CMSC/Math 456: Cryptography (Fall 2022)

Lecture 24

Daniel Gottesman

Administrative

No class Thursday!

Problem set #8 is due Dec. 1 at *midnight*.

This class is being recorded

Timeline of SSL/TLS

Protocol	Year	Year Deprecated
SSL 2.0	1995	2011
SSL 3.0	1996	2015
TLS 1.0	1999	2021
TLS 1.1	2006	2021
TLS 1.2	2008	
TLS 1.3	2018	

Cryptographic protocols have decades-long lifetimes. Often protocols are used well beyond the point where there are known practical attacks. New protocols therefore need to be designed with future developments in mind.

This class is being recorded

Quantum Computers

A quantum computer is built using extremely small components, like single atoms or microscopic superconducting circuits. These small components behave quantum-mechanically, and their memories can be in a superposition of many different values at the same time.

Quantum computers can run quantum algorithms, which take advantage of superposition and can solve certain problems much faster than any classical computer.

Quantum algorithms cannot run on a classical computer. The classification of efficient/inefficient algorithms is different on a quantum computer.

For some problems, a quantum computer will be much faster. For others, it offers little or no improvement.

This class is being recorded

Quantum Algorithms for Crypto

Shor's algorithm: Solves factoring and discrete log efficiently. (The time is limited by the time to perform modular exponentiation.)

Consequence: RSA and Diffie-Hellman (including with elliptic curves) are insecure against a quantum computer.

Grover's algorithm: Speeds up exhaustive search from $O(N)$ to $O(\sqrt{N})$.

Consequence: AES and other symmetric cryptosystems need to double key lengths to retain the same level of security against a quantum computer.

Collision-finding: Instead of a birthday attack needing $O(\sqrt{N})$ hash function evaluations, needs $O(N^{1/3})$.

Consequence: Hash functions need to increase output lengths by x1.5 to retain the same level of security against a quantum computer.

This class is being recorded

Quantum Timelines

Today's quantum computers have ~100 qubits (= quantum bits).

> Cryptographic algorithms probably require on the order of 1 million high-fidelity qubits.

How long will this take?

> The IBM Quantum roadmap says that they will have 4,000 qubit devices in 2025.

It's certainly possible that quantum computers will be a threat to cryptographic systems in 20 years.

> So we need protection against quantum computation for any protocol likely to last that long and for anything that needs to stay secret for that long.

This class is being recorded

Post-Quantum Cryptography

The main need is a replacement for public key cryptography.

One approach, known as post-quantum cryptography, is to design new practical public-key encryption/KEM and digital signature protocols.

The idea is to base the security off of different computational problems with no known quantum algorithm to break them.

We will discuss this more next week.

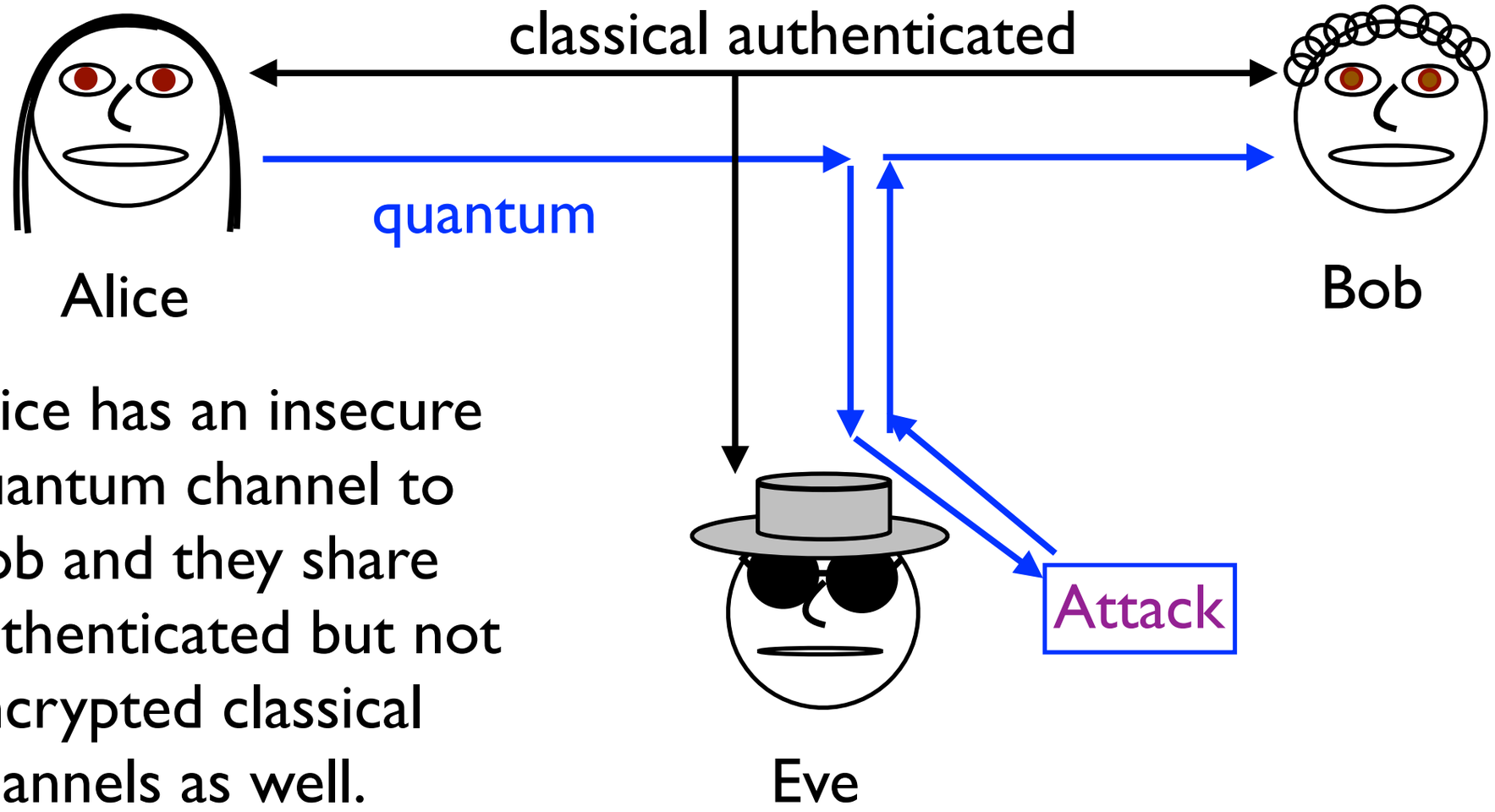
Note, though, that these protocols will still be vulnerable to breakthroughs in classical or quantum algorithms.

This class is being recorded

Quantum Key Distribution

Another option is to leverage properties of quantum mechanics to make a new kind of key exchange protocol.

It is known as quantum key distribution (QKD) and involves Alice and Bob sending quantum states between them.



Alice has an insecure quantum channel to Bob and they share authenticated but not encrypted classical channels as well.

This class is being recorded

Some Quantum Properties

Here are two relevant properties of quantum states:

No-Cloning Theorem: There is no quantum operation that will take an arbitrary quantum state and make two copies of it.

Information-Disturbance Relation: Any measurement to learn some information about a quantum state will alter it.

These are related properties:

- If you could make copies of a quantum state, you could learn information by measuring only the copies.
- If you could gain information about a state without changing it, you could make many measurements to learn all about it and then make a new copy from scratch.

This class is being recorded

Different Bases

Quantum states are vectors in a complex vector space with an inner product (a Hilbert space).

> The main thing we need to know is that a single qubit has states corresponding to different bases of the Hilbert space.

In particular, we can consider an "X basis" and a "Z basis."

Z basis states: $|0\rangle$ and $|1\rangle$.

X basis states: $|+\rangle$ and $|-\rangle$.

Angle brackets denote a quantum state.

We can think of the Z basis states as the usual bit values. The X basis states are two different superpositions of $|0\rangle$ and $|1\rangle$.

> We can also think of $|+\rangle$ and $|-\rangle$ as the X-basis versions of 0 and 1.

This class is being recorded

Measurements

To learn about a quantum state (i.e., to convert quantum information into classical information), we need to measure it.

We can make measurements in different bases.

- A Z-basis measurement on a Z-basis state gives the index of the state, i.e. $|0\rangle$ gives result 0 and $|1\rangle$ gives result 1.
- An X-basis measurement on an X-basis state gives the X-basis value, i.e. $|+\rangle$ gives result 0 and $|-\rangle$ gives result 1.
- An X-basis measurement on a Z-basis state gives a random result: 50% prob. of 0 and 50% prob. of 1 regardless of state.
- A Z-basis measurement on an X-basis state gives a random result: 50% prob. of 0 and 50% prob. of 1 regardless of state.

Repeating the same type of measurement twice in a row will give the same result. But switching measurement types will result in random results (measurement-disturbance).

This class is being recorded

BB84 Protocol

This class is being recorded

BB84 Protocol

1. Alice chooses many random bits and bases and sends the corresponding qubit states to Bob. E.g., if she chooses basis X and bit 1, she sends $|-\rangle$.

This class is being recorded

BB84 Protocol

1. Alice chooses many random bits and bases and sends the corresponding qubit states to Bob. E.g., if she chooses basis X and bit 1, she sends $|-\rangle$.
2. For each qubit received, Bob chooses a random basis to measure in and records the resulting bit values.

This class is being recorded

BB84 Protocol

1. Alice chooses many random bits and bases and sends the corresponding qubit states to Bob. E.g., if she chooses basis X and bit 1, she sends $|-\rangle$.
2. For each qubit received, Bob chooses a random basis to measure in and records the resulting bit values.
3. Alice announces the bases she used and Alice and Bob discard any bit values corresponding to a qubit where Bob guessed the wrong basis to measure in. At this point, in an ideal world, Alice and Bob would have identical bit strings.

This class is being recorded

BB84 Protocol

1. Alice chooses many random bits and bases and sends the corresponding qubit states to Bob. E.g., if she chooses basis X and bit 1, she sends $|-\rangle$.
2. For each qubit received, Bob chooses a random basis to measure in and records the resulting bit values.
3. Alice announces the bases she used and Alice and Bob discard any bit values corresponding to a qubit where Bob guessed the wrong basis to measure in. At this point, in an ideal world, Alice and Bob would have identical bit strings.
4. Alice and Bob choose a subset of bits to announce and compare using the classical channels. If the error rate is too high, they abort the protocol.

This class is being recorded

BB84 Protocol

1. Alice chooses many random bits and bases and sends the corresponding qubit states to Bob. E.g., if she chooses basis X and bit 1, she sends $|-\rangle$.
2. For each qubit received, Bob chooses a random basis to measure in and records the resulting bit values.
3. Alice announces the bases she used and Alice and Bob discard any bit values corresponding to a qubit where Bob guessed the wrong basis to measure in. At this point, in an ideal world, Alice and Bob would have identical bit strings.
4. Alice and Bob choose a subset of bits to announce and compare using the classical channels. If the error rate is too high, they abort the protocol.
5. Error correction: Alice and Bob use error-correcting codes to eliminate any disagreements in their bit strings.

This class is being recorded

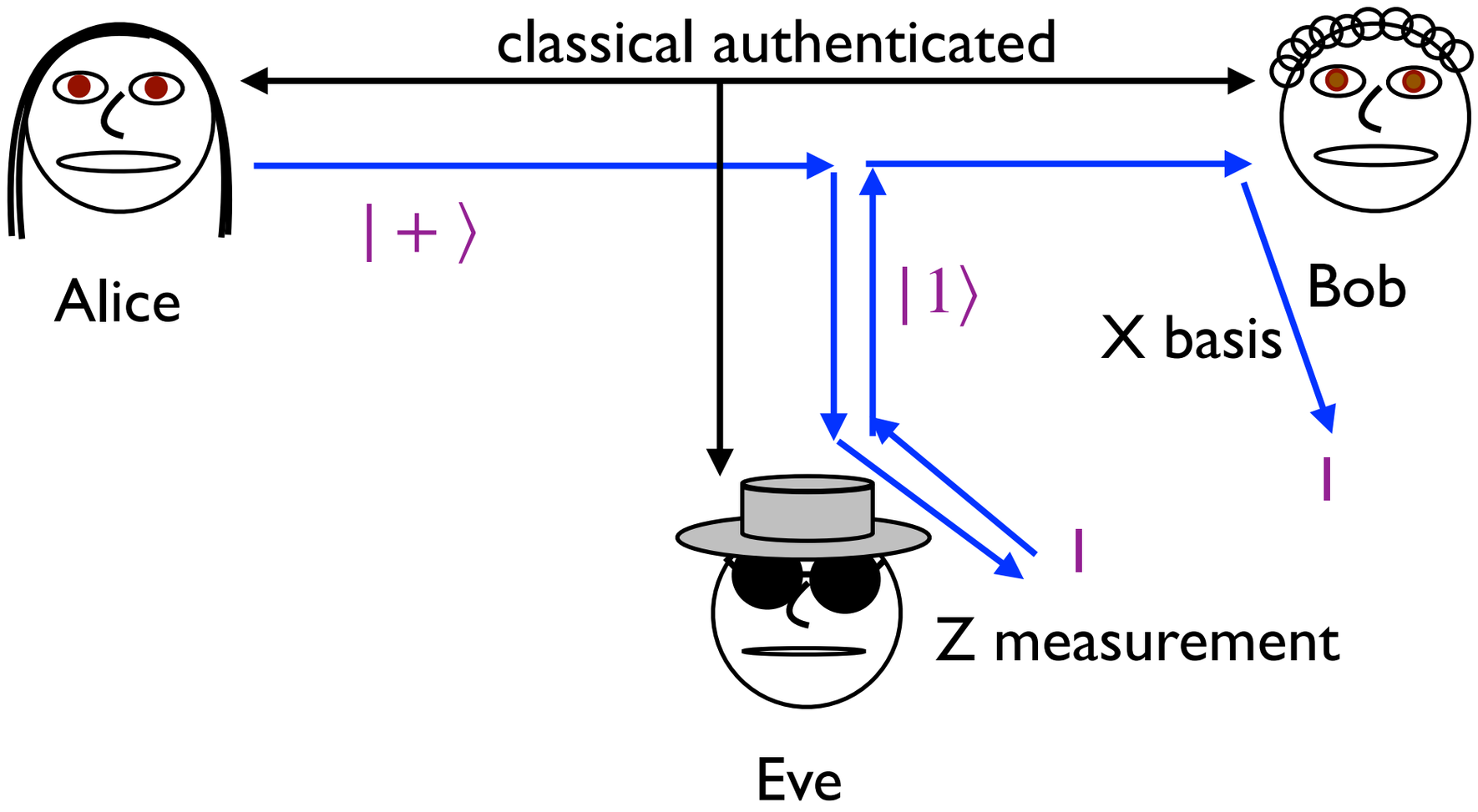
BB84 Protocol

1. Alice chooses many random bits and bases and sends the corresponding qubit states to Bob. E.g., if she chooses basis X and bit 1, she sends $|-\rangle$.
2. For each qubit received, Bob chooses a random basis to measure in and records the resulting bit values.
3. Alice announces the bases she used and Alice and Bob discard any bit values corresponding to a qubit where Bob guessed the wrong basis to measure in. At this point, in an ideal world, Alice and Bob would have identical bit strings.
4. Alice and Bob choose a subset of bits to announce and compare using the classical channels. If the error rate is too high, they abort the protocol.
5. Error correction: Alice and Bob use error-correcting codes to eliminate any disagreements in their bit strings.
6. Privacy amplification: Alice and Bob choose random parities of their bit strings to use as their final key.

This class is being recorded

Security Intuition

Since Alice does not announce her choice of basis, Eve has to guess which one to use. If she guesses wrong and Bob guesses right (50% chance), she can introduce errors (50% chance).



This class is being recorded

Post-Processing

The error correction step is needed to remove any naturally-occuring errors introduced during transmission of the state.

The privacy amplification step eliminates any small amounts of information Eve might have gained.

> Eve might have gotten lucky and learned one bit without introducing any errors.
> And a small number of errors could have been caused by Eve but they also could have been caused by noisy quantum communication. So we can't rule out that Eve knows a few qubits.

But in order to successfully predict the parity of a subset of bit values, Eve must know all of the bits in the subset.

This class is being recorded

Information-Theoretic Security

We can rigorously prove (with *no* computational assumption) that either

1. Eve is detected by Alice and Bob with very high probability, or
2. Alice and Bob generate a shared key about which Eve has very little information.

This proof holds against arbitrary attacks by Eve consistent with the threat model: I.e., Eve may measure and modify the states in the quantum communications channel as much as she likes.

In particular, there is no limit on the amount of computation Eve is allowed to do.

Security is information-theoretic like the one-time pad. (Sometimes referred to as unconditional security.)

This class is being recorded

Authenticated Channels

It is necessary that the classical channels be authenticated to avoid a man-in-the-middle attack.

There exist classical one-time MACs with information-theoretic security and small keys.

So:

- QKD upgrades symmetric-key cryptography to provide information-theoretic security for many uses with a small key (by continually refreshing keys for the one-time pad).
- It also upgrades public-key cryptography to provide forward secrecy with information-theoretic future security: Use digital signatures to provide the authentication; even if the computational assumption underlying the digital signatures fails in the future, it is too late to play man-in-the-middle and subvert the QKD protocol.

This class is being recorded

Quantum Repeaters

Because QKD cannot distinguish between errors caused by natural noise and errors caused by an eavesdropper (who will try to hide by imitating real noise), over long distances (hundreds of km), QKD stops working.

> To reach longer distances, QKD needs repeaters to regenerate the signal and correct errors.
>
> However, a normal classical repeater will measure the state and make copies of it. This will again look like an eavesdropper and so will not work for QKD.

To make a quantum network capable of supporting QKD, we need quantum repeaters which correct errors in a quantum-mechanically coherent way.

This class is being recorded

Technology for QKD

QKD is fundamentally much easier than quantum computers to build, since it only requires transmission of single qubits.

The quantum states needed for QKD can be transmitted using single photons (quantum particles of light).

Consequently, QKD devices already exist and have been commercially available for nearly 20 years.

However, quantum repeaters are more difficult and still only exist in experimental prototype form.
Progress has been slower than for quantum computers, even though they require fewer qubits.

Another approach to extending distance is to use a satellite as a relay.

This class is being recorded

Limitations of QKD

- QKD is not a full replacement for public key cryptography. In particular, it doesn't provide a good way to replace digital signatures and can't replace the existing certificate authority and public key infrastructure.
- Without quantum repeaters, the range is limited. A stop-gap is to assume trusted intermediate nodes, but that is a big potential security hole.
- QKD does not have any particular protection against denial of service, side-channel attacks and other attacks based on the implementation, although the relevant attacks are different than for classical cryptosystems.
- Currently, the rate of key generation is significantly lower than classical communication rates. Sometimes instead of using the keys generated by QKD for a one-time pad, they are instead used to re-key AES or another symmetric system, but that surrenders information-theoretic security.

This class is being recorded