Running times

Given n-bit int. N:

- **Addition and subtraction in Z_N**: linear time $T_+ = O(n)$
- **Modular multiplication in Z_N**: naively $T_\times = O(n^2)$
- **Modular exponentiation in Z_N (g^x)**:

$$O\Big((\log x) \cdot T_\times \Big) \leq O\Big((\log x) \cdot n^2 \Big) \leq O(n^3)$$

Dan Boneh