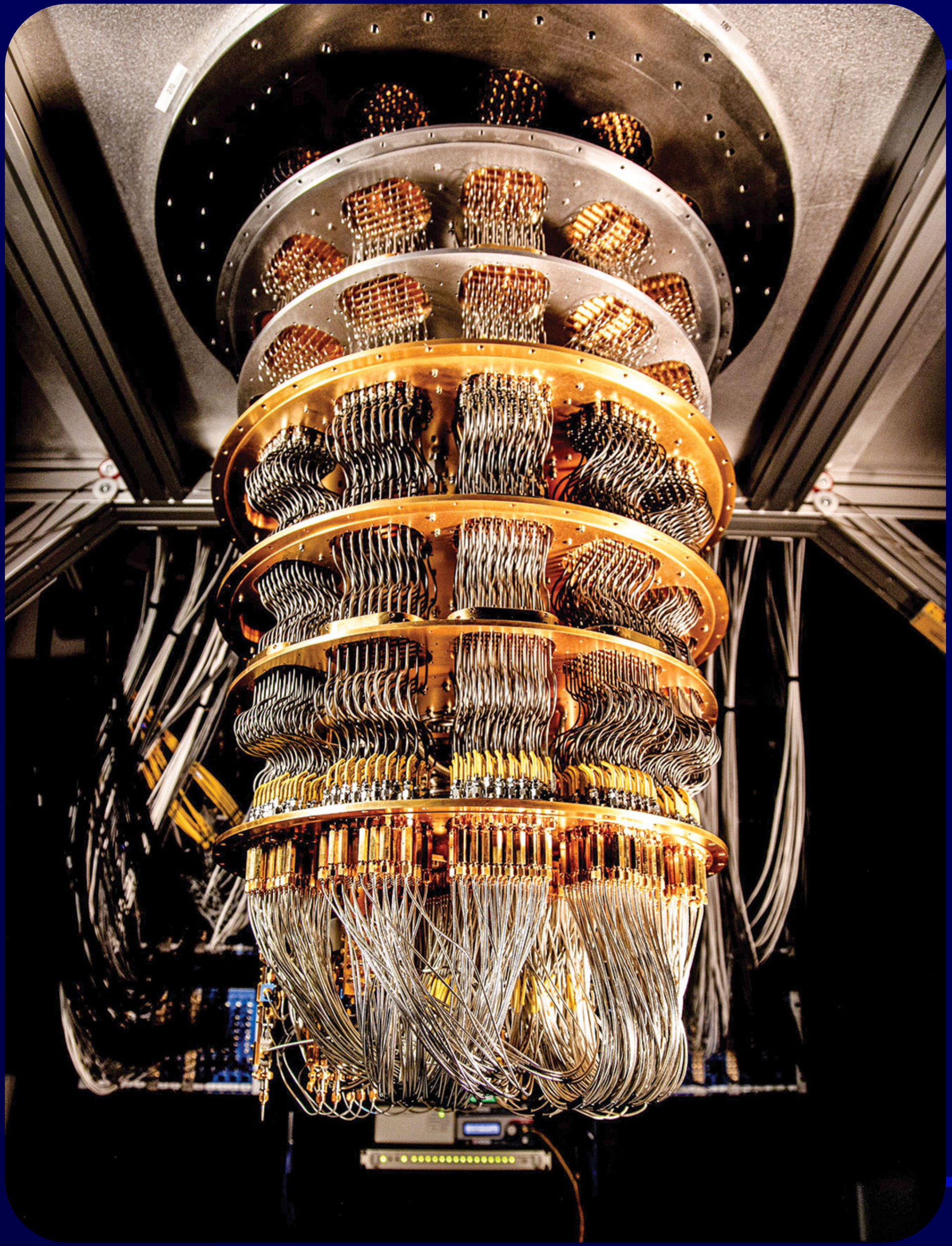
Post-Quantum Cryptography Neural Network

Paper by Abel C. H. Chen
Presented by Sadra Setarehdan

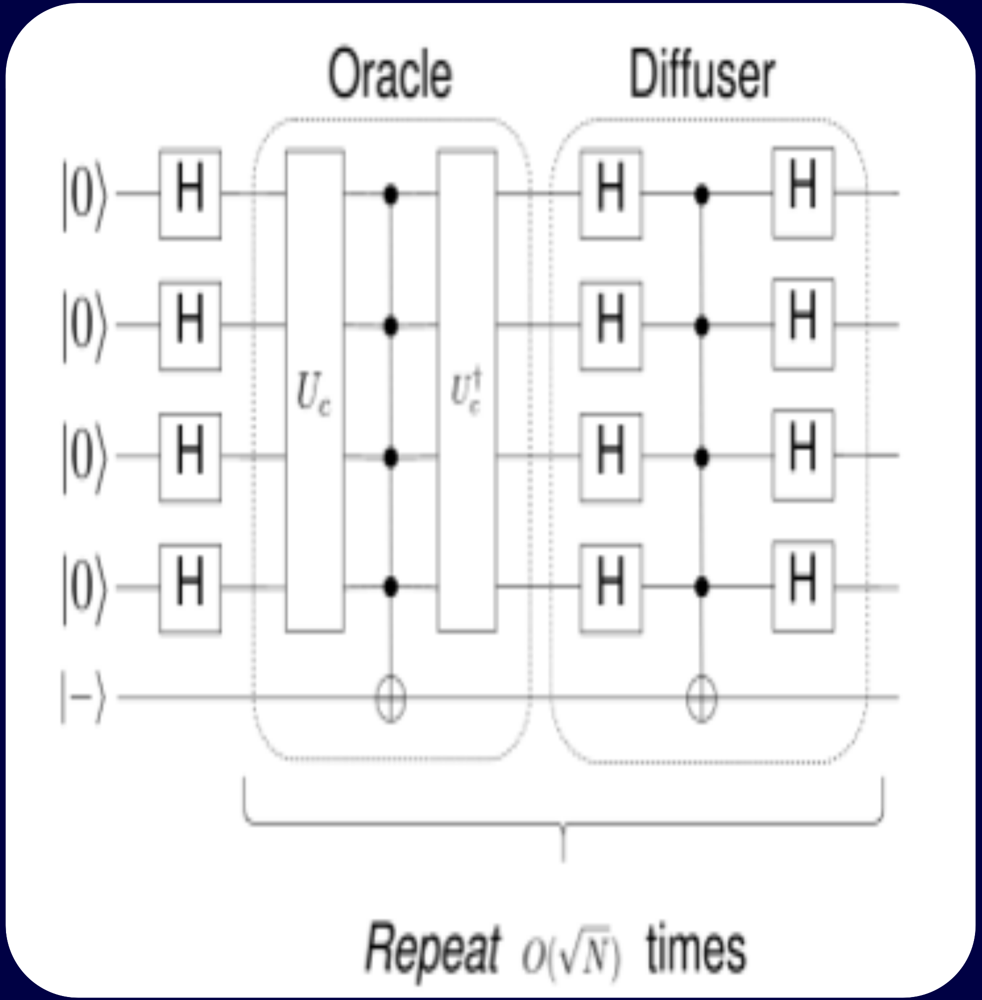


What is Quantum Computing?

Quantum computers are machines that use the properties of quantum physics to store data and perform computations. Classical computers encode information in binary “bits” that can either be 0s or 1s. In a quantum computer, the basic unit of memory is a quantum bit or qubit.

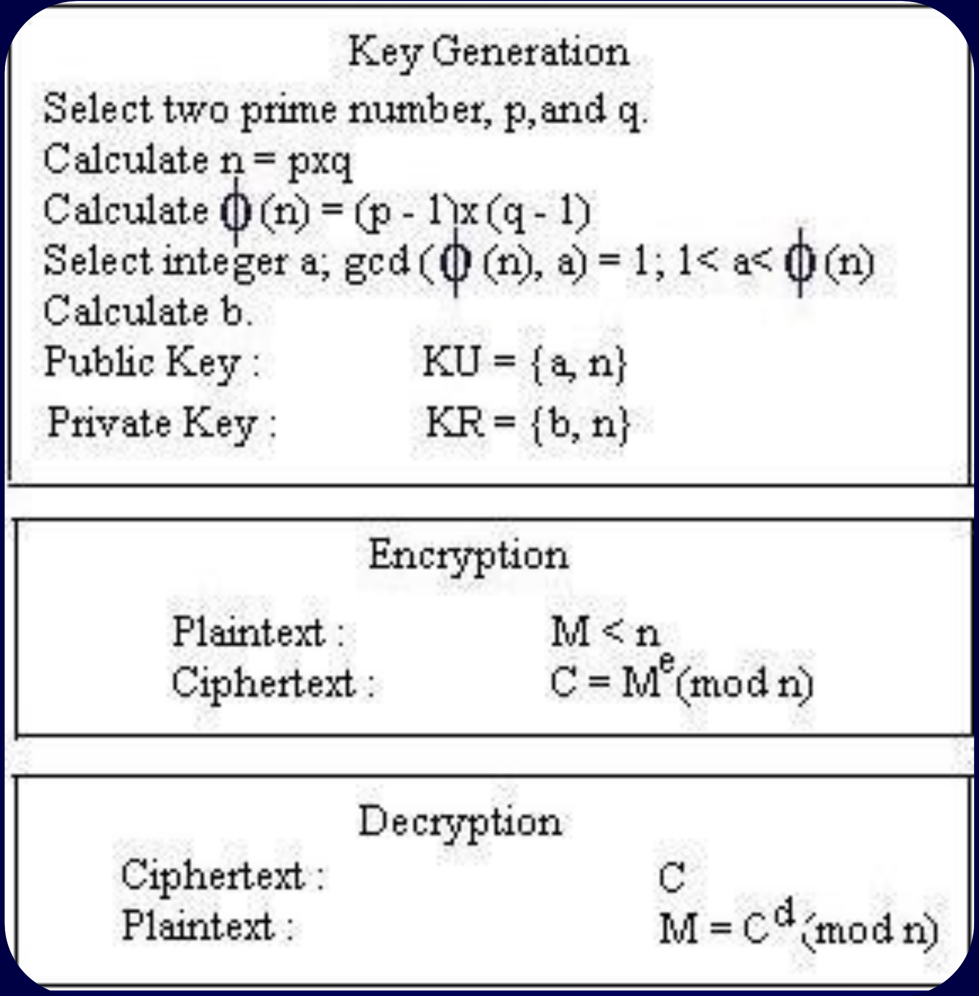
Qubits can be in many different arrangements all at once, a property known as quantum superposition.

AES



Grover's algorithm breaks AES

RSA



Key Generation

Select two prime number, p, and q.
Calculate n = pxq
Calculate $\phi(n) = (p - 1) x (q - 1)$
Select integer a; $gcd(\phi(n), a) = 1; 1 < a < \phi(n)$
Calculate b.
Public Key : KU = {a, n}
Private Key : KR = {b, n}

Encryption

Plaintext : $M < n$
Ciphertext : $C = M^e (mod\ n)$

Decryption

Ciphertext : C
Plaintext : $M = C^d (mod\ n)$

Shor's algorithm breaks RSA

How To Read A Tough Paper

Abstract

Purpose of the study → Innovations and ideas → Experiment

Sections guide

Section II

Code-based PQC

Introduce McEliece Method

Section III

PQC neural network

Adding random perturbations

Section IV

Practical demonstration

Evaluation methods

Section V

Conclusion and Discussion

Hamming Code method

$$G = generator\ matrix$$
$$H = error\ detecting\ matrix$$
$$R = decoder\ matrix$$
$$x = plaintext$$

$$y = xG$$
$$x = yR$$

$$z = y'H$$

McEliece cryptography method

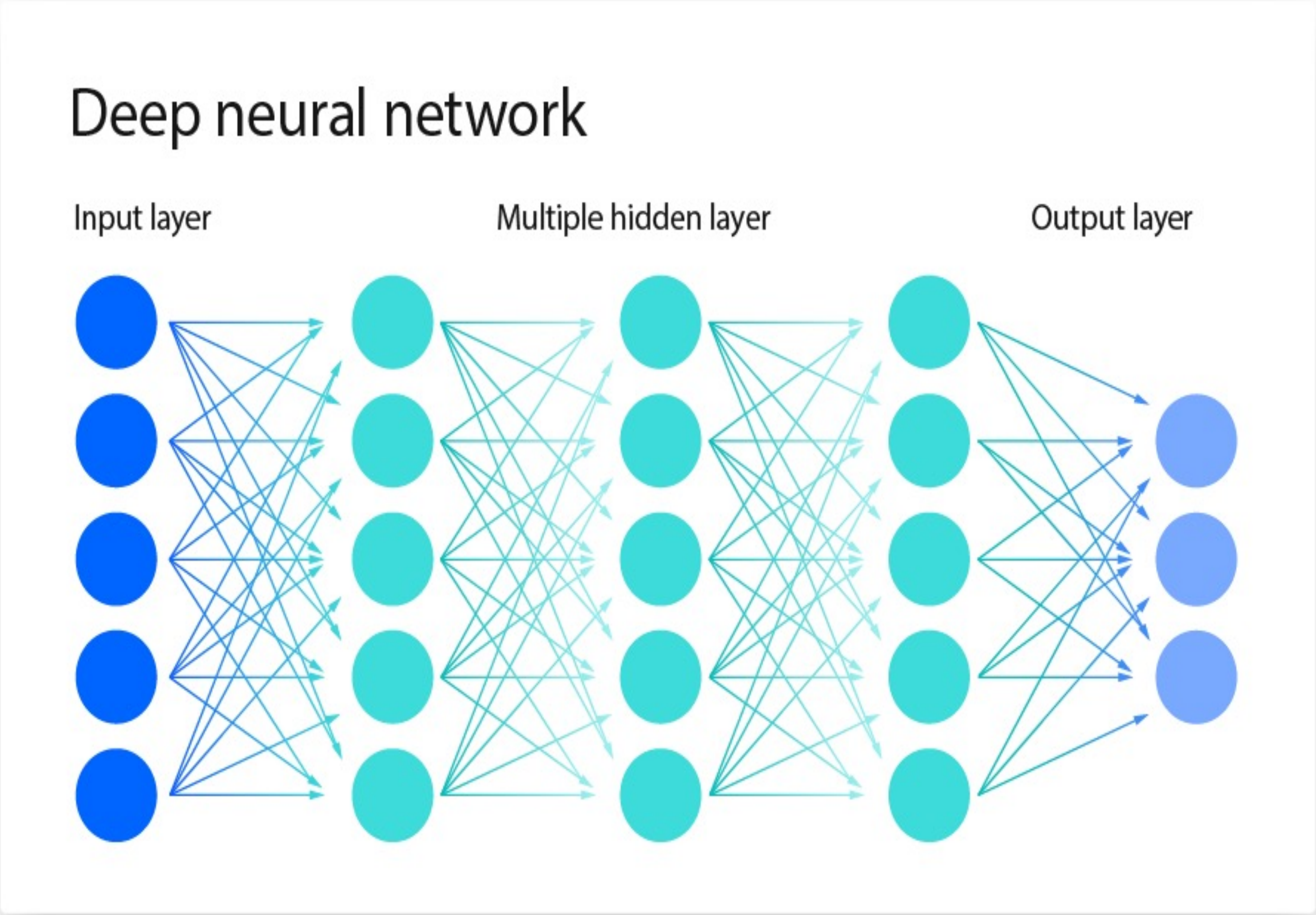
$$S = Scrambler\ matrix$$
$$G = generator\ matrix$$
$$P = permutation\ matrix$$
$$x = plaintext$$

$$G' = SGP$$

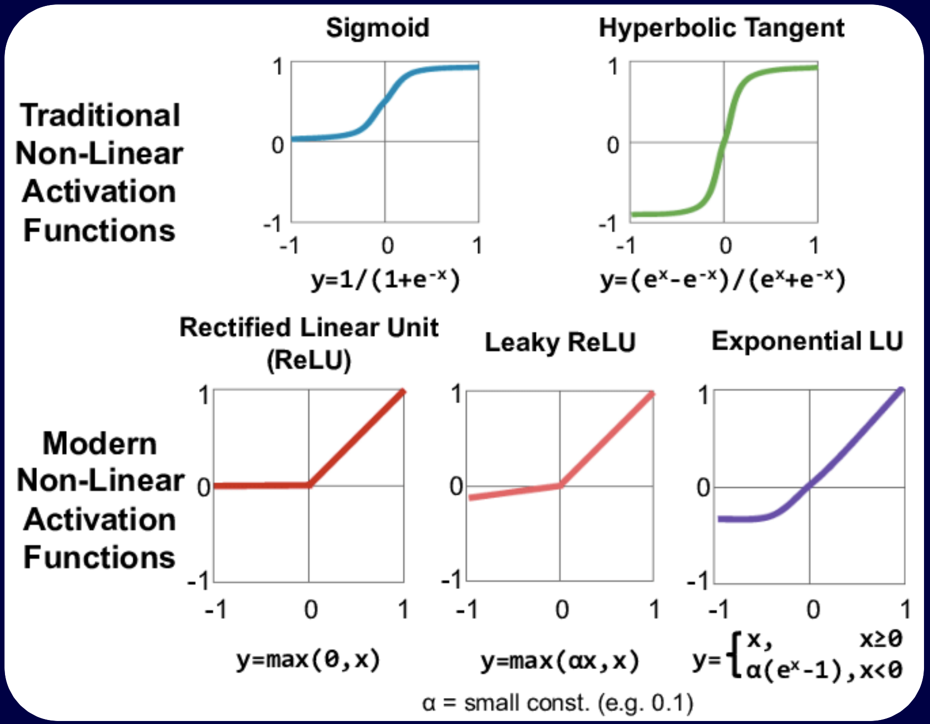
$$y = xG' + r = xSGP + r$$

$$yP^{-1} = xG'P^{-1} = xSGPP^{-1}$$
$$yP^{-1} = xSG$$
$$yP^{-1}R = xS$$
$$yP^{-1}RS^{-1} = x$$

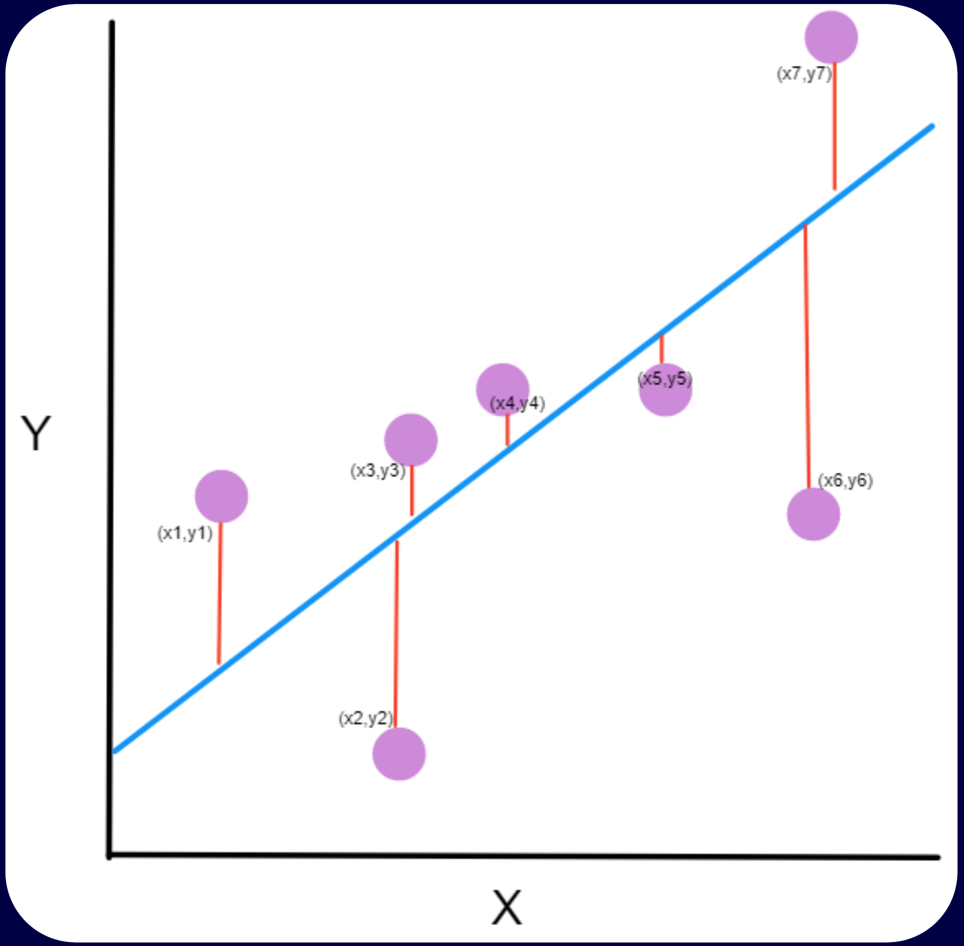
Neural Networks



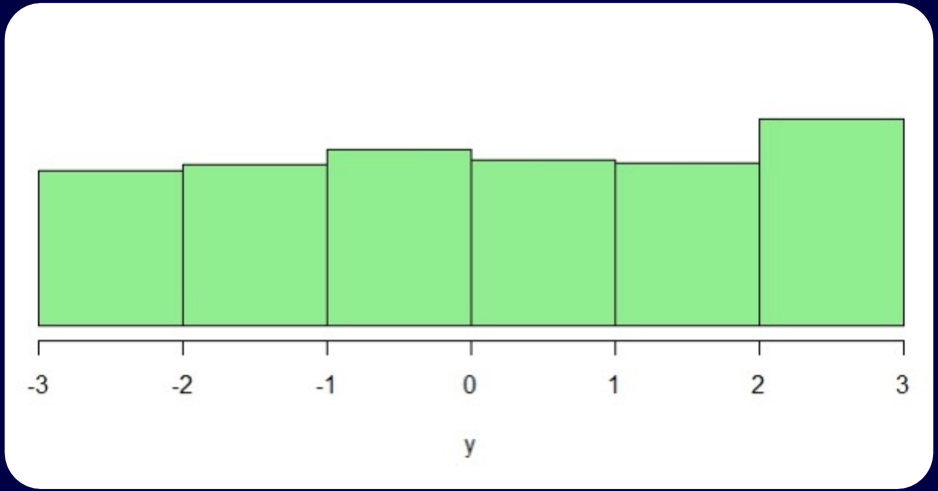
Non-Linear Activation Function



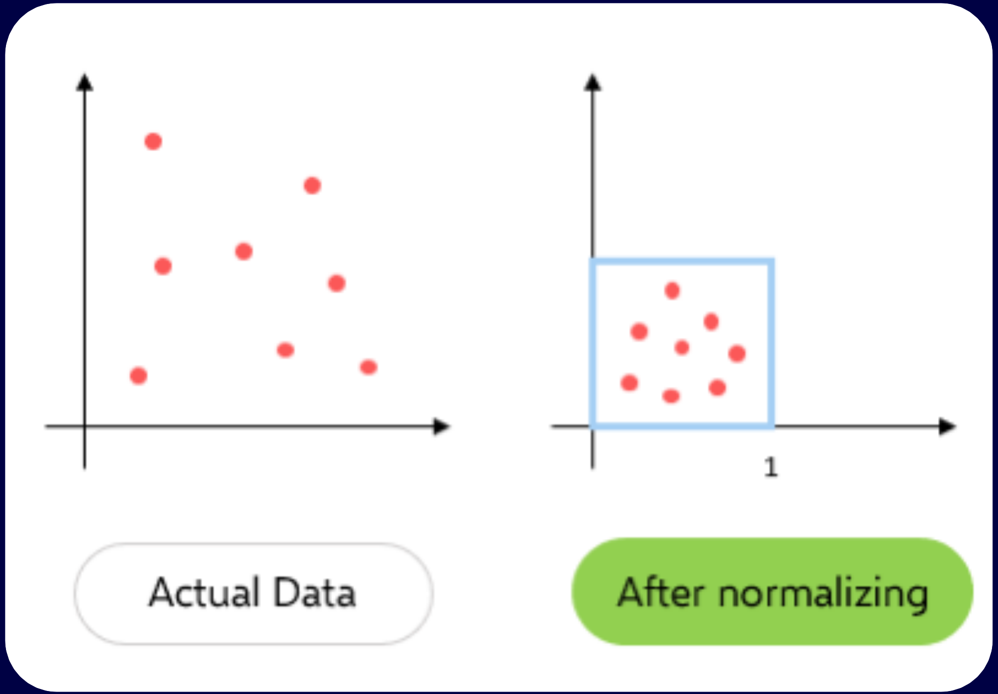
MSE



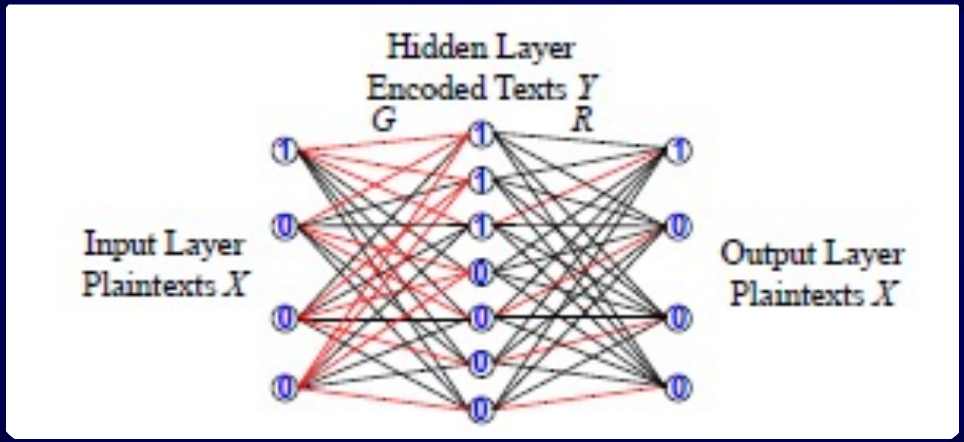
Uniform Distribution



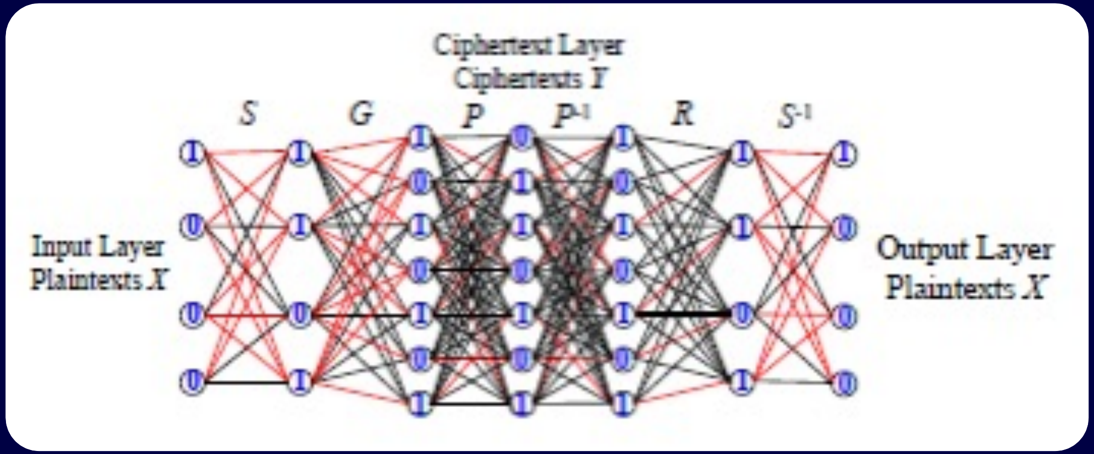
Normalization



Hamming code



McEliece



Cellular network signals (Practical experiment)

BLE I. THE MSEs AND CDF VALUES UNDER DIFFERENT VAL
OF α

Weight α	The MSEs of output layer	The chi-test CDF values of random numbers	The chi-test CDF values of ciphertexts Y'
0.1	3.74E-05	0.009227	0.303414
0.2	5.86E-05	0.009227	0.202276
0.3	6.84E-05	0.009227	0.089382
0.4	8.27E-05	0.009227	**0.038992**
0.5	0.0001	0.009227	**0.018034**
0.6	0.0001	0.009227	**0.013643**
0.7	0.0002	0.009227	**0.016572**
0.8	0.0002	0.009227	**0.012751**
0.9	0.0003	0.009227	**0.017519**
1	0.0003	0.009227	**0.017685**

Thank you!

Presented by Sadra Setarehdan