

Hot Topics in Physical Informatics

November 10-13, 2013

The Fourth Conference Room of Jixian Hotel, Hunan University, Changsha, China.

Program (**changes in red**)

Nov 10 (Sunday)

18:30 Opening Reception

Nov 11 (Monday)

8:30-9:00 Gathering/discussions (coffee/tea, soft drinks)

9:00-9:15 Opening Ceremonies

SESSION-1. Chair: Phil Hemmer

9:15-10:00 M. Suhail Zubairy (TAMU): Protocol for counterfactual optical communication (I)

10:00-10:45 Eleni Diamanti (CNRS - Télécom ParisTech): Implementation of quantum cryptographic protocols using practical photonic systems (I)

10:45-11:05 Refreshment discussions (coffee/tea, soft drinks)

SESSION-2. Chair: Vadim Makarov

11:05-11:30 Renato Renner (ETH): Quantum cryptography with local Bell tests (R)

11:30-11:55 Daniela Frauchiger (ETH): A Practical Approach to True Quantum Randomness Generation (R)

11:55-12:20 Zhengqiang Yin (U. Sci. Tech. CN): Measurement-device-independent quantum key distribution with uncharacterized qubit sources (R)

12:20-13:45 Lunch (provided)

SESSION-3. Chair: Renato Renner

13:45-14:10 Yuxiang Yang (Tsinghua): Reliable quantum replication at the Heisenberg limit (R)

14:10-14:55 Robert Alicki (Gdansk): Stability versus reversibility in information processing (I)

14:55-15:40 Vadim Makarov (Waterloo): Hacking of quantum cryptography (I)

15:40-16:00 Refreshment discussions (coffee/tea, soft drinks)

SESSION-4. Chair: Suhail Zubairy

- 16:00-16:45 Horace Yuen (Northwestern): Conditional and unconditional quantum security (I)
- 16:45-17:00 Yessica Saez (TAMU): Bit errors in the Kirchhoff-law-Johnson-noise secure key exchange (R)
- 17:00-17:25 Laszlo Kish (TAMU): Facts, myths and fights about the KLJN classical physical key exchanger (R)

17:25-18:00 Refreshment discussions (coffee/tea, soft drinks, snack)

18:00-19:30 Debate about the unconditional security of quantum key distribution

- *Can a perfectly secure key be generated in QKD and under what security measure?*
- *Can practical implementations of QKD ever be made as secure as predicted by the security proofs?*

Pro-Team: Eleni Diamanti, Renato Renner

Con-Team: Vadim Makarov, Horace Yuen

Moderator: Giacomo Mauro D'Ariano (Pavia)

Nov 12 (Tuesday)

8:45-9:00 Gathering/discussions (coffee/tea, soft drinks)

SESSION-5. Chair: Derek Abbott

- 9:00-9:30 Janusz Smulko (Univ. Gdansk): Performance analysis of the "intelligent" Kirchhoff-law-Johnson-noise secure key exchange (I)
- 9:30-10:10 Robert Mingesz (Univ. Szeged): Experimental study of the Kirchhoff-Law-Johnson-Noise secure key exchange (I)
- 10:10-10:45 James M. Chappell (Adelaide): Is unconditionally secure classical communication without a public key possible? (I)

10:45-11:05 Refreshment discussions (coffee/tea, soft drinks)

SESSION-6. Chair: Neal Anderson

- 11:05-11:30 Shan Gao (Chinese Acad. Sci.): On the possibility of nonlinear quantum dynamics and superluminal communication (R)
- 11:30-11:55 Lachlan J. Gunn (Adelaide): Physical-layer encryption on the public internet: a stochastic approach to the Kish-Sethuraman cipher (R)

12:00-13:30 Lunch (provided)

13:30-13:45 Refreshment discussions (coffee/tea, soft drinks)

SESSION-7. Chair: Michel Dyakonov

13:45-14:30 Renato Renner (ETH): Landauer's Principle revisited (I)

14:30-15:15 Neal Anderson (Amherst): Irreversible Information Loss: Fundamental Notions and Physical Costs (I)

15:15-15:35 Refreshment discussions (coffee/tea, soft drinks)

SESSION-8. Chair: Horace Yuen

15:35-16:20 Wolfgang Porod (Univ. Notre Dame): Physical and Logical Reversibility in Computation (I)

16:20-16:50 John D. Norton (Pittsburgh): A No Go Result for the Thermodynamics of Computation (I)

16:50-17:20 Laszlo B. Kish (TAMU): Demons: Maxwell demon; Szilard engine; and Landauer's erasure-dissipation (I)

17:20-18:00 Refreshment discussions (coffee/tea, soft drinks, snack)

18:00-19:30 Debate on reversible computing and the validity of Landauer's principle

- *Are reversible computers possible or they do violate thermodynamics?*
- *Are non-reversible (dissipative) Brownian computers possible and, if yes, do they dissipate more heat than regular computers?*
- *Does (non-secure) erasure of memories dissipate more heat, or the writing of the same amount of information?*
- *Is Landauer's principle valid; or the same is true for writing the information; or it is simply invalid?*

Pro Team: Neal Anderson, Renato Renner

Pro for logically-reversible-but-dissipative-Brownian computers, Con for the Rest: Ferdinand Peper (NICT)

Con Team: Robert Alicki, Laszlo B. Kish, Wolfgang Porod

Moderator: Dave Ferry/Alexander Kirk (ASU)

Nov 13 (Wednesday)

8:45-9:00 Refreshment discussions (coffee/tea, soft drinks)

SESSION-9. Chair: Robert Alicki

9:00-9:45 Phil Hemmer (TAMU): Biological spinoffs of room-temperature diamond-based quantum computers (I)

9:45-10:30 Michel Dyakonov (Montpellier): Prospects for Quantum Computing: Extremely Doubtful (I)

10:30-10:50 Refreshment discussions (coffee/tea, soft drinks)

SESSION-10. Chair: Ferdinand Peper

10:50-11:35 Giacomo Mauro D'Ariano: Quantum field theory as emergent from pure processing of quantum information (I)

11:35-12:05 Derek Abbott: Allion mixtures: where random digits obey thermodynamic principles (I)

12:05-12:40 Makoto Naruse (NICT): Near-field nanophotonics for computing and security (I)

12:40-14:00 Lunch (provided)

SESSION-11. Chair: Janusz Smulko

14:00-14:45 Ferdinand Peper (NICT): On token-based fluctuation-driven circuits and their energy consumption (I)

14:35-15:05 Dave Ferry/Alexander Kirk (ASU): Are there quantum jumps? (I)

15:05-15:25 Refreshment discussions (coffee/tea, soft drinks)

SESSION-12. Chair: Makoto Naruse

15:25-15:50 Fabing Duan (Adelaide): Noise-enhanced transmission efficacy of aperiodic signals in nonlinear systems (R)

15:50-16:25 He Wen: Noise-based logic: Why noise for deterministic logic? (R)

16:25-16:40 Laszlo Kish: Why is neural spike transfer stochastic? String verification in the brain (R)

16:40-17:15 Refreshment discussions (coffee/tea, soft drinks, snack)

17:15-18:45 Debate Session about the future of quantum computing.

-Will general-purpose quantum computing be feasible?

-If special-purpose quantum computing (new computer for each task) will be used, what purpose and what limitations (accuracy, dissipation, etc)?

-Team-independent question: Is D-Wave's computer an analog computer with quantum devices and classical bits, a quantum computer with qubits, or else?

Pro Team: Phil Hemmer, Suhail Zubairy

Partial-Pro/Con: Derek Abbott, Dave Ferry/Alexander Kirk

Con Team: Michel Dyakonov, Laszlo Kish

Moderator: Wolfgang Porod (Univ. Notre Dame)

18:45 Farewell