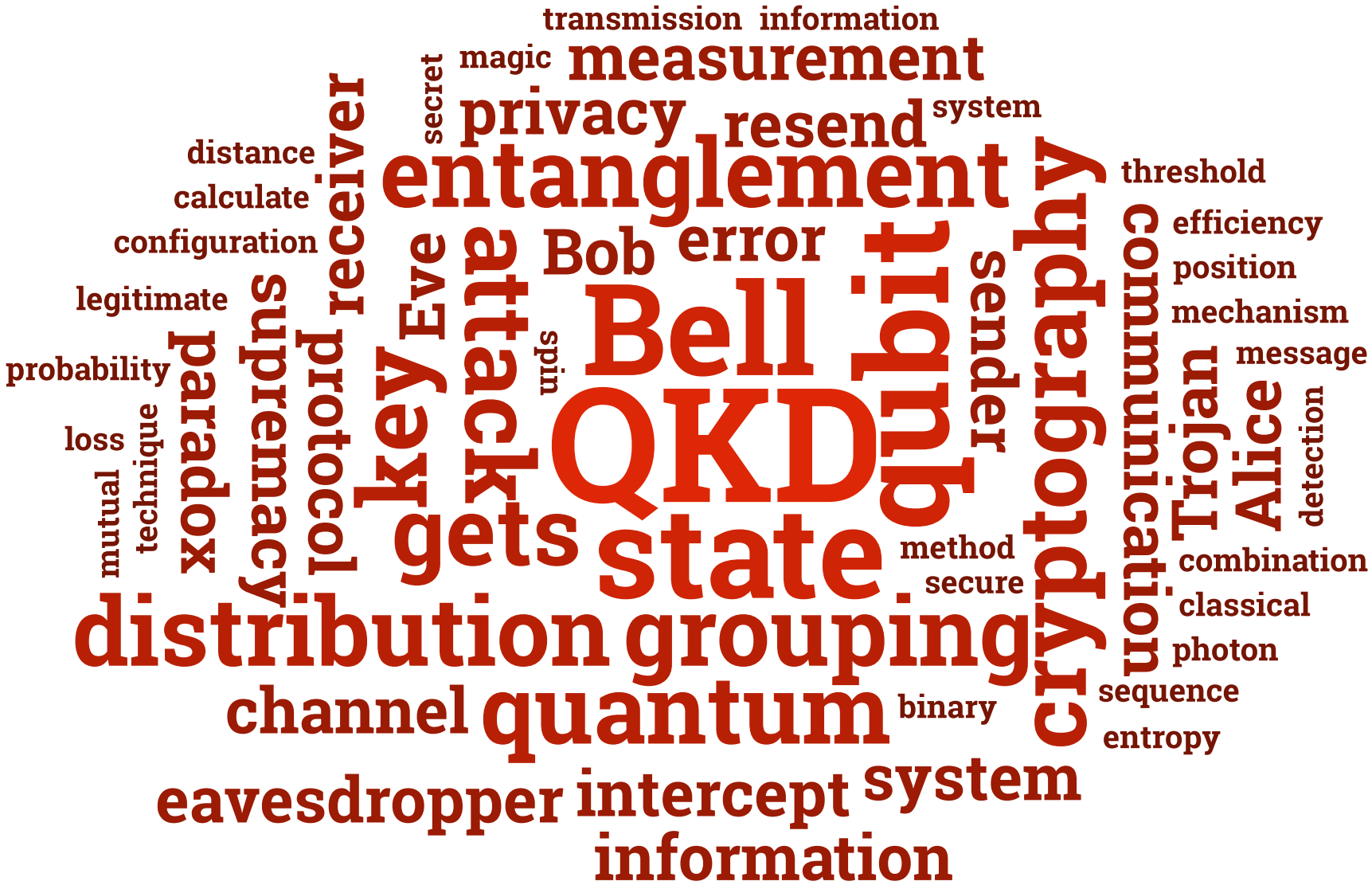
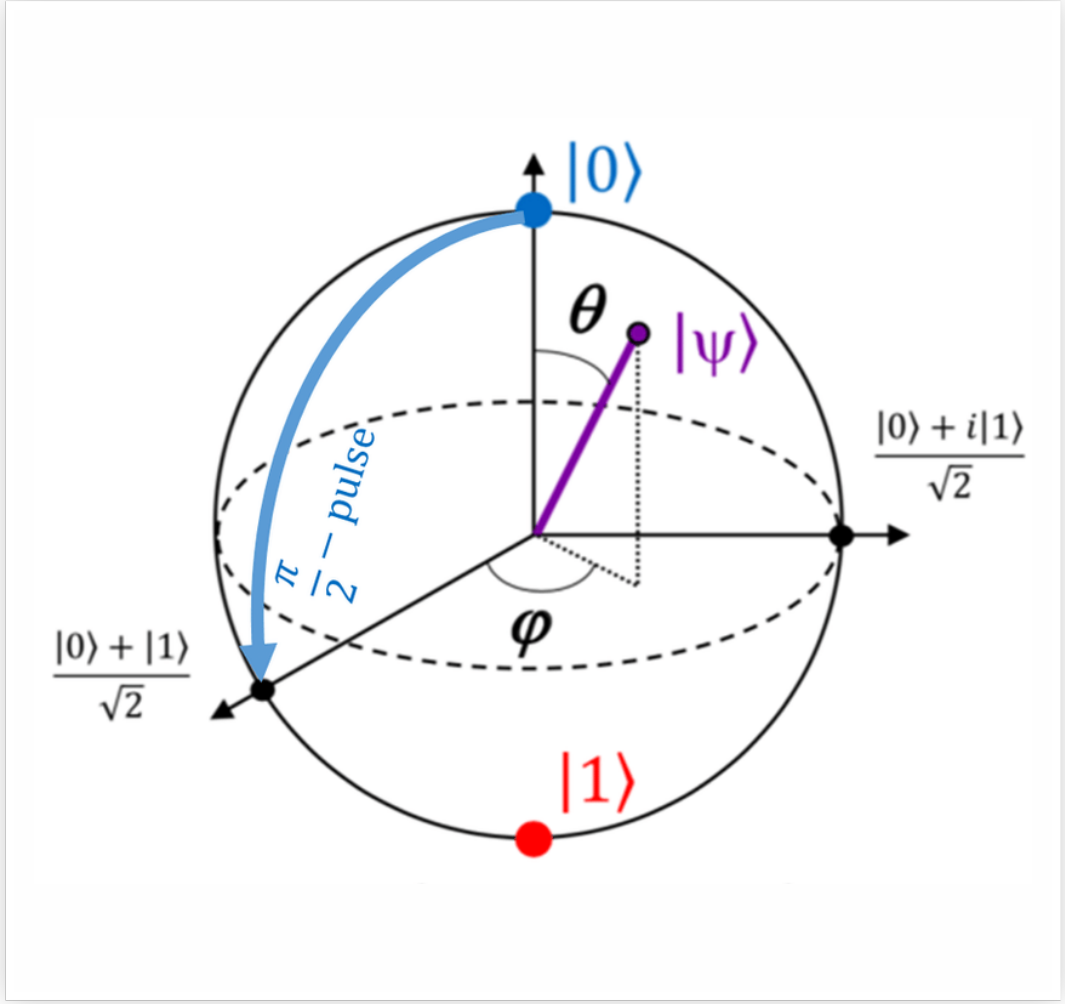
# Quantum Key Distribution Based on Random Grouping Bell State Measurement


transmission
information
measurement
magic
secret
privacy
resend
system
entanglement
distance
calculate
configuration
receiver
threshold
efficiency
position
mechanism
message
Alice
detection
Trojan
communication
cryptography
qubit
sender
error
Bob
attack
Eve
key
protocol
supremacy
paradox
legitimate
probability
loss
mutual
technique
spin
Bell
QKD
gets
state
method
secure
combination
classical
photon
sequence
entropy
distribution
grouping
channel
quantum
binary
eavesdropper
intercept
system
information

# Qubits




- Complex 2D-Hilbert space
- No general phase
- Normalization
- Two independent parameters

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle$$

# Bell States

$$|\phi^{\pm}\rangle = \frac{1}{\sqrt{2}}\left(\,|00\rangle \pm |11\rangle\,\right)$$

$$|\psi^{\pm}\rangle = \frac{1}{\sqrt{2}}\left(\,|01\rangle \pm |10\rangle\,\right)$$

- **Basis in four-dimensional state space**
- **Maximum entangled state of 2 qubits**
- **Easy to combine and measure**

  (in comparison with peers)

# QKD Timeline

**BB84**
first QKD protocol
1984

**E91**
EPR paradox
1991

**Gao**
first BSM usage
2008

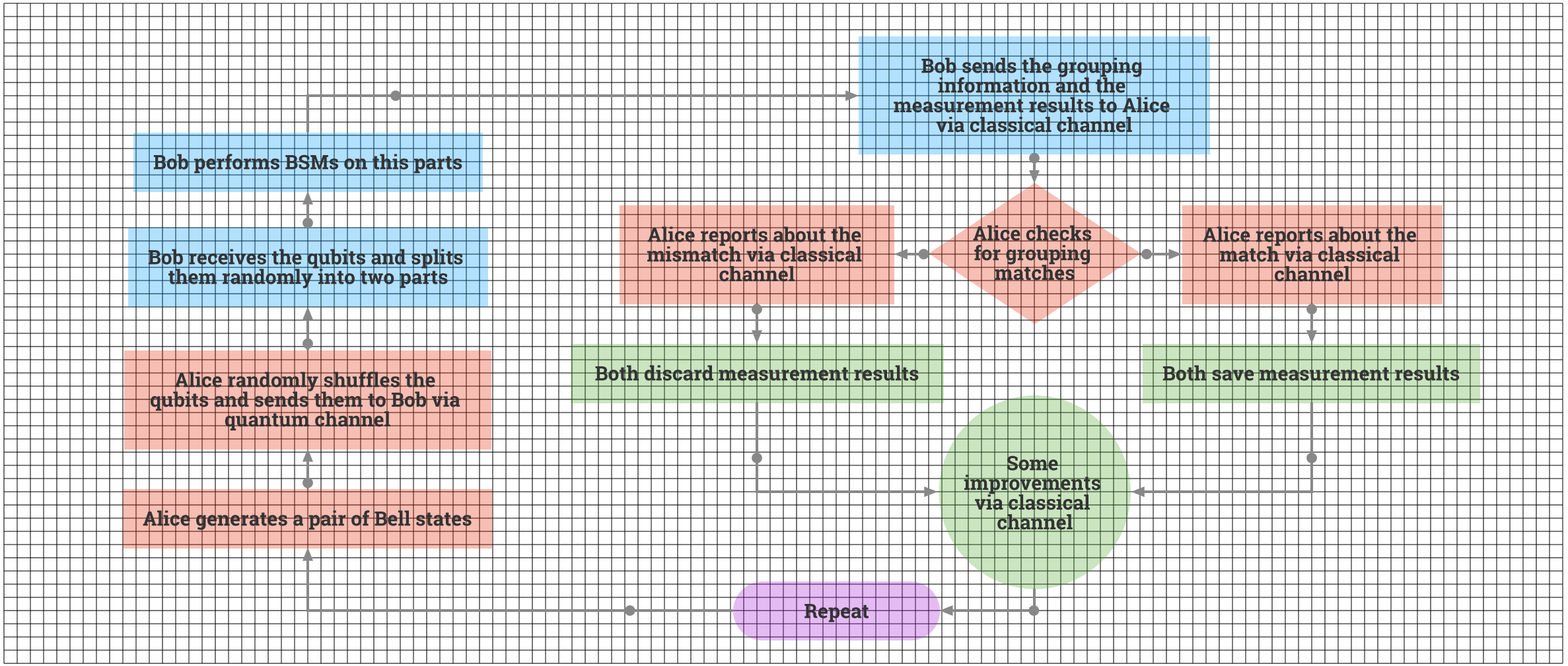
**Yuan**
2 BSM combination
2008

**Protocol***
Random Grouping
2020

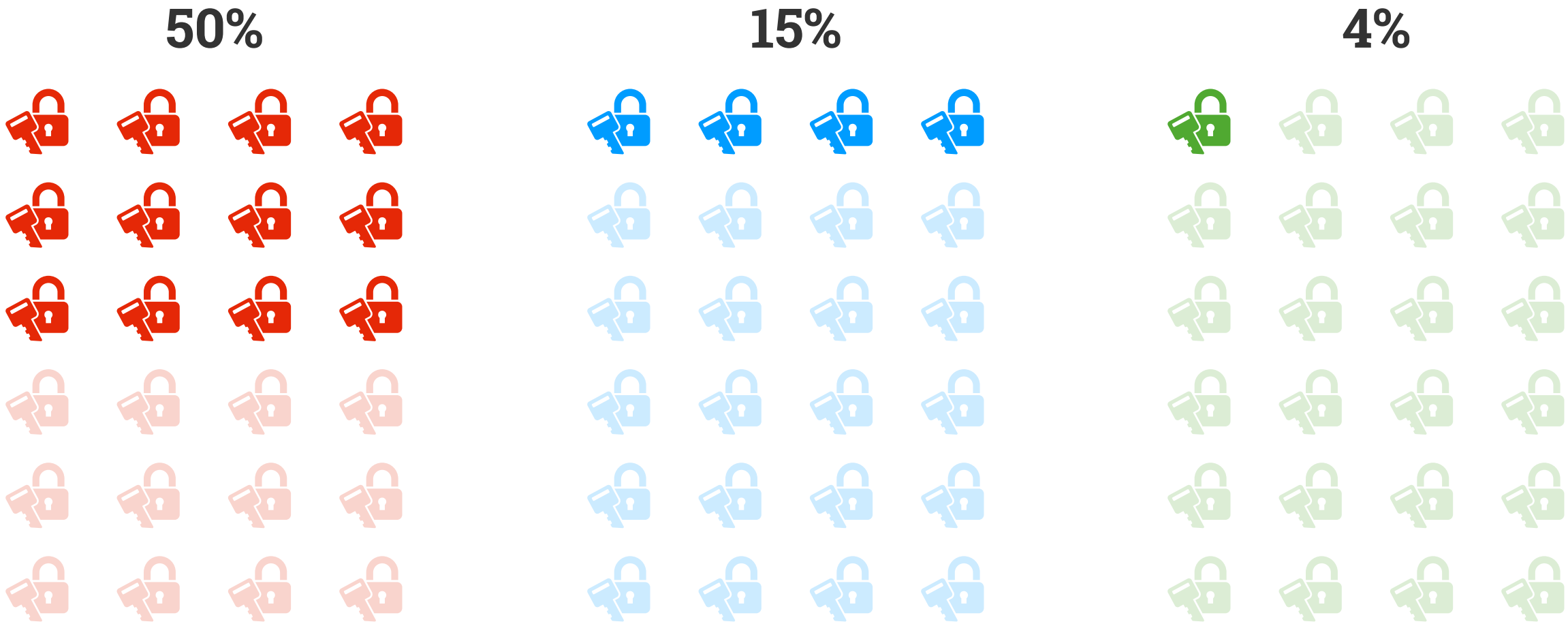
# Groupings & Spooky Scary Formulas

$$
\begin{aligned}
|\mathcal{C}\rangle_{1234} = |\phi^-\rangle_{12} \otimes |\phi^+\rangle_{34} &= \frac{1}{2}\big(\,|00\rangle_{12} - |11\rangle_{12}\,\big) \otimes \big(\,|00\rangle_{34} + |11\rangle_{34}\,\big) = \\
&= \frac{1}{2}\big(\,|0000\rangle + |0011\rangle - |1100\rangle - |1111\rangle\,\big)_{1234} = \\
&= \frac{1}{4}\big(2\,|0000\rangle + 2\,|0011\rangle - 2\,|1100\rangle - 2\,|1111\rangle\,\big)_{1234} = \\
&= \frac{1}{4}\big(\big[\,|0000\rangle - |0101\rangle + |1010\rangle - |1111\rangle\,\big] + \big[\,|0000\rangle + |0101\rangle - |1010\rangle - |1111\rangle\,\big] + \\
&+ \big[\,|0011\rangle - |0110\rangle + |1001\rangle - |1100\rangle\,\big] + \big[\,|0011\rangle + |0110\rangle - |1001\rangle - |1100\rangle\,\big]\big)_{1234} = \\
&= \frac{1}{4}\big([|00\rangle_{13}|00\rangle_{24} - |00\rangle_{13}|11\rangle_{24} + |11\rangle_{13}|00\rangle_{24} - |11\rangle_{13}|11\rangle_{24}] + \\
&+ [|00\rangle_{13}|00\rangle_{24} + |00\rangle_{13}|11\rangle_{24} - |11\rangle_{13}|00\rangle_{24} - |11\rangle_{13}|11\rangle_{24}] + \\
&+ [|01\rangle_{13}|01\rangle_{24} - |01\rangle_{13}|10\rangle_{24} + |10\rangle_{13}|01\rangle_{24} - |10\rangle_{13}|10\rangle_{24}] + \\
&+ [|01\rangle_{13}|01\rangle_{24} + |01\rangle_{13}|10\rangle_{24} - |10\rangle_{13}|01\rangle_{24} - |10\rangle_{13}|10\rangle_{24}]\big) = \\
&= \frac{1}{2}\big(|\phi^+\rangle_{13}|\phi^-\rangle_{24} + |\phi^-\rangle_{13}|\phi^+\rangle_{24} + |\psi^+\rangle_{13}|\psi^-\rangle_{24} + |\psi^-\rangle_{13}|\psi^+\rangle_{24}\big)
\end{aligned}
$$

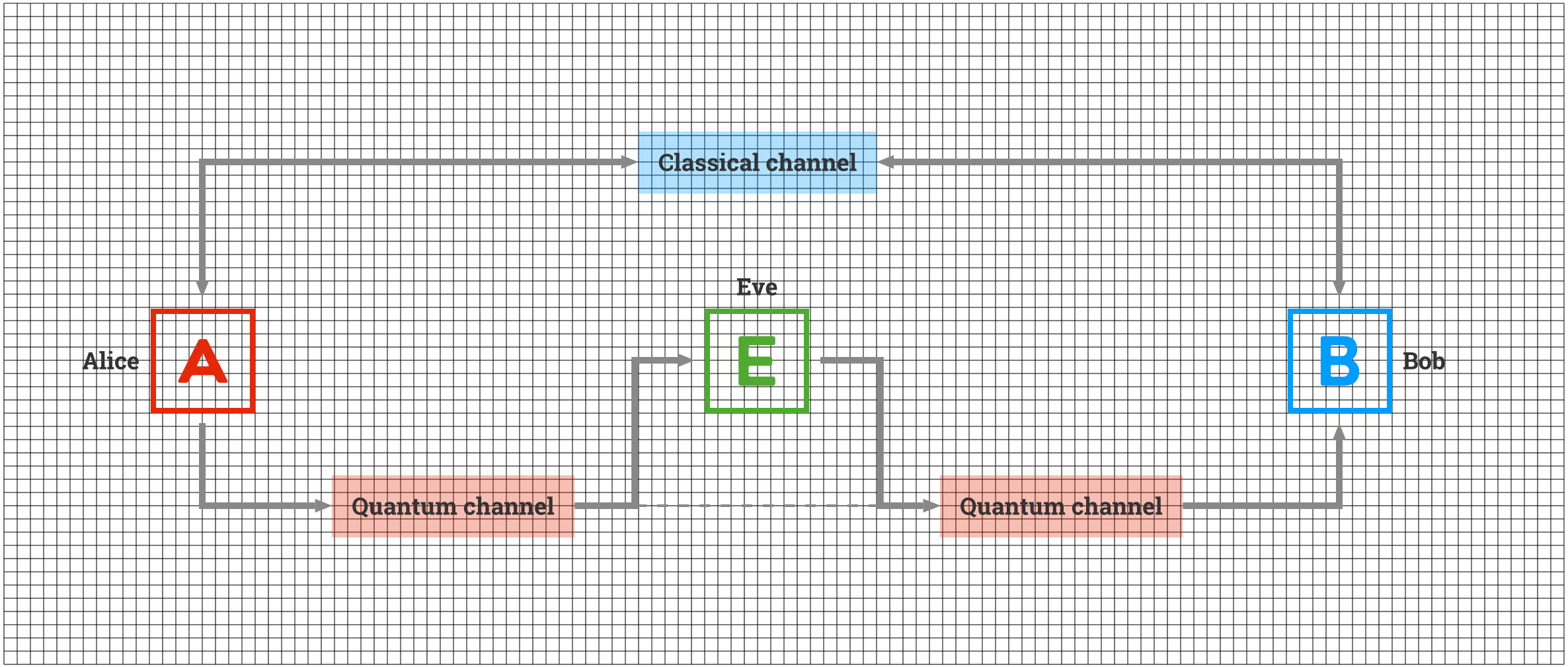
# Key Distribution Algorithm



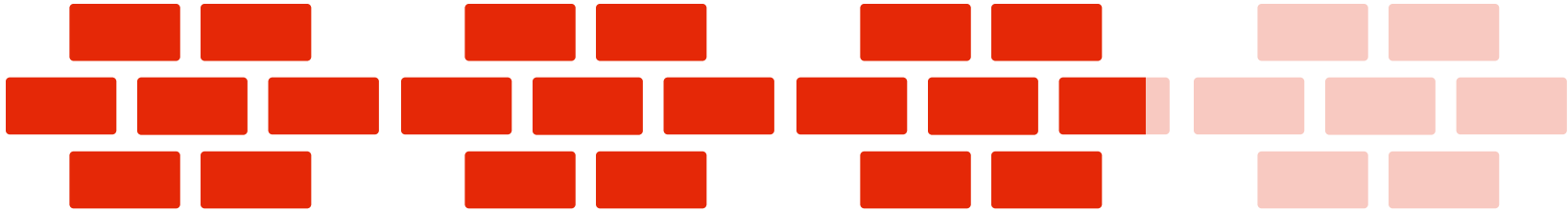
# Qubit Error Ratio



# Intercept-Resend Attack

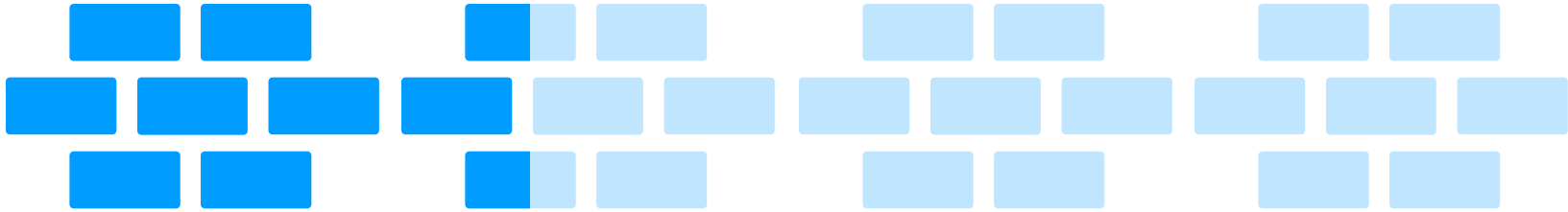


# 72



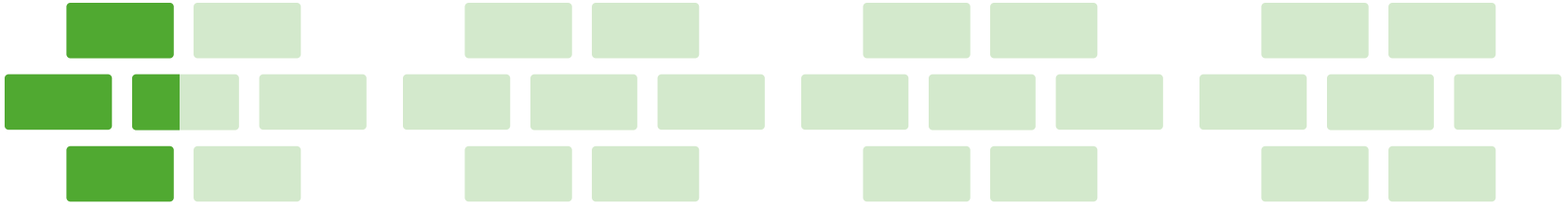
bits needed to detect Eve in **BB84**

# 33



bits needed to detect Eve in **E91**

# 11



bits needed to detect Eve in **Protocol***

# Outcome

- **Protocol* is superior to counterparts**
- **Protocol* can be experimentally implemented**
- **Protocol* has a range of further improvements**

# Current Problems

- QKD usually relies on having authenticated classical channel
- Quantum gates noise makes probabilistic estimates worse
- QKD systems are still quite expensive

# Questions?