Optical Quantum Fingerprinting

Barry C. Sanders

(with Richard Cleve, Rolf Horn, and Karl-Peter Marzlin)

IQIS, University of Calgary, http://www.iqis.org/

Fields Institute Conference on Quantum Information and Quantum Control,
Toronto, 19-23 July 2004

Members of Calgary's Institute for QIS

Faculty (7)

- R. Cleve (Comp Sci)
- D. Feder (Th. Physics)
- P. Høyer (Comp Sci)
- K.-P. Marzlin (Th. Physics)
- A. Lvovsky (Exp. Physics)
- B. C. Sanders (Th. Physics)
- J. Watrous (Comp Sci)
- Affiliates (4): D. Hobill (Gen. Rel.), R. Thompson (ion trap), R. Scheidler & H. Williams (crypto)

Postdocs (5)

S. Ghose, H. Klauck, H. Roehrig, A. Scott, J. Walgate

Students (12)

I. Abu-Ajamieh, M. Adcock, S. Fast, D. Gavinsky, G. Gutoski, T. Harmon, Y. Kim, S. van der Lee, K. Luttmer, A. Morris, X. S. Qi, Z. B. Wang

Research Assistants (3)

L. Hanlen, R. Horn, G. Howard

Institute for Quantum Information Science at the University of Calgary

Outline

A. Motivation
B. Digital Fingerprinting
C. Quantum Fingerprinting
D. Optical Quantum Fingerprinting
E. Proposed Experiment
F. Conclusions

A. Motivation

Institute for
Quantum Information Science
at the University of Calgary

Fingerprints

- A fingerprint identifies the object/person using relatively little information.
- Especially useful in cases when storage or transmission of data is limited or costly.

Simultaneous Message Passing

- A. C. Yao introduced the simultaneous message passing model in 1979.
- Two parties send bit strings m_A and m_B to a referee who calculates a function $f(m_A, m_B)$.
  - Important for software protection and piracy.
- Fingerprinting in the simultaneous message passing model: f=Eq:

$$\mathrm{Eq}(m_A, m_B) = \begin{cases} 0 & \text{if} m_A \neq m_B, \\ 1 & \text{if} m_A = m_B \end{cases}$$

Quantum Communication Complexity

- Simultaneous message passing is one example of communication complexity, which considers the information transmission required for a specific task.
- Quantum teleportation, remote state preparation and superdense coding are examples of basic q. communication protocols.
- Quantum fingerprinting demonstrates a savings in communication complexity by exploiting quantum vs classical channels.

B. Digital Fingerprinting

Fingerprinting Scheme

Alice

Bob

messages

10001110101….

encoding

{101011 …1000101}

fingerprints

101001…

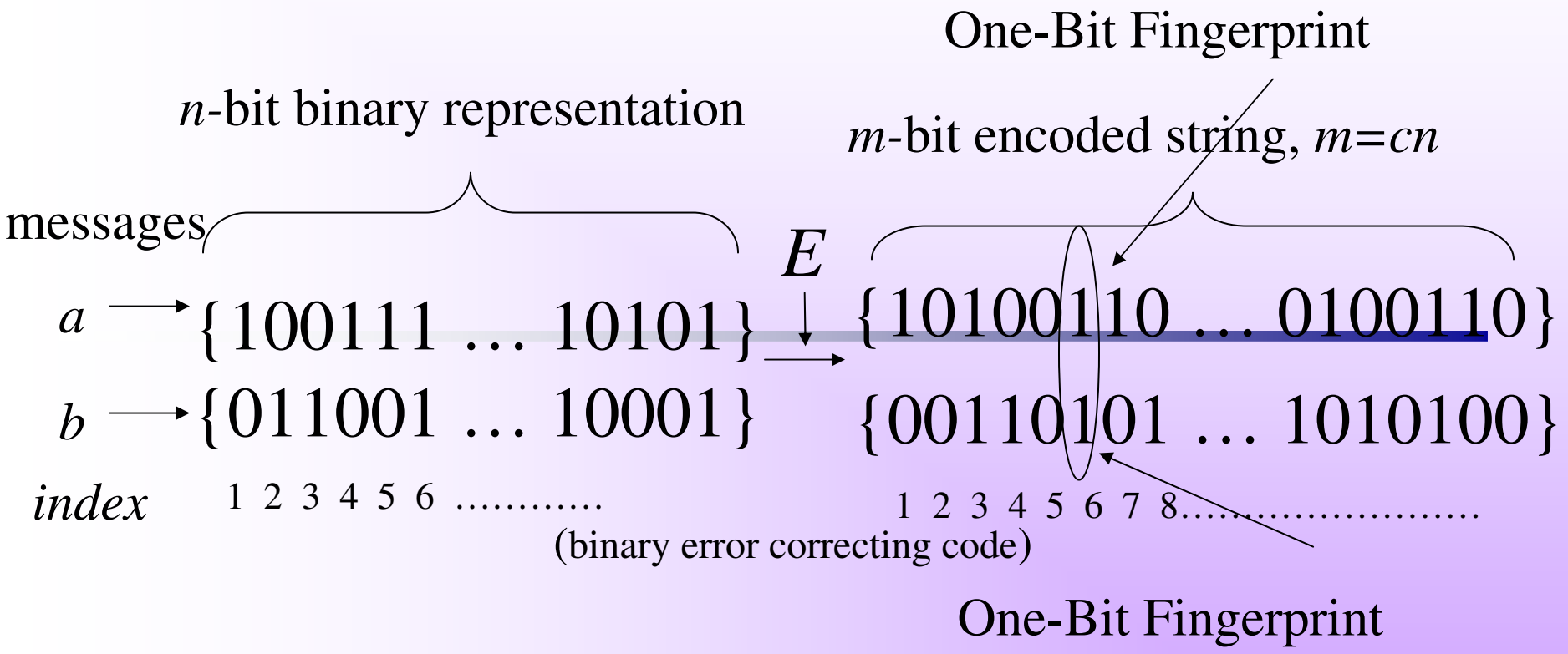
001101…

Roger

Fingerprinting with & w/o shared randomness

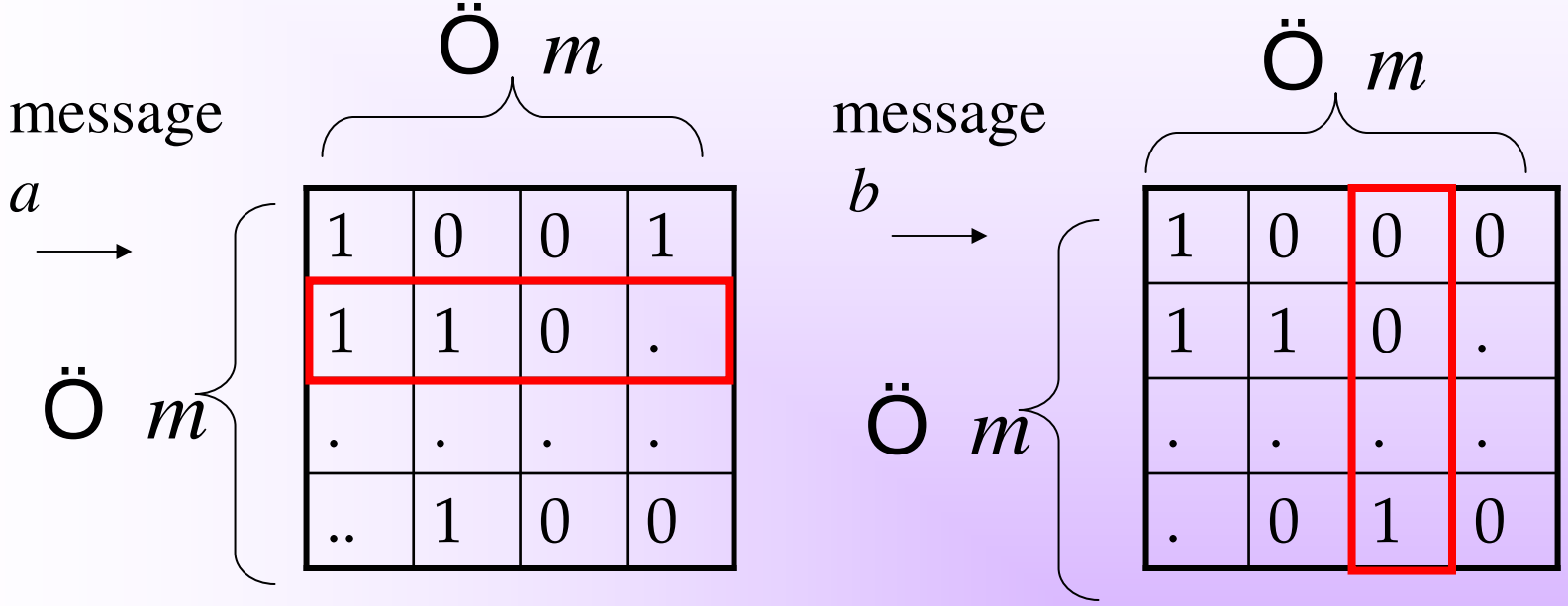
- Without shared randomness: Alice and Bob each independently produce a fingerprint from the message according to some predetermined (but not necessarily deterministic - may have private randomness) process.
- With shared randomness: Alice and Bob use a shared resource to construct the fingerprint.
- For (encoded) message length m, the cost of fingerprinting scales as $\ddot{O}\ m$ (w/o shared randomness) and as $\log m$ (w/o shared randomness).

One-Bit-At-A-Time Fingerprinting



n-bit message to *m*-bit codes to sequence of one-bit fingerprints with index of single bit generated randomly (shared randomness).

Ö m Scaling (no shared randomness)



Row index 1

Fingerprint for b = {01 110…}

Column index 2

Fingerprint for a = {10 00…1}

Errors and Guarantees

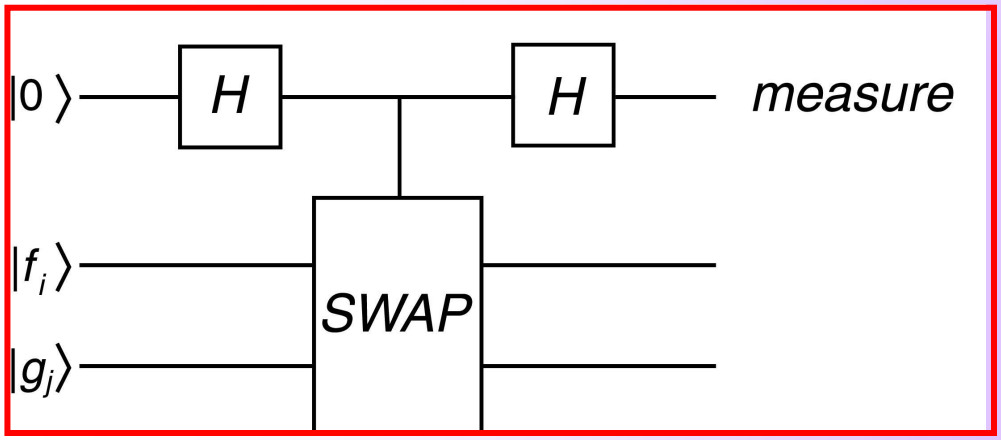
- Fingerprinting can have errors - we concentrate on one-sided errors such that inferring different fingerprints is always correct but inferring same is prone to error.
- One-sided errors can be valuable; for example holding a suspect whilst checking fingerprints: don't want to release a felon but holding an innocent person longer for further checking is acceptable.
- Guarantee is based on Worst-Case Scenario (WCS): malicious supplier produces messages to maximize p_{err}.
- For one-sided error scheme, Roger employs a deterministic protocol (no random numbers)

C. Quantum Fingerprinting

Quantum Fingerprinting

- Buhrman (2001) showed that q. fingerprinting reduces the cost of fingerprinting w/o shared randomness from $\ddot{O}\ m$ to $\log_2 m$.
- Use error correcting codes that maximize Hamming distance between code words $|E_i(m)\rangle$, then transmit state

$$|f(m_A)\rangle = \frac{1}{\sqrt{m}} \sum_{i=1} |i\rangle |E_i(m_A)\rangle$$



- Compare states using ancilla & cSWAP
  - § Referee measures $r=1$ with probability

$$(1 - |\text{Æ}\, f / \ g\text{æ}\,|^2)/2$$

$$(H \otimes I \otimes I)(\text{cSWAP})(H \otimes I \otimes I)|0\rangle_{\text{anc}} |f(m_A)\rangle |f(m_B)\rangle$$

Measurement outcome and inference

- Roger obtains $r=0,1$; infers $\mathrm{Eq}(m_A, m_B)=1-r$.
- One-sided error scheme: same messages yield $r=0$ and different messages yield either $r=0$ (with prob p_{err}) or $r=1$ (with prob p_{success}).

$$p_{\mathrm{err}} = 1 - p_{\mathrm{success}} = (1+\delta)/2 \text{ for } \delta \equiv |\langle f|g\rangle|^2.$$

- In the WCS, supplier always sends different messages so $r=0$ results are errors; thus p_{err} is the one-sided error for the WCS.

D. Optical Quantum Fingerprinting

Optical Q. Fingerprinting

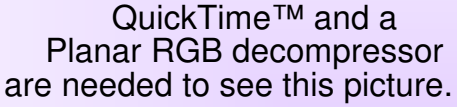
- Qubits can be realized as polarization-encoded single photons.
- The 'quantum advantage' in fingerprinting is not just asymptotic: scales all the way to single-qubit level (de Beaudrap, PRA, 2004).
- cSWAP is not achievable in linear quantum optics, but an optical realization is possible for single-qubit fingerprinting of two-bit messages; we propose such an experiment.

Polarization States

- A single photon can be encoded in a superposition of the two polarization states $|0\rangle$ (eg horizontal) and $|1\rangle$ (eg vertical).
- The single qubit state is parametrized by polar and azimuthal angles on the 'Bloch sphere':

$$|\theta, \phi\rangle = |(\cos\theta, \mathrm{e}^{i\phi}\sin\theta)^{\mathrm{T}}\rangle = \cos\theta|0\rangle + \mathrm{e}^{i\phi}\sin\theta|1\rangle$$

- Best states are widely separated on Bloch sphere; for $M=4$, use 'tetrahedral states'.


QuickTime™ and a
Planar RGB decompressor
are needed to see this picture.

‘Tetrahedral States’

$$\text{Introduce } \Omega \equiv (\theta, \phi).$$

The four maximally separated fingerprint states are thus

$$F = \{|\Omega_k\rangle; \Omega_0 = (0,0) \text{ or } \Omega_k = (2\cos^{-1}(1/\sqrt{3}), \frac{2\pi}{3}ik) \text{for } k = 1,2,3\}$$

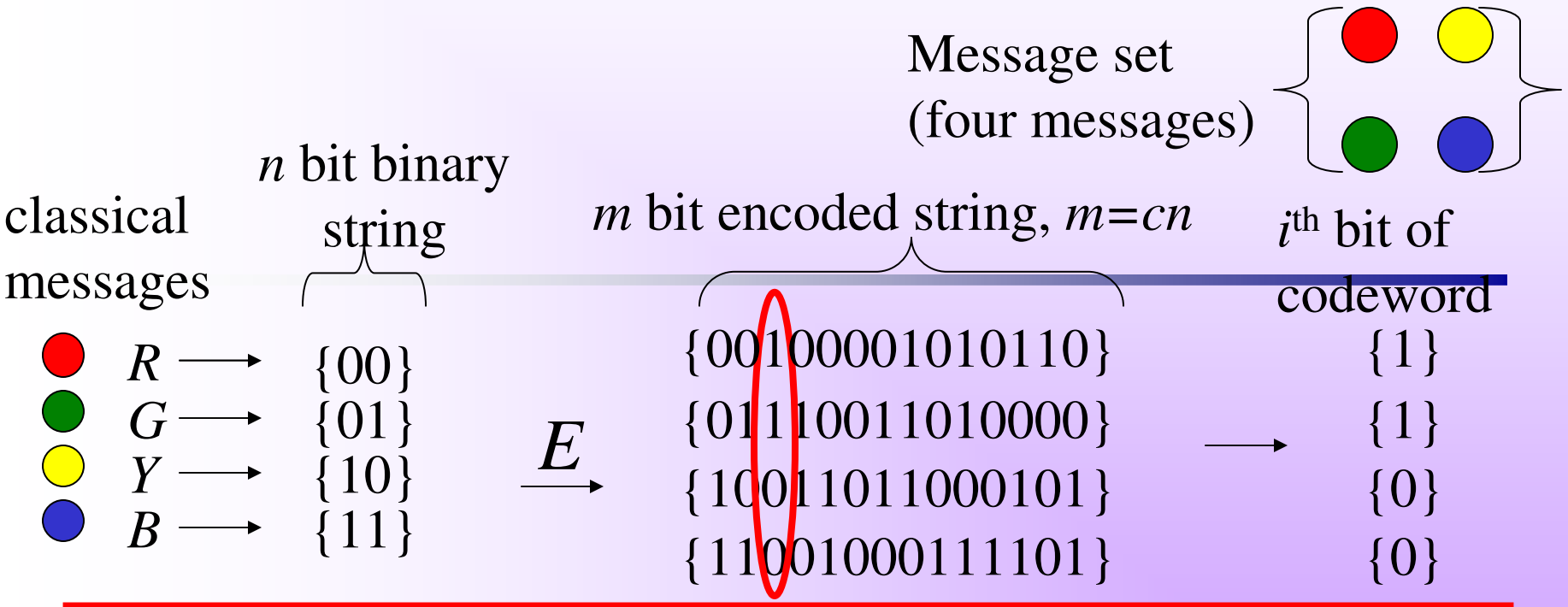
The indistinguishability of any two unequal states is determined by

$$\delta(\Omega', \Omega) \equiv |\langle\Omega'|\Omega\rangle|^2 = \left|\cos\frac{\theta'}{2}\cos\frac{\theta}{2} + \mathrm{e}^{\mathrm{i}(\phi-\phi')}\sin\frac{\theta'}{2}\sin\frac{\theta}{2}\right|^2,$$

which is *1/3* for the tetrahedral states. Thus,

$$p_{\text{success}} = 1 - p_{\text{err}} = 1/3$$

cf: classical WCS one-bit fingerprinting



$a=b \Rightarrow E_i(a) = E_i(b)$ but not converse so, in the worst case scenario (WCS), referee always fails.

Replacing the cSWAP

- No cSWAP in deterministic linear optics.
- Discriminating the tetrahedral states is possible via the Hong-Ou-Mandel dip: the two photons are directed into two ports of a 1:1 beam splitters, and the output is guaranteed *not* to produce a coincidence if the two photons are indistinguishable.
- Seeing a coincidence guarantees they are different with same error as cSWAP:

$$p_{\text{success}} = 1/3$$

Shared Entanglement

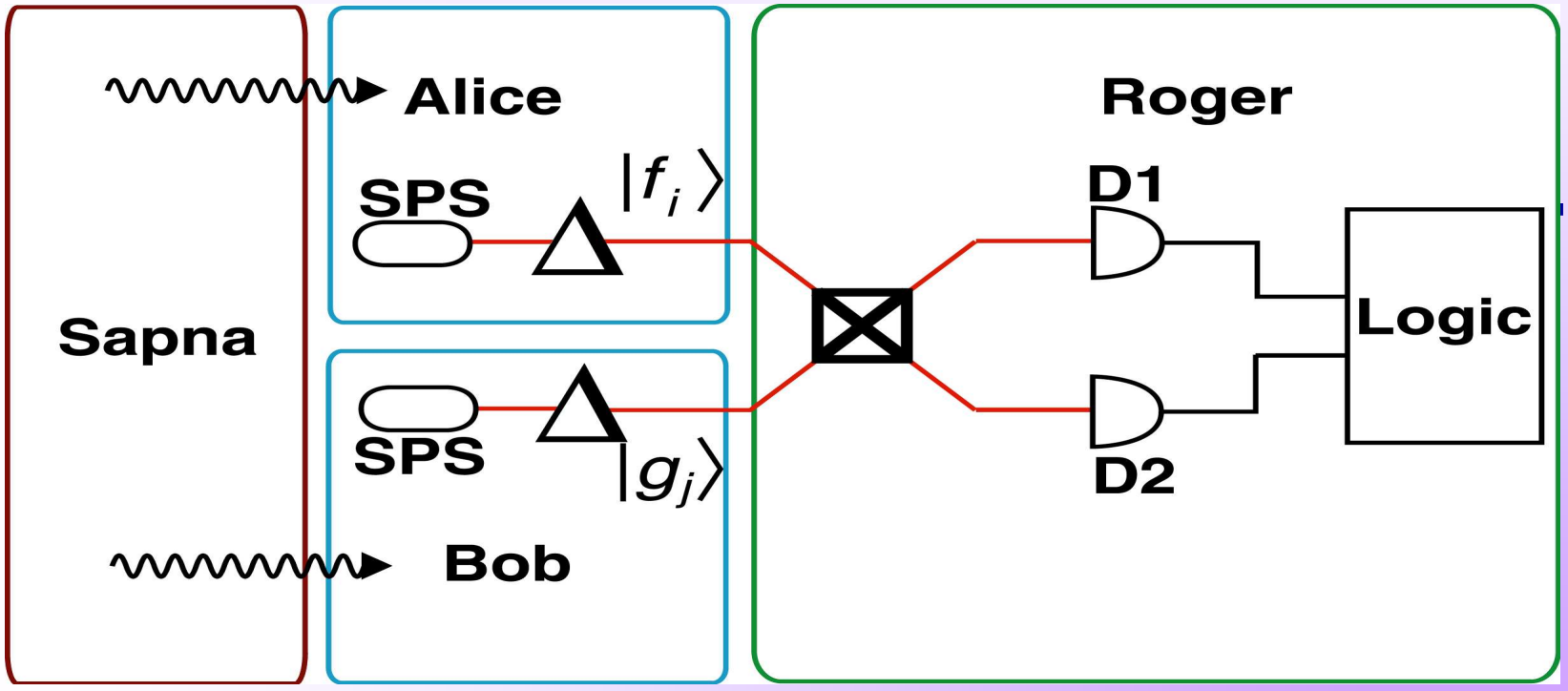
- Suppose Alice and Bob share a pure maximally-entangled two photon Bell 'singlet' state

$$|\Psi^-\rangle \equiv 2^{-1/2}[|01\rangle - |10\rangle]$$

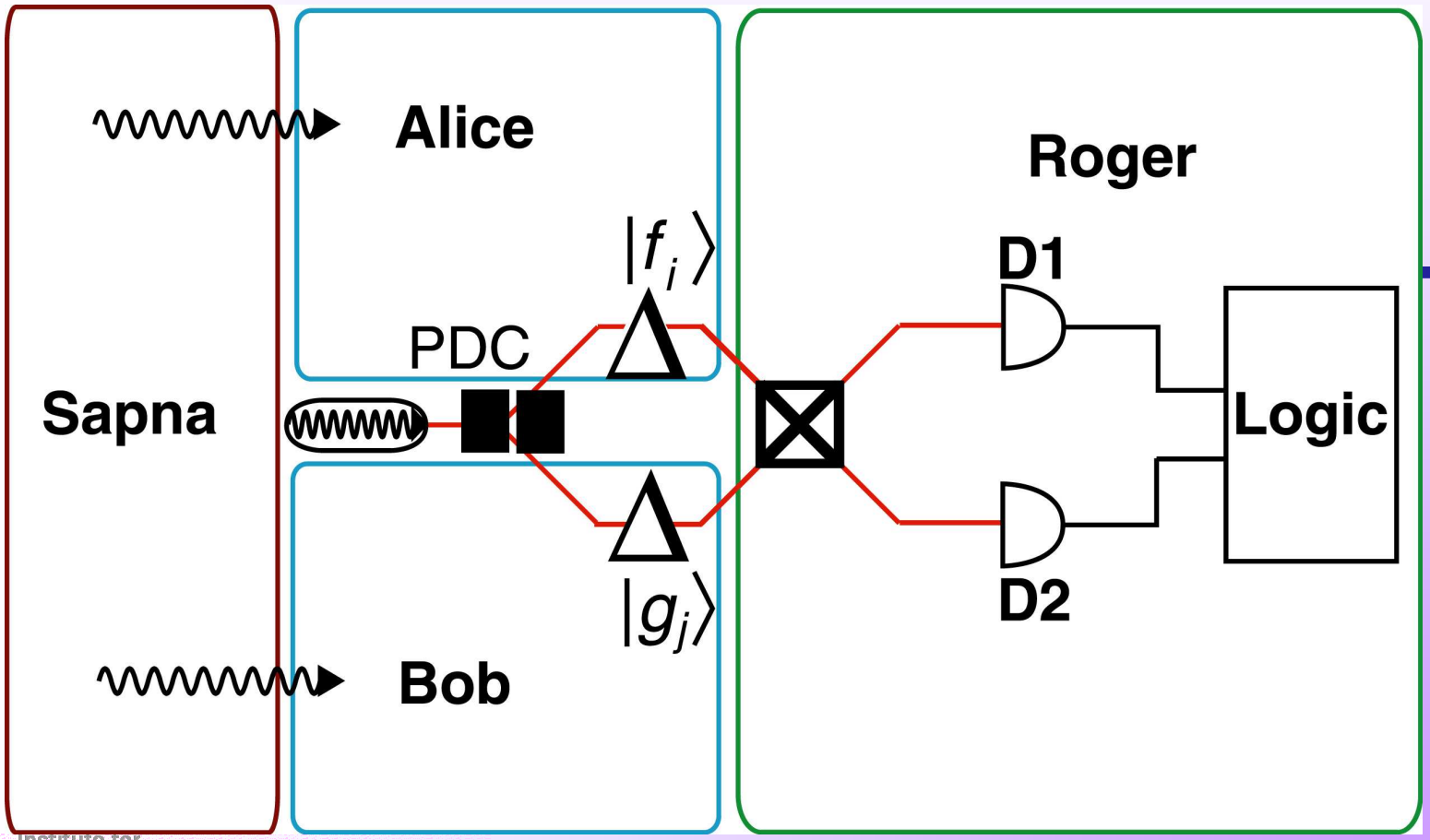
- Alice and Bob each perform one of the Pauli operations σ_X, σ_Y, σ_Z, σ_I depending on message received: the Bell singlet state is invariant if they perform same operation; otherwise uields a different Bell state.
- Shared entanglement produces 100% successful q. fingerprinting, which is unachievable for single-bit fingerprinting regardless of amount of shared random bits: classical bound is $p_{\text{success}} = 2/3$.

E. Proposed Experiment

With Independent Single-Photon Sources



With Shared Parametric Down Converter



F Conclusions

Institute for
Quantum Information Science
at the University of Calgary

Conclusions

- *M=4,* single qubit q. fingerprinting is feasible in linear quantum optics.
- Optical q. fingerprinting gives one-sided error success rate of 1/3 in WCS compared to zero for one-bit fingerprinting in WCS.
- Entangled resource produces 100% success rate, which is better than success rate of 2/3 for classical scheme with arbitrarily large shared randomness (Cleve, Horn, Lvovsky, Sanders).
- Scaling to more qubits is possible using postselected cSWAP gate.