Secure Key Distribution

ASSUMPTIONS

Perfectly/Indistinguishably Random Key Generators

$$Adv_{PRG}[A, G] = \left| \Pr_{k \xleftarrow{R} K}[A[G(k)] = 1] - \Pr_{r \xleftarrow{R} \{0,1\}^n}[A(r) = 1] \right| \leqslant 1/2^{80}$$

Perfect/Unbreakable within life cycle Encryption

Modular Arithmetic

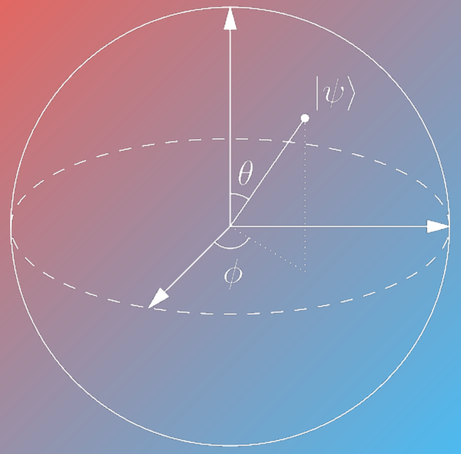
$$m \equiv c \bmod p$$

Classical Crypto

$$(g^a)^b \equiv (g^b)^a$$

Classical Attacks

Quantum Crypto



Quantum Attacks

State of Quantum

KMB09

Modular Arithmetic

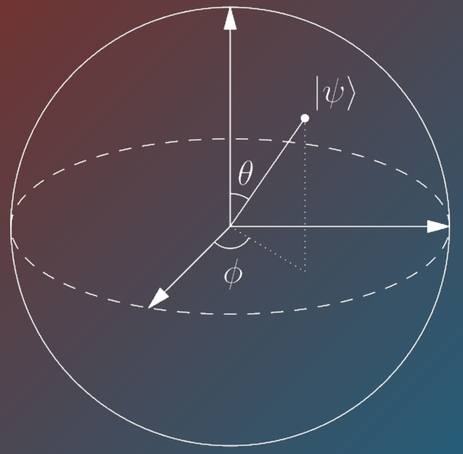
$$m \equiv c \bmod p$$

Classical Crypto

$$(g^a)^b \equiv (g^b)^a$$

Classical Attacks

Quantum Crypto



Quantum Attacks

State of Quantum

KMB09

MODULAR ARITHMETIC

Preliminary

Addition $a \pm b \bmod n = [a \bmod n \pm b \bmod n] \bmod n$

Multiplication $a \times b \bmod n = [a \bmod n \times b \bmod n] \bmod n$

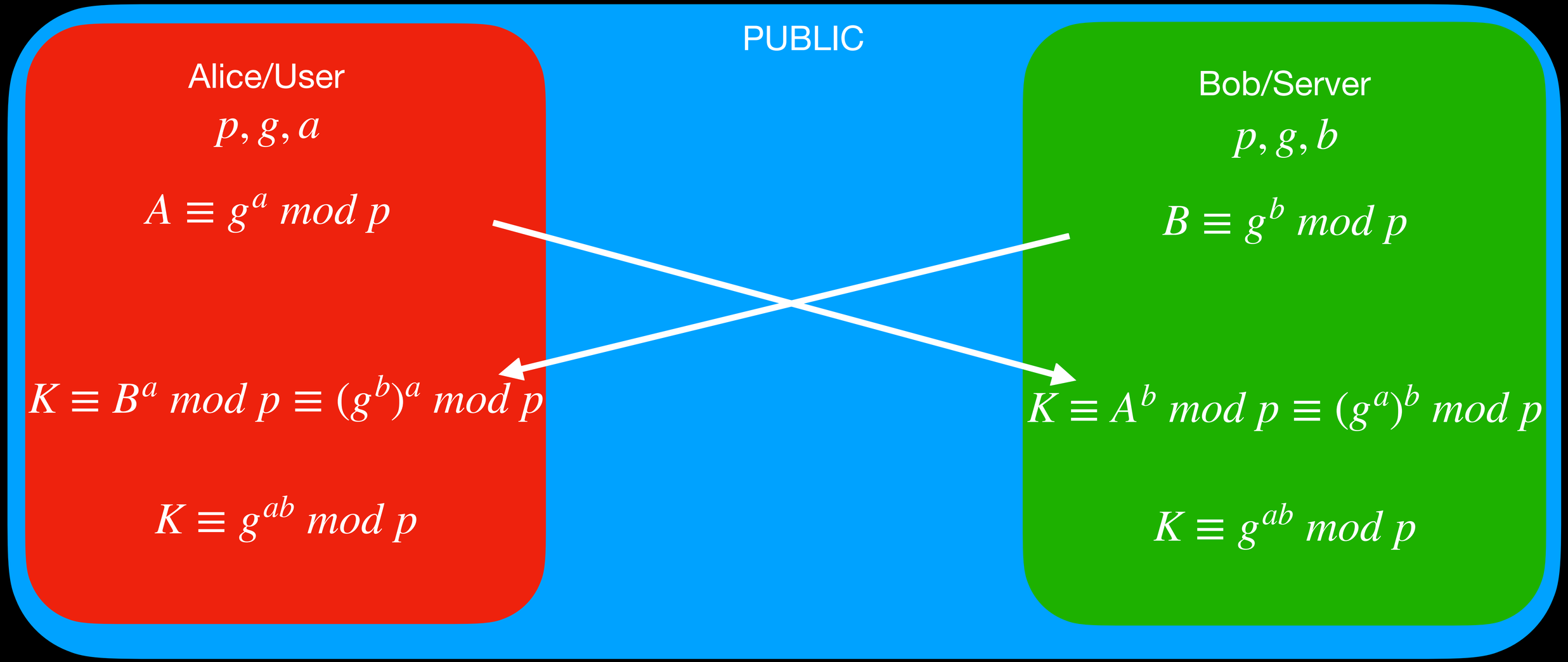
Division $\frac{a}{k} \equiv \frac{b}{k} \bmod \frac{n}{gcd(n,k)}$

Exponents $p^k \equiv q^k \bmod n$

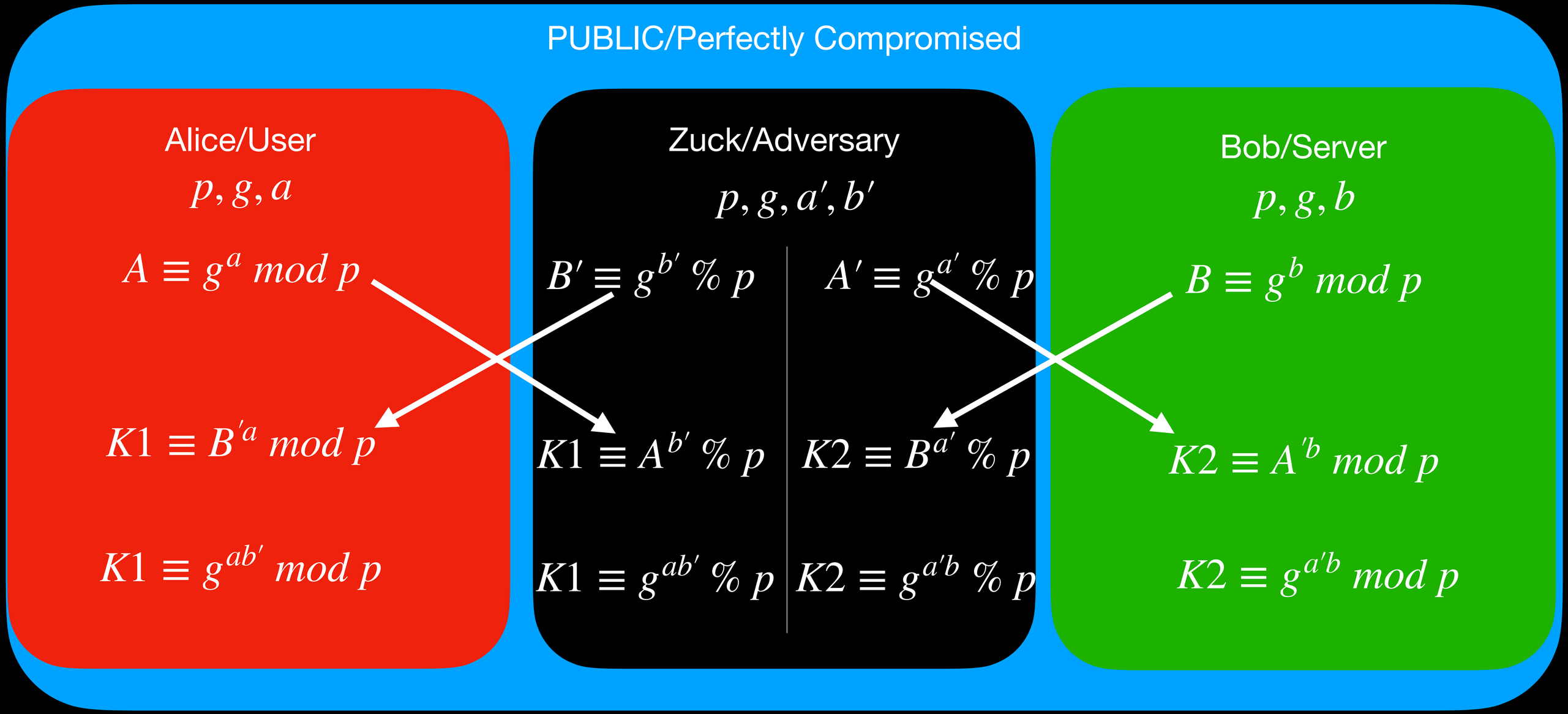
Chaining $m \bmod n \equiv (m \bmod n) \bmod n$

Classical Crypto

Diffie-Hellman Protocol



DH Man-in-Middle



Other Classical Attacks

- Logjam attack allows a man-in-middle to downgrade vulnerable TLS connections to 512-bit export-grade cryptography. This allows the attacker to read/write all data passed over the connection. Servers affected support DHE_EXPORT ciphers and ALL modern web browsers are affected.
- Prime Numbers are a rare commodity. Tests on 512-bit primes on TLS show that Logjam can be used to downgrade connections to 80% of TLS servers supporting DHE_EXPORT.
- It is further estimates that an academic team can break 768-bit and a state can break 1024-bit. About 20% web servers, more than half VPN servers and about a third SSH servers can therefore be compromised.
- Learn Logjam *https://www.youtube.com/watch?v=VHOrGWyGeww*

Other Classical Attacks

- Information theory, sha256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 string for typical extange
- Classically redundancy is done in the stream cipher encc stage and usually not in the key distribution stage.
- If anything is needed the HTTP protocol does MD5 hash and does it intrinsically.

Modular Arithmetic

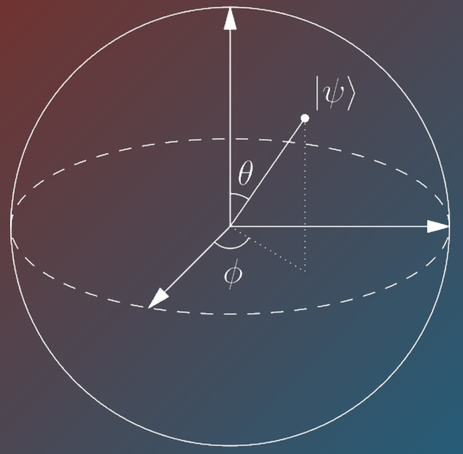
$$m \equiv c \bmod p$$

Classical Crypto

$$(g^a)^b \equiv (g^b)^a$$

Classical Attacks

Quantum Crypto



Quantum Attacks

State of Quantum

KMB09

Modular Arithmetic

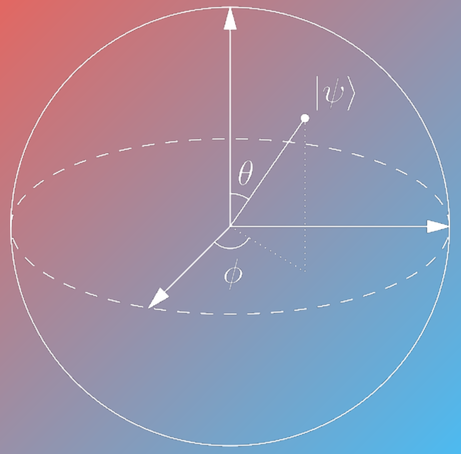
$$m \equiv c \bmod p$$

Classical Crypto

$$(g^a)^b \equiv (g^b)^a$$

Classical Attacks

Quantum Crypto



Quantum Attacks

State of Quantum

KMB09

$\mathcal{H}$

Preparation

ρ

Channel

$\mathcal{E}$

Linear, Completely Positive, Trace Preserving Map

Measure

M

Kraus Decomposition

For Channel $\varepsilon : \mathcal{B}(\mathcal{H}_A) \rightarrow \mathcal{B}(\mathcal{H}_B)$

$$\varepsilon(\rho_A) = \sum_{j=1}^{d} K_j \rho_A K^{\dagger}{}_j$$

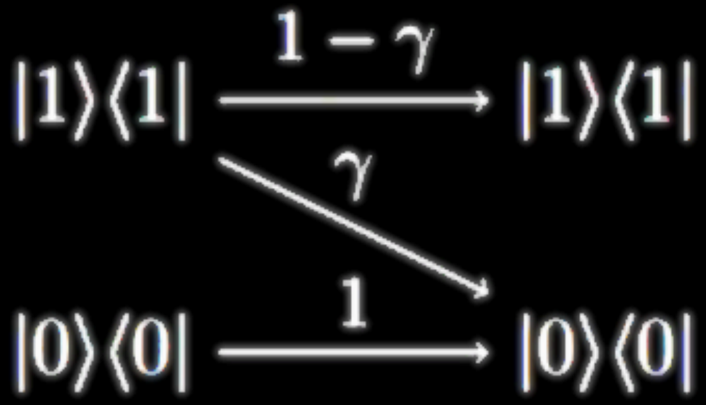
Where

$$K_j : \mathcal{H}_A \rightarrow \mathcal{H}_B \forall\, j \in \{1,2...,d\}$$

With

$$d \leq dim(\mathcal{H}_A) dim(\mathcal{H}_B)\ and\ \sum_{j=1}^{d} K_j K^{\dagger}{}_j = \mathbb{I}_A$$

Example: Amplitude damping channel; $0 \leq \gamma \leq 1$



Kraus operators:

$$K_1 = \sqrt{\gamma}|0\rangle\langle 1| \longrightarrow K_1|1\rangle\langle 1|K_1^\dagger = \gamma|0\rangle\langle 0|$$
$$K_2 = |0\rangle\langle 0| + \sqrt{1-\gamma}|1\rangle\langle 1|.$$

$$\Rightarrow K_1^\dagger K_1 + K_2^\dagger K_2 = \mathbb{I}.$$

PS: In a unitary evolution, the Unitary Operator itself is a Kraus Operator

QKD PROTOCOLS

PREPARE AND MEASURE

ENTANGLEMENT BASED

CLASSICAL POST PROCESSING

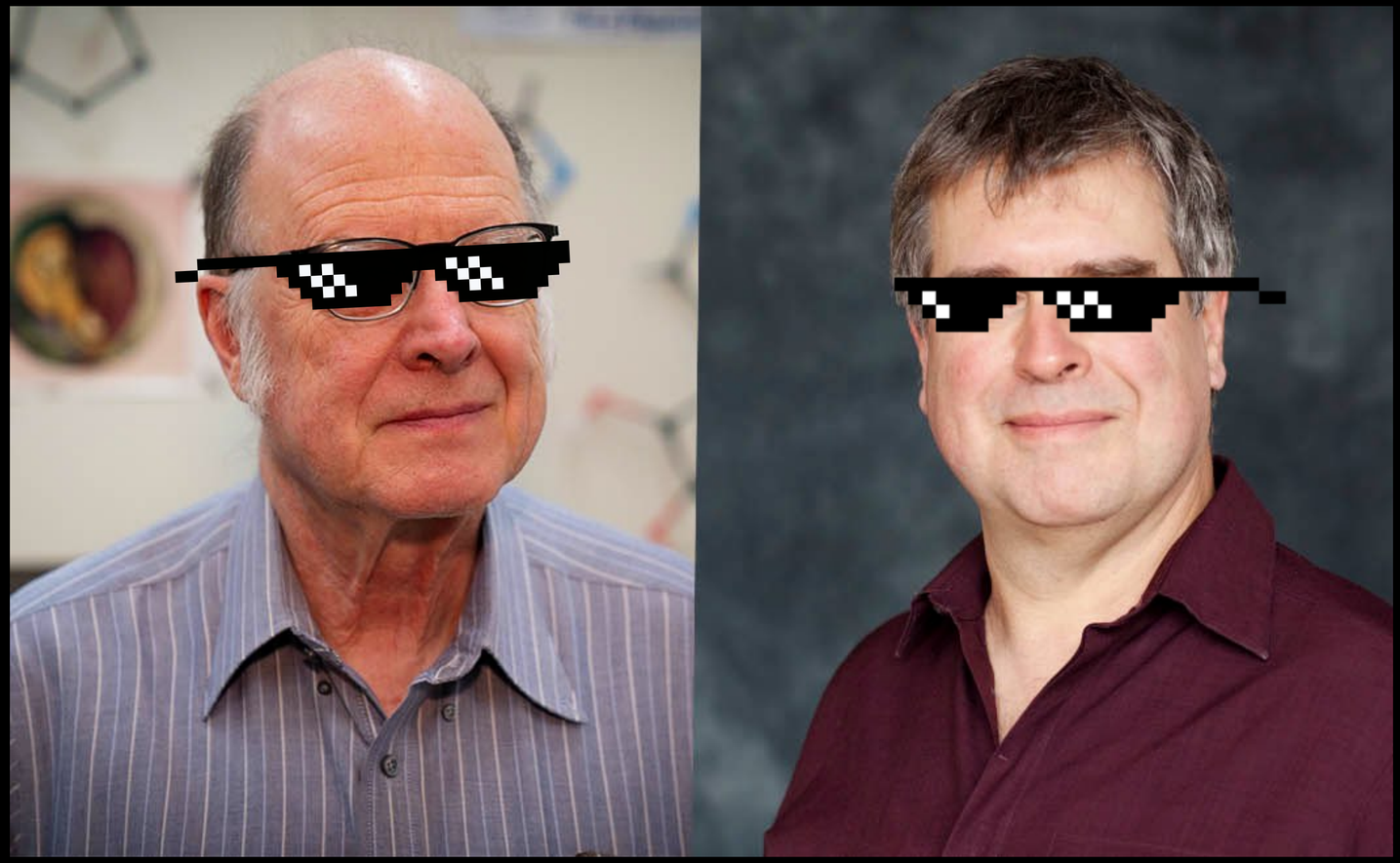
QKD PROTOCOLS

PREPARE AND MEASURE

ENTANGLEMENT BASED

CLASSICAL POST PROCESSING

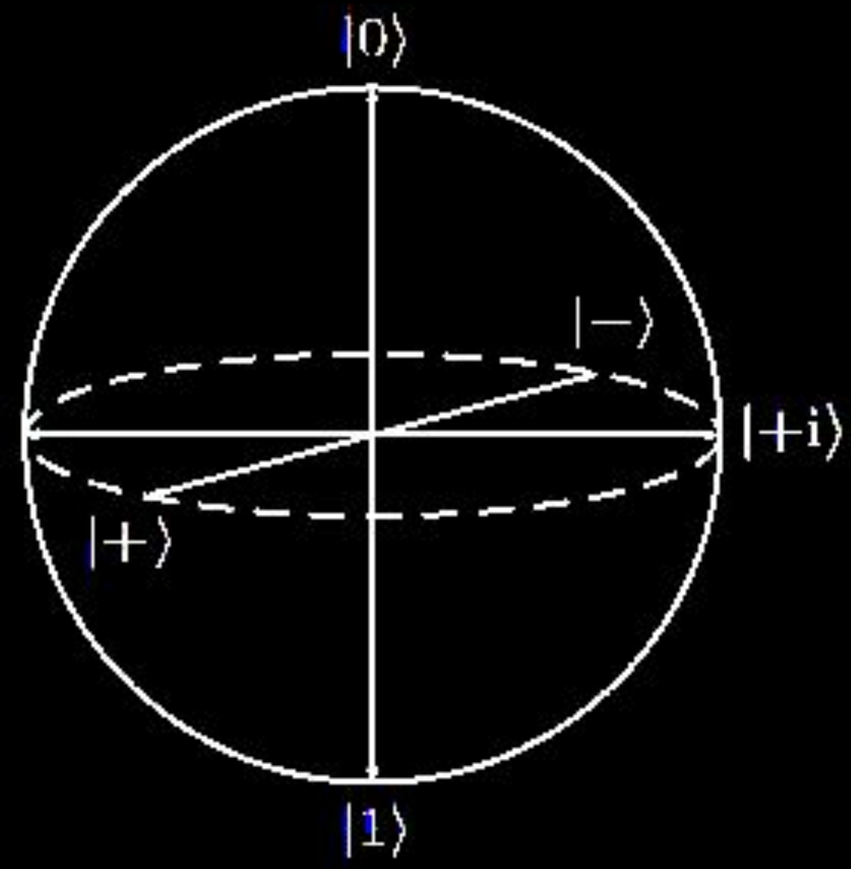
BB84 Begins



Charles Bennet and Giles Brassard

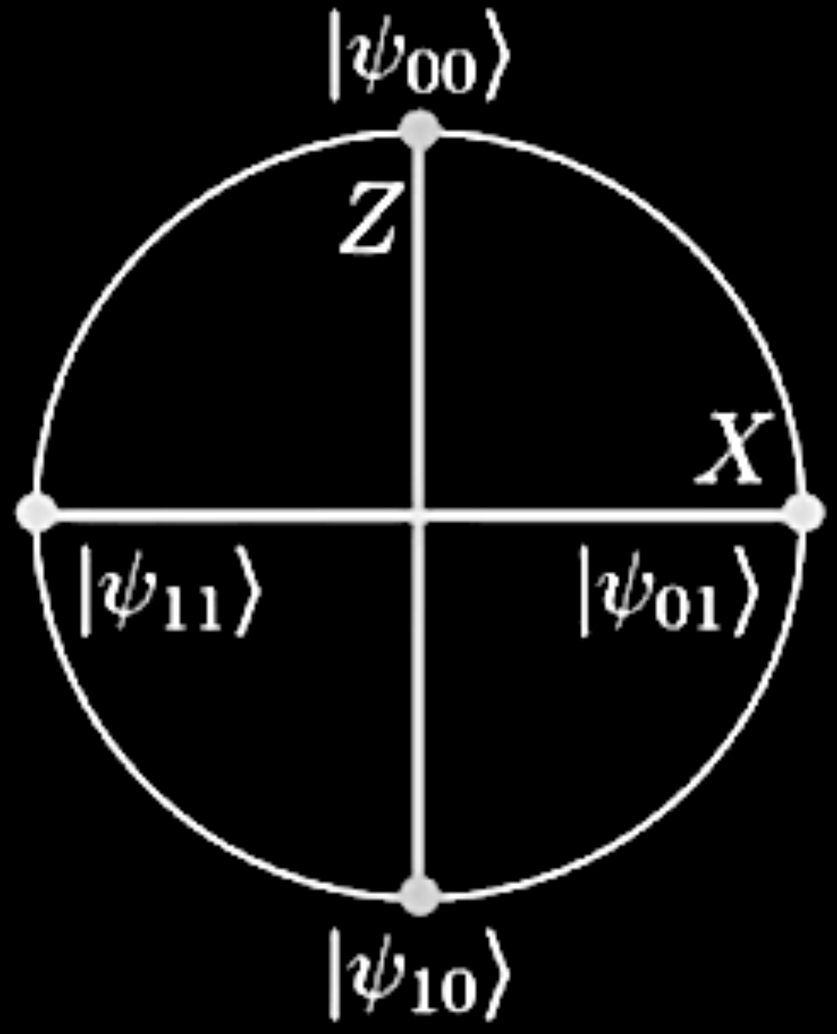
Six State Protocol

- The BB84 uses only 2 bases spanning a plane in the sphere
- With 6-State spans the entire sphere
- This increases bobs chance of error from ½ to ⅔ but also reduces eves chances of correct bases. A consequence I that more bits need to be discarded
- Overall the secret key rate of 6-State>BB84 (from analysis over large cases)
- All steps are same as BB84



PNS Attack & SARG04

- Only sifting step is different
- Say Alice has State |ψ00>
- AFTER bob makes measurement she announces a pair |ψ00> & |ψ01>, notes 0 (C Basis) as key bit.
- Case: Computational Basis
  - If he gets |ψ00> then INVALID
  - Since Z basis and X basis are indistinguishable
- Case: Hadamard Basis
  - If |ψ01> then INVALID
  - Since Z and X basis are indistinguishable
  - Only |ψ11> is VALID since it => |ψ00> ONLY



QKD PROTOCOLS

PREPARE AND MEASURE

ENTANGLEMENT BASED

CLASSICAL POST PROCESSING

QKD PROTOCOLS

PREPARE AND MEASURE

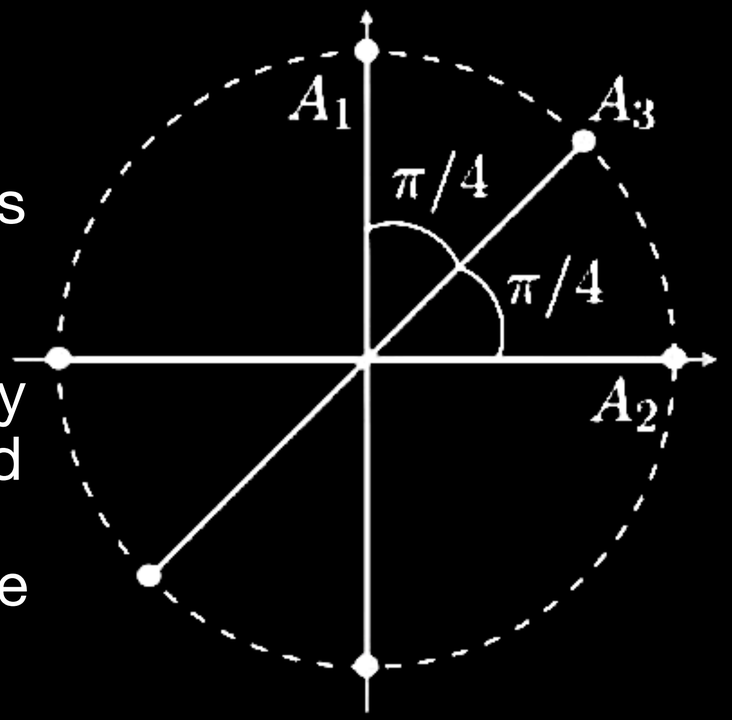
ENTANGLEMENT BASED

CLASSICAL POST PROCESSING

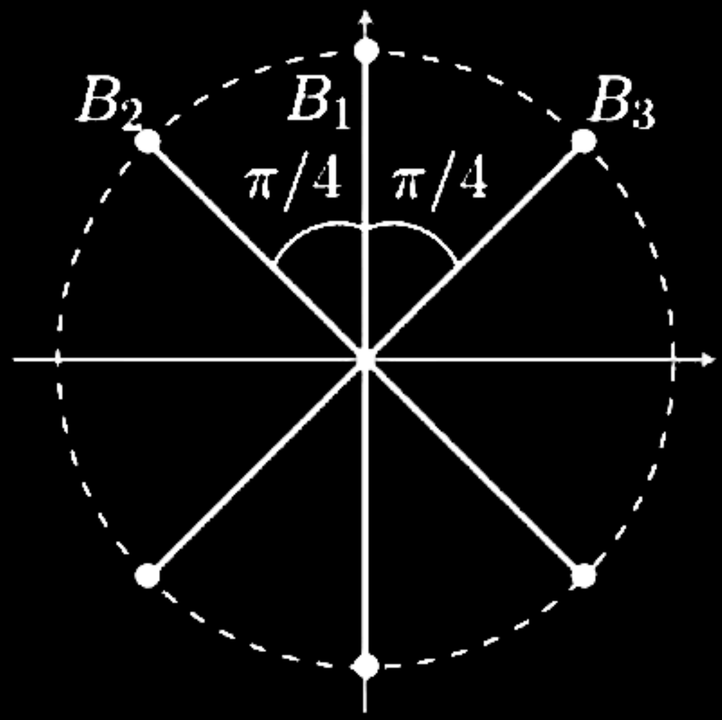
Ekert Protocol

- KeyGen may be under adversary's control
- If Eve tampers then by monogamy states will not be maximally mixed
- Since bases are anti correlated we chose key bases and test bases

Alice



Bob



$$A_1 = Z.$$

$$A_2 = X.$$

$$A_3 = \frac{1}{\sqrt{2}}(Z + X).$$

$$B_1 = Z.$$

$$B_2 = \frac{1}{\sqrt{2}}(Z - X).$$

$$B_3 = \frac{1}{\sqrt{2}}(Z + X).$$

Maximally Mixed State Generated

$$|\Psi^-\rangle_{AB} = \frac{1}{\sqrt{2}}(|01\rangle_{AB} + |10\rangle_{AB})$$

Primary State

Ekert Protocol

Testing Info Leak with CHSH

Classical

Four classical random variables: $A_1,\ A_2,\ B_3,\ B_2$

Realizations: $+1,\ -1$

$$A_1(B_3 + B_2) + A_2(B_3 - B_2) = \pm 2$$

$$|\langle A_1(B_3 + B_2) + A_2(B_3 - B_2)\rangle| \leq 2$$

$$S := |\langle A_1 B_3\rangle + \langle A_1 B_2\rangle + \langle A_2 B_3\rangle - \langle A_2 B_2\rangle| \leq 2$$

Quantum

Quantum observables: $A_1,\ A_2,\ B_3,\ B_2$

Expectation value:

$$\langle A_i B_j\rangle = \mathrm{Tr}\,(A_i \otimes B_j \rho)$$

Example for Ekert protocol:

$A_1 = Z,\ B_3 = \frac{1}{\sqrt{2}}(Z + X),\ \rho = |\Psi^-\rangle\langle\Psi^-|$

$$\langle A_1 B_3\rangle = \langle\Psi^-| Z \otimes \frac{1}{\sqrt{2}}(Z + X)\,|\Psi^-\rangle = -\frac{1}{\sqrt{2}}$$

Calculate CHSH value S:

$$S = |\langle A_1 B_3\rangle + \langle A_1 B_2\rangle + \langle A_2 B_3\rangle - \langle A_2 B_2\rangle| = 2\sqrt{2}$$

Ekert Protocol

Process

- A and B distribute a certain amount of Primary States between themselves.
- For each state A and B randomly choose a measurement from sets {Ai}, {Bi}
- A and B announce their bases for each measurement. The result pairs A1B1 and A3B3 form the sifted key and all other pairs are used to check CHSH
- Error Correction and Privacy Amplification

The BB84 Rises

You either die a hero, or get studied long enough to see yourself become entangled

- Alice Created 2n qubit pairs in maximally entangled state say Phi+
- She randomly selects n of these to be later used in error estimation
- Batman fans please don’t come after me
- A selects a random classical bit string ‘b’ of len 2n and if bi = 1 applies H transform to her half of corresponding qubit pair.
- She sends the other half of all qubit pairs to B and announces b and the positions of check qubits
- Bob applies H transform for all bi = 1

The BB84 Rises

Error Correction

- A & B measure the check Qubits in C basis and estimate errors. If more than some ’t’ (we’ll come back to this) errors occur then ABORT.
- If <t errors then they use CSS code built from C1 and C2 correction scheme to correct errors in remaining n bits and get perfectly entangled len m key.
- They measure m qubit phi+ in C basis and therefore get the shared secret key

- CSS is Calderbank-Shor-Steane Code:
- Assume for now it is given (details in Classical Post Processing) such that it encodes n qubites into m qubits and corrects upto t errors.
- C1 and C2 are classical error correction codes

Information reconciliation and privacy amplification[edit]

The quantum key distribution protocols described above provide Alice and Bob with nearly identical shared keys, and also with an estimate of the discrepancy between the keys. These differences can be caused by eavesdropping, but also by imperfections in the transmission line and detectors. As it is impossible to distinguish between these two types of errors, guaranteed security requires the assumption that all errors are due to eavesdropping. Provided the error rate between the keys is lower than a certain threshold (27.6% as of 2002[7]), two steps can be performed to first remove the erroneous bits and then reduce Eve's knowledge of the key to an arbitrary small value. These two steps are known as **information reconciliation** and **privacy amplification** respectively, and were first described in 1992.[8]

Information reconciliation is a form of error correction carried out between Alice and Bob's keys, in order to ensure both keys are identical. It is conducted over the public channel and as such it is vital to minimise the information sent about each key, as this can be read by Eve. A common protocol used for information reconciliation is the **cascade protocol**, proposed in 1994.[9] This operates in several rounds, with both keys divided into blocks in each round and the parity of those blocks compared. If a difference in parity is found then a binary search is performed to find and correct the error. If an error is found in a block from a previous round that had correct parity then another error must be contained in that block; this error is found and corrected as before. This process is repeated recursively, which is the source of the cascade name. After all blocks have been compared, Alice and Bob both reorder their keys in the same random way, and a new round begins. At the end of multiple rounds Alice and Bob have identical keys with high probability; however, Eve has additional information about the key from the parity information exchanged. However, from a coding theory point of view information reconciliation is essentially source coding with side information, in consequence any coding scheme that works for this problem can be used for information reconciliation. Lately turbocodes,[10] LDPC codes[11] and polar codes[12] have been used for this purpose improving the efficiency of the cascade protocol.

Privacy amplification is a method for reducing (and effectively eliminating) Eve's partial information about Alice and Bob's key. This partial information could have been gained both by eavesdropping on the quantum channel during key transmission (thus introducing detectable errors), and on the public channel during information reconciliation (where it is assumed Eve gains all possible parity information). Privacy amplification uses Alice and Bob's key to produce a new, shorter key, in such a way that Eve has only negligible information about the new key. This can be done using a universal hash function, chosen at random from a publicly known set of such functions, which takes as its input a binary string of length equal to the key and outputs a binary string of a chosen shorter length. The amount by which this new key is shortened is calculated, based on how much information Eve could have gained about the old key (which is known due to the errors this would introduce), in order to reduce the probability of Eve having any knowledge of the new key to a very low value.