Near-maximal Polarisation Entanglement for Device-Independent Quantum Key Distribution at 2.1 μm

Adetunmise Charles Dada\textsuperscript{1,2}, Jędrzej Kaniewski\textsuperscript{3}, Corin Gawith\textsuperscript{3}, Martin Lavery\textsuperscript{3}, Robert H. Hadfield\textsuperscript{2}, Daniele Faccio\textsuperscript{4}, and Matteo Clerici\textsuperscript{2}

1. James Watt School of Engineering, University of Glasgow, Glasgow G12 8QQ, UK.
2. Faculty of Physics, University of Warsaw, Pasteura 5, 02-093 Warsaw, Poland
4. School of Physics and Astronomy, University of Glasgow, Glasgow G12 8QQ, UK.
\textsuperscript{†}adetunmise.dada@glasgow.ac.uk

I. Introduction and Motivation

\begin{itemize}
\item Quantum-enhanced optical systems operating within the 2–2.5 μm region have the potential to revolutionize emerging applications in communications, sensing and metrology.
\item However, until now, sources of entangled photons have been realized mainly in the near-infrared 700–1550 nm spectral window.
\item Above 2 μm lies an atmospheric transparency window with nearly one-third of the solar blackbody radiation of what is typical at telecom wavelengths [1] (see Fig. 1).
\item This makes the 2–2.5 μm spectral region highly promising for quantum-secured links, such as for daylight satellite-to-ground and satellite-to-satellite quantum communications.
\item Guided-wave optics is also rapidly developing into the 2-μm region to satisfy the need for larger bandwidths due to the increasing volumes of data traffic.
\item Solutions such as novel hollow-core photonic bandgap fibres working in the mid-infrared offer reduced optical nonlinearities and lower losses and are currently under test for network implementations.
\end{itemize}

II. Summary of Key Results

\begin{itemize}
\item Using custom-designed lithium niobate crystals for opportunistic parametric down-conversion and tailored superconducting-nanowire single-photon detectors, we demonstrate:
\item Full-state quantum tomography and near-maximal two-photon entanglement at 2.1μm.
\item Capability of the measured state for device-independent (DI) quantum key distribution (QKD).
\end{itemize}

III. Experimental Setup

\begin{itemize}
\item The setup consists of mirrors (M1, M2), attenuator/energy controller (EC), lenses (L1 and FC1,2), the PPLN crystal (C), Ge filter (F0), a D-shaped pickoff mirror (D), 50-mm passband filters (F1,2), halfwave plates (H1,2), quarter-wave plates (Q1,2), polarizers (P1,2), single-mode fibers (SMF1,2), superconducting nanowire single-photon detectors (SNSPD1/2).
\item We used periodically poled, magnesium-doped lithium niobate crystals (MgO-PPLN; Covesion Ltd.), with lengths 1 mm and 0.3 mm cut for type-0 and type-2 phase matching, respectively.
\end{itemize}

IV. Coincidence to Accidents Ratio

\begin{itemize}
\item Measured coincidence-to-accidental ratio (CAR) as a function of the averaged single count rates between detectors 1 and 2, for the (a) type-0 and (b) type-2 sources. The insets show the plots on logarithmic scales.
\item The 'single' counts include the detector dark count rates of ≈500 Hz in each arm.
\item For the type-0(2) measurement, we projected the state onto |V,V⟩(H,H) and measured a CAR of 607 ±105 (354±127), ~3 times the state-of-the-art.
\end{itemize}

V. Quantum State Tomography

\begin{itemize}
\item The integration time was 30 minutes for each measurement.
\end{itemize}

VI. Entanglement @ 2.1μm & Suitability for DI QKD

We obtain:
\begin{itemize}
\item CHSH-Bell parameter \( S = 2.7 ± 0.03 > 2 \) (local bound)
\item Entanglement of Formation: \( E = 0.6746 \)
\item Concurrence: \( \sqrt{E} = 0.7642 \)
\end{itemize}

Self-testing for singlet state:
\begin{itemize}
\item Threshold for CHSH Bell parameter \( \sqrt{S'} = (16 + 4\sqrt{2})/17 = 2.11 \), and \( S' > S \)
\end{itemize}

Weak form of Self-testing [6]
\begin{itemize}
\item Certifies the quantum state without full determination of the measurement.
\item Not previously been addressed experimentally
\item We show a violation of the three-setting inequality with \( E = 4.777 ± 4 \) (local bound)
\end{itemize}

For an Ekert91-based QKD protocol [7], we compute:
\begin{itemize}
\item Quantum bit error rate (QBER): 5.43%.
\item Lower bound on the DI secure key rate: \( R = 0.417 \) bits/pair > 0
\end{itemize}


Funding:
EPSRC IAA (EP/R511705/1); UKRI (Fellowship “InTempo” EP/S001573/1); HOMING programme of the Foundation for Polish Science; European Regional Development Fund. EPSRC Quantum Communications hub EP/T001011/1, Royal Academy of Engineering Chairs in Emerging Technologies scheme.

For more details, please see [1] or scan the QR code to read the paper.