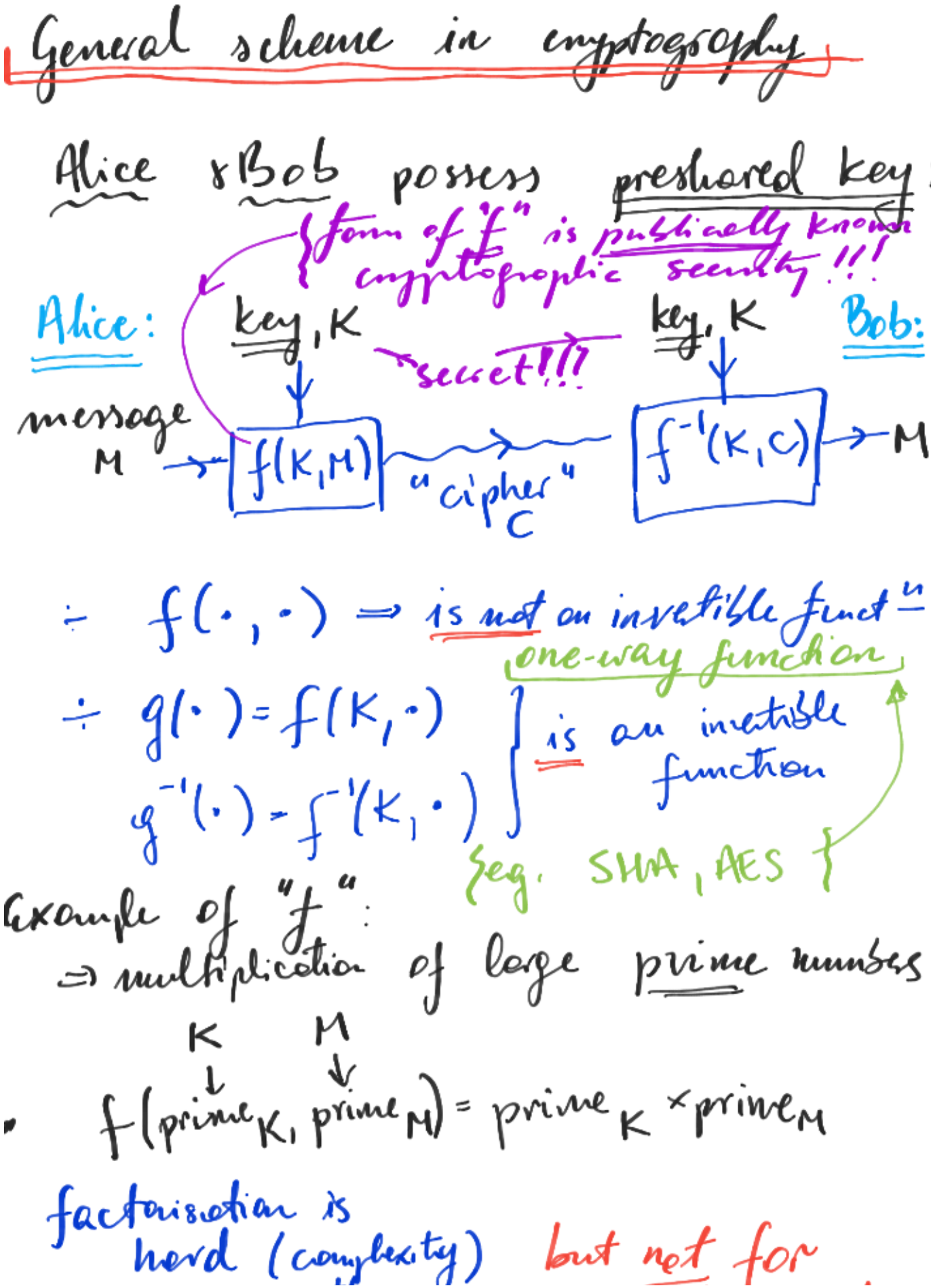
12. Quantum cryptography

Consider registering 1100-AQI Advanced QI: Entanglement and non-locality



Theory $\in$ BQP

quantum computers (Shor's algorithm)

- $g(\cdot) = f(\text{prime}_K, \cdot)$

easy to invert once we know the key

$\Rightarrow$ just division by a prime...

$g^{-1}(c) = c / \text{prime}_K = \text{prime}_M \Rightarrow M$

NB. • in reality other one-way functions (e.g. AES-256 (256 bits key))

$\Rightarrow$ "substitution-permutation networks"

• there exists one-way (hashing) functions whose complexity is also beyond quantum computers

"post-quantum cryptography"

• real problem

factoring $\Leftrightarrow$ discrete logarithm in RSA

Riemann hypothesis

(Rivest-Shamir-Adleman)

RSA: Public-key cryptosystem

Alice $[K_{priv}, (K_{public})]$ → announced and used by Bob to encode the message

discrete logarithm: $b^P = a \pmod n$ ⇒ hard: $n = \text{prime}_1 \times$

$\Rightarrow$ find integer P over

a group "prime"

RSA : Code at home !

Alice

① $n = p_1 \cdot p_2$ (large primes)

② $\lambda(n) = LCM(p_1 - 1, p_2 - 1)$

③ choose "e" coprime to $\lambda(n)$
$e < \lambda(n)$ $GCD(e, \lambda(n)) = 1$

④ compute d s.t. $e \cdot d = 1 \pmod{\lambda(n)}$

$[K_{priv} = d \;,\; K_{pub} = (n, e)]$

Bob

$C = M^e \pmod n$

$C =$ "encrypted message"

$M = C^d \pmod n$

OK, but only a problem because we want to encrypt long messages with short keys ! { AES-256 / RSA ≥ 1024

⇒ If we could have secret key K and message M to be of same length!

⇒ "one-time pad" full security (proved already by Shannon 1949)

Vernam cipher ("XOR") : (Gilbert Vernam, 1919 patent)

$K \oplus M = C \Rightarrow C \oplus K = M$

$K \oplus M = C \rightarrow M = C \oplus K$

important! a) need very good RNG to generate "random" keys of length m.

[QRNGs: ÷ Id Quantique ÷ QuSIDE

b) need a way to securely distribute keys...

Quantum Key Distribution

Aim: Alice & Bob want to establish secret (& random) string of bits ⇒ KEY

Bennet & Brassard 1984 BB84

Alice & Bob repeat over many rounds:

① Alice randomly chooses basis $\{|0\rangle, |1\rangle\}$ or $\{|+\rangle, |-\rangle\}$ in which randomly encodes: "0", "1"

{NB. impl: photons in $\{|\leftrightarrow\rangle, |\updownarrow\rangle\}$ or $\{|\nearrow\rangle, |\nwarrow\rangle\}$ send via fibre to Bob.

② Bob randomly chooses basis to measure $\{|0\rangle, |1\rangle\}$ or $\{|+\rangle, |-\rangle\}$

③ two-way communication via authenticated public classical channel

⇒ B announces which basis he used in each round (without the outcomes!)

. A afterwards announces which rounds to keep.

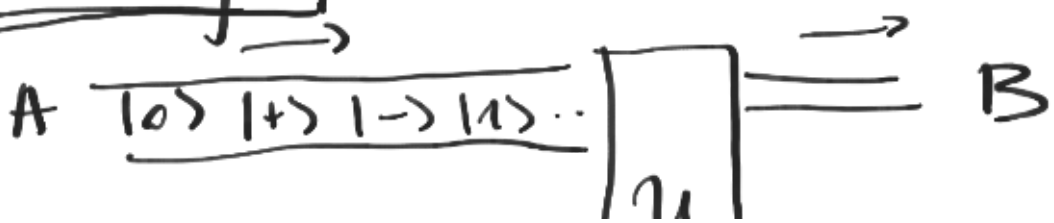
rounds	1	2	3	4	5	6	...
1) Alice	0	—	+	1	—	0	...
2) Bob	0/1	0/1	+/×	0/1	0/1	+/×	...
3) compatible?	✓	×	✓	✓	×	×	...

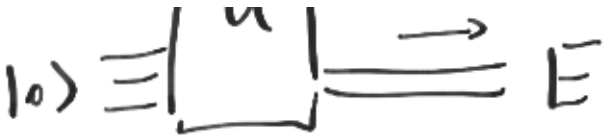
④ Sifting stage:
Alice & Bob keep only compatible rounds.
(≈ half of them will survive)

⑤ Error (eavesdropping) estimation
Alice & Bob sacrifice some {log(# total rounds)} rounds to verify the rate of errors (%)
(two-way communication)
⇒ establish QBER
(quantum bit error rate)

⇒ assume worst-case scenario:
all errors (aBER) are a result of Eavesdropping.

Security:



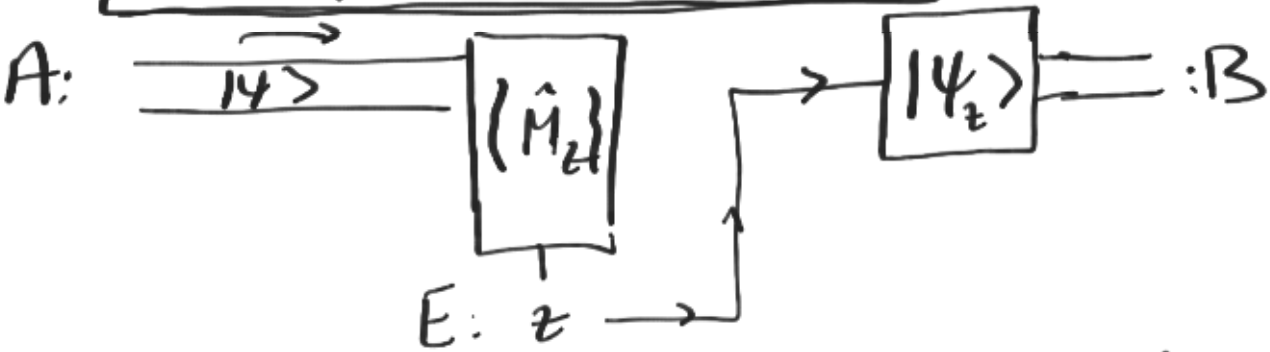


Eve: • waits until Alice & Bob announce which basis are compatible
• wants to be as strongly as possible correlated with bit-strings of Alice & Bob

We must consider the most general attack of Eve that quantum mechanics allows!

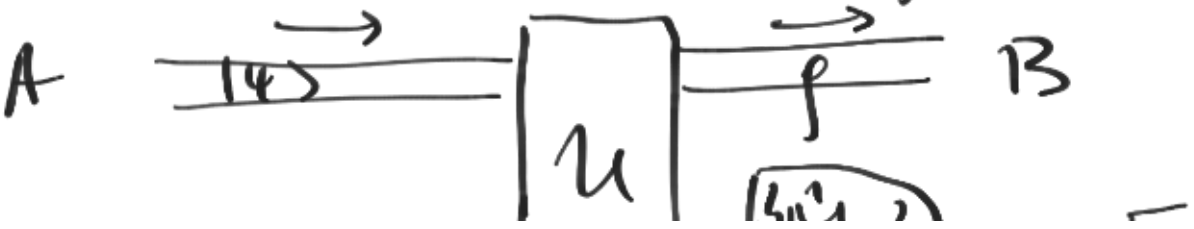
Let us consider:

(a) Intercept and resend



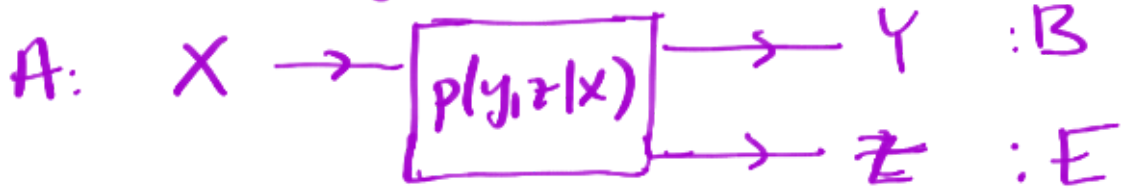
Eve measures the state sent by Alice and for an outcome z prepares $|4_z\rangle$ to be sent to Bob.
{some strategy for every round}
⇒ IID condition

(b) Individual attacks (more powerful)



{again: some strategy for every round}
⇒ IID condition

⇒ after sifting stage:



Apply Csiszar-Körner Theorem!

bits									
Alice	X	0	1	0	1	0	0	1	..
Bob	Y	0	1	1	1	0	1	1	.. ⇒ QBER
Eve	Z	1	1	1	0	1	0	1	... 25%

⑥ Alice & Bob perform
Error Correction (EC)
and Privacy Amplification (PA)
to obtain secret key:

$$C_s = I(A:B) - I(A:E)$$

(asymptotic key-rate)

(*) as long as $I(A:B) > I(A:E)$

① $I(A:B) = 1 - h(QBER)$
{bit-flip channel}

② $I(A:E) = ?$

(c) $I(A:E)$ - ?

Need to consider the optimal (a) I&R or (b) indiv. attack to obtain it as a function of QBER

(a) Simple I&R

Eve mimics Bob:
- measures in $\{|0\rangle, |1\rangle\}$ or $\{|+\rangle, |-\rangle\}$ with $p = \frac{1}{2}$
- resends the measured state to Bob

$\Rightarrow$ QBER $= \frac{1}{2} \times \frac{1}{2} = \frac{1}{4} = 25\%$

$\frac{1}{2}$: prob. that Eve measures in wrong basis

$\frac{1}{2}$: prob. that given Eve measured in the wrong basis Bob gets it wrong

(1) $I(A:B) = 1 - h(\text{QBER}) \approx 0.189$

(2) bit error rate for Eve:

$\Rightarrow e_E = \left(\frac{1}{2}\right) \cdot \left(\frac{1}{2}\right) = \frac{1}{4}$

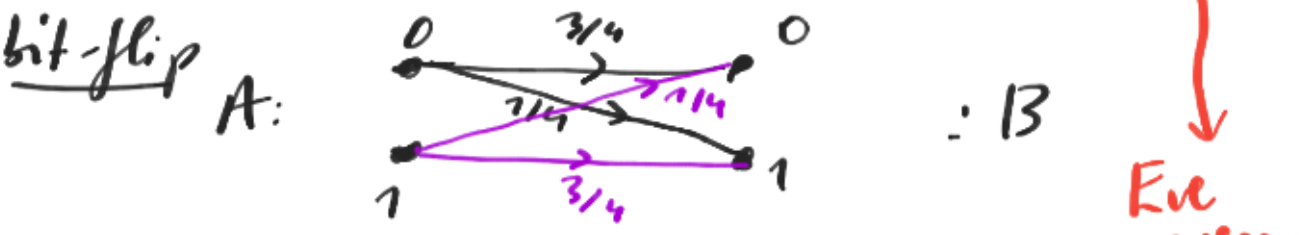
$\frac{1}{2}$: wrongly chosen basis by Eve

$\frac{1}{2}$: prob. that given Eve chose the wrong basis, she gets it wrong

$\Rightarrow I(A:E) = I(A:B) \approx 0.189$ WRONG!

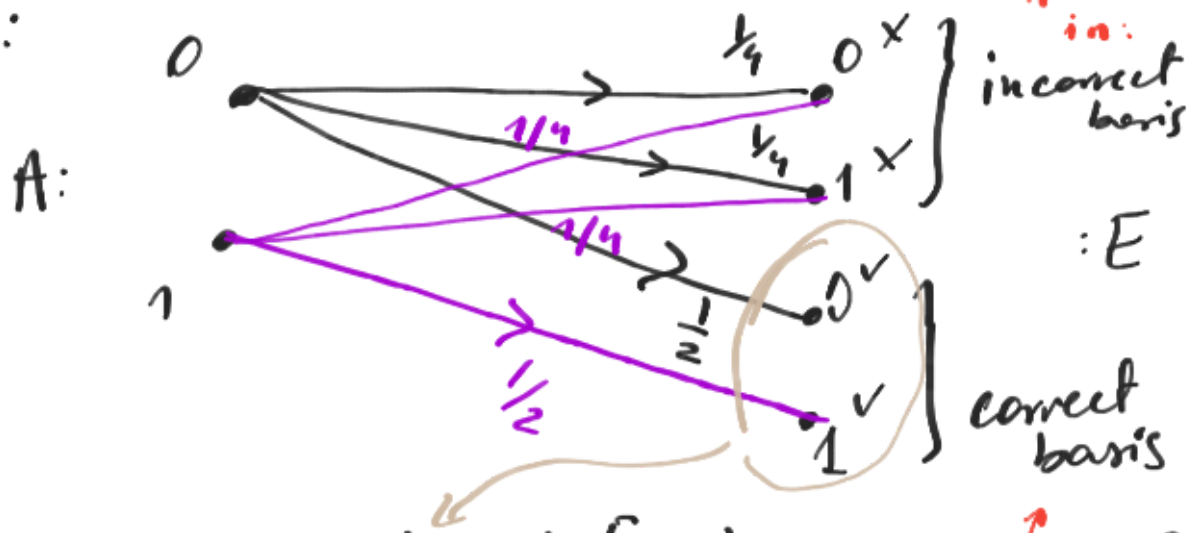
Eve knows (public) which rounds are acepted !!

bit-flip



Eve measures in:

but:



$$I(A:E) = \frac{1}{2}$$ { Eve knows whether she measured in correct basis }

⇒ even worse $I(A:E) > I(A:B)$

Conclusion:

QBER ↑ $QBER_{th} = 25\%$ ⇒ they must abort

{ ⇒ note that $I(B:E) = I(A:E) = \frac{1}{2}$ }

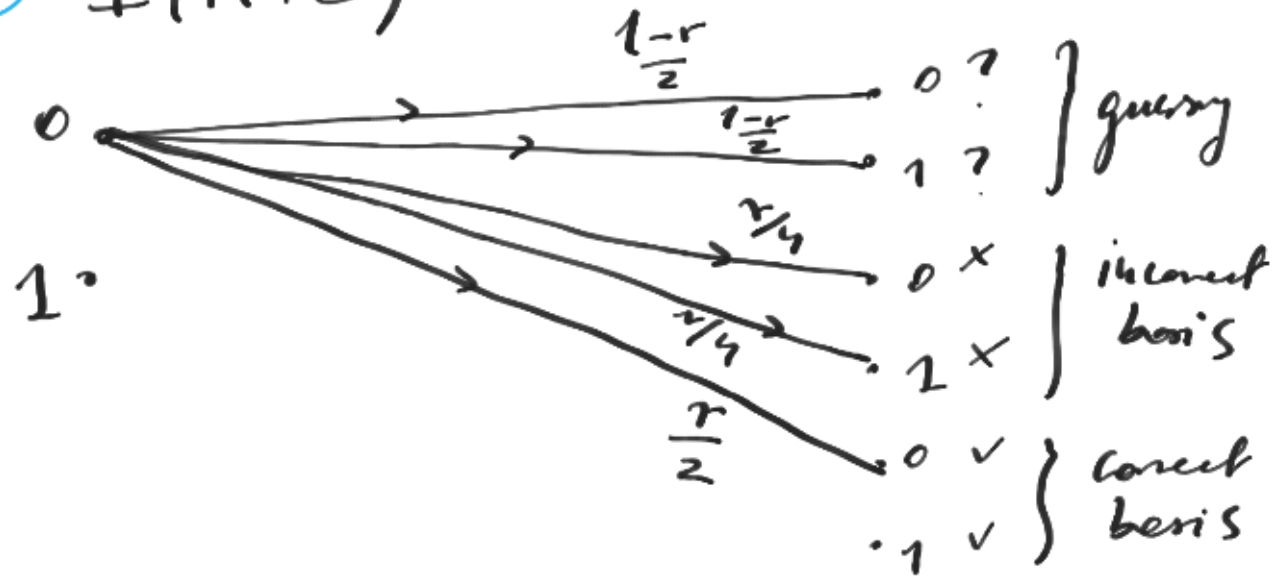
(a) generalised I & R

- only fraction "r" intercepted by Eve

. for the rest "1-r" Eve guesses.

$\Rightarrow QBER = \frac{r}{4}$ ① $\Rightarrow I(A:B) = 1 - h\left(\frac{r}{4}\right)$

② $I(A:E)$



$I(A:E) = \frac{r}{2}$ (余 $= I(B:E)$)

{ ⇒ otherwise ! $B \to A$
$C_S = I(A:B) - I(B:E)$

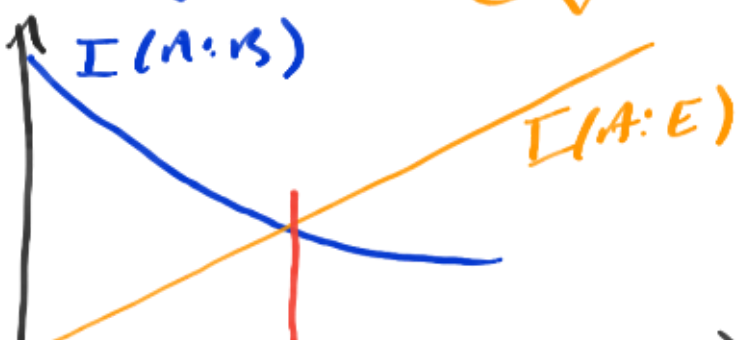
gen. I & R : (with $A \to B \in \{0,1\}^A$)

$C_S = I(A:B) - I(A:E) =$

$= 1 - h\left(\frac{r}{4}\right) - \frac{r}{2}$

$= \underbrace{1 - h(QBER)}_{} - \underbrace{2\,QBER}_{} > 0$

$C_S > 0$



$QBER_{th} = 17.1\%$

$\Rightarrow$

$QBER \geq QBER_{th} = 17.1\%$

they must abort!

{otherwise do EC+PA and get secure ?! key}

?? What about more general attacks?

(b) individual $\Rightarrow$ Exercises

Aside: (beyond IID $\Rightarrow$ CKT does not apply...)

$\Uparrow$

(c) collective $C_S \geq I(A:B) - \chi(A:E)$

$I(A:E) \leq \chi(A:E)$

[Devetak-Winter 2005]

$\chi(A:E) = S(\tilde{\rho}_E) - \sum_z p_z S(\rho_{E|z})$

{Holevo quantity}

$QBER \leq 11\%$

$\Uparrow$

(d) coherent {same as for collective...}

Proofs: highly

non-trivial

EXERCISES

Individual attacks

IsRf 1) Eve measures at θ to 0°.
2) Eve measures at θ_{opt} r-fraction.
3) Optimal phase-covariant cloning
($\Leftrightarrow$ optimal ind. attack)