universität wien

Quantum advantage for probabilistic one-time programs

Marie-Christine Roehsner[1,*], Joshua A. Kettlewell[2,3,*], Tiago B. Batalhão[1,2,3,4]
Joseph F. Fitzsimons[2,3,5] and Philip Walther[1,5]

[1]University of Vienna, Faculty of Physics, Boltzmanngasse 5, 1090 Vienna, Austria
[2]Singapore University of Technology and Design, 8 Somapah Road, Singapore 487372
[3]Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, Singapore 117543
[4]Centro de Ciências Naturais e Humanas, Universidade Federal do ABC, Avenida dos Estados 5001, 09210-580, Santo André, São Paulo, Brazil
[5]Erwin Schrödinger International Institute for Mathematics and Physics, University of Vienna, 1090 Vienna, Austria

Nature Communications Volume 9, 5225 (2018) or arxiv.org/abs/1709.09724

What is a one-time program (OTP)?

- A function that can be executed once and only one
- One copy allows the user to learn f(x) for one x of his choice
- The user learns nothing about f(x’) for x’≠x

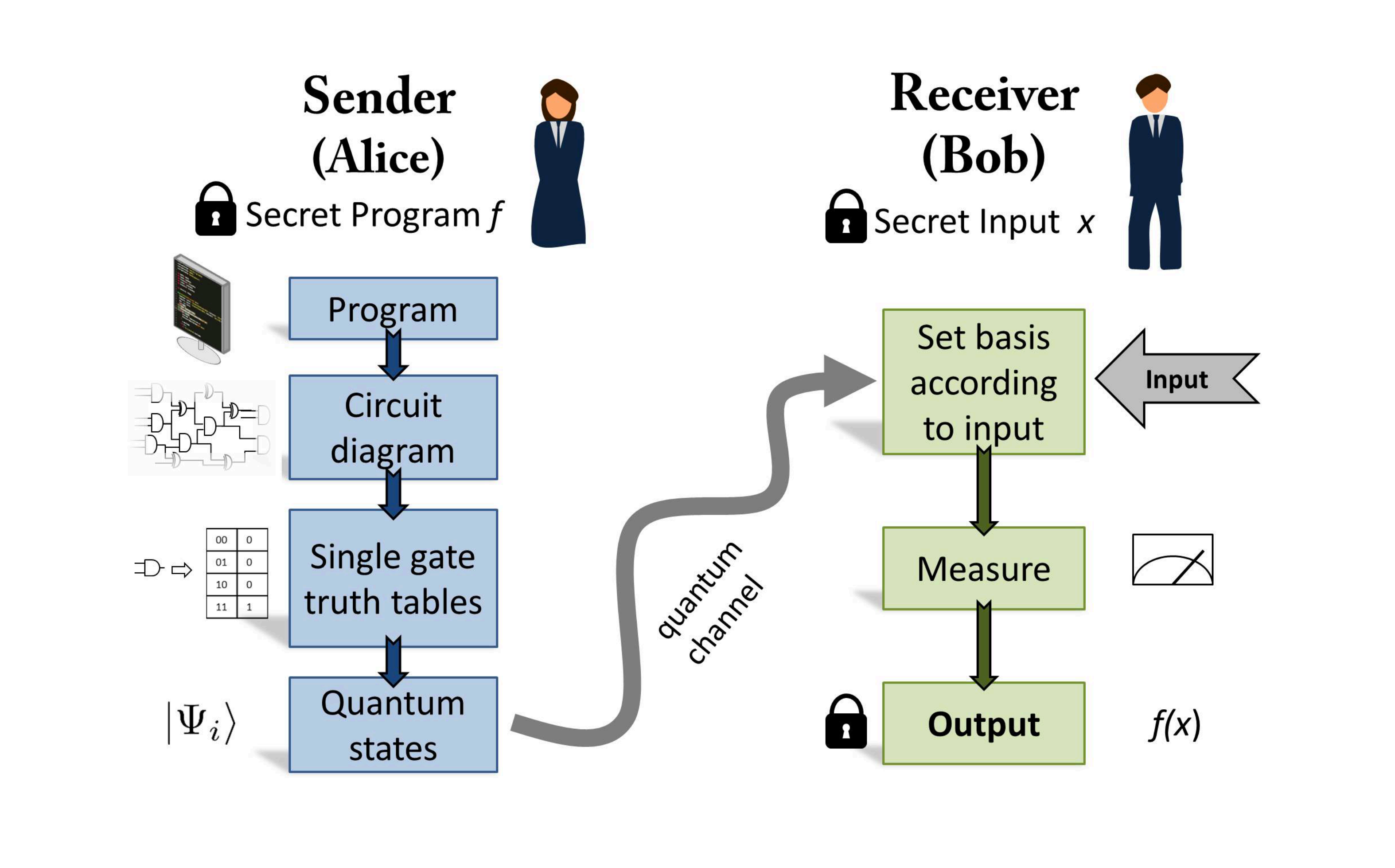
Previous work

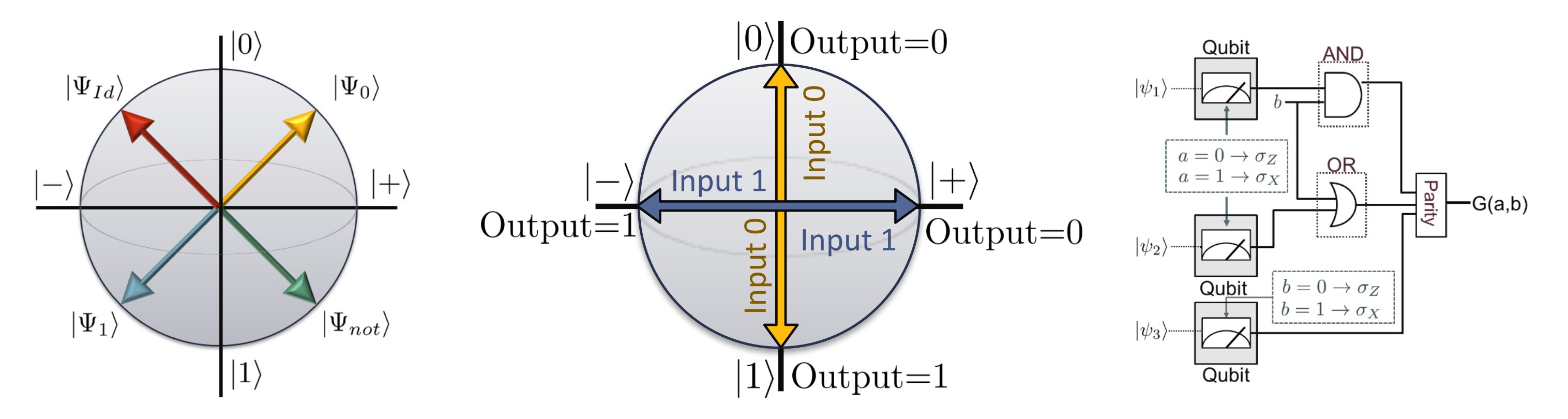
- Classical one-time programs are only possible using one-time hardware
- Perfect, information theoretically secure, quantum one-time programs are impossible

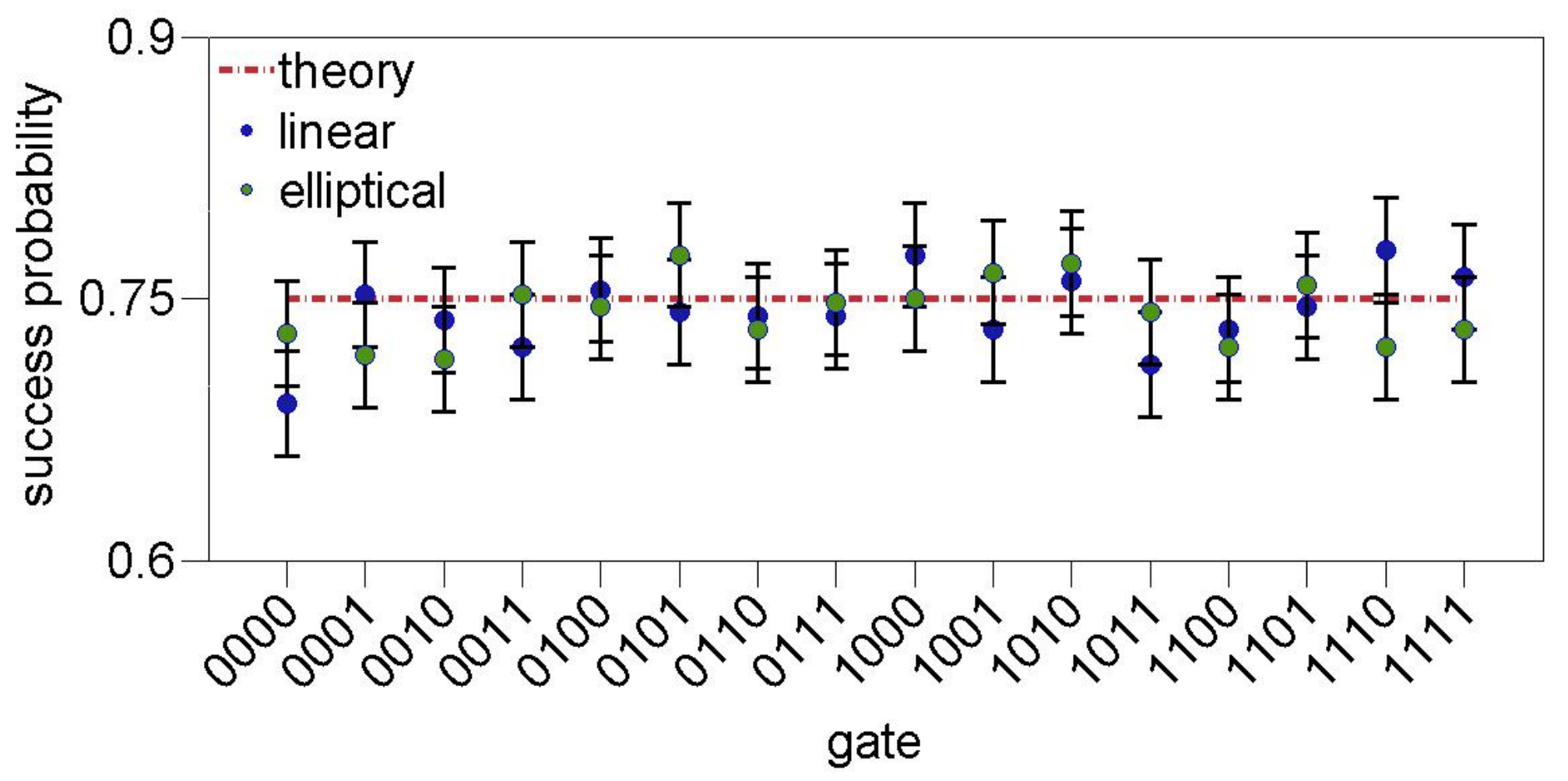
Goldwasser et al., *One-time programs.* Advances in Cryptology - CRYPTO 2008
Broadbent et al., *Quantum One-Time Programs.* Advances in Cryptology - CRYPTO 2013

Our scheme

- **Probabilistic:** Allowing for error in the outcome circumvents no-go results
- **Hybrid:** We use quantum states to encode classical software
- **Practical:** We only use single-qubit states
- **Secure:** Our protocol is information theoretically secure







The encoding

1. Alice breaks her classical software down to 2-input 1-output logic gates
2. Each of those gates can be encoded using three single bit gates plus a fixed classical circuit
3. The single bit gates are encoded as quantum states and sent to Bob
4. Bob measures the gates in one of two bases depending on his input
5. The output of the measurement corresponds to the output of the gate
6. They repeat this until the whole program is implemented

Success probability

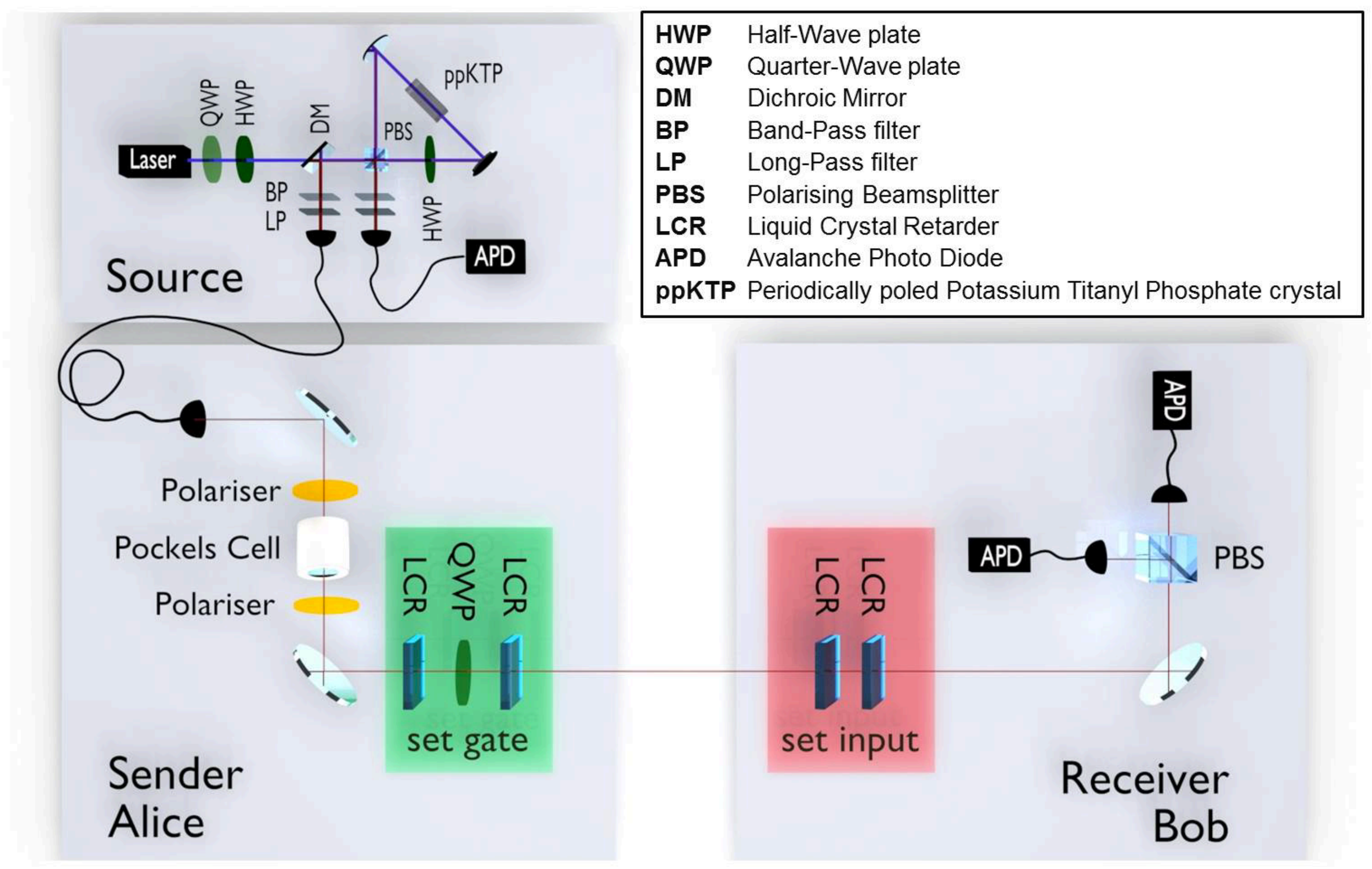
- **Single bit gates:** 85.36%
- **2-input 1-output gates:** 75%
- Experiment in good agreement with theoretical predictions

The Experiment

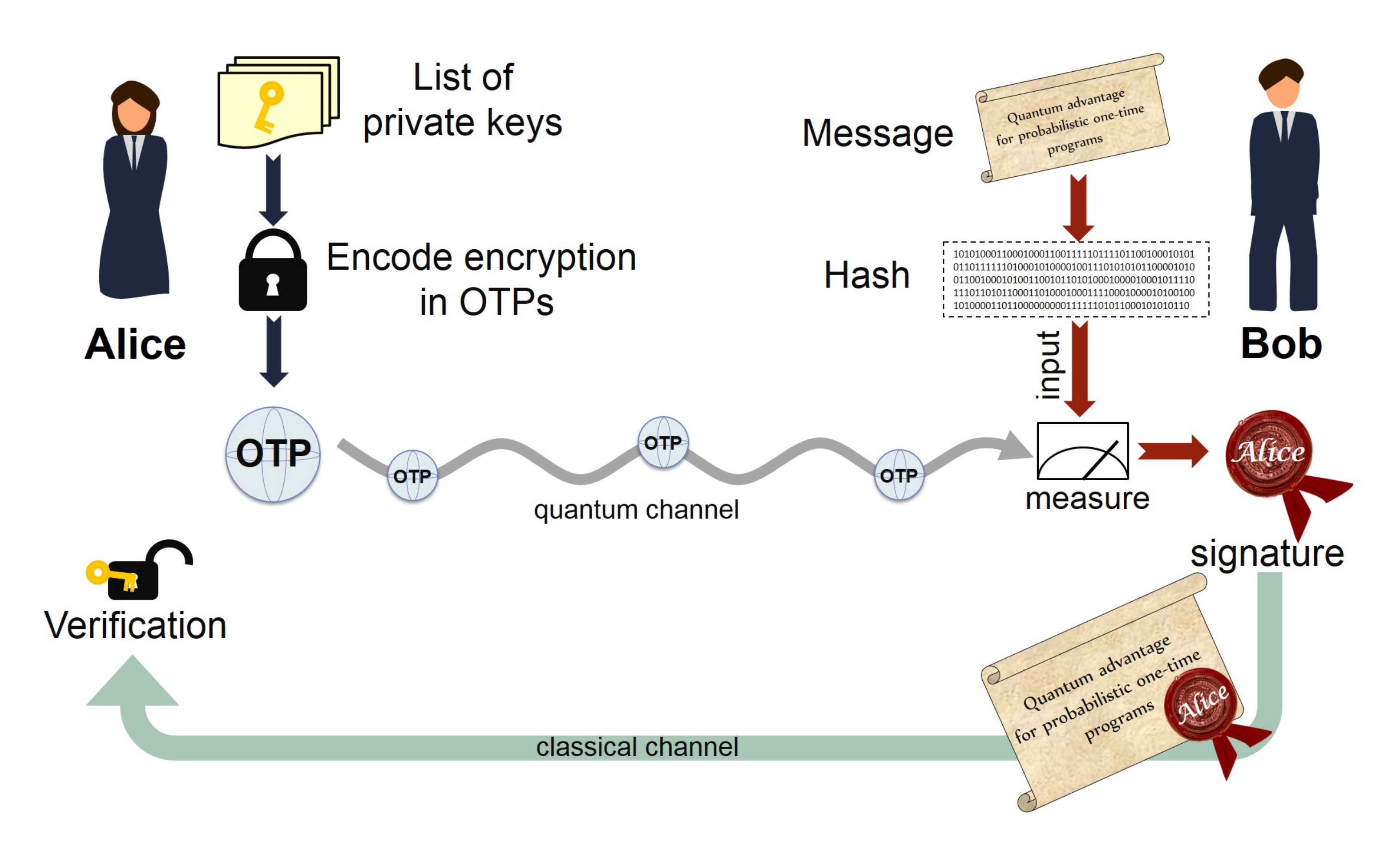
- **Qubits:** Polarisation of single photons
- **Source:** Heralded single photon source & fast switch to control photon transmission
- **State preparation:** the gate states are set by LCRs and a fixed QWP
- **Measurement basis:** Bob uses LCRs to set his measurement basis

Dealing with losses

Photon losses could compromise the security of the scheme, so we developed a subroutine that makes the protocol loss tolerant:
For the each gate Alice produced a random bit *c* and if
c=0 she sends the original quantum state
c=1 she sends the orthogonal state
} *Maximally mixed state*
Only after Bob announces which states he received Alice reveals *c*

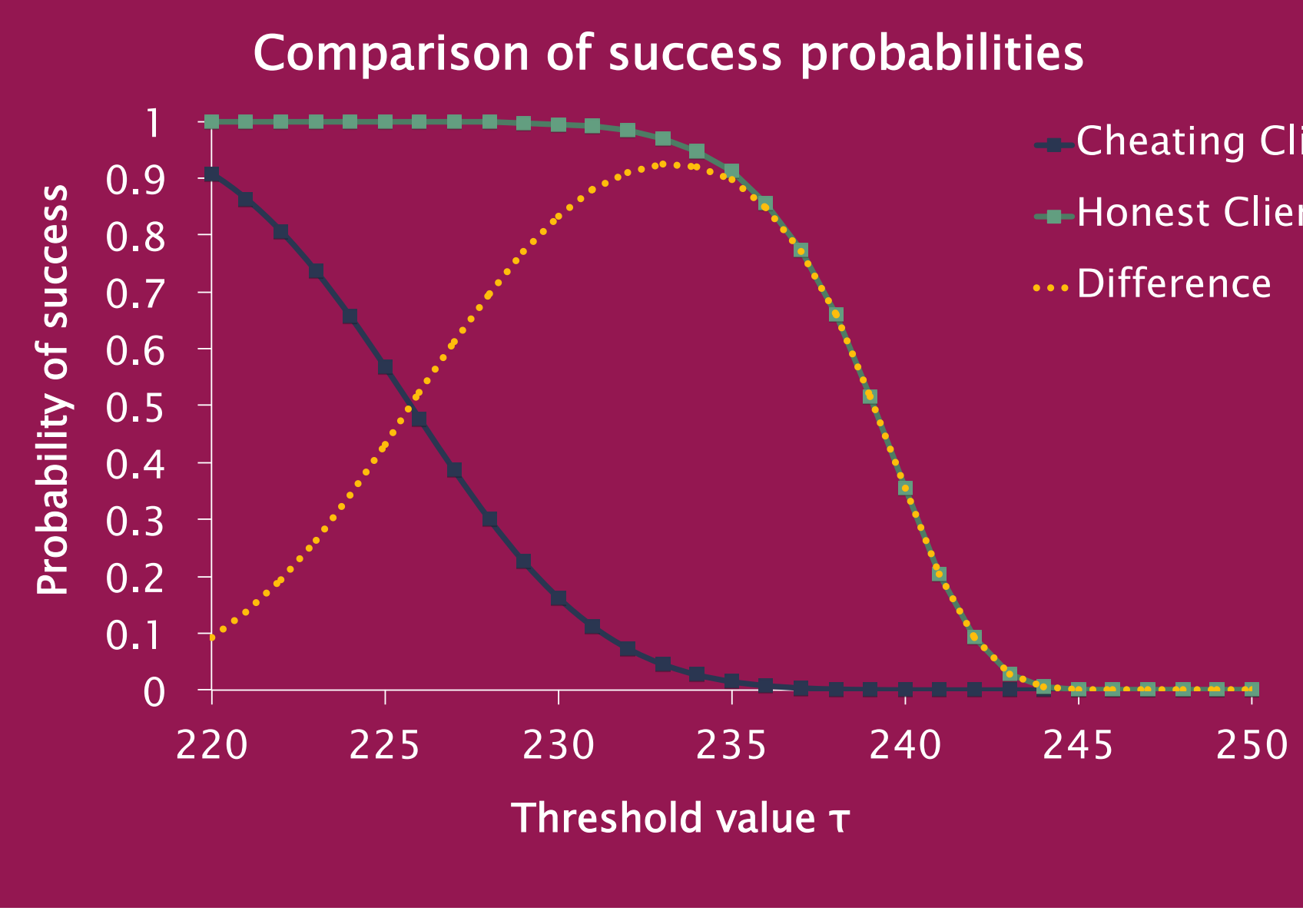


HWP	Half-Wave plate
QWP	Quarter-Wave plate
DM	Dichroic Mirror
BP	Band-Pass filter
LP	Long-Pass filter
PBS	Polarising Beamsplitter
LCR	Liquid Crystal Retarder
APD	Avalanche Photo Diode
ppKTP	Periodically poled Potassium Titanyl Phosphate crystal


List of private keys
Alice
Encode encryption in OTPs
OTP
OTP
OTP
OTP
quantum channel
Verification
Message
Quantum advantage for probabilistic one-time programs
Hash
input
measure
Bob
Alice
signature
classical channel
Quantum advantage for probabilistic one-time programs
Alice

One-time digital signatures

- Alice grants Bob one-time power of attorney
- OTPs are used to create the signature (later be verified by Alice)
- Compensation for probabilistic nature: Alice sends many individual encryptions to create one signature - if the expected percentage of signature outcomes is correct she accepts
- By increasing the number of copies the success probability can get the overall success probability arbitrarily close to one



universität wien
VDS VIENNA · DOCTORAL · SCHOOL · PHYSICS
VCQ Vienna Center for Quantum Science and Technology
AFOSR
FWF Der Wissenschaftsfonds.
FFG Forschung wirkt.
TURIS
ESI Erwin Schrödinger International Institute for Mathematics and Physics
UNIQORN Affordable Quantum Communication for Everyone