Quantum Attacks on Symmetric Cryptography Schemes

Based on *Kuwakado, H et al. (IEEE) pp. 2682–2685 (2010).*

Ali Almasi, Arman Maghsoudnia

Sharif University of Technology

February 3, 2023

Dirac's Notation

- Bra-Ket Notation

$$|\psi\rangle = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_d \end{pmatrix}$$

$$\langle\psi| = \begin{pmatrix} \alpha_1^* & \cdots & \alpha_d^* \end{pmatrix}$$

- Inner Product

$$\langle\psi|\phi\rangle = \langle\psi|\,|\phi\rangle$$

- Standard Basis (a.k.a. Computational Basis)

$$\{|0\rangle, |1\rangle, \cdots, |d\rangle\}$$

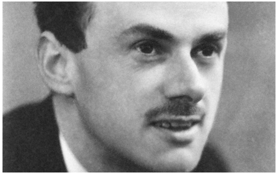


Figure: Paul Dirac [1902-1984]

Tensor Product

Definition

The **Kronecker product** of two complex matrices $A_{m\times n}$ and $B_{p\times q}$, which is denoted by $\boldsymbol{A}\otimes\boldsymbol{B}$, is an $(mp)\times(nq)$ matrix defined by

$$A\otimes B=\begin{pmatrix} a_{11}B & a_{12}B & \cdots & a_{1n}B \\ a_{21}B & a_{22}B & \cdots & a_{2n}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1}B & a_{m2}B & \cdots & a_{mn}B \end{pmatrix},$$

where each $a_{ij}B$ denotes a $p\times q$ submatrix.

The Fallen Fruit Myth

- Classical physical systems can be formulated as continuous-time dynamical system.
- The state space of a system consisting of n particles is $\mathbb{R}^{2n}$.
- The evolution of the system is described by Newton's second law.

$$F = m\frac{d^2x}{dt^2}$$

Postulate 1: State Space

Postulate 1

Every isolated physical system is associated with a Hilbert space known as the system's **state space**. The **state vector** (or more succinctly, **state**) of the system is a unit vector in the corresponding state space [1].

Postulate 1: State Space

Postulate 1

Every isolated physical system is associated with a Hilbert space known as the system's **state space**. The **state vector** (or more succinctly, **state**) of the system is a unit vector in the corresponding state space [1].

Example (Qubits)

A **qubit** is a quantum system whose state space is the two-dimensional Hilbert space $\mathbb{C}^2$. The state of a qubit can be written as

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,, \tag{1}$$

where $\alpha, \beta \in \mathbb{C}$, $|\alpha|^2 + |\beta|^2 = 1$, and $|0\rangle$ and $|1\rangle$ denote vectors $\begin{pmatrix}1\\0\end{pmatrix}$ and $\begin{pmatrix}0\\1\end{pmatrix}$.

A qubit can be in a *superposition* of $|0\rangle$ and $|1\rangle$, as stated in Equation 1.

Postulate 2: Evolution of Quantum Systems

Postulate 2

This postulate may be presented in two ways, which can be proven to be equivalent [1]:

- The state of a closed quantum system evolves according to Schrödinger's equation,

$$i\hbar \frac{d\left|\psi(t)\right\rangle}{dt} = H\left|\psi(t)\right\rangle,$$

  where $\psi(t)$ is the state of system at time t, H is a Hermitian operator known as the system's Hamiltonian, and $\hbar$ is Planck's constant.

Postulate 2: Evolution of Quantum Systems

Postulate 2

This postulate may be presented in two ways, which can be proven to be equivalent [1]:

- The state of a closed quantum system evolves according to Schrödinger's equation,

$$i\hbar \frac{d\,|\psi(t)\rangle}{dt} = H\,|\psi(t)\rangle\,,$$

  where $\psi(t)$ is the state of system at time t, H is a Hermitian operator known as the system's Hamiltonian, and $\hbar$ is Planck's constant.
- If the state of a closed quantum system at time t_1 is $|\psi(t_1)\rangle$, the state at time $t_2 > t_1$ is determined by

$$|\psi(t_2)\rangle = U\,|\psi(t_1)\rangle$$

  where U is a unitary operator that only depends on $t_2 - t_1$.

Postulate 2: Evolution of Quantum Systems

- The term *quantum gate* is used to refer to these unitary operators henceforth.
- Although there are an infinite number of quantum gates that can be applied to a single qubit, a few of them are of particular interest.

Gate Name	Matrix	Diagram
Pauli-I	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$-\boxed{I}-$
Pauli-X	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$-\boxed{X}-$
Pauli-Y	$\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$	$-\boxed{Y}-$
Pauli-Z	$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$	$-\boxed{Z}-$
Hadamard	$\begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}$	$-\boxed{H}-$

Postulate 3: Compound Quantum Systems

Postulate 3

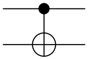
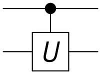
The state space of a compound quantum system composed of n individual systems with state spaces $V_1, \ldots, V_n$ is the tensor product of the individual state spaces, $V_1 \otimes \cdots \otimes V_n$. If each component system is in state $|v_i\rangle$, then the joint state of the compound system is $|v_1\rangle \otimes \cdots \otimes |v_n\rangle$ [1].

Postulate 3: Compound Quantum Systems

Postulate 3

The state space of a compound quantum system composed of n individual systems with state spaces $V_1, \ldots, V_n$ is the tensor product of the individual state spaces, $V_1 \otimes \cdots \otimes V_n$. If each component system is in state $|v_i\rangle$, then the joint state of the compound system is $|v_1\rangle \otimes \cdots \otimes |v_n\rangle$ [1].

- The time evolution of a compound quantum system composed of two subsystems with state spaces V and W is determined by unitary operators operating on the space $V \otimes W$.

Gate Name	Matrix	Diagram
CNOT	$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$	
Controlled-U	$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & U_{11} & U_{12} \\ 0 & 0 & U_{21} & U_{22} \end{pmatrix}$	

"I think that a particle must have a separate reality independent of measurements. That is, an electron has spin, location and so forth even when it is not being measured. I like to think the moon is there even if I am not looking at it."

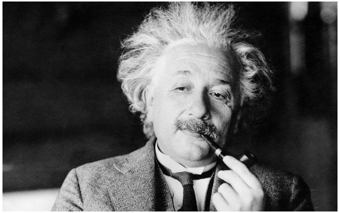


Figure: Albert Einstein [1879-1955]

Postulate 4: Quantum Measurement

Postulate 4

A measurement on a quantum system is a collection of operators $M = \{M_1, \ldots, M_m\}$ that satisfy $\sum_{i=1}^{m} M_i^\dagger M_i = I$. When a quantum system in the state $|\psi\rangle$ is measured using a collection of measurement operators M, the probability of the measurement outcome being i is derived by

$$p(i) = \left\langle \psi \left| M_i^\dagger M_i \right| \psi \right\rangle,$$

and the system collapses to the state

$$\frac{M_i|\psi\rangle}{\sqrt{\left\langle \psi \left| M_i^\dagger M_i \right| \psi \right\rangle}}$$

following the measurement [1].

The Impact of Quantum Computers on Cryptography

- Problems can be solved much faster with quantum computers
- Shor's algorithm as a game changer
- RSA and DH are theoretically broken by Shor's algorithm
- What about symmetric cryptography?

Quantum Query Model

Definition

For a function $f : \{0,1\}^n \to \{0,1\}^m$, an ***f*-quary gate** is an operator $U_f : (\mathbb{C}^2)^{\otimes n} \otimes (\mathbb{C}^2)^{\otimes m} \to (\mathbb{C}^2)^{\otimes m} \otimes (\mathbb{C}^2)^{\otimes n}$ which operates on an n-qubit main register together with an m-qubit ancilla register and is defined as

$$\forall \left|x\right\rangle \in (\mathbb{C}^2)^{\otimes n} \quad \forall \left|y\right\rangle \in (\mathbb{C}^2)^{\otimes m}, \qquad U_f(\left|x\right\rangle \left|y\right\rangle) = \left|x\right\rangle \left|y \oplus f(x)\right\rangle, \tag{2}$$

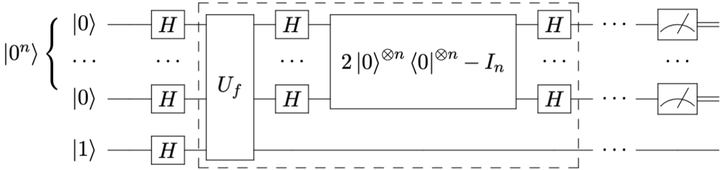
where $\oplus$ denotes bitwise XOR.

Grover's Search Algorithm

Unstructured Search

Input: Given an oracle access to a function $f : \{0,1\}^n \to \{0,1\}$ and the promise that $card(\{x \in \{0,1\}^n \ : \ f(x) = 1\}) = t$
Output: An $x \in \{0,1\}^n$ such that $f(x) = 1$.

Grover proposed the following algorithm.



Grover's Search Algorithm

- Define:

$$|G\rangle = \frac{1}{\sqrt{t}} \sum_{x:f(x)=1} |x\rangle , \qquad |B\rangle = \frac{1}{\sqrt{2^n - t}} \sum_{x:f(x)=0} |x\rangle , \qquad \sin\theta = \sqrt{\frac{t}{2^n}}$$

- After the kth Grover iteration

$$|\psi_k\rangle = \sin(2k+1)\theta\, |G\rangle + \cos(2k+1)\theta\, |B\rangle . \tag{3}$$

- If k is chosen to be the closest integer to $\frac{\pi}{4}\sqrt{\frac{2^n}{t}} - \frac{1}{2}$, the probability of error is bounded by $\frac{t}{2^n}$
- Therefore, one is able to solve the unstructured search problem by $O(\sqrt{\frac{2^n}{t}})$ queries to the oracle
- Exhaustive search of a k-bit key in time $2^{\frac{k}{2}}$ with Grover's algorithm
- We can easily double the key length

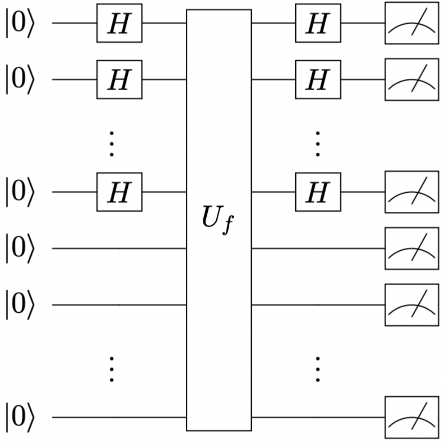
Simon's Algorithm

Simon's Problem

Input: Given an oracle access to a Boolean function $f : \{0,1\}^n \to \{0,1\}^n$ and the promise that there exists $s \in \{0,1\}^n$ such that for any $(x,y) \in \{0,1\}^n$, $[f(x) = f(y)] \Leftrightarrow [x \oplus y \in \{0^n, s\}]$.
Output: Find s.

- Can be solved classically by searching for collisions
- The optimal time to solve it is therefore $\theta(2^{\frac{n}{2}})$

Simon's Algorithm



Simon's Algorithm

1. After the first set of Hadamards: $\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle |0\rangle$
2. Applying the f-query gate: $\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle \, |f(x)\rangle$
3. Measuring the second register: $\frac{1}{\sqrt{2}}(|z\rangle + |z \oplus s\rangle) \, |f(z)\rangle$
4. Applying the second set of Hadamards:

$$\frac{1}{\sqrt{2}} \frac{1}{\sqrt{2^n}} \Big(\sum_{y \in \{0,1\}^n} (-1)^{y \cdot z} \left(1 + (-1)^{y \cdot s}\right) |y\rangle \Big) \, |f(z)\rangle$$

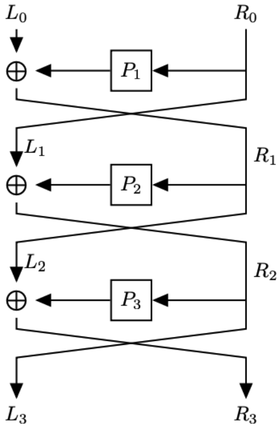
5. Measuring the first register: $|y\rangle \, |f(z)\rangle$ where $y \cdot s = 0$
6. Repeat steps 1 to 5 $O(n)$ times, to obtain $n - 1$ independent vectors and solve the linear system to obtain s.

Quantum Distinguisher for 3-round Feistel Ciphers

Theorem (Luby-Rackoff)

If P_1, P_2 and P_3 are pseudorandom functions, then the Feistel network is a pseudorandom permutation on $2n$ bits.

In the presence of a quantum attacker, the above theorem is no longer true!



Quantum Distinguisher for 3-round Feistel Ciphers

- Fix two arbitrary strings $\alpha \neq \beta$. Define $f : \{0,1\}^{n+1} \rightarrow \{0,1\}^n$ such that:

$$f(b, L_0) = \begin{cases} \mathcal{W}(L_0, \alpha) \oplus \beta & \text{if } b = 0 \\ \mathcal{W}(L_0, \beta) \oplus \alpha & \text{if } b = 1 \end{cases} \tag{4}$$

- We observe that for any $(b, L_0) \neq (b', L_0')$,

$$f(b, L_0) = f(b', L_0') \iff b = b' \oplus 1 \;\; L_0 = L_0' \oplus f_{k_1}(\alpha) \oplus f_{k_1}(\beta) \tag{5}$$

References I

[1] M. A. Nielsen and I. L. Chuang, *Quantum computation and quantum information: 10th anniversary edition*. Cambridge University Press, 2010, ISBN: 9780511976667. DOI: 10.1017/CBO9780511976667.