Quantum Entropy Expansion and Propagation Overview

Technical white paper

February 15, 2020

Originally published December 20th, 2019

quantropi.com

Executive Summary

This white paper provides a technical explanation of Quantropi's Quantum Entropy Expansion and Propagation (QEEP) technology. Please visit Quantropi's website at https://www.quantropi.com for more information.

Quantropi's QEEP allows for the generation and secure exchange of ultra-high entropy cryptographic keys to secure application-layer communication links and to securely encrypt data with FIPS 140-2 compliant cryptographic algorithms, as well as the One-Time-Pad.

The QEEP technology, patented by Quantropi in 2019, uses quantum permutation gates. QEEP uses these quantum gates to concentrate a high level of entropy (up to 1,000,000 bits) and release that entropy to given inputs, in turn rendering these inputs indistinguishable from truly random.

This document gives an overview of the QEEP technology. For more information about its use in applications such as Quantropi's QRNG, QKD, and QOTP, please refer to our website and other white paper resources.

Terms

Cryptography

Key — A piece of information that determines the functional output of a cryptographic algorithm. For encryption algorithms, a key specifies the transformation of plaintext data into ciphertext. A key is not synonymous with 'password', although a key can be derived from a password via a Key-Derivation-Function (**KDF**).

Key Exchange — The process by which cryptographic keys are exchanged between two parties, allowing the use of a cryptographic algorithm, for instance to create a secure communication channel.

Entropy — A measure of the number of ways in which a system may be arranged, or information uncertainty — typically measured in **bits**.

Asymmetric Algorithm — A cryptographic system that uses pairs of keys: public keys that can be distributed widely, and private keys which are known only to the owner. Asymmetric algorithms are commonly applied to solve the key-exchange problem, e.g., via the Diffie-Hellman protocol, or public-key-infrastructure (**PKI**). Examples for asymmetric algorithms are **RSA**, **ECC**, or **ED25519**.

Symmetric Algorithm — A cryptographic system that uses the same key for encryption of plaintext data and decryption of ciphertext data. Commonly used to encrypt the communication channel, and requires either a pre-shared secret, or a key exchange to have taken place prior to starting the communication. Examples of symmetric algorithms are **AES**, **RC4**, or **3DES**.

Perfect Secrecy — The condition that a ciphertext C contains absolutely no additional information about a plaintext M. Thus every possible M is equally likely correct. Perfect secrecy provides the upper bound of information theoretical security.

One-Time-Pad — A cryptographic algorithm that cannot be cracked: it provides mathematically provable perfect secrecy. A given plaintext data M is combined with a true random key K via modular addition (**XOR**). Needs truly random keys to satisfy perfect secrecy requirements, and also requires secure exchange of the OTP keys.

Quantum Key Distribution

BB84 — A protocol to mutually agree on a measurement basis to select random measurement outcomes.

QBER — The **Qubit** Error Rate, a statistical measure that allows to determine whether an attacker is eavesdropping on the key exchange.

PSK — The pre-shared secret that provides mutual authentication for the two parties participating in the quantum key exchange.

Quantum Computing

Qubit — The basic unit of quantum information. Physically a two-state quantum-mechanical system that allows for coherent superpositions of states simultaneously.

Superposition — A fundamental principle of quantum mechanics describing that two or more quantum states can be added together (superposed) and the result is another valid quantum state. Mathematically, the linear combinations of solutions to the Schroedinger equation.

Eigenstate — Represents the physical state of a **qubit** quantum system, and has two attributes: an **eigenvector** and an **eigenvalue**.

Eigenvector — A bit-string represented in Dirac notation that describes the orthonormal basis of the (quantum-representation) of the system, i.e. the unit vectors of the Hilbert space.

Eigenvalue — The decimal value of each bit-string associated with an **eigenvector**, represents the information value of the **eigenstate**.

System Hamiltonian — An operator defined by the Schroedinger equation that acts on a given eigenvector to obtain the eigenvalue of the quantum system.

Perturbator — An operator acting on the **eigenstate** of a quantum system to change that **eigenstate**, i.e., an operator that adds change to a quantum system.

Quantum Gate — The building blocks of quantum computers. Quantum-mechanically they are **perturbators** to the **qubit** quantum system, and practically allow us to make calculations with quantum computers.

Introduction

With current rapid advancements towards main-stream quantum computing technology in line with IBM's 2018 predictions of quantum-computing industry viability within 5 years, as well as Google's 2019 achievement of Quantum Supremacy, we are getting close to being able to solve complex mathematical problems that would take classical super-computers hundreds of thousands of years to work through.

At the same time, intractable (it is possible to find a solution, but would take an impractical amount of time to do so) mathematical puzzles form the basis for today's cryptographic algorithms protecting information secrecy, privacy and integrity. These puzzles are trivially solvable with quantum computers. Together with our increasing economic and social dependency on data and the communication networks to transmit that data, quantum computers pose a significant existential threat to modern society.

1. NIST-IR 8105, last accessed February 2020, https://doi.org/10.6028/NIST.IR.8105
2. K. Svore, “Quantum Computing: Transforming the Digital Age”, Quantum Optimization Workshop, 2014.

The immediate need to find solutions that address and mitigate the quantum threat was highlighted in a status report on Post-Quantum Cryptography by the Computer Security Resource Center at the National Institute of Standards and Technology (NIST CSRC), urging individuals, enterprises and governments to begin preparing their information systems today to being able to resist the imminent adoption of quantum computing.[1]

Protecting Against the Quantum Threat

The quantum threat’s most immediate impact will be on current mechanisms of securing communication channels. These channels rely on establishing cryptographic keys between two parties who wish to communicate over the channel. To provide quantum-security, these keys must be of high entropy, and the key-exchange needs to be carried out securely. Unfortunately, the key generation and exchange mechanisms in place today are no challenge for even modest quantum computers: a study published by Microsoft Research[2] predicts that it would take a quantum computer less than 100 seconds to recover the key and thus break the communication link.

Currently proposed solutions to mitigating the quantum threat fall into two main categories:

1. **Post-Quantum Cryptography** — the development of new cryptographic algorithms that even quantum computer cannot compute a solution for in practical time.

2. **Quantum Key Distribution** — the use of quantum systems, such as photons, to protect data encoded into the systems against measurement.

These solutions have significant shortcomings with respect to practicality, maturity, and commercial viability for wide-spread adoption at scale.

We Are Here To Help

Quantropi was founded to accelerate the adoption of quantum-secure technologies today, and to fill the void of commercially viable technology solutions that provide a low-friction upgrade and integration path to make today’s existing information systems and network infrastructure quantum-secure.

By harnessing the power of quantum mechanics, we are not only building solutions that make communication networks quantum secure, but also more efficient at a reduced energy footprint.

Building the Quantum Internet

At Quantropi, we believe that as we step into the era of ubiquitous digital technology where our economies are driven by the creation of data, the communication of that data, as well as technologies such as machine learning and artificial intelligence to distill and act on insights derived from the data, the need for highly secure communication networks that protect information secrecy, privacy and integrity against actors with access to quantum computing technology will become as much of a foundational element for our societies, as access to clean water and food.

Our technology solutions are founded on the principle that one can only counter the quantum threat with quantum. However, the applications and integrations of these quantum technologies need to be applied in an evolutionary approach: after 50+ years of technology investments and building up the existing communication networks and information systems, it is highly irrational to think that we can rip out and replace what already exists: instead we advocate solutions that can work and integrate with existing infrastructure and systems to protect them against the quantum threat and ultimately bring about the Quantum Internet.

Quantum Entropy Expansion and Propagation

Within the context of quantum-safe communication, both **QKD** and **PQC** try to solve the problem of **key exchange** - that is establishing a cryptographic key between two parties *Alice* and *Bob* in such a way that a third party, *Eve*, cannot know the key even under the assumption that Eve has access to a quantum computer.

Post-Quantum Cryptography aims at distributing the key securely from *Alice* to *Bob* by transforming the key information in such a way that it would take even a quantum computer an impractical amount of time to recover the correct transformation. In other words it extends the concept of security through intractability to the domain of quantum computing.

Quantum Key Distribution on the other hand takes a different approach: instead of transforming the key information, the information is encoded onto information carriers — commonly photons — that are **untouchable**, i.e., measurement of the quantum system (the photon) carrying the information is protected by the Uncertainty Principle. The two communicating parties following a pre-defined key exchange protocol such as **BB84**, can detect the presence of an eavesdropper on the channel through increased **QBER**.

Quantropi's solution called **Quantum Entropy Expansion and Propagation**, or **QEEP**, is a third approach next to PQC and QKD, and turns information systems into quantum information systems such that information becomes **uninterpretable**. Information, such as a key, undergoes a transformation through a quantum perturbation process such that every possible interpretation of the resulting information becomes equally likely to be correct. This creates a uniform superposition state protecting the information through the Generalized Uncertainty Principle.

Unlike PQC approaches, the transformation of information is not based on complex mathematics, but on quantum mechanics. QEEP uses quantum permutation gates, a type of quantum gate typically found in quantum computing as the perturbation operator. This makes QEEP provably secure, magnitudes faster and provides significant energy savings over PQC.

Unlike QKD approaches using fragile quantum systems that collapse under measurement as information carriers to achieve quantum safe key exchange, QEEP protects the information itself with quantum perturbation. This makes

QEEP independent of the underlying communication infrastructure and allows QEEP to provide an evolutionary upgrade path for existing infrastructure.

A Quantum Representation of Information

Consider a classical computing system: a physical system with registers that store information. Take for instance a system with an 8-bit register: each of the eight slots of the register stores a single bit of information, with the register being either on or off, encoded as 1 or 0. To represent the physical state of the information stored in this register, computer scientists commonly use bit-strings. For example, the bit-string '01001101' describing the physical state of the register encodes the binary number 010011012 representing the information value of a decimal number 77_{10}.

In addition to this classical representation of information described above, quantum computing provides us with a quantum-mechanical representation of information. While information systems based on qubits require such a representation to be accurately described, it is rarely applied to classical bits - however, it can describe classical information just as accurately.

While classical bits are in exactly one of two states, 0 or 1, a qubit contains coherent superpositions of both states. Thus to describe the general quantum state of a qubit, we turn to quantum mechanics and represent the quantum state as a linear superposition of its two orthonormal basis vectors in a Hilbert space. These basis vectors are usually written in Dirac notation and labeled with the bit strings of the information value they represent. For example:

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \qquad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

and together form the computational basis spanning the two-dimensional Hilbert space of the qubit. The quantum system generated by two qubits would span a four-dimensional Hilbert space represented by four basis vectors as:

$$|00\rangle = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \qquad |01\rangle = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} \qquad |10\rangle = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} \qquad |11\rangle = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}$$

In general, an n-qubit system would be represented by a superposition state in a 2^n-dimensional Hilbert space.

Since a qubit state is a superposition of the basis states, we can describe a single qubit by a linear combination of the basis vectors:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \qquad |\alpha|^2 + |\beta|^2 = 1$$

where α and β are complex numbers describing probability amplitudes. We can now see that classical bits can also be described quantum mechanically: a classical computer system is a 2-level system (voltage on, or voltage off). We then have one unit vector for voltage on, and another unit vector for voltage off. However, for classical computer systems, both levels of the state are mutually exclusive (either on or off, but not both at the same time). Thus, a classical bit system is a special case of a qubit system with the following properties of the coefficients:

$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \qquad \alpha, \beta \in [0,1] \qquad \alpha = 1, \beta = 0 \qquad \alpha = 0, \beta = 1$

When we measure a qubit, we perform an irreversible operation in which information is gained about the state of a qubit and the qubit collapses to a basis state $|0\rangle$ with probability $||\alpha||2$ and $||1\rangle$ with probability $||\beta||2$.

Quantum Permutation Gates

Quantum Logic Gates (short: "Quantum Gates") operate on qubits. Mathematically, operators are a linear transformation of the qubit state vectors in Hilbert space and are represented by $2^n \times 2^n$ unitary ("reversible") complex matrices. Quantum-mechanically, quantum gates act as perturbation operators to the qubit states and allow us to do computations.

One quantum gate is of particular interest in quantum computing: the **Hadamard** gate maps the qubit basis states $|0\rangle$ and $|1\rangle$ to two superposition states with equal weight. Many quantum algorithms use the Hadamard gate as an initial step to map m qubits initialized with a $|0\rangle$ basis state to a superposition of all 2^m orthogonal states with equal weight. However, the Hadamard transform also find applications outside of quantum computing. For example, the Hadamard transform is widely used in classical computing for data encryption, signal processing, and data compression such as **JPEG** and **MPEG-4**.

In general, we find two classes of quantum gates in quantum computing:

1. Non-classical gates allow for the massively parallel computing power that quantum computers are recognized for. An example of a non-classical gate is the Hadamard gate. The 1-qubit Hadamard gate has the matrix representation:

   $$H = H^{-1} = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

   and creates a superposed state with equal weights to the bases:

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

2. Classical behaviour gates, instead of mixing eigenstates, swap the eigenstates. Classical behaviour gates have a representation through permutation matrices. A permutation matrix is obtained by swapping the rows of an identity matrix. An example of a classical behaviour gate is the **Pauli** gate. The 1-qubit Pauli gate has the matrix representation:

   $$P = P^{-1} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

   and flips the eigenstate:

   $$P|0\rangle = |1\rangle \qquad P|1\rangle = |0\rangle$$

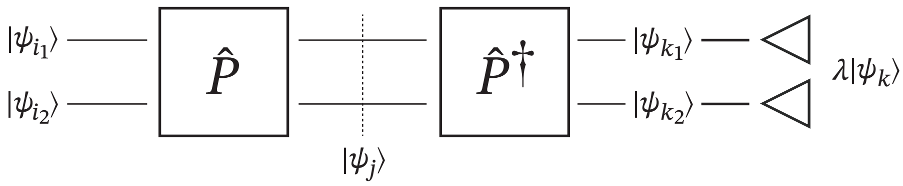

Figure 1: State transformation using permutation gates

In general, as n-qubit quantum gates are represented via matrices of dimension $2^n \times 2^n$ matrix, operating on the 2^n eigenstates, it immediately follows, that the number of unique permutation gates is $(2^n)!$. These properties make quantum permutation gates useful for information security.

Consider a 2-qubit system with an initial state $|\psi_{ji}\rangle$ as illustrated in Figure 2. The initial state $|\psi_i\rangle$ is operated on with a permutation gate P to create a transformed state $|\psi_j\rangle$ that we can transmit over a network. On the receiving end, we use the inverse permutation gate P^{-1} to operate on $|\psi_j\rangle$ to generate a transformed state $|\psi_k\rangle$ that we can then measure to obtain the information value λ associated with this state.

From an information security point of view, two questions are key:

1. Suppose you have knowledge about $|\psi_j\rangle$, can you obtain knowledge about $|\psi_i\rangle$?
2. Suppose you have knowledge about $|\psi_j\rangle$, can you obtain knowledge about P or P^{-1}?

To answer these questions, let us first look at an example for the 2-qubit case:

- First, we established in the previous section, that there are $(2^n)! = (2^2)! = 4! = 24$ possible permutation gates for $n=2$.
- Suppose *Alice* picked gate P_{19} to transform her state $|\psi_i\rangle = |01\rangle$ into $|\psi_j\rangle = |01\rangle$
- Now, suppose $|\psi_j\rangle$ is observable by *Bob*.
- To *Bob* the question is : how could $|\psi_j\rangle$ have been created by *Alice*?

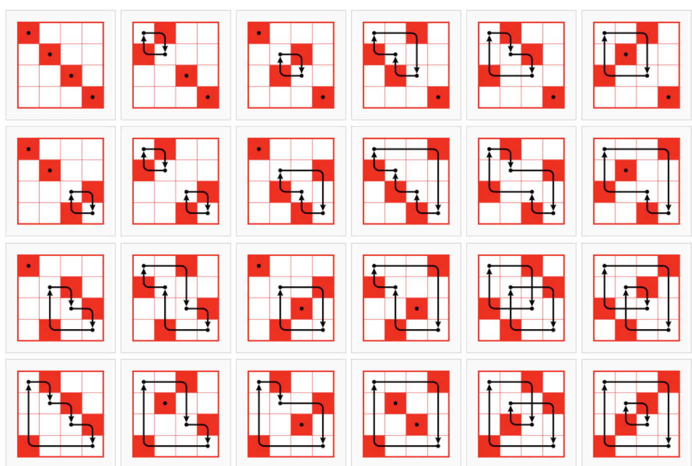

Figure 2: The 24 permutation gates for a 2-qubit system.

- Surprisingly, $|\psi_j\rangle$ could have been created from any possible $|\psi_i\rangle$ state:
  - from $|\psi_i\rangle = |00\rangle$ via $P_1, P_4, P_7, P_{10}, P_{18}, P_{20}$
  - from $|\psi_i\rangle = |01\rangle$ via $P_0, P_5, P_6, P_{11}, P_{19}, P_{21}$
  - from $|\psi_i\rangle = |10\rangle$ via $P_2, P_3, P_8, P_9, P_{22}, P_{23}$
  - from $|\psi_i\rangle = |11\rangle$ via $P_{12}, P_{13}, P_{14}, P_{15}, P_{16}, P_{17}$
- Each of the gates appears exactly once, and for each possible state $|\psi_i\rangle$, there are $(2^n-1)!$ possible gates producing the observed state $|\psi_j\rangle$.
- Each permutation gate and state $|\psi_i\rangle$ are equally likely to have produced the observed state $|\psi_j\rangle$

We say the information in $|\psi_j\rangle$ exists in a uniform superposition of all possible interpretations of the meaning of $|\psi_j\rangle$.

Concretely, each quantum permutation gate P_i becomes a measurement basis under which we can measure $|\psi_j\rangle$. Only under the correct measurement basis — the same gate selected by *Alice*, would *Bob*'s and *Alice*'s interpretations of state $|\psi_j\rangle$ be the same.

Now consider *Bob* blindly picked a gate P_i at random.

- Naively, *Bob* would have a 1 in 24 chance to exactly pick the right P_i .
- At the same time, *Bob* has a 6 in 24 = 1 in 6 chance to pick some P_i that ends up producing the right interpretation of $|\psi_j\rangle$ into $|\psi_i\rangle$.
- Third, *Bob* could directly guess $|\psi_i\rangle$ without even trying to guess P_i. He has a 1 in 6 chance to do so

Thus, from an optimal strategy point of view, the best *Bob* can do, is to guess $|\psi_i\rangle$ with a chance of $1/2^n$ for an n-qubit state. From an information security point of view this satisfies the requirements of **Perfect Secrecy**.

Entropy Expansion

Claude Shannon in 1948 defined **Information Entropy** as the measure of uncertainty in the information and is formulated as:

$$H = log_2 D$$

For a classical n-bit system, n bits can describe 2^n pieces of information (in computer science, commonly bit-strings interpreted into decimal numbers). The entropy in such a system is:

$$H = log_2 2 = n = n * 2^0$$

No surprise here: a classical bit can only attain one of two discrete values, 0 and 1 thus contains maximally one bit of Shannon information.

In contrast, a qubit can take on information values of 0, 1, and any combination of either. This superposition allows for additional degrees of freedom that increase the uncertainty in the information — or entropy. Yet, ultimately we need to measure the qubit at which point we collapse the

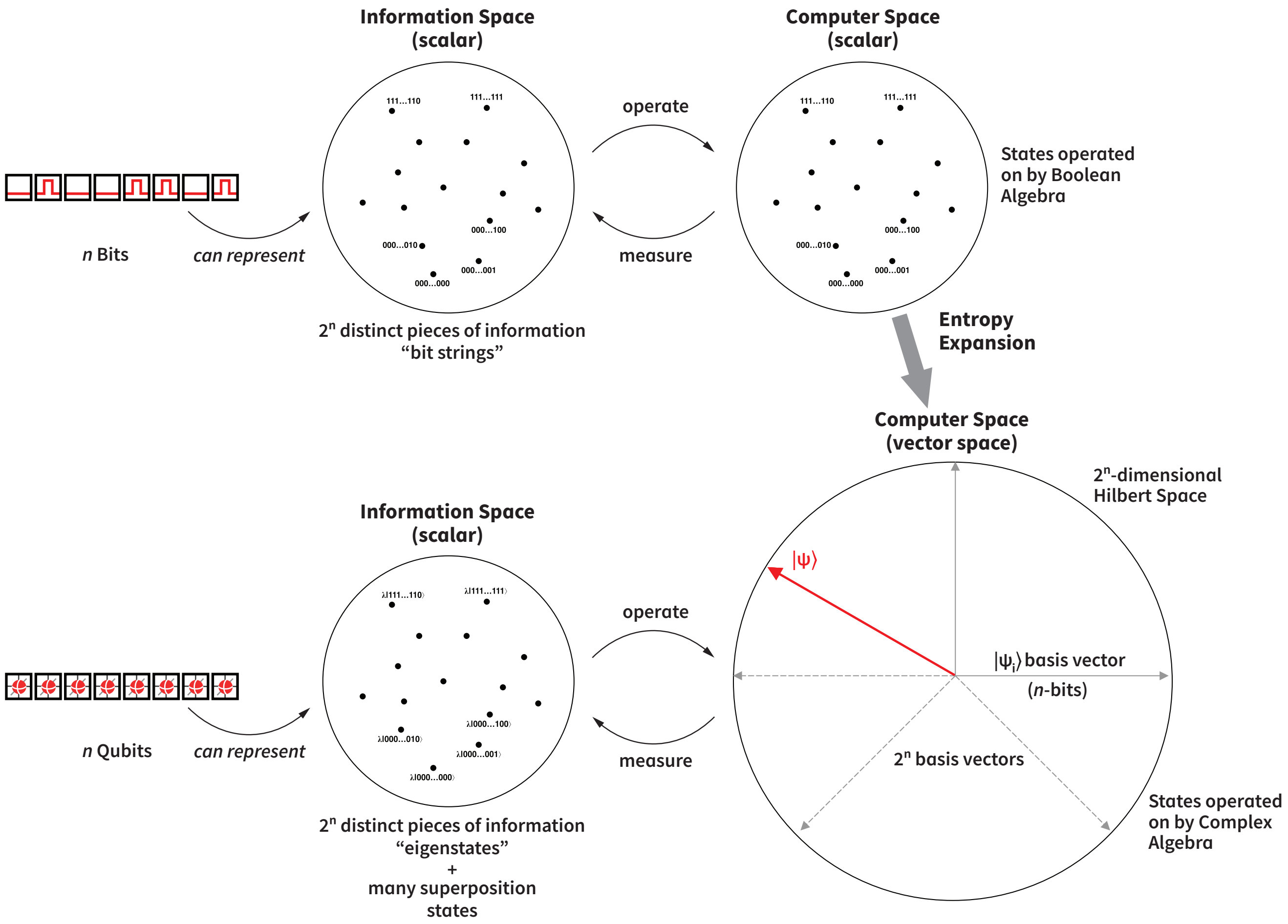

Figure 3: The information required to express the information and computation spaces of classical bits and quantum bits are different. To express qubit states in Hilbert space we need more information even though measurement of the states collapses them to a 2^n information space.

probability amplitudes and project the state space back into a 2^n information space (see Figure 3).

However, within the computational space things are different: the superpositions created by quantum gates that generate varying degrees of freedom.

Within the frame of reference that initial states correspond to basis vectors (e.g., $|00\rangle$, $|01\rangle$, $|10\rangle$, or $|01\rangle$ for a 2-qubit system) and allowing transformations by quantum gates we introduce 2^n additional degrees of freedom over classical bits: we are operating with $2^n \times 2^n$ operators in a 2^n-dimensional Hilbert space where each vector carries n bits of information. Thus the required information to describe state vectors in this space is:

$$H = log_2 2 = n * 2^n$$

Restricting allowable transformations to permutation gates only creates an entropy spectrum that is slightly biased: each permutation gate corresponds to a unique 1:1 mapping of one basis vector to another basis vector, without repetitions. Thus the required information to describe this sub-space is:

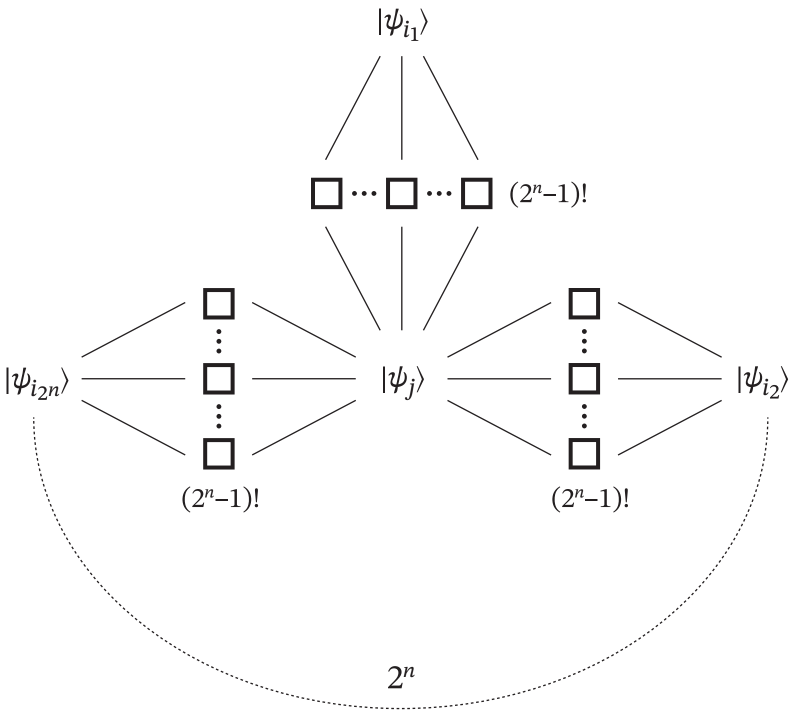

Figure 4: Superposition paths of 2-qubit transformation

$H = log_2 2 = log_2(2^n)!$

For large n, this reduces to:

$n \to \infty : H = (n-2)2^n$

We call this increase of information entropy introduced by application of permutation gates "Entropy Expansion". It is this Entropy Expansion that allows for information security: classical information with two exclusive discrete states allows each bit of information to carry exactly one bit of uncertainty, whereas in the quantum world, information states itself carry uncertainty such that each bit of information can carry more than one bit of uncertainty.

How does this not violate our classical understanding of Shannon entropy? The uncertainty in quantum information is "inherent": to extract a particular information from the quantum system, we have to perform a measurement. This measurement collapses the quantum state into a classical state corresponding to the probabilities associated with the probability amplitude coefficients (e.g., α and β) and the information entropy is then contained within the Shannon boundary.

Entropy Propagation

We have seen in the previous section, that information security stems from the different interpretation possibilities of the transformed state , after being operated on with a permutation gate — in particular, all interpretations are equally likely to be correct. We can visualize this relationship as a state-transformation path diagram as shown in Figure 4.

For a given observed state $|\psi_j\rangle$, this state could have been produced from any of the 2^n initial states $|\psi_i\rangle$ with equal likelihood, via any of the $(2^n-1)!$ paths (permutation gates). We can now calculate the probability of an observer Eve obtaining the correct initial state $|\psi_i\rangle$ by brute force enumeration of the entire space of possible paths to $|\psi_j\rangle$.

This probability is equal to directly guessing the initial state $|\psi_i\rangle$. Coming back to the two central questions about information security stated in the previous section, we now have a quantum mechanical explanation:

1. "An observed state $|\psi_j\rangle$ does not leak information about $|\psi_i\rangle$" is a direct outcome of the Uncertainty Principle between the permutation operator and the System Information Hamiltonian H_0. This Uncertainty Principle $[H_0 , P] \neq 0$ tells us that the relationship between $|\psi_j\rangle$ and $|\psi_i\rangle$ is one of perfect secrecy. This Uncertainty alone, however does not guarantee security under re-use: consider the XOR operator, for example which does not commute with the System Information Hamiltonian (satisfies the Uncertainty Principle), but we know from the One-Time Pad that we can only use the operator once (hence the "one-time" in the name).
2. "An observed state $|\psi_j\rangle$ does not leak information about P" is a direct outcome of the Uncertainty Principle $[P , P'] \neq 0$ between permutation operators. This Uncertainty Principle tells us that we can re-use the operator, but the security is not necessarily perfect.

The QEEP mechanism presented in this white paper satisfies both Uncertainty Principles, thus representing a mechanism that is both: reusable and protected by perfect secrecy. However, this also allows us to freely distribute a transformed state $|\psi_j\rangle$ without fear of compromise of either the initial state $|\psi_i\rangle$, or the randomly selected permutation gate P. Of particular interest is the following observation: we may freely distribute $|\psi_j\rangle$ thus over any network medium that can carry the state, and security does not stem from an inability to measure state $|\psi_j\rangle$ but an inability to correctly interpret state $|\psi_j\rangle$ without knowledge of the permutation gate P that was used to prepare $|\psi_j\rangle$.

Since quantum gates are reversible computational constructs, they are mathematically expressed as unitary matrices. Quantum-mechanically, this allows a receiver, Bob, to recover the initial state $|\psi_i\rangle$ with an inverse quantum gate $G^\dagger$, from a state $|\psi_i\rangle$ prepared and transformed by Alice via a corresponding quantum gate G, even when the transmitted state $|\psi_j\rangle$ is a superposed state.

We call this ability to take any state $|\psi_i\rangle$, operate on it with a quantum gate G to produce a transformed state $|\psi_j\rangle$, distributing $|\psi_j\rangle$ freely without fear of compromise of the initial state or the quantum gate, and recovering the initial state $|\psi_i\rangle$ from $|\psi_j\rangle$ with a inverse quantum gate $G^\dagger$ at the receiver end, "Entropy Propagation".

If our transmission mechanism allows sending and receiving of quantum states, we can use any quantum gate G for this process. However, by restricting the Quantum Entropy Expansion and Propagation process to Permutation Gates, we decouple information entropy from infrastructure, as the transformed states $|\psi_j\rangle$ are transmittable over classical communication channels. Why we are able to do so, may not be intuitively obvious.

In general a quantum state is defined as a linear combination of basis vectors with complex coefficients representing probability amplitudes such that the sum over the square norm of the coefficients equals 1 (i.e., the sum of probabilities equals 1). In the case that the coefficients are such that any measurement of the state would with a probability of 1 collapse to the equivalent classical state, then such a state is transmittable over classical infrastructure: operating on the state and measuring the state can be combined in a single action and the outcome can be digitally encoded and transmitted over classical infrastructure.

Conclusions

In this white paper, we presented a novel approach for the transformation of information via quantum permutation gates, called Quantum Entropy Expansion and Propagation ("QEEP"). We described our approach through the mathematical framework of quantum-mechanics.

The result of transforming an (quantum-)information state with a permutation gate is a transformed state that does not leak information about either the operator (permutation gate) or the initial state. The protection of both initial state and operator are a direct result of the two Uncertainty Principles that govern the QEEP mechanism. Furthermore, any possible interpretation of the transformed state has equal likelihood of being correct without knowledge of the operator that was used to generate the transformed state — satisfying the property of Perfect Secrecy ("uncrackable").

In the case that quantum channels at our disposal, we can allow for the use of any quantum gate satisfying both Uncertainty Principles. However, of most practical use today is the subset of quantum gates called permutation gates that create transformed states which we can present with classical information bits and transmit over classical communication channels.

These properties allow for the QEEP to be a perfect solution to the key-exchange problem over existing infrastructure, as a cost-effective, energy-efficient, and scalable alternative to both photonic Quantum-Key-Distribution and Post-Quantum Cryptography.