Korea University, 27 March 2019

Nguyen Ba An
Thang Long University (TLU)

Thang Long Institute of Mathematics & Applied Sciences (TIMAS)

MOST RECENT WORK

Simultaneous observation of particle and wave behaviors of entangled photons

SCIENTIFIC REPORTS

Sci. Rep. 7, 42539 (2017)

Zhong-Xiao Man[1], Yun-Jie Xia[1] & Nguyen Ba An[2]

ARTICLE

DOI: 10.1038/s41467-017-01058-6

OPEN

Entanglement of photons in their dual wave-particle nature

Adil S. Rab[1], Emanuele Polino[1], Zhong-Xiao Man[2], Nguyen Ba An[3], Rosario Lo Franco[4,5] & Fabio Sciarrino[1]

Yun-Jie Xia[2], Nicolò Spagnolo[1],

nature COMMUNICATIONS

Nature Communications 8, 915 (2017)

Deterministic joint remote preparation of an equatorial hybrid state via high-dimensional Einstein–Podolsky–Rosen pairs: active versus passive receiver

Quantum Inf Process (2018) 17:75

C.T. Bich, L.T. Dat, N.V. Hop, N.B. An

Nonstandard protocols for joint remote preparation of a general quantum state and hybrid entanglement of any dimension

PHYSICAL REVIEW A 98, 042329 (2018)

N.B. An, L.T. Dat & J. Kim

Designs of interactions between discrete- and continuous-variable states for generation of hybrid entanglement

Quantum Inf. Process. 18:685 (2019)

S. A. Podoshvedov, N.B. An

TODAY's TALK

On "QUANTUM DIALOGUE"

which belongs to

CRYPTOGRAPHY

Alice

Bob

Eve

- Alice want to send a meassge to Bob
- Eve’s in the line to eavesdrop
- How to secure the communication?

PRIVATE-KEY SYSTEM

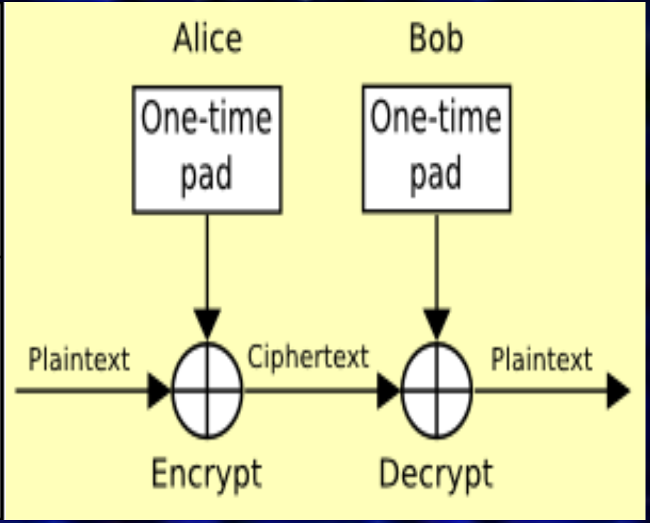
(Vernam 1917)

ENCRYPT

	0 0 1 1 0 1 0 1	Plaintext
⊕	1 1 1 0 0 0 1 1	Secret Key
=	1 1 0 1 0 1 1 0	Ciphertext

DECRYPT

	1 1 0 1 0 1 1 0	Ciphertext
⊕	1 1 1 0 0 0 1 1	Secret Key
=	0 0 1 1 0 1 0 1	Plaintext



Absolute Secure

BUT:

“One-time use” → INCONVENIENT

PUBLIC-KEY SYSTEM

(Rivest-Shamir-Adlman [RSA] 1997)

Alice: PA, SA

Bob: PB, SB

PX[SX[m]] = SX[PX[m]] = m

If Alice wants to send M = m + s to Bob

Alice encodes: PB[m] + SA[s] and sends to Bob

Bob decodes: SB[PB[m]] + PA[SA[s]] = m + s

Good: CONVENIENT (Now in use)

BAD: Unproven Security
& Broken by Quantum Computer

QUANTUM CRYPTOGRAPHY

Uses: - QUANTUM RESOURCES

- QUANTUM LAWS

(Nocloning, Measure → Disturbance,…)

→ QKD (BB84, E91,B92, …): UNCONDITIONAL SECURITY

(even in presence of qu-computers)

BUT:

Question: Can ones communicate **without** a prior QKD (as in emergency situations)?

Answer: YES, by **QUANTUM DIALOGUE!**

QUANTUM DIALOGUE:

Way to securely exchange info

(like to securely talk with each other)

without a prior QKD

HOW TO PERFORM

QUANTUM DIALOGUE?

Alice prepares

$$|\Psi\rangle_{AB} = |0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B$$

Sends B to Bob. Bob applies I, X, Z or Y on B if wants to send 2 bits $00, 01, 10$ or 11, then returns B to Alice

$$\begin{aligned} I \otimes I\,|\Psi\rangle_{AB} &= |0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B \\ I \otimes X\,|\Psi\rangle_{AB} &= |0\rangle_A|1\rangle_B + |1\rangle_A|0\rangle_B \\ I \otimes Z\,|\Psi\rangle_{AB} &= |0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B \\ I \otimes Y\,|\Psi\rangle_{AB} &= |0\rangle_A|0\rangle_B - |1\rangle_A|1\rangle_B \end{aligned}$$

Alice makes Bell measuremwnt to learn Bob's 2 bits.

Twice Holevo's bound (1973) $\Longrightarrow$ SUPERDENSE CODING (1992)

Now: Bob wants to send Alice i, j and Alice wants to send Bob m, n

Alice prepares $|\Psi_{m,n}\rangle_{AB} : \begin{cases} |\Psi_{0,0}\rangle_{AB} = |0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B \\ |\Psi_{0,1}\rangle_{AB} = |0\rangle_A|1\rangle_B + |1\rangle_A|0\rangle_B \\ |\Psi_{1,0}\rangle_{AB} = |0\rangle_A|0\rangle_B - |1\rangle_A|1\rangle_B \\ |\Psi_{1,1}\rangle_{AB} = |0\rangle_A|0\rangle_B - |1\rangle_A|1\rangle_B \end{cases}$

$C_{00} = I, C_{01} = X, C_{10} = Z, C_{11} = Y$

$I \otimes C_{ij}\, |\Psi_{m,n}\rangle_{AB} = |\Psi_{m\oplus i, n\oplus j}\rangle_{AB}$

- Alice sends B to Bob, Bob applies C_{ij} on B and returns to Alice
- **Alice's Bell measurement** $\rightarrow |\Psi_{m\oplus i,n\oplus j}\rangle_{AB}$ **to learn** i, j
- **Alice announce** $m \oplus i, n \oplus j \Longrightarrow$ **Bob learns** m, n

QUANTUM DIALOGUE [NBA, PLA 328,6 (2004)]

QUANTUM DIALOGUE

 (m,n)

 (i,j)

1) A $|\Psi_{m,n}\rangle_{AB}$ → B

2) C_{ij} B

A ← B

3) BM[AB] = $|\Psi_{m\oplus i,n\oplus j}\rangle_{AB}$

→ gets Bob's i,j

Then sends → $m \oplus i, n \oplus j$

4) Gets m,n

Security to be discussed later!

Another possible way to perform QUANTUM DIALOGUE

Exploiting NONSELECTIVE MEASUREMENT
(= Measurement without reading the outcome)

- Classically,
  Measurement without reading outcome = Doing Nothing

- Quantumly,
  Measurement without reading outcome = Making Sense

⇓

QUANTUM DIALOGUE

MATHEMATICAL PRELIMINARIES

For N = odd prime

$\exists$ complete set of $N+1$ MUBs (basis $\beta = 0, 1, \ldots, N-1$ and basis "$N+1$")

Each basis has N orthonormal states

A kth state $(k = 0, 1, \ldots, N-1)$ of a βth basis

$$|\beta; k\rangle = \frac{1}{\sqrt{N}} \sum_{l=0}^{N-1} \Omega^{\beta l^2 + kl} |l\rangle$$

$$\left|\langle \beta'; k' | \beta; k\rangle\right|^2 = \frac{1}{N}; \forall k, k'; \beta \neq \beta'$$

QD by Nonselective measurement

- Alice: $\beta \in \{0, 1, ..., N-1\}$
- Bob: $\beta' \in \{0, 1, ..., N-1\}$
- They wish to exchange their numbers securely

QD by Nonselective measurement

- Alice prepares (with β to be exchanged and k, q fixed)

$$|\beta; k, q\rangle_{AB} = \frac{1}{\sqrt{N}} \sum_{l=0}^{N-1} \Omega^{\beta l^2 + kl} |l\rangle_1 |q + l\rangle_2$$

Then Alice sends quNit B to Bob

- Bob measures B in basis β' (the to-be-exchanged number)

Then returns B to Alice without reading outcome (nonselective meas.)

$\Longrightarrow$ QuNits A and B become in a mixed (NOT pure) state

$$\rho_{AB}(\beta, \beta', k, q) = \sum_{p=0}^{N-1} \Pi_A(\beta', p) |\beta; k, q\rangle_{AB} \langle \beta; k, q| \Pi_A(\beta', p),$$

$$\Pi_A(\beta', p) = |\beta'; p\rangle_A \langle \beta'; p|$$

QD by Nonselective measurement

- Alice, having both A and B, measures them in β-basis (in which he prepared $|\beta;k,q\rangle_{AB}$) to find $|\beta;k',q'\rangle_{AB}$ with probability

$$P_{AB}(\beta,\beta',k,q,k',q') = \frac{1}{N}\delta_{k-k',2(\beta-\beta')(q-q')}$$

$$\Longrightarrow \beta' = \beta + \frac{k'-k}{2(q-q')}$$

That is, Alice gets Bob's number β'

Then Alice announce $\beta+\beta' \Longrightarrow$ Bob gets Alice's β.

THE INFO EXCHANGE IS DONE!

CAN BE REPEATED TO DO QUANTUM DIALOGUE

EVE's ATTACKS

CAPTURE-AND-REPLACE ATTACK

- Eve creates her own $|\beta''; k'', q''\rangle_{CD}$ (β'', k'', q'' at her choice) and CAPTURES B, store it on the way Alice $\to$ Bob

Then REPLACES B by C to be sent to Bob.

- Bob nonselectively measure C in basis β', then send it to Alice
- On the way Bob $\to$ Alice, Eve CAPTURES C, measures CD in basis β'' to get β'

Then, nonselectively measures B (from memory) in basis β' and sends it toAlice.

- Alice measures AB to get β' too, then announce $\beta + \beta'$ to allows Bob know β

THUS, Eve perfectly eavesdrops (If no SECURITY CHECK)

SECURITY CHECK

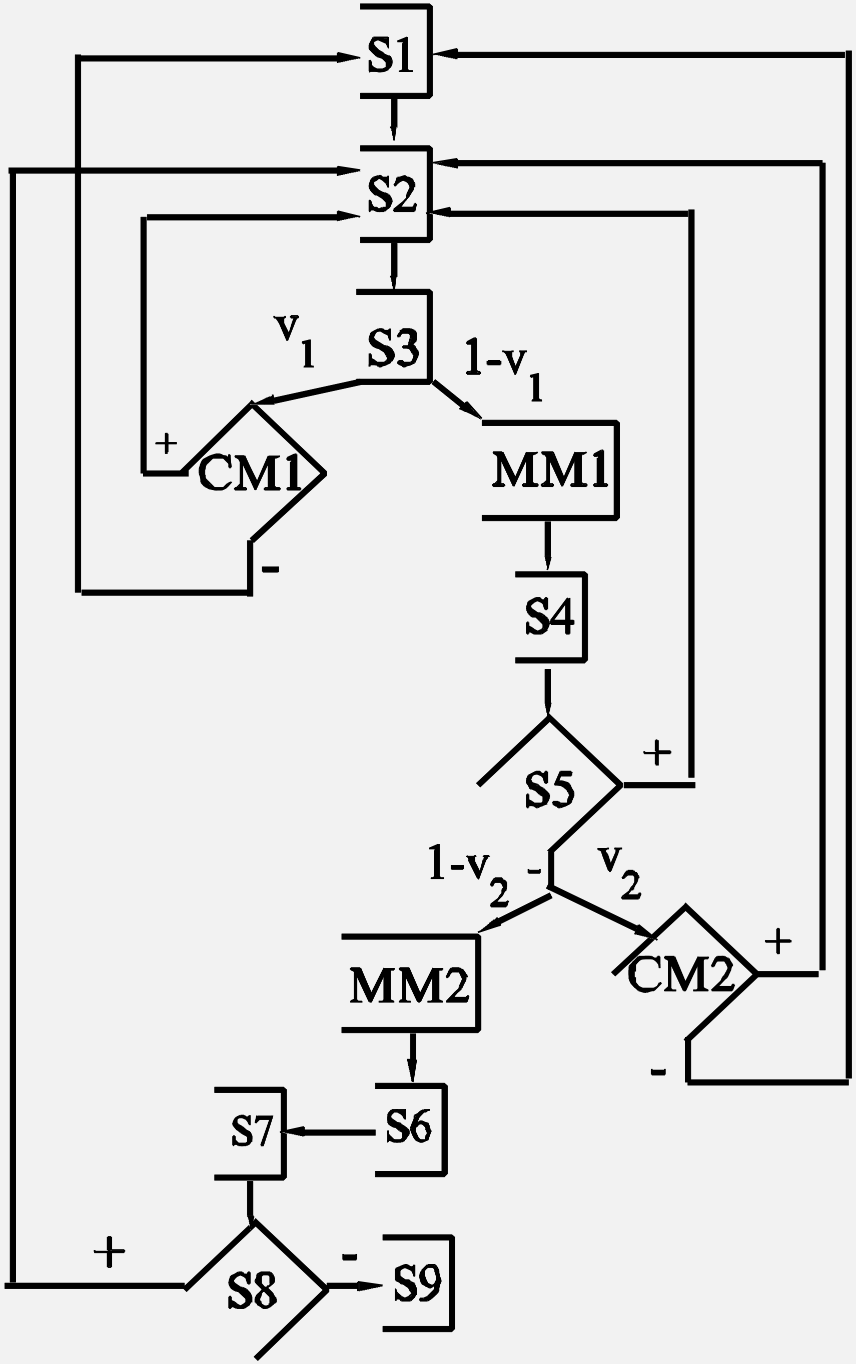
To detect Eve in this and other kinds of attacks,
two CONTROL MODES (CM) are introduced:

- CM1 (On the way Alice $\rightarrow$ Bob)

Bob measures B in computational basis and publishes outcome
Alice also measures A in computational basis.
Then they compare their outcomes to detect Eve

- CM2 (On the way Bob $\rightarrow$ Alice).

Alice and Bob reveal their choices and check some equality to detect Eve


S1
S2
S3
v1
1-v1
+
CM1
-
MM1
S4
S5
+
1-v2
-
v2
MM2
CM2
+
-
S6
S7
+
S8
-
S9

CONCLUSION

- Exploiting Quantum Physics
  [Quantum resources,
  quantum unitary operations,
  quantum measurements
  (even nonselective measurements), …]
  allows secure exchange of info without
  a prior QKD, like in a (quantum) dialogue

- The words “QUANTUM DIALOGUE”
  first appeared in [NBA, PLA 328, 6 (2004)]
- See also [NBA, J. Kor. Phys. Soc. 47, 562 (2005)
  and Adv. Nat. Sci.: Nanosci. Nanotech. 9, 025001
  (2018)]

- There have been many publications that extend QD in
  various directions taking into accounts real factors (2005)

Thank you 감사 합니다 !

and hope to see you again ! 또 보자