

# Quantum key distribution based on private states

Karol Horodecki <sup>(1)</sup>, Michal Horodecki <sup>(1)</sup>, Pawel Horodecki <sup>(2)</sup>  
Debbie Leung <sup>(3)</sup>, Hoi-Kwong Lo <sup>(4)</sup> & Jonathan Oppenheim <sup>(5)</sup>

(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

[quant-ph/0309110,0506189,0510067](#) + unpublished rumors

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

# Outline

Background: E92 & Lo-Chau-security proof (+protocol)

- Quantum Key (ebits,  $\gamma$  states)
- Distillation (trusted imperfect states)
- Distribution (untrusted states)
- Moral
  - entanglement  $\neq$  key
  - channel with zero quantum capacity but nonzero key capacity

**Quantum key** A bipartite quantum state (possessed by *Alice & Bob*) that provides a secure key as local measurement outcome

e.g. 1 ebit:  $|00\rangle + |11\rangle_{AB} \otimes |\psi\rangle_E \rightarrow |00\rangle\langle 00| + |11\rangle\langle 11|_{AB} \otimes \rho_E$

↑

purified by “Frank”  
(secure local garbage bins of Alice & Bob  
inaccessible to Eve )

↑

$|\Phi_2\rangle$

$$|\Phi_d\rangle = |00\rangle + \dots + |d-1\ d-1\rangle$$

$$\Phi_d = |\Phi_d\rangle\langle\Phi_d|$$

**Quantum key** A bipartite quantum state (possessed by *Alice & Bob*) that provides a secure key as local measurement outcome

$$\text{e.g. 1 ebit: } |00\rangle + |11\rangle_{AB} \rightarrow |00\rangle\langle 00| + |11\rangle\langle 11|_{AB} \otimes |\psi\rangle_E \otimes \rho_E$$

Most general: HHH0 0309110

$$U_t (\Phi_{d AB} \otimes |\psi\rangle\langle\psi|_{A'B'E}) U_t^\dagger \rightarrow \sum_{i=1}^d |ii\rangle\langle ii|_{AB} \otimes \rho_E$$

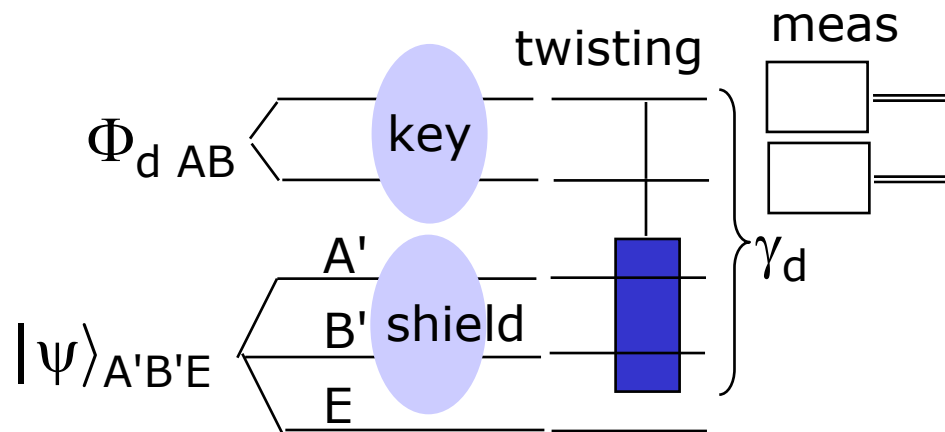
purified by "Frank"

$$\text{Twisting operation } U_t = \sum_{ij} |ij\rangle\langle ij|_{AB} \otimes U_{ij A'B'}$$

# Quantum key

$$\gamma_d = U_t (\Phi_{d AB} \otimes |\psi\rangle\langle\psi|_{A'B'E}) U_t^\dagger$$

$$\text{Twisting operation } U_t = \sum_{ij} |ij\rangle\langle ij|_{AB} \otimes U_{ij A'B'}$$



Intuition 1: meas commute with twisting  $U_t$

2: A'B' acts as "shield" for the "key" in AB

## Quantum key

$$\gamma_d = U_t (\Phi_{d AB} \otimes |\psi\rangle\langle\psi|_{A'B'E}) U_t^\dagger$$

Story ends here if the world is

(1) error-free

(perfect)

(2) contains only good people

(trusted)

# Quantum key distillation from imperfect but trusted iid source $\rho^{\otimes n}$

Easy approach: first distilling ebits

$$\rho_{AB}^{\otimes n} \rightarrow \approx \Phi_2^{\otimes n D(\rho)} \quad D(\rho) = \text{distillable entanglement}$$

DW03, HHHO 0506189:

**Most general:** directly get  $C(\rho) = (1/n) \log d_2$  keybits

$$\rho_{ABA'B'}^{\otimes n} \rightarrow \approx \sum_{i=1}^{d^2} |ii\rangle\langle ii|_{AB} \otimes \rho_E$$

**Restricted:** first distill "a"  $\gamma$  state:

$$\rho_{ABA'B'}^{\otimes n} \rightarrow \approx \gamma_{d1}$$

then generate  $K(\rho) = (1/n) \log d_1$  keybits

Clearly:  $D(\rho) \leq K(\rho) \leq C(\rho)$       Surprise: (1)  $\forall \rho \ K(\rho) = C(\rho)$ ,  
(2)  $\exists \rho \ K(\rho) \gg D(\rho)$   
(3)  $\exists \rho \ K(\rho) > 0 = D(\rho)$

# Outline

Will use E92 & Lo-Chau-security proof (+protocol) as the platform of discussion. Prepapre-measure scheme will be discussed on the side.

- Quantum Key (ebits,  $\gamma$  states)
- Distillation (trusted imperfect states)
- Distribution (untrusted states)
- Moral
  - entanglement  $\neq$  key
  - channel with zero quantum capacity but nonzero key capacity

## Quantum key distribution given untrusted $\gamma$

Bruteforce method:

Extract secure keybits via entanglement distillation  
e.g. Lo-Chau (LC) protocol

Why, by attempting to distill ebits, can untrusted states be turned into a secure key?

Can attempts to distill  $\gamma$  states work on untrusted states?

NB Entanglement distillation for the sake of generating a key is far-suboptimal or infeasible if the untrusted state  $\rho$  has  $K(\rho) \gg D(\rho)$  or if  $0 = D(\rho)$

## Quantum key distribution given untrusted $\gamma$

Here (HLLO 0510067, HHHLLO 06@#?!\$) :

(a) recap LC for regular QKD based on untrusted ebits

(b) related untrusted  $\gamma$  to untrusted ebits

- first "untwist"  $\gamma$  in one's imagination.

- within one's imagination, apply LC

[i.e. bit & phase error estimation + ent purification]

In the bases "without imagination," above means bit & phase error estimation + ent purification + final key extraction all in "twisted" basis. We'll see how.

## Quantum key distribution given untrusted *ebits*

(a) Lo-Chau protocol (for regular QKD) recap

(0) Share  $n$  bipartite systems

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

(2) Randomly select  $2m$  test systems.

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

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

(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 *ebits*

NB. The Bell measurement gives classical meaning to  $p_x, p_z$ . So random sampling theory applies -- with high prob  $p_x, p_z$  on test systems  $\approx$  that in the untested systems.

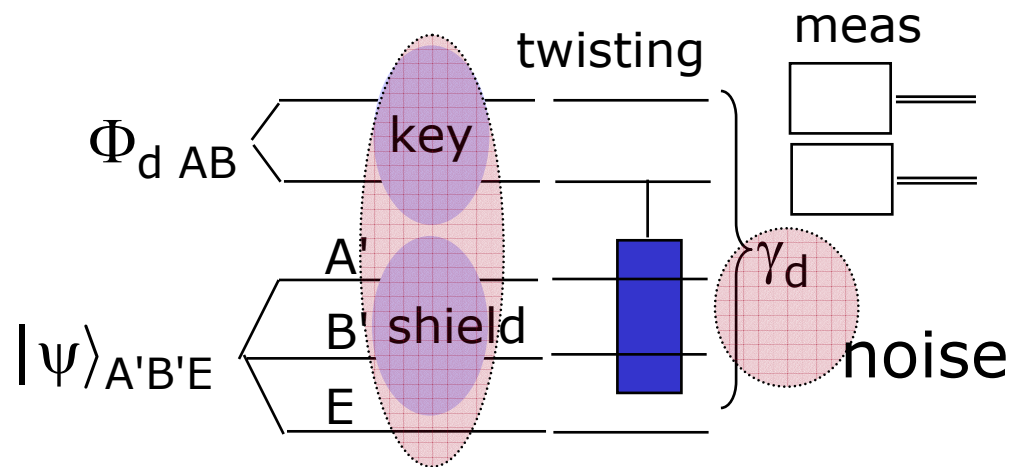
*Just for the relevant part of the protocol:* the Bell measurement has no effect.

Reason: measurement of  $XX, ZZ$  (on any state) commutes with Bell measurement,  $\therefore$  expectation of  $XX, ZZ$  unaffected by including/omitting the Bell measurement.  $\therefore$  Can imagine the Bell measurement in security proof without doing it.

**Subtlety:** Expectation of  $XX$  is indirectly inferred from those of  $XI, IX$ . The outcome statistics of measuring  $XI, IX$  are affected by the Bell measurement (meas of  $XI, IX$  don't commute with Bell meas), but the combined estimate of expectation of  $XX$  is unaffected.

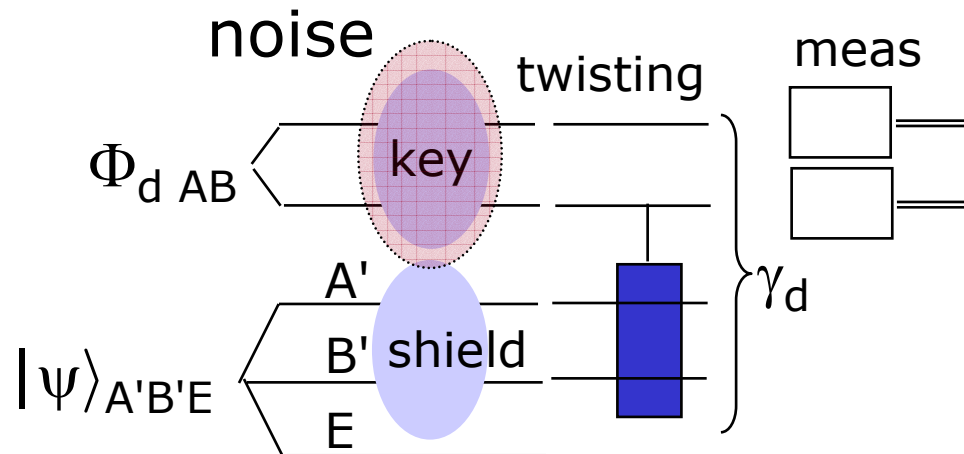
# Quantum key distribution given untrusted $\gamma$

Now, if Alice and Bob are given untrusted  $\gamma$  states  
since  $\gamma = U_t (\text{Bell states} \otimes \text{shield}) U_t^\dagger$



# Quantum key distribution given untrusted $\gamma$

Now, if Alice and Bob are given untrusted  $\gamma$  states  
 since  $\gamma = U_t (\text{Bell states} \otimes \text{shield}) U_t^\dagger$



So, **IF** Alice and Bob can undo  $U_t$ , they can then apply  
 Lo-Chau procedure to get nearly pure ebits in key  
 system, redo  $U_t$ , and measure out secure key.

untwist

retwist

## Quantum key distribution given untrusted $\gamma$

Starting with untrusted  $\gamma$

### (0) UNTWIST

- (1) Imagine the  $n$  systems have been measured in Bell basis.
- (2) Randomly select  $2m$  test systems.
  - (a) On  $m$  of them, estimate phase error rate  $p_z$   
(expectation of  $XX$ )
  - (b) On the rest, estimate bit error rate  $p_x$   
(expectation of  $ZZ$ )
- (3) Apply entanglement purification on the rest if estimates of  $p_x, p_z$  below threshold

### (0<sup>†</sup>) RETWIST

- (4) Measure  $\gamma$  to get key

## Quantum key distribution given untrusted $\gamma$

Starting with untrusted  $\gamma$

### (0) UNTWIST

- (1) Imagine the  $n$  systems have been measured in Bell basis.
- (2) Randomly select  $2m$  test systems.
  - (a) On  $m$  of them, estimate phase error rate  $p_z$   
(expectation of  $XX$ )
  - (b) On the rest, estimate bit error rate  $p_x$   
(expectation of  $ZZ$ )
- (3) Apply entanglement purification on the rest if estimates of  $p_x, p_z$  below threshold
- (4) Measure ebits to get key

### (0<sup>†</sup>) RETWIST

## Quantum key distribution given untrusted $\gamma$

Starting with untrusted  $\gamma$

### (0) UNTWIST

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

(2) Randomly select  $2m$  test systems.

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

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

### (0<sup>†</sup>) RETWIST

#### (0) UNTWIST

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

(4) Measure ebits to get key

### (0<sup>†</sup>) RETWIST

## Quantum key distribution given untrusted $\gamma$

Starting with untrusted  $\gamma$

### (0) UNTWIST

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

(2) Randomly select  $2m$  test systems.

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

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

### (0<sup>†</sup>) RETWIST

(0) UNTWIST Shor-Preiskill 00:

(3') Measure **imperfect** ebits to get raw key

(4') Apply **privacy amplification and error correction on raw key** based on  $p_x, p_z$  if  $p_x, p_z$  below threshold

### (0<sup>†</sup>) RETWIST

## Quantum key distribution given untrusted $\gamma$

Starting with untrusted  $\gamma$

### (0) UNTWIST

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

(2) Randomly select  $2m$  test systems.

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

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

### (0<sup>+</sup>) RETWIST

For QKD with untrusted  $\gamma$ :

(3') Measure **key part of imperfect  $\gamma$  states** to get raw key

(4') Apply **privacy amplification and error correction on raw key** based on  $p_x, p_z$  if  $p_x, p_z$  below threshold

## Quantum key distribution given untrusted $\gamma$

Starting with untrusted  $\gamma$

How?

- (1) Imagine the  $n$  systems have been measured in **twisted** Bell basis  $\{\gamma_{2k} = U_t ( [I \otimes \sigma_k \Phi_{2AB} I \otimes \sigma_k] \otimes |\psi\rangle\langle\psi|_{A'B'E} ) U_t^\dagger \}_k$
- (2) Randomly select  $2m$  test systems.
  - (a) On  $m$  of them, estimate **twisted** phase error rate  $p_z$   
(expectation of  $U_t ( XX \otimes |\psi\rangle\langle\psi|_{A'B'E} ) U_t^\dagger$  )
  - (b) On the rest, estimate **twisted** bit error rate  $p_x$   
(expectation of  $U_t ( ZZ \otimes |\psi\rangle\langle\psi|_{A'B'E} ) U_t^\dagger$  )

For QKD with untrusted  $\gamma$ :

- (3') Measure **key part of imperfect  $\gamma$  states** to get raw key
- (4') Apply **privacy amplification and error correction on raw key** based on  $p_x, p_z$  if  $p_x, p_z$  below threshold

## Quantum key distribution given untrusted $\gamma$

### How-to

Randomly select  $2m$  test systems.

(a) On  $m$  of them, estimate twisted phase error rate  $p_z$   
(expectation of  $U_t ( XX \otimes |\psi\rangle\langle\psi|_{A'B'E} ) U_t^\dagger$  )

(b) On the rest, estimate twist bit error rate  $p_x$   
(expectation of  $U_t ( ZZ \otimes |\psi\rangle\langle\psi|_{A'B'E} ) U_t^\dagger$  )

Since  $U_t$  commute with  $ZZ$  (also  $ZI, IZ$ )  
just measure key part of  $\gamma$  states.

## Quantum key distribution given untrusted $\gamma$

### How-to

Randomly select  $2m$  test systems.

(a) On  $m$  of them, estimate **twisted** phase error rate  $p_z$   
(expectation of  $U_t ( XX \otimes |\psi\rangle\langle\psi|_{A'B'E} ) U_t^\dagger )$

call it  $O$

Previous solution HLLO 0510067 first distilled  $O(m)$  ebits for the teleportation of  $A'$  to Bob.

Since  $m \ll n$ , applies to the case even when  $K(\rho) \gg D(\rho) > 0$ .

What if  $K(\rho) > D(\rho) = 0$  ?

Needs a new technique ...

The exponential quantum deFinetti Theorem  
which gives many other advantages  
(Renner PhD Thesis 05).

## Quantum key distribution given untrusted $\rho$

### How-to

Randomly select  $2m$  test systems.

- (a) On  $m$  of them, estimate **twisted** phase error rate  $p_z$   
(expectation of  $U_t ( \text{XX} \otimes |\psi\rangle\langle\psi|_{A'B'E} ) U_t^\dagger )$

Label test system by superscripts  $[1], \dots, [m]$  call it  $O$

The goal is to find  $p_z^{\text{est}} := \text{tr}(\rho^{[1,\dots,m]} (O^{[1]} + O^{[2]} + \dots + O^{[m]}))$ .

Express  $O = \sum_{i=1}^t \alpha_i O_i$  s.t. each  $O_i$  can be estimated by LOCC.

Divide the  $m$  test systems into  $t$  parts, and estimate one  $O_i$  on each part ( $O_i$ 's may not commute).

# Quantum key distribution given untrusted $\rho$

## How-to

Randomly select  $2m$  test systems.

- (a) On  $m$  of them, estimate **twisted** phase error rate  $p_z$   
(expectation of  $U_t ( \mathbf{XX} \otimes |\psi\rangle\langle\psi|_{A'B'E} ) U_t^\dagger$  )

Label test system by superscripts  $[1], \dots, [m]$

The goal is to find  $p_z^{\text{est}} := \text{tr}(\rho^{[1,\dots,m]} (O^{[1]} + O^{[2]} + \dots + O^{[m]}))$ .

Express  $O = \sum_{i=1}^t \alpha_i O_i$  s.t. each  $O_i$  can be estimated by LOCC.

Divide the  $m$  test systems into  $t$  parts, and estimate one  $O_i$  on each part ( $O_i$ 's may not commute).

call it  $O$

By the Quantum deFinetti Theorem (Renner PhD Thesis 2005)

$$\rho^{[1,\dots,m]} \approx \int d\mu \mu^{\otimes m} \quad [\text{NB almost tensor power state}]$$

$$p_z^{\text{est}} \approx m \int d\mu \text{tr}(\mu O) = m \int d\mu \sum_{i=1}^t \alpha_i \text{tr}(\mu O_i)$$

Each  $\text{tr}(\mu O_i)$  can be well estimated due to  $\rho^{[1,\dots,m]} \approx \int d\mu \mu^{\otimes m}$  and the Chernoff bound.

## Quantum key distribution given untrusted $\rho$

### (b) TWISTED Lo-Chau protocol for QKD BASED on $\gamma/\rho$

(1) Imagine the  $n$  systems have been measured in Twisted Bell basis  $\{\gamma_{2k} = U_t ( [I \otimes \sigma_k \Phi_{2 AB} I \otimes \sigma_k] \otimes |\psi\rangle\langle\psi|_{A'B'E} ) U_t^\dagger \}_k$

(2) Randomly select  $2m$  test systems.

(a) On  $m$  of them, estimate twisted phase error rate  $p_z$   
(expectation of  $U_t ( XX \otimes |\psi\rangle\langle\psi|_{A'B'E} ) U_t^\dagger$ )

(b) On the rest, estimate twist bit error rate  $p_x$   
(expectation of  $U_t ( ZZ \otimes |\psi\rangle\langle\psi|_{A'B'E} ) U_t^\dagger$ )

local meas

(3') Measure key part of imperfect  $\gamma$  states to get raw key

(4') Apply privacy amplification and error correction on raw key based on  $p_x, p_z$  if  $p_x, p_z$  below threshold

Note -- prepare-measure scheme possible

## Discussion

### Our method:

- Works for all  $\rho$  with  $K(\rho) \neq 0$  (distillability doesn't matter)
- Does not distill, but embed a distillation argument via the Shor-Preskill reduction

### Note:

- For a "bound entangled" quantum channel that is thought to create  $\rho$ , can still distribute key securely, while channel has no quantum capacity (ability to transmit unknown quantum states).
- When little is known about the shared state, either
  - (a) guess a  $\gamma$ , and assume the state is noisy version of it (error rate and key rate depends on our guess) (prep-meas)
  - (b) do tomography to find good guess of  $\gamma$  (q. memory needed)

The End  
Thank You