Exact Counting Analytics: Revisiting AdScale

Watson Ladd

December 16, 2024

Introduction

- Review of AdScale: Scalable Private Advertising with Practical Trusted Third Parties

Introduction

- Review of AdScale: Scalable Private Advertising with Practical Trusted Third Parties
- Joint with Matthew Green, Ian Miers

Introduction

- Review of AdScale: Scalable Private Advertising with Practical Trusted Third Parties
- Joint with Matthew Green, Ian Miers
- Exploring the tradeoffs in reporting

Introduction

- Review of AdScale: Scalable Private Advertising with Practical Trusted Third Parties
- Joint with Matthew Green, Ian Miers
- Exploring the tradeoffs in reporting
- 2016

The system

- One hot encoding of what creative sent

The system

- One hot encoding of what creative sent
- Limited metadata for inclusion in histogram

The system

- One hot encoding of what creative sent
- Limited metadata for inclusion in histogram
- Helper only decrypts final value due to homomorphic encryption (no mult)

The system

- One hot encoding of what creative sent
- Limited metadata for inclusion in histogram
- Helper only decrypts final value due to homomorphic encryption (no mult)
- Could integrate differential privacy in post-processing

The system

- One hot encoding of what creative sent
- Limited metadata for inclusion in histogram
- Helper only decrypts final value due to homomorphic encryption (no mult)
- Could integrate differential privacy in post-processing
- Chattier, but clever ways to trade off work

The system

- One hot encoding of what creative sent
- Limited metadata for inclusion in histogram
- Helper only decrypts final value due to homomorphic encryption (no mult)
- Could integrate differential privacy in post-processing
- Chattier, but clever ways to trade off work
- Security: greedy but curious - learn a ballot but lose ability to get the totals

What can we learn from this

- Capability-performance tradeoff (esp. for helpers)

What can we learn from this

- Capability-performance tradeoff (esp. for helpers)
- Slightly different security properties

What can we learn from this

- Capability-performance tradeoff (esp. for helpers)
- Slightly different security properties
- Very similar kinds of data (full power of Prio not used today)

What can we learn from this

- Capability-performance tradeoff (esp. for helpers)
- Slightly different security properties
- Very similar kinds of data (full power of Prio not used today)
- Differential privacy not only game in town

What can we learn from this

- Capability-performance tradeoff (esp. for helpers)
- Slightly different security properties
- Very similar kinds of data (full power of Prio not used today)
- Differential privacy not only game in town
- Privacy budget exhaustion: can we accept in billing?

Third parties

- Independence hard to justify

Third parties

- Independence hard to justify
- The more work, the tougher it is to do

Third parties

- Independence hard to justify
- The more work, the tougher it is to do
- Touching every item strengthens security

Third parties

- Independence hard to justify
- The more work, the tougher it is to do
- Touching every item strengthens security
- But forces helpers to have stringent availability

Third parties

- Independence hard to justify
- The more work, the tougher it is to do
- Touching every item strengthens security
- But forces helpers to have stringent availability

Exact counts

- Felt for applications introducing randomness nonstarter

Exact counts

- Felt for applications introducing randomness nonstarter
- No worse than today

Expressiveness

- Can only count!

Expressiveness

- Can only count!
- Divide by public metadata

Expressiveness

- Can only count!
- Divide by public metadata
- Current system similar

Expressiveness

- Can only count!
- Divide by public metadata
- Current system similar
- Limited expressiveness avoids DP

Expressiveness

- Can only count!
- Divide by public metadata
- Current system similar
- Limited expressiveness avoids DP
- Also less developed then

Expressiveness

- Can only count!
- Divide by public metadata
- Current system similar
- Limited expressiveness avoids DP
- Also less developed then
- Makes some legitimate applications very hard

Expressiveness

- Can only count!
- Divide by public metadata
- Current system similar
- Limited expressiveness avoids DP
- Also less developed then
- Makes some legitimate applications very hard
- Oriented to single user

Are we making the right tradeoffs?