Hybrid Quantum Generative Adversarial Network to protect communications.

Autor: Jorge Calleja García

Tutor: Miguel Arevalillo Herráez

1. Introducción.

La computación clásica tiene límites. Tiene unos límites físicos que no puede sobrepasar. La ley de Moore nos dice que cada 2 años se aumenta por dos la potencia de los procesadores. [1]
Para cumplir con la ley de Moore, el diseño del transistor debe reducir la distancia entre la fuente y el drenaje por un factor de 2 en cada generación de tecnología. Esto reduce el área en un factor de 2, duplicando así el número de transistores por chip. [2]
Todo nos hace pensar que habrá un límite que es la relación entre la física clásica y la física cuántica.

$$\lambda = h/p \tag{1}$$

(1) Es la ecuación de De Broglie, que une el momento lineal con la longitud de onda. [3]Como regla general, la mecánica clásica se convierte en una mala descriptora de la naturaleza cuando la longitud de onda de ese objeto está en el mismo orden que su tamaño.
Para una pelota de tenis, esto es algo así como 10^{-34} metros, que es mucho menor que la pelota de tenis. Incluso para moléculas de tamaño mediano, usar la física newtoniana para describir cómo rebotan es razonable.
Es una escala móvil, no un salto discontinuo. Cuanto mayor es la masa / momento, más clásicamente se comporta la materia "similar a una partícula" y menos “cuántica”.
Cuando más pequeños sean los transistores más cercanos estarán del comportamiento cuántico y más lejanos estarán presentar un comportamiento clásico.

> “The idea behind digital computers may be explained by saying that these machines are intended to carry out any operations which could be done by a human computer. The human computer is supposed to be following fixed rules; he has no authority todeviate from them in any detail.

> We may suppose that these rules are supplied in abook, which is altered whenever he is put on to a new job. He has also an unlimited supply of paper on which he does his calculations.” Alan Turing

Al igual que nuestras computadoras digitales estándar, las computadoras cuánticas se basan en esta misma idea básica. La principal diferencia es que usan qubits , una variante del bit que puede manipularse de manera cuántica.
Hay que destacar que, a pesar de los siglos, los sistemas de cifrado clásicos y los modernos o actuales se diferencian muy poco entre sí. En el fondo, hacen las mismas operaciones, si bien los primeros estaban orientados a letras o caracteres, y los segundos lógicamente a bits y bytes. Pero los principios en los que se basan para conseguir su objetivo de enmascarar la información siguen siendo los mismos, la difusión y la confusión
La invención de la criptografía asimétrica, también conocida como criptografía de clave pública, ha sido el logro más importante de la criptografía moderna. En este sistema, cada usuario genera un par de claves, una clave pública, distribuida libremente a todos, y una clave privada, mantenida en el máximo secreto. Alice puede cifrar un mensaje usando la clave pública de Bob, pero solo Bob puede descifrarlo usando su clave privada.
Sin embargo, para implementar esta característica, tenemos que usar funciones matemáticas que generalmente son difíciles de resolver pero, una vez que se conoce una solución, no es tan difícil verificarla. Las implementaciones contemporáneas de algoritmos matemáticos hacen uso de factorización de enteros, logaritmo discreto y relaciones de curva elíptica. No es el alcance de este cuaderno entrar en los detalles de este proceso, que es ampliamente discutido en la literatura.
Digamos que ofrece un buen compromiso entre seguridad y practicidad, superando el problema de la generación de claves de una sola vez y, lo más importante, el intercambio de claves. De hecho, en casos de uso real, casi todas las principales implementaciones de criptografía se realizan de forma asimétrica (aunque a veces en combinación con claves simétricas), como TLS, S / MIME, PGP, OMEMO, OTR, etc.
El advenimiento de las computadoras cuánticas ha planteado un problema inesperado para la criptografía de clave pública. Se ha demostrado que una computadora cuántica puede resolver todos los algoritmos matemáticos actualmente en uso de una manera mucho más eficiente. Gracias a las propiedades de la Transformada Cuántica de Fourier (QFT) y su implementación en el algoritmo de Shor, el tiempo necesario para encontrar una solución general para el problema se reduce de ser exponencial a ser solo polinomial, abriendo así una ventana para posibles ataques de fuerza bruta .
En la actualidad, las computadoras cuánticas no son lo suficientemente potentes para realizar estas operaciones en grandes cantidades, pero en un futuro no muy lejano podrían serlo, lo que se suele llamar NISQ era, Noisy Intermediate-Scale Quantum, tanto

que los expertos en criptografía han comenzado a discutir estrategias para fortalecer los protocolos criptográficos en caso de computadoras cuánticas ampliamente disponibles. Este campo se llama criptografía post-cuántica.
Las computadoras cuánticas también presentan otra ventaja extraordinaria, que puede conducir a un secreto perfecto. Almacenar información en forma de qubits es el primer paso en la implementación de la criptografía cuántica, la ciencia de intercambiar información de manera segura utilizando la física cuántica. Esto se logra mediante el establecimiento de un canal cuántico, un aparato especial capaz de entregar información cuántica en forma de qubits. La confidencialidad está garantizada por las leyes de la mecánica cuántica, una forma notable de llamar a la física en ayuda de las matemáticas.
El campo de la inteligencia artificial (IA) ha experimentado un crecimiento sobresaliente en las últimas dos décadas. Ha demostrado ser eficaz en el manejo de áreas complejas como el reconocimiento de voz, el reconocimiento de imágenes y muchas otras. Una rama interesante y en evolución que se introdujo hace años, pero que sólo ha experimentado un buen crecimiento en los últimos años, es la encriptación de la IA. Después de que Google anunciara que había tenido éxito en la enseñanza de la encriptación de redes neuronales en presencia de espías, el interés de varios investigadores de todo el mundo por desarrollar nuevas redes neuronales capaces de realizar diversas tareas de criptografía se ha extendido rápidamente en este campo particular. En este documento se dan los primeros pasos para lograr una comunicación segura entre más de dos partes utilizando la encriptación en las redes neuronales. Relacionamos la idea del esquema de cifrado simétrico de dos partes de Google con un esquema de cifrado de varias partes.

2. Estado del arte.

Primero de todo, voy a hablar sobre el sistema de redes neuronales con el objetivo de mejorar el cifrado de la información que comparten entre ellas las computadoras, ya que es el sistema que ha hecho que este trabajo de investigación nazca.

2.1. «Learning to protect communications with adversarial neural cryptography»

Google en 2016, explico a todo el mundo como desarrollar un sistema GAN para cifrar las comunicaciones, esto hizo que la investigación sobre este area creciera mucho desde ese año hasta ahora.
La solución de Google es la siguiente, es necesario que explique bien este sistema ya que todo este trabajo se basa en la modificación de sus sistema para poder obtener mejores resultados que su red GAN clásica:

Hay tres redes neuronales GAN:
Alice
La red Alice concatena dos entradas de N-bits (el texto plano y la clave) en un vector de entrada 2N, usando -1 y 1 para representar los valores de los bits. Este vector se procesa a través de una capa FC de 2N×2N, luego enviado a través de una sucesión de cuatro capas convolucionales de 1-D. Las capas convolucionales se describen en términos de su tamaño de ventana, profundidad de entrada y profundidad de salida. Cada una tiene un "paso", la cantidad por que la ventana se desplaza a cada paso. Las capas de hormigón son [4, 1, 2], [2, 2, 4], [1, 4, 4], y con zancadas de 1, 2, 1, 1. Intuitivamente, la primera capa desliza una ventana de tamaño 4 a través de la 2N elementos de salida de la capa FC, emitiendo dos números (profundidad de salida 2), con el paso 1. Nosotros usar una unidad no lineal sigmoide después de cada capa, excepto la última. Después de la capa final, donde el la salida se reduce a los elementos N, usamos una unidad no lineal de tanh. (Recordemos que el tanh tiene una salida entre [-1, 1], llevando los valores de vuelta a un rango que puede mapear a valores binarios). El La red de Bob es idéntica a la red de Alice La red de Eve sólo toma el texto cifrado como entrada, y por lo tanto tiene una primera capa de N × 2N FC.
Hay dos sistemas en nuestra implemantación. Vamos a crear un sistema de Redes Generativas Antagónicas (GAN) híbrido, con un generador cuántico en el interior de una de las redes.
Hay 3 redes neuronales Alice, Bob y Eve. Las tres van a tener la misma configuración, por simplicidad y por

2.2. Deepfakes.

2.3. Gan caótica.

Hay un grupo de investigadores que han hecho un sistema GAN añadiendole conceptos de la teoría del caos. Ellos proponen que es una buena solución debido a que los sistemas caóticos tienen dos propiedades muy interesantes que ayudan para proteger las comunicaciones, que al fin y al cabo es nuestro objetivo a desarrollar en este trabajo. La primera de las motivaciones es que cuando tenemos un sistema dinámico no lineal cualquier pequeña diferencia entre las condiciones iniciales, aunque sea una diferencia infinitesimal produce resultados muy diferentes entre sí. La otra vertiente es la potencialidad del mapeo logístico que tiene utilidades para la generación de números pseudo-aleatorios. Su investigación fue básicamente:

3. Fundamentos.

3.1. Computación cuántica.

En la computación cuántica se trata con el equivalente de bits llamados qubits , que notoriamente pueden manejar información en un estado no binario gracias a una propiedad de los sistemas cuánticos llamada superposición (a veces se dice que pueden representar 0s y 1s en al mismo tiempo).

$$c1\,|0\rangle + c_2\,|1\rangle \tag{2}$$

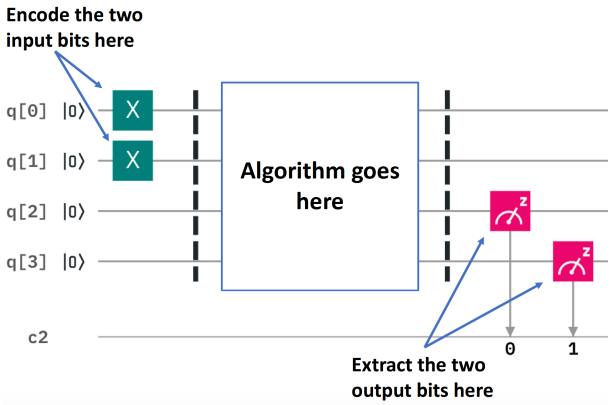
Sobre estos qubits se pueden realizar operaciones. La función que cambia las propiedades de cada qubit es el operador es una función que va de un espacio de estados físicos a otro espacio de estados físicos.
Una función de onda ψ (x ; t) es una forma de representar el estado físico de un sistema de partículas. Usualmente es una función compleja, de cuadrado integrable y univaluada de las coordenadas espaciales de cada una de las partículas. Las propiedades mencionadas de la función de onda permiten interpretarla como una función de cuadrado integrable.
Con cada observable físico, hay asociado un operador que se usa con la función de onda. Supóngase que la función de onda asociada con un valor cuantizado definido (valor propio) del observable se denota por Ψn, y el operador se representa por O. La acción del operador está dado por:

$$O\Psi_n = o_n\Psi_n \tag{3}$$

Un circuito cuántico es una serie de operaciones aplicadas a qubits que cambian su estado, por ejemplo , cambiando su fase relativa. Los Qubits se pueden representar geométricamente con una llamada esfera de Bloch , por lo que una operación en un qubit corresponde a una rotación del vector de estado cuántico en este espacio virtual.

C:/root/Escritorio/Quantum/assets/800px-Bloch_sphere.svg.png

Esfera de Bloch. Imagen obtenida de [4].



C:/root/Escritorio/Quantum/assets/Puerta cuántica.png

3.2. Criptografía

3.2.1. Teoría de números aleatorios

3.3. Redes neuronales

Partiendo de que una red neuronal cuántica es cualquier circuito cuántico con parámetros continuos entrenables.
Pues aquí hablaré de seguridad informática, de criptografía.
De computación cuántica.
De teoría de número aleatorios.
De redes neuronales.
De GAN.
Hay dos maneras de realizar un algoritmo de aprendizaje automático cuánticoEn lugar de simular una computadora cuántica dentro del software de aprendizaje automático convencional, tomaríamos todas las mejores características del software de aprendizaje profundo y las haríamos verdaderamente nativas de los dispositivos cuánticos.

4. Planificación.

En nuestro proyecto vamos a contar con los siguientes perfiles:

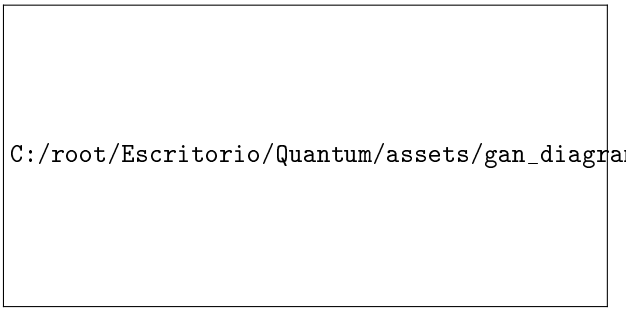
- Un desarrollador cuántico.

- Un analista de computación cuántica.
- Un analista de redes neuronales.
- Un desarrollador de redes neuronales.
- Un analista de seguridad informática.
- Un jefe de proyectos.

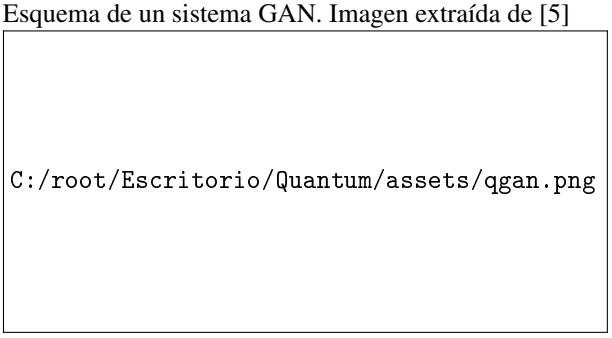
La planificación de GP.
——————————>
————————————————————>
————————————————————————————————->

5. Análisis teórico.

5.1. Fundamento del algoritmo



Esquema de un sistema GAN. Imagen extraída de [5]



Esquema de un sistema QGAN. Imagen extraída de [6]

5.2. Propuesta de implementación

6. Herramientas.

Para realizar nuestros experimentos vamos a hacer uso de las siguientes herramientas:

- Anaconda: Anaconda es una distribución gratuita y de código abierto de los lenguajes de programación Python y R para la informática científica (ciencia de los datos, aplicaciones de aprendizaje automático, procesamiento de datos a gran escala, análisis predictivo, etc.), que tiene como objetivo simplificar la gestión y el despliegue de los paquetes. Las versiones de los paquetes son administradas por el sistema de gestión de paquetes conda.

- Jupyter Notebook: El Cuaderno Jupyter es un entorno informático interactivo basado en la web para crear documentos ipynb. Un documento Jupyter Notebook es un documento JSON, siguiendo un esquema versionado, y que contiene una lista ordenada de celdas de entrada/salida que pueden contener código, texto (usando Markdown), matemáticas, gráficos y medios enriquecidos. Un Cuaderno Jupyter puede convertirse a una serie de formatos de salida de estándar abierto (HTML, diapositivas de presentación, LaTeX, PDF, ReStructuredText, Markdown, Python) .

- Keras: Es una API de redes neuronales de alto nivel, escrita en Python y capaz de funcionar sobre TensorFlow, CNTK o Theano. Fue desarrollado con el objetivo de permitir una rápida experimentación. El objetivo es conseguir desarrollar redes neuronales con rápidez.

- Numpy: Es una biblioteca para el lenguaje de programación Python, que añade soporte para matrices y conjuntos multidimensionales, junto con una gran colección de funciones matemáticas de alto nivel para operar en estos conjuntos.

- Matplotlib: Es una biblioteca de representación en 2D de Python que produce figuras de calidad de publicación en una variedad de formatos de copia impresa y entornos interactivos a través de plataformas.

- Pandas: Es una biblioteca de software escrita para el lenguaje de programación Python para la manipulación y análisis de datos. En particular, ofrece estructuras de datos y operaciones para manipular tablas numéricas y series temporales.

- Qiskit:

- Simulador cuántico:

- PennyLane: En PennyLane, los cálculos cuánticos se representan como objetos de nodo cuántico . Se utiliza un nodo cuántico para declarar el circuito cuántico, y también vincula el cálculo a un dispositivo específico que lo ejecuta. Los nodos cuánticos se pueden crear fácilmente utilizando el decorador qnode. QNodes puede interactuar con cualquiera de las bibliotecas numéricas y de aprendizaje automático compatibles (NumPy , PyTorch y TensorFlow), lo que se indica al proporcionar un interface argumento opcional al crear un QNode. Cada interfaz

permite que el circuito cuántico se integre perfectamente con estructuras de datos específicas de la biblioteca (por ejemplo, matrices NumPy o tensores Pytorch / TensorFlow) y optimizadores .

- Desde el primer día, PennyLane ha proporcionado dos características clave que creemos que serán cruciales para QML a corto plazo: i) diferenciación automática de circuitos cuánticos; y ii) una abstracción QNode para construir cálculos híbridos cuántico-clásicos y multidispositivos.
- Por defecto, QNodes usa la interfaz NumPy. Las otras interfaces de PennyLane se presentan con más detalle en la sección de interfaces .

7. Implementación.

[Documento de Google].
[Comienzo a definir la red neuronal].
El sistema generador cuántico funciona de la siguiente manera:
Puerta de NOP:

$$NOT = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{4}$$

Puerta de Hadamard:
Esta puerta consiste en aplicar al estado

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{5}$$

8. Evaluación.

Primero. GAN de Google. He implementado la GAN de Google con el objetivo de usar la misma GAN para todas las pruebas, ya que si su red está mejor implementado igual los resultados no son consistentes con mis observaciones.
Segundo. Intentar mejorar la red.
Tercero. Prueba con números cuánticos y GAN.
Cuarto. Prueba con protocolo cuantico y GAN.

9. Conclusiones.

Realizar una red neuronal no híbrida, hacer una red neuronal puramente cuántica.

Referencias

[1] Markku Kinnunen. Examining the limits of mooreâs law: possible influence of technological convergence on redefining the curriculum in ict institutions. 2015.

[2] Mark Lundstrom. Moore's law forever? *Science*, 299(5604):210–211, 2003.

[3] C.S. Río. Física cuántica, 2016.

[4] Esfera de bloch. https://es.wikipedia.org/wiki/Esfera$_d e_B loch$. *Accessed* : $2020 - 03 - 06$.

[5] Google generative adversarial networks. https://developers.google.com/machine-learning/gan/gan$_s tructure$. *Accessed* : $2020 - 03 - 06$.

[6] Quantum generative adversarial networks. hhttps://pennylane.ai/qml/demos/tutorial$_Q GAN.html$. *Accessed* : $2020 - 03 - 06$.