Indian Institute of Science, Bengaluru

Paper Summary: Grover Meets Simon – Quantumly Attacking the FX-construction

Name:	Rajiv Sangle
Institute email:	rajivsangle@iisc.ac.in
Course Code:	E0 213
Course Title:	Quantum-Safe Cryptography
Course Instructors:	Dr. Sanjit Chatterjee, Dr. Tapas Pandit

1 Motivation and Preliminaries to Quantum Cryptanalysis

Key-whitening or combining the message with portions of the key is one of the widely used techniques to increase the effective key length and to enhance the security of a cipher. With the discovery of Grover's algorithm, that provides quadratic speedup to brute-force search, the effective key length is reduced by half against a quantum adversary. A simple by-pass to this Grover's attack is to double the key length.
Not only does this increase the computational resources but as we shall, such a design is not secure against a quantum- CPA (chosen-plaintext attack). The authors in this paper show that a clever combination of Grover's algorithm and Simon's algorithm in parallel can break a block cipher that is naively protected by whitening keys with the same time complexity required by just Grover's algorithm to break the underlying cipher.
The quantum adversary in this case, however, requires additional space resources. Therefore, whitening keys do not provide any additional security guarantees to protect the block cipher against a quantum adversary.

1.1 Grover's Algorithm to break Block Cipher

For any generic block cipher with E_k as the encryption function (Enc):

$$\text{Enc}(m) = E_k(m)$$

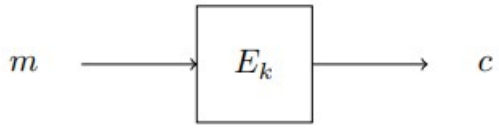


Figure 1.1 Block Cipher

Given a pair (m, c) of a chosen-plaintext and corresponding cipher-text respectively, the problem of finding k can be achieved by constructing a Grover Oracle such that:

$$f(x) = 1 \ ; \ E_x(m) = c \text{ and } f(x) = 0 : \text{ otherwise}$$

Thus a quantum adversary with a chosen-plaintext and corresponding cipher-text pair (m, c), and access to the above Grover's Oracle can break the cipher and recover the key k in $O^{n/2}$ time, where n is the length of the key k.

1.2 Simon's Algorithm to break Even-Mansour Cipher

The Even-Mansour (EM) construction makes use of two secret whitening keys (k_1, k_2), and a public permutation P. The encryption function (Enc) is therefore:

$$\text{Enc}(m) = P(m \oplus k_1) \oplus k_2$$

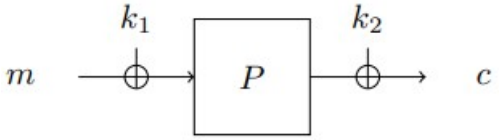


Figure 1.2 Even-Mansour construction

Now the function defined as, $f(x) := \text{Enc}(m) + P(m \oplus x)$ is periodic in k_1.
Therefore, the EM cipher can broken by extracting the secret key k_1 in $O(n)$ time using Simon's algorithm on the function $f(x)$, and then evaluating $k_2 = \text{Enc}(m) + P(m \oplus k_1)$ once k_1 is known.

2 The FX-construction

The FX-scheme is a combination of Block Cipher and Even-Mansour Cipher. It aims to combine the security of the whitening keys (k_1, k_2) by replacing the public permutation P with a secure block cipher E_{k_0}:

$$\text{Enc}(m) = E_{k_0}(m \oplus k_1) + k_2$$

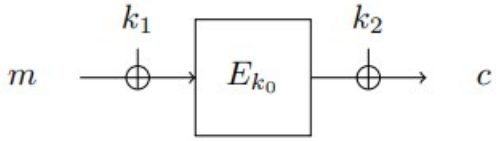


Figure 2.1 FX scheme

For the rest of the discussion henceforth, m is the size of the key k_0, and n is the size of the keys k_1 and k_2.

The 3-tuple $(k_0, k_1, k_2) \in {F_2}^{m+2n}$ thus defines the key space.

The overhead of replacing the public permutation P with E_{k_0} does not significantly affect the efficiency from an implementation point of view.

Classically if an adversary is given oracle access to both the FX encryption scheme and the block cipher E_{k_0} within it as well, then with q number of queries, the success probability of the adversary is bounded by $\frac{q^2}{2^{m+n}}$.

2.1 How to Quantumly attack the FX-construction?

The authors of this paper showed that whitening keys (k_1, k_2) used to further strengthen a block cipher E_{k_0} do not provide an additional security against a quantum adversary under the chosen plaintext attack (CPA).

They showed that the FX scheme can be broken in $O(m+n).2^{m/2}$ quantum steps which is of the same order required to break the underlying block cipher without whitening keys.
However, additional space resources are required as we shall discuss later.

As shown earlier in Section 1.1 and Section 1.2, a block cipher and an Even-Mansour cipher can broken by an quantum chosen plaintext attack (CPA) using the Grover's Algorithm and Simon's Algorithm respectively. Therefore, at a high level, it seems logical that the FX construction which is formed by combining both the block cipher and the Even-Mansour schemes can be attacked by combining Grover's Algorithm and Simon's algorithm.

Though it is not straightforward to simply combine the two algorithms because how both these algorithms work is different in the way in which they extract information.

Grover's algorithm which is a particular instance of the general Amplitude Amplification Algorithm inherently requires all the information in superposition at the same time, and with each iteration, the wave function amplitude is redistributed within the superposition states.
The measurement on this superposition is done only after the optimal number of iterations have been achieved thus measuring the target state highly probable.

Simon's algorithm, on the other hand, requires $O(n)$ measurements to be performed at the end of each iteration.
These measurement results then need to be collected and solved as a system of linear equations, the solution of which is the desired secret period or the secret key in our case.

This technical conflict in the mode of operation of these two algorithms can be solved by running parallel instances of Simon's algorithm on different quantum circuits.
This is where Simon's algorithm is made $O(1)$ in time using parallel instances, but it incurs an additional space complexity ideally of $O(n)$. For practical implementation, the space resources required could be more than $O(n)$ and we keep this in mind during further analysis.

Moreover, we make use of the 'deferred measurement principle' of quantum computation and postpone the measurements to the very end of the entire iteration in the Simon algorithm.

2.2 Quantumly breaking the FX-construction

The encryption function (Enc) of the FX scheme is $\text{Enc}(x) = E_{k_0}(x + k_1) + k_2$.

Now let us consider the following function $f(k, x)$ defined as follows:

$$f(k, x) := \text{Enc(x)} + E_k(x) = E_{k_0}(x + k_1) + k_2 + E_k(x)$$

It is easy to easy that for the correct key ($k = k_0$), $f(k, x) = f(k, x + k_1)$ for all values of x.
Therefore, $f(k_0, x)$ has a period k_1 in the argument x.

However, for $k \neq k_0$ it is highly unlikely that

$$f(k, x) = f(k, x + k_1^{'}) \text{ or } E_{k_0}(x + k_1) + E_k(x) = E_{k_0}(x + k_1 + k_1^{'}) + E_k(x + k_1^{'}).$$

Therefore, $f(k, x)$ is not periodic in x with high probability for $k \neq k_0$.

Using these observations, at a high level we can observe that the way to break the FX scheme is to test for the periodicity (using Simon's algorithm) of every $f(k, x)$ by defining a Grover search over $k \in {F_2}^m$.
Hence, the entire parallel Simon Algorithm will be encoded as the Grover Oracle to check for which values of k, $f(k, x)$ is periodic in x.

Thus the outer Grover loop over $k \in {F_2}^m$ will run for around $2^{m/2}$, and the Simon inner loop encoded in the Grover Oracle will have linear polynomial time complexity that not exactly $O(n)$ but greater than that as we shall see subsequently.

Before going any further, it is worthwhile to briefly mention the Amplitude Amplification Algorithm which is a generalization of the original Grover's Algorithm.
This result was established by **Brassard, Hoyer, Mosca and Tapp**:

Theorem 1 (Brassard, Hoyer, Mosca and Tapp). *Let $\mathcal{A}$ be any quantum algorithm on q qubits that uses no measurement. Let $\mathcal{B} : \mathbb{F}_2^q \to \{0, 1\}$ be a function that classifies outcomes of $\mathcal{A}$ as good or bad. Let $p > 0$ be the initial success probability that a measurement of $\mathcal{A}|\mathbf{0}\rangle$ is good. Set $k = \lceil \frac{\pi}{4\theta} \rceil$, where θ is defined via $\sin^2(\theta) = p$. Moreover, define the unitary operator $Q = -\mathcal{A}S_0\mathcal{A}^{-1}S_{\mathcal{B}}$, where the operator $S_{\mathcal{B}}$ changes the sign of the good state*

$$|x\rangle \mapsto \begin{cases} -|x\rangle & \text{if } \mathcal{B}(x) = 1 \\ |x\rangle & \text{if } \mathcal{B}(x) = 0 \end{cases},$$

while S_0 changes the sign of the amplitude only for the zero state $|\mathbf{0}\rangle$.

Then after the computation of $Q^k\mathcal{A}|\mathbf{0}\rangle$, a measurement yields good with probability at least $\max\{1 - p, p\}$.

3 The actual Grover + Simon attack

In the FX-construction, $f_{k_0,k_1,k_2}(x)$ is Enc(x), and $g(k,x)$ is $E_k(x)$

Therefore $f : {F_2}^m \times {F_2}^{3n} \to {F_2}^n$ with $(k_0,k_1,k_2,x) \to g(k_0, x+k_1) + k_2$ where $g : {F_2}^m \times {F_2}^n \to {F_2}^n$

Therefore, the Simon function is defined as $f' : {F_2}^m \times {F_2}^n \to {F_2}^n$ with $(k,x) \to f_{k_0,k_1,k_2}(x) + g(k,x)$

We can see that $f'(k = k_0, x)$ is periodic in x with period k_1.

Here $k \in {F_2}^m$ and $\{x_j\}, \{u_j\} \in {F_2}^n$ where $j \in \{1, ..., l\}$

3.1 The Unitary Operation A

1. Prepare an initial state of $|\psi_0\rangle = |0\rangle^{\otimes(m+nl+nl)}$.
2. Apply Hadamard Gate on the first $m+nl$ qubits.
   $|\psi_3\rangle = \left(\frac{1}{2}\right)^{\frac{m+nl}{2}} \sum_{\{k,x_j\}} |k\rangle |x_1\rangle ... |x_l\rangle |0\rangle^{\otimes nl}$
3. Apply $U_{f'}$ on all qubits. The functional result of f' is stored in the last nl qubits.
   $|\psi_1\rangle = \left(\frac{1}{2}\right)^{\frac{m+nl}{2}} \sum_{\{k,x_j\}} |k\rangle |x_1\rangle ... |x_l\rangle \left|f'(k,x_1)\right\rangle ... \left|f'(k,x_l)\right\rangle$
4. Apply Hadamard on the qubits in position $m+1...m+nl$ (i.e. on $|x_1\rangle ... |x_l\rangle$)
   $|\psi_3\rangle = \left(\frac{1}{2}\right)^{\frac{m+nl}{2}} \left(\frac{1}{2}\right)^{\frac{nl}{2}} \sum_{\{k,u_j,x_j\}} |k\rangle (-1)^{<u_1,x_1>} |u_1\rangle ... (-1)^{<u_l,x_l>} |u_l\rangle \left|f'(k,x_1)\right\rangle ... \left|f'(k,x_l)\right\rangle$

These four steps define the Operator A.

Note that if we measure the last nl qubits of $|\psi_4\rangle$ and assume that $k = k_0$ which is the 'good state'.
For an arbitrary n-qubit state $|z_i\rangle = (-1)^{<u_i,x_i>} |u_i\rangle$
$|z_i\rangle$ is entangled with $\left|f'(k_0,x_i)\right\rangle$
Therefore $|z_i\rangle$ would collapse into a state that is consistent with the measurement of $\left|f'(k_0,x_i)\right\rangle$
$|z_i\rangle$ is 'proper' if x_i and $x_i + k_1$ are the only preimages of $\left|f'(k_0,x_i)\right\rangle$. Then a proper superposition $|z_i\rangle$ collapses into the following superposition:
$((-1)^{<u_i,x_i>} + (-1)^{<u_i,x_i+k_1>}) |u_i\rangle = (-1)^{<u_i,x_i>}(1 + (-1)^{<u_i,k_1>}) |u_i\rangle$
It is clear that $|u_i\rangle$ have a non-vanishing amplitude if and only if $< u_i, k_1 >= 0$.
Hence, a measurement of a proper state yields some uniformly random $u_i \in U$,
where $U = \{u \in F_2 | < u, k_1 >= 0\}$.
k_1 can thus be found out from these set of $\{u_i\}$ by Gaussian elimination.

3.2 The Classifier B

We now resume our discussion about the quantum state evolution of $|\psi_4\rangle$.
Assuming that we have some classifier $B : {F_2}^{m+nl} \to 0, 1$ that is able to distinguish between the 'good subspace' $|\psi_{good}\rangle$ and the 'bad subspace' $|\psi_{bad}\rangle$ of $|\psi_4\rangle$.
The 'good subspace' is spanned by the set of basis kets $|x\rangle$ for which $B(x) = 1$. Whereas the 'bad subspace' is spanned by the set of basis kets $|x\rangle$ for which $B(x) = 0$.

Therefore, $|\psi_4\rangle = |\psi_{good}\rangle + |\psi_{bad}\rangle$.

Now we see how the Classifier B distinguishes the 'good' and the 'bad' states.
We define a classical Boolean function as follows:
$B : {F_2}^{m+nl} \to \{0,1\}$ that maps $(k, u_1, ..., u_l) \to \{0,1\}$.

Since this is a chosen plaintext attack (CPA), the adversary has access to the encryption function Enc(x) or $f_{k_0,k_1,k_2}(x)$ to query t random plaintext-ciphertext pairs (m_i, c_i).

Here $t = \frac{3m+nl}{n}$

In B, we hardwire for t random pairs $m_i, m_i^{'} \in {F_2}^n$ with $m_i \neq m_i^{'}$ the values,

$y_i = f_{k_0,k_1,k_2}(m_i) + f_{k_0,k_1,k_2}(m_i^{'}) = g_{k_0,m_i+k_1} + g_{k_0,m_i^{'}+k_1},$

which can be computed via $2t$ function evaluations of $f_{k_0,k_1,k_2}(.)$

Now we check the following two steps:

1. Let $U^{'} =< u_1, ..., u_l >$ be the linear span of all u_i. If $dim(U^{'}) \neq n-1$, output 0.
   Otherwise compute a basis of $U^{'}$, and use Gaussian elimination to compute the unique vector $k_1^{'} \in {F_2}^n \setminus \{0\}$ orthogonal to $U^{'}$.
2. Check via $2t$ function evaluations of $g(.,.)$ whether
   $y_i \stackrel{?}{=} g(k, m_i + k_1^{'}) + g(k, m_i^{'} + k_1^{'})$ for all $i = 1, ..., t$

Thus, we can now encode B as a unitary operator S_B that can conditionally add a negative phase to the 'good' states $B(x) = 1$ in the superposition $|\psi_4\rangle$.

3.3 Putting it all together: $Q = -AS_0A^{-1}S_B$

S_0 selectively adds a negative phase to $|0\rangle^{\otimes p}$ where $p = m + nl + nl$
Therefore, $S_0 = |0\rangle^p \langle 0|^p - I^p$.
S_0 can be easily implemented in a quantum circuit using a multi-controlled Z (MCZ) gate padded with X gates around it.

The complete amplification process is realized by repeatedly applying the unitary operator Q to the initial state ${}_0 = A|0\rangle^{\otimes(m+nl+nl)}$, i.e., we compute $Q^k A\,|0\rangle^{\otimes(m+nl+nl)}$ and measure the system for $k = \frac{\pi}{4arcsin(2^{-m/2})}$ number of iterations.

A measurement after these k iterations reveals k_0 with a high probability, and an application of B on a good state also reveals the correct value for k_1.
Thus, now for an arbitrary value of x, k_2 can be evaluated as

$$k_2 = f_{k_0,k_1,k_2}(x) + g(k_0, x + k_1)$$

4 What if $k_1 = 0^n$?

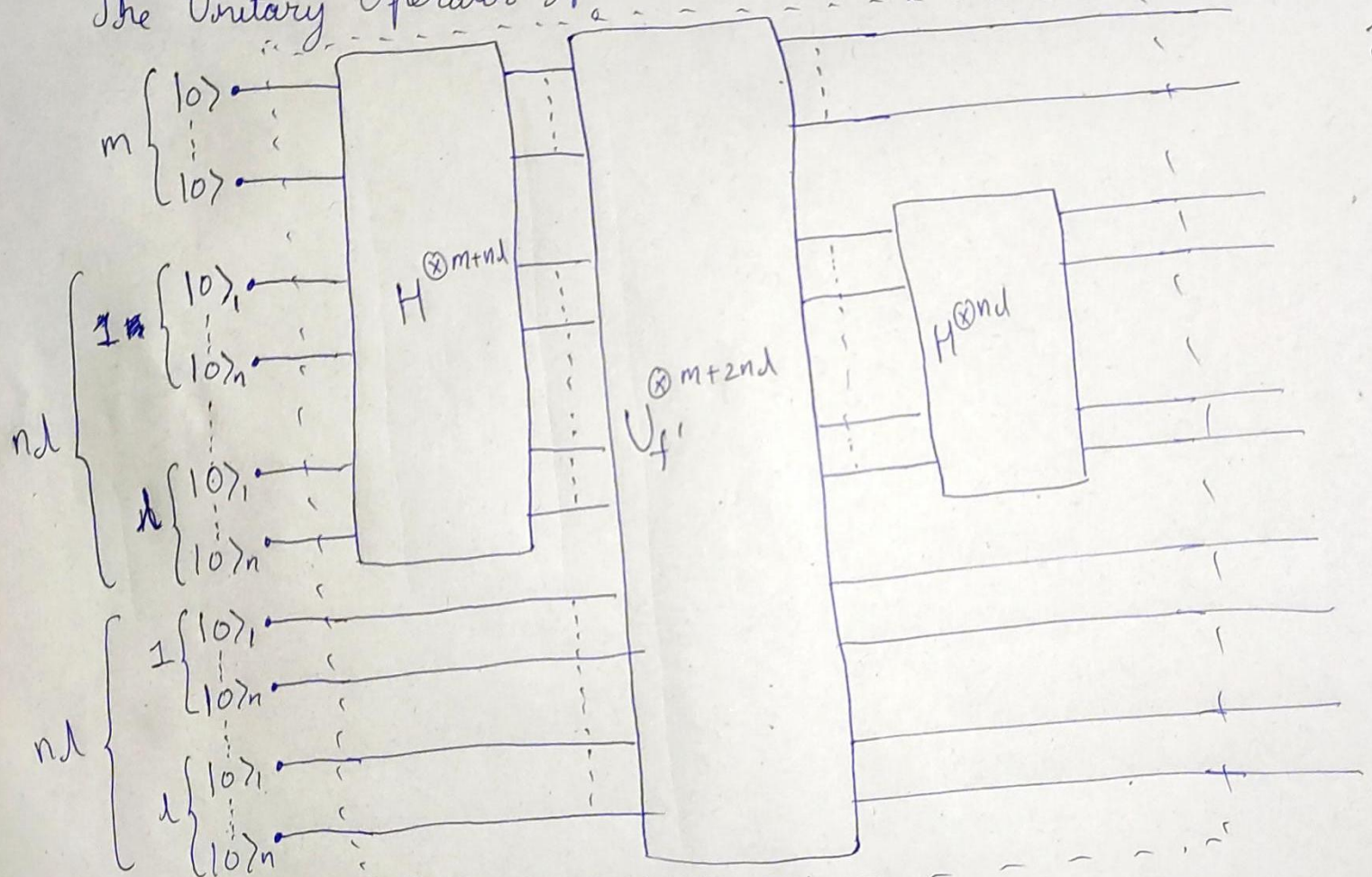
When $k_1 = |0\rangle^{\otimes n}$ we obtain a constant function with $f^{'}(k_0, .) = k_2$ for all values of x.
Therefore Simon's algorithm is not useful.

Therefore, we have two different treatments to handle the case $k_1 = 0$.

1. In the case of $k \neq k_0$, the function $f^{'}(k, .)$ is almost 'balanced' in each output bit because of the randomness of $g(k, .)$.
   Therefore, we can use a **generalized version of Deutsch-Jozsa Algorithm** to decide for which values of k the function $f^{'}(k, .)$ is constant.
2. We can also perform a **Grover's search** for k_0. Once k_0 is found, $k_2 = f_{k_0,k_1,k_2}(x) + g(k_0, x)$ can be found out for any arbitrary value of x.
   It can be shown that for $k_1 = 0^n$, $\{k_0, k_2\}$ can be determined with probability at least $1 - 2^{-m}$ using $2^{m/2}O(m)$ oracle queries and $m + 1$ qubits.

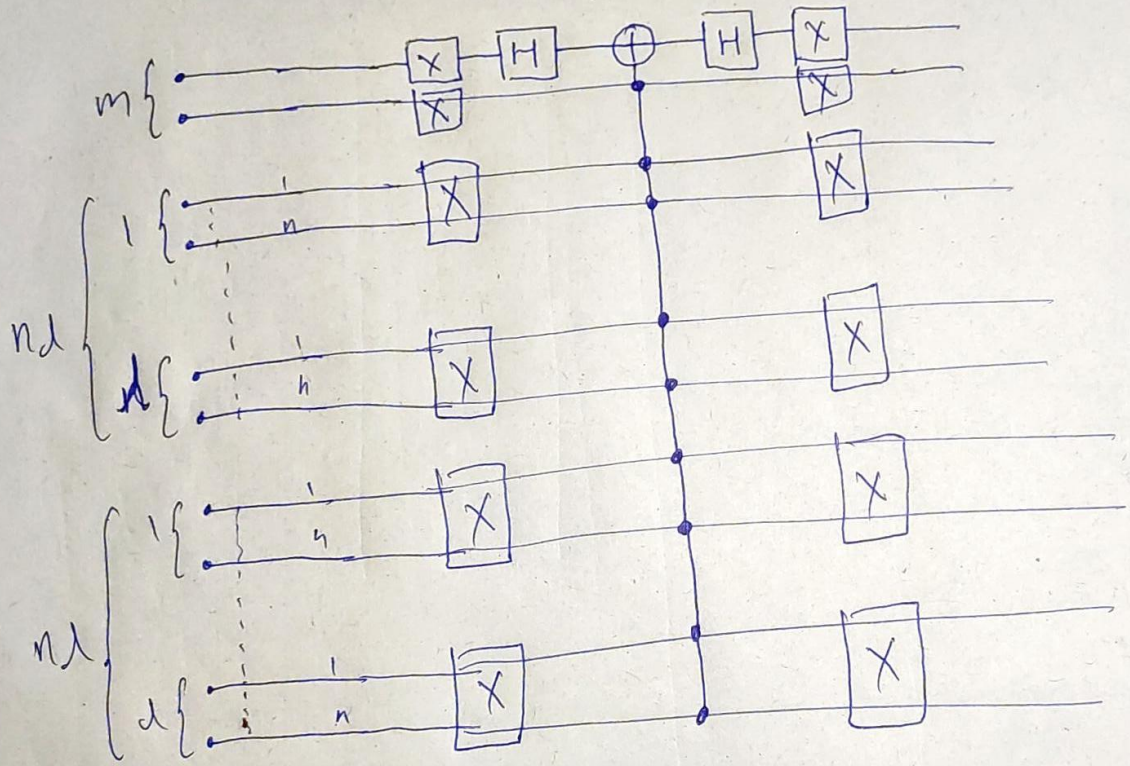
5 Circuit for the Superposition Attack

The Unitary Operator A:



The dotted region encapsulates the operator A.

The Unitary Operator S_0:



Therefore $Q = -A \delta A^{-1} S_B$