

Quantum Cryptography

Quantum Cryptography

Lecture 27

And that will be all...

Quantum Cryptography

Quantum Cryptography

- Quantum information: Using microscopic physical state of “quantum systems” (spin of atoms/sub-atomic particles, polarization of photons etc.) to encode information (and generate randomness)

Quantum Cryptography

- Quantum information: Using microscopic physical state of “quantum systems” (spin of atoms/sub-atomic particles, polarization of photons etc.) to encode information (and generate randomness)
- **Quantum Key-Distribution**: Can expand a short (one-time) shared secret key into a long one over public channels, **without computational restrictions on the adversary**, (with some physical idealization assumptions, and assuming quantum mechanics)

Quantum Cryptography

- Quantum information: Using microscopic physical state of “quantum systems” (spin of atoms/sub-atomic particles, polarization of photons etc.) to encode information (and generate randomness)
- **Quantum Key-Distribution**: Can expand a short (one-time) shared secret key into a long one over public channels, **without computational restrictions on the adversary**, (with some physical idealization assumptions, and assuming quantum mechanics)
 - Need special “quantum channels” (optic fibers, free space...)

Quantum Cryptography

- Quantum information: Using microscopic physical state of “quantum systems” (spin of atoms/sub-atomic particles, polarization of photons etc.) to encode information (and generate randomness)
- **Quantum Key-Distribution**: Can expand a short (one-time) shared secret key into a long one over public channels, **without computational restrictions on the adversary**, (with some physical idealization assumptions, and assuming quantum mechanics)
 - Need special “quantum channels” (optic fibers, free space...)
 - Commercially available today

Quantum Cryptography

- Quantum information: Using microscopic physical state of “quantum systems” (spin of atoms/sub-atomic particles, polarization of photons etc.) to encode information (and generate randomness)
- **Quantum Key-Distribution**: Can expand a short (one-time) shared secret key into a long one over public channels, **without computational restrictions on the adversary**, (with some physical idealization assumptions, and assuming quantum mechanics)
 - Need special “quantum channels” (optic fibers, free space...)
 - Commercially available today
- Beyond QKD: some (limited) multi-party computation results; also, security for “quantum information”

Qubits

Qubits

- State of a system (or of some aspect of it -- like polarization of a photon) is represented, according to quantum mechanics, by a vector of complex numbers

Qubits

- State of a system (or of some aspect of it -- like polarization of a photon) is represented, according to quantum mechanics, by a vector of complex numbers
- We will use such a system to encode discrete information (bits)

Qubits

- State of a system (or of some aspect of it -- like polarization of a photon) is represented, according to quantum mechanics, by a vector of complex numbers
- We will use such a system to encode discrete information (bits)
- Qubit refers to a quantum state that allows encoding (and decoding) one bit of information

Qubits

- State of a system (or of some aspect of it -- like polarization of a photon) is represented, according to quantum mechanics, by a vector of complex numbers
- We will use such a system to encode discrete information (bits)
- Qubit refers to a quantum state that allows encoding (and decoding) one bit of information
- But there are several possible ways to encode/decode the information, leading to interesting properties

Qubits

- State of a system (or of some aspect of it -- like polarization of a photon) is represented, according to quantum mechanics, by a vector of complex numbers
- We will use such a system to encode discrete information (bits)
- Qubit refers to a quantum state that allows encoding (and decoding) one bit of information
- But there are several possible ways to encode/decode the information, leading to interesting properties
- A system of multiple qubits shows even more interesting properties, beyond just holding all the bits of information

Measuring

Measuring

- Measurement: reading the state of a qubit (presumably to decode the information encoded in it)

Measuring

- Measurement: reading the state of a qubit (presumably to decode the information encoded in it)
- Basic principle: measuring alters the system

Measuring

- Measurement: reading the state of a qubit (presumably to decode the information encoded in it)
- **Basic principle: measuring alters the system**
- A metaphor: need to read the direction of a virtual needle using a "cross"

Measuring

- Measurement: reading the state of a qubit (presumably to decode the information encoded in it)
- **Basic principle: measuring alters the system**
- A metaphor: need to read the direction of a virtual needle using a "cross"
 - If either leg of the cross is aligned with the needle, we just learn its alignment (nothing happens to the needle)

Measuring

- Measurement: reading the state of a qubit (presumably to decode the information encoded in it)
- **Basic principle: measuring alters the system**
- A metaphor: need to read the direction of a virtual needle using a "cross"
 - If either leg of the cross is aligned with the needle, we just learn its alignment (nothing happens to the needle)
 - Otherwise the needle will move to one of the legs, and we learn which one

Measuring

- Measurement: reading the state of a qubit (presumably to decode the information encoded in it)
- **Basic principle: measuring alters the system**
- A metaphor: need to read the direction of a virtual needle using a "cross"
 - If either leg of the cross is aligned with the needle, we just learn its alignment (nothing happens to the needle)
 - Otherwise the needle will move to one of the legs, and we learn which one
 - To which leg it moves is probabilistic, depending on its original position (which we do not learn)

Measuring

- Measurement: reading the state of a qubit (presumably to decode the information encoded in it)
- **Basic principle: measuring alters the system**
- A metaphor: need to read the direction of a virtual needle using a "cross"
 - If either leg of the cross is aligned with the needle, we just learn its alignment (nothing happens to the needle)
 - Otherwise the needle will move to one of the legs, and we learn which one
 - To which leg it moves is probabilistic, depending on its original position (which we do not learn)
 - In either case at the end the needle is aligned along a leg of the cross (as reported by the measurement)

Measuring: Another metaphor

Measuring: Another metaphor

- Qubits as “cards” that can be read using “card readers”

Measuring: Another metaphor

- Qubits as "cards" that can be read using "card readers"
- Cards come in two colors (red and blue), and have a value 0/1 on them. Cannot tell the color or the value of a card w/o "reading" it

Measuring: Another metaphor

- Qubits as "cards" that can be read using "card readers"
- Cards come in two colors (red and blue), and have a value 0/1 on them. Cannot tell the color or the value of a card w/o "reading" it
 - If a red card is inserted into a red reader, it reports the value on the card correctly

Measuring: Another metaphor

- Qubits as "cards" that can be read using "card readers"
- Cards come in two colors (red and blue), and have a value 0/1 on them. Cannot tell the color or the value of a card w/o "reading" it
 - If a red card is inserted into a red reader, it reports the value on the card correctly
 - If a red card is read by a blue reader, then the card gets transformed into a blue card with a random value!

Measuring: Another metaphor

- Qubits as "cards" that can be read using "card readers"
- Cards come in two colors (red and blue), and have a value 0/1 on them. Cannot tell the color or the value of a card w/o "reading" it
 - If a red card is inserted into a red reader, it reports the value on the card correctly
 - If a red card is read by a blue reader, then the card gets transformed into a blue card with a random value!
 - And the reader will report that value

Measuring: Another metaphor

- Qubits as “cards” that can be read using “card readers”
- Cards come in two colors (red and blue), and have a value 0/1 on them. Cannot tell the color or the value of a card w/o “reading” it
 - If a red card is inserted into a red reader, it reports the value on the card correctly
 - If a red card is read by a blue reader, then the card gets transformed into a blue card with a random value!
 - And the reader will report that value
- Think of color as “axis-parallel” or “diagonal” needle/cross position

Measuring: Another metaphor

- Qubits as "cards" that can be read using "card readers"
- Cards come in two colors (red and blue), and have a value 0/1 on them. Cannot tell the color or the value of a card w/o "reading" it
 - If a red card is inserted into a red reader, it reports the value on the card correctly
 - If a red card is read by a blue reader, then the card gets transformed into a blue card with a random value!
 - And the reader will report that value
- Think of color as "axis-parallel" or "diagonal" needle/cross position
 - Note: not exploiting all possibilities, but already useful

BB84

BB84

- A protocol for “key distribution” by Bennett and Brassard

BB84

- A protocol for “key distribution” by Bennett and Brassard
- Alice and Bob want to generate a long one time pad (for information theoretically secure encryption)

BB84

- A protocol for “key distribution” by Bennett and Brassard
- Alice and Bob want to generate a long one time pad (for information theoretically secure encryption)
- But only public channels to communicate over

BB84

- A protocol for “key distribution” by Bennett and Brassard
- Alice and Bob want to generate a long one time pad (for information theoretically secure encryption)
- But only public channels to communicate over
 - Suppose in addition a “quantum channel” (controlled by the adversary) to send qubits

BB84

- A protocol for “key distribution” by Bennett and Brassard
- Alice and Bob want to generate a long one time pad (for information theoretically secure encryption)
- But only public channels to communicate over
 - Suppose in addition a “quantum channel” (controlled by the adversary) to send qubits
 - And the public channel is authenticated (for now), so that the adversary cannot inject messages into it

BB84

- A protocol for “key distribution” by Bennett and Brassard
- Alice and Bob want to generate a long one time pad (for information theoretically secure encryption)
- But only public channels to communicate over
 - Suppose in addition a “quantum channel” (controlled by the adversary) to send qubits
 - And the public channel is authenticated (for now), so that the adversary cannot inject messages into it
- BB84 allows them to generate a secret shared keys

BB84

- A protocol for “key distribution” by Bennett and Brassard
- Alice and Bob want to generate a long one time pad (for information theoretically secure encryption)
- But only public channels to communicate over
 - Suppose in addition a “quantum channel” (controlled by the adversary) to send qubits
 - And the public channel is authenticated (for now), so that the adversary cannot inject messages into it
- BB84 allows them to generate a secret shared keys
- Will describe in terms of red/blue cards and card-readers

BB84

BB84

- Alice prepares several cards, randomly colored and with random values (all of which she knows)

BB84

- Alice prepares several cards, randomly colored and with random values (all of which she knows)
- She sends the cards to Bob (through an unfaithful courier)

BB84

- Alice prepares several cards, randomly colored and with random values (all of which she knows)
- She sends the cards to Bob (through an unfaithful courier)
- Bob reads all the cards using red or blue readers randomly

BB84

- Alice prepares several cards, randomly colored and with random values (all of which she knows)
- She sends the cards to Bob (through an unfaithful courier)
- Bob reads all the cards using red or blue readers randomly
- Bob publicly tells Alice which color reader was used for each card. Now Alice tells Bob which color each card was.

BB84

- Alice prepares several cards, randomly colored and with random values (all of which she knows)
- She sends the cards to Bob (through an unfaithful courier)
- Bob reads all the cards using red or blue readers randomly
- Bob publicly tells Alice which color reader was used for each card. Now Alice tells Bob which color each card was.
- Bob discards all cards where he chose the wrong color

BB84

- Alice prepares several cards, randomly colored and with random values (all of which she knows)
- She sends the cards to Bob (through an unfaithful courier)
- Bob reads all the cards using red or blue readers randomly
- Bob publicly tells Alice which color reader was used for each card. Now Alice tells Bob which color each card was.
- Bob discards all cards where he chose the wrong color
- Among the other cards, Alice and Bob check for consistency: Bob sends the values he obtained for a random subset of the cards; if any value is wrong, Alice alerts Bob and they abort the protocol (or try to "reconcile" the difference)

BB84

- Alice prepares several cards, randomly colored and with random values (all of which she knows)
- She sends the cards to Bob (through an unfaithful courier)
- Bob reads all the cards using red or blue readers randomly
- Bob publicly tells Alice which color reader was used for each card. Now Alice tells Bob which color each card was.
- Bob discards all cards where he chose the wrong color
- Among the other cards, Alice and Bob check for consistency: Bob sends the values he obtained for a random subset of the cards; if any value is wrong, Alice alerts Bob and they abort the protocol (or try to "reconcile" the difference)
- Else Alice and Bob "almost agree on" the values on the remaining cards and it is "mostly hidden" from Eve: Raw keys

BB84

BB84

- Alice and Bob “almost agree on” the values on the remaining cards and it is “mostly hidden” from Eve: **Raw keys**

BB84

- Alice and Bob “almost agree on” the values on the remaining cards and it is “mostly hidden” from Eve: **Raw keys**
 - Why (intuitively)?

BB84

- Alice and Bob “almost agree on” the values on the remaining cards and it is “mostly hidden” from Eve: **Raw keys**
- Why (intuitively)?
- **No-cloning**: Eve cannot save copies of the cards

BB84

- Alice and Bob “almost agree on” the values on the remaining cards and it is “mostly hidden” from Eve: **Raw keys**
 - Why (intuitively)?
 - **No-cloning**: Eve cannot save copies of the cards
 - If Eve reads a card (using red or blue reader) she doesn't know its original color

BB84

- Alice and Bob “almost agree on” the values on the remaining cards and it is “mostly hidden” from Eve: **Raw keys**
 - Why (intuitively)?
 - **No-cloning**: Eve cannot save copies of the cards
 - If Eve reads a card (using red or blue reader) she doesn't know its original color
 - Suppose she sends it to Bob as a blue card, but originally the card was red. Suppose Bob reads it using red reader

BB84

- Alice and Bob “almost agree on” the values on the remaining cards and it is “mostly hidden” from Eve: **Raw keys**
 - Why (intuitively)?
 - **No-cloning**: Eve cannot save copies of the cards
 - If Eve reads a card (using red or blue reader) she doesn't know its original color
 - Suppose she sends it to Bob as a blue card, but originally the card was red. Suppose Bob reads it using red reader
 - Consistency check will discover the tampering if the random value obtained by Bob doesn't match original value on card

BB84

- Alice and Bob “almost agree on” the values on the remaining cards and it is “mostly hidden” from Eve: **Raw keys**
- Why (intuitively)?
- **No-cloning**: Eve cannot save copies of the cards
- If Eve reads a card (using red or blue reader) she doesn't know its original color
 - Suppose she sends it to Bob as a blue card, but originally the card was red. Suppose Bob reads it using red reader
 - Consistency check will discover the tampering if the random value obtained by Bob doesn't match original value on card
- Eve might get lucky and remain undetected if she alters only a few cards (so Alice and Bob may disagree on those cards)

BB84

- Alice and Bob “almost agree on” the values on the remaining cards and it is “mostly hidden” from Eve: **Raw keys**
 - Why (intuitively)?
 - **No-cloning**: Eve cannot save copies of the cards
 - If Eve reads a card (using red or blue reader) she doesn't know its original color
 - Suppose she sends it to Bob as a blue card, but originally the card was red. Suppose Bob reads it using red reader
 - Consistency check will discover the tampering if the random value obtained by Bob doesn't match original value on card
 - Eve might get lucky and remain undetected if she alters only a few cards (so Alice and Bob may disagree on those cards)
 - But then Eve can read only (at most) those cards

Raw Keys to Good Keys

Raw Keys to Good Keys

- Raw Keys:

Raw Keys to Good Keys

- Raw Keys:
 - There maybe a few positions where Alice's and Bob's copies of the keys differ

Raw Keys to Good Keys

- Raw Keys:
 - There maybe a few positions where Alice's and Bob's copies of the keys differ
 - Eve might have some information about the keys

Raw Keys to Good Keys

- Raw Keys:
 - There maybe a few positions where Alice's and Bob's copies of the keys differ
 - Eve might have some information about the keys
- Distilling raw keys to good (i.e., almost uniformly random) keys is important in other contexts too

Raw Keys to Good Keys

- Raw Keys:
 - There maybe a few positions where Alice's and Bob's copies of the keys differ
 - Eve might have some information about the keys
- Distilling raw keys to good (i.e., almost uniformly random) keys is important in other contexts too
- Two step (classical) protocol, over authenticated public channel

Raw Keys to Good Keys

- Raw Keys:
 - There maybe a few positions where Alice's and Bob's copies of the keys differ
 - Eve might have some information about the keys
- Distilling raw keys to good (i.e., almost uniformly random) keys is important in other contexts too
- Two step (classical) protocol, over authenticated public channel
 - **Reconciliation**: Alice and Bob calculate and compare several randomized "parity check bits" to isolate and discard errors

Raw Keys to Good Keys

- Raw Keys:
 - There maybe a few positions where Alice's and Bob's copies of the keys differ
 - Eve might have some information about the keys
- Distilling raw keys to good (i.e., almost uniformly random) keys is important in other contexts too
- Two step (classical) protocol, over authenticated public channel
 - **Reconciliation**: Alice and Bob calculate and compare several randomized "parity check bits" to isolate and discard errors
 - This reveals further information to Eve, but now Alice and Bob agree on the same key (with overwhelming probability)

Raw Keys to Good Keys

- Raw Keys:
 - There maybe a few positions where Alice's and Bob's copies of the keys differ
 - Eve might have some information about the keys
- Distilling raw keys to good (i.e., almost uniformly random) keys is important in other contexts too
- Two step (classical) protocol, over authenticated public channel
 - **Reconciliation**: Alice and Bob calculate and compare several randomized "parity check bits" to isolate and discard errors
 - This reveals further information to Eve, but now Alice and Bob agree on the same key (with overwhelming probability)
 - **Privacy amplification**: Use an extractor to extract a suitably shorter key so that Eve has little information about the new key

Raw Keys to Good Keys

- Raw Keys:
 - There maybe a few positions where Alice's and Bob's copies of the keys differ
 - Eve might have some information about the keys
- Distilling raw keys to good (i.e., almost uniformly random) keys is important in other contexts too
- Two step (classical) protocol, over authenticated public channel
 - **Reconciliation**: Alice and Bob calculate and compare several randomized "parity check bits" to isolate and discard errors
 - This reveals further information to Eve, but now Alice and Bob agree on the same key (with overwhelming probability)
 - **Privacy amplification**: Use an extractor to extract a suitably shorter key so that Eve has little information about the new key
 - Alice picks a seed at random and publicly sends it to Bob; shared key is defined as $\text{Extract}(\text{RawKey}, \text{Seed})$

Using QKD

Using QKD

- Alice and Bob need an authenticated public-channel

Using QKD

- Alice and Bob need an authenticated public-channel
 - Can use one-time MAC with a short key (2-Universal Hash functions work)

Using QKD

- Alice and Bob need an authenticated public-channel
 - Can use one-time MAC with a short key (2-Universal Hash functions work)
- Originally several idealizations required for security: crucially depends on reliable quantum channels and devices

Using QKD

- Alice and Bob need an authenticated public-channel
 - Can use one-time MAC with a short key (2-Universal Hash functions work)
- Originally several idealizations required for security: crucially depends on reliable quantum channels and devices
 - Many idealizations can be removed using quantum error-correction, quantum repeaters, self-testing devices

Using QKD

- Alice and Bob need an authenticated public-channel
 - Can use one-time MAC with a short key (2-Universal Hash functions work)
- Originally several idealizations required for security: crucially depends on reliable quantum channels and devices
 - Many idealizations can be removed using quantum error-correction, quantum repeaters, self-testing devices
 - Commercial products available

Using QKD

- Alice and Bob need an authenticated public-channel
 - Can use one-time MAC with a short key (2-Universal Hash functions work)
- Originally several idealizations required for security: crucially depends on reliable quantum channels and devices
 - Many idealizations can be removed using quantum error-correction, quantum repeaters, self-testing devices
- Commercial products available



Quantum Channel

Quantum Channel

- Transmitting an unknown qubit is delicate (even if uncertainty is a single bit of information): the entire state needs to be sent over a "quantum channel"

Quantum Channel

- Transmitting an unknown qubit is delicate (even if uncertainty is a single bit of information): the entire state needs to be sent over a "quantum channel"
- Recall that one may not be able to measure the information accurately. (Else could have used a classical channel to send that information)

Quantum Channel

- Transmitting an unknown qubit is delicate (even if uncertainty is a single bit of information): the entire state needs to be sent over a “quantum channel”
 - Recall that one may not be able to measure the information accurately. (Else could have used a classical channel to send that information)
 - e.g.: optic fibers carrying photons

Quantum Channel

- Transmitting an unknown qubit is delicate (even if uncertainty is a single bit of information): the entire state needs to be sent over a “quantum channel”
 - Recall that one may not be able to measure the information accurately. (Else could have used a classical channel to send that information)
 - e.g.: optic fibers carrying photons
- Quantum teleportation: Pre-processing quantum communication

Quantum Channel

- Transmitting an unknown qubit is delicate (even if uncertainty is a single bit of information): the entire state needs to be sent over a “quantum channel”
 - Recall that one may not be able to measure the information accurately. (Else could have used a classical channel to send that information)
 - e.g.: optic fibers carrying photons
- Quantum teleportation: Pre-processing quantum communication
 - If share some “entangled” qubits are shared a priori, then can use a classical channel to “teleport” an unknown qubit (without reading it)

Entanglements

Entanglements

- A system with multiple qubits exhibits complex behavior

Entanglements

- A system with multiple qubits exhibits complex behavior
- Two qubits can be correlated in more ways than two cards (or needles) can be (classically)

Entanglements

- A system with multiple qubits exhibits complex behavior
- Two qubits can be correlated in more ways than two cards (or needles) can be (classically)
 - And more than even cards with hidden state variables (other than color and value)

Entanglements

- A system with multiple qubits exhibits complex behavior
- Two qubits can be correlated in more ways than two cards (or needles) can be (classically)
 - And more than even cards with hidden state variables (other than color and value)
 - Called entanglement

Entanglements

- A system with multiple qubits exhibits complex behavior
- Two qubits can be correlated in more ways than two cards (or needles) can be (classically)
 - And more than even cards with hidden state variables (other than color and value)
 - Called entanglement
 - “EPR (Einstein–Podolsky–Rosen) paradox”: spooky action at a distance

Entanglements

- A system with multiple qubits exhibits complex behavior
- Two qubits can be correlated in more ways than two cards (or needles) can be (classically)
 - And more than even cards with hidden state variables (other than color and value)
 - Called entanglement
 - “EPR (Einstein–Podolsky–Rosen) paradox”: spooky action at a distance
 - Measuring two entangled qubits (cards) appears co-ordinated, as if the two card readers communicate with each other

Entanglements

- A system with multiple qubits exhibits complex behavior
- Two qubits can be correlated in more ways than two cards (or needles) can be (classically)
 - And more than even cards with hidden state variables (other than color and value)
 - Called entanglement
 - “EPR (Einstein–Podolsky–Rosen) paradox”: spooky action at a distance
 - Measuring two entangled qubits (cards) appears co-ordinated, as if the two card readers communicate with each other
- Bell inequality: showing, more generally, limit of correlation than is possible classically. Experimentally violated by quantum systems (with caveats)

QKD History

QKD History

- Bennett and Brassard proposed BB84 in 1984

QKD History

- Bennett and Brassard proposed BB84 in 1984
 - Similar ideas by Wiesner in early 1970s

QKD History

- Bennett and Brassard proposed BB84 in 1984
 - Similar ideas by Wiesner in early 1970s
- QKD scheme based on entanglement by Ekert in 1990

QKD History

- Bennett and Brassard proposed BB84 in 1984
 - Similar ideas by Wiesner in early 1970s
- QKD scheme based on entanglement by Ekert in 1990
- Several other schemes by now

QKD History

- Bennett and Brassard proposed BB84 in 1984
 - Similar ideas by Wiesner in early 1970s
- QKD scheme based on entanglement by Ekert in 1990
- Several other schemes by now
- Security definitions originally based on information leaked to Eve

QKD History

- Bennett and Brassard proposed BB84 in 1984
 - Similar ideas by Wiesner in early 1970s
- QKD scheme based on entanglement by Ekert in 1990
- Several other schemes by now
- Security definitions originally based on information leaked to Eve
 - But key distribution needs composability (because key will be used for other tasks later, and attack may not be separately on QKD and subsequent use)

QKD History

- Bennett and Brassard proposed BB84 in 1984
 - Similar ideas by Wiesner in early 1970s
- QKD scheme based on entanglement by Ekert in 1990
- Several other schemes by now
- Security definitions originally based on information leaked to Eve
 - But key distribution needs composability (because key will be used for other tasks later, and attack may not be separately on QKD and subsequent use)
 - Universally Composable Security for QKD (2005)

QKD History

- Bennett and Brassard proposed BB84 in 1984
 - Similar ideas by Wiesner in early 1970s
- QKD scheme based on entanglement by Ekert in 1990
- Several other schemes by now
- Security definitions originally based on information leaked to Eve
 - But key distribution needs composability (because key will be used for other tasks later, and attack may not be separately on QKD and subsequent use)
 - Universally Composable Security for QKD (2005)
- Original proofs of security considered restricted Eve (e.g., in BB84 Eve that measured/transformed each transmitted qubit separately)

QKD History

- Bennett and Brassard proposed BB84 in 1984
 - Similar ideas by Wiesner in early 1970s
- QKD scheme based on entanglement by Ekert in 1990
- Several other schemes by now
- Security definitions originally based on information leaked to Eve
 - But key distribution needs composability (because key will be used for other tasks later, and attack may not be separately on QKD and subsequent use)
 - Universally Composable Security for QKD (2005)
- Original proofs of security considered restricted Eve (e.g., in BB84 Eve that measured/transformed each transmitted qubit separately)
 - Complete proof in 1996, followed by several refined proofs

QKD History

QKD History

- BB84 implemented at IBM Research in 1989: 32cm free air quantum channel

QKD History

- BB84 implemented at IBM Research in 1989: 32cm free air quantum channel
- Geneva, 2002: 23 km optical fiber cable quantum channel

QKD History

- BB84 implemented at IBM Research in 1989: 32cm free air quantum channel
- Geneva, 2002: 23 km optical fiber cable quantum channel
- DARPA network, Boston (since 2003): Between Boston University, Harvard and BBN Technologies

QKD History

- BB84 implemented at IBM Research in 1989: 32cm free air quantum channel
- Geneva, 2002: 23 km optical fiber cable quantum channel
- DARPA network, Boston (since 2003): Between Boston University, Harvard and BBN Technologies
 - With wireless links too

QKD History

- BB84 implemented at IBM Research in 1989: 32cm free air quantum channel
- Geneva, 2002: 23 km optical fiber cable quantum channel
- DARPA network, Boston (since 2003): Between Boston University, Harvard and BBN Technologies
 - With wireless links too
- Longer links, larger networks

QKD History

- BB84 implemented at IBM Research in 1989: 32cm free air quantum channel
- Geneva, 2002: 23 km optical fiber cable quantum channel
- DARPA network, Boston (since 2003): Between Boston University, Harvard and BBN Technologies
 - With wireless links too
- Longer links, larger networks
 - Possibly using "quantum repeaters"

Beyond QKD

Beyond QKD

- Information-theoretically secure coin-tossing

Beyond QKD

- Information-theoretically secure coin-tossing
 - Impossible classically

Beyond QKD

- Information-theoretically secure coin-tossing
 - Impossible classically
 - With quantum channels, known to exist when some limited adversarial bias is allowed

Beyond QKD

- Information-theoretically secure coin-tossing
 - Impossible classically
 - With quantum channels, known to exist when some limited adversarial bias is allowed
 - Zero bias coin-tossing is still impossible

Beyond QKD

- Information-theoretically secure coin-tossing
 - Impossible classically
 - With quantum channels, known to exist when some limited adversarial bias is allowed
 - Zero bias coin-tossing is still impossible
- Information-theoretically secure commitment?

Beyond QKD

- Information-theoretically secure coin-tossing
 - Impossible classically
 - With quantum channels, known to exist when some limited adversarial bias is allowed
 - Zero bias coin-tossing is still impossible
- Information-theoretically secure commitment?
 - Impossible even with quantum channels

Beyond QKD

- Information-theoretically secure coin-tossing
 - Impossible classically
 - With quantum channels, known to exist when some limited adversarial bias is allowed
 - Zero bias coin-tossing is still impossible
- Information-theoretically secure commitment?
 - Impossible even with quantum channels
- Secret-sharing: requiring quantum communication for reconstruction

Beyond QKD

Beyond QKD

- Quantum computation: a large field (still not practical), using quantum gates to manipulate qubits

Beyond QKD

- Quantum computation: a large field (still not practical), using quantum gates to manipulate qubits
 - “Efficient” algorithm for factorization

Beyond QKD

- Quantum computation: a large field (still not practical), using quantum gates to manipulate qubits
 - “Efficient” algorithm for factorization
- Cryptography for qubits

Beyond QKD

- Quantum computation: a large field (still not practical), using quantum gates to manipulate qubits
 - “Efficient” algorithm for factorization
- Cryptography for qubits
 - Authenticating qubits

Beyond QKD

- Quantum computation: a large field (still not practical), using quantum gates to manipulate qubits
 - “Efficient” algorithm for factorization
- Cryptography for qubits
 - Authenticating qubits
 - Encrypting qubits

Beyond QKD

- Quantum computation: a large field (still not practical), using quantum gates to manipulate qubits
 - “Efficient” algorithm for factorization
- Cryptography for qubits
 - Authenticating qubits
 - Encrypting qubits
 - Multi-party computation when inputs and outputs are qubits

Beyond QKD

- Quantum computation: a large field (still not practical), using quantum gates to manipulate qubits
 - “Efficient” algorithm for factorization
- Cryptography for qubits
 - Authenticating qubits
 - Encrypting qubits
 - Multi-party computation when inputs and outputs are qubits
 - Known when 5/6th-majority is honest

Beyond QKD

- Quantum computation: a large field (still not practical), using quantum gates to manipulate qubits
 - “Efficient” algorithm for factorization
- Cryptography for qubits
 - Authenticating qubits
 - Encrypting qubits
 - Multi-party computation when inputs and outputs are qubits
 - Known when 5/6th-majority is honest
- Classical/Quantum cryptography secure against computationally bounded quantum adversaries?

Beyond QKD

- Quantum computation: a large field (still not practical), using quantum gates to manipulate qubits
 - “Efficient” algorithm for factorization
- Cryptography for qubits
 - Authenticating qubits
 - Encrypting qubits
 - Multi-party computation when inputs and outputs are qubits
 - Known when 5/6th-majority is honest
- Classical/Quantum cryptography secure against computationally bounded quantum adversaries?
 - Several OWF candidates are not quantum-OWF

Quantum Cryptography

Quantum Cryptography

- Goal: Don't depend on computational restrictions on the adversary

Quantum Cryptography

- Goal: Don't depend on computational restrictions on the adversary
- Quantum Key Distribution: information theoretic security, if reliable quantum channels/devices available

Quantum Cryptography

- Goal: Don't depend on computational restrictions on the adversary
- Quantum Key Distribution: information theoretic security, if reliable quantum channels/devices available
 - Still needs a small (one-time) shared key to authenticate the classical channel (MAC)

Quantum Cryptography

- Goal: Don't depend on computational restrictions on the adversary
- Quantum Key Distribution: information theoretic security, if reliable quantum channels/devices available
 - Still needs a small (one-time) shared key to authenticate the classical channel (MAC)
 - Needs quantum channels: today limited to short distances

Quantum Cryptography

- Goal: Don't depend on computational restrictions on the adversary
- Quantum Key Distribution: information theoretic security, if reliable quantum channels/devices available
 - Still needs a small (one-time) shared key to authenticate the classical channel (MAC)
 - Needs quantum channels: today limited to short distances
- No magic bullet: not all functionalities of PKE; other cryptographic concepts (like commitment) remain impossible

Quantum Cryptography

- Goal: Don't depend on computational restrictions on the adversary
- Quantum Key Distribution: information theoretic security, if reliable quantum channels/devices available
 - Still needs a small (one-time) shared key to authenticate the classical channel (MAC)
 - Needs quantum channels: today limited to short distances
- No magic bullet: not all functionalities of PKE; other cryptographic concepts (like commitment) remain impossible
- Evolving theory and practice

A Quick Summary

A Quick Summary

- Encryption

A Quick Summary

- Encryption
- Authentication

A Quick Summary

- SKE/PKE, Homomorphic Encryption, IBE, ABE

- Encryption

- Authentication

A Quick Summary

- SKE/PKE, Homomorphic Encryption, IBE, ABE
- Security definitions: CPA/CCA

- Encryption

- Authentication

A Quick Summary

- SKE/PKE, Homomorphic Encryption, IBE, ABE
- Security definitions: CPA/CCA
- Abstractions: OWF/Hardcore bits, Trapdoor-OWP, ...

- Encryption

- Authentication

A Quick Summary

- Encryption

- Authentication

- SKE/PKE, Homomorphic Encryption, IBE, ABE
- Security definitions: CPA/CCA
- Abstractions: OWF/Hardcore bits, Trapdoor-OWP, ...
- Constructions: Using RSA, DDH, bilinear pairings, ...

A Quick Summary

- Encryption

- Authentication

- SKE/PKE, Homomorphic Encryption, IBE, ABE
- Security definitions: CPA/CCA
- Abstractions: OWF/Hardcore bits, Trapdoor-OWP, ...
- Constructions: Using RSA, DDH, bilinear pairings, ...

- Hash functions, MACs, Signatures, Ring sign. etc.

A Quick Summary

- Encryption

- SKE/PKE, Homomorphic Encryption, IBE, ABE
- Security definitions: CPA/CCA
- Abstractions: OWF/Hardcore bits, Trapdoor-OWP, ...
- Constructions: Using RSA, DDH, bilinear pairings, ...

- Authentication

- Hash functions, MACs, Signatures, Ring sign. etc.
- Security definitions: Collision resistance (various), existential forgery, ..

A Quick Summary

- Encryption

- SKE/PKE, Homomorphic Encryption, IBE, ABE
- Security definitions: CPA/CCA
- Abstractions: OWF/Hardcore bits, Trapdoor-OWP, ...
- Constructions: Using RSA, DDH, bilinear pairings, ...

- Authentication

- Hash functions, MACs, Signatures, Ring sign. etc.
- Security definitions: Collision resistance (various), existential forgery, ..
- Constructions: Based on hash functions (also Random Oracles + Trapdoor OWP)

A Quick Summary

- SKE/PKE, Homomorphic Encryption, IBE, ABE
 - Security definitions: CPA/CCA
 - Abstractions: OWF/Hardcore bits, Trapdoor-OWP, ...
 - Constructions: Using RSA, DDH, bilinear pairings, ...
- Encryption
 - Authentication
 - Secure multi-party computation
- Hash functions, MACs, Signatures, Ring sign. etc.
 - Security definitions: Collision resistance (various), existential forgery, ..
 - Constructions: Based on hash functions (also Random Oracles + Trapdoor OWP)

A Quick Summary

- SKE/PKE, Homomorphic Encryption, IBE, ABE
 - Security definitions: CPA/CCA
 - Abstractions: OWF/Hardcore bits, Trapdoor-OWP, ...
 - Constructions: Using RSA, DDH, bilinear pairings, ...
- Encryption
 - Authentication
 - Hash functions, MACs, Signatures, Ring sign. etc.
 - Security definitions: Collision resistance (various), existential forgery, ..
 - Constructions: Based on hash functions (also Random Oracles + Trapdoor OWP)
 - Secure multi-party computation
 - Oblivious Transfer, ZK Proofs, Yao's garbled circuit

A Quick Summary

- Encryption
 - SKE/PKE, Homomorphic Encryption, IBE, ABE
 - Security definitions: CPA/CCA
 - Abstractions: OWF/Hardcore bits, Trapdoor-OWP, ...
 - Constructions: Using RSA, DDH, bilinear pairings, ...
- Authentication
 - Hash functions, MACs, Signatures, Ring sign. etc.
 - Security definitions: Collision resistance (various), existential forgery, ..
 - Constructions: Based on hash functions (also Random Oracles + Trapdoor OWP)
- Secure multi-party computation
 - Oblivious Transfer, ZK Proofs, Yao's garbled circuit
 - Private set intersection

A Quick Summary

- Encryption
 - SKE/PKE, Homomorphic Encryption, IBE, ABE
 - Security definitions: CPA/CCA
 - Abstractions: OWF/Hardcore bits, Trapdoor-OWP, ...
 - Constructions: Using RSA, DDH, bilinear pairings, ...
- Authentication
 - Hash functions, MACs, Signatures, Ring sign. etc.
 - Security definitions: Collision resistance (various), existential forgery, ..
 - Constructions: Based on hash functions (also Random Oracles + Trapdoor OWP)
- Secure multi-party computation
 - Oblivious Transfer, ZK Proofs, Yao's garbled circuit
 - Private set intersection
 - (Didn't cover: More secure protocols, more efficient protocols for special tasks, Universal Composition)

A Quick Summary

- Encryption
 - SKE/PKE, Homomorphic Encryption, IBE, ABE
 - Security definitions: CPA/CCA
 - Abstractions: OWF/Hardcore bits, Trapdoor-OWP, ...
 - Constructions: Using RSA, DDH, bilinear pairings, ...
- Authentication
 - Hash functions, MACs, Signatures, Ring sign. etc.
 - Security definitions: Collision resistance (various), existential forgery, ..
 - Constructions: Based on hash functions (also Random Oracles + Trapdoor OWP)
- Secure multi-party computation
- E-Cash & Anonymous credentials
 - Oblivious Transfer, ZK Proofs, Yao's garbled circuit
 - Private set intersection
 - (Didn't cover: More secure protocols, more efficient protocols for special tasks, Universal Composition)

A Quick Summary

- Encryption
 - SKE/PKE, Homomorphic Encryption, IBE, ABE
 - Security definitions: CPA/CCA
 - Abstractions: OWF/Hardcore bits, Trapdoor-OWP, ...
 - Constructions: Using RSA, DDH, bilinear pairings, ...
- Authentication
 - Hash functions, MACs, Signatures, Ring sign. etc.
 - Security definitions: Collision resistance (various), existential forgery, ..
 - Constructions: Based on hash functions (also Random Oracles + Trapdoor OWP)
- Secure multi-party computation
- E-Cash & Anonymous credentials
 - Oblivious Transfer, ZK Proofs, Yao's garbled circuit
 - Private set intersection
 - (Didn't cover: More secure protocols, more efficient protocols for special tasks, Universal Composition)
- Voting

A Quick Summary

- Encryption
 - SKE/PKE, Homomorphic Encryption, IBE, ABE
 - Security definitions: CPA/CCA
 - Abstractions: OWF/Hardcore bits, Trapdoor-OWP, ...
 - Constructions: Using RSA, DDH, bilinear pairings, ...
- Authentication
 - Hash functions, MACs, Signatures, Ring sign. etc.
 - Security definitions: Collision resistance (various), existential forgery, ..
 - Constructions: Based on hash functions (also Random Oracles + Trapdoor OWP)
- Secure multi-party computation
- E-Cash & Anonymous credentials
 - Oblivious Transfer, ZK Proofs, Yao's garbled circuit
 - Private set intersection
 - (Didn't cover: More secure protocols, more efficient protocols for special tasks, Universal Composition)
- Voting
- PIR

A Quick Summary

- SKE/PKE, Homomorphic Encryption, IBE, ABE
 - Security definitions: CPA/CCA
 - Abstractions: OWF/Hardcore bits, Trapdoor-OWP, ...
 - Constructions: Using RSA, DDH, bilinear pairings, ...
- Encryption
 - Authentication
 - Hash functions, MACs, Signatures, Ring sign. etc.
 - Security definitions: Collision resistance (various), existential forgery, ..
 - Constructions: Based on hash functions (also Random Oracles + Trapdoor OWP)
 - Secure multi-party computation
 - E-Cash & Anonymous credentials
 - Oblivious Transfer, ZK Proofs, Yao's garbled circuit
 - Private set intersection
 - (Didn't cover: More secure protocols, more efficient protocols for special tasks, Universal Composition)
 - Voting
 - PIR
 - Formal methods, Generic groups/Random Oracle, Quantum crypto...

A Quick Summary

- Encryption

- SKE/PKE, Homomorphic Encryption, IBE, ABE
- Security definitions: CPA/CCA
- Abstractions: OWF/Hardcore bits, Trapdoor-OWP, ...
- Constructions: Using RSA, DDH, bilinear pairings, ...

- Authentication

- Secure multi-party computation

- Hash functions, MACs, Signatures, Ring sign. etc.
- Security definitions: Collision resistance (various), existential forgery, ..
- Constructions: Based on hash functions (also Random Oracles + Trapdoor OWP)

- E-Cash & Anonymous credentials

- Voting

- PIR

- Oblivious Transfer, ZK Proofs, Yao's garbled circuit
- Private set intersection
- (Didn't cover: More secure protocols, more efficient protocols for special tasks, Universal Composition)

- Formal methods, Generic groups/Random Oracle, Quantum crypto...

- Didn't cover: Leakage-resilience, Obfuscation, Steganography, Game-theoretic crypto, lattices, ...

A Quick Summary

standardized

- Encryption

- Authentication

- Secure multi-party computation

- E-Cash & Anonymous credentials

- Voting

- PIR

- Formal methods, Generic groups/Random Oracle, Quantum crypto...

- SKE/PKE, Homomorphic Encryption, IBE, ABE
- Security definitions: CPA/CCA
- Abstractions: OWF/Hardcore bits, Trapdoor-OWP, ...
- Constructions: Using RSA, DDH, bilinear pairings, ...

- Hash functions, MACs, Signatures, Ring sign. etc.
- Security definitions: Collision resistance (various), existential forgery, ..
- Constructions: Based on hash functions (also Random Oracles + Trapdoor OWP)

- Oblivious Transfer, ZK Proofs, Yao's garbled circuit
- Private set intersection
- (Didn't cover: More secure protocols, more efficient protocols for special tasks, Universal Composition)

- Didn't cover: Leakage-resilience, Obfuscation, Steganography, Game-theoretic crypto, lattices, ...

A Quick Summary

standardized

- Encryption

- Authentication

- Secure multi-party computation

- E-Cash & Anonymous credentials

- Voting

- PIR

- Formal methods, Generic groups/Random Oracle, Quantum crypto...

- SKE/PKE, Homomorphic Encryption, IBE, ABE
- Security definitions: CPA/CCA
- Abstractions: OWF/Hardcore bits, Trapdoor-OWP, ...
- Constructions: Using RSA, DDH, bilinear pairings, ...

- Hash functions, MACs, Signatures, Ring sign. etc.
- Security definitions: Collision resistance (various), existential forgery, ..
- Constructions: Based on hash functions (also Random Oracles + Trapdoor OWP)

- Oblivious Transfer, ZK Proofs, Yao's garbled circuit
- Private set intersection
- (Didn't cover: More secure protocols, more efficient protocols for special tasks, Universal Composition)

- Didn't cover: Leakage-resilience, Obfuscation, Steganography, Game-theoretic crypto, lattices, ...

A Quick Summary

standardized

- Encryption

- SKE/PKE, Homomorphic Encryption, IBE, ABE
- Security definitions: CPA/CCA
- Abstractions: OWF/Hardcore bits, Trapdoor-OWP, ...
- Constructions: Using RSA, DDH, bilinear pairings, ...

- Authentication

- Hash functions, MACs, Signatures, Ring sign. etc.
- Security definitions: Collision resistance (various), existential forgery, ..
- Constructions: Based on hash functions (also Random Oracles + Trapdoor OWP)

- Secure multi-party computation

- E-Cash & Anonymous credentials

- Oblivious Transfer, ZK Proofs, Yao's garbled circuit
- Private set intersection
- (Didn't cover: More secure protocols, more efficient protocols for special tasks, Universal Composition)

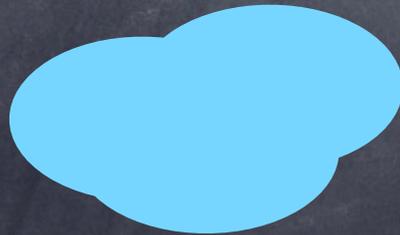
- Voting

- PIR

- Formal methods, Generic groups/Random Oracle, Quantum crypto...

- Didn't cover: Leakage-resilience, Obfuscation, Steganography, Game-theoretic crypto, lattices, ...

That's All Folks!



That's All Folks!

