Arts and Sciences / Department of Physics

Qubit-based clock synchronization for QKD systems using a Bayesian approach

Roderick D. Cochran and Daniel J. Gauthier

INTRODUCTION

Quantum key distribution (QKD) provides a method for two users to exchange a provably secure key. However, like any communication protocol, the two users must synchronize their data streams.

- **Qubit-based synchronization protocols** directly use the transmitted quantum states for synchronization
- Avoids the need for additional classical synchronization hardware.
- We use a **Bayesian probabilistic algorithm** that incorporates all published information to efficiently find the clock offset without sacrificing any secure key [1].

CLOCK OFFSET

The relative offset Δ between Alice and Bob's clocks after n communication bins is modeled with the equation

$$\Delta \;=\; t_0 \;+\; (\tau_A - \tau_B)n \;+ \varepsilon.$$

where τ_A and τ_B are Alice's and Bob's communication clock periods, t_0 is an initial timing offset, and ε is higher-order timing errors in n.

- We adjust for these accrued timing differences by regularly performing offset recovery

MODEL SYSTEM

We use an efficient three-state BB84 prepare-and-measure protocol with decoy states.

- Send only 3 polarization states: horizontal (H), left circular (L), and right circular (R)
- Send some states with a lower mean photon number (decoy states)

Figure 1

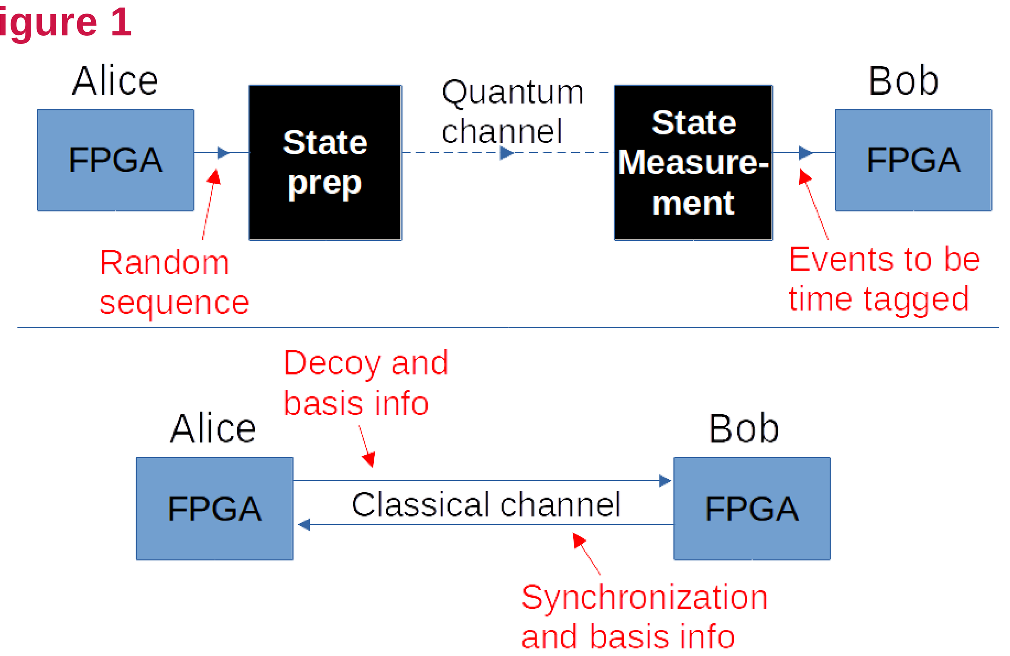


Figure 1:

- Alice sends qubits to Bob who measures and timetags them
- After the measurement phase, Alice shares decoy and basis info. Bob uses these to find the synchronization, then shares the synchronization and basis info

QUBIT-BASED SYNCHRONIZATION ALGORITHM

We divide Alice's published information into sufficiently short batches N that the relative clock offset Δ is approximately constant.

- Uses **Fast Fourier Transforms** to count the number of each unique event pairing for each potential offset Δ (*e.g.,* Alice sends a decoy state in the H/V basis and Bob records an H state).
- Generates **probability lookup tables** for all the different Alice/Bob event combinations
- Uses all knowledge of the system characteristics: state fidelities, mean photon numbers, channel loss, etc.

Using Bayesian analysis, we find the **synchronization probability** in the **low mean photon number limit:**

$$p(S_j|B_1,\ldots,B_{M+N}) \approx \frac{\prod_{k=1}^{j-1} p(B_k|\bar{S}_j) \prod_{k=j}^{j+N} p(B_k|S_j) \prod_{k=j+N+1}^{M+N} p(B_k|\bar{S}_j)}{\sum_{i=1}^{M}\left(\prod_{k=1}^{i-1} p(B_k|\bar{S}_i) \prod_{k=i}^{i+N} p(B_k|S_i) \prod_{k=i+N+1}^{M+N} p(B_k|\bar{S}_i)\right)}$$

SIMULATIONS

We use simulated data to test how well our algorithm performs with various dark counts and channel transmissions.

Figure 2:

- How the predicted synchronization confidence p matches the actual frequency f of finding the correct offset
- Note $1-p$ better illustrates the transition to high-certainty synchronization.
- Synchronization confidence increases with N
- p matches f best at the lower value of μ.

Figure 2

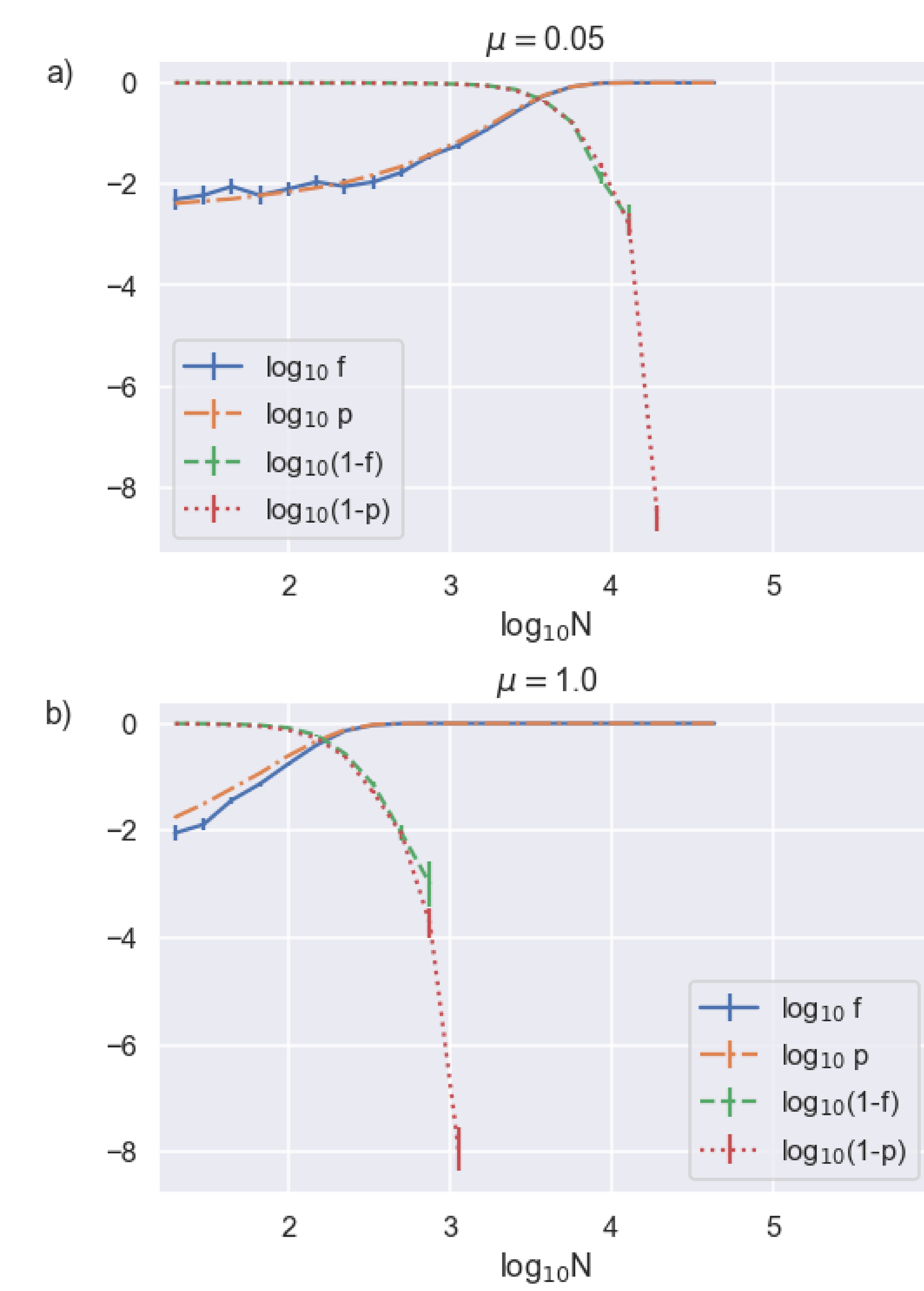


Figure 3:

- For higher values of μ, the synchronization converges to 1 at a lower value of N

Figure 3

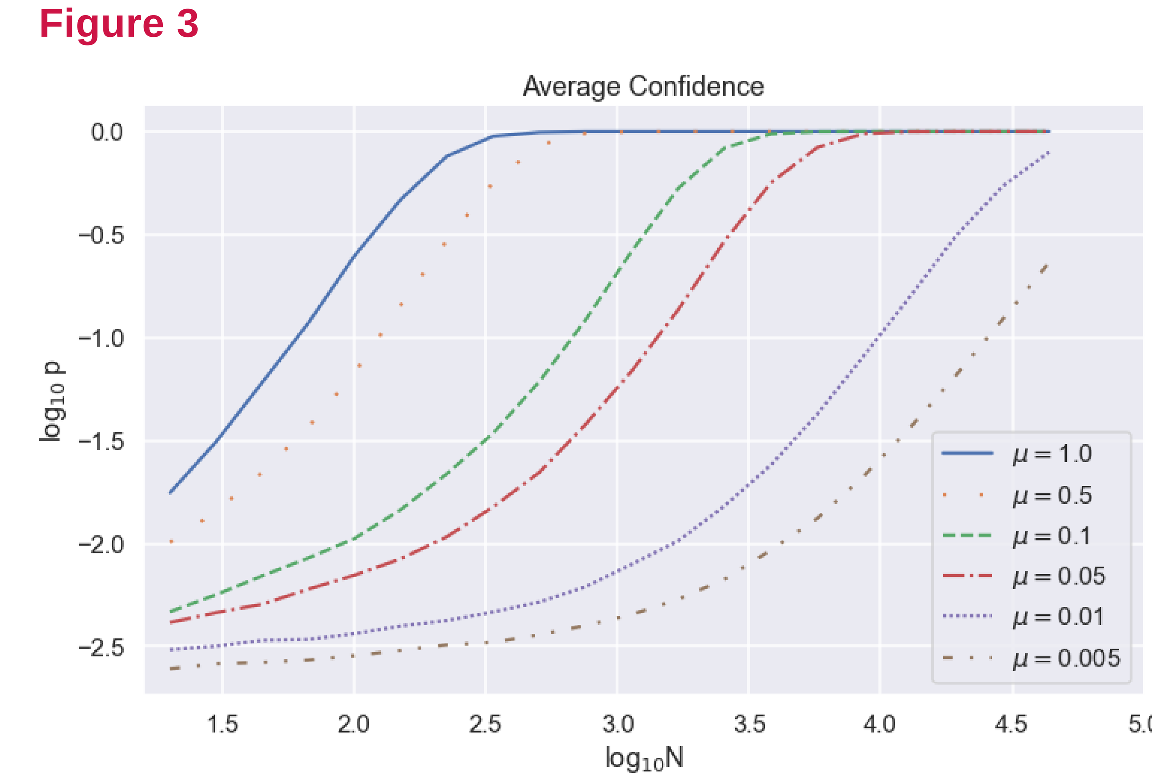
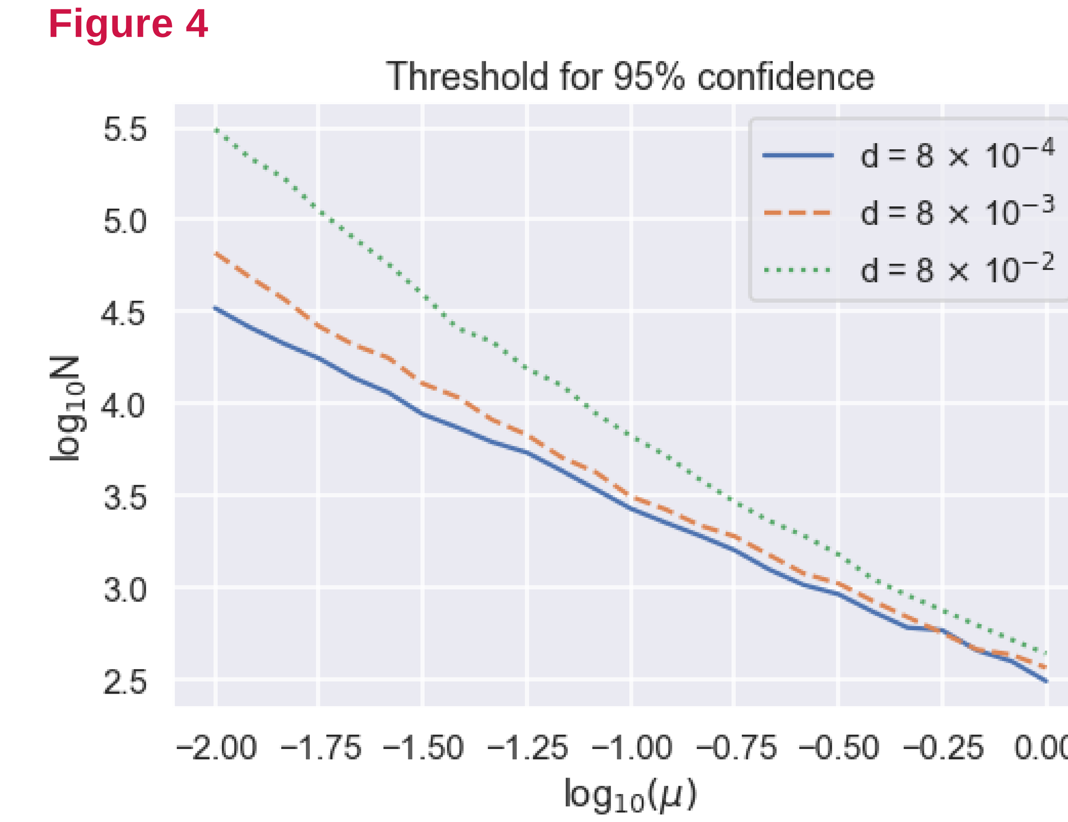


Figure 4:

- The batch length N necessary to achieve 95% confidence is inversely proportional to μ.
- This proportionality changes with different dark count rates d.

Figure 4



CONCLUSIONS

In conclusion, we develop a novel probabilistic approach to qubit-based clock synchronization using Bayesian analysis. By exploiting correlations between information Alice already shares publicly, such as basis and decoy state choices, and Bob's detection events, we can find the correct synchronization clock offset without sacrificing any secret key.

E-mail: **cochran.467@osu.edu**
Address: Physics Research Building, 191 W Woodruff Ave, Columbus, OH, 43210

BIBLIOGRAPHY

1 Cochran, R.D.; Gauthier, D.J. Qubit-Based Clock Synchronization for QKD Systems Using a Bayesian Approach. Entropy 2021, 23, 988. https://doi.org/10.3390/e23080988

ACKNOWLEDGEMENTS

This material is based on research sponsored by NASA under grant 80NSSC20K0629 and the Air Force Research Laboratory and the Southwestern Council for Higher Education under agreement FA8650-19-2-9300. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright notation thereon. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of NASA, the Southwestern Council for Higher Education and the Air Force Research Laboratory (AFRL), or the U.S. Government.