differential privacy, but at what cost?
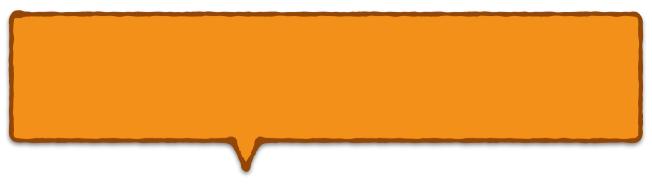
for any A, r, S,

$$\Pr[M(A) = S] \leqslant \exp(\text{epsilon}) \times \Pr[M(A \pm r) = S].$$

for any A, B, S,

$$\Pr[M(A) = S] \leq \exp(\text{epsilon} \times |A\text{-}B|) \times \Pr[M(B) = S].$$

**Strong bounds for similar input data.
Loose bounds for dissimilar data.**

but at what cost?

differential privacy,

Smooth transition from protection of small

groups to disclosure about large groups.

Controlled decay under multiple questions.

No cryptographic assumptions. (future proof)

No assumptions about attacker methodology.