**Supplemental content:**

**SIG-DB: leveraging homomorphic encryption to Securely Interrogate privately held Genomic DataBases**

Alexander J. Titus1,2,\*, Audrey Flower3, Patrick Hagerty4, Paul Gamble3, Charlie Lewis5, Todd Stavish3, Kevin P. O’Connell1, Greg Shipley5, and Stephanie M. Rogers1

1B.Next, In-Q-Tel, Arlington, VA, USA

2Quantitative Biomedical Sciences, Dartmouth College, Hanover, NH, USA

3Lab41, In-Q-Tel, Arlington, VA, USA

4CosmiQ, In-Q-Tel, Arlington, VA, USA

5Cyber Reboot, In-Q-Tel, Arlington, VA USA

\*Corresponding author: bnext@iqt.org

**Abstract**

Genomic data are becoming increasingly valuable as we develop methods to utilize the information at scale and gain a greater understanding of how genetic information relates to biological function. Advances in synthetic biology and the decreased cost of sequencing are increasing the amount of privately held genomic data. As the quantity and value of private genomic data grows, so does the incentive to acquire and protect such data, which creates a need to store and process these data securely. We present an algorithm for the Secure Interrogation of Genomic DataBases (SIG-DB). The SIG-DB algorithm enables databases of genomic sequences to be searched with an encrypted query sequence without revealing the query sequence to the Database Owner or any of the database sequences to the Querier. SIG-DB is the first application of its kind to take advantage of locality-sensitive hashing and homomorphic encryption to allow generalized sequence-to-sequence comparisons of genomic data.

**Supplemental Figure 4:**

A

B

C