

# Secure Quantum Clock Synchronization

Jianwei Lee, Lijiong Shen, Alessandro Cerè, James Troupe,  
Christian Kurtsiefer, Antia Lamas-Linares



# Timing Consistency

## Financial Markets

- Between buyers and sellers

- Sub-millisecond accuracy

## Global Positioning

- Between satellites and receivers

- Few nanosecond accuracy

# Synchronisation of Remote Clocks

Distribution of Time and Frequency

Alice



$t$

Bob

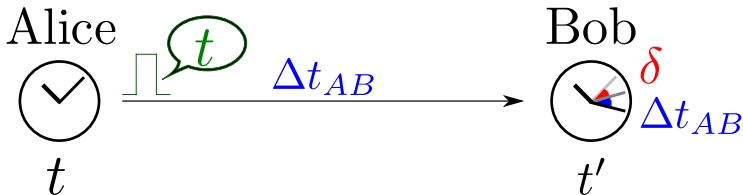


$\delta$

$t'$

# Time Distribution

## One-Way Synchronisation



$$\Delta t_{AB} = \frac{\text{Distance}}{c_n}$$

$$\delta = t' - t - \Delta t_{AB}$$

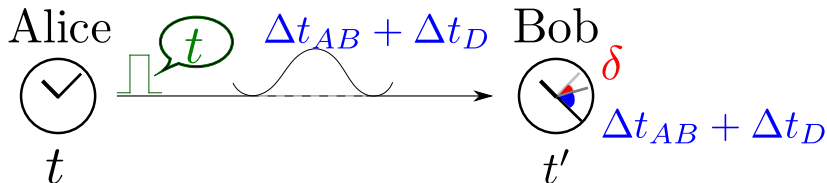
---

<sup>1</sup> Narula, L. and Humphreys, T., arXiv:1710.05798 (2017)

<sup>2</sup> Used in Global Navigation Satellite Systems

# One-way Synchronisation

Cannot Detect Delays

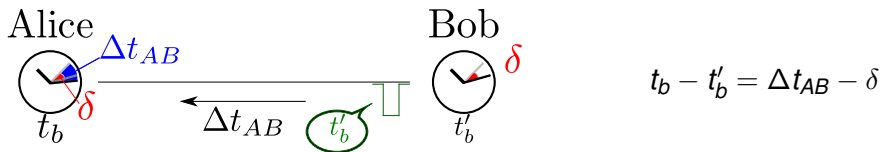
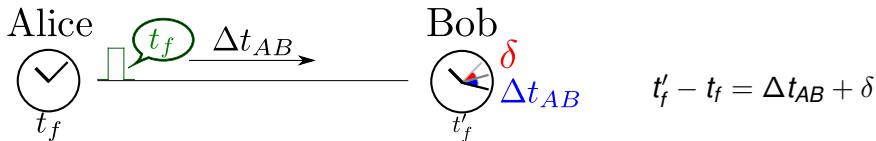


Bob unaware of additional delay  $\rightarrow$  wrong  $\delta$

Cannot be prevented by Authentication or Cryptography!

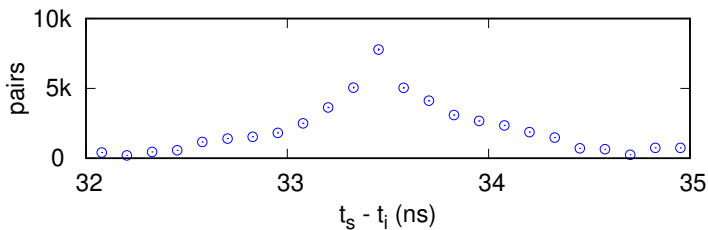
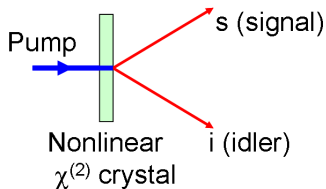
Security requires an independent distance measurement

# Distance-Independent Clock Synchronisation

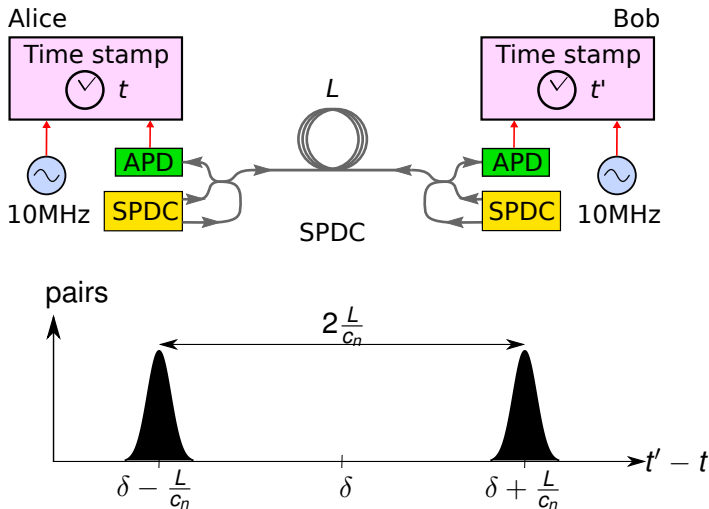


$$\delta = \frac{(t'_f - t_f) - (t_b - t'_b)}{2}$$

# Time-Correlated Photon Pairs from SPDC



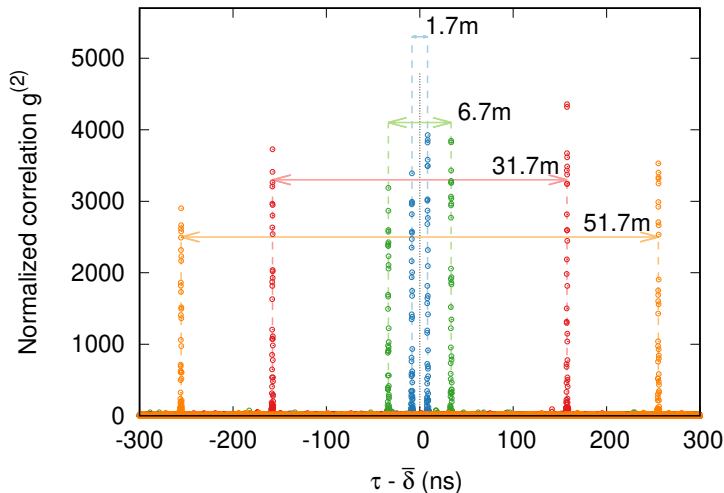
# Symmetric Clock Synchronisation with SPDC



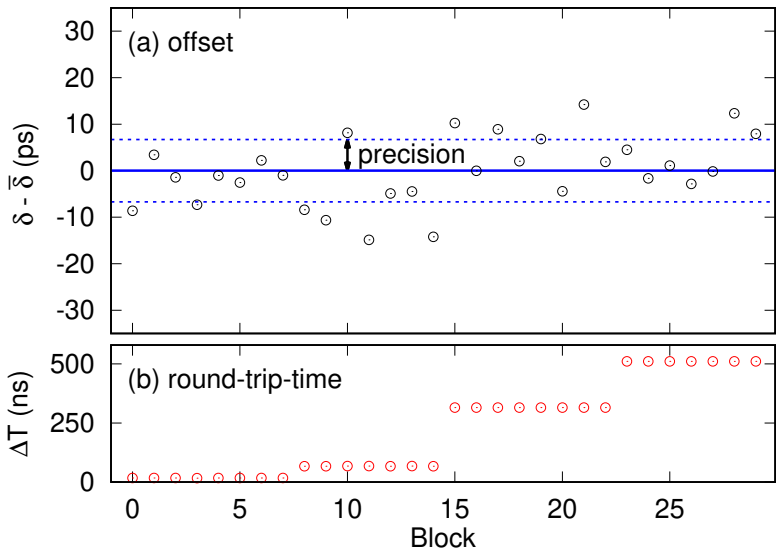


# Constant $\delta$ , Varying $L$

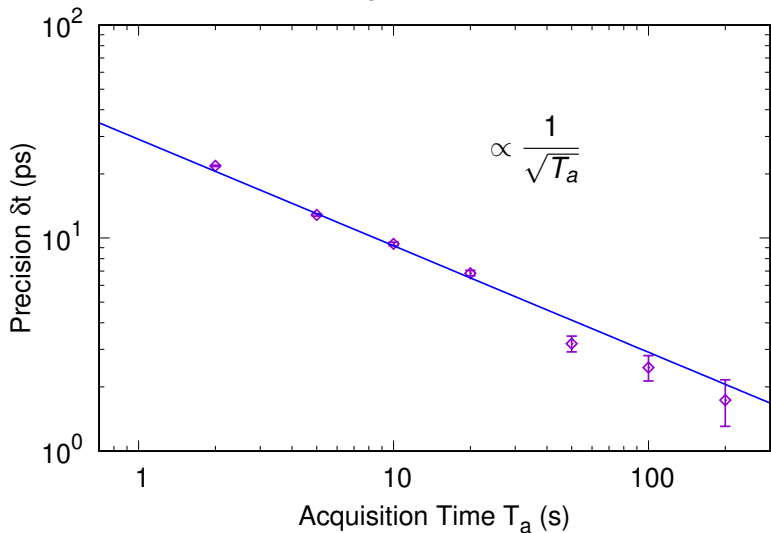
## Common Frequency Reference



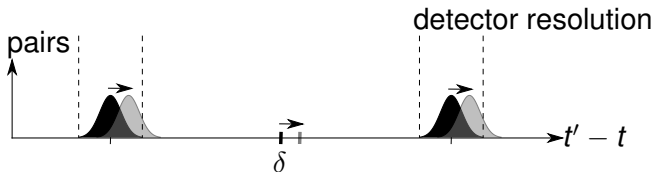
# Clock Synchronisation Independent of Distance



# Synchronization Precision over Acquisition Time



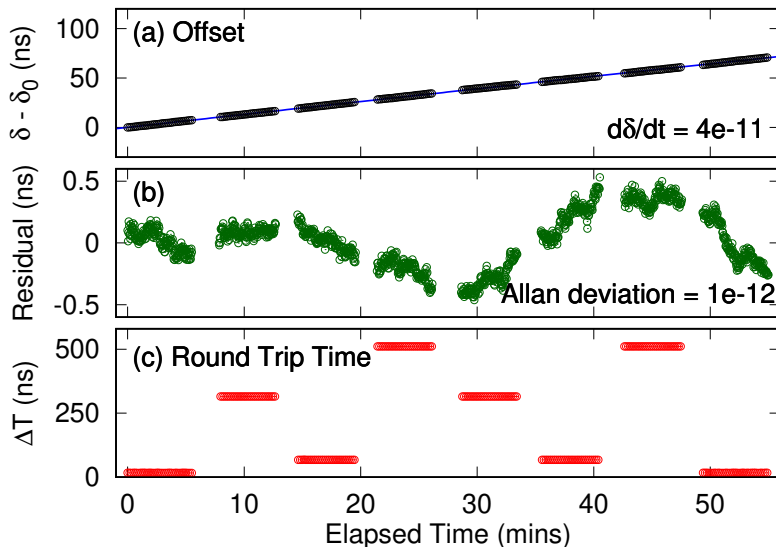
With Independent Frequency References  
the Clock offset  $\delta$  drifts with time



precision < peak drift < detector resolution

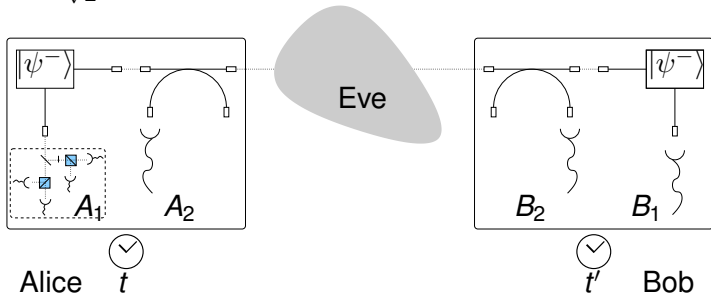
for 2 sec:      0.02 ns < 0.10 ns < 0.60 ns

# Drifting $\delta$ , Varying $L$ Independent Frequency References



# Secure Clock Synchronisation

$$|\psi^{-}\rangle = \frac{1}{\sqrt{2}} (|HV\rangle - |VH\rangle)$$



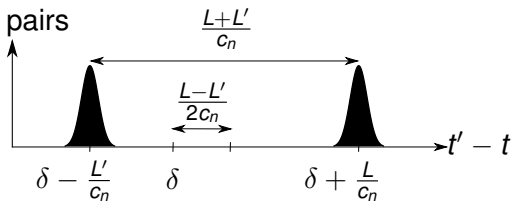
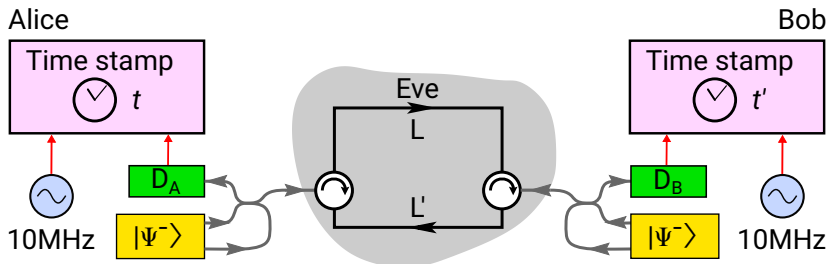
## Violation of Bell's Inequality:

Ensures photons detected are part of the same entangled pair

## Symmetric Clock Synchronisation:

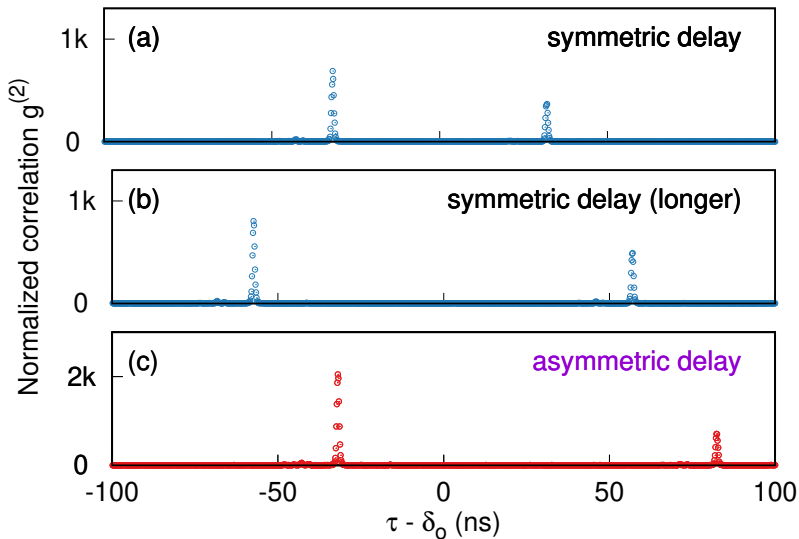
Ensures distance-independence of clock-differences

# Asymmetric Delay Attack



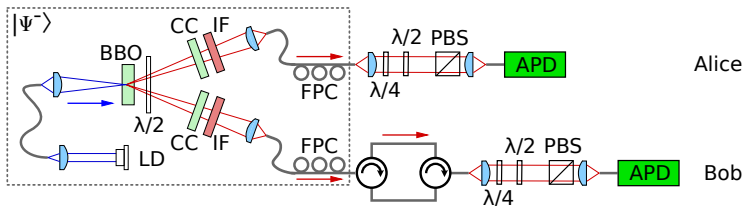
$\delta \neq$  midpoint between two coincidence peaks

# Estimated Offset Shift



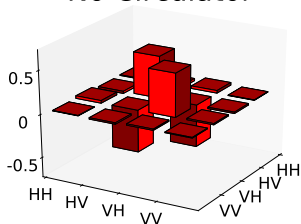


# State Tomography with Circulators

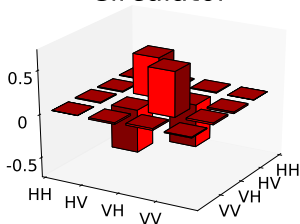


$$n \times 180^\circ \text{ rotation: } |\psi\rangle_B \rightarrow \pm |\psi\rangle_B \quad |\Psi^-\rangle \rightarrow \pm |\Psi^-\rangle$$

No Circulator



Circulator



# Summary

Remote clock synchronisation using two SPDC sources<sup>1</sup>

- Independent of separation

- Intrinsic Clock Instabilities can be resolved

- Does not require trustworthy estimate of separation

- Secure against Symmetric Delay Attacks

---

<sup>1</sup>Appl. Phys. Lett. 114, 101102 (2019)