Macroscopic CV quantum operations and states

Continuous-Variable Quantum Computing on Encrypted Data
&
Quantum Control of Mechanical Oscillators

Ulrik L. Andersen

Qubiz

Quantum Innovation Center

Qubiz shall exploit the very strong Danish research position within quantum technology for value creation in the form of growth of new high-tech businesses and employment in Danish society

Innovation Fund Denmark

RESEARCH, TECHNOLOGY & GROWTH

80MKr for two year

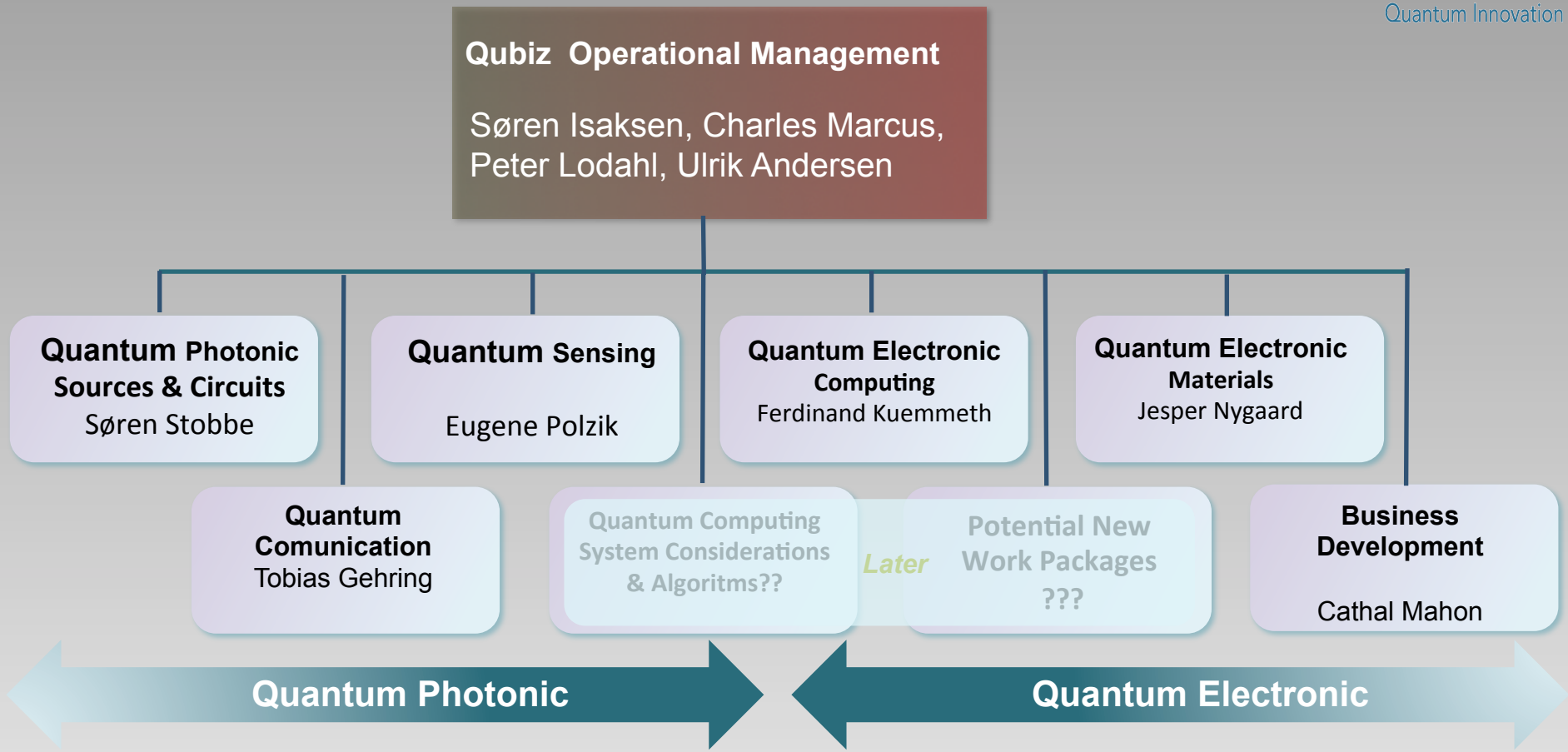
DTU

KØBENHAVNS UNIVERSITET

AARHUS UNIVERSITET

3 Danish Universities
3 External university partners
18 Companies

Qubiz
Quantum Innovation Center



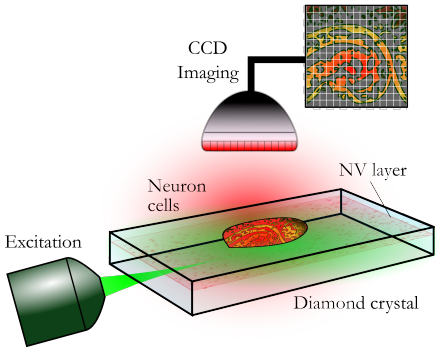
Qubiz
Quantum Innovation Center

Qubiz activities at DTU

Continuous variable quantum key distribution towards MDI
(AIT, York, UCSB, Cryptomathic, NKT Photonics)

- Cheap compact sources
- QRNG
- Broadband efficient detectors
- Synchronization
- Efficient post-processing
- Security analysis

Diamond magnetometry
(Ulm Univ, Lepzig Univ, Philips BioCells)



- Spatial resolution - 1micron
- Sensitivity – 1nT/Hz^1/2
- Brain tissue imaging
- Cancer cell imaging

Continuous-Variable Quantum Computing on Encrypted Data

Kevin Marshall[1], Christian S. Jacobsen[2], Clemens Schäfermeier[2],
Tobias Gehring[2], Christian Weedbrook[3], Ulrik L. Andersen[2]

(1) Department of Physics, University of Toronto, Canada
(2) Department of Physics, Technical University of Denmark, Denmark
(3) CipherQ, Canada

ArXiv: 1607.07372

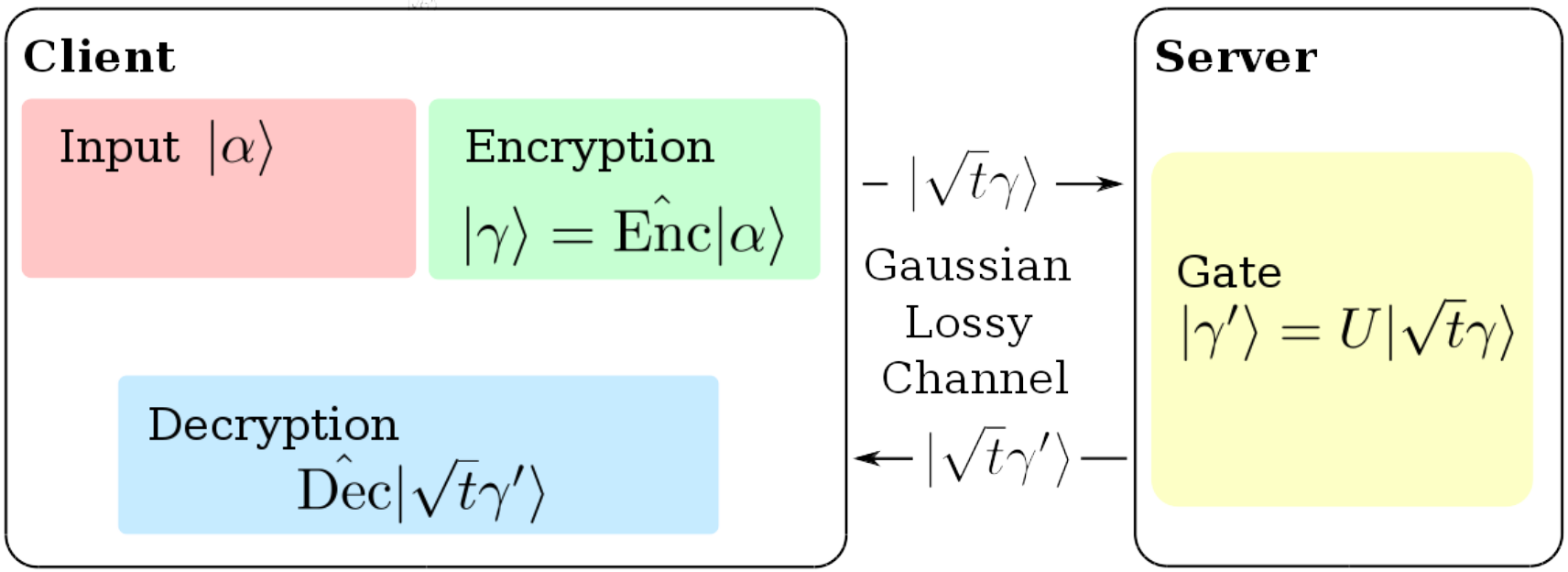
Quantum Computing in a Cloud

IBM Quantum Computer in a Cloud

- Security of your data

Security in Quantum Cloud Computing

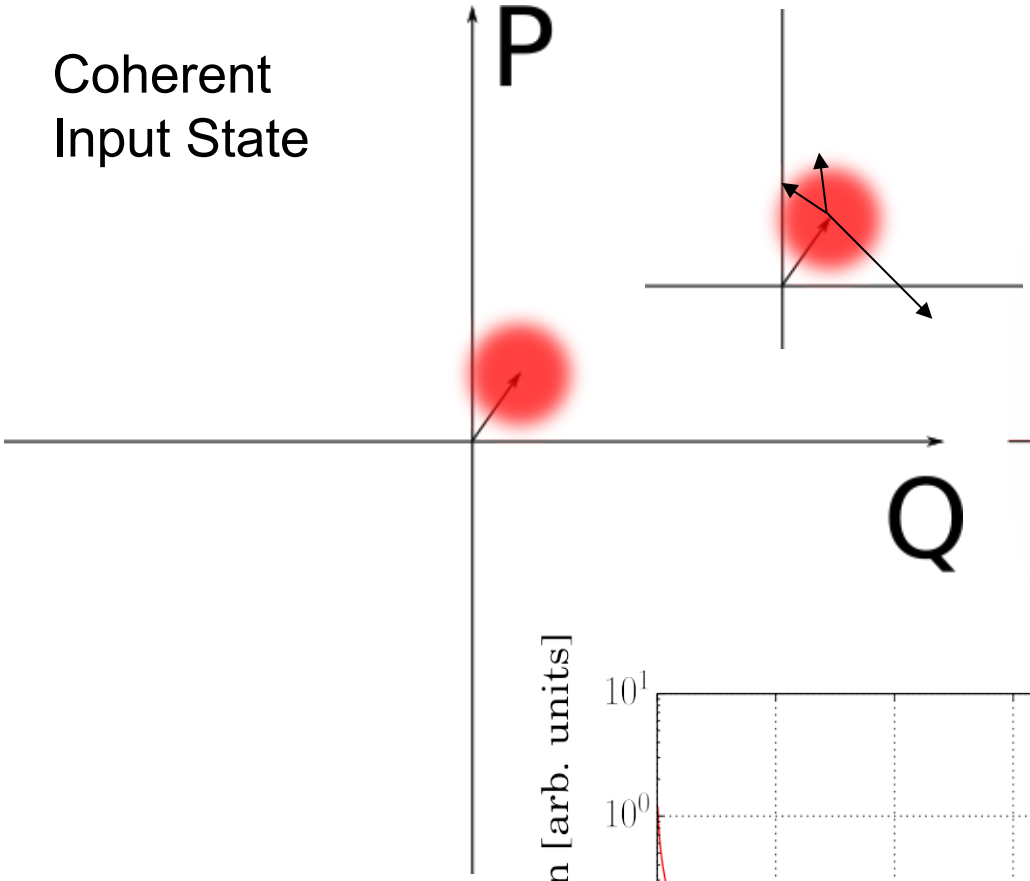
Quantum Computing on Encrypted Data



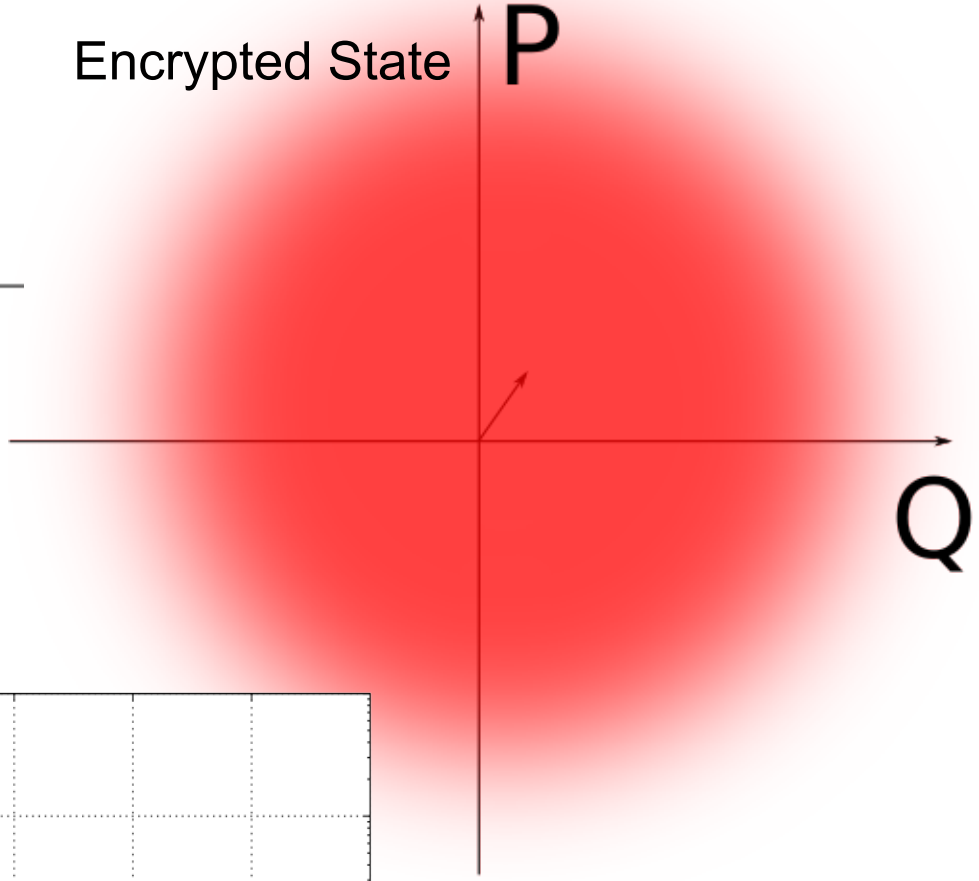
[1] L. Yu, et al., Phys. Rev. A 90, 050303 (2014)
[2] A. Broadbent, et al., in Foundations of Computer Science, 2009. FOCS '09. 50th Annual IEEE Symposium on (2009), 517, ISSN 0272-5428.

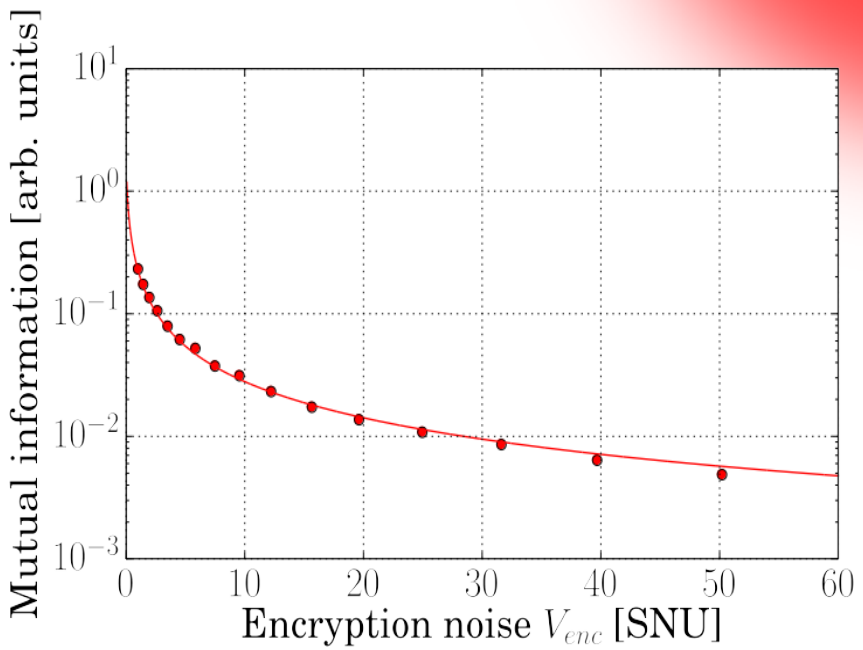
Encryption

Coherent
Input State



Encrypted State





A Continuous-Variable Universal Quantum Computer

Set of gates necessary for continuous-variable universal computing:

Displacement gates	Z(T), X(T)
“Squeezing” gate	$U_2(T)$
Cubic phase gate (“non-gaussian”)	$U_3(T)$
Fourier gate	F
Controlled-not gate	C_Z

Implementation of U_3 gate remains a challenge

Decryption

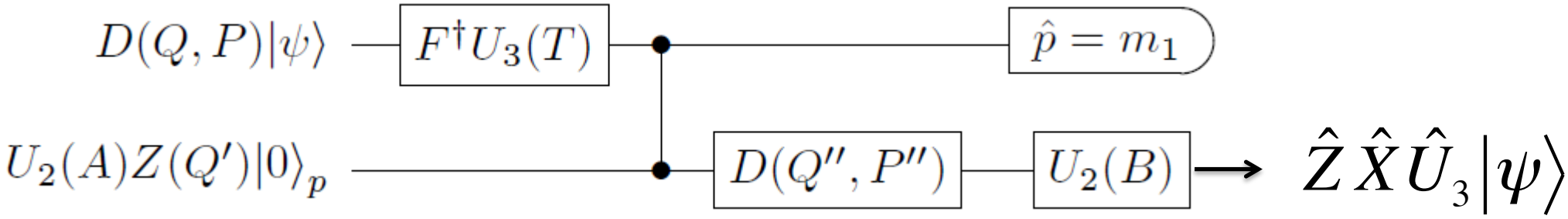
Decryption operation

Gate	Decryption Operation
Z(T)	X(-Q)Z(-P)
X(T)	X(-Q)Z(-P)
$U_2(T)$	X(-Q)Z(-2QT-P)
$U_3(T)$	$X(-Q)Z(3Q^2T-P)U_2(-3QT)$
F	X(P)Z(-Q)
C_Z	$X_1(-Q_1)Z_1(-Q_2-P_1) \otimes X_2(-Q_2)Z_2(-Q_1-P_2)$

For all Gaussian gates it is sufficient to use displacement operations to decrypt

$$\hat{C}_G \hat{G} \hat{D}(Q,P)\left|\psi\right\rangle = \hat{G}\left|\psi\right\rangle$$

The U_3 gate



A and Q' are randomly chosen by client
B depends on A and Q

Communication from Client to Server:

- Value of B

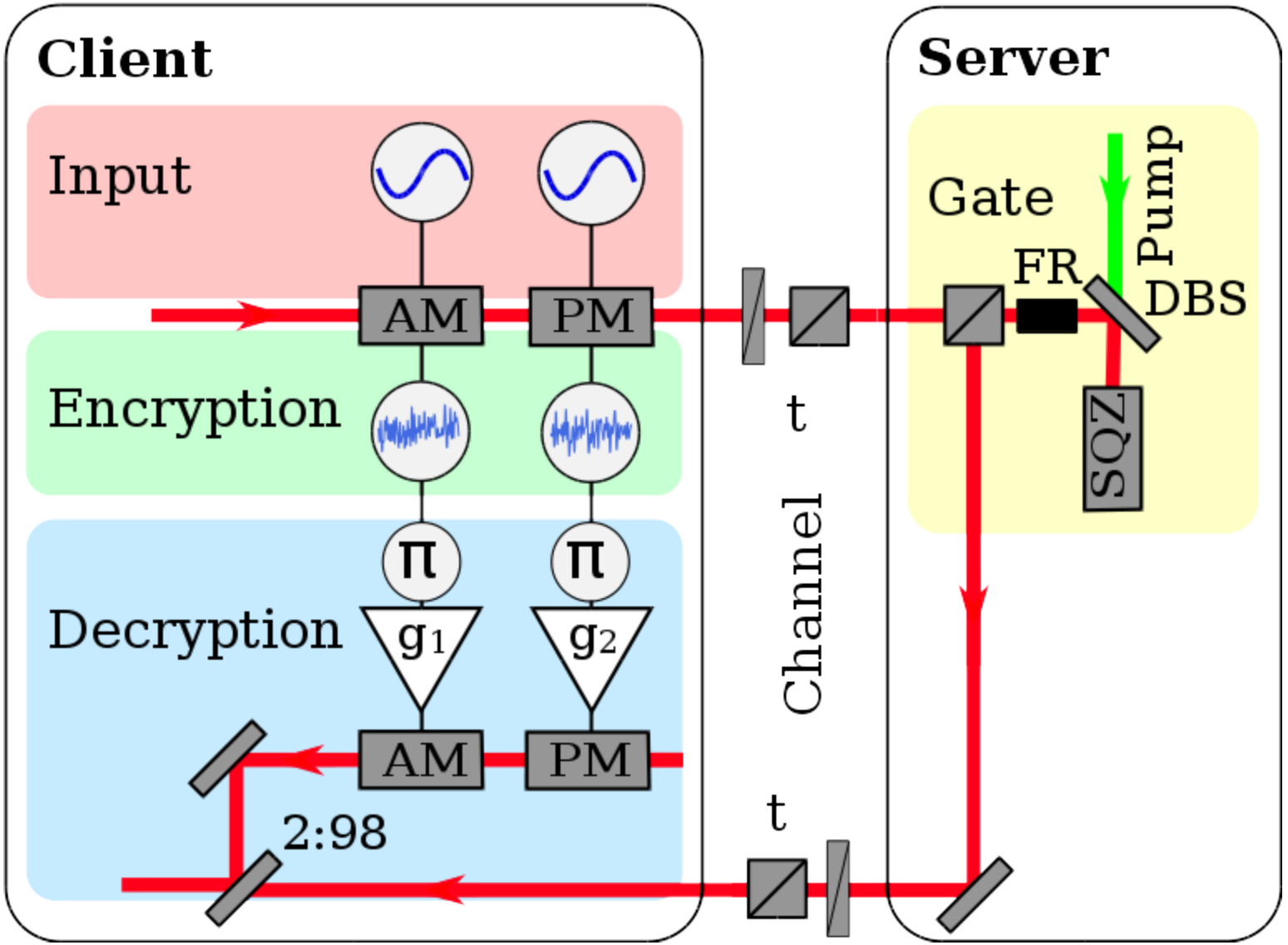
Communication from Server to Client:

- Value of m_1

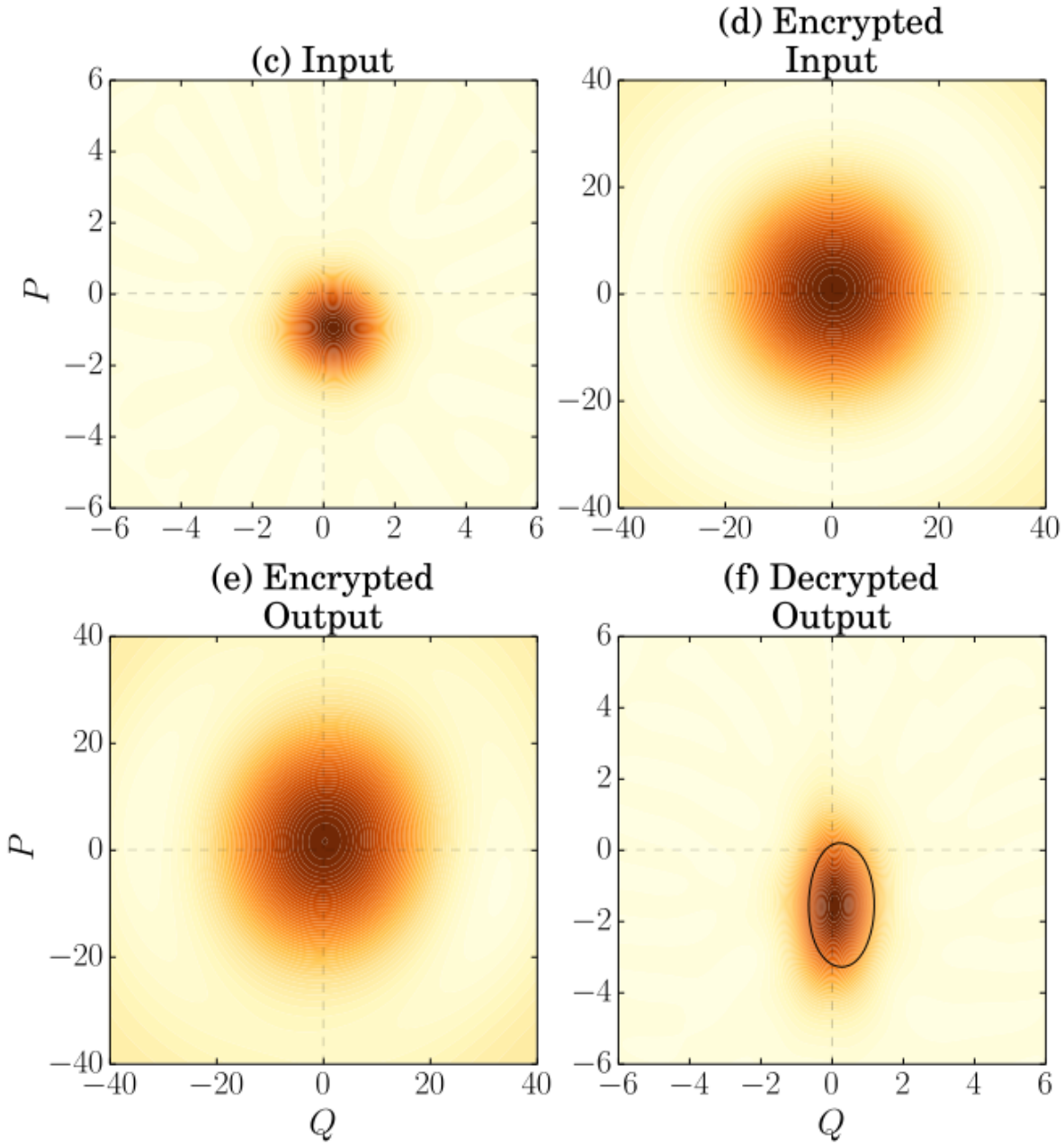
One round of classical communication needed for U_3 gate implementation

Experiment: Squeezing Gate

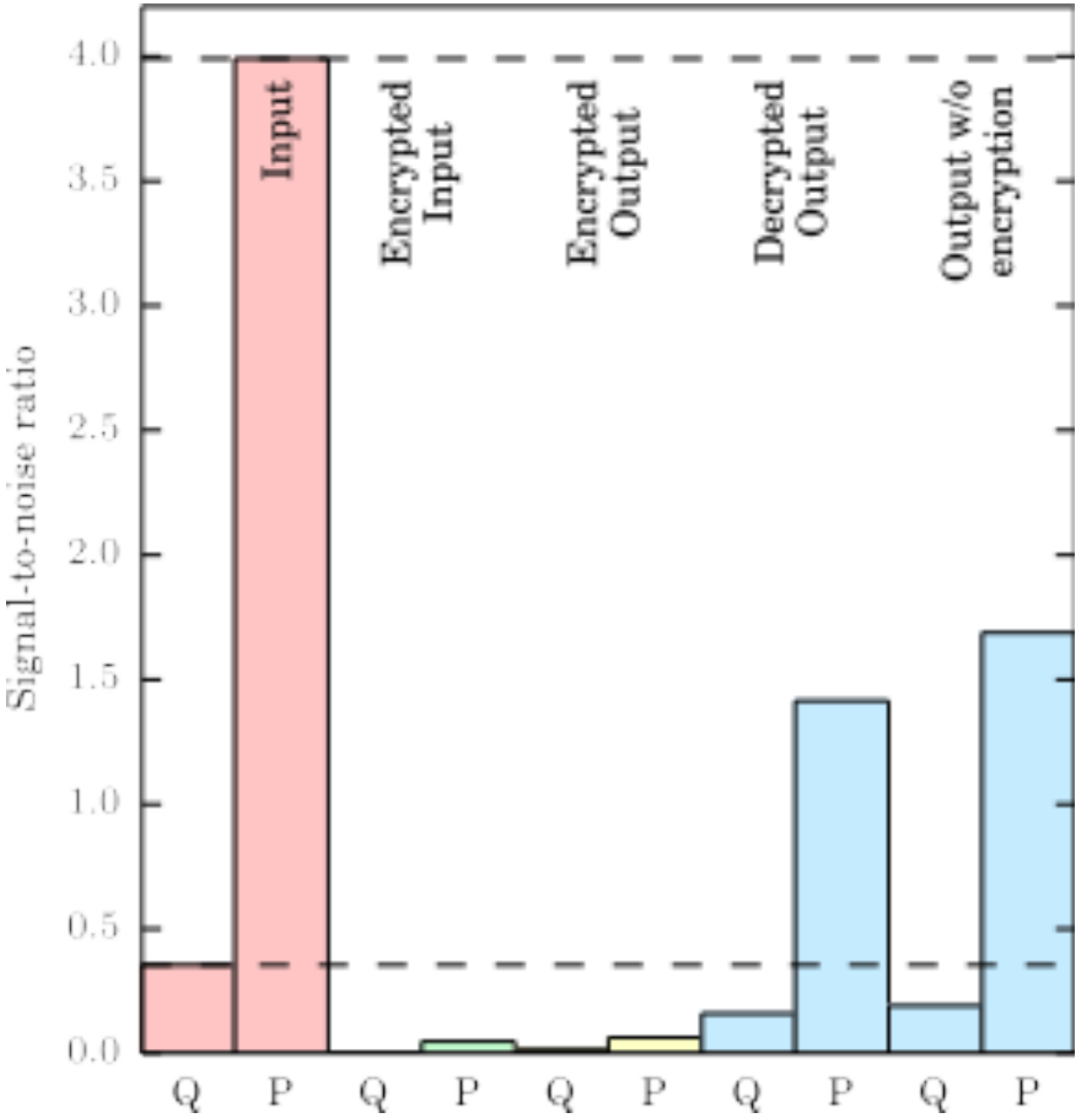
U_2 gate: phase shift, squeezing, phase shift



Results: Reconstructed Quantum States Step by Step

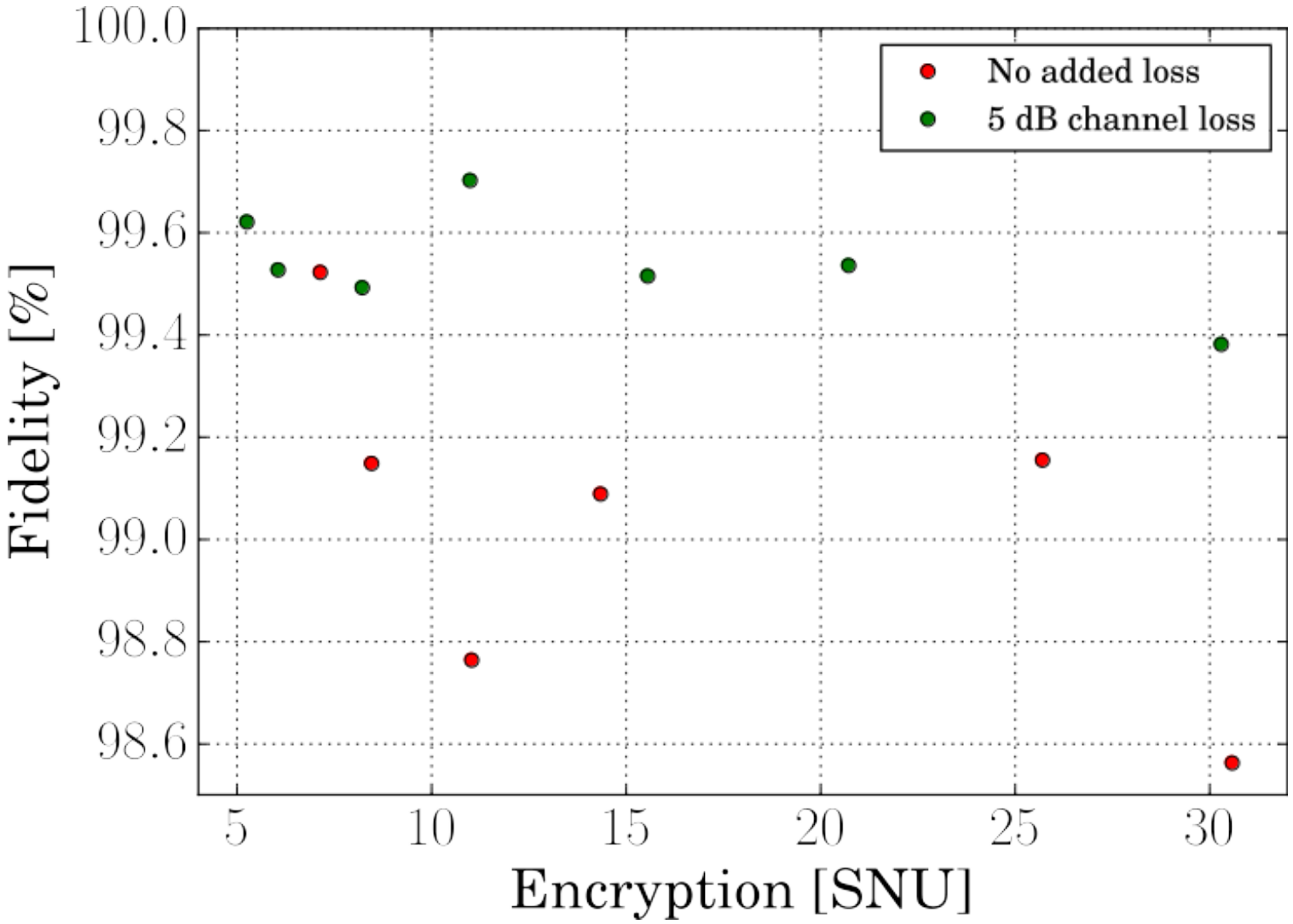


Signal-to-Noise Ratio



Fidelity

Comparion: How good does the encrypted protocol work versus the unencrypted one?



Conclusion & Outlook

Continuous-Variable Quantum Computing on Encrypted Data

- Simple encryption and decryption using displacements and no communication
-
- Exception: U_3 gate
  - U_3 gate implementation uses extra squeezing
  - One round of classical communication
  - Two modes from client to server

Remaining challenges:

- Formalized security proof (finite encryption variance leaks information)
- Implementation of U_3 gate

ArXiv: 1607.07372