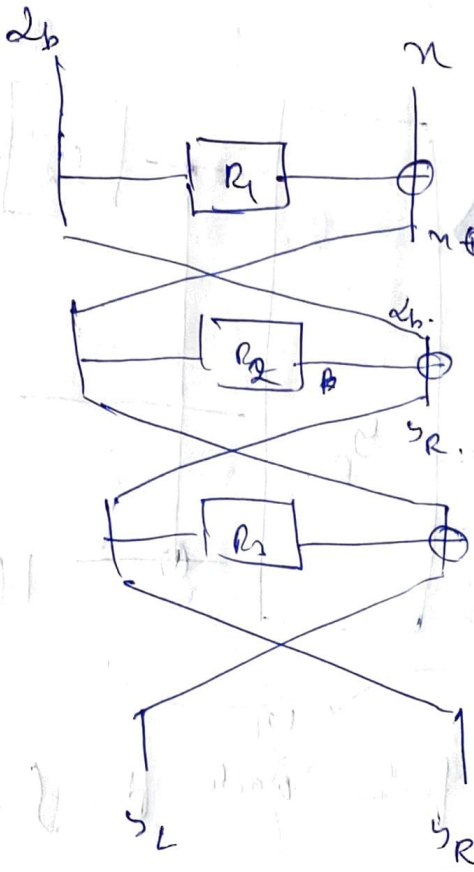
Let U_α be a quantum gate.

Another implicit assumption is that adversary can get both y_R (the right part of the cipher text)

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

$$f(b, x) = x_b \oplus y_R$$

since, $E_K(y_L, y_R) = E_K(x_b, x)$.



$\equiv \quad y_R \oplus x_b = R_2\left(x \oplus R_1(x_b)\right)$

$$\therefore \quad f(b, x) = x_b \oplus y_R = R_2(x \oplus R_1(x_b))$$

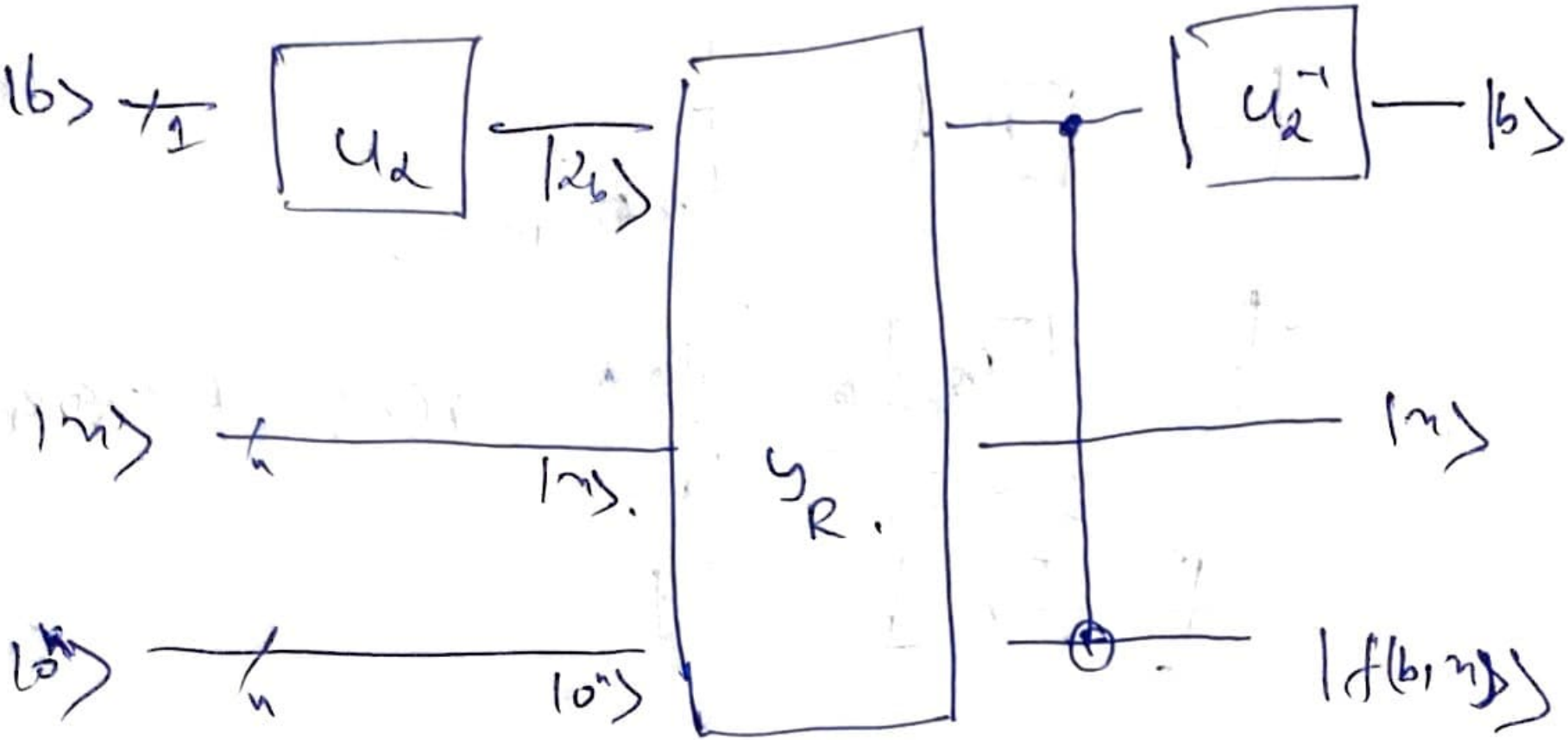
Let $\quad \mathcal{I} = \mathcal{I} \,||\, R_1(x_0) \oplus R_1(x_1)$

$$f(1 \oplus b, x \oplus R_1(x_0) + R_1(x_1)) =$$

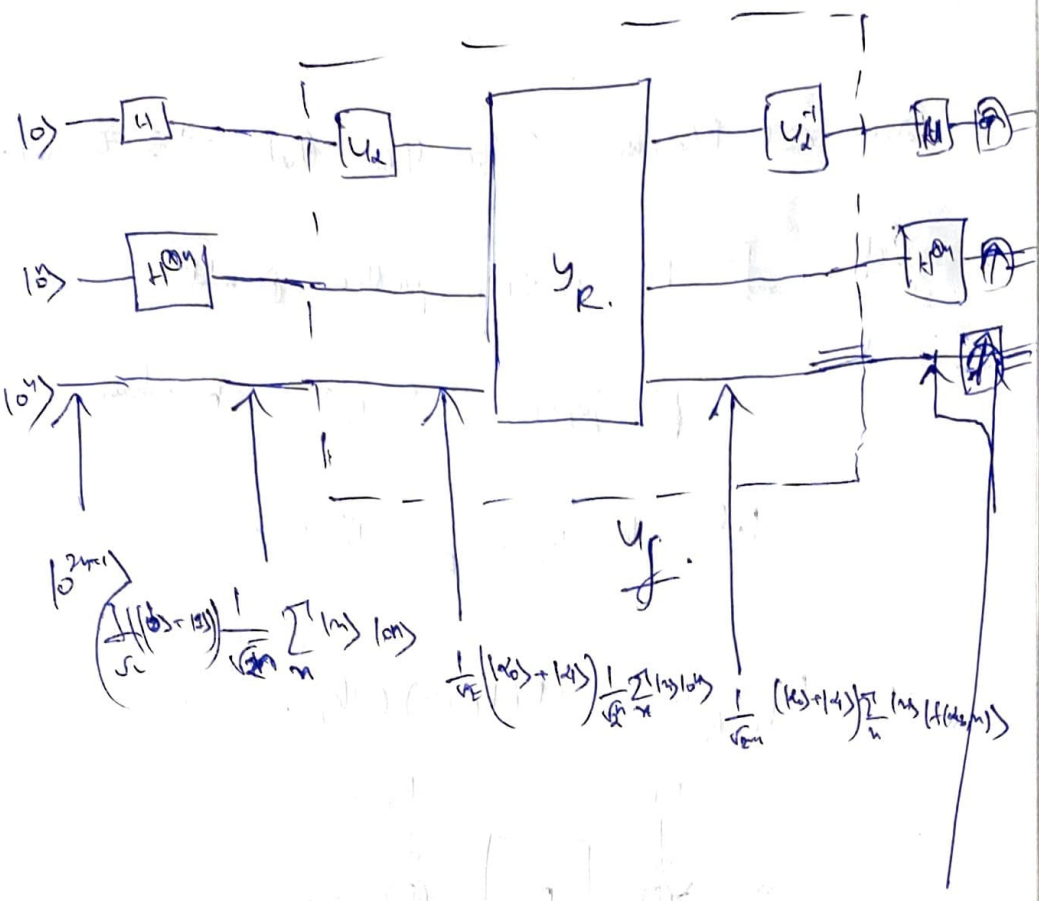
$$R_2(x + R_1(x_0) \oplus R_1(x_1) \oplus R_1(x_{b \oplus 1}))$$

$$= \begin{cases} R_2(x \oplus R_1(x_0)) & \text{if } b=0 \\ R_2(x \oplus R_1(x_1)) & \text{if } b=1 \end{cases}$$

$$\therefore \quad f(1 \oplus b, x \oplus R_1(x_0) \oplus R_1(x_1)) = f(b, x).$$



Simon's function oracle for f.



If $\mathcal{E} = \mathcal{E}_U$

then f will have a shift $s = R_1(k_0) \oplus R_1(k_1)$ with high probability.

if $\mathcal{E} = U$, Random function

then $s = 0^{n+1}$.

So if we measure and in the circuit $O(n)$ times and find

$s = 0^{n-1}$, then, $\mathcal{E} = U$

else $\mathcal{E} = \mathcal{E}_U$ with probability.

One-Round Even-Mansour Cipher key recovery attack

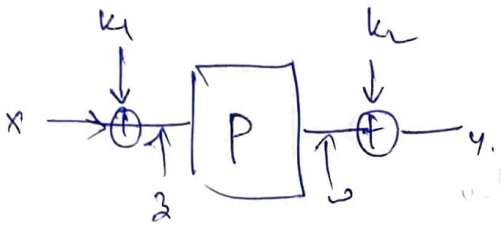
~~Even and Mansour have shown that this construction is~~

Let P be a some public permutation

$$P: \{0,1\}^n \to \{0,1\}^n \quad \text{bijection.}$$

Let $k_1, k_2 \xleftarrow{\$} \{0,1\}^n$.

$$E_{k_1,k_2}(x) = P(k_1 \oplus x) \oplus k_2.$$



Even and Mansour have shown that the above construction is safe in the random oracle model upto $2^{n/2}$ queries, ~~Since~~ again security proof follows from birthdays paradox.

Classical attack:

There are Encryption Oracle queries.

$$(x_i, y_i) \qquad E_{k_1,k_2}(x_i) = y_i$$

and public permutation queries carried by adversary the

$P(x_i) =$

$$\text{Table} = \left(E_{k_1,k_2}(x_i) \oplus P(x_i), \; i \right)$$

Sort the table over first coordinate

$$1 \le i \le 2^{n/2}$$

By birthday paradox, there will be collisions.

Let there are x_j such pairs.

$$E_{k_1,k_2}(x_{l_i}) \oplus P(x_{l_i}) = E_{k_1,k_2}(x_{l_j}) \oplus P(x_{l_j})$$

$$\Rightarrow \quad k_1^{(l_i,j)} = x_{l_i} \oplus x_{l_j}$$

$$k_2^{(l_i,j)} = E_{k_1,k_2}(x_{l_i}) \oplus P(x_{l_j}).$$

The above discussion follows from next.

If $x \oplus x^* = k_1$

then $E(x) = P(x \oplus k_1) \oplus k_2$

$$= P(x^*) \oplus k_2$$

$$E(x^*) = P(x) \oplus k_2.$$

$$E(x) \oplus E(x^*) = P(x) \oplus P(x^*).$$

$\Rightarrow$

$\Rightarrow \quad E(x) \oplus P(x) = E(x') \oplus P(x')$.

So verify for each of the possible

$k_1^{(i,j)}$ & $k_2^{(i,j)}$

So the query complexity of this attack is

$O(2^{n/2})$.

Now we will construct a ~~Quantum~~ attack. in quantum setup. for key recovery. for one round Even-Mansour cipher.

$f : \{0,1\}^n \longrightarrow \{0,1\}^n$.

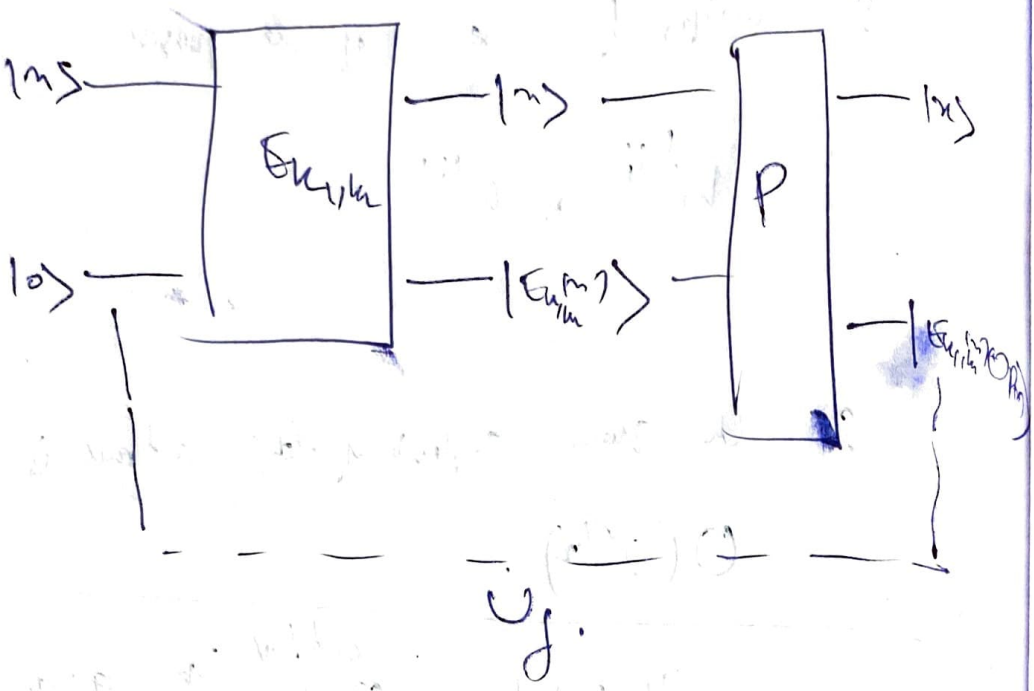
$f(x) = E_{k_1,k_2}(x) \oplus P(x)$

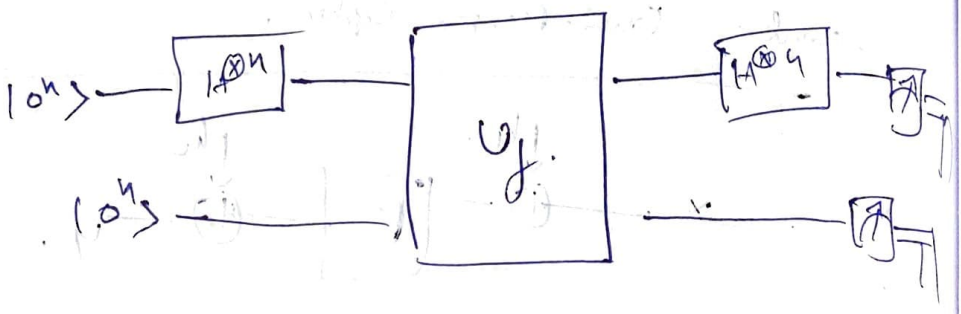
$= P(x \oplus k_1) \oplus k_2 \oplus P(x)$

Note:

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

Shor's function





$O(n)$ measurements, we will retrieve

k with high probability.

Once k_2 has been recovered.

$P(k_1)$ is ~~known~~ known to us as P is public.

$$E_{k_1,k_2}(0) = P(k_1) \oplus k_2$$

$$\Rightarrow k_2 = E_{k_1,k_2}(0) \oplus P(k_1).$$

Thus the complete keys k_1, k_2 has been recovered in $O(q)$ queries.

References:

1) Breaking Symmetric Cryptosystems using Quantum Period finding
Marc Kaplan, Gaetan Leurent et al.

2) On security Notions for Encryption in Quantum world
Celine Chevalier, Ehsan Ebrahimi et al.

3) Minimalism in Cryptography: The Even-Mansour scheme revisited.
Orr Dunkelman, Nathan Keller & Adi Shamir.