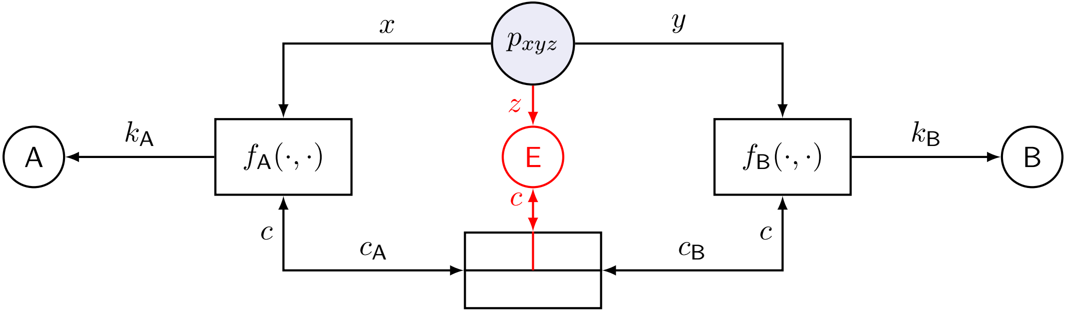
Lecture 18

Information theoretic key agreement

Nicola Laurenti November 27, 2020

Lecture 18— Contents

Cryptographic vs Information theoretic key agreement



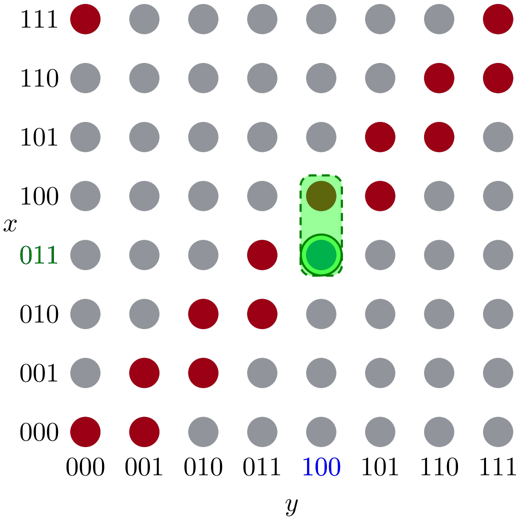
Cryptographic

- x, y, z are independent
- $x \to c_{\mathsf{A}}$ and $y \to c_{\mathsf{B}}$ one way
- computational secrecy

Information theoretic

- unconditional (strong) secrecy
- x and y must be dependent
- z may be dependent with x, y

The eavesdropper observes the public channel only



x and y correlated:

$$x \sim \mathcal{U}(\mathcal{X}),\ y \sim \mathcal{U}(\mathcal{Y}),$$

$$(x, y) \sim \mathcal{U}(T_{xy})\ ,\ T_{xy} \subset \mathcal{X} \times \mathcal{Y}$$

1. randomness sharing:

$$(x, y) = (011, 100)$$

observing $y = 100$, B knows
$x \in T_{x|y}(100) = \{011, 100\}$

2. information reconciliation:

$$c_\mathsf{A} = x \bmod 2 = 1$$

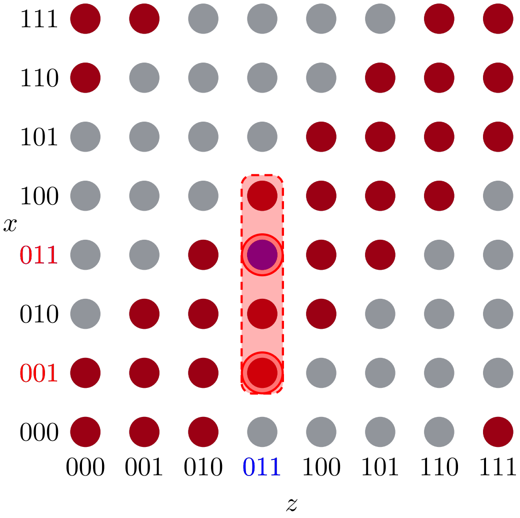
from c_A, B knows: $x = 011$

from c_A, E knows: $x = ??1$

3. privacy amplification:

$$k_\mathsf{A} = k_\mathsf{B} = \lfloor x/2 \rfloor = 01$$

With correlated eavesdropper observation z



x, y and z correlated:

$$T_{xyz} \subset \mathcal{X} \times \mathcal{Y} \times \mathcal{Z}$$

1. randomness sharing:
$$(x, y, z) = (011, 100, 011)$$
by observing $z = 011$,
E knows $x \in T_{x|z}(011)$
$T_{x|z}(011) = \{001, 010, 011, 100\}$
2. information reconciliation:
$$c_\mathsf{A} = x \bmod 2 = 1$$
from c_A, E knows: $x = 0?1$
3. privacy amplification:
$$k_\mathsf{A} = k_\mathsf{B} = \lfloor x/2 \rfloor \bmod 2 = 1$$

How many key bits can we obtain?

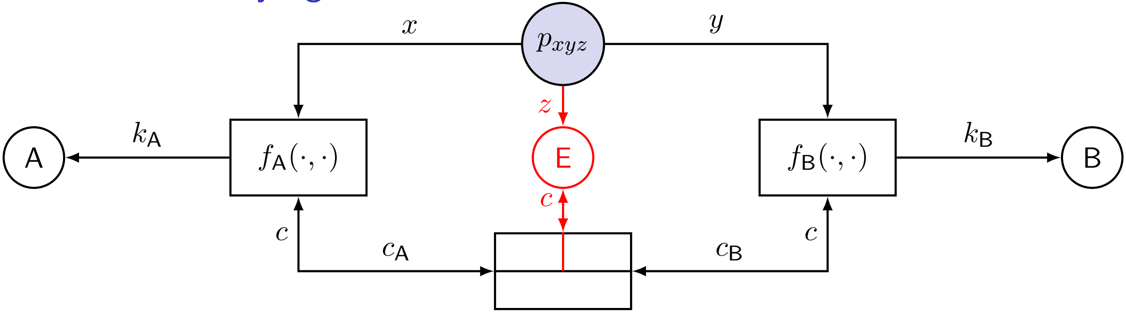
In the example, the final key length $\ell(k) = \log_2 |\mathcal{K}|$ is given by:

$\log_2 \lvert\mathcal{X}\rvert$	entropy of x
$-\log_2 \lvert T_{x\lvert y}\rvert$	redundancy needed for reconciliation
$-\log_2 \left(\lvert\mathcal{X}\rvert / \lvert T_{x\lvert z}\rvert\right)$	information leaked to E
$= \log_2 \lvert T_{x\lvert z}\rvert - \log_2 \lvert T_{x\lvert y}\rvert$	final key length
($\log_2 \lvert\mathcal{X}\rvert - \log_2 \lvert T_{x\lvert y}\rvert$	if E has no observation z)

The roles of A and B (x and y, resp.) can be reversed obtaining

$$\ell(k) = \log_2 \left|T_{y|z}\right| - \log_2 \left|T_{y|x}\right|$$

Unconditional key agreement: source model



Ideal counterpart

correctness $k_{\mathsf{A}} = k_{\mathsf{B}} = k$

uniformity $k \sim \mathcal{U}(\mathcal{K})$

secrecy k statistically independent of (z, c)

Unconditional distinguishability

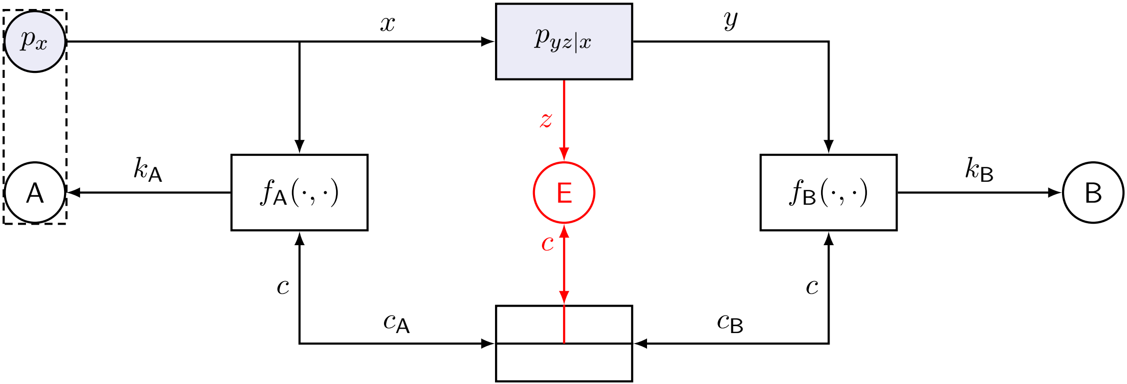
from ideal can be measured in terms of

correctness $d_{\mathsf{V}}(p_{k_{\mathsf{A}}k_{\mathsf{B}}}, p_{k^\star_{\mathsf{A}}k^\star_{\mathsf{B}}}) = \mathrm{P}\left[k_{\mathsf{A}} \neq k_{\mathsf{B}}\right]$

uniformity $\mathrm{D}\left(p_k \| p_{k^\star}\right) = \log_2 |\mathcal{K}| - H(k_{\mathsf{A}})$

secrecy $\mathrm{D}\left(p_{kzc} \| p_{k^\star z^\star c^\star}\right) = I(k_{\mathsf{A}}, k_{\mathsf{B}}; z, c)$

Unconditional key agreement: channel model



A distributed source of correlated random variables p_{xy} can be implemented as the cascade of a source p_x and a (possibly noisy) channel $p_{y|x}$

The correlated eavesdropper observations z can be accounted for in a wiretap channel model $p_{yz|x}$

Memoryless sources

Consider n-symbol sequences, $\mathbf{x} = [x_1, \dots, x_n]$ (and similarly for $\mathbf{y}$ and $\mathbf{z}$) and memoryless sources, $p_{\mathbf{xyz}}(\mathbf{a}, \mathbf{b}, \mathbf{c}) = \prod_{i=1}^{n} p_{xyz}(a_i, b_i, c_i)$

Definition

$R_\mathsf{k} \geq 0$ is an achievable secret key rate for the source p_{xyz} if, $\forall n$, there exist: key spaces $\{\mathcal{K}_n\}$ and schemes $f_{\mathsf{A},n}(\cdot, \cdot)$ and $f_{\mathsf{B},n}(\cdot, \cdot)$ such that

cardinality: $|\mathcal{K}_n| \geq 2^{nR_\mathsf{k}}$

correctness: $\lim_{n\to\infty} \mathrm{P}\left[k_\mathsf{A} \neq k_\mathsf{B}\right] = 0$

secrecy: $\lim_{n\to\infty} I(k_\mathsf{A}, k_\mathsf{B}; \mathbf{z}, c_\mathsf{A}, c_\mathsf{B}) = 0$

uniformity: $\lim_{n\to\infty} nR_\mathsf{k} - H(k_\mathsf{A}) = 0$

Definition

The secret key capacity of the memoryless source p_{xyz} is

$$C_\mathsf{k} = \sup\left\{R_\mathsf{k} \;:\; R_\mathsf{k} \text{ is an achievable secret key rate}\right\}$$

Memoryless sources

Theorem

If $R_\mathsf{k} < I(x;y) - I(x;z) = H(x|z) - H(x|y)$ *or* $R_\mathsf{k} < I(x;y) - I(y;z) = H(y|z) - H(y|x)$ *, then* R_k *is an achievable secret key rate for the source* p_{xyz}*.*

Intuition

Suppose that $R_\mathsf{k} < H(x|z) - H(x|y)$. By making use of typical sequences, we have as $n \to \infty$

$$\left|T_{x|y}\right| \to 2^{nH(x|y)} \quad , \quad \left|T_{x|z}\right| \to 2^{nH(x|z)}$$

so that, by the hypothesis on R_k,

$$\begin{aligned} nR_\mathsf{k} &\leq n[H(x|z) - H(x|y)] \\ \ell(k) &\leq \log_2 \left|T_{x|z}\right| - \log_2 \left|T_{x|y}\right| \end{aligned}$$

and we can leverage the uniform source result for the existence of f_A, f_B.
The proof for $R_\mathsf{k} < H(y|z) - H(y|x)$ is analogous.

Secret key capacity

The above result is a lower bound for the secret key capacity

$$C_{\mathsf{k}} = \max R_{\mathsf{k}} \geq \max \{H(x|z) - H(x|y), H(y|z) - H(y|x)\}$$

Upper bounds can be found by either:

- assuming E has no correlated observations, that is $z = \emptyset$

$$C_{\mathsf{k}} \leq H(x) - H(x|y) = I(x;y)$$

- assuming that B also knows z, that is $y' = (y, z)$. Then:

$$C_{\mathsf{k}} \leq H(x|z) - H(x|y') = H(x|z) - H(x|y,z) = I(x;y|z)$$

General bounds are therefore

$$I(x;y) - \min \{I(x;z), I(y;z)\} \leq C_{\mathsf{k}} \leq \min \{I(x;y), I(x;y|z)\}$$

Memoryless channels

Consider n-symbol sequences, $\mathbf{x} = [x_1, \ldots, x_n]$ (and similarly for $\mathbf{y}$ and $\mathbf{z}$) and memoryless channels, $p_{\mathbf{yz}|\mathbf{x}}(\mathbf{b}, \mathbf{c}|\mathbf{a}) = \prod_{i=1}^{n} p_{yz|x}(b_i, c_i|a_i)$

Definition

$R_\mathsf{k} \geq 0$ is an achievable secret key rate for the memoryless channel $p_{yz|x}$ if there exists a memoryless source p_x such that R_k is an achievable secret key rate for the resulting joint memoryless source p_{xyz}

$$p_{xyz}(a, b, c) = p_{yz|x}(b, c|a) p_x(a)$$

Definition

The secret key capacity of the memoryless channel $p_{yz|x}$ is

$$C_\mathsf{k} = \sup \{ R_\mathsf{k} \; : \; R_\mathsf{k} \text{ is an achievable secret key rate} \}$$

Memoryless channels

Theorem

If there exists some input PMD p_x *such that* $R_\mathsf{k} < I(x;y) - I(x;z)$ *or* $R_\mathsf{k} < I(x;y) - I(y;z)$ *, then* R_k *is an achievable secret key rate for channel* $p_{yz|x}$.

Proof.

Follows from the definition and the corresponding theorem for joint memoryless sources □

Corollary

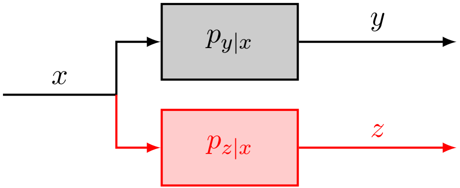
For a memoryless channel, the secret key capacity satisfies the bounds

$$\max_x \left[I(x;y) - \min\left\{I(x;z), I(y;z)\right\}\right] \leq C_\mathsf{k} \leq \max_x \left[\min\left\{I(x;y), I(x;y|z)\right\}\right]$$

Markovian WTCs

Definition

We call a WTC $p_{yz|x}$ Markovian if the two outputs y, z are conditionally independent given the input x, that is $p_{yz|x}(b, c|a) = p_{y|x}(b|a)p_{z|x}(c|a)$



In a Markovian WTC,

$$H(y|x, z) = H(y|x) \quad , \quad H(z|x, y) = H(z|x)$$

Markovian WTCs

Proposition

In a Markovian WTC, $I(y;z) \le I(x;z)$

Proof.

$$\begin{aligned} I(y;z) &= H(z) - H(z|y) \\ &\le H(z) - H(z|x,y) \\ &= H(z) - H(z|x) = I(x;z) \end{aligned}$$

□

Proposition

In a Markovian WTC,
$I(x;y|z) = I(x;y) - I(y;z) \le I(x;y)$

Proof.

$$\begin{aligned} I(x;y|z) &= H(y|z) - H(y|x,z) \\ &= H(y|z) - H(y|x) \\ &= H(y) - I(y;z) - H(y) + I(x;y) \\ &= I(x;y) - I(y;z) \le I(x;y) \end{aligned}$$

□

Markovian WTCs

Theorem

In a Markovian WTC, $C_\mathsf{k} = \max_x I(x;y|z) = \max_x [I(x;y) - I(y;z)] > C_\mathsf{s}$

Proof.

By the first Proposition, the tighter lower bound is

$$C_\mathsf{k} \geq \max_x [I(x;y) - I(y;z)]$$

By the second Proposition, the tighter upper bound is

$$C_\mathsf{k} \leq \max_x I(x;y|z)$$

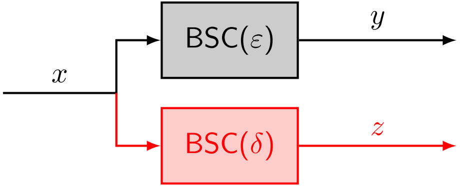
By the second Proposition, the two bounds coincide as

$$\max_x [I(x;y) - I(y;z)] = C_\mathsf{k} = \max_x I(x;y|z)$$

□

Secret key capacity for the wiretap BSC

Let the channels from A to B and from A to E be memorlyess binary symmetric with error rates ε and δ, respectively



For all values of ε, δ the secret key capacity is attained with $x \sim \mathcal{U}(\{0,1\})$ and reverse reconciliation B $\rightarrow$ A: it yields

$$C_\mathsf{k} = I(x;y) - I(y;z) = h_2(\varepsilon) - h_2(\gamma)$$

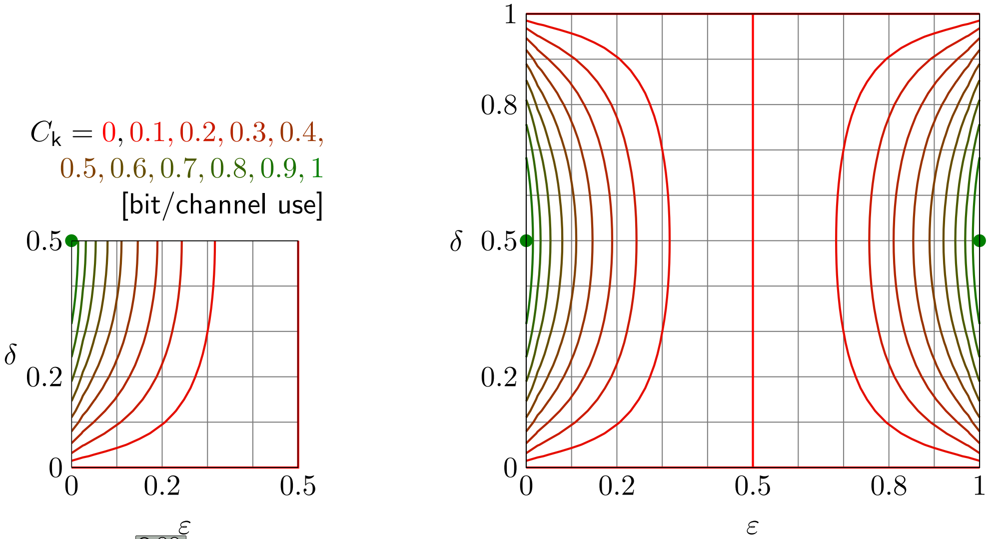
where $\gamma = \varepsilon + \delta - 2\varepsilon\delta$ and $h_2(\varepsilon) = \varepsilon \log_{1/2} \varepsilon + (1-\varepsilon) \log_{1/2}(1-\varepsilon)$.

Observe that $\left|\varepsilon - \frac{1}{2}\right| > \left|\gamma - \frac{1}{2}\right|$ for all $\delta \in (0,1)$, so that $C_k > 0$ unless the channel from A to E is perfect.

Secret key capacity for the wiretap BSC

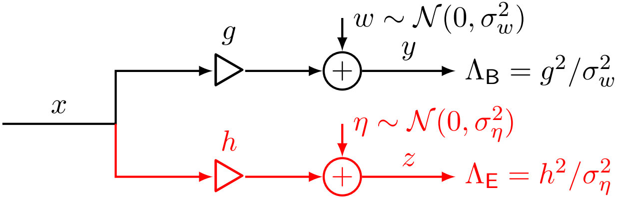
$C_{\mathsf{k}} = 0, 0.1, 0.2, 0.3, 0.4, 0.5, 0.6, 0.7, 0.8, 0.9, 1$

[bit/channel use]



Secret key capacity for the wiretap AWGN channel

Let the channels A $\rightarrow$ B and A $\rightarrow$ E be additive white Gaussian noise



For all values of $\Lambda_\mathsf{B}, \Lambda_\mathsf{E}$ the secret key capacity is achieved with $x \sim \mathcal{N}(0, P)$ and reverse reconciliation. It is given by

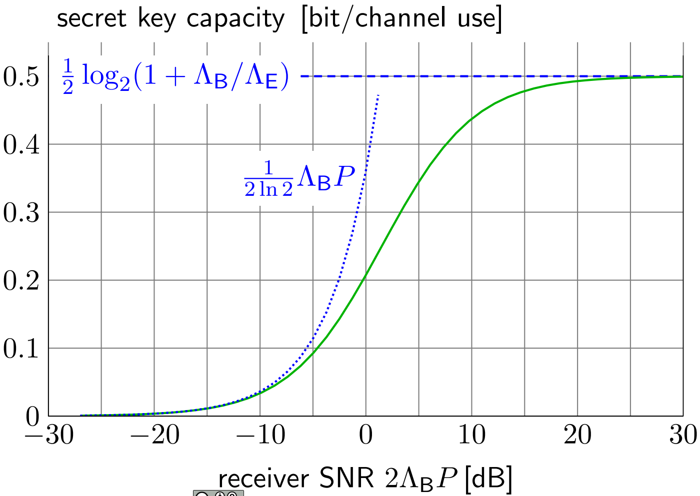
$$C_\mathsf{k} = I(x; y) - I(y; z) = \frac{1}{2} \log_2 \frac{1 - \rho_{yz}^2}{1 - \rho_{xy}^2} = \frac{1}{2} \log_2 \frac{1 + (\Lambda_\mathsf{B} + \Lambda_\mathsf{E})P}{1 + \Lambda_\mathsf{E} P}$$

Observe that $C_\mathsf{k} > 0$ for all $\Lambda_\mathsf{E} < \infty$, that is unless the channel from A to E is noiseless.

$$\lim_{P \to \infty} C_\mathsf{k} = \frac{1}{2} \log_2 \left(1 + \frac{\Lambda_\mathsf{B}}{\Lambda_\mathsf{E}} \right) \quad , \quad C_\mathsf{k} \asymp \frac{\Lambda_\mathsf{B} P}{2 \ln 2} \quad \text{as } P \to 0$$

Secret key capacity for wiretap AWGN

For equal SNR $\Lambda_B = \Lambda_E$



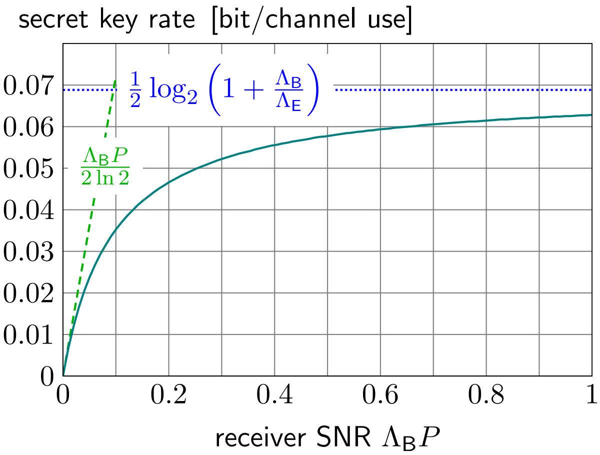
Gaussian input

Contrary to the unconstrained capacity C_{AB} and akin to the secrecy capacity C_s,
C_k saturates as $P \to \infty$.
In the low SNR regime, as $P \to 0$, C_k is independent of Λ_E

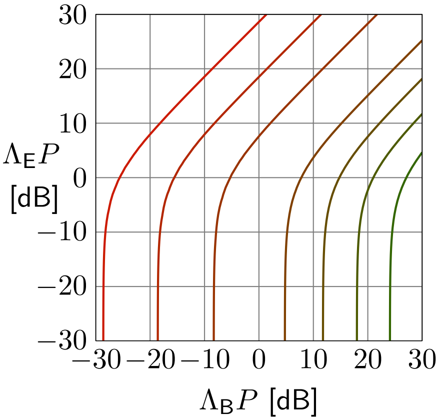
Secret key capacity for wiretap AWGN

Contrary to the secrecy capacity, $C_k > 0$ for any Λ_B, Λ_E.

SNR ratio $\Lambda_B/\Lambda_E = -10\,\text{dB}$



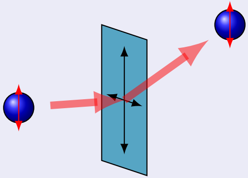
$C_k = 0.001, 0.01, 0.1, 1, 2, 3, 4,$ [bit/channel use]

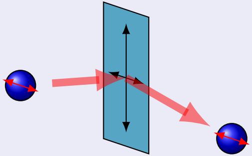


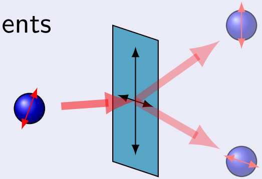
Quantum laws for cryptography

Uncertainty principle

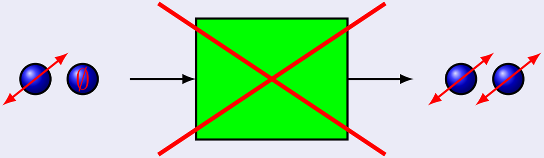
A quantum state can only be observed through projective measurements



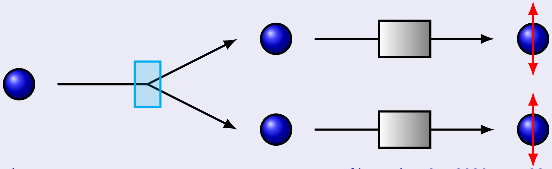




No cloning theorem [Wootters-Zurek, '82]



Entanglement



The *qubit*

- basic unit measure for quantum information
- quantum state in a 2-D space

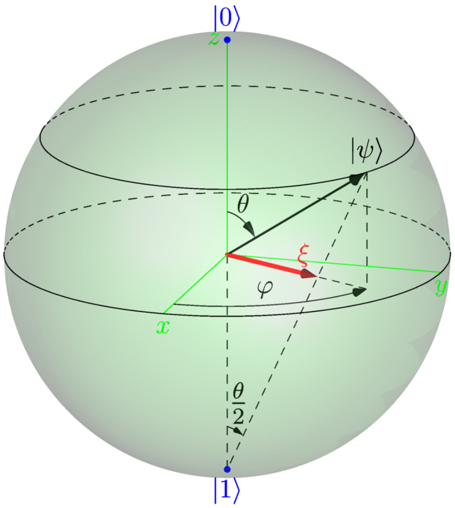
$$|\gamma\rangle = \alpha|0\rangle + \beta|1\rangle$$

  in cui $|\alpha|^2 + |\beta|^2 = 1$

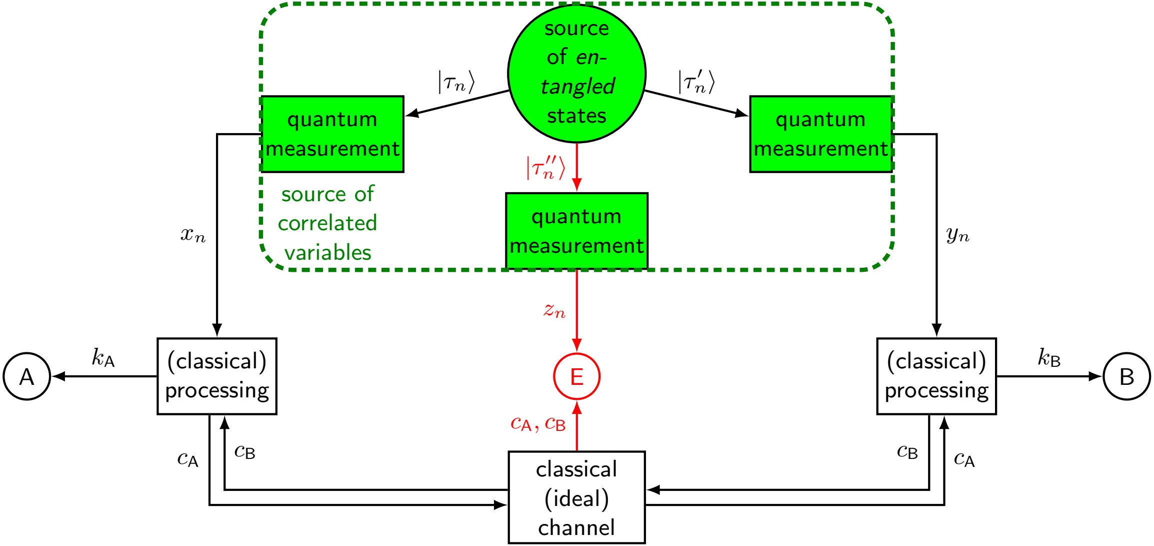
- by measuring $|\gamma\rangle$ on the $(\langle 0|, \langle 1|)$ basis, we have $\mathrm{P}\left[|\gamma\rangle \rightarrow |0\rangle\right] = |\alpha|^2$ e $\mathrm{P}\left[|\gamma\rangle \rightarrow |1\rangle\right] = |\beta|^2$

Example of physical qubits

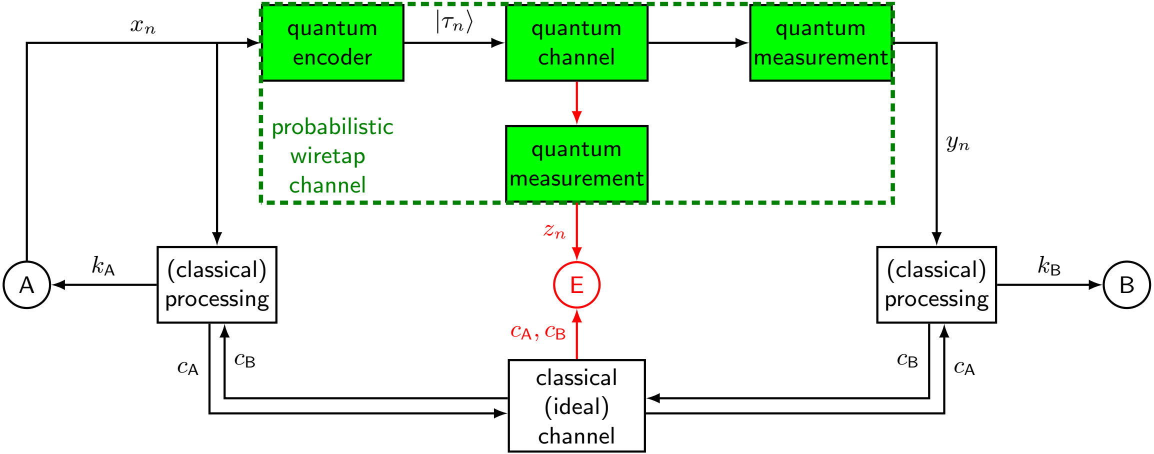
- Polarization of a photon
- Arrival time for a photon wrt a given threshold
- Spin of an electron
- ...



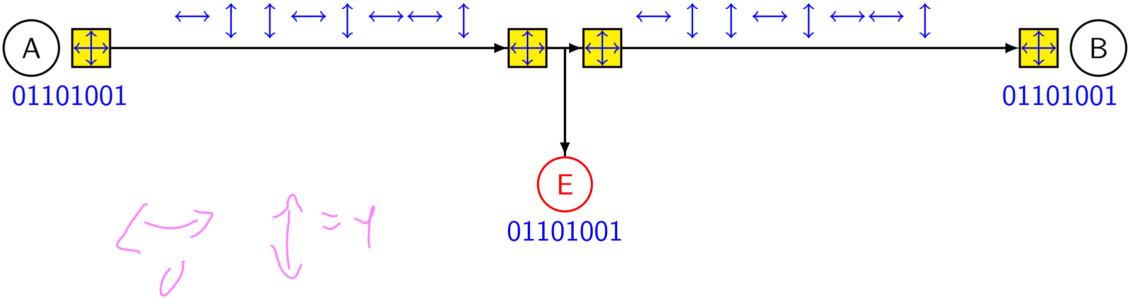
Source model for QKA



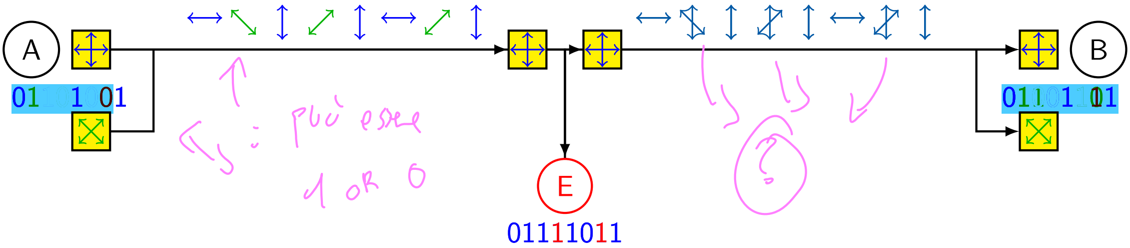
Channel model for QKA



The “efficient BB84” protocol



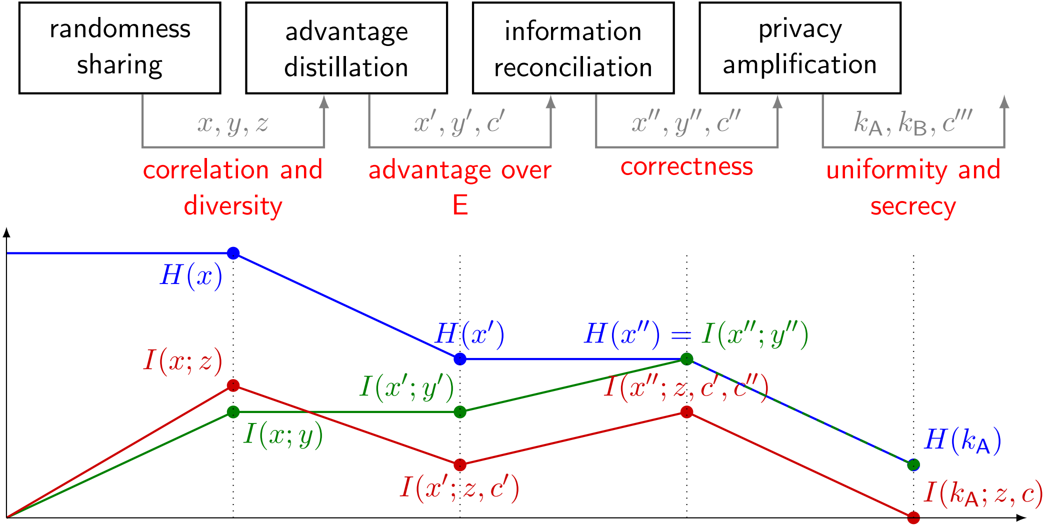
The "efficient BB84" protocol



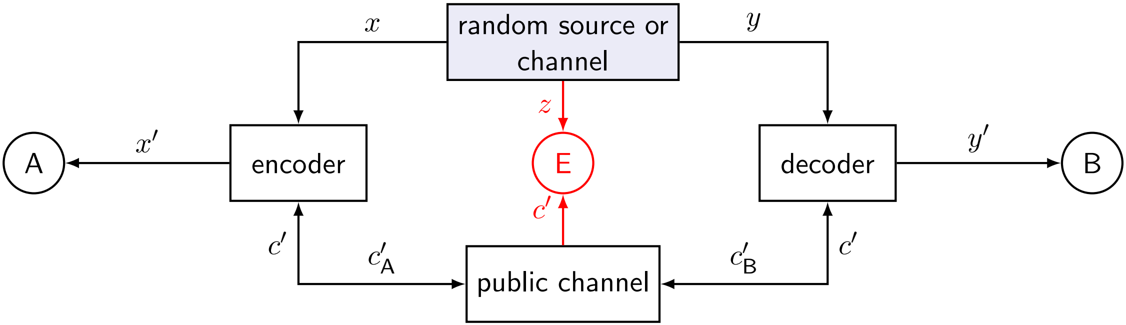
Security vs performance

# of transmitted qubits	n_{tot}
majority rate $\leftrightarrow\!\!\!\!\updownarrow$	p
missed detection probability	$P_{\text{md}} = \left(\frac{1}{2} + p - \frac{1}{2}p^2\right)^{n_{\text{tot}}}$
average key length	$\mathrm{E}\left[\ell\right] = n_{\text{tot}} p^2$

Divide et impera



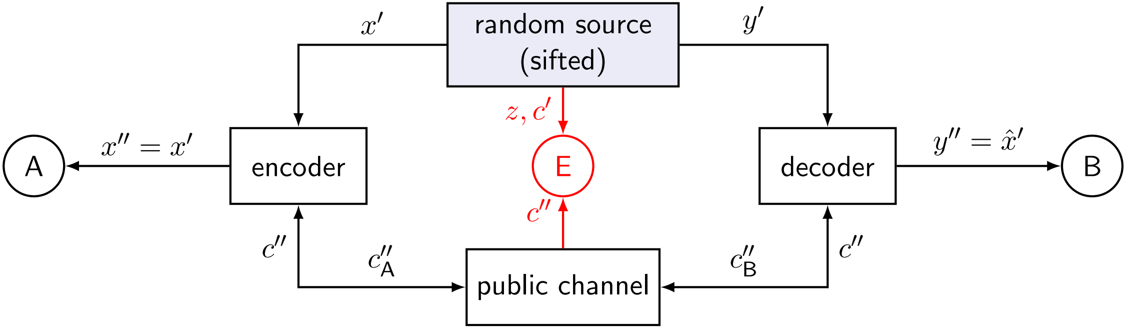
Advantage distillation



Aim

To choose subsequences x' from x, and y' from y by agreeing on their indices $c' = (c'_A, c'_B)$ publicly, so that $I(x'; y') \simeq I(x; y)$, and $I(x'; z) \ll I(x; z)$, with the minimum leakage of information $I(x; c')$ to E.

Information reconciliation



Aim

To allow B to reliably reconstruct $\hat{x}' = x'$, by transmitting $c'' = (c''_A, c''_B)$ publicly, with the minimum leakage of information $I(x'; c'')$ to E.

Information reconciliation

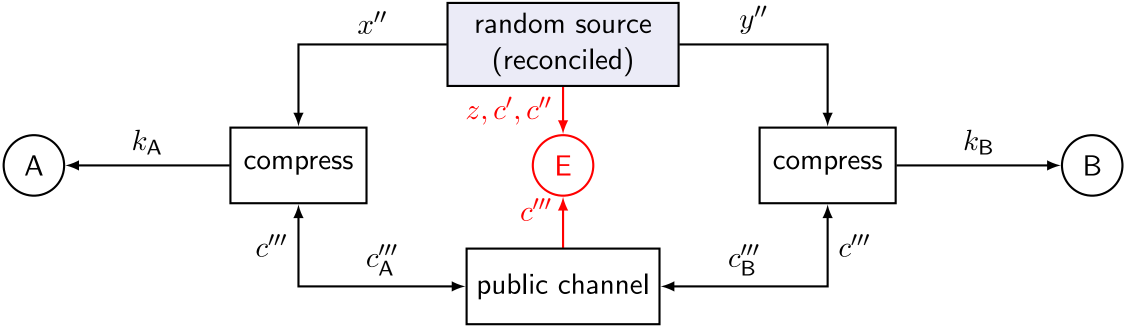
Coding techniques for reconciliation fall into one of the categories:

cascade iteratively (and interactively) split the keys to locate single errors and correct them, c'' is the sequence of parity bits [Brassard-Salvail, ‘93]

systematic pick a systematic generating matrix $\mathbf{G} = \begin{bmatrix} \mathbf{I}_n \\ \mathbf{A} \end{bmatrix}$ for a $(n+r, n)$ linear code $\mathcal{C}$
Alice transmits $\mathbf{c}'' = \mathbf{A}\mathbf{x}'$.
Bob chooses $\hat{\mathbf{x}}' = \arg\min_{\mathbf{a}\in\mathcal{C}} d(\mathbf{a}, \mathbf{y})$
Examples: LDPC [Mondin *et al.*, ‘10], BCH [Traisilanun *et al.*, ‘07]

hashing given a parity check matrix $\mathbf{H}$ for a $(n, n-r)$ linear code
Alice transmits $\mathbf{c}'' = \mathbf{H}\mathbf{x}'$, that is the syndrome of $\mathbf{x}'$.
Bob chooses $\hat{\mathbf{x}}' = \arg\min_{\mathbf{a}:\mathbf{H}\mathbf{a}=\mathbf{c}''} d(\mathbf{a}, \mathbf{y})$
Examples: Winnow [Buttler *et al.*, ‘03], LDPC [Elkouss *et al.*, ‘09]

Privacy amplification



Aim

To allow A and B to remove any information E might have, and any non-uniformity from $\hat{k} = k$ by publicly agreeing on a compressing function, and with the minimum amount of compression.

Choosing a privacy amplification matrix

- Must be chosen randomly, after transmission
- Should be compactly representable

Assume we know that Eve has observed some t-bit linear function of the reconciled key

$$(\mathbf{z}, \mathbf{c}) = \mathbf{M}\mathbf{x}'' \quad , \qquad \text{with } \mathbf{M} \in \{0,1\}^{t \times n}$$

(include $\mathbf{c}$ observed during reconciliation)

Theorem ([Bennett *et al.*, '95])

If the compressing function $\mathbf{A}$ is chosen uniformly from a class of universal hashing $s \times n$ matrices, then on average (over $\mathbf{M}$ and $\mathbf{A}$)

$$I(\mathbf{k}; \mathbf{z}, \mathbf{c}, \mathbf{A}) \leq \frac{1}{2^b \ln 2}$$

where $b = n - t - s$ is a margin obtained by shortening the final key

Choosing a privacy amplification matrix

Once we choose a hashing matrix $\mathbf{A}$, we would like to obtain

1. $H(\mathbf{k}) = s$ (perfect uniformity)
2. $I(\mathbf{k}; \mathbf{z}, c) = 0$ (perfect secrecy)

Lemma 1

If $\mathrm{rank}(\mathbf{A}) = s$ and $\mathbf{x}''$ is uniform over $\{0,1\}^n$, then $\mathbf{k}$ is uniform over $\{0,1\}^s$

Example: binary Toeplitz matrices

- $\mathbf{A}$ is uniquely specified by $n + s - 1$ bits $\mathbf{a} = [a_{-r+1}, \ldots, a_{n-1}]$
- If $\mathbf{a}$ is uniform in $\{0,1\}^{n+s-1}$, $\mathrm{P}\left[\text{rank}(\mathbf{A}) < s\right] = 1/2^{n-s+1}$

Lemma 2

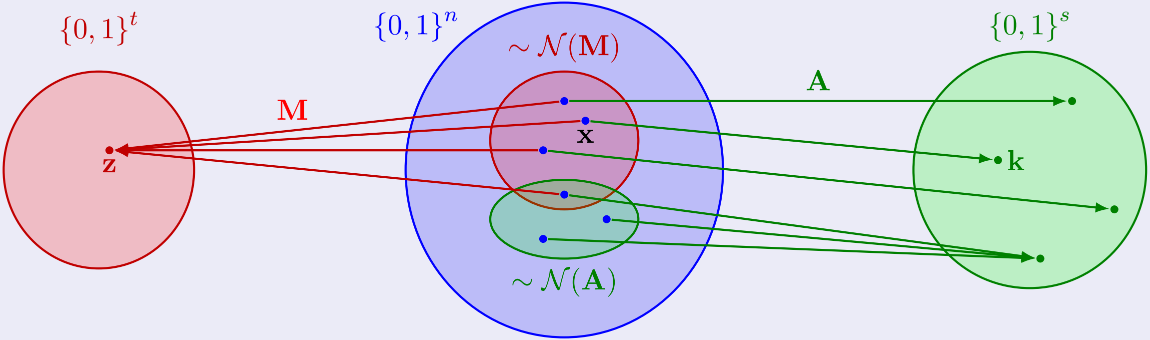
If $\dim \mathcal{N}(\mathbf{M}) - \dim\left(\mathcal{N}(\mathbf{M}) \cap \mathcal{N}(\mathbf{A})\right) = \mathrm{rank}(\mathbf{A})$ and $\mathbf{x}''$ is uniform over $\{0,1\}^n$, then $I(\mathbf{k}; \mathbf{z}, c) = 0$

Choosing a privacy amplification matrix

Theorem

If $\dim \mathcal{N}(\mathbf{M}) - \dim(\mathcal{N}(\mathbf{M}) \cap \mathcal{N}(\mathbf{A})) = s$ *and* $\mathbf{x}''$ *is uniform over* $\{0,1\}^n$*, then* $\mathbf{k}$ *is uniform and perfectly secret.*

Illustration



Unconditionally secure authentication

keyed hash function applied to the concatenation of all messages transmitted by each terminal in a protocol round, $t = T(k; u)$

- $\{T(k; \cdot)\}$ form a (ε-almost) strongly universal$_2$ class [Wegman-Carter, '81][Stinson, '94]
- requires a long secure key k, renewed every round

keyed hash function + tag encryption with one time pad $t = T(k_0; u) \oplus k_n$

- $\{T(k; \cdot)\}$ (ε-almost) strongly universal$_2$ class
- shorter key $k : n$, renewed at every round; longer key k_0 need not be renewed [Stinson, '96]

Authentication requires hundreds of secure bits per round, that can be taken from the previously generated keys, thus lowering the net key rate.

Crypto vs Info theoretic key agreement

Cryptographic key agreement	Info theoretic key agreement
independent generation of initial randomness	requires correlated initial randomness
perfect correctness and uniformity	asymptotic correctness and uniformity
provides computational security	provides unconditional security
no hypotheses on adversary's info	requires knowledge of eavsdropper channel
requires authenticated public channel	requires authenticated public channel

Summary

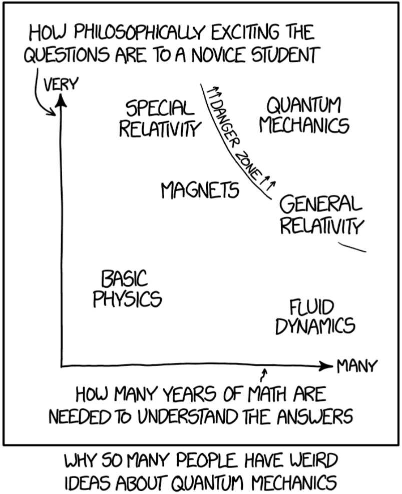
In this lecture we have:

- presented a general model for key agreement in the source- and channel-based variants
- introduced the notion of key reconciliation and privacy amplification
- defined the information theoretic measures of secret key rate and secret key capacity
- shown and discussed secret key capacity values for the BSC and the AWGN channels
- presented practical methods to achieve key agreement in 3 steps, including quantum

Assignment

- class notes

End of lecture



Quantum, reproduced from xkcd URL: xkcd.com/1861