Covert Channel [Haeberlin et al SEC ‘11]

• Key assumption in differential privacy implementations:
  – The querier can only observe the result of the query, and nothing else.
  – This answer is guaranteed to be differentially private.

• In practice: The querier can observe other effects.
  – We saw examples like timing channels.
Fix for Timing Channels

- Every query takes the same time
  - Unnecessary loss in throughput!
  - Or get no answer ...

- We can make the timing channel differentially private
Covert Channel [Haeberlin et al SEC ‘11]

• Key assumption in differential privacy implementations:
  – The querier can only observe the result of the query, and nothing else.
  – This answer is guaranteed to be differentially private.

• In practice: The querier can observe other effects.
  – Here is another one …
Laplace mechanism

Private Database

Noisy Answer

Aggregate Query: \( q \)

\( q(D) + \text{Lap}(S(q)/\varepsilon) \)

Analyst

e.g., COUNT

Sensitivity

-10
-5
0
5
10
Standard Implementation

\[ Y \leftarrow F^{-1}(U) = -\lambda \ln(1 - U) \]

- Exponential Distribution
- Uniformly random between [0,1)
- Random integer in \{0,1\}
- Laplace Distribution
- Uniformly random between (0,1)

\[ Y \leftarrow (2Z - 1) \cdot \lambda \ln(U) \]
Least significant bits and Laplace Mechanism [Mironov CCS ‘12]

• Suppose Laplace mechanism is implemented using standard floating point,
• Certain outputs are more likely than others

\[ x = 1 \odot \pi \quad \text{and} \quad x + 9 \cdot 2^{-54} \]

\[ \text{LN}(\cdot) \]

\[ \text{LN}(x) \quad \text{and} \quad \text{LN}(x + 9 \cdot 2^{-54}) \]
Least significant bits and Laplace Mechanism

• Suppose Laplace mechanism is implemented using standard floating point,
• Certain outputs may not appear.
Least significant bits and Laplace Mechanism

• Suppose Laplace mechanism is implemented using standard floating point,
• Both can happen simultaneously
Least significant bits and Laplace Mechanism

• Sensitivity computation under floating point is also tricky (assume left to right summation in the following example):

\[ n = 2^{30} + 1 \]

\[ x_1 = 2^{30}, x = -2^{-23}, \ldots, x_n = -2^{-23} \]

\[ f(x_1, \ldots, x_n) = \sum_{i=1}^{n} x_i = 2^{30} - 2^{30} 2^{-23} = 2^{30} - 128 \]

\[ f(x_1 + 1, \ldots, x_n) = x_1 + 1 = 2^{30} + 1 \]