Regards Croisés Mathématiques & Physique
Bloc 3 : Cryptographie

Lucie Le Briquer

19 décembre 2017

1 Cryptographie classique (Jean-Goubault Larrecq)

Cf. poly (en sautant la partie 3 et dans les transparents passer de sûreté inconditionnelle à chiffrement symétrique)

2 Cryptographie quantique (Frédéric Grosshans)

2.1 Ordinateurs quantiques

Première motivation (Feiman 1982) : ordinateurs quantiques pour simuler l'ensemble des problèmes quantiques de même taille.

1994, Peter Shor : algorithme de Shor $\rightarrow$ Factorisation. Il montre que si l'on peut construire un ordinateur quantique alors on pourrait factoriser un nombre de n bit en $O(n^3)$ opérations.
Or la factorisation est au cœur de tous les problèmes de cryptographie à clé symétrique.
Désormais on a la généralisation de ce résultat de factorisation à tout sous-groupe abélien.

Problème : ordinateurs quantiques d'ici 20, 50, 100 ans qui permettraient craquer la crypto classique. Deux grandes lignes de solutions :

1. Post-quantum crypto (NIST)
2. Crypto quantique

2.2 Cryptographie quantique

La crypto asymétrique devrait être assez résistante aux ordinateurs quantiques selon les premières études. Le processus de factorisation exploite en revanche le caractère symétrique dans le cas des cryptages symétriques, ceux-ci seraient donc plus enclins à être craqués.

Exemple. (distribution quantique de clés)
Alice envoie des objets quantiques à Bob.

Alice	Eve	Bob
kfsbgjcxlzt	k..b...x..t	0fsFgjcxlzU
avdoygv	$\longleftrightarrow$	avdoygv

Les mesures de l'espion Eve induisent des pertubations mesurables $\Rightarrow$ génération d'une clé secrète entre Bob et Alice.

Ce système nécessite que Bob et Alice soient reliés par une fibre optique pour utiliser la crypto quantique à photon unique (Single Photon QKD) :

- portée limitée à une centaine de kilomètres (2017 : QKD Satellite/Terre par une équipe chinoise)
- taux de clé faibles (quelques kbit/s)

Classical One-Time-Pad

- very long range (Paris-Pavia)
- not so small rate (1CD/year)
- but the data has to stay here

2.3 Qubits

Qubits est le terme donné en 1996 pour bit quantique, système quantique à 2 niveaux (spin $\frac{1}{2}$). Soit ψ un état quantique on note :

$$|\psi\rangle = \alpha|0\rangle + \beta 1\rangle$$

sa décomposition sur la base quantique (opérateur appelé *ket*).

$$\begin{pmatrix}\alpha\\ \beta\end{pmatrix} = \alpha\begin{pmatrix}1\\ 0\end{pmatrix} + \beta\begin{pmatrix}0\\ 1\end{pmatrix}$$

$\alpha, \beta \in \mathbb{C}$ avec $\alpha^2 + \beta^2 = 1$. On a aussi l'opérateur *bra* :

$$\langle\psi| = (\alpha^* \ \beta^*)$$

$$|\varphi\rangle = \delta|0\rangle + \gamma|1\rangle$$

Alors :

$$\begin{aligned}\text{(bra-ket)} \quad \langle\psi|\varphi\rangle = (\alpha^* \ \beta^*).\begin{pmatrix}\delta\\ \gamma\end{pmatrix} &= \alpha^*\delta + \beta^*\gamma \\ &= \Big(\alpha^*\langle 0| + \beta^*\langle 1|\Big)\Big(\delta|0\rangle + \gamma|1\rangle\Big) \\ &= \alpha^*\delta\langle 0|0\rangle + \alpha^*\gamma\langle 0|1\rangle + \beta^*\delta\langle 1|0\rangle + \beta^*\gamma\langle 1|1\rangle \\ &= \alpha^*\delta\langle 0|0\rangle + \beta^*\gamma\langle 1|1\rangle\end{aligned}$$

Mesure de $|\psi\rangle$ dans la base $|0\rangle, |1\rangle$

$$P(0) = |\langle 0|\psi\rangle|^2 = |\alpha|^2 \qquad P(1) = |\langle 1|\psi\rangle|^2 = |\beta|^2$$

Prenons la base $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$. On a bien $\langle +|-\rangle = 0$. Et :

$$P(-) = |\langle -|\psi\rangle|^2 = \frac{1}{2}\Big|(\langle 0| - \langle 1|)(\alpha|0\rangle + \beta|1\rangle)\Big|^2 = \frac{1}{2}|\alpha - \beta|^2$$

De même,

$$P(+) = \frac{1}{2}|\alpha + \beta|^2$$

2.3.1 Billets de Wiesner (1969-1982)

Quantum money is a proposed design of bank notes making them impossible to forge, by using quantum physics. The idea influenced the development of quantum key distribution protocols used in quantum cryptography.

The idea was put forward in about 1970 by Stephen Wiesner, a graduate student at Columbia University, though it was rejected by a number of scientific journals, meaning that it remained unpublished until 1983.[1]

How it works [edit]

In addition to a unique serial number on each bank note (these notes are actually more like cheques, since a verification step with the bank is required for each transaction), there is a series of isolated two-state quantum systems.[2] For example, photons in one of four polarizations could be used: at 0°, 45°, 90° and 135° to some axis, which is referred to as the vertical. Each of these is a two-state system in one of two bases: the horizontal basis has states with polarizations at 0° and 90° to the vertical, and the diagonal basis has states at 45° and 135° to the vertical.

At the bank, there is a record of all the polarizations and the corresponding serial numbers. On the bank note, the serial number is printed, but the polarizations are kept secret. Thus, whilst the bank can always verify the polarizations by measuring the polarization of each photon in the correct basis without introducing any disturbance, a would-be counterfeiter ignorant of the bases cannot create a copy of the photon polarization states, since even if he knows the two bases, if he chooses the wrong one to measure a photon, it will change the polarization of the photon in the trap, and the forged banknote created will be with this wrong polarization.

For each photon, the would-be counterfeiter has a probability $3/4$ of success in duplicating it correctly. If the total number of photons on the bank note is N, a duplicate will have probability $(3/4)^N$ of passing the bank's verification test. If N is large, this probability becomes exponentially small. The fact that a quantum state cannot be copied is ultimately guaranteed by its proof by the no-cloning theorem, which underlies the security of this system.

2.3.2 QKD par Bennett-Brassard (1984)

BB84[1] [2]is a quantum key distribution scheme developed by Charles Bennett and Gilles Brassard in 1984. It is the first quantum cryptography protocol.[3] The protocol is provably secure, relying on the quantum property that information gain is only possible at the expense of disturbing the signal if the two states one is trying to distinguish are not orthogonal (see no-cloning theorem). It is usually explained as a method of securely communicating a private key from one party to another for use in one-time pad encryption.[4]

Description [edit]

In the BB84 scheme, Alice wishes to send a private key to Bob. She begins with two strings of bits, a and b, each n bits long. She then encodes these two strings as a string of n qubits:

$$|\psi\rangle = \bigotimes_{i=1}^{n} |\psi_{a_i b_i}\rangle,$$

where a_i and b_i are the i-th bits of a and b respectively. Together, $a_i b_i$ give us an index into the following four qubit states:

$$\begin{aligned}
|\psi_{00}\rangle &= |0\rangle, \\
|\psi_{10}\rangle &= |1\rangle, \\
|\psi_{01}\rangle &= |+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle, \\
|\psi_{11}\rangle &= |-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle.
\end{aligned}$$

Note that the bit b_i is what decides which basis a_i is encoded in (either in the computational basis or the Hadamard basis). The qubits are now in states that are not mutually orthogonal, and thus it is impossible to distinguish all of them with certainty without knowing b.

Alice sends $|\psi\rangle$ over a public and authenticated quantum channel $\mathcal{E}$ to Bob. Bob receives a state $\mathcal{E}(\rho) = \mathcal{E}(|\psi\rangle\langle\psi|)$, where $\mathcal{E}$ represents both the effects of noise in the channel and eavesdropping by a third party we'll call Eve. After Bob receives the string of qubits, all three parties, namely Alice, Bob and Eve, have their own states. However, since only Alice knows b, it makes it virtually impossible for either Bob or Eve to distinguish the states of the qubits. Also, after Bob has received the qubits, we know that Eve cannot be in possession of a copy of the qubits sent to Bob, by the no-cloning theorem, unless she has made measurements. Her measurements, however, risk disturbing a particular qubit with probability ½ if she guesses the wrong basis.

Bob proceeds to generate a string of random bits b' of the same length as b and then measures the string he has received from Alice, a'. At this point, Bob announces publicly that he has received Alice's transmission. Alice then knows she can now safely announce b. Bob communicates over a public channel with Alice to determine which b_i and b'_i are not equal. Both Alice and Bob now discard the qubits in a and a' where b and b' do not match.

From the remaining k bits where both Alice and Bob measured in the same basis, Alice randomly chooses $k/2$ bits and discloses her choices over the public channel. Both Alice and Bob announce these bits publicly and run a check to see whether more than a certain number of them agree. If this check passes, Alice and Bob proceed to use information reconciliation and privacy amplification techniques to create some number of shared secret keys. Otherwise, they cancel and start over.

2.3.3 Intrication, téléportation et relais

Intrication. Soit deux Qubits.

$$|\psi\rangle_A = \alpha|0\rangle + \beta|1\rangle \qquad |\varphi\rangle_B = \gamma|0\rangle + \delta|1\rangle$$

Alors :

$$|\psi\rangle|\varphi\rangle_B = \alpha\gamma|00\rangle + \alpha\gamma|01\rangle + \beta\gamma|10\rangle + \beta\delta|11\rangle$$

$\neq |\phi^+\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$ car $\Rightarrow \alpha\gamma = 0$ et $\beta\gamma = 0$ mais on doit avoir $\alpha\gamma \neq 0$ et $\beta\delta \neq 0$.

Base de Bell. On a 4 états :

$$|\phi^\pm\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle) \qquad |\psi^\pm\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)$$

$|\phi^+\rangle_{AB}$, et soit un état $|\psi\rangle_{A'}$. Mesure de Bell sur AA'.

$$\begin{aligned}
&(\alpha|0\rangle_{A'} + \beta|1\rangle_{A'})(\frac{1}{\sqrt{2}}|00\rangle_{AB} + \frac{1}{\sqrt{2}}|11\rangle_{AB}) \\
&= \frac{1}{\sqrt{2}}\Big[\alpha|000\rangle + \beta|111\rangle + \alpha|011\rangle + \beta|100\rangle\Big] \\
&= \frac{1}{2}\Big[\alpha(|\phi^+\rangle + |\phi^-\rangle).|0\rangle + \beta(|\phi^+\rangle - \phi^-\rangle).|1\rangle + \alpha(|\psi^+\rangle + |\psi^-\rangle)|.1\rangle + \beta(|\psi^+\rangle - |\psi^-\rangle).|0\rangle\Big] \\
&\frac{1}{2}\Big(|\phi^+\rangle|\psi\rangle + |\phi^-\rangle\sigma_2|\psi\rangle + |\psi^+\rangle\sigma_X|\psi\rangle + |\psi^-\rangle\sigma_X\sigma_2|\psi\rangle\Big)
\end{aligned}$$

où $\sigma_Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ et $\sigma_X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

3 Computing on enciphered data (Elham Kashefi)

3.1 Contexte

$$f: \begin{cases} \{0,1\}^n & \longrightarrow & \{0,1\}^n \\ x & \longmapsto & f(x) \end{cases}$$

$f(x)$ but computing f is costly, so we need a server to do it, but we don't want it to know the data it's working on.

$$\begin{array}{ccc} \text{(cheap)} & & \text{(costly)} \\ \text{Client} & & \text{Server} \\ \varepsilon_K(x) & \longrightarrow & f(\varepsilon_K(x)) \\ K\text{secret know to client} & & \downarrow \\ D_K f(\varepsilon_K(x)) & \longleftarrow & \longleftarrow \end{array}$$

$D_f f(\varepsilon_k(x)) = f(D_K \varepsilon_K(x)) = f(x)$.

1. $\varepsilon(x)$ hiding
2. ε, D easy $\longrightarrow$ complexity independant of f.

Exemple. One-time pad

$$\varepsilon_r(m) = m \oplus r \qquad \varepsilon(m_1) \cdot \varepsilon(m_2) \neq \varepsilon(m_1 \cdot m_2)$$

Remarque. $\oplus$ réversible Any f can be dcomposed into addition and multiplication.

$$\begin{cases} m_1 \longrightarrow \varepsilon_{r_1}(m_1) \\ m_2 \longrightarrow \varepsilon_{r_2}(m_2) \end{cases} \longrightarrow \varepsilon(m_1) + \varepsilon(m_2) = \varepsilon(m_1 + m_2)$$

"Computing on the edge of chaos". Fully homorphic Encryption (FHE).
(1) Hiding :

- Computationnal $\leftarrow$ Some computationnal problem being assumed hard $\rightarrow$ indéchiffrable car calculs trop complexes
- Informationnal $\leftarrow$ no assumption

Impossibility of informationally secure FHE.

A simple FHE scheme
$N = PQ$, N integer. Cient $P, Q \longrightarrow N$, N becomes a public information ; P remains the client's keys.

- factoring is hard
- indistinguishability assumption

$$x \in \mathbb{Z}_N \qquad \text{vs} \qquad x = PQ + \theta \quad Q \in \mathbb{Z}_Q,\ \theta \in [,] \text{ then } \mathbb{Z}_p$$

cannot distinguish if x comes from a totally random process in $\mathbb{Z}_N$ or if the alea comes from a smaller space.

$$\varepsilon_P(m_1) = m_1 + PQ_1 + \theta_1 \mod N$$

With the same key : $\varepsilon_r(m_1) = m_1 + r$ and $\varepsilon_r(m_2) = m_2 + r$
$\Rightarrow$ $\varepsilon(m_1 + m_2) = m_1 + m_2$; no longer hidden.

Why hiding ? In "normal" one-time pad we use a random key in $\mathbb{Z}_N$. Here the key is random :

$$\underbrace{P}_{\text{fixed}} \cdot \underbrace{Q}_{\in \text{Rand}(\mathbb{Z}_Q)} + \underbrace{\theta_1}_{\in \text{Rand(small range)}}$$

Lets consider $\varepsilon(m_2) = m_2 + PQ_2 + \theta_2$, then :

$$\varepsilon(m_1) + \varepsilon(m_2) = (m_1 + m_2) + P(\underbrace{Q_1 + Q_2}_{\in \mathbb{Z}_Q}) + (\theta_1 + \theta_2) = \varepsilon(m_1, m_2)$$

$\theta_1 + \theta_2$ remains small if θ_1, θ_2 small enough.

$$D_{\theta,P}(Y) = Y - [Y/P]P - \theta \mod N$$

works if θ is small. Can we guarantee θ is small ?
If many multiplications $\longrightarrow$ θ range increases $\longrightarrow$ decryption doesn't work.
$\longrightarrow$ While hiding P, θ from server, make server to decrease θ : *boots trapping.*

$$\text{From } \varepsilon(m) = m + PQ + \theta \;\Rightarrow\; \varepsilon'(m) = m + PQ + \underbrace{\theta'}_{\text{smaller range}}$$

but huge overhead. It's an active research field.

3.2 Quantum Computing on encrypted data (Joe Fitzsimons)

161110107 on arxive.org

Motivations.

- Quantum computers are coming. 20−qbits machines exist $\longrightarrow$ 100−qbits would not be classicaly simulated. So soon we will have quantum devices that cannot be simulated classicaly.
- Possible application for machine learning, simulation (already requires some secrecy)
- Quantum testing : how do we know Q. Computer works correctly ?

3.2.1 Quantum computing simple gate

Rappel. a qbit

$$\begin{pmatrix}\alpha\\ \beta\end{pmatrix} = \alpha|0\rangle + \beta|1\rangle = \alpha\begin{pmatrix}1\\0\end{pmatrix} + \beta\begin{pmatrix}0\\1\end{pmatrix}$$

Tensor product :

$$\begin{pmatrix}\alpha_1\\ \beta_1\end{pmatrix} \otimes \begin{pmatrix}\alpha_2\\ \beta_2\end{pmatrix} \otimes \begin{pmatrix}\alpha_3\\ \beta_3\end{pmatrix} = \begin{pmatrix}\alpha_1\begin{pmatrix}\alpha_2\\ \beta_2\end{pmatrix}\\ \beta_1\begin{pmatrix}\alpha_2\\ \beta_2\end{pmatrix}\end{pmatrix} \otimes \begin{pmatrix}\alpha_3\\ \beta_3\end{pmatrix} = \begin{pmatrix}\alpha_1\alpha_2\alpha_3\\ \alpha_1\beta_2\alpha_3\\ \alpha_1\alpha_2\beta_3\\ \alpha_1\beta_2\beta_3\\ \beta_1\alpha_2\alpha_3\\ \beta_1\beta_2\alpha_3\\ \beta_1\alpha_2\beta_3\\ \beta_1\beta_2\beta_3\end{pmatrix}$$

$$(\alpha_1|0\rangle + \beta_1|1\rangle) \otimes (\alpha_2|0\rangle + \beta_2|1\rangle) = \alpha_1\alpha_2|00\rangle + \alpha_1\beta_2|01\rangle + \beta_1\alpha_2|10\rangle + \beta_1\beta_2|11\rangle$$

$$\underbrace{\begin{pmatrix} a & b \\ c & d \end{pmatrix}}_{\text{unitary}} \underbrace{\begin{pmatrix} \alpha \\ \beta \end{pmatrix}}_{\text{qbit}} = \underbrace{\begin{pmatrix} \alpha' \\ \beta' \end{pmatrix}}_{\text{qbit}}$$

$UU^T = I$

Exemples.

- $$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

  $H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

- $\forall \alpha \in [0, 2\pi]$,

  $$J(\alpha) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & e^{i\alpha} \\ 1 & -e^{i\alpha} \end{pmatrix}$$

  For any 2×2 unitary Y matrix, $\exists \alpha, \beta, \gamma, \theta$ can be written as

  $$U(\alpha, \beta, \gamma, \theta) = e^{i\theta} J(\alpha) J(\beta) J(\gamma)$$

- 4×4 :

  $$\Lambda Z = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

  $$\Lambda Z(H_1 \otimes H_2)|0\rangle|0\rangle = \Lambda Z \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + |1\rangle}{\sqrt{2}} \right)$$

  $$\Lambda Z \begin{array}{rcl} |00\rangle & = & |00\rangle \\ |01\rangle & = & |01\rangle \\ |10\rangle & = & |10\rangle \\ |11\rangle & = & -|11\rangle \end{array}$$

  $$\frac{1}{2}\Lambda Z(|00\rangle + |01\rangle + |10\rangle + |11\rangle)\frac{1}{2}(|00\rangle + |01\rangle + |10\rangle - |11\rangle)$$

  entangled, i.e. cannot be written as $|\psi_1\rangle \otimes \psi_2$

Universal gate set. ΛZ, $J(\alpha)$, i.e. any $U_{2^n \times 2^n}$ can be decomposed using $\otimes$ as a sequence of $\Lambda Z, J(\alpha)$

3.2.2 Quantum computation

data	$\longrightarrow$	qbits
gate	$\longrightarrow$	unitary
composition	$\longrightarrow$	$\otimes$
read out data	$\longrightarrow$	Measurement

Single qbit projective measurement is defined using an orthonormal basis for $\mathbb{C}^2$. Given basis $|\psi_1\rangle, |\psi_2\rangle$, to implement $M^{\{|\psi_1\rangle, |\psi_2\rangle\}}$ over an input quantum state $|\mathcal{S}\rangle$ we apply the projection to :

$$\begin{cases} |\langle\psi_1|\mathcal{S}\rangle|^2 & |\psi_1\rangle \\ |\langle\psi_2|\mathcal{S}\rangle|^2 & |\psi_2\rangle \end{cases}$$

Exercice. $|\mathcal{S}\rangle = \begin{pmatrix}\alpha\\ \beta\end{pmatrix} = \alpha|0\rangle + \beta|1\rangle$. Basis $\begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix}$. $M^{\{|0\rangle,|1\rangle\}}|\mathcal{S}\rangle$?

$$\begin{cases} |\langle 0|\mathcal{S}\rangle|^2 & |0\rangle \\ |\langle 1|\mathcal{S}\rangle|^2 & |1\rangle \end{cases}$$

As,

$$\langle 0|\mathcal{S}\rangle = \begin{pmatrix}1\\0\end{pmatrix}^T \begin{pmatrix}\alpha\\ \beta\end{pmatrix} = \begin{pmatrix}1 & 0\end{pmatrix} \begin{pmatrix}\alpha\\ \beta\end{pmatrix} = \alpha$$

$$\langle 1|\mathcal{S}\rangle = \begin{pmatrix}0\\1\end{pmatrix}^T \begin{pmatrix}\alpha\\ \beta\end{pmatrix} = \begin{pmatrix}0 & 1\end{pmatrix} \begin{pmatrix}\alpha\\ \beta\end{pmatrix} = \beta$$

Then,

$$\begin{cases} |\langle 0|\mathcal{S}\rangle|^2 = |\alpha|^2 & |0\rangle \\ |\langle 1|\mathcal{S}\rangle|^2 = |\beta|^2 & |1\rangle \end{cases}$$

$\varepsilon_K(m) = m + K \quad \varepsilon(m_1) + \varepsilon(m_2) = \varepsilon(m_1 + m_2)$

How to hide $J(\alpha)$ from server ?

$$\begin{array}{ccc} \text{Client} & & \text{Q.Server} \\ \alpha & \longrightarrow & J(\alpha)|\mathcal{S}\rangle \\ \text{secret} & \longleftarrow & J(\alpha)|\mathcal{S}\rangle \end{array}$$

Assumption : $|\mathcal{S}\rangle = |0\rangle + |1\rangle$.

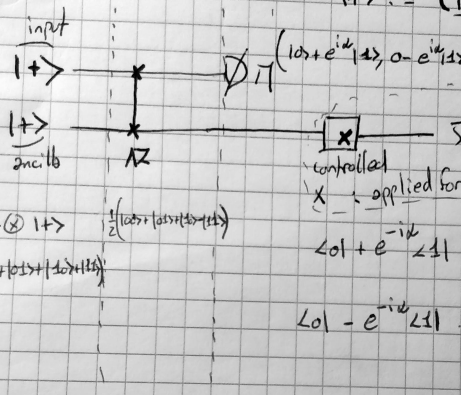
$$\begin{array}{ccc} \text{Client} & & \text{Q.Server} \\ \alpha & \longrightarrow & M^{\{|0\rangle,|1\rangle\}} J(\alpha)(|0\rangle + |1\rangle)\ (*) \\ \text{secret} & \longleftarrow & \end{array}$$

$*$: must compute it without knowing α.

How to hide $S(\alpha)$ from Server?

Client: α (secret) ⟶ QServer $\{|0\rangle,|1\rangle\}$: $\Pi\ S(\alpha)(|0\rangle+|1\rangle)$: must compute it without knowing α.

$$|+\rangle := \frac{(|0\rangle+|1\rangle)}{\sqrt{2}}$$



$$X=\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$$

$|+\rangle\otimes|+\rangle = \frac{1}{2}(|00\rangle+|01\rangle+|10\rangle+|11\rangle)$; $\frac{1}{2}(|00\rangle+|01\rangle+|10\rangle-|11\rangle)$

$$\langle 0|+e^{-i\alpha}\langle 1| \longrightarrow \begin{cases} (|0\rangle+e^{i\alpha}|1\rangle)\otimes(|0\rangle+|1\rangle+e^{-i\alpha}|0\rangle-e^{-i\alpha}|1\rangle) \\ \quad = (1+e^{-i\alpha})|0\rangle+(1-e^{-i\alpha})|1\rangle \ ; s=0 \text{ with probability } \frac{1}{2} \\ (1-e^{-i\alpha})|0\rangle+(1+e^{i\alpha})|1\rangle \ ; s=1 \text{ with probability } \frac{1}{2} \end{cases}$$

$$\langle 0|-e^{-i\alpha}\langle 1| \longrightarrow$$

In any case, we get $s=0$ i.e. $S(\alpha)|+\rangle$ after controlled X.

Let's introduce $P(\theta)=\begin{bmatrix}1 & 0\\ 0 & e^{i\theta}\end{bmatrix}$; $P(\theta)P(-\theta)=Id$.

i.e. $(\text{controlled } X)\,\Pi^{|+\alpha\rangle,|-\alpha\rangle}\,\Lambda Z(|+\rangle\otimes|+\rangle) = (\text{controlled } X)\,\Pi^{|+\alpha\rangle,|-\alpha\rangle}\,P(\theta)P(-\theta)\,\Lambda Z(|+\rangle\otimes|+\rangle)$ ①

$P(-\theta)\otimes Id$ implicitly to match ΛZ's dimensions

Or, $P(-\theta)$ and ΛZ are diagonal, hence commute.

① $= (\text{controlled } X)\,\Pi^{|+\alpha\rangle,|-\alpha\rangle}\,P(\theta)\,\Lambda Z((P(-\theta)|+\rangle)\otimes|+\rangle) = (\text{controlled } X)\,\Pi^{|+_{\alpha+\theta}\rangle,|-_{\alpha+\theta}\rangle}\,\Lambda Z(|+_\theta\rangle\otimes|+\rangle)$