Keeping secrets
Communication

Rolf Landauer: Information is physical!

sound waves, photons, electrical signals, paper and ink, etc.

Alice

Bob

Rolf Landauer: Information is physical!
The problem of privacy

Alice

Eve

Bob
The science of secrets

**Cryptography:** How to protect secret information

Alice encrypts the message → *encrypted message* → Bob decrypts the message

**Cryptanalysis:** How to uncover the secrets of others

Alice encrypts the message

Bob decrypts the message

Eve
Alice and Bob share secret key information that Eve does not know.

Without $K$, Eve cannot use $C$ to figure out $M$. 
Key is a single letter: $K = "W"

Rotate inner wheel so align A with W

Encryption: Outer letters to inner ones

**DEAR BOB** becomes **ZAWN XKK**

(This cipher is not hard for Eve to "break"
For Alice to **send** a secret message to Bob, they must already **share** a secret key. Nevertheless,

- The key can be **prearranged**.
- It does not matter **where** the key comes from (A → B, B → A, third party, etc.).
- Key has no **meaning** – can be **random**.
- They can **reuse** the key. However ....
How to measure information

Claude Shannon (1948): The amount of information in a message depends on the number of possible messages.

\[ I = \text{How many yes/no questions are needed to guess the message?} \]

\[ = \text{How many bits (0/1) are needed to write message in a binary code?} \]

Using \( n \) bits, we can represent \( 2^n \) possible messages.
Redundancy

The alphabet contains 26 letters, so each letter represents about 5 bits \((2^5 = 32)\).

Shannon found that you could guess ordinary English text using only \(~2\) yes/no questions per letter (in the long run).

- some letters are more likely
- some letter combinations are more likely
- overall message usually "makes sense"

*a*l *h*t *s *o*d
d*e* n*t *l*t*e*

*** **** ** ****
**** *** ********
a*l *h*t *s *o*d
d*e* n*t *l*t*e*

all that is gold
does not glitter
Known and unknown

Eve does not know:
- the key: $I(K)$ bits
- the plaintext: $I(M) \approx 2 \times L$ bits

Eve does know:
- the ciphertext: $I(C) \approx 5 \times L$ bits

Given a long enough message, Eve has enough information to figure out both $M$ and $K$ – at least in principle!
Examples: Cryptograms and Enigma

Simple substitution cipher ("newspaper-type" puzzle)

\[ K = \text{scrambling rule for the alphabet} \]

\[ I(K) = 88 \text{ bits!} \]

Eve should be able to "break" such a cipher for messages longer than \(~30\) letters

German Enigma system

- 3 (of 6) continually shifting rotors
- "plugboard" yields more possible keys

\[ I(K) = 87 \text{ bits!} \]

\textit{NB: The computation required to "break" Enigma is much harder (but still possible)}
One-time pad

Keep introducing new key information. **Never re-use it!**

Eve's information never catches up!

World War II: Shannon uses these ideas to prove the **SIGSALY** system is secure.

Cold War: USSR mistakenly re-uses keys for their "one-time" pad system. US spots this and is able to decrypt some messages (**Venona** project).
One-time pad

Keep introducing new key information. **Never** re-use it!

Eve's information never catches up!

World War II: Shannon uses these ideas to prove the SIGSALY system is secure.

Cold War: USSR mistakenly re-uses keys for their "one-time" pad system. US spots this and is able to decrypt some messages (Venona project).

How do Alice and Bob **distribute new keys**? (Note that Eve wins if she knows a key that Alice and Bob believe is secret.)
Public-key cryptography

Use separate encryption and decryption keys.

plaintext $M$

\[ C = e(M, K) \]

ciphertext $C$

plaintext $M$

\[ M = d(C, K^*) \]

ciphertext $C$

Eve may know $K$ ("public key") but not $K^*$. 
Public-key cryptography

Encryption key $K$
Decryption key $K^*$

logically equivalent?

Generating $K^*$ is easy
Computing $K^* \rightarrow K$ is easy
Computing $K \rightarrow K^*$ is **hard**!

How it works: Bob generates $K^*, K$.
Bob announces $K$ to Alice (and Eve!)
Alice can use $K$, but Eve can't find $K^*$

Popular choice: **Factoring**

$P, Q \rightarrow PQ$ (easy)

$PQ \rightarrow P, Q$ (hard)

But using a **quantum computer**, factoring is relatively easy!
The quantum veil
Wave-particle duality

Light propagates in a wave-like way but interacts in a particle-like way. The same is true for electrons, etc.

Wave frequency and wavelength determine particle energy and momentum

\[ E = \frac{hc}{\lambda} \]

Wave intensity determines particle probability.

\[ \mathcal{P} = |\psi|^2 \]
Two slits, photon by photon

Weak light: One photon at a time!
Which slit?

Introduce devices that can record which slit the photon passes.
No interference effect is observed!

Quantum interference can only occur when the system is informationally isolated. No physical record formed!
Spins and qubits

- **Spin** is the internal angular momentum of a quantum particle (e.g., an electron).
- We can measure the spin along any axis (X, Z, ...). The result is always either +1 or -1 (in units of $\hbar/2$).
- Spin states: → ← ↑ ↓ etc.
- Qubits have all of the usual features of quantum systems: superposition, uncertainty, entanglement.

A spin is a qubit.
Quantum cryptography

Big news: Charles Bennett and Gilles Brassard win the 2018 Wolf Prize in Physics!

One reason: In 1984, Bennett and Brassard showed how to use quantum physics to solve the **key distribution problem**!
Key distribution problem

How can Alice and Bob create a secret key that they know Eve cannot know?

BB idea: Alice and Bob can exchange quantum particles and public messages.
Bob announces which measurements he made (but not the results). Alice announces which of those choices were "correct". At the end: Common random bits that can be used as a key!
What about Eve?

- Alice and Bob's public conversation tells Eve nothing about the values of their key bits.
- If Eve makes her own measurements of the qubits, she will disturb their quantum states.
- Alice and Bob can check for this by "sacrificing" a few of their key bits for comparison.
"Cloning" qubits?

- Sneaky scheme: Eve makes her own copies ("clones") of the qubits. She measures them later, after Bob has announced his measurements.
- Quantum no-cloning theorem: It is impossible to duplicate the quantum state of a particle!
- "Quantum information" cannot be copied!

Artur Ekert (1991): Alice and Bob can do quantum key distribution by sharing entangled qubits.
Quantum entanglement

A pair of quantum systems can be in an **entangled state**. Neither system by itself has a definite state.

Example: Total spin zero (TSZ) state

- If we measure particles 1 and 2 along the same axis, we always obtain **opposite** results.
- If we measure them along different axes, we see **correlations**.
- Einstein: "Spooky action at a distance"!
Bell's theorem

Commonsense view of correlations:
1. Each particle's behavior is the result of a hidden "program".
2. The particle programs may be created together but function separately.

John Bell (1964): This sensible idea cannot be true for entangled quantum systems!
A strange relationship

Two quantum particles can have a relationship that has no "classical" analogue.

"Pseudotelepathy"

- It is tricky to say exactly how the particles do what they do, but ....
- **We** cannot use entanglement to send messages faster than light.
- Ekert: Use entanglement for key distribution. Any Eve measurements destroy the entanglement in a detectable way.

No-signaling principle
Noise or Eve?

Alice prepares quantum systems (entangled qubits, etc.)

Bob observes the quantum systems he receives.

Alice and Bob must assume that all noise is due to Eve – but noise is inevitable!
Distilling entanglement

Suppose Alice and Bob share many qubit pairs with "noisy" entanglement.

They may perform local quantum operations and exchange classical messages.

Alice and Bob end up with fewer pairs having "pure" entanglement.
Suppose Alice and Bob share many qubit pairs with "noisy" entanglement. They may perform local quantum operations and exchange classical messages. Alice and Bob end up with fewer pairs having "pure" entanglement.

Key distribution can be absolutely secure if and only if entanglement distillation is possible!
Monogamy of entanglement
The Newlywed Game

Alice and Bob have a relationship.

Interview them separately. Possible questions:

\( X? = \) Do you like to dance?
\( Y? = \) Do you like to eat oysters?

Individual answers are not predictable, but Alice and Bob give **correlated** answers.

Our variant: Each Alice/Bob pair is asked only once. Questions may be different!
A curious relationship

Are Alice and Bob cheating the game?

*Maybe.* But we can never catch them at it or prove that they are!

<table>
<thead>
<tr>
<th>P(agree)</th>
<th>X?</th>
<th>Y?</th>
</tr>
</thead>
<tbody>
<tr>
<td>X?</td>
<td>100%</td>
<td>0%</td>
</tr>
<tr>
<td>Y?</td>
<td>0%</td>
<td>0%</td>
</tr>
</tbody>
</table>

No-signaling principle: The choice of Alice question has no observable effect on Bob's answer (and vice versa).
A question of monogamy

Could Alice have exactly the same relationship with someone else (Bill)?

Yes!

Suppose we ask Bob X? and Bill Y?

• If we ask Alice X? then Bob and Bill's answers must disagree.
• If we ask Alice Y? then Bob and Bill's answers must agree.
A question of monogamy

Could Alice have exactly the same relationship with someone else (Bill)?

No!

Suppose we ask Bob X? and Bill Y?

<table>
<thead>
<tr>
<th>X?</th>
<th>Y?</th>
</tr>
</thead>
<tbody>
<tr>
<td>100%</td>
<td>0%</td>
</tr>
<tr>
<td>0%</td>
<td>0%</td>
</tr>
</tbody>
</table>

- If we ask Alice X? then Bob and Bill's answers must disagree.
- If we ask Alice Y? then Bob and Bill's answers must agree.

The Alice-Bob relationship is monogamous.

No-signaling principle
The Alice-Bob relationship remains monogamous even if the probabilities are not quite 100% and 0%.

This can be achieved using an entangled pair of qubits.

Quantum entanglement is monogamous!
If Alice and Bob can share pairs of particles with "pure" entanglement, Eve is automatically excluded!

Alice and Bob can use their exclusive statistical relationship to generate a secure cryptographic key.
Alice and Bob bought their quantum key distribution system from a vendor. It's a "black box" with buttons and lights.

But maybe the vendor is really Eve!

Maybe the system does not really function exactly as advertised!
Black box security

It doesn't matter. Alice and Bob can still guarantee the secrecy of their key!

Our proof of monogamy (and thus privacy) only depends on:

• no-signaling principle
• observable correlations

If Alice and Bob observe the right kinds of correlations in their system, they can use it to obtain a key that is provably secret from Eve even if quantum mechanics is actually wrong.
Privacy and the quantum

Privacy is an essential part of the quantum world.

• We only observe interference if the system is informationally isolated.
• We cannot faithfully copy quantum information.
• We can use quantum physics to distribute a secret key.
• The relationship between entangled particles is monogamous.
• The monogamy of quantum entanglement does not depend on the truth of quantum mechanics itself – only the no-signaling principle!
What we're doing now

General operational theories

• "Boxworld" – systems are "boxes" with inputs and outputs that obey the no-signaling principle

• Such theories can have entanglement, monogamy, no-cloning theorem, key distribution protocols, etc.

What features are shared?

How is quantum theory special?

NSP: The value of $a$ does not affect the probabilities of $d$, etc.