In fully homomorphic encryption, the noise grows during the computation. To reduce the noise, we use bootstrap operations.

Problem

Minimize the number of bootstrap operations so that the noise is at most $L \in \mathbb{N}$ at every gate.

Input (with $L = 2$):

\[
\begin{array}{c}
\text{noise calculation:} \\
\text{max}(\cdot, \cdot) \\
1 + \text{max}(\cdot, \cdot) \\
0
\end{array}
\]

Output:

Our Results (Benhamouda, Lepoint, Mathieu, Zhou, SODA’17)

- Polynomial-time $L$-approximation algorithm
- NP-hard for $(L - \epsilon)$-approximation under the Unique Games Conjecture

Technical novelty: new rounding scheme for the standard linear program