Featured film: QKD based on twisted-ebits

Synopsis:

Four dangerous physicists Karol, Michal, Pawel, Jonathan were put in captivity in two adjacent jail-rooms. They tried to secretly agree on an escape plot, but their conversations across the wall were always overheard by the guard.

One day, they discovered some joint quantum states pre-shared across the rooms. Running QKD by first distilling ebits had failed (state not distillable).

Were the states noisy-twisted-ebits left behind from previous escapees, or were they set by the guard? Can they escape?

QKD based on twisted-ebits

Karol Horodecki [1], Michal Horodecki [1], Pawel Horodecki [2]
Debbie Leung [3], Hoi-Kwong Lo [4] & Jonathan Oppenheim [5]

quant-ph/0309110,0506189,0510067,0608195

Matthias Christandl, Stephanie Wehner, Andreas Winter
Guest-appearance (Renato Renner)

(1) Univeristy of Gdańsk, Poland
(2) Technical University of Gdańsk, Poland
(3) University of Waterloo, Canada (previously Caltech, USA)
(4) University of Toronto, Canada
(5) University of Cambridge, United Kingdom

$Funding: EU grants RESQ, QUPRODIS, PROSECCO; PMSRiT, Cambridge MIT-Institute, Newton Trust, NSF, Tolman Foundation, Croucher Foundation, NSERC, CRC, CFI, OIT, PREA, CIPI, CIAR$

Scene selection:

Chapters 1-4
Early days

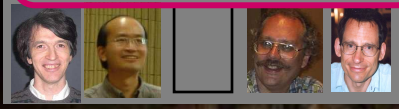
BB84
E92
6-state protocol

Chapters 5-8
Coping w/ noise

Privacy amplification
Error correction

Chapters 9-12
A triumph - Unconditional security

Mayers 96
Lo-Chau 98
Shor-Preskill 00



Chapters 13-16
A twist

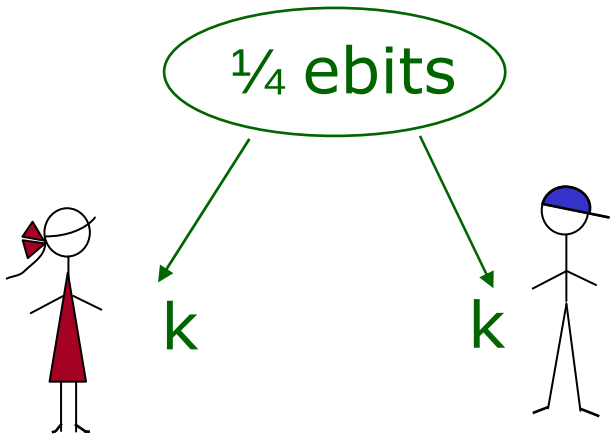
Twisted ebits
HHH0 03,05

Chapters 17-20
Twisted QKD

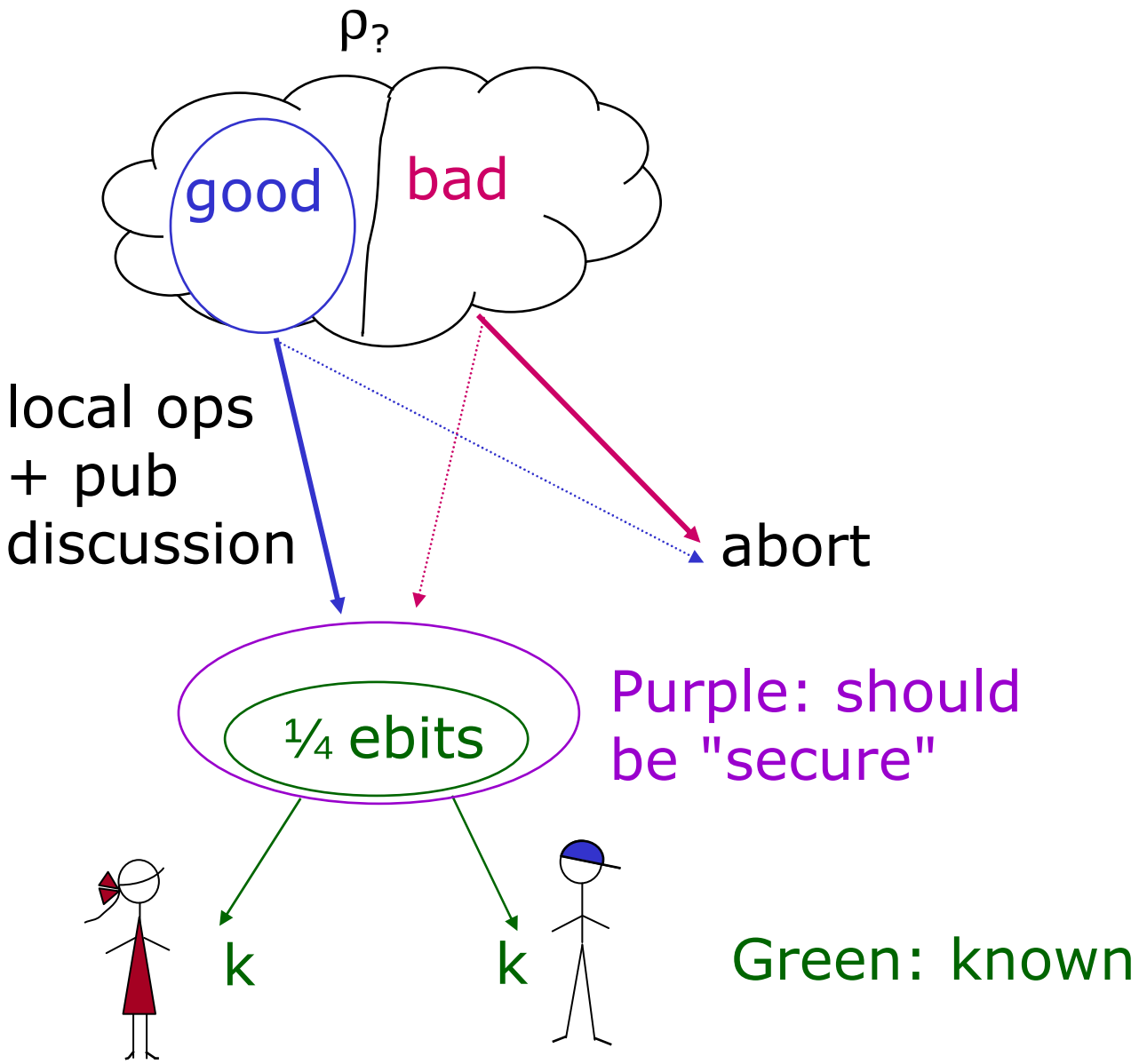
QKD based on twisted ebits
Unconditional security

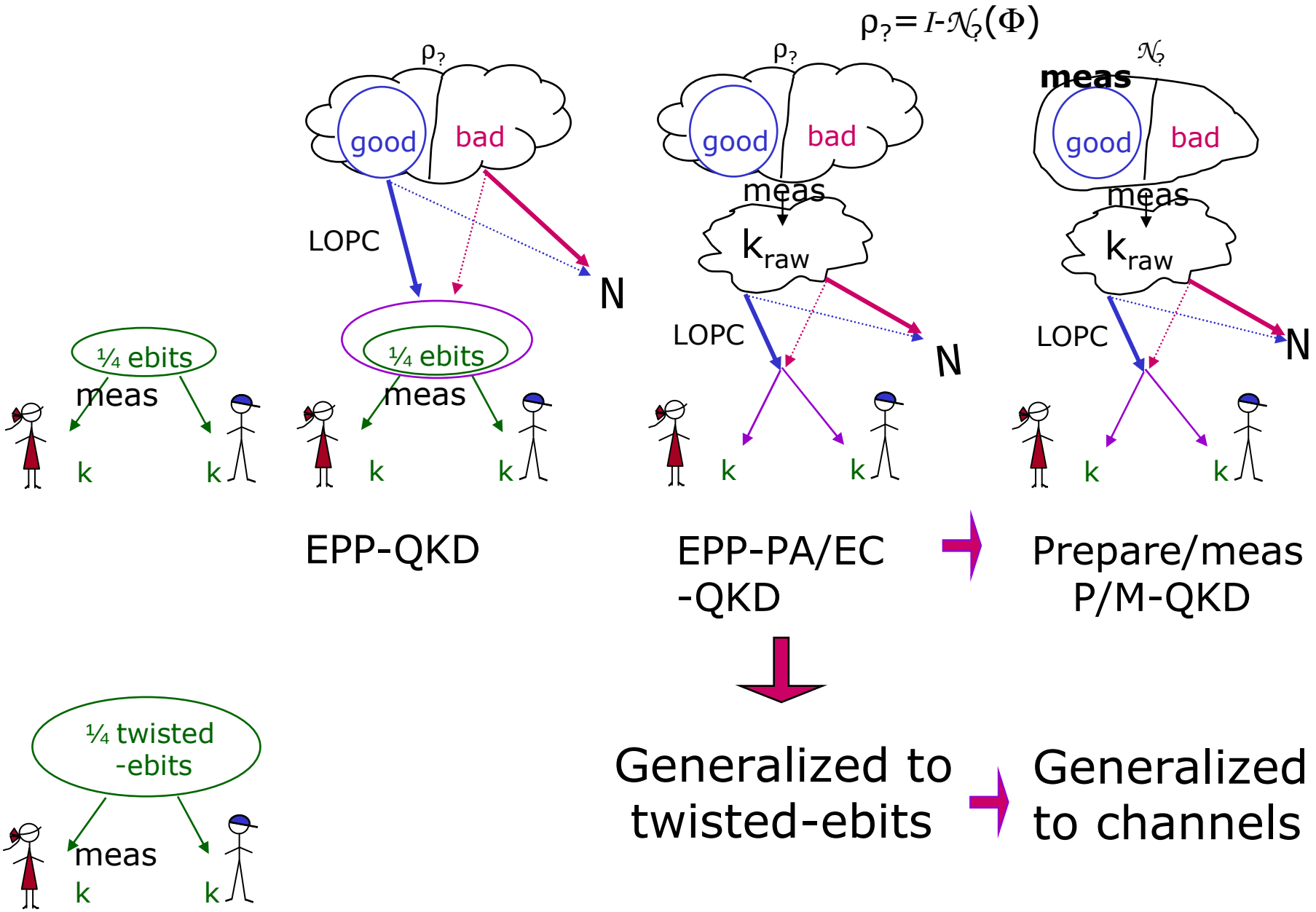
Chapters 21-14
Back to channels

QKD
without
Quantum
capacity



Green: known


ρ?
good
bad
local ops
+ pub
discussion
abort
¼ ebits
Purple: should
be "secure"
k
k
Green: known


ρ?
good
bad
LOPC
N
¼ ebits
meas
k
k
ρ?
good
bad
meas
k raw
LOPC
N
k
k
ρ? = I-N?(Φ)
N?
meas
good
bad
meas
k raw
LOPC
N
k
k
EPP-QKD
EPP-PA/EC
-QKD
Prepare/meas
P/M-QKD
¼ twisted
-ebits
meas
k
k
Generalized to
twisted-ebits
Generalized
to channels

Quantum key A bipartite quantum state possessed by and **known to** Alice and Bob that can be measured locally (WLOG in |0i,|1i basis) to give a secure key

e.g. 1 ebit: $|00i+|11i_{AB}$! $|00ih00|+|11ih11|_{AB}$

$- |\psi i_E$ ↑ $- \rho_E$

purification

inaccessible to Eve

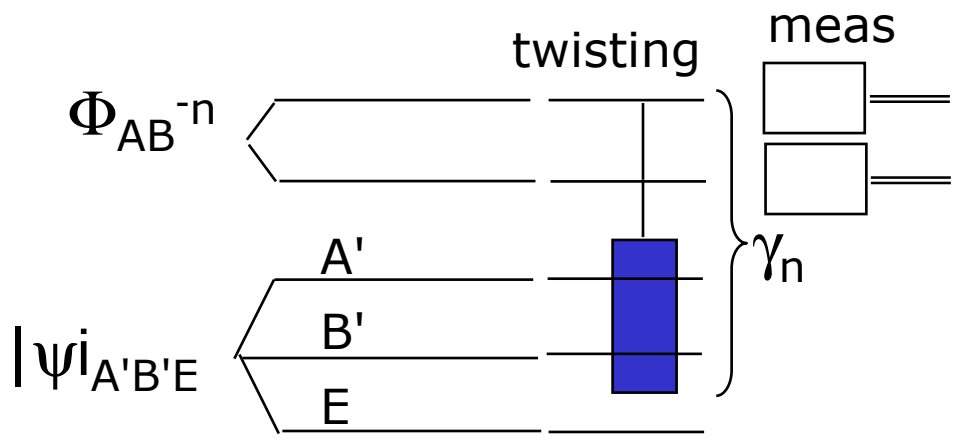
For simplicity, consider 2^n dim

n ebits: $\Phi^{-n} = (|\Phi ih\Phi|)^{-n}$

Quantum key (most general)

$\gamma_n = U_t\ (\Phi^{-n} - |\psi ih\psi|_{A'B'E})\ U_t^{y}$

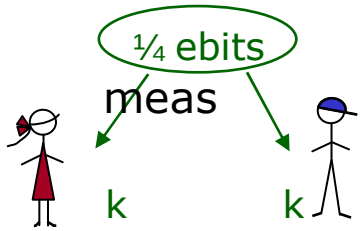
Twisting operation $U_t = \sum_{ij} |ijihij|_{AB} - U_{ij\ A'B'}$

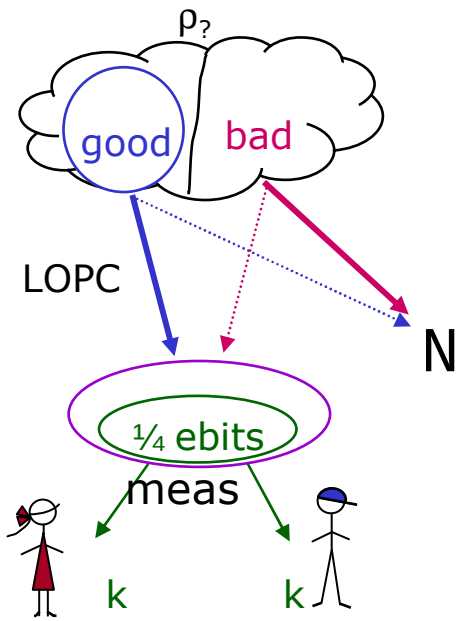


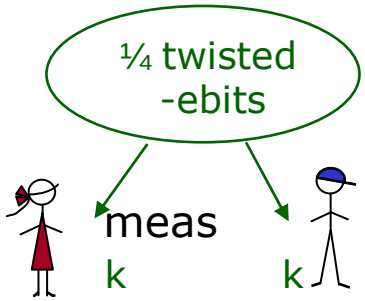
Intuition : (1) meas commute with twisting U_t

(2) U_t does not affect E

Quantum key distribution (given untrusted $\rho_?$)







Bruteforce method:

ebit-purification-QKD

By first distilling entanglement

e.g. Lo-Chau (LC) protocol

Quantum key distribution (given untrusted $\rho_?$)

Lo-Chau protocol (EPP-QKD) recap

(0) Share n bipartite systems, joint state $\rho_?$

(1) Imagine the n systems have been measured in Bell basis.

(2) Randomly select 2m test systems.

(a) On m of them, estimate Z error rate p_z
(expectation of XX) (or $\mathrm{E}[XI \pounds IX]$)

(b) On the rest, estimate X error rate p_x
(expectation of ZZ) (or $\mathrm{E}[ZI \pounds IZ]$)

(3) Apply entanglement purification on the rest if estimates of p_x, p_z are below threshold

(4) Measure ebits to get key

Quantum key distribution (given untrusted $\rho_?$)

Lo-Chau-Shor-Prekill (PA/EC-QKD) recap

(0) Share n bipartite systems, joint state $\rho_?$

(1) Imagine the n systems have been measured in Bell basis.

(2) Randomly select 2m test systems.

(a) On m of them, estimate Z error rate p_z
(expectation of XX) (or $\mathrm{E}[XI \pounds IX]$)

(b) On the rest, estimate X error rate p_x
(expectation of ZZ) (or $\mathrm{E}[ZI \pounds IZ]$)

(3) Measure ~~ebits~~ rest of $\rho_?$ to get noisy key k_{raw}

(4) Apply ~~entanglement purification~~ error correction and privacy amplification on the rest if estimates of p_x, p_z are below threshold

distillation used in proof, but not in the actual protocol

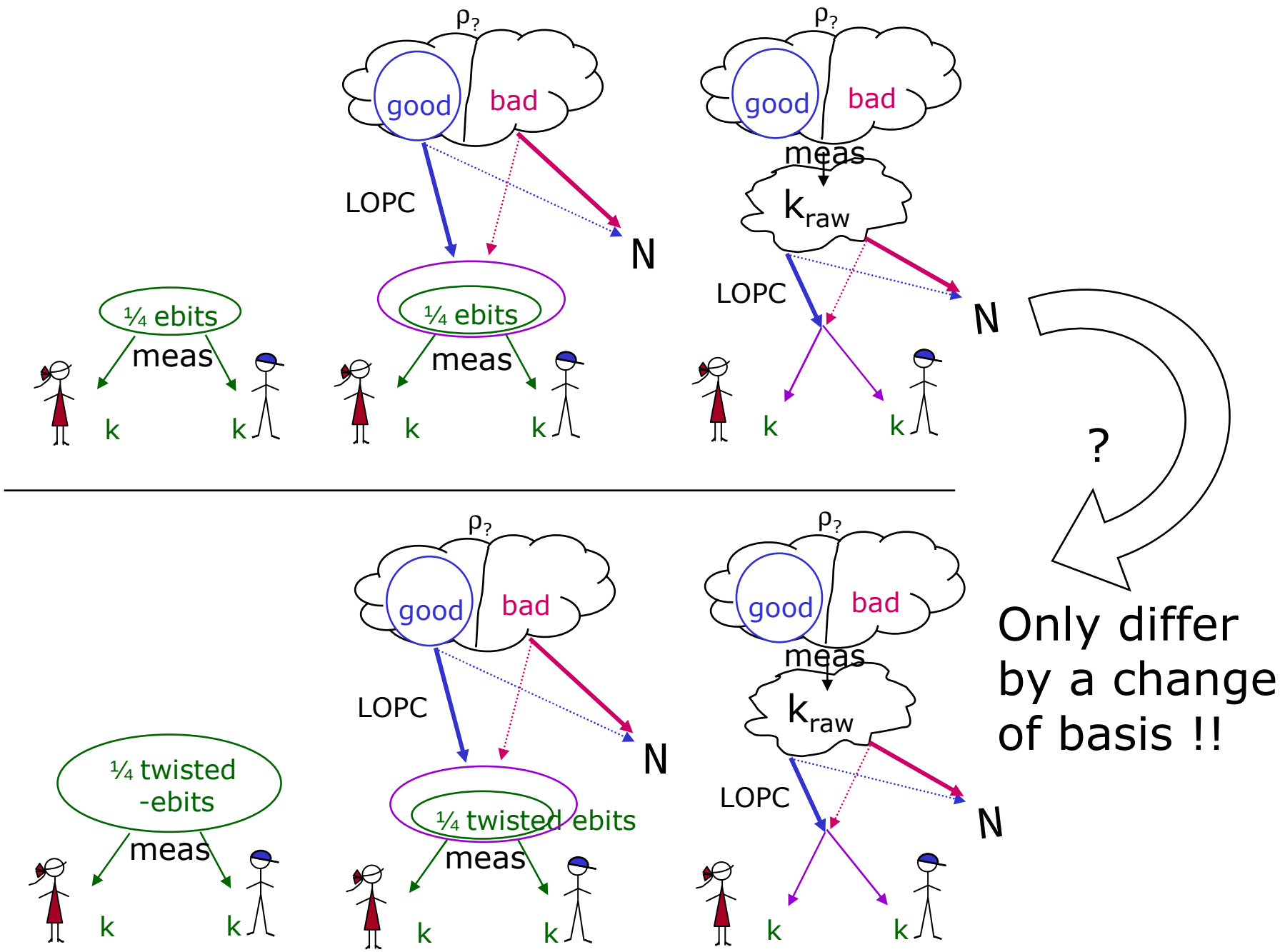
Quantum key distribution (given untrusted $\rho_?$)

Motivation:

In the scenario when Alice and Bob know their shared state, there are noisy twisted ebits with
- little distillable entanglement but high key rate
- no distillable entanglement but nonzero (e.g. 0.02) key rate

In the scenario when they don't know/trust their shared state, if $\rho_?$ is close to such state, distilling ebits and then measuring a key give "poor rate."

Can twisted ebits be "distilled" directly?


ρ?
good
bad
LOPC
N
¼ ebits
meas
k
k
ρ?
good
bad
meas
k raw
LOPC
N
k
k
?
Only differ
by a change
of basis !!
¼ twisted
-ebits
meas
k
k
ρ?
good
bad
LOPC
N
¼ twisted ebits
meas
k
k
ρ?
good
bad
meas
k raw
LOPC
N
k
k

Quantum key distribution (given untrusted $\rho_?$)

Trivially, silly-ly, and forbiddenly ....

Alice and Bob apply some appropriate U_t & run Lo-Chau protocol for entanglement distillation, and apply U_t^y, then, they're distilling twisted ebits ...

Better still, apply U_t and run Lo-Chau-Shor-Preskill EC/PA-QKD protocol (that only pretends to distill).

Mathematically that's correct (just can't be done ;P

Quantum key distribution (given untrusted $\rho_?$)

(a) Lo-Chau-Shor-Prekill (PA/EC-QKD) TWISTED

(0) Share n bipartite systems, joint state $\rho_?$

Apply U_t^{-n}

(1) Imagine the n systems measured in Bell basis.

(2) Randomly select 2m test systems.

(a) On m of them, estimate Z error rate p_z
(expectation of XX)

(b) On the rest, estimate X error rate p_x
(expectation of ZZ)

(3) Measure rest of $\rho_?$ to get noisy key k_{raw}

(4) Apply EC/PA on the rest if estimates of p_x, p_z · threshold

Finally, apply U_t^{-ny}

Quantum key distribution (given untrusted $\rho_?$)

(a) Lo-Chau-Shor-Prekill (PA/EC-QKD) TWISTED

(0) Share n bipartite systems, joint state $\rho_?$

(1) Imagine the n systems measured in TWISTED Bell basis.

Apply U_t^{-n}

(2) Randomly select 2m test systems.

(a) On m of them, estimate Z error rate p_z
(expectation of XX)

(b) On the rest, estimate X error rate p_x
(expectation of ZZ)

(3) Measure rest of $\rho_?$ to get noisy key k_{raw}

(4) Apply EC/PA on the rest if estimates of p_x, p_z · threshold

Finally, apply U_t^{-ny}

Quantum key distribution (given untrusted $\rho_?$)

(a) Lo-Chau-Shor-Prekill (PA/EC-QKD) TWISTED

(0) Share n bipartite systems, joint state $\rho_?$

(1) Imagine the n systems measured in TWISTED Bell basis.

Apply U_t^{-n}

(2) Randomly select 2m test systems.

(a) On m of them, estimate Z error rate p_z
(expectation of XX)

(b) On the rest, estimate X error rate p_x
(expectation of ZZ)

Apply U_t^{-ny}

(3) Measure rest of $\rho_?$ to get noisy key k_{raw}

(4) Apply EC/PA on the rest if estimates of p_x, p_z · threshold

Quantum key distribution (given untrusted $\rho_?$)

(a) Lo-Chau-Shor-Prekill (PA/EC-QKD) TWISTED

(0) Share n bipartite systems, joint state $\rho_?$

(1) Imagine the n systems measured in TWISTED Bell basis.

(2) Randomly select 2m test systems.

(a) On m of them, estimate twisted phase error rate p_z
(expectation of $U_t\ XX_{AB} - II_{A'B'}\ U_t^y$)

(b) On the rest, estimate twisted bit error rate p_x
(expectation of $U_t\ ZZ_{AB} - II_{A'B'}\ U_t^y = ZZ$
$\therefore$ reduces to finding $\mathrm{E}\,[ZI \pounds IZ]$)

(3) Measure ebits rest of $\rho_?$ to get noisy key k_{raw}

(4) Apply EC/PA on the rest if estimates of p_x, $p_z \cdot$ threshold

To estimate twisted Z error rate:

Label test system by superscripts [1] , ..., [m]

The goal is to find $p_{t\text{-}z}^{est} := tr(\rho^{[1,\ldots,m]} (O^{[1]} + O^{[2]} + \ldots + O^{[m]}))/m$

where $O = U_t (XX_{AB} - I_{A'B'}) U_t^y$

Express $O = \sum_{i=1}^{t} \alpha_i O_i$ where O_i are product obs (est via LOCC)

Divide the m test systems into t parts, estimate O_i on i-th part.

Sounds good ... Does it really work ??

To estimate twisted Z error rate:

Label test system by superscripts [1] , ..., [m]

The goal is to find $p_{t\text{-}z}^{est} := tr(\rho^{[1,\ldots,m]} (O^{[1]} + O^{[2]} + \ldots + O^{[m]}))/m$

where $O = U_t (XX - I_{A'B'}) U_t^y$

Express $O = \sum_{i=1}^{t} \alpha_i O_i$ where O_i are product obs (est via LOCC)

Divide the m test systems into t parts, estimate O_i on i-th part.

Guest appearance -- Renner ++ 05 -- Quantum deFinetti Thm

$\rho^{[1,\ldots,m]}$ ¼ $sd\mu\ \mu_{-m}$ (comes from sampling m sys from n)

μ_{-m} : almost tensor power state -- if meas $\mathcal{M}^m$ is applied, Chernoff-like bounds hold for output statistics

Similarly for reductions of μ_{-m} to each i-th part

$p_{t\text{-}z}^{(direct)\ est}$ ¼ $sd\mu\ tr(\mu\ O) = sd\mu \sum_{i=1}^{t} \alpha_i\ tr(\mu\ O_i)$ ¼ $p_{t\text{-}z}^{(indirect)\ est}$

what an ideal meas will approx

what the actual meas will approx

Remarks:

(1)

Note that $O = U_t (XX - I_{A'B'}) U_t^y = \sum_{i=1}^{t} \alpha_i O_i$

and we estimate the product obs O_i .

Can choose any product basis for operators (matrices) independent of U_t !!

i.e The quantum meas are fixed.
"Twisting" is just the choice of the α_i and can be chosen on a classical computer AFTER getting the data. The choice can min the Z error rate and max the key rate ! (i.e. the twist is to re-interpret the Z-error estimation data, peeling off contributions from noise characterized as harmless.)

Remarks:

(2)

Security parameter related to the singlet fidelity of the associated distillation protocol, is roughly the same as in the composable security parameter in the UC framework (Ben-Or Mayers 04, cf Renner's talk as well).

Remarks:

(3)

Consider an unknown state $\rho_?$ that is suspected to be many copies of one of these bound entangled noisy twisted states.

Interpret it as arising from an insecure channel that can only creates bound entanglement.

Then, the channel "supports" QKD, withOUT quantum capacity.

Remarks:

(4)

If the sender measures her share of $\rho_?$ prescribed by our QKD scheme, before sending the other half through a channel, a prep-meas scheme can be obtained.

For our example of bound-entangled $\rho_?$, the prep-meas scheme is just the 6-state protocol (with most of the qubits sent in the computation basis).

Again, the current result gives a new way to calculate how much PA has to be done, therefore channels used to be called "too noisy" can now be used.

Remarks:

(5)

Qn: can all entanglement-binding channel be used for QKD?

The End
Thank You