The Phantom Tollbooth: Privacy-Preserving Toll Collection in the Presence of Driver Collusion

Sarah Meiklejohn (UC San Diego)
Keaton Mowery (UC San Diego)
Stephen Checkoway (UC San Diego)
Hovav Shacham (UC San Diego)
Motivation: how tolling works today
Motivation: how tolling works today
Motivation: how tolling works today
Motivation: how tolling works today

This process leaves a lot to be desired in terms of flexibility:
Motivation: how tolling works today

This process leaves a lot to be desired in terms of flexibility:

• How do we charge more according to the time of day?
Motivation: how tolling works today

This process leaves a lot to be desired in terms of flexibility:

- How do we charge more according to the time of day?

- Or as drivers enter city centers?
Motivation: how tolling works today
Motivation: how tolling works today
Motivation: how tolling works today
Motivation: how tolling works today

Core tension between privacy and desire for more flexible toll pricing
Motivation: how tolling works today

Core tension between privacy and desire for more flexible toll pricing

• In this talk we’ll see our system, Milo, which allows for fine-grained pricing policies without sacrificing drivers’ privacy
Motivation: how tolling works today

Core tension between privacy and desire for more flexible toll pricing

- In this talk we’ll see our system, Milo, which allows for fine-grained pricing policies without sacrificing drivers’ privacy

- In the process, we strongly guarantee that drivers remain honest
Previous work [BKS05, BC06, TDKP07, dJJ08, ...]
Previous work [BKS05, BC06, TDKP07, dJJ08, ...]

USENIX Security 2009: VPriv [PBB]
Previous work [BKS05, BC06, TDKP07, dJJ08, ...]

USENIX Security 2009: VPriv [PBB]

- **Fine-grained policy**: uses small road segments (where, when)
Previous work [BKS05, BC06, TDKP07, dJJ08, ...]

USENIX Security 2009: VPriv [PBB]

- **Fine-grained policy**: uses small road segments (where, when)
- **Privacy**: uses Tor to maintain anonymity while driver uploads segments
Previous work [BKS05, BC06, TDKP07, dJJ08, ...]

USENIX Security 2009: VPriv [PBB]

- **Fine-grained policy**: uses small road segments (where, when)
- **Privacy**: uses Tor to maintain anonymity while driver uploads segments
- **Honesty**: relies on audits wherein driver is asked to verify locations
Previous work [BKS05, BC06, TDKP07, dJJ08,...]

USENIX Security 2009: VPriv [PBB]

- **Fine-grained policy**: uses small road segments (where, when)
- **Privacy**: uses Tor to maintain anonymity while driver uploads segments
- **Honesty**: relies on audits wherein driver is asked to verify locations

USENIX Security 2010: PrETP [BRTPVG]

- **Fine-grained policy**: again uses small road segments
- **Privacy**: drivers commit to segments in a way that eliminates need for Tor
- **Honesty**: again relies on audits
Previous work [BKS05, BC06, TDKP07, dJJ08, …]

USENIX Security 2009: VPriv [PBB]

- **Fine-grained policy**: uses small road segments (where, when)
- **Privacy**: uses Tor to maintain anonymity while driver uploads segments
- **Honesty**: relies on audits wherein driver is asked to verify locations

USENIX Security 2010: PrETP [BRTPVG]

- **Fine-grained policy**: again uses small road segments
- **Privacy**: drivers commit to segments in a way that eliminates need for Tor
- **Honesty**: again relies on audits
A potential problem: keeping colluding drivers honest
A potential problem: keeping colluding drivers honest

In these audits, we see a challenge/response behavior:
A potential problem: keeping colluding drivers honest

In these audits, we see a challenge/response behavior:
A potential problem: keeping colluding drivers honest

In these audits, we see a challenge/response behavior:
A potential problem: keeping colluding drivers honest

In these audits, we see a challenge/response behavior:
A potential problem: keeping colluding drivers honest

In these audits, we see a challenge/response behavior:
A potential problem: keeping colluding drivers honest

In these audits, we see a challenge/response behavior:
A potential problem: keeping colluding drivers honest

In these audits, we see a challenge/response behavior:

Proof of payment
A potential problem: keeping colluding drivers honest

In these audits, we see a challenge/response behavior:

Proof of payment
A potential problem: keeping colluding drivers honest

In these audits, we see a challenge/response behavior:

Proof of payment

So the authority reveals to the driver the segment in which he was seen! This information can then be shared to help drivers avoid cameras in the future.
A potential problem: keeping colluding drivers honest

In these audits, we see a challenge/response behavior:

So the authority reveals to the driver the segment in which he was seen! This information can then be shared to help drivers avoid cameras in the future.
A potential problem: keeping colluding drivers honest

In these audits, we see a challenge/response behavior:

So the authority reveals to the driver the segment in which he was seen! This information can then be shared to help drivers avoid cameras in the future.
A potential problem: keeping colluding drivers honest

In these audits, we see a challenge/response behavior:

USENIX Security 2011: Milo

- **Fine-grained policy**: uses same small road segments (where, when)
- **Privacy**: drivers commit to segments in a way similar to PrETP
- **Honesty**: audit protocol no longer reveals locations to drivers
Outline
Outline

Cryptographic background
Outline

Cryptographic background

Milo
Outline

Cryptographic background

Milo

Evaluation

Conclusions
Outline

Cryptographic background
- Commitment schemes
- Zero-knowledge proofs
- Blind identity-based encryption

Milo

Evaluation

Conclusions
Commitments [BCC88, P91]
Commitments [BCC88, P91]
Commitments [BCC88, P91]

My favorite number is 42
Commitments [BCC88,P91]

My favorite number is 42

42
Commitments [BCC88, P91]

My favorite number is 42
Commitments [BCC88,P91]

My favorite number is 42
Commitments [BCC88,P91]

My favorite number is 42
Commitments [BCC88, P91]

My favorite number is 42
Commitments [BCC88,P91]

My favorite number is 42

C = Open(c)
Commitments [BCC88,P91]

My favorite number is 42

$$42$$

$$C = \text{Open}(c)$$
Commitments [BCC88,P91]

There are two important properties of commitments:

My favorite number is 42
There are two important properties of commitments:

- **Hiding**: Bob didn’t know the value in $c$ until Alice gave him $\text{Open}(c)$
There are two important properties of commitments:

- **Hiding**: Bob didn’t know the value in $c$ until Alice gave him $\text{Open}(c)$

- **Binding**: Alice couldn’t change the value in $c$ after giving Bob the envelope
Zero-knowledge proofs [GMR89,BdSMP91]
The value in $c$ is between 0 and 100
Zero-knowledge proofs [GMR89,BdSMP91]

The value in $c$ is between 0 and 100

$\pi$ $c = \text{envelope}$
Zero-knowledge proofs \[\text{[GMR89, BdSMP91]}\]

The value in \(c\) is between 0 and 100
Zero-knowledge proofs [GMR89,BdSMP91]

The value in $c$ is between 0 and 100.

Okay, I believe you!

\[ \Pi \rightarrow C = \text{envelope} \]
Zero-knowledge proofs [GMR89,BdSMP91]

The value in $c$ is between 0 and 100

There are two important properties of zero-knowledge proofs:

$\pi C = \square$

Okay, I believe you!
Zero-knowledge proofs [GMR89,BdSMP91]

The value in \( c \) is between 0 and 100

\[ \Pi \Rightarrow C = \text{envelope} \]

Okay, I believe you!

There are two important properties of zero-knowledge proofs:

- **Soundness**: Alice can’t convince Bob of something that isn’t true
Zero-knowledge proofs [GMR89, BdSMP91]

The value in \( c \) is between 0 and 100

There are two important properties of zero-knowledge proofs:

- **Soundness**: Alice can’t convince Bob of something that isn’t true
- **Zero knowledge**: Bob doesn’t learn anything about Alice’s exact number

Okay, I believe you!
Zero-knowledge proofs [GMR89, BdSMP91]

The value in $c$ is between 0 and 100

There are two important properties of zero-knowledge proofs:

- **Soundness**: Alice can’t convince Bob of something that isn’t true

- **Zero knowledge**: Bob doesn’t learn anything about Alice’s exact number

Zero-knowledge proofs are much more general than this, but this range proof is the only type we will need
Blind identity-based encryption (IBE)
Blind identity-based encryption (IBE)

Regular [S84,BF01,C01]:
Blind identity-based encryption (IBE)

Regular [S84, BF01, C01]:

c = Enc(“Bob”, m)
Blind identity-based encryption (IBE)

Regular [S84,BF01,C01]:

\[ c = \text{Enc}(\text{“Bob”}, m) \]
Blind identity-based encryption (IBE)

Regular [S84,BF01,C01]:

\[ c = \text{Enc}(“Bob”, m) \]
Blind identity-based encryption (IBE)

Regular [S84,BF01,C01]:

\[ c = \text{Enc(“Bob”, m)} \]

Alice \[ \rightarrow \]нять “Bob” \[ \leftarrow \] SK_{Bob}
Blind identity-based encryption (IBE)

Regular [S84,BF01,C01]:

\[ c = \text{Enc}(“Bob”, m) \]

\[ m = \text{Dec}(\text{sk}_{Bob}, c) \]
Blind identity-based encryption (IBE)

Regular [S84,BF01,C01]:

\[ c = \text{Enc}(\text{“Bob”}, m) \]

\[ m = \text{Dec}(\text{sk}_{\text{Bob}}, c) \]

Blind [GH07]:

Alice

Bob

sk_{Bob}
Blind identity-based encryption (IBE)

Regular [S84,BF01,C01]:

\[ c = \text{Enc}(\text{"Bob"}, m) \]

Blind [GH07]:

\[ c = \text{Enc}(\text{"Bob"}, m) \]

\[ m = \text{Dec}(sk_{\text{Bob}}, c) \]
Blind identity-based encryption (IBE)

Regular [S84,BF01,C01]:

\[ c = \text{Enc(“Bob”, m)} \]

Bob

m = \text{Dec(}sk_{Bob}, c)\]

Bob


Blind [GH07]:

\[ c = \text{Enc(“Bob”, m)} \]

Bob

req(“Bob”)
Blind identity-based encryption (IBE)

Regular [S84,BF01,C01]:
\[ c = \text{Enc}(\text{“Bob”}, m) \]
\[ \text{“Bob”} \]
\[ \text{sk}_{\text{Bob}} \]
\[ m = \text{Dec}(\text{sk}_{\text{Bob}}, c) \]

Blind [GH07]:
\[ c = \text{Enc}(\text{“Bob”}, m) \]
\[ \text{req}(\text{“Bob”}) \]
\[ \text{resp}(\text{sk}_{\text{Bob}}) \]
Blind identity-based encryption (IBE)

Regular [S84,BF01,C01]:
\[ c = \text{Enc}(“Bob”, m) \]

1. Extract \( sk_{Bob} \) from \( \text{resp} \)
2. \( m = \text{Dec}(sk_{Bob}, c) \)

Blind [GH07]:
\[ c = \text{Enc}(“Bob”, m) \]

\( \text{req}(“Bob”) \)
\( \text{resp}(sk_{Bob}) \)
Blind identity-based encryption (IBE)

Regular [S84,BF01,C01]:
\[ c = \text{Enc}(\text{“Bob”}, m) \]

1. \[ m = \text{Dec}(\text{sk}_{\text{Bob}}, c) \]

So the authority doesn’t learn which key is being extracted

Blind [GH07]:
\[ c = \text{Enc}(\text{“Bob”}, m) \]

1. \[ \text{req}(\text{“Bob”}) \]
2. \[ \text{resp}(\text{sk}_{\text{Bob}}) \]

So the authority doesn’t learn which key is being extracted
Outline

- Cryptographic background
- Milo
  A generic toll collection system
  A look back at (adapted) PrETP
  A new Audit protocol
- Evaluation
- Conclusions
privacy-preserving toll pricing works
privacy-preserving toll pricing works

segments
How privacy-preserving toll pricing works

segments
How privacy-preserving toll pricing works
How privacy-preserving toll pricing works

segments
How privacy-preserving toll pricing works

segments
(A-B, 13:01-13:02)
How privacy-preserving toll pricing works

segments
(A-B, 13:01-13:02)
How privacy-preserving toll pricing works

segments
(A-B, 13:01-13:02)
How privacy-preserving toll pricing works

segments
(A-B, 13:01-13:02)
(B-C, 13:02-13:03)
How privacy-preserving toll pricing works

segments
(A-B, 13:01-13:02)
(B-C, 13:02-13:03)
How privacy-preserving toll pricing works

segments
(A-B, 13:01-13:02)
(B-C, 13:02-13:03)
How privacy-preserving toll pricing works
How privacy-preserving toll pricing works
How privacy-preserving toll pricing works

OBU
How privacy-preserving toll pricing works

OBU segments
How privacy-preserving toll pricing works

TSP

OBU segments
How privacy-preserving toll pricing works

Payment

OBU segments
How privacy-preserving toll pricing works
How privacy-preserving tolling works:

1. Check information and charge driver what they owe.

2. TSP

3. Payment

4. OBU

segments
How privacy-preserving tolling works:

Check information and charge driver what they owe

TSP

Payment

OBU segments

TC
How privacy-preserving tolling works

TSP

Check information and charge driver what they owe

Payment

OBU segments

TC
How privacy-preserving tolling works:

Check information and charge driver what they owe

TSP

Payment

Audit

TC

OBU segments
How privacy-preserving tolling works

1. Check information and charge driver what they owe

2. Check outcome of Audit to ensure driver is being honest

TSP

Audit

OBU segments

Payment

TC
An adapted version of PrETP
An adapted version of PrETP
An adapted version of PrETP

Commitment to segment price $p_i$
An adapted version of PrETP

\{C_i, \Pi_i\}_i

Commitment to segment price \(p_i\)

NIZK that the value in \(c_i\) is in the proper range
An adapted version of PrETP
An adapted version of PrETP

1. Verify each NIZK $\pi_i$
2. Compute total price

$\left\{ C_i, \Pi_i \right\}_i$
An adapted version of PrETP

1. Verify each NIZK $\pi_i$
2. Compute total price

$\{C_i, \Pi_i\}_i$
An adapted version of PrETP

1. Verify each NIZK $\pi_i$
2. Compute total price

$\{C_i, \Pi_i\}_i$
An adapted version of PrETP

1. Verify each NIZK $\pi_i$
2. Compute total price

$(\text{where, when})$
An adapted version of PrETP

1. Verify each NIZK $\pi_i$
2. Compute total price

(where, when)
An adapted version of PrETP

1. Verify each NIZK $\pi_i$
2. Compute total price

Find commitment $c_j$ for $(\text{where, when})$
An adapted version of PrETP

1. Verify each NIZK $\pi_i$
2. Compute total price

Find commitment $c_j$ for (where,when)

(where,when)

$\{c_i, \pi_i\}_i$

c_j, Open(c_j)
An adapted version of PrETP

1. Verify each NIZK $\pi_i$
2. Compute total price

1. $c_j$ vs. (where, when)
2. $c_j$ vs. $\text{Open}(c_j)$
3. Correct segment price $p_j$

Find commitment $c_j$ for (where, when)
An adapted version of PrETP

1. Verify each NIZK $\pi_i$
2. Compute total price

Find commitment $c_j$ for (where, when)

1. $c_j$ vs. (where, when)
2. $c_j$ vs. $\text{Open}(c_j)$
3. Correct segment price $p_j$

NIZK zero knowledge and commitment hiding guarantee driver privacy

NIZK soundness guarantees price $p_i$ is in the right range (e.g., non-negative)

Commitment binding guarantees $c_j$ is the right commitment for (where, when)
“PrETP with sugar on top”: our new Audit protocol
“PrETP with sugar on top”: our new Audit protocol
“PrETP with sugar on top”: our new Audit protocol

Blind IBE of the opening to $c_i$, using (where,when) as identity

$\{C_i, C'_i, \Pi_i\}_i$
“PrETP with sugar on top”: our new Audit protocol
“PrETP with sugar on top”: our new Audit protocol

1. Verify each NIZK $\pi_i$
2. Compute total price

$\{c_i, C_i, \pi_i\}_i$
“PrETP with sugar on top”: our new Audit protocol

1. Verify each NIZK $\pi_i$
2. Compute total price

$\{c_i, C_i, \pi_i\}_i$
“PrETP with sugar on top”: our new Audit protocol

1. Verify each NIZK $\pi_i$
2. Compute total price

\{c_i, C_i, \pi_i\}_i
“PrETP with sugar on top”: our new Audit protocol

1. Verify each NIZK $\pi_i$
2. Compute total price

$\{c_i, C_i, \pi_i\}_i$

req(where, when)
“PrETP with sugar on top”: our new Audit protocol

1. Verify each NIZK $\pi_i$
2. Compute total price $\{c_i, C_i, \pi_i\}_i$

req(where,when)
“PrETP with sugar on top”: our new Audit protocol

1. Verify each NIZK $\pi_i$
2. Compute total price

\[ \{c_i, C_i, \pi_i\}_i \]

req(where, when)

resp(sk_{where, when})
“PrETP with sugar on top”: our new Audit protocol

1. Verify each NIZK $\pi_i$
2. Compute total price

1. Extract $sk_{\text{where, when}}$
2. Trial decrypt each $C_i$
3. $c_j$ vs. $\text{Open}(c_j)$
4. Correct segment price $p_j$

$\{c_1, c_2, \ldots, c_i\}$
“PrETP with sugar on top”: our new Audit protocol

1. Verify each NIZK $\pi_i$
2. Compute total price

1. Extract $sk_{\text{where, when}}$
2. Trial decrypt each $C_i$
3. $c_j$ vs. $\text{Open}(c_j)$
4. Correct segment price $p_j$

NIZK zero knowledge and commitment hiding guarantee driver privacy

NIZK soundness guarantees price $p_i$ is in the right range (e.g., non-negative)

Commitment binding guarantees $c_j$ is the right commitment for (where, when)
“PrETP with sugar on top”: our new Audit protocol

1. Verify each NIZK $\pi_i$
2. Compute total price

1. Extract $sk_{\text{where, when}}$
2. Trial decrypt each $C_i$
3. $c_j$ vs. $\text{Open}(c_j)$
4. Correct segment price $p_j$

NIZK zero knowledge and commitment hiding guarantee driver privacy

NIZK soundness guarantees price $p_i$ is in the right range (e.g., non-negative)

Commitment binding guarantees $c_j$ is the right commitment for (where,when)

IBE blindness guarantees that driver doesn’t learn segment (where,when)
Outline

- Cryptographic background
- Milo
- Evaluation
  - Implementation details
  - Milo’s performance
- Conclusions
Implementation
Implementation

Used MIRACL [Scott] for blind IBE, ZKPDL [MEKHL’10] for commitments and NIZKs
Implementation

Used MIRACL [Scott] for blind IBE, ZKPDL [MEKHL’10] for commitments and NIZKs

Collected timing information on both a MacBook Pro (acting as the TC) and an ARM v5TE (acting as the OBU)
Implementation

Used MIRACL [Scott] for blind IBE, ZKPDL [MEKHL’10] for commitments and NIZKs

Collected timing information on both a MacBook Pro (acting as the TC) and an ARM v5TE (acting as the OBU)

When are blind IBE operations happening?
Implementation

Used **MIRACL** [Scott] for blind IBE, **ZKPDL** [MEKHL’10] for commitments and NIZKs

Collected timing information on both a **MacBook Pro** (acting as the **TC**) and an **ARM v5TE** (acting as the **OBU**)

When are blind IBE operations happening?

- **Encryption**: during Payment process
- **Extraction**: during Audit (OBU as authority, TC as user)
- **Decryption**: during Audit (TC needs to trial decrypt each ciphertext)
Various measurements: time and space
Various measurements: time and space

<table>
<thead>
<tr>
<th>Operation</th>
<th>Time (ms)</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Laptop</td>
<td>ARM</td>
</tr>
<tr>
<td>Creating parameters</td>
<td>75.12</td>
<td>1083.61</td>
</tr>
<tr>
<td>Encryption</td>
<td>82.11</td>
<td>1187.82</td>
</tr>
<tr>
<td>Blind extraction (user)</td>
<td>13.13</td>
<td>214.06</td>
</tr>
<tr>
<td>Blind extraction (authority)</td>
<td>11.21</td>
<td>175.25</td>
</tr>
<tr>
<td>Decryption</td>
<td>78.31</td>
<td>1131.58</td>
</tr>
</tbody>
</table>

Time for blind IBE
Various measurements: time and space

<table>
<thead>
<tr>
<th>Operation</th>
<th>Laptop</th>
<th>ARM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creating parameters</td>
<td>75.12</td>
<td>1083.61</td>
</tr>
<tr>
<td>Encryption</td>
<td>82.11</td>
<td>1187.82</td>
</tr>
<tr>
<td>Blind extraction (user)</td>
<td>13.13</td>
<td>214.06</td>
</tr>
<tr>
<td>Blind extraction (authority)</td>
<td>11.21</td>
<td>175.25</td>
</tr>
<tr>
<td>Decryption</td>
<td>78.31</td>
<td>1131.58</td>
</tr>
</tbody>
</table>

Time for blind IBE

cost for OBU during Audit is reduced
Various measurements: time and space

<table>
<thead>
<tr>
<th>Operation</th>
<th>Time (ms)</th>
<th>Object</th>
<th>Size (B)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Laptop</td>
<td>ARM</td>
<td></td>
</tr>
<tr>
<td>Creating parameters</td>
<td>75.12</td>
<td>1083.61</td>
<td></td>
</tr>
<tr>
<td>Encryption</td>
<td>82.11</td>
<td>1187.82</td>
<td></td>
</tr>
<tr>
<td>Blind extraction (user)</td>
<td>13.13</td>
<td>214.06</td>
<td></td>
</tr>
<tr>
<td>Blind extraction (authority)</td>
<td>11.21</td>
<td><strong>175.25</strong></td>
<td></td>
</tr>
<tr>
<td>Decryption</td>
<td>78.31</td>
<td>1131.58</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>NIZK</td>
<td>5455</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Commitment</td>
<td>130</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Ciphertext</td>
<td>366</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Total Pay segment</td>
<td>5955</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Audit message</td>
<td>494</td>
</tr>
</tbody>
</table>

Time for blind IBE

Size for messages

cost for OBU during Audit is reduced
Various measurements: time and space

<table>
<thead>
<tr>
<th>Operation</th>
<th>Time (ms)</th>
<th></th>
<th>Object</th>
<th>Size (B)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Laptop</td>
<td>ARM</td>
<td>NIZK</td>
<td>5455</td>
</tr>
<tr>
<td>Creating parameters</td>
<td>75.12</td>
<td>1083.61</td>
<td>Commitment</td>
<td>130</td>
</tr>
<tr>
<td>Encryption</td>
<td>82.11</td>
<td>1187.82</td>
<td>Ciphertext</td>
<td>366</td>
</tr>
<tr>
<td>Blind extraction (user)</td>
<td>13.13</td>
<td>214.06</td>
<td>Total Pay segment</td>
<td>5955</td>
</tr>
<tr>
<td>Blind extraction (authority)</td>
<td>11.21</td>
<td>175.25</td>
<td>Audit message</td>
<td>494</td>
</tr>
<tr>
<td>Decryption</td>
<td>78.31</td>
<td>1131.58</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Time for blind IBE

Size for messages

Cost for OBU during Audit is reduced

NIZK size dominates total size
Various measurements: time and space

<table>
<thead>
<tr>
<th>Operation</th>
<th>Time (ms)</th>
<th>Object</th>
<th>Size (B)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Laptop</td>
<td>ARM</td>
<td></td>
</tr>
<tr>
<td>Creating parameters</td>
<td>75.12</td>
<td>1083.61</td>
<td></td>
</tr>
<tr>
<td>Encryption</td>
<td>82.11</td>
<td>1187.82</td>
<td></td>
</tr>
<tr>
<td>Blind extraction (user)</td>
<td>13.13</td>
<td>214.06</td>
<td></td>
</tr>
<tr>
<td>Blind extraction (authority)</td>
<td>11.21</td>
<td>175.25</td>
<td></td>
</tr>
<tr>
<td>Decryption</td>
<td>78.31</td>
<td>1131.58</td>
<td></td>
</tr>
</tbody>
</table>

---

**Table 2:**

<table>
<thead>
<tr>
<th>Length</th>
<th>Time step</th>
<th>Segments</th>
<th>Time for TC (s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 mile</td>
<td>1 minute</td>
<td>2000</td>
<td>55.68</td>
</tr>
<tr>
<td>1 mile</td>
<td>1 hour</td>
<td>1000</td>
<td>33.51</td>
</tr>
<tr>
<td>2 miles</td>
<td>1 hour</td>
<td>500</td>
<td>10.45</td>
</tr>
</tbody>
</table>

Time for blind IBE

Time for TC to perform Audit

NIZK size dominates total size

Size for messages

cost for OBU during Audit is reduced
Various measurements: time and space

<table>
<thead>
<tr>
<th>Operation</th>
<th>Time (ms)</th>
<th>Object</th>
<th>Size (B)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Laptop</td>
<td>ARM</td>
<td></td>
</tr>
<tr>
<td>Creating parameters</td>
<td>75.12</td>
<td>1083.61</td>
<td></td>
</tr>
<tr>
<td>Encryption</td>
<td>82.11</td>
<td>1187.82</td>
<td></td>
</tr>
<tr>
<td>Blind extraction (user)</td>
<td>13.13</td>
<td>214.06</td>
<td></td>
</tr>
<tr>
<td>Blind extraction (authority)</td>
<td>11.21</td>
<td>175.25</td>
<td></td>
</tr>
<tr>
<td>Decryption</td>
<td>78.31</td>
<td>1131.58</td>
<td></td>
</tr>
<tr>
<td>NIZK</td>
<td></td>
<td>5455</td>
<td></td>
</tr>
<tr>
<td>Commitment</td>
<td></td>
<td>130</td>
<td></td>
</tr>
<tr>
<td>Ciphertext</td>
<td></td>
<td>366</td>
<td></td>
</tr>
<tr>
<td>Total Pay segment</td>
<td></td>
<td>5955</td>
<td></td>
</tr>
<tr>
<td>Audit message</td>
<td></td>
<td>494</td>
<td></td>
</tr>
</tbody>
</table>

**Time for blind IBE**
- Time to iterate dominates cost for TC
- Audit is reduced

**Size for messages**
- Cost for OBU during

**Time for TC to perform Audit**

<table>
<thead>
<tr>
<th>Length</th>
<th>Time step</th>
<th>Segments</th>
<th>Time for TC (s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 mile</td>
<td>1 minute</td>
<td>2000</td>
<td>55.68</td>
</tr>
<tr>
<td>1 mile</td>
<td>1 hour</td>
<td>1000</td>
<td>33.51</td>
</tr>
<tr>
<td>2 miles</td>
<td>1 hour</td>
<td>500</td>
<td>10.45</td>
</tr>
</tbody>
</table>
Outline

Cryptographic background

Milo

Evaluation

Conclusions
Conclusions
Conclusions

We presented Milo, a privacy-preserving electronic toll collection system
Conclusions

We presented Milo, a privacy-preserving electronic toll collection system

• Guarantees honesty even in the face of driver collusion

• Did so using blind IBE

• Found that computational overhead was manageable, significantly cheaper than certain alternatives
Conclusions

We presented **Milo**, a privacy-preserving electronic toll collection system

- Guarantees honesty even in the face of **driver collusion**
- Did so using blind IBE
- Found that computational overhead was manageable, significantly cheaper than certain alternatives

Future work:

- Possibly formalizing security definitions
- Find **cheaper methods** for achieving same security properties
Conclusions

We presented **Milo**, a privacy-preserving electronic toll collection system

- Guarantees honesty even in the face of driver collusion
- Did so using blind IBE
- Found that computational overhead was manageable, significantly cheaper than certain alternatives

Future work:

- Possibly formalizing security definitions
- Find cheaper methods for achieving same security properties

Thanks! Any questions?