Title: Interactive Quantum Information Theory - Dave Touchette

Date: Nov 26, 2014 04:00 PM

URL: http://pirsa.org/14110183

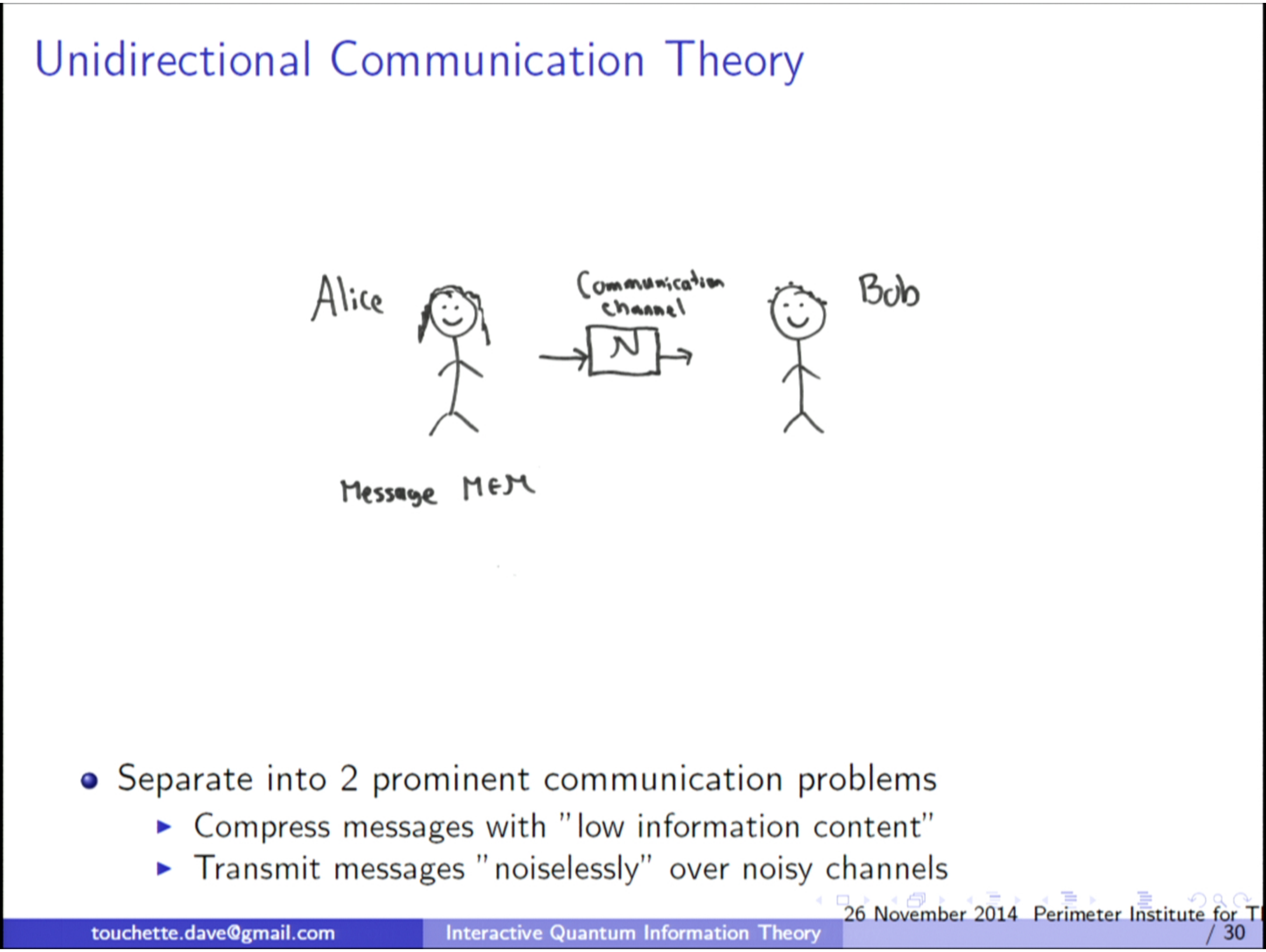
Abstract: <p>In unidirectional communication theory, two of the most prominent problems are those of compressing a source of information and of transmitting data noiselessly over a noisy channel. In 1948, Shannon introduced information theory as a tool to address both of these problems. Since then, information theory has flourished into an important field of its own. It has also been successfully extended to the quantum setting, where it has also served to address questions about quantum source compression and transmission of classical and quantum data over noisy quantum channels.</p>

<p>However, in interactive communication theory, more specifically communication complexity, it is much more recently that tools from information theory have been successfully applied. Indeed, the interactive nature of communication protocols in this setting imposes new constraints and tools specific to this setting need to be developed, both for the interactive analogue of source compression and that of coding for noisy channels. The exciting field of classical interactive information theory has been very active in recent years.</p>

<p>We discuss recent works for its quantum counterpart. In particular, we discuss joint work showing that a constant factor overhead is sufficient for robustly implementing interactive quantum communication over noisy channels [1]. We also discuss work introducing a new notion of quantum information complexity that exactly captures the amortized cost per copy for implementing many copies of a communication task in parallel, such that compressing to this information complexity leads to a bounded-round direct sum theorem [2].</p>

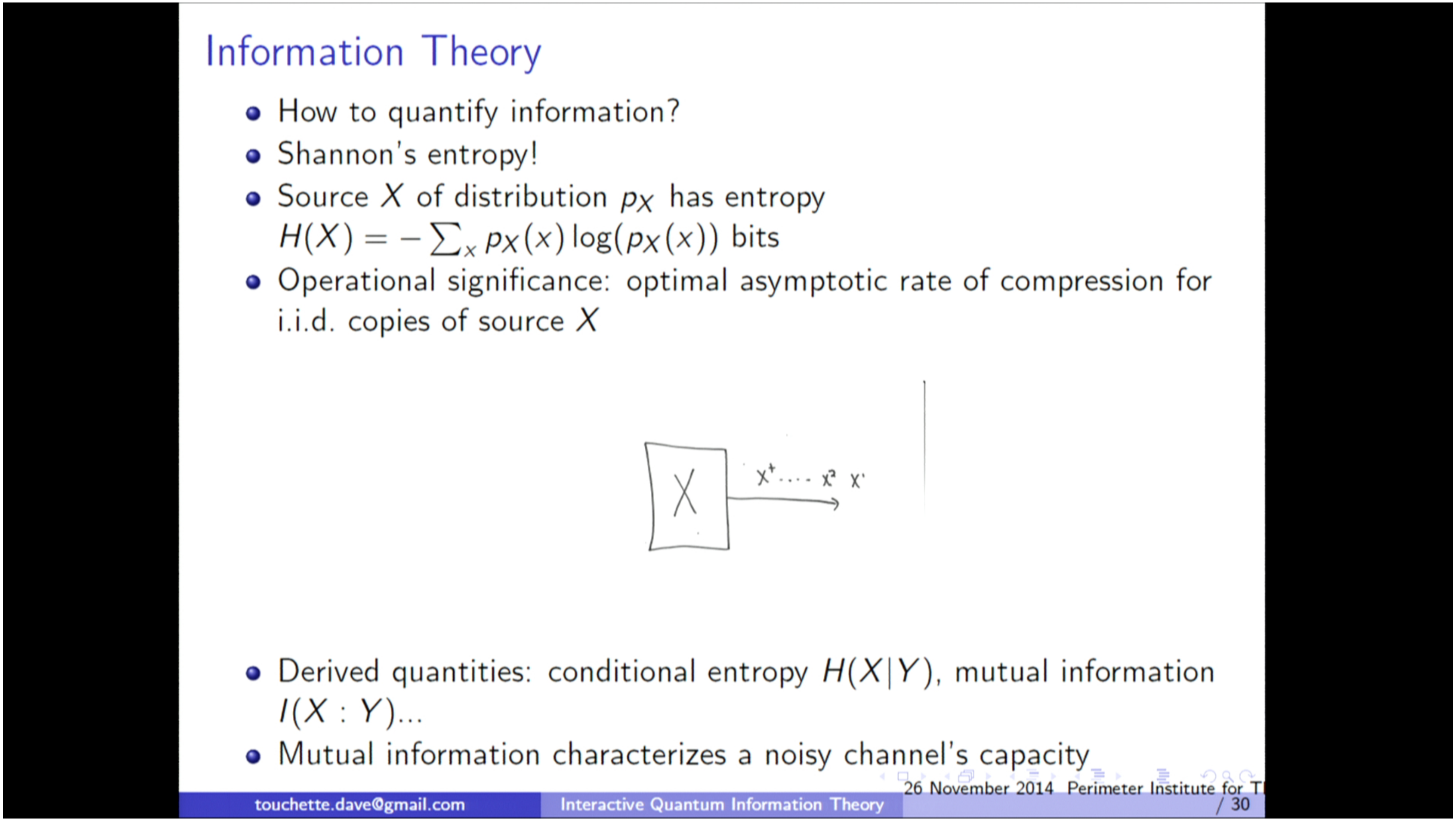
<p>For both of these, we further discuss many interesting potential research directions that follow.</p>

<p>[1] joint work with Gilles Brassard, Ashwin Nayak, Alain Tapp, Falk Unger, QIPâ€™14, FOCSâ€™14 [2] Merge of arXiv:1404.3733 and arXiv:1409.4391, to appear at QIPâ€™15</p>



Unidirectional Communication Theory

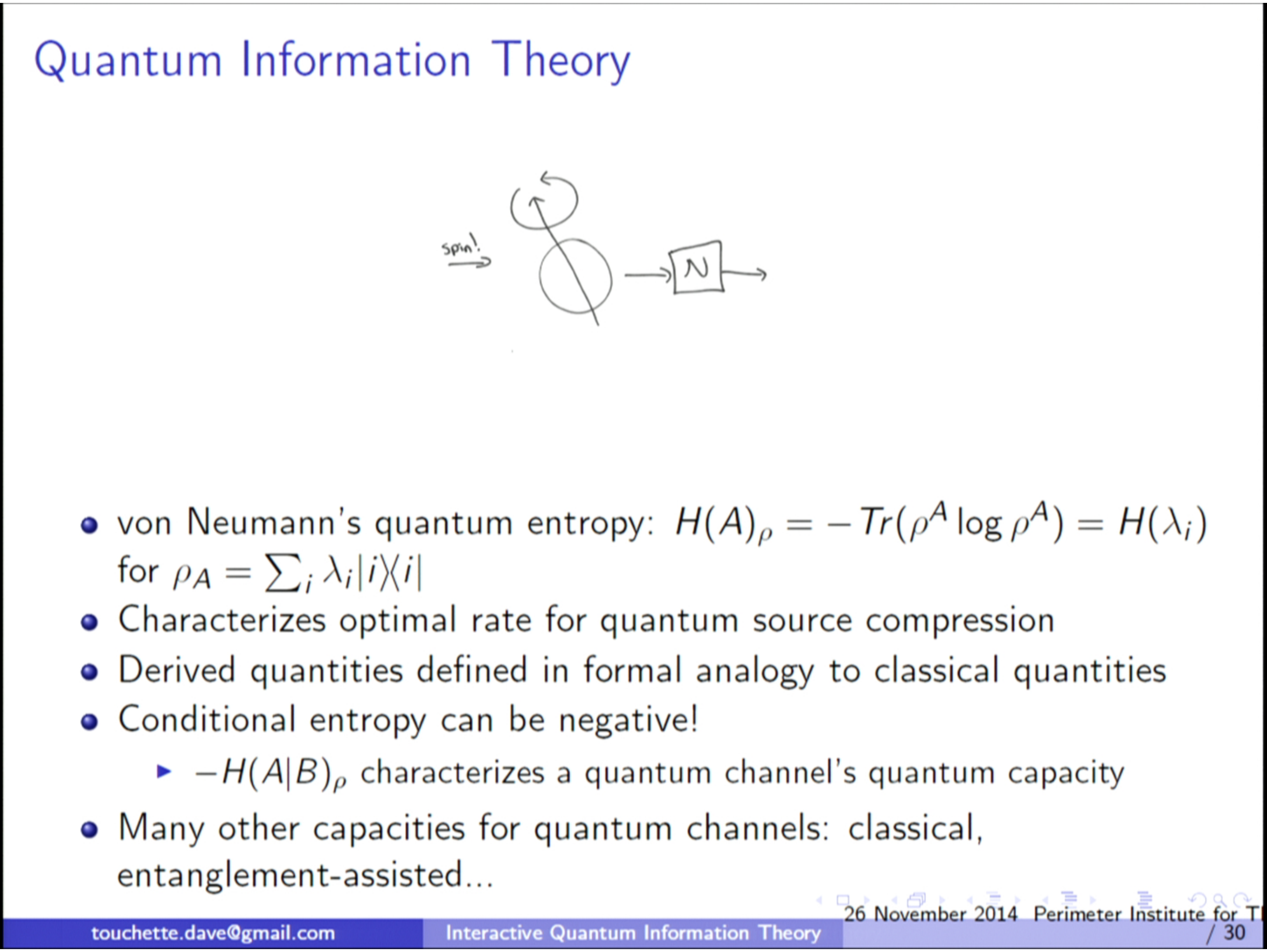
- Separate into 2 prominent communication problems
  - Compress messages with "low information content"
  - Transmit messages "noiselessly" over noisy channels



Information Theory

- How to quantify information?
- Shannon's entropy!
- Source X of distribution p_X has entropy $H(X) = -\sum_x p_X(x) \log(p_X(x))$ bits
- Operational significance: optimal asymptotic rate of compression for i.i.d. copies of source X

- Derived quantities: conditional entropy $H(X|Y)$, mutual information $I(X : Y)$...
- Mutual information characterizes a noisy channel's capacity

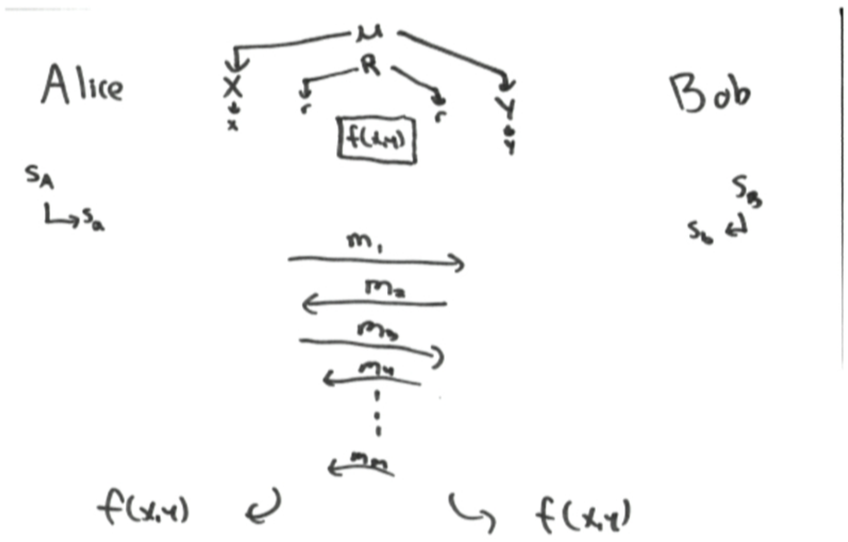


Quantum Information Theory

- von Neumann's quantum entropy: $H(A)_\rho = -Tr(\rho^A \log \rho^A) = H(\lambda_i)$ for $\rho_A = \sum_i \lambda_i |i\rangle\langle i|$
- Characterizes optimal rate for quantum source compression
- Derived quantities defined in formal analogy to classical quantities
- Conditional entropy can be negative!
  - $-H(A|B)_\rho$ characterizes a quantum channel's quantum capacity
- Many other capacities for quantum channels: classical, entanglement-assisted...

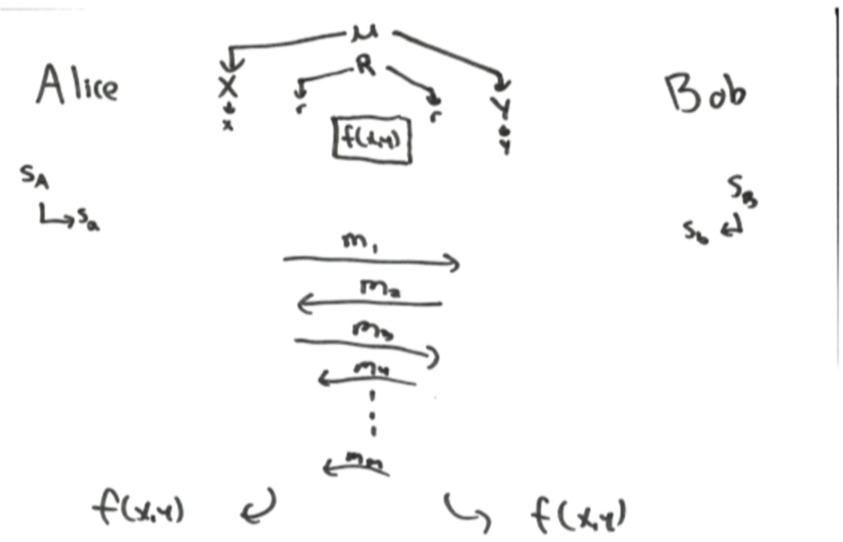
Interactive communication theory

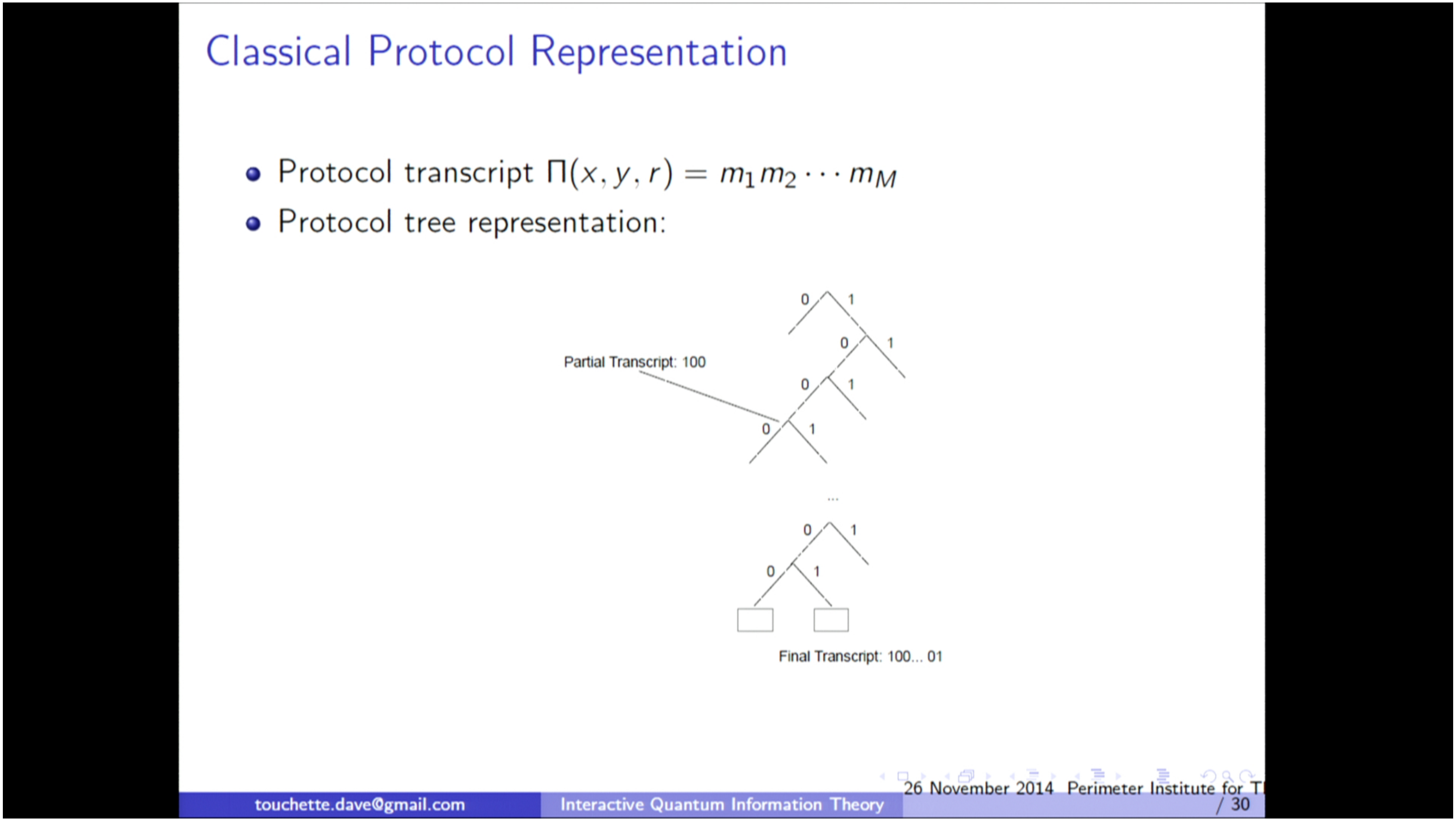
- Communication complexity of tasks, e.g. bipartite functions or relations



Interactive communication theory

- Communication complexity of tasks, e.g. bipartite functions or relations



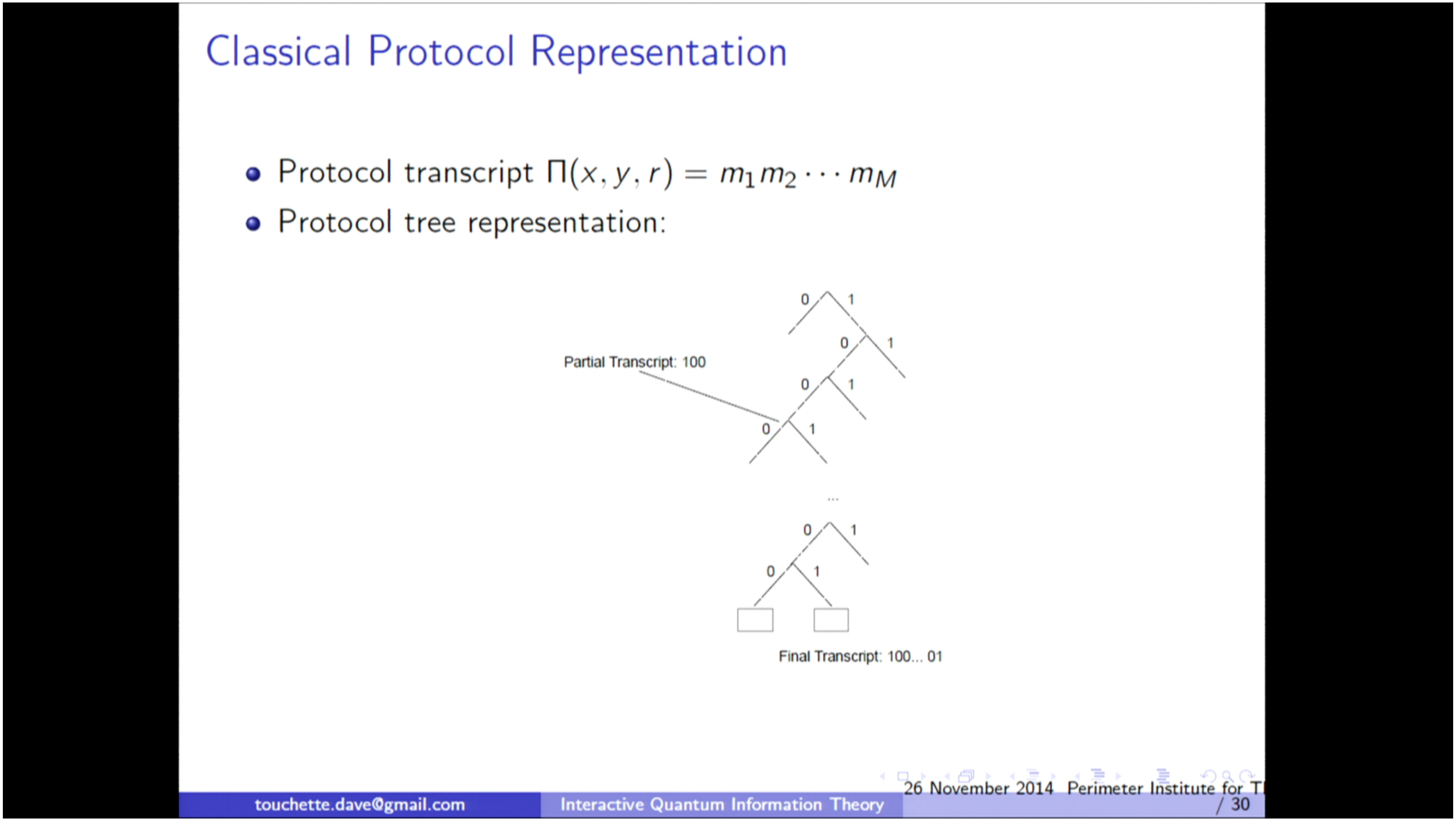


Classical Protocol Representation

- Protocol transcript $\Pi(x, y, r) = m_1 m_2 \cdots m_M$
- Protocol tree representation:

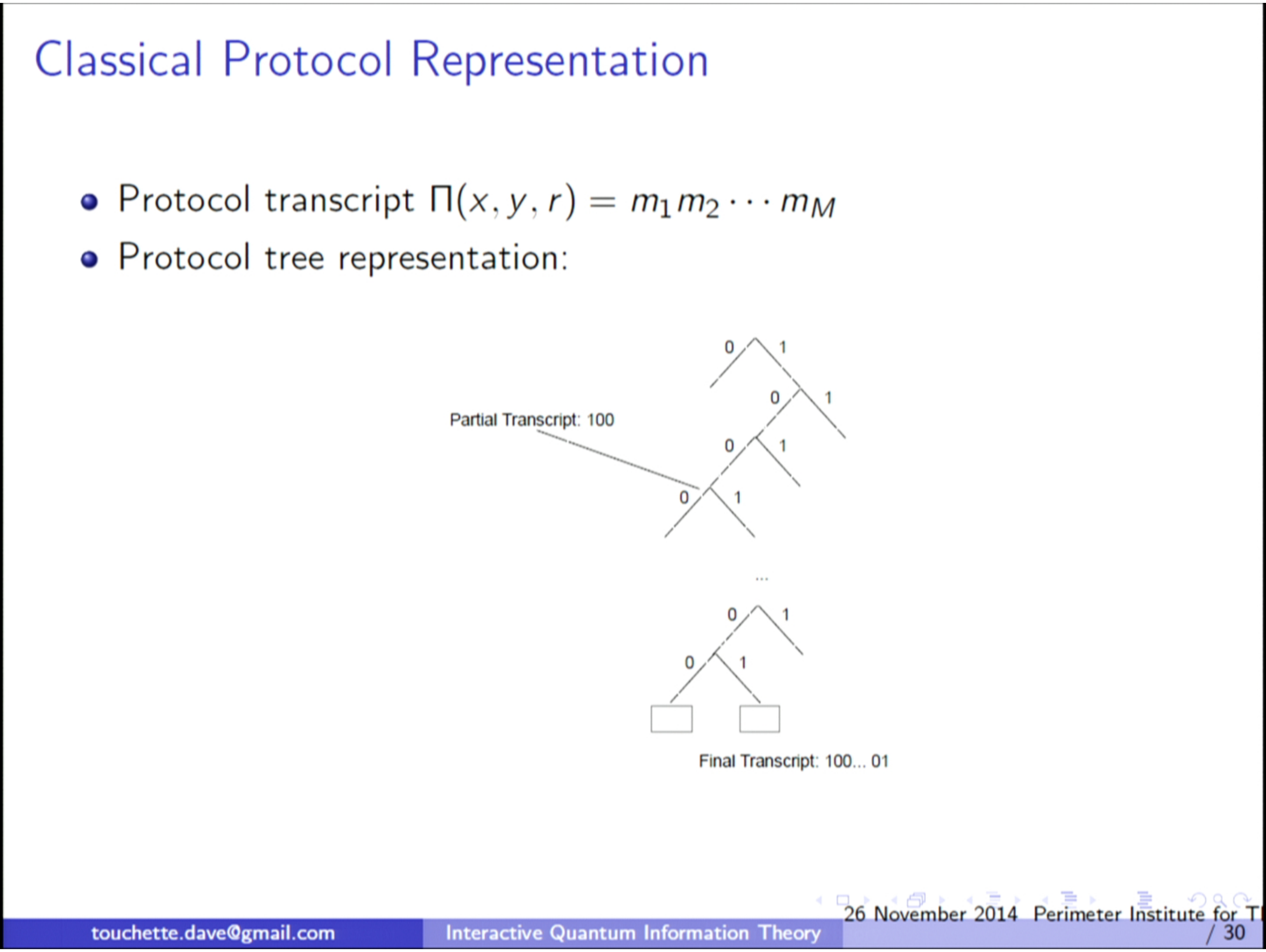
Partial Transcript: 100

Final Transcript: 100... 01



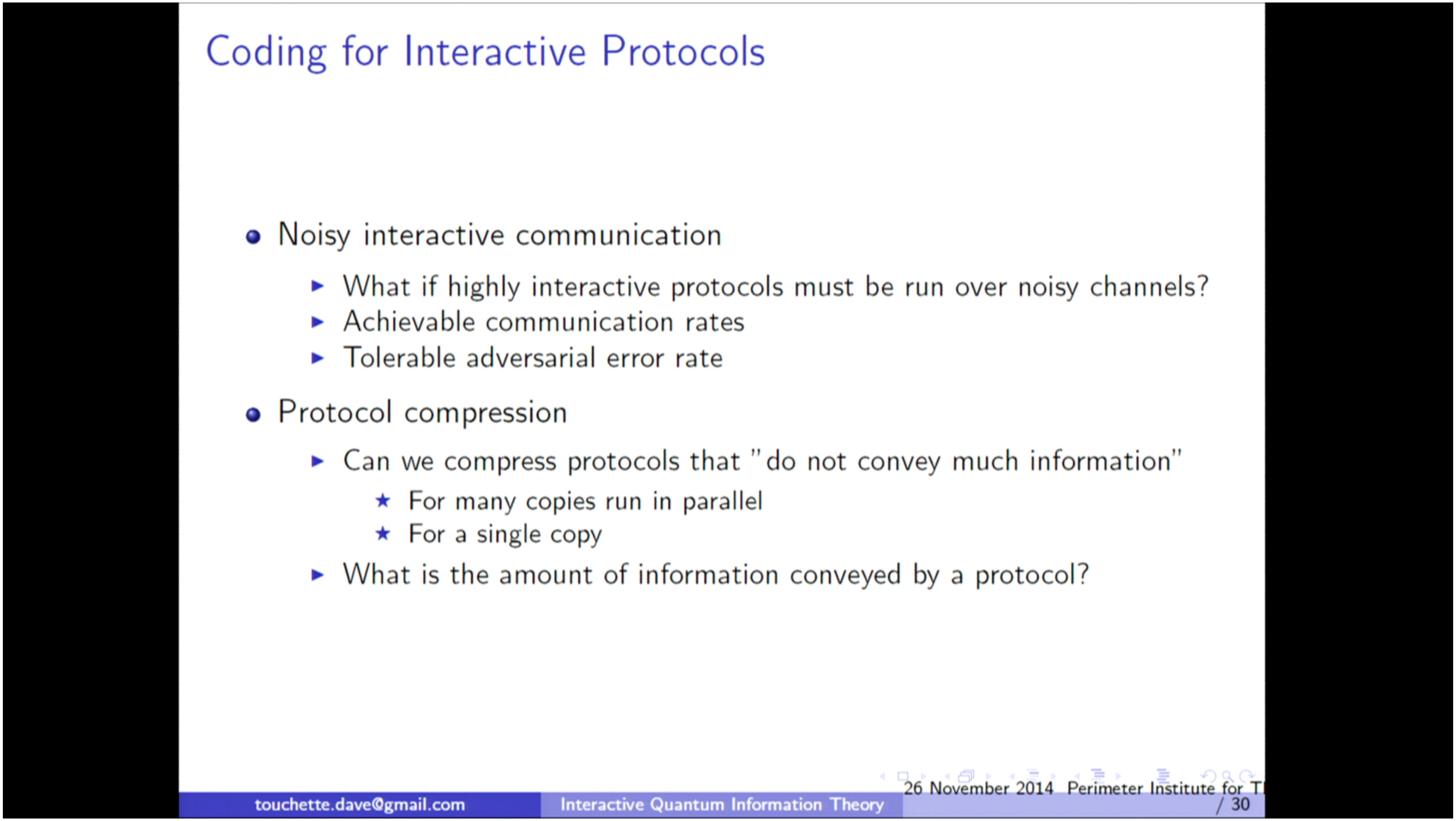
Classical Protocol Representation

- Protocol transcript $\Pi(x, y, r) = m_1 m_2 \cdots m_M$
- Protocol tree representation:



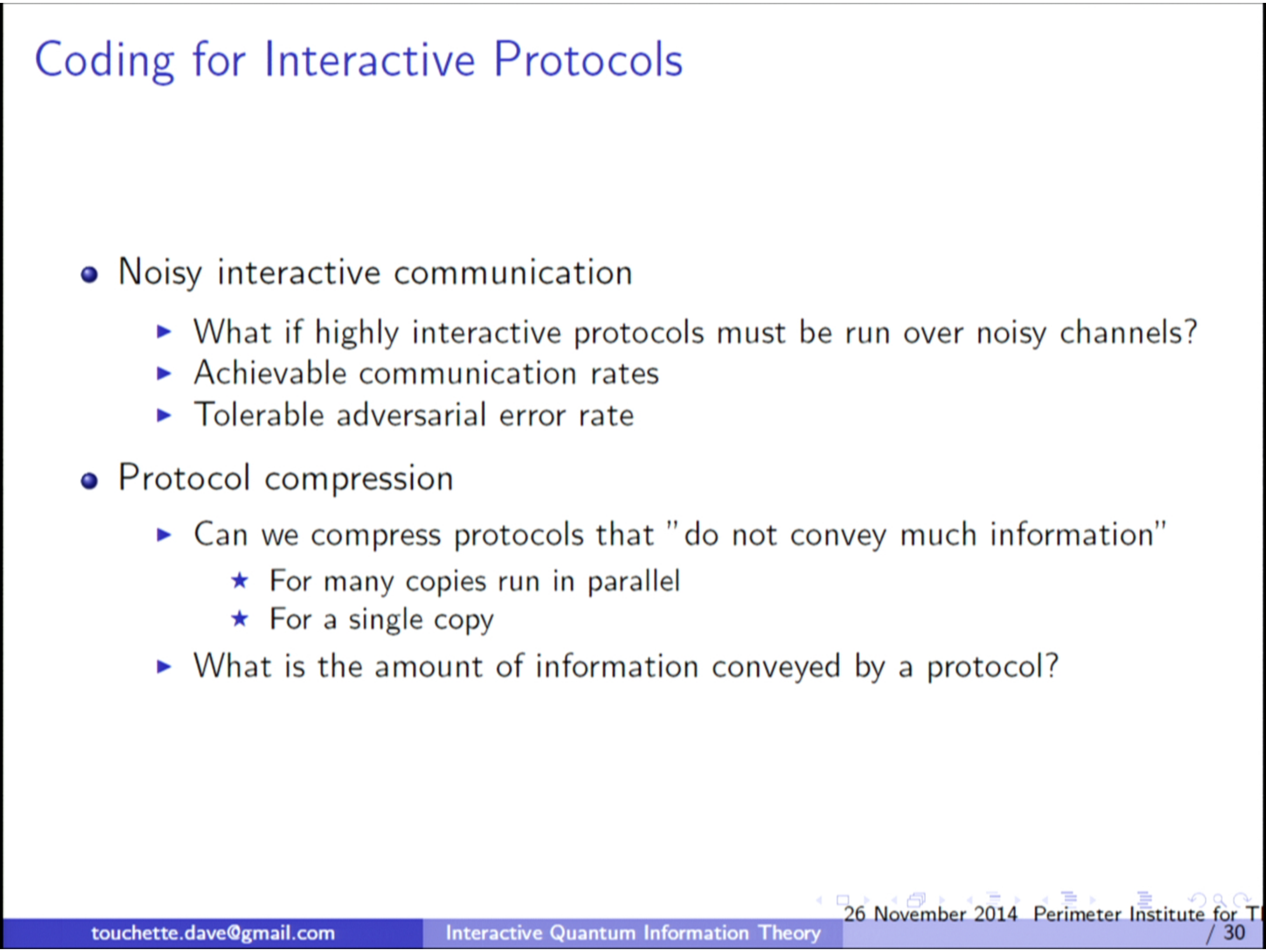
Classical Protocol Representation

- Protocol transcript $\Pi(x, y, r) = m_1 m_2 \cdots m_M$
- Protocol tree representation:



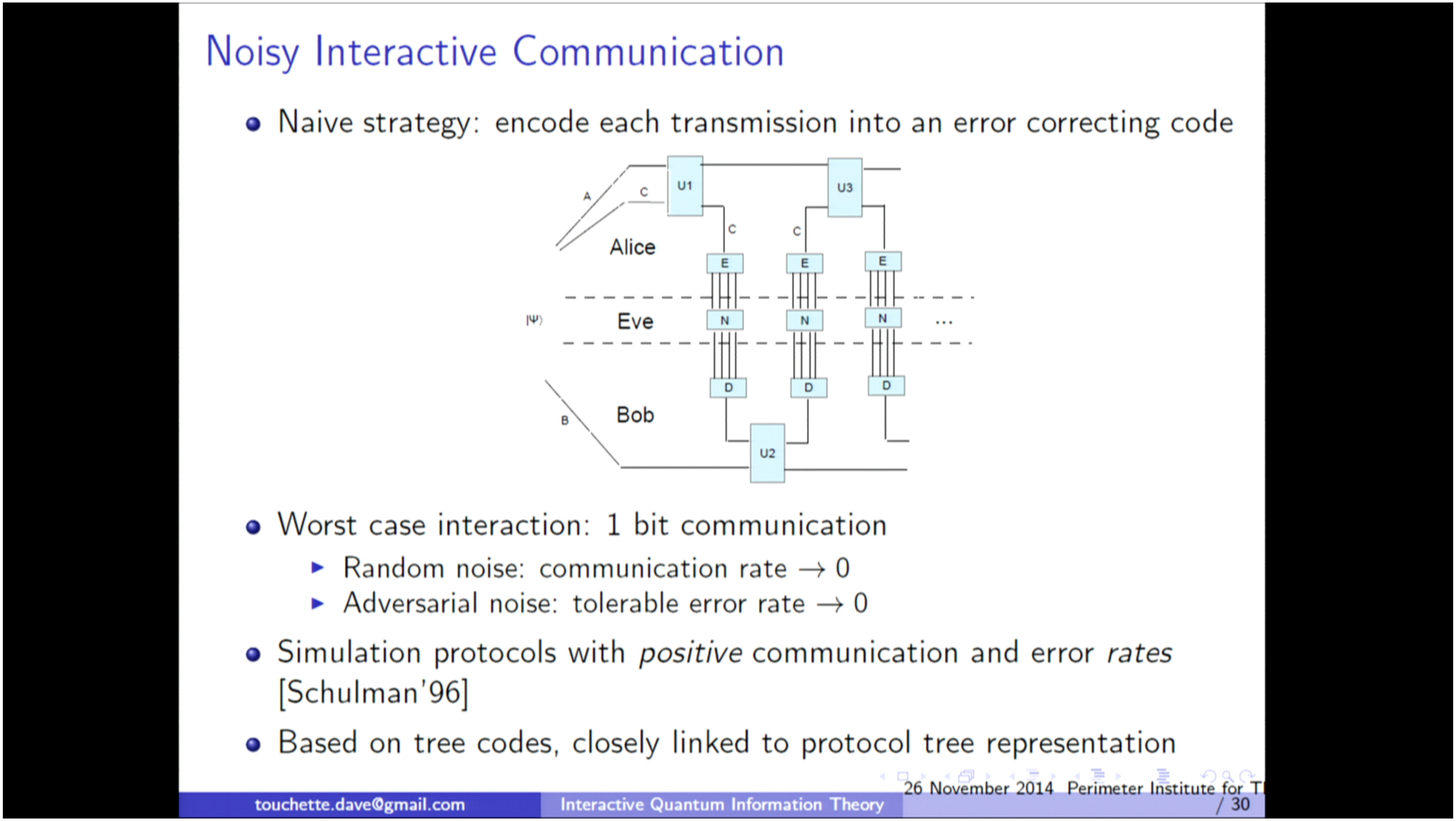
Coding for Interactive Protocols

- Noisy interactive communication
  - What if highly interactive protocols must be run over noisy channels?
  - Achievable communication rates
  - Tolerable adversarial error rate
- Protocol compression
  - Can we compress protocols that "do not convey much information"
    - ★ For many copies run in parallel
    - ★ For a single copy
  - What is the amount of information conveyed by a protocol?



Coding for Interactive Protocols

- Noisy interactive communication
  - What if highly interactive protocols must be run over noisy channels?
  - Achievable communication rates
  - Tolerable adversarial error rate
- Protocol compression
  - Can we compress protocols that "do not convey much information"
    - ★ For many copies run in parallel
    - ★ For a single copy
  - What is the amount of information conveyed by a protocol?



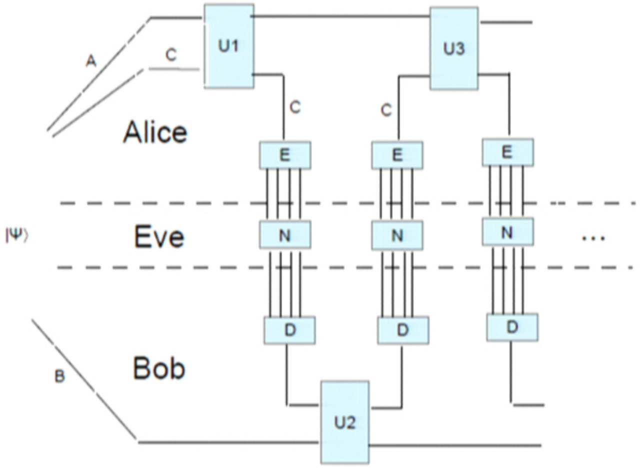
Noisy Interactive Communication

- Naive strategy: encode each transmission into an error correcting code

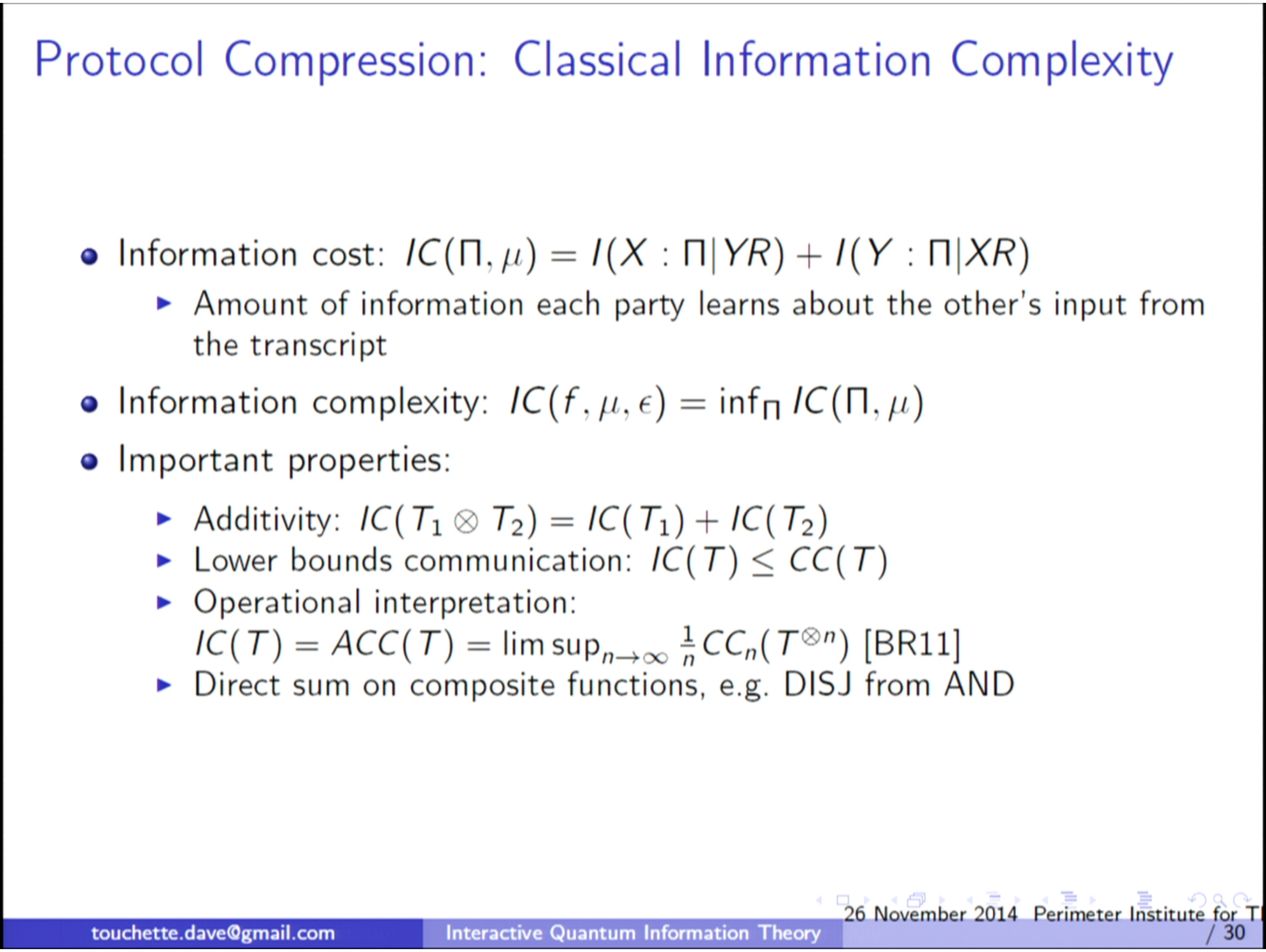
- Worst case interaction: 1 bit communication
  - Random noise: communication rate → 0
  - Adversarial noise: tolerable error rate → 0
- Simulation protocols with *positive* communication and error *rates* [Schulman'96]
- Based on tree codes, closely linked to protocol tree representation

Noisy Interactive Communication

- Naive strategy: encode each transmission into an error correcting code

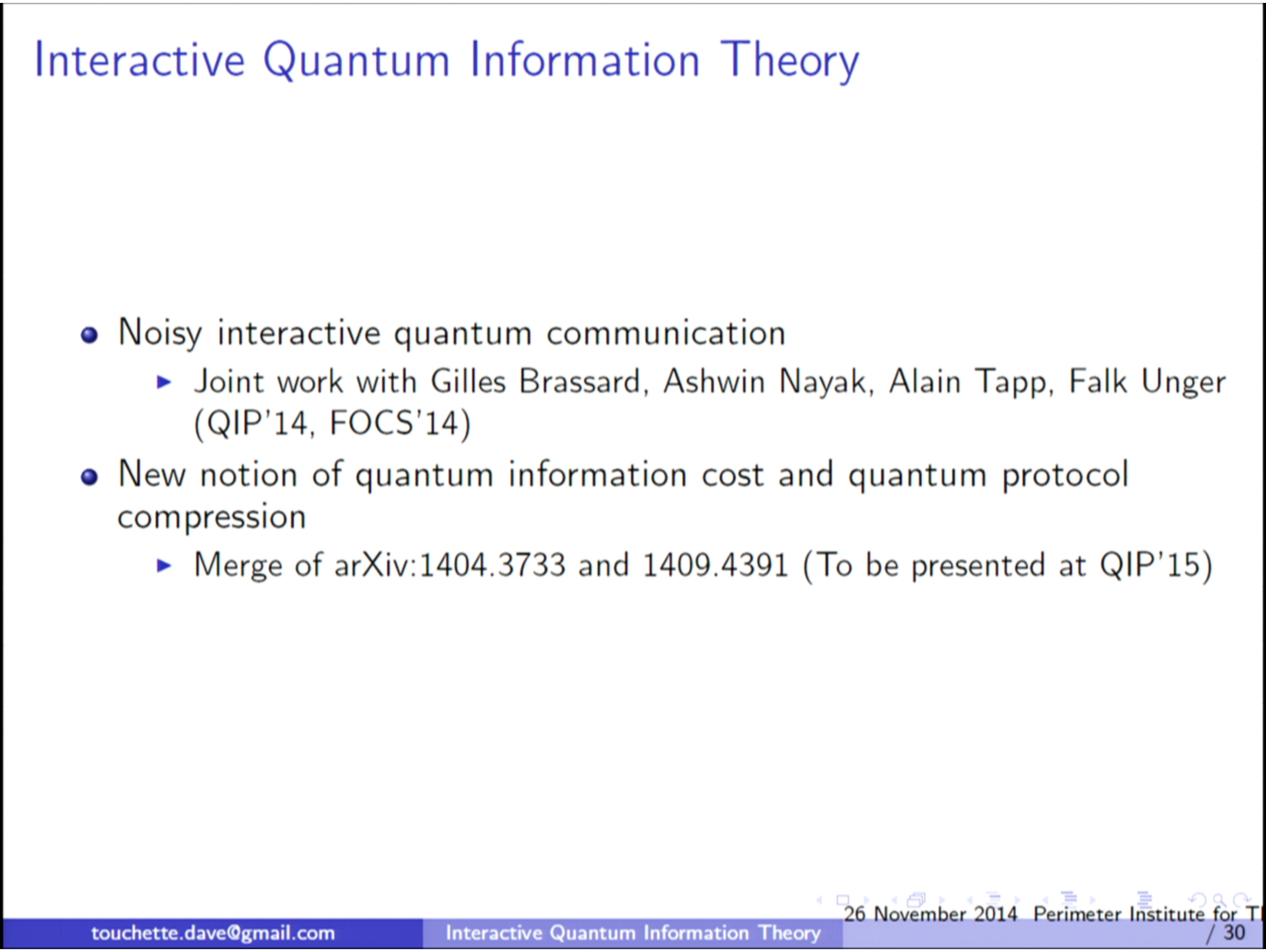


- Worst case interaction: 1 bit communication
  - Random noise: communication rate → 0
  - Adversarial noise: tolerable error rate → 0
- Simulation protocols with *positive* communication and error *rates* [Schulman'96]
- Based on tree codes, closely linked to protocol tree representation



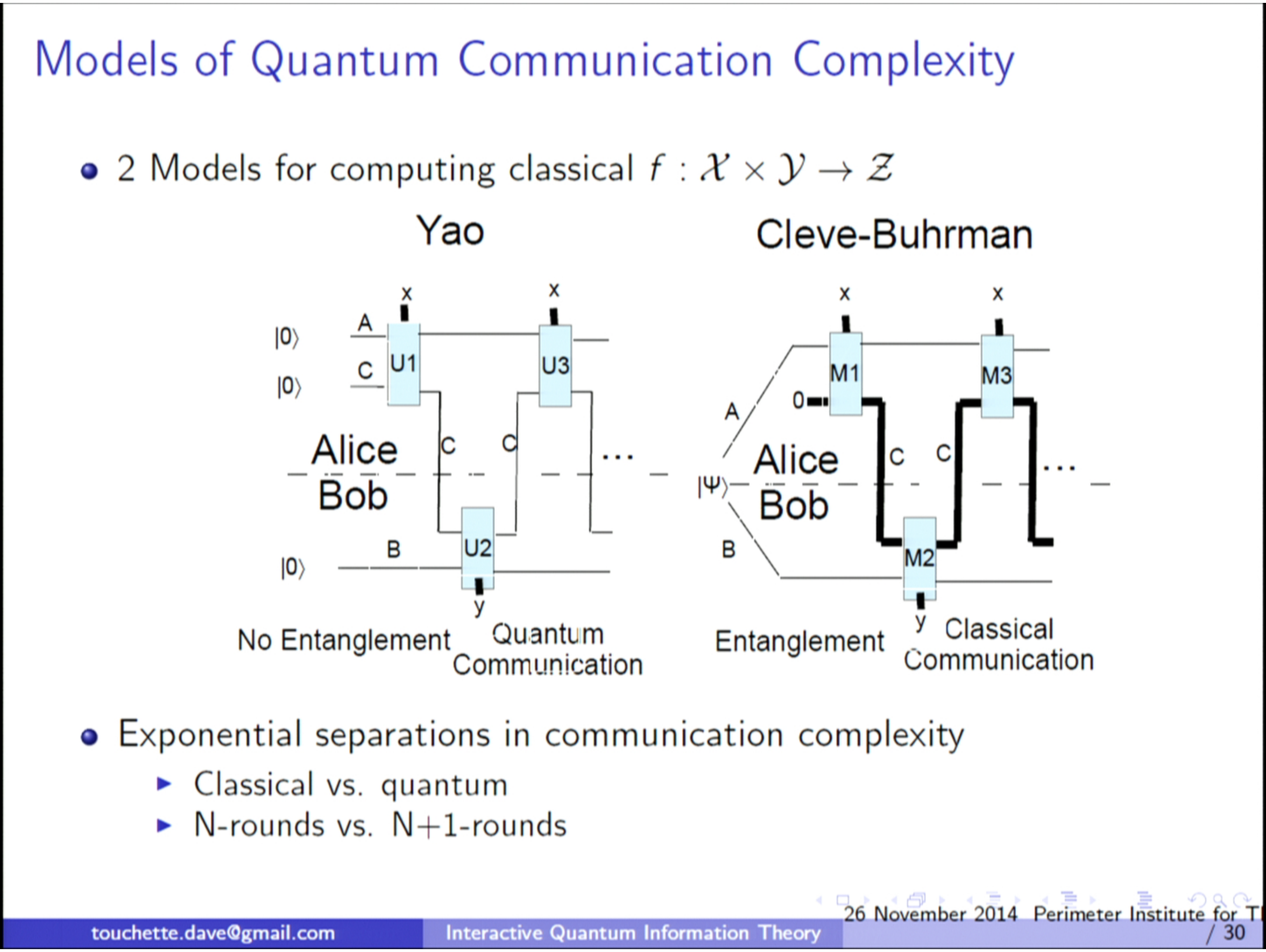
Protocol Compression: Classical Information Complexity

- Information cost: $IC(\Pi, \mu) = I(X : \Pi | YR) + I(Y : \Pi | XR)$
  - Amount of information each party learns about the other's input from the transcript
- Information complexity: $IC(f, \mu, \epsilon) = \inf_{\Pi} IC(\Pi, \mu)$
- Important properties:
  - Additivity: $IC(T_1 \otimes T_2) = IC(T_1) + IC(T_2)$
  - Lower bounds communication: $IC(T) \leq CC(T)$
  - Operational interpretation: $IC(T) = ACC(T) = \limsup_{n \to \infty} \frac{1}{n} CC_n(T^{\otimes n})$ [BR11]
  - Direct sum on composite functions, e.g. DISJ from AND



Interactive Quantum Information Theory

- Noisy interactive quantum communication
  - Joint work with Gilles Brassard, Ashwin Nayak, Alain Tapp, Falk Unger (QIP'14, FOCS'14)
- New notion of quantum information cost and quantum protocol compression
  - Merge of arXiv:1404.3733 and 1409.4391 (To be presented at QIP'15)



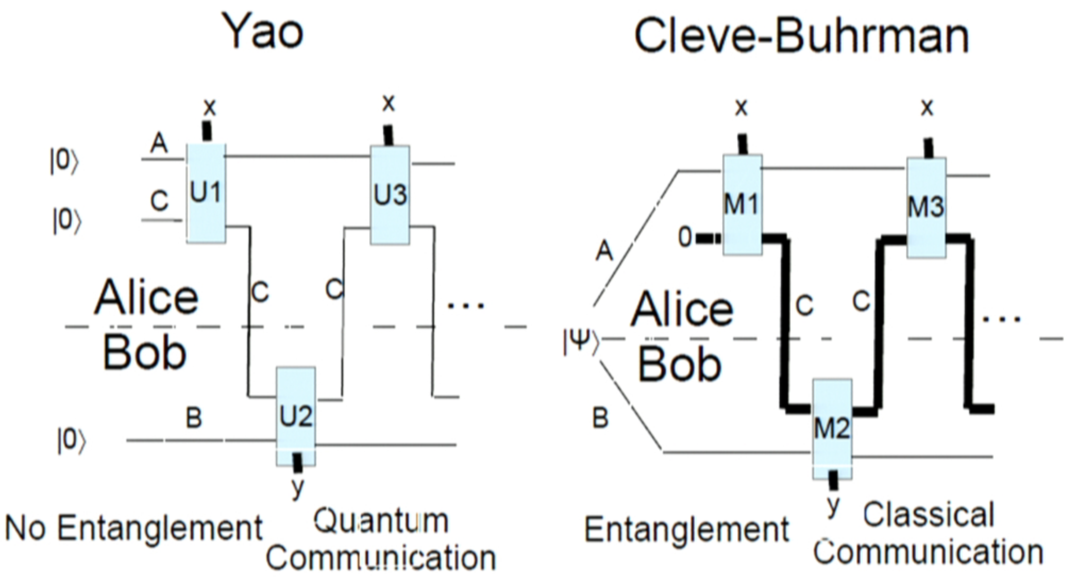
Models of Quantum Communication Complexity

- 2 Models for computing classical $f : \mathcal{X} \times \mathcal{Y} \to \mathcal{Z}$

- Exponential separations in communication complexity
  - Classical vs. quantum
  - N-rounds vs. N+1-rounds

Models of Quantum Communication Complexity

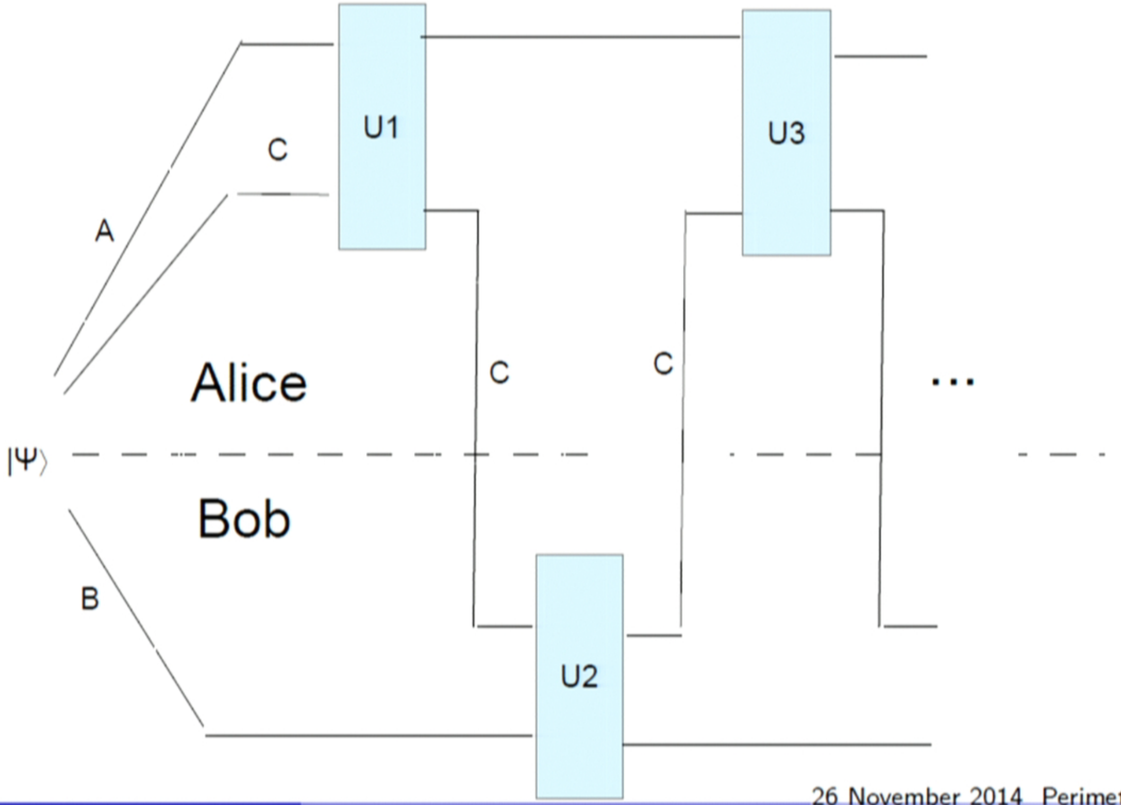
- 2 Models for computing classical $f : \mathcal{X} \times \mathcal{Y} \to \mathcal{Z}$

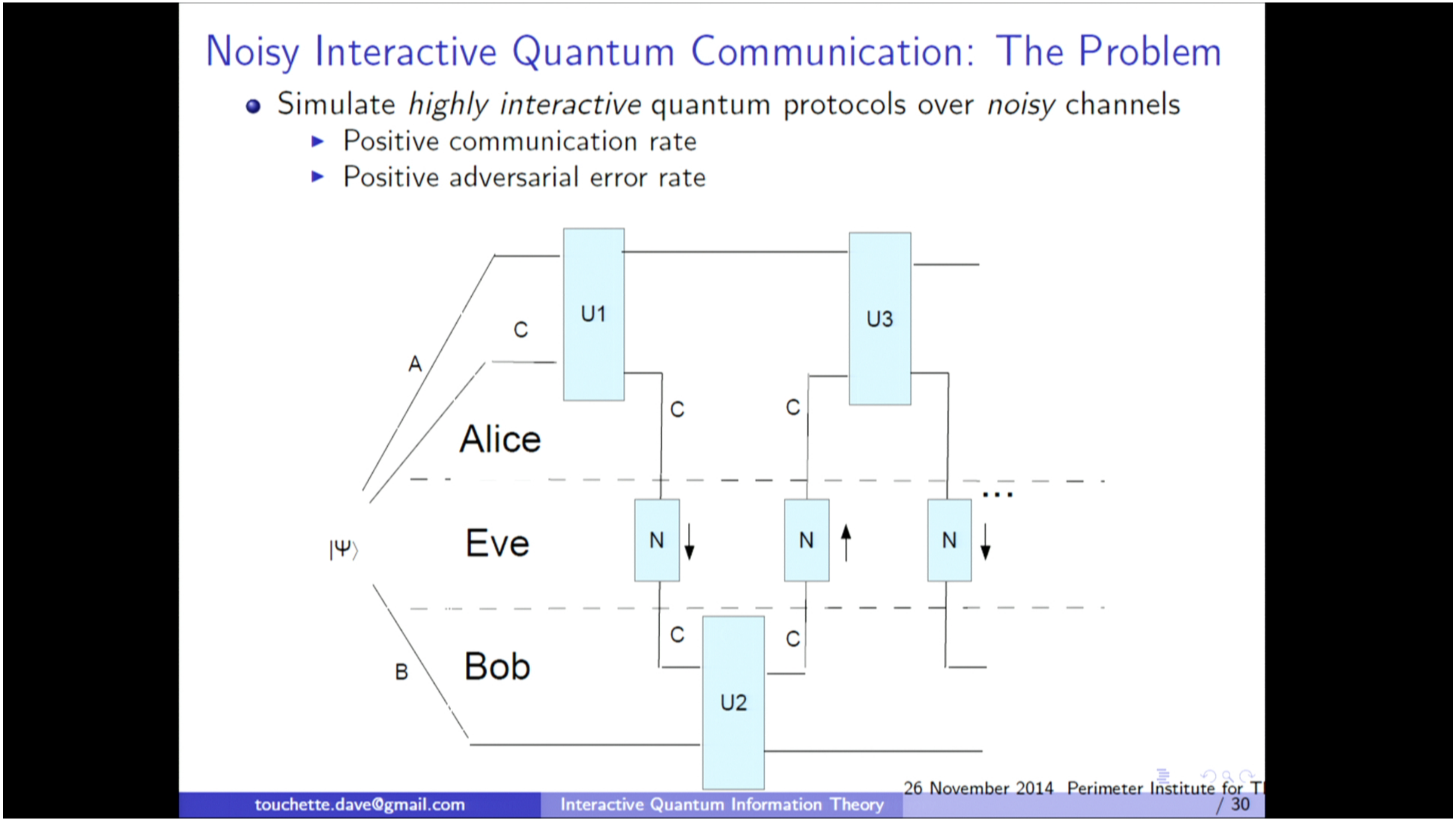


- Exponential separations in communication complexity
  - Classical vs. quantum
  - N-rounds vs. N+1-rounds

Noisy Interactive Quantum Communication: The Problem

- Simulate *highly interactive* quantum protocols over *noisy* channels
  - Positive communication rate
  - Positive adversarial error rate



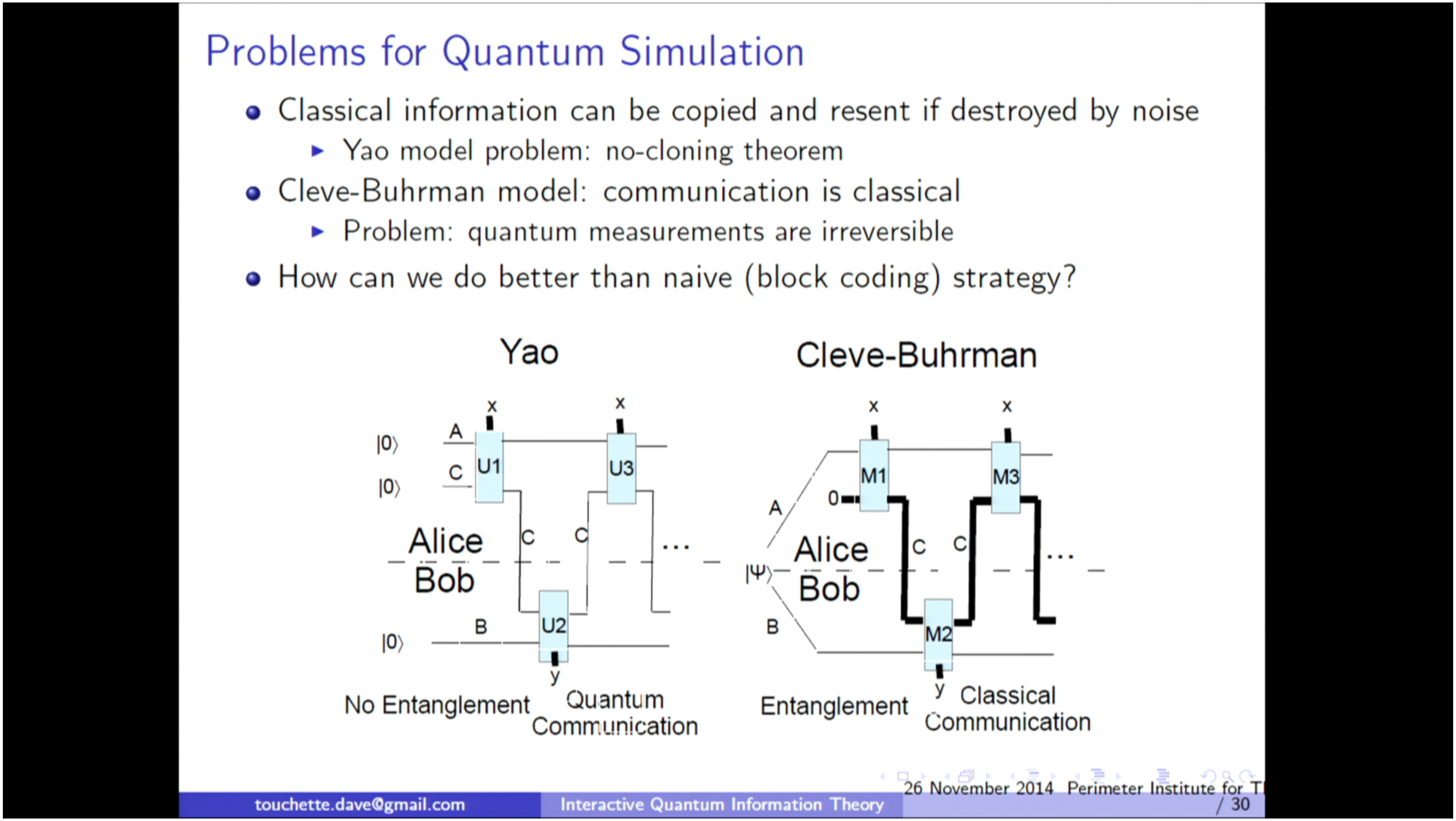


Noisy Interactive Quantum Communication: The Problem

- Simulate *highly interactive* quantum protocols over *noisy* channels
  - Positive communication rate
  - Positive adversarial error rate

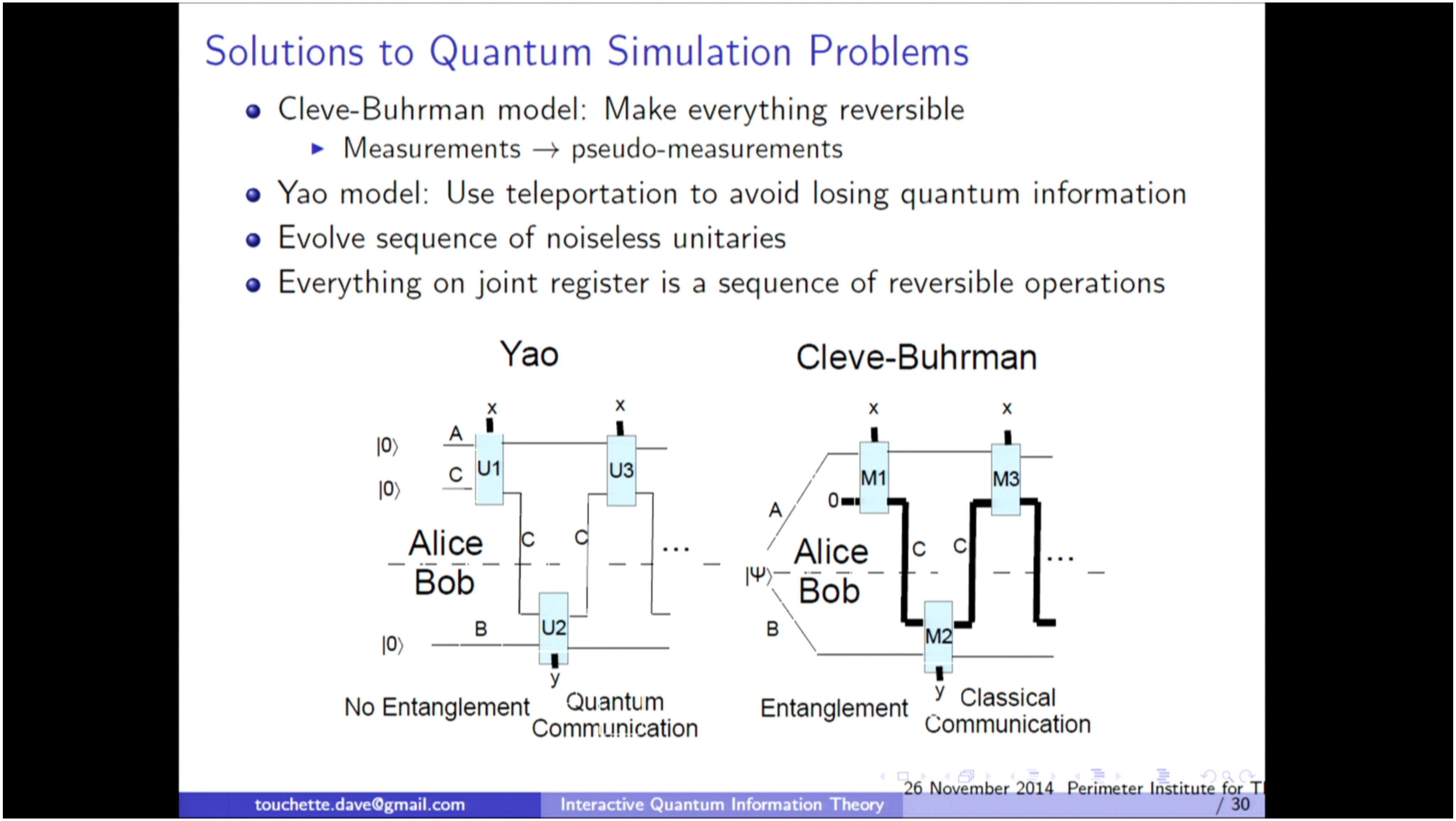
touchette.dave@gmail.com Interactive Quantum Information Theory 26 November 2014 Perimeter Institute for T

/ 30



Problems for Quantum Simulation

- Classical information can be copied and resent if destroyed by noise
  - Yao model problem: no-cloning theorem
- Cleve-Buhrman model: communication is classical
  - Problem: quantum measurements are irreversible
- How can we do better than naive (block coding) strategy?

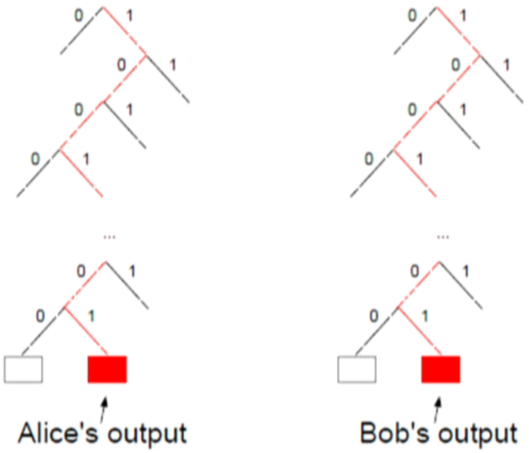


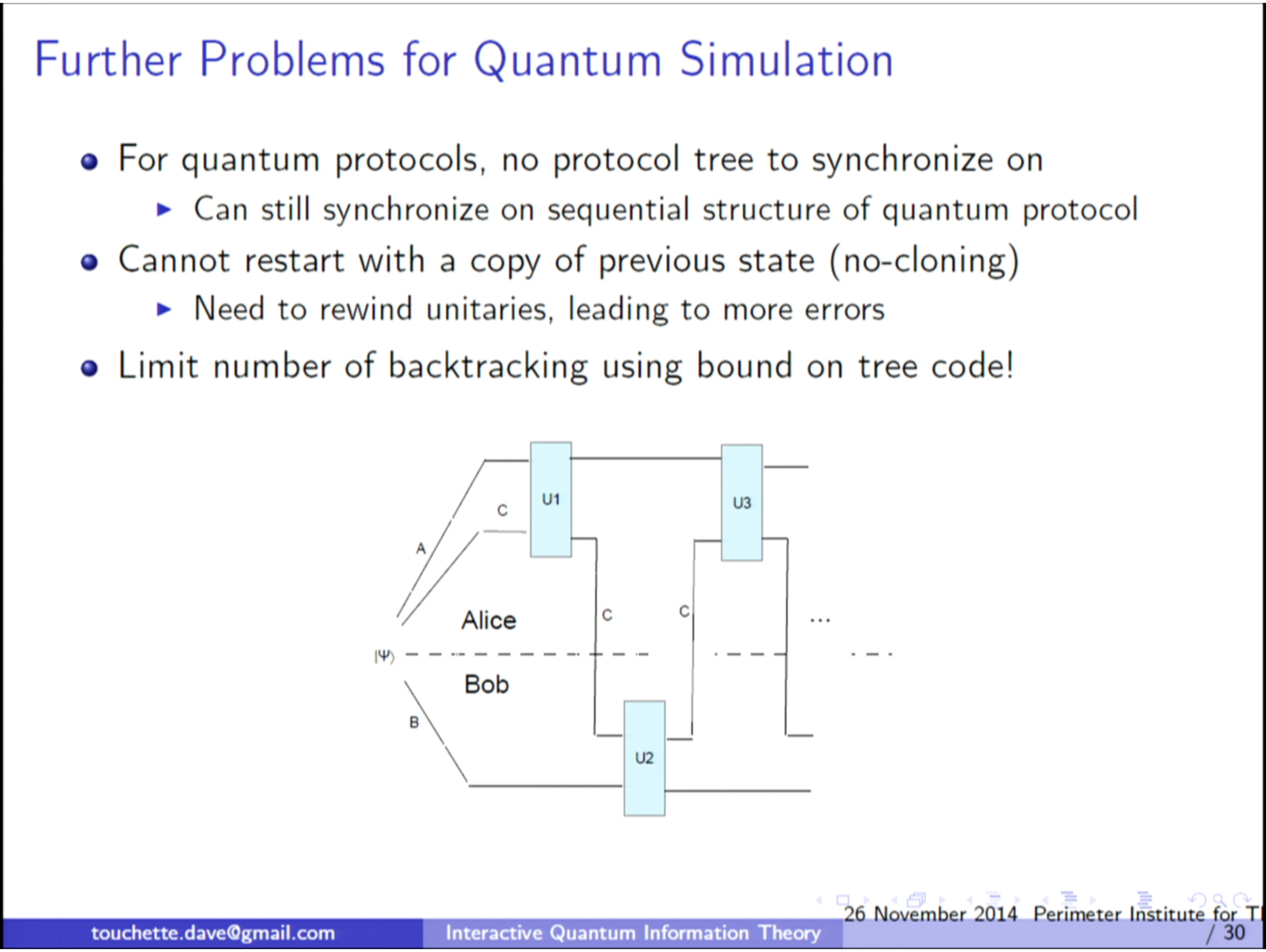
Solutions to Quantum Simulation Problems

- Cleve-Buhrman model: Make everything reversible
  - Measurements → pseudo-measurements
- Yao model: Use teleportation to avoid losing quantum information
- Evolve sequence of noiseless unitaries
- Everything on joint register is a sequence of reversible operations

Quantum Simulation Protocol

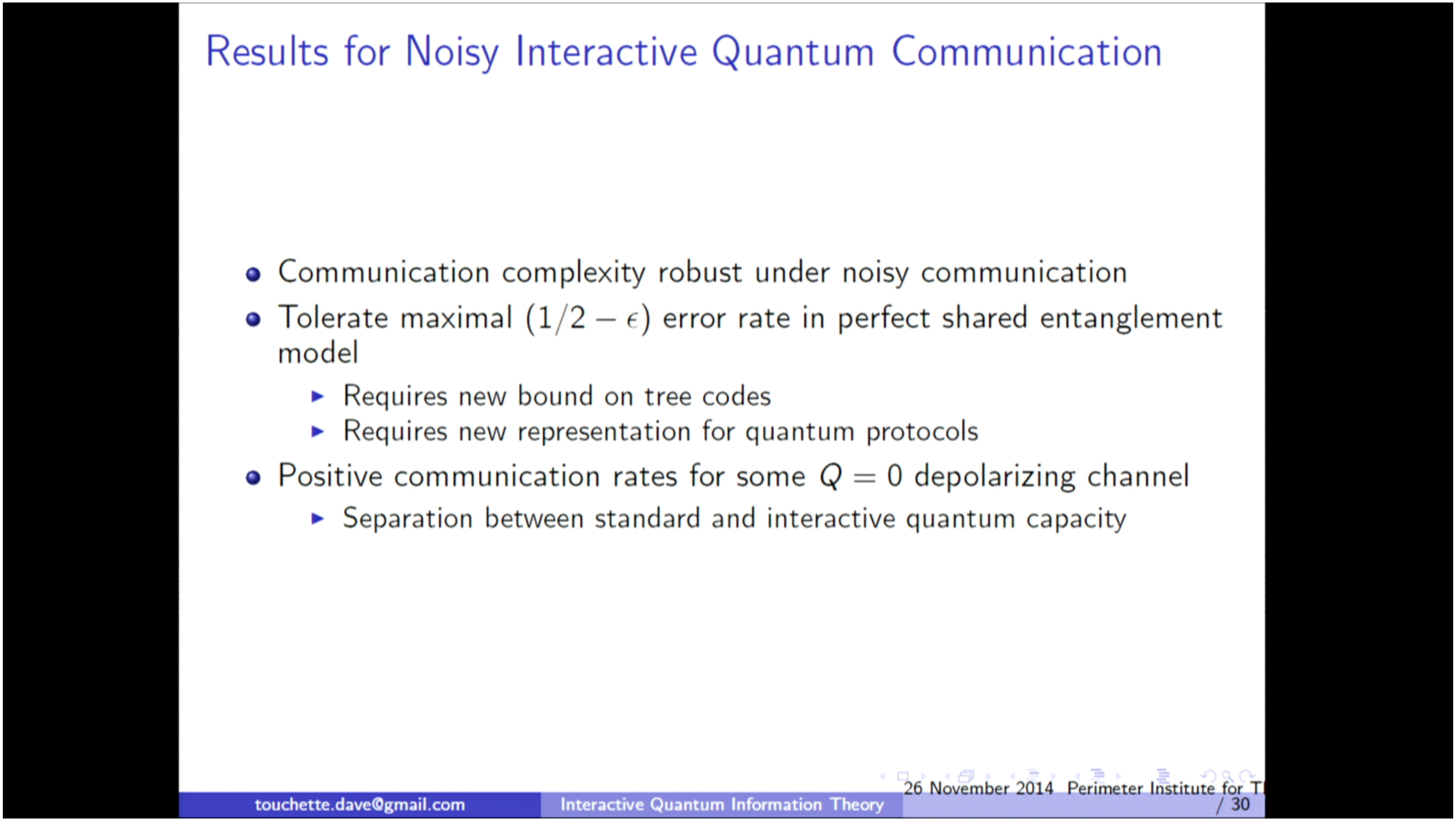
- Yao: To distribute EPR pairs, use tools from quantum coding theory
- For interaction, use tools from classical interactive coding
- Can we use classical simulation protocols: No!
  - Classical goal: Alice and Bob agree on transcript
  - Here: Contains mostly random teleportation outcomes





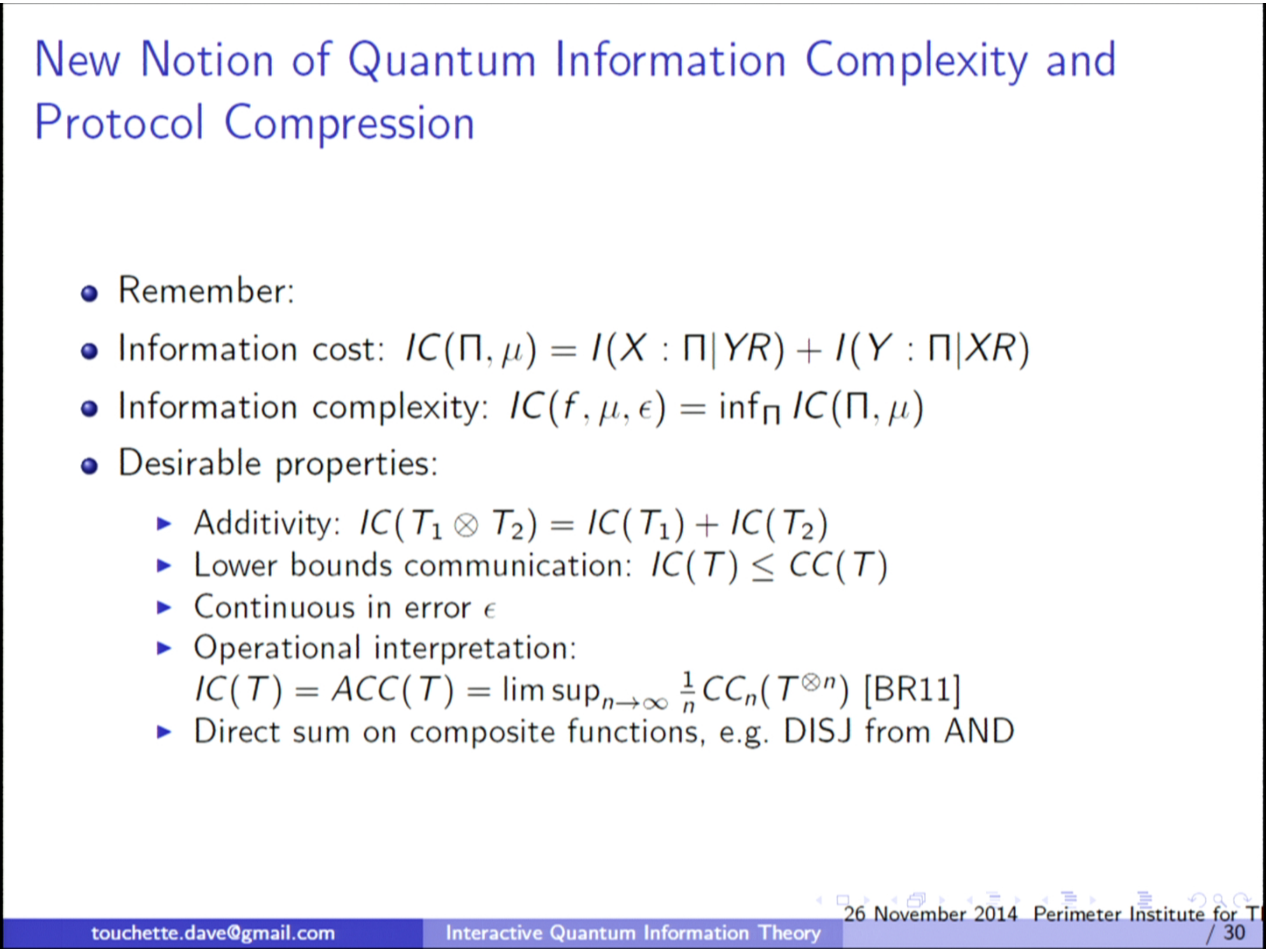
Further Problems for Quantum Simulation

- For quantum protocols, no protocol tree to synchronize on
  - Can still synchronize on sequential structure of quantum protocol
- Cannot restart with a copy of previous state (no-cloning)
  - Need to rewind unitaries, leading to more errors
- Limit number of backtracking using bound on tree code!



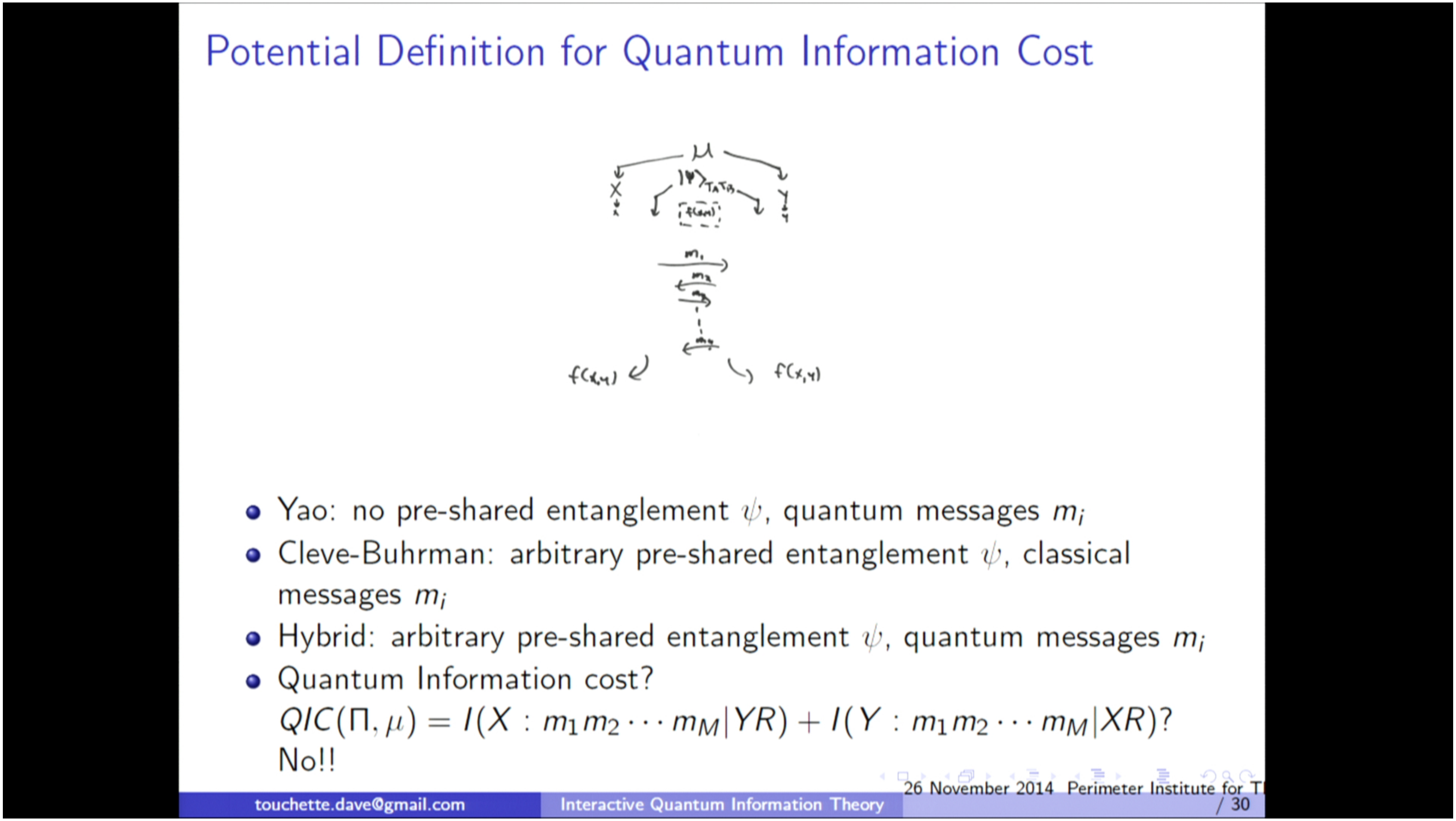
Results for Noisy Interactive Quantum Communication

- Communication complexity robust under noisy communication
- Tolerate maximal $(1/2 - \epsilon)$ error rate in perfect shared entanglement model
  - Requires new bound on tree codes
  - Requires new representation for quantum protocols
- Positive communication rates for some $Q = 0$ depolarizing channel
  - Separation between standard and interactive quantum capacity



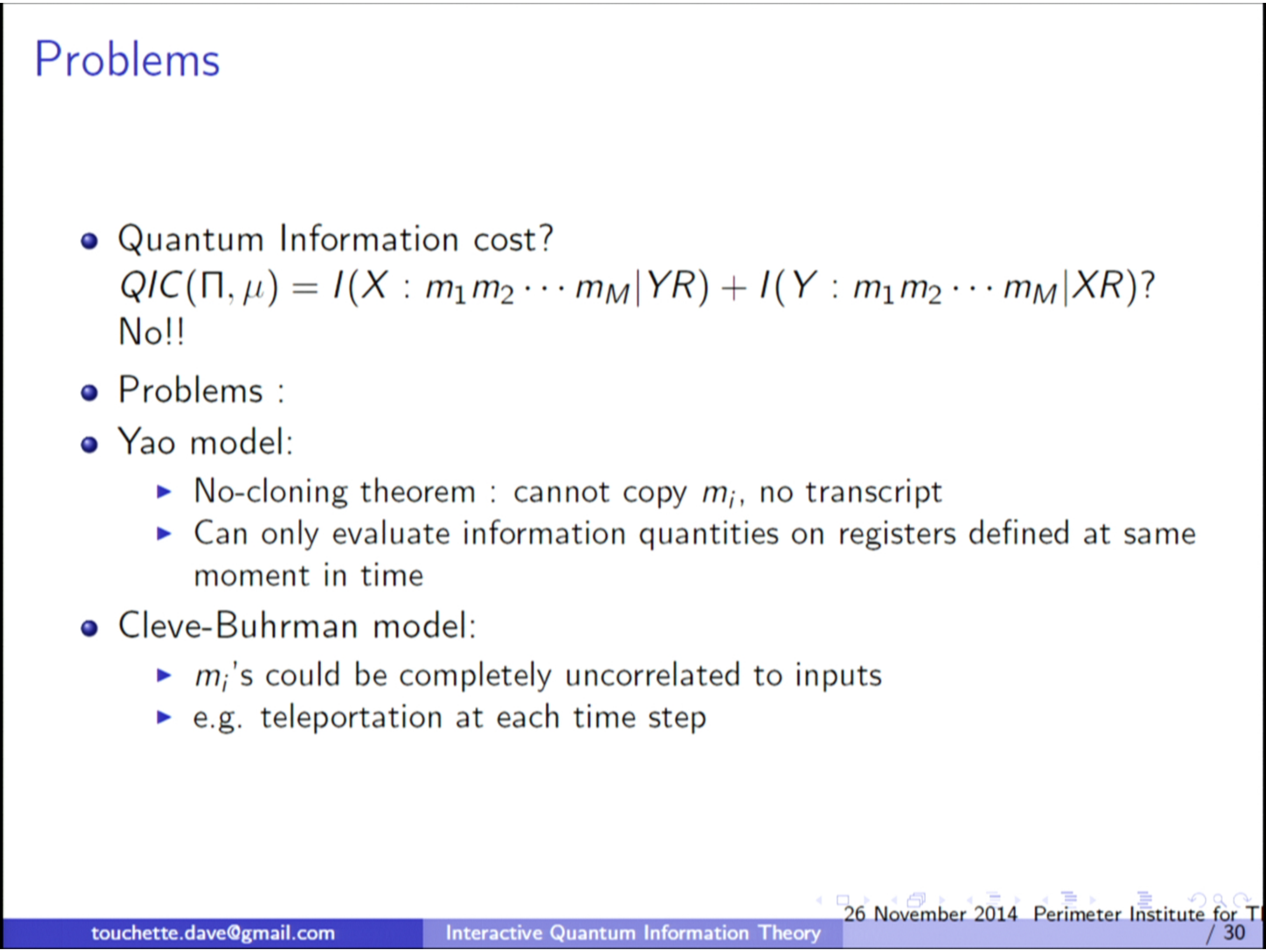
New Notion of Quantum Information Complexity and Protocol Compression

- Remember:
- Information cost: $IC(\Pi, \mu) = I(X : \Pi | YR) + I(Y : \Pi | XR)$
- Information complexity: $IC(f, \mu, \epsilon) = \inf_{\Pi} IC(\Pi, \mu)$
- Desirable properties:
  - Additivity: $IC(T_1 \otimes T_2) = IC(T_1) + IC(T_2)$
  - Lower bounds communication: $IC(T) \leq CC(T)$
  - Continuous in error ϵ
  - Operational interpretation: $IC(T) = ACC(T) = \limsup_{n \to \infty} \frac{1}{n} CC_n(T^{\otimes n})$ [BR11]
  - Direct sum on composite functions, e.g. DISJ from AND



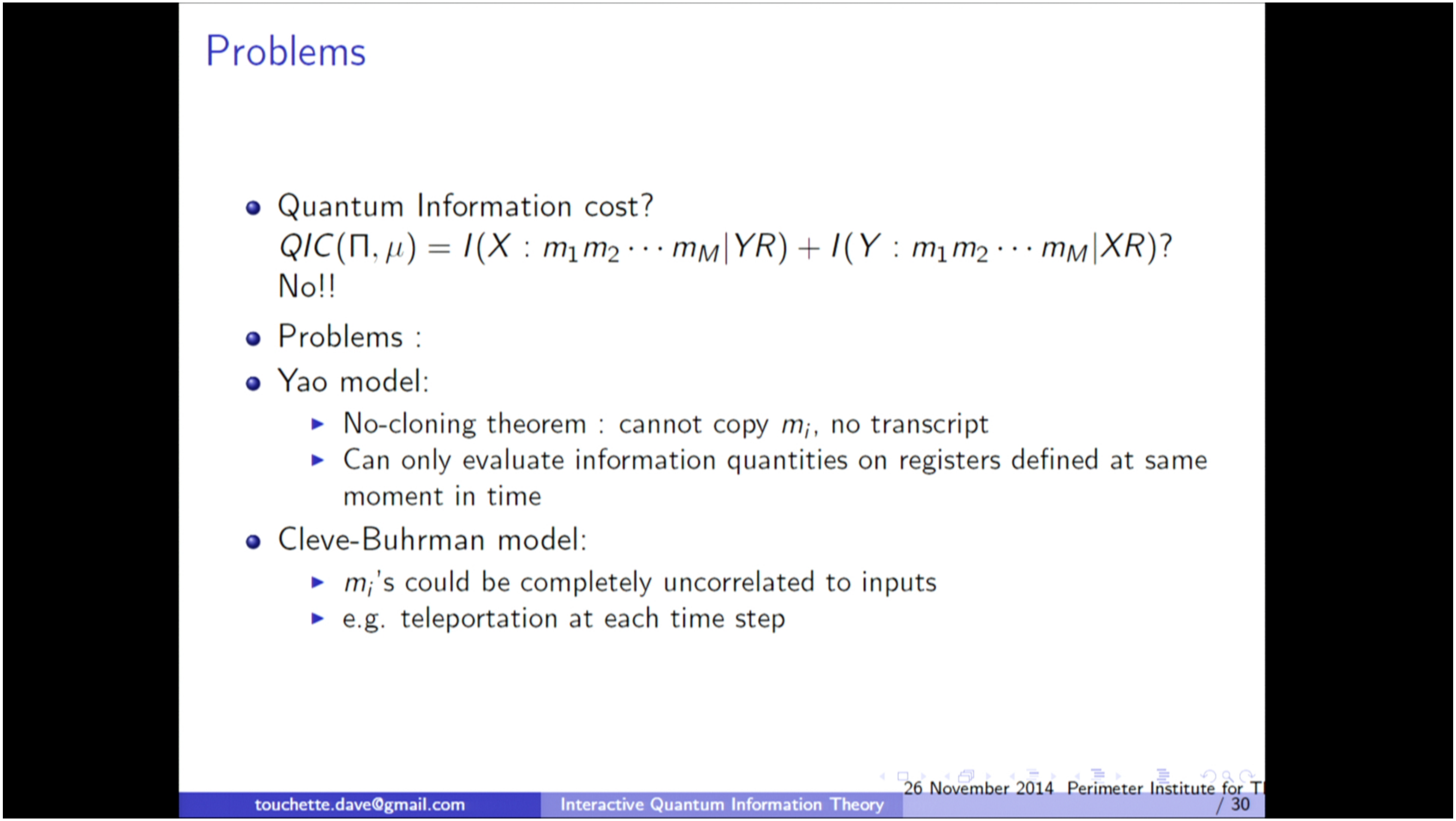
Potential Definition for Quantum Information Cost

- Yao: no pre-shared entanglement ψ, quantum messages m_i
- Cleve-Buhrman: arbitrary pre-shared entanglement ψ, classical messages m_i
- Hybrid: arbitrary pre-shared entanglement ψ, quantum messages m_i
- Quantum Information cost?
  $QIC(\Pi, \mu) = I(X : m_1 m_2 \cdots m_M | YR) + I(Y : m_1 m_2 \cdots m_M | XR)$?
  No!!



Problems

- Quantum Information cost?
  $QIC(\Pi, \mu) = I(X : m_1 m_2 \cdots m_M | YR) + I(Y : m_1 m_2 \cdots m_M | XR)$?
  No!!
- Problems :
- Yao model:
  - No-cloning theorem : cannot copy m_i, no transcript
  - Can only evaluate information quantities on registers defined at same moment in time
- Cleve-Buhrman model:
  - m_i's could be completely uncorrelated to inputs
  - e.g. teleportation at each time step

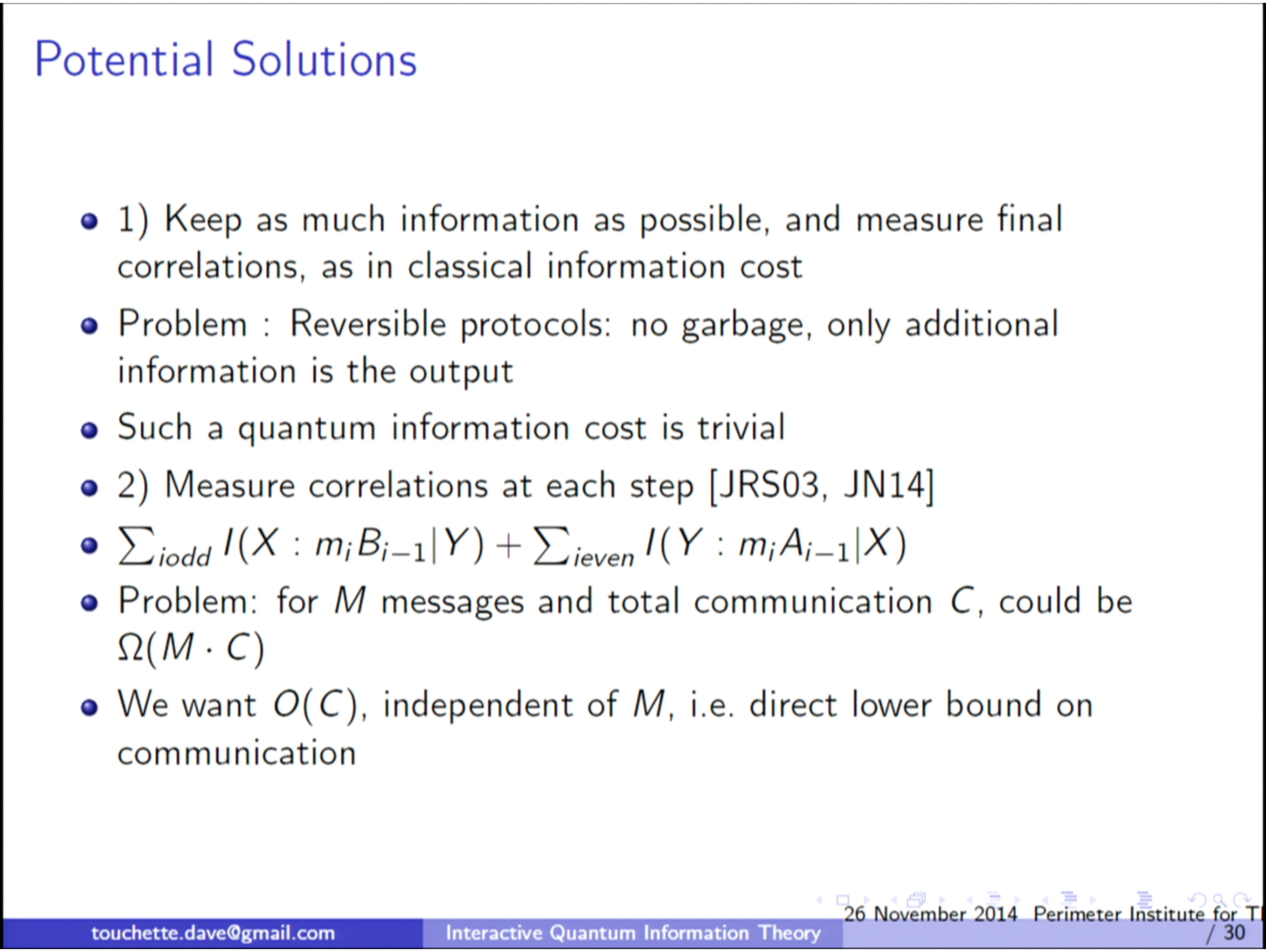


Problems

- Quantum Information cost?

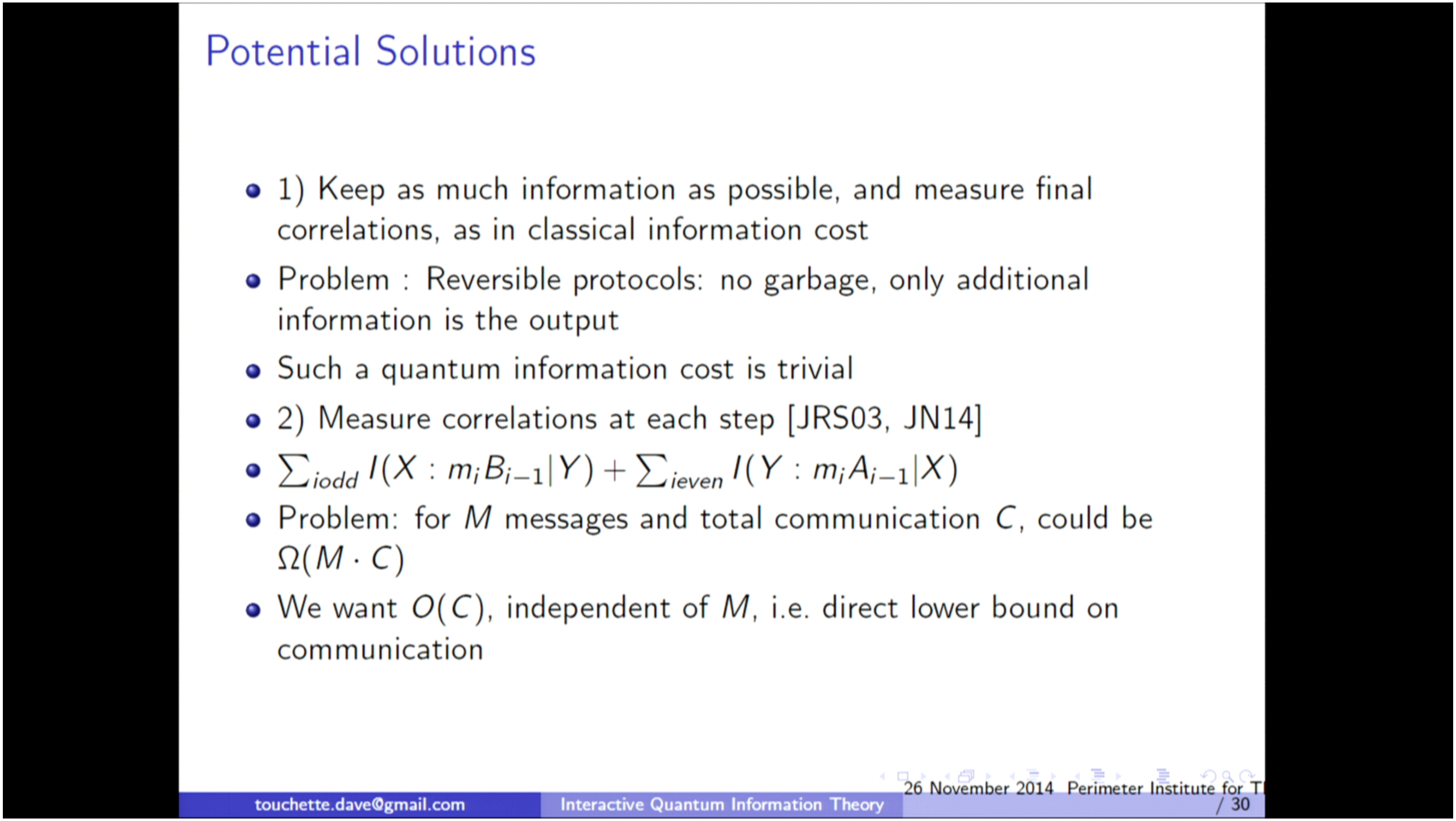
  $QIC(\Pi, \mu) = I(X : m_1 m_2 \cdots m_M | YR) + I(Y : m_1 m_2 \cdots m_M | XR)$?

  No!!
- Problems :
- Yao model:
  - No-cloning theorem : cannot copy m_i, no transcript
  - Can only evaluate information quantities on registers defined at same moment in time
- Cleve-Buhrman model:
  - m_i's could be completely uncorrelated to inputs
  - e.g. teleportation at each time step



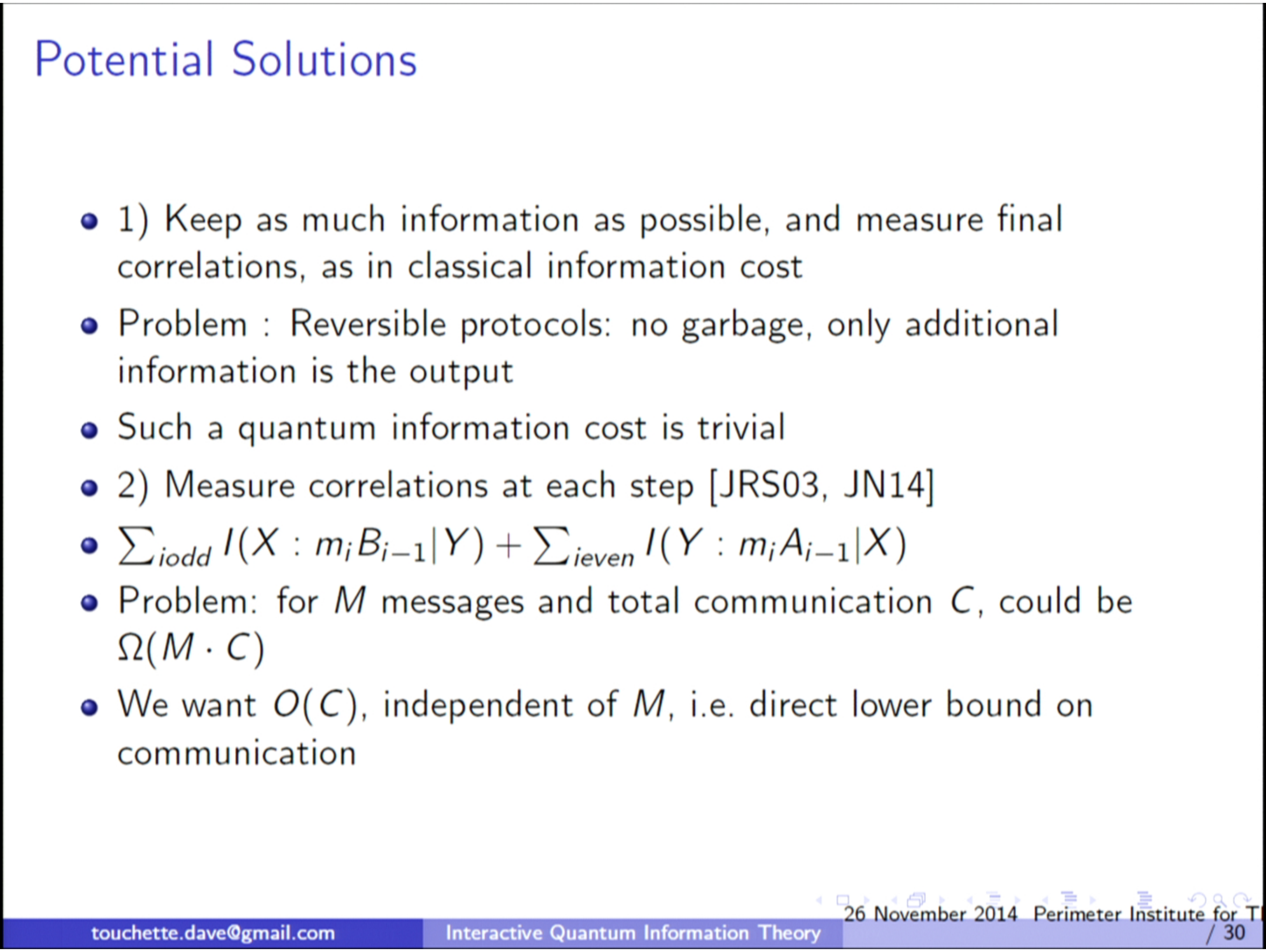
Potential Solutions

- 1) Keep as much information as possible, and measure final correlations, as in classical information cost
- Problem : Reversible protocols: no garbage, only additional information is the output
- Such a quantum information cost is trivial
- 2) Measure correlations at each step [JRS03, JN14]
- $\sum_{iodd} I(X : m_i B_{i-1} | Y) + \sum_{ieven} I(Y : m_i A_{i-1} | X)$
- Problem: for M messages and total communication C, could be $\Omega(M \cdot C)$
- We want $O(C)$, independent of M, i.e. direct lower bound on communication



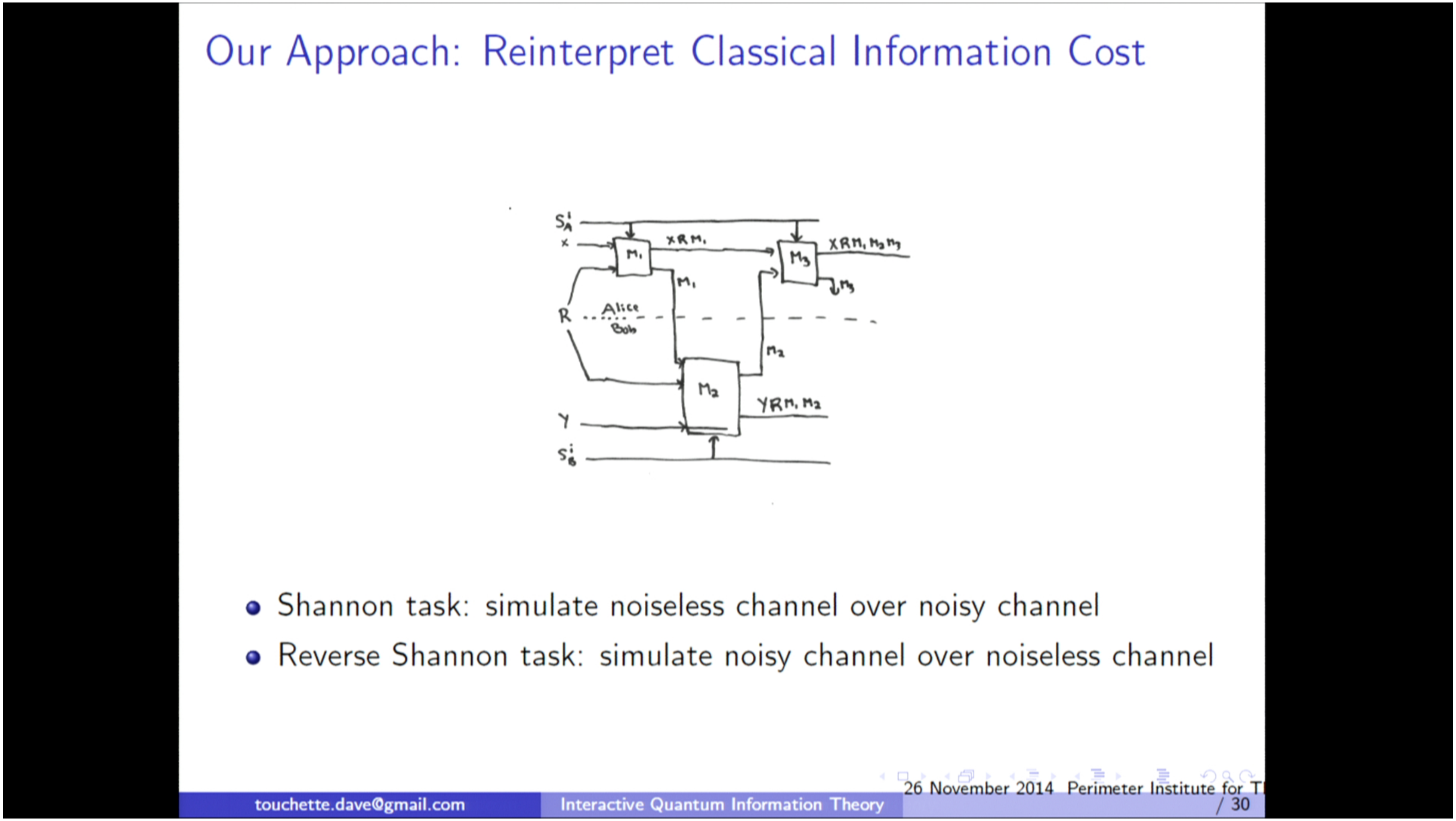
Potential Solutions

- 1) Keep as much information as possible, and measure final correlations, as in classical information cost
- Problem : Reversible protocols: no garbage, only additional information is the output
- Such a quantum information cost is trivial
- 2) Measure correlations at each step [JRS03, JN14]
- $\sum_{iodd} I(X : m_i B_{i-1} | Y) + \sum_{ieven} I(Y : m_i A_{i-1} | X)$
- Problem: for M messages and total communication C, could be $\Omega(M \cdot C)$
- We want $O(C)$, independent of M, i.e. direct lower bound on communication



Potential Solutions

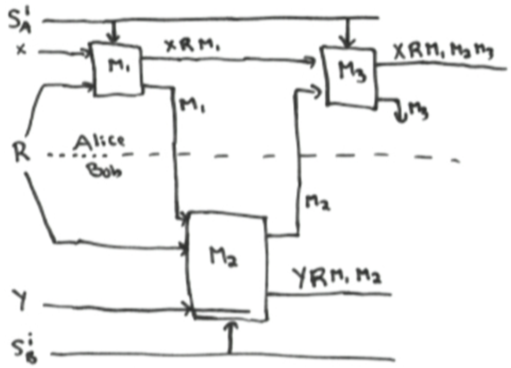
- 1) Keep as much information as possible, and measure final correlations, as in classical information cost
- Problem : Reversible protocols: no garbage, only additional information is the output
- Such a quantum information cost is trivial
- 2) Measure correlations at each step [JRS03, JN14]
- $\sum_{iodd} I(X : m_i B_{i-1} | Y) + \sum_{ieven} I(Y : m_i A_{i-1} | X)$
- Problem: for M messages and total communication C, could be $\Omega(M \cdot C)$
- We want $O(C)$, independent of M, i.e. direct lower bound on communication



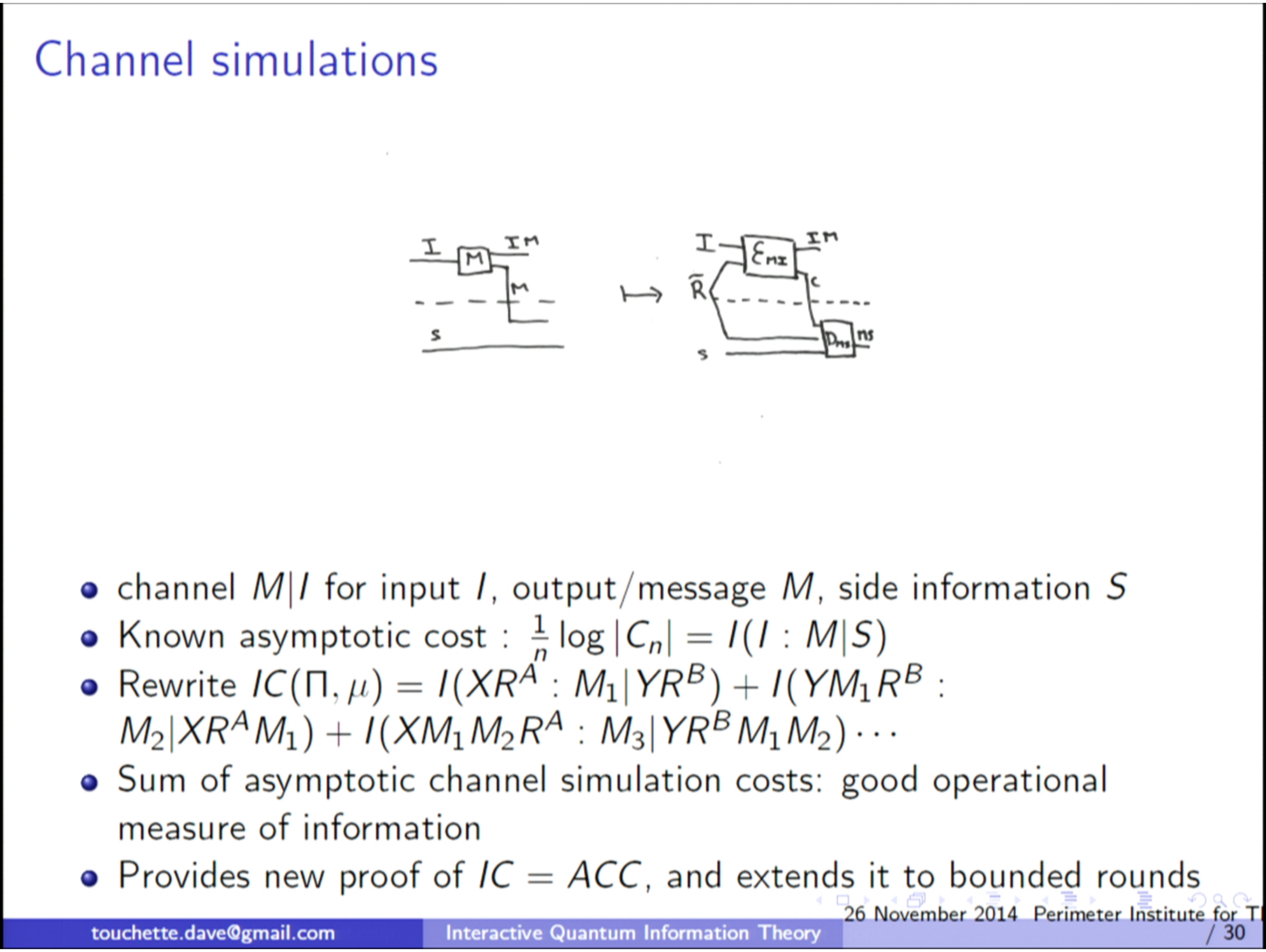
Our Approach: Reinterpret Classical Information Cost

- Shannon task: simulate noiseless channel over noisy channel
- Reverse Shannon task: simulate noisy channel over noiseless channel

Our Approach: Reinterpret Classical Information Cost

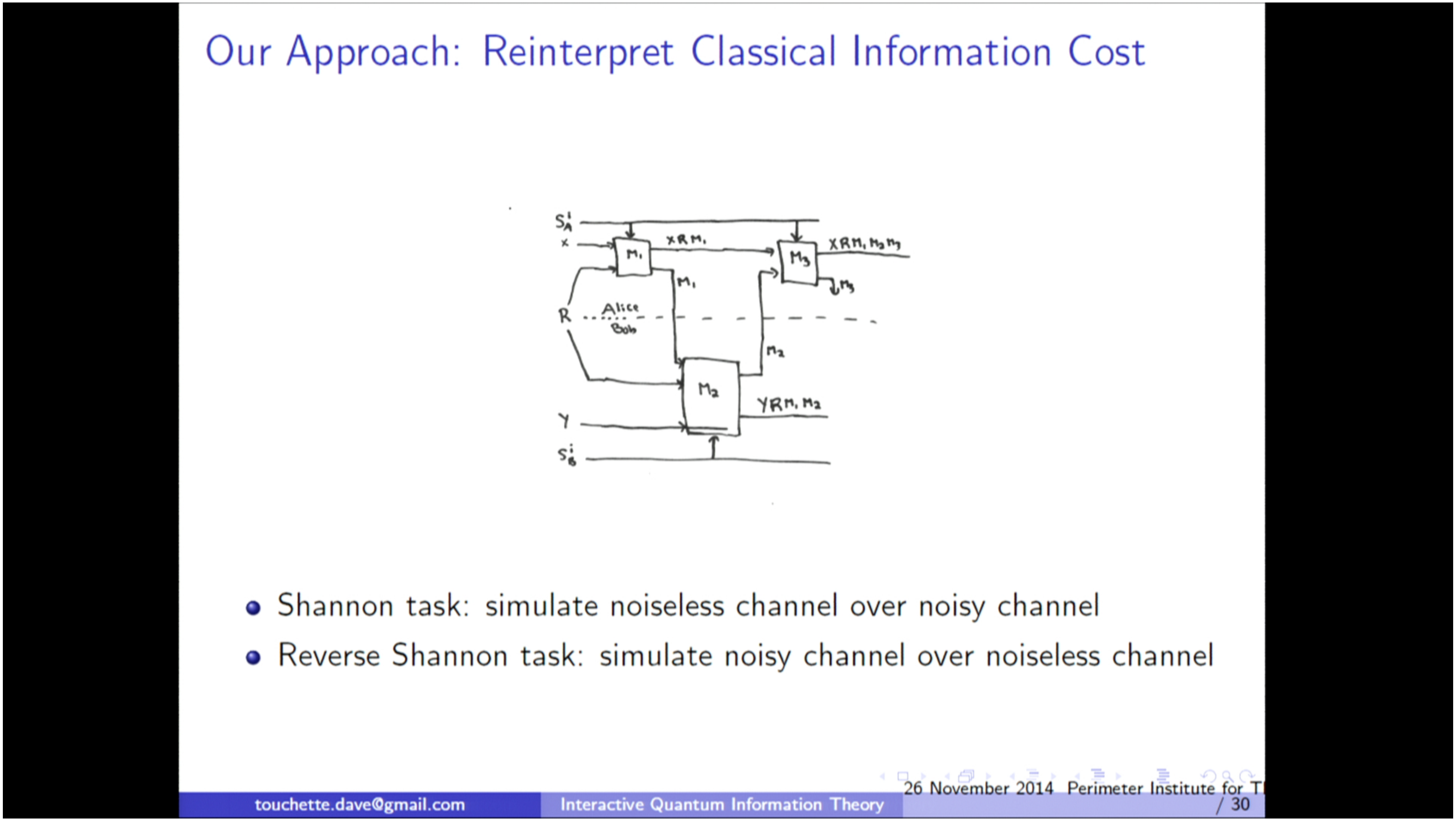


- Shannon task: simulate noiseless channel over noisy channel
- Reverse Shannon task: simulate noisy channel over noiseless channel



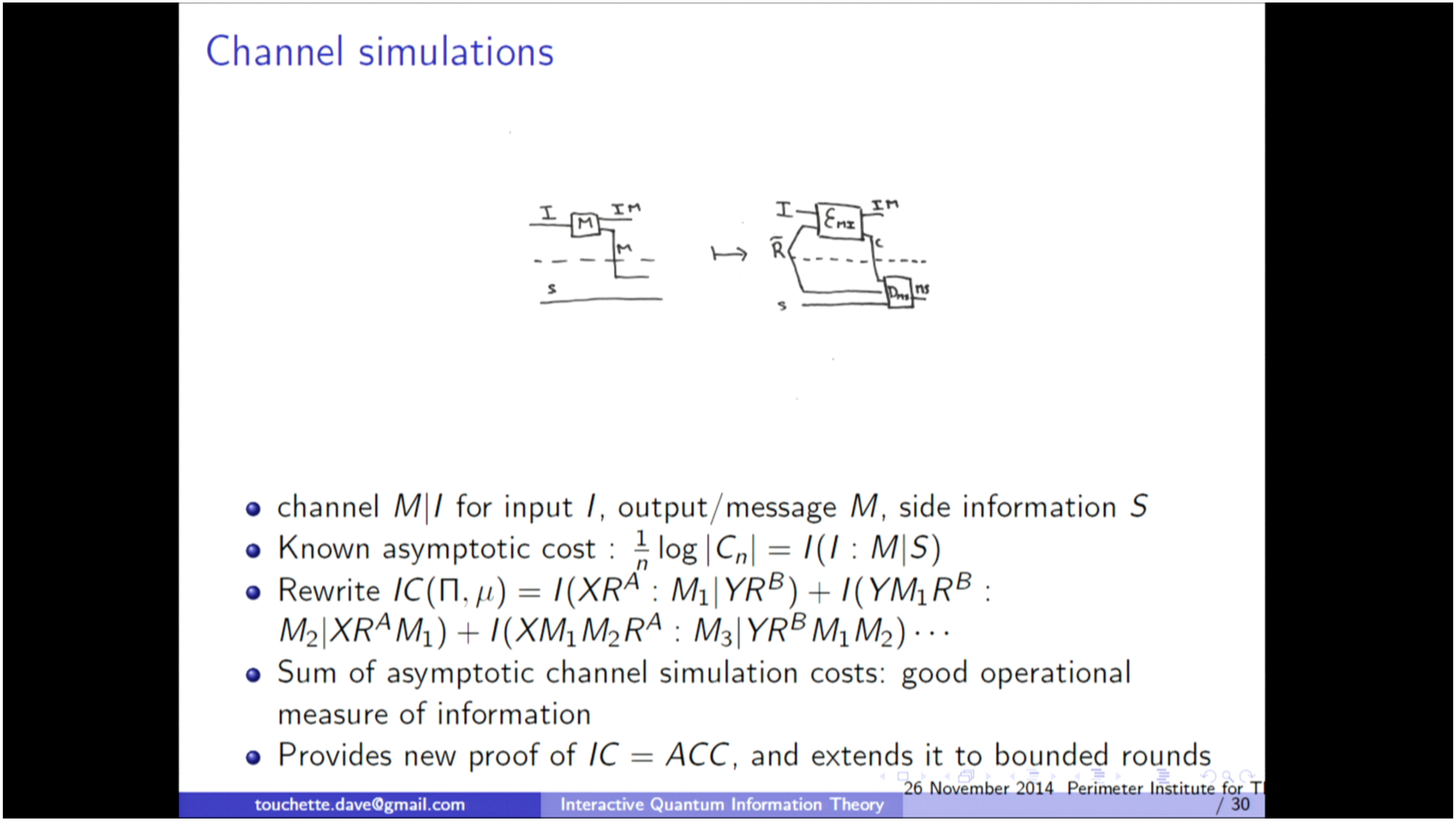
Channel simulations

- channel $M|I$ for input I, output/message M, side information S
- Known asymptotic cost : $\frac{1}{n}\log|C_n| = I(I : M|S)$
- Rewrite $IC(\Pi, \mu) = I(XR^A : M_1|YR^B) + I(YM_1R^B : M_2|XR^AM_1) + I(XM_1M_2R^A : M_3|YR^BM_1M_2)\cdots$
- Sum of asymptotic channel simulation costs: good operational measure of information
- Provides new proof of $IC = ACC$, and extends it to bounded rounds



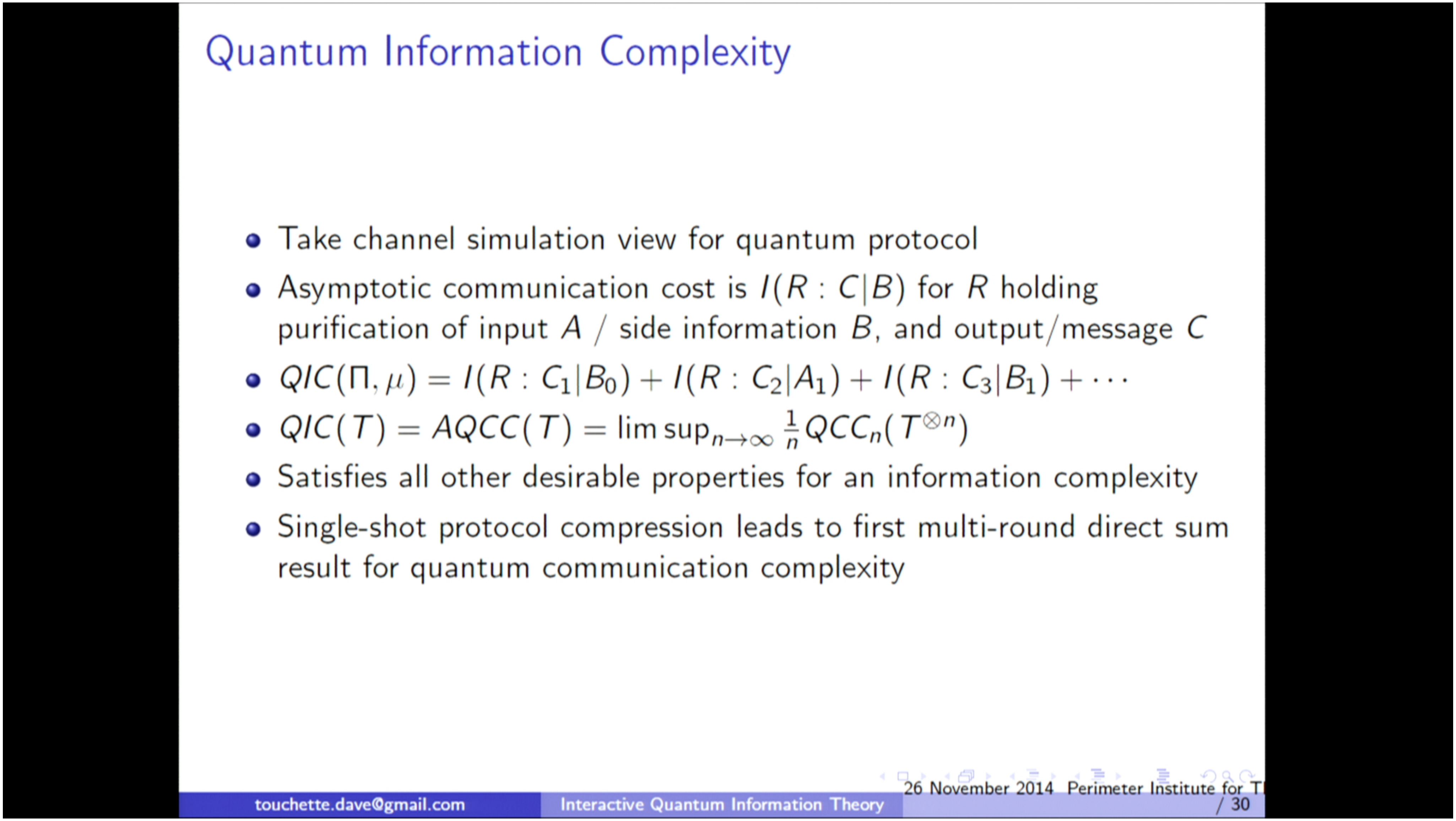
Our Approach: Reinterpret Classical Information Cost

- Shannon task: simulate noiseless channel over noisy channel
- Reverse Shannon task: simulate noisy channel over noiseless channel



Channel simulations

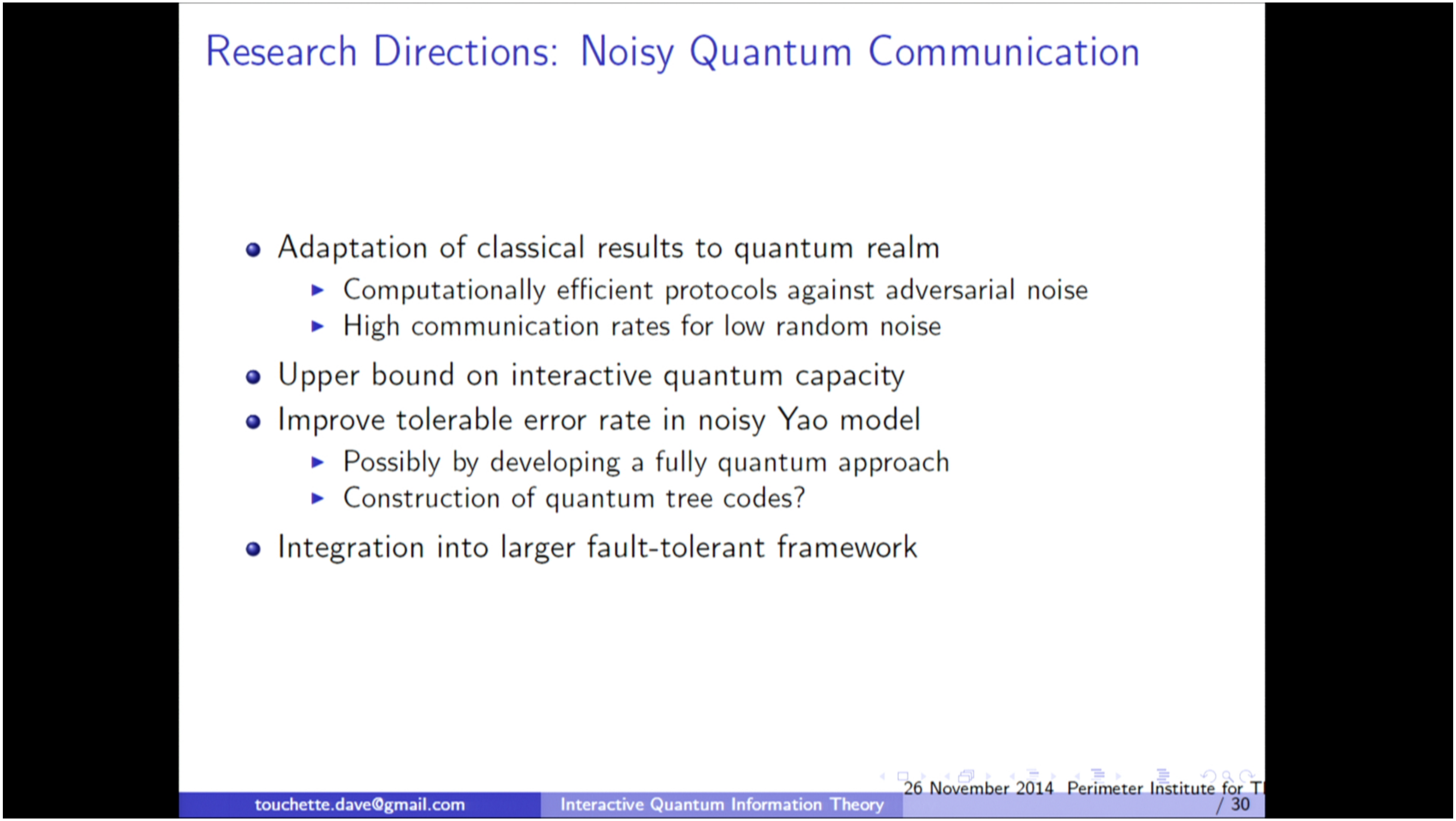
- channel $M|I$ for input I, output/message M, side information S
- Known asymptotic cost : $\frac{1}{n}\log|C_n| = I(I : M|S)$
- Rewrite $IC(\Pi,\mu) = I(XR^A : M_1|YR^B) + I(YM_1R^B : M_2|XR^AM_1) + I(XM_1M_2R^A : M_3|YR^BM_1M_2)\cdots$
- Sum of asymptotic channel simulation costs: good operational measure of information
- Provides new proof of $IC = ACC$, and extends it to bounded rounds



Quantum Information Complexity

- Take channel simulation view for quantum protocol
- Asymptotic communication cost is $I(R:C|B)$ for R holding purification of input A / side information B, and output/message C
- $QIC(\Pi,\mu) = I(R:C_1|B_0) + I(R:C_2|A_1) + I(R:C_3|B_1) + \cdots$
- $QIC(T) = AQCC(T) = \limsup_{n\to\infty} \frac{1}{n} QCC_n(T^{\otimes n})$
- Satisfies all other desirable properties for an information complexity
- Single-shot protocol compression leads to first multi-round direct sum result for quantum communication complexity

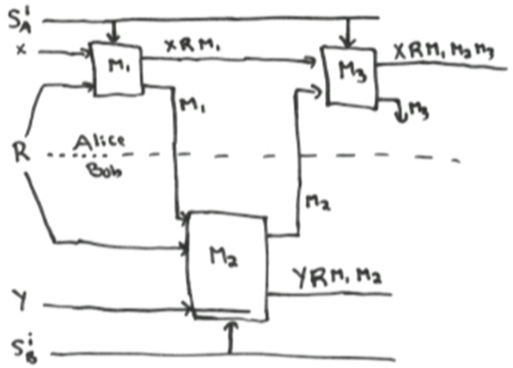
touchette.dave@gmail.com Interactive Quantum Information Theory 26 November 2014 Perimeter Institute for T / 30



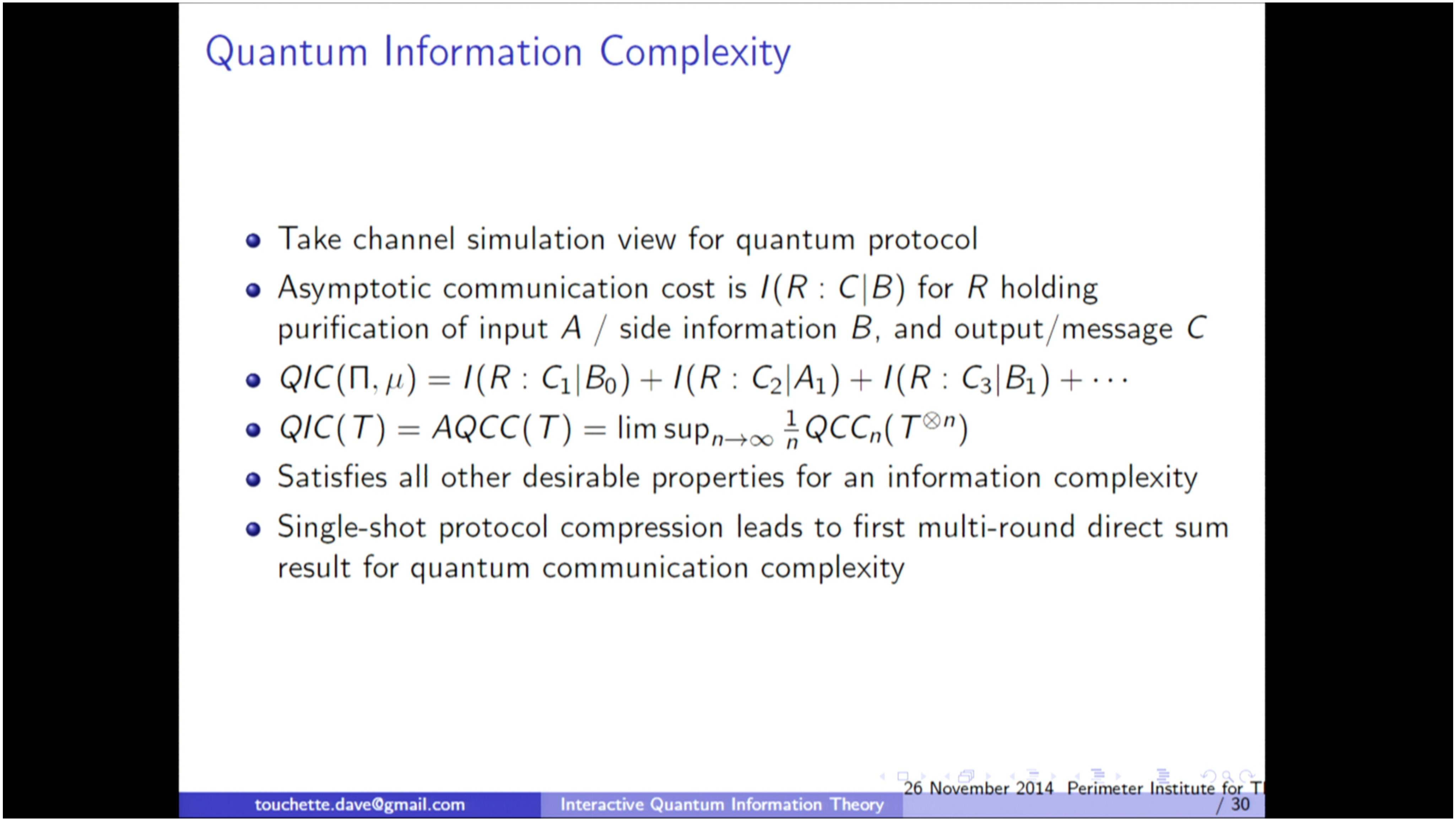
Research Directions: Noisy Quantum Communication

- Adaptation of classical results to quantum realm
  - Computationally efficient protocols against adversarial noise
  - High communication rates for low random noise
- Upper bound on interactive quantum capacity
- Improve tolerable error rate in noisy Yao model
  - Possibly by developing a fully quantum approach
  - Construction of quantum tree codes?
- Integration into larger fault-tolerant framework

Our Approach: Reinterpret Classical Information Cost



- Shannon task: simulate noiseless channel over noisy channel
- Reverse Shannon task: simulate noisy channel over noiseless channel



Quantum Information Complexity

- Take channel simulation view for quantum protocol
- Asymptotic communication cost is $I(R:C|B)$ for R holding purification of input A / side information B, and output/message C
- $QIC(\Pi,\mu) = I(R:C_1|B_0) + I(R:C_2|A_1) + I(R:C_3|B_1) + \cdots$
- $QIC(T) = AQCC(T) = \limsup_{n\to\infty} \frac{1}{n} QCC_n(T^{\otimes n})$
- Satisfies all other desirable properties for an information complexity
- Single-shot protocol compression leads to first multi-round direct sum result for quantum communication complexity