Group Time-based One-time Passwords and its Application to Efficient Privacy-Preserving Proof of Location

Zheng Yang¹, Chenglu Jin², Jianting Ning³
Zengpeng Li⁴, Dinh Tien Tuan Anh⁵, Jianying Zhou⁵

¹Southwest University, China
²CWI Amsterdam, Netherlands
³Fujian Normal University, China
⁴Shandong University, China
⁵Singapore University of Technology and Design, Singapore
Overview

• Background
Overview

• Background
• Group Time-based One-Time Passwords (GTOTP)
Overview

• Background
• Group Time-based One-Time Passwords (GTOTP)
• Privacy-Preserving Proof of Location
Overview

• Background
• Group Time-based One-Time Passwords (GTOTP)
• Privacy-Preserving Proof of Location
• Evaluation
Overview

• Background
• Group Time-based One-Time Passwords (GTOTP)
• Privacy-Preserving Proof of Location
• Evaluation
• Summary and Open Questions
Time-based One-time Passwords (TOTP)
Time-based One-time Passwords (TOTP)

- Time-based One-time Passwords
Time-based One-time Passwords (TOTP)

- **Time-based One-time Passwords**
- TOTP as an authentication factor:
  - Lightweight: very efficient to generate
  - Easy to use
Time-based One-time Passwords (TOTP)

• Time-based One-time Passwords
• TOTP as an authentication factor:
  • Lightweight: very efficient to generate
  • Easy to use
• TOTP can be realized using
  • Symmetric keys shared between the prover and the verifier
  • Asymmetric method: hash-based or digital signatures
Time-based One-time Passwords

• Traditional hash-based TOTPs

\[ x_0 \rightarrow H \rightarrow x_1 \rightarrow H \rightarrow x_2 \rightarrow H \rightarrow \ldots \rightarrow x_{N-1} \rightarrow H \rightarrow x_N \]

Secret known to the prover

Verify Point (VP) known to the verifier/public
Time-based One-time Passwords

- Traditional hash-based TOTPs

\[
\begin{align*}
X_0 & \rightarrow H \rightarrow X_1 \rightarrow H \rightarrow X_2 \rightarrow H \rightarrow \cdots \rightarrow X_{N-1} \rightarrow H \rightarrow X_N
\end{align*}
\]

- Secret known to the prover
- Verify Point (VP) known to the verifier/public
- \( T_{\text{start}} \)
Time-based One-time Passwords

- Traditional hash-based TOTPs

\[ X_0 \xrightarrow{H} X_1 \xrightarrow{H} X_2 \xrightarrow{\cdots} X_{N-1} \xrightarrow{H} X_N \]

- Secret known to the prover
- Verify Point (VP) known to the verifier/public
- Usage direction from \( T_{end} \) to \( T_{start} \)
Time-based One-time Passwords

- Traditional hash-based TOTPs
  - One key pair per user (x₀, xₙ)
    - Asymmetric: verifier compromise resilience
    - No identity privacy: each verify point xₙ is associated with one prover, and the verifier knows the identity of the prover

H(x₀) → H(x₁) → H(x₂) → ... → H(xₙ-1) → H(xₙ)

T_end ← Usage direction → T_start

Secret known to the prover

Verify Point (VP) known to the verifier/public
TOTP with Privacy?
TOTP with Privacy?

• Group Signature: privacy-preserving signatures
  • Computationally expensive: many exponentiations or pairings
  • Not fit for resource-constrained devices or applications
TOTP with Privacy?

• Group Signature: privacy-preserving signatures
  • Computationally expensive: many exponentiations or pairings
  • Not fit for resource-constrained devices or applications

How to efficiently and generically transform a traditional (asymmetric) TOTP into a GTOTP scheme?
Group TOTP

Group Members (Provers)

Trusted Registration Authority (RA)

Verifier
Group TOTP

Group Members (Provers)  Trusted Registration Authority (RA)  Verifier

Local Initialization → $\text{VP}_a, \text{VP}_b, \ldots$
Group TOTP

Group Members (Provers)  Trusted Registration Authority (RA)  Verifier

SK_a  SK_b

Local Initialization  \( V_{P_a}, V_{P_b}, \ldots \)
Group TOTP

Group Members (Provers)
- SK_a
- SK_b

Local Initialization
- VP_a, VP_b, ...

Trusted Registration Authority (RA)
- Group Verification State Generation ($K_{RA}, VP_a, VP_b, ...$)

Verifier
- VST_G
Group TOTP

Group Members (Provers)
- SK_a
- SK_b

Local Initialization
- VP_a, VP_b, ...

Trusted Registration Authority (RA)
- K_RA

Verifier
- VST_G

Group Verification State Generation (K_RA, VP_a, VP_b, ...)
Group TOTP

Group Members (Provers)

SKₐ, SKₐ

Local Initialization

Trusted Registration Authority (RA)

K_RA

Group Verification State Generation (K_RA, VPₐ, VPₐ, …)

Verifier

VST_G

Auxₐ, Auxₐ, …

VPₐ, VPₐ, …
Group TOTP

Group Members (Provers)

Veriﬁer

Trusted Registration Authority (RA)

Local Initialization

SKₐ

Auxₐ

SK₋

Aux₋

VPₐ, VP₋, ...

Auxₐ, Aux₋, ...

Group Veriﬁcation State

Generation (Kₐ, VPₐ, VP₋, ...)

VSTₐ, VST₋, ...

Kₐ
Group TOTP

Group Members (Provers)
- SK\textsubscript{a}, Aux\textsubscript{a}
- SK\textsubscript{b}, Aux\textsubscript{b}

Local Initialization

Trusted Registration Authority (RA)
- K\textsubscript{RA}

Group Verification State
- VP\textsubscript{a}, VP\textsubscript{b}, ...
- Aux\textsubscript{a}, Aux\textsubscript{b}, ...

Password Gen (Sk\textsubscript{i}, Aux\textsubscript{i}, T)
- PW\textsubscript{i}

Verifier
- VST\textsubscript{G}
Group TOTP

Group Members (Provers)
- SK\textsubscript{a}
- SK\textsubscript{b}
- Aux\textsubscript{a}
- Aux\textsubscript{b}

Local Initialization

Trusted Registration Authority (RA)
- K\textsubscript{RA}
- VP\textsubscript{a}, VP\textsubscript{b}, ...
- Aux\textsubscript{a}, Aux\textsubscript{b}, ...

Group Verification State Generation (K\textsubscript{RA}, VP\textsubscript{a}, VP\textsubscript{b}, ...)

Verifier
- VST\textsubscript{G}

Password Gen (Sk\textsubscript{i}, Aux\textsubscript{i}, T)

Verify (T, PW\textsubscript{i}, VST\textsubscript{G})
Group TOTP

Group Members (Provers)
- SKₐ
- SKₐ
- Auxₐ
- Auxₐ

Local Initialization

Trusted Registration Authority (RA)
- K_RA
- VPₐ, VPₐ, ...
- Auxₐ, Auxₐ, ...

Group Verification State Generation (K_RA, VPₐ, VPₐ, ...)

Verifier
- VST_G

Password Gen (Skᵢ, Auxᵢ, T)

Verify (T, PWᵢ, VST_G)

If needed, Open Password (PWᵢ, K_RA), and reveal the identity of the password sender
Security Properties
Security Properties

- **Traceability**: adversary cannot create a password associated with an uncompromised secret seed of an uncorrupted member, such that the password is **valid** but **cannot be opened as associated with** the corresponding member.
Security Properties

• **Traceability**: adversary cannot create a password associated with an uncompromised secret seed of an uncorrupted member, such that the password is **valid** but **cannot be opened as associated with** the corresponding member.

• **Anonymity**: adversary cannot distinguish one group member’s password from another’s.
Detailed Construction of VST\textsubscript{G} Generation
Detailed Construction of $\text{VST}_G$ Generation

Locally generated TOTP instances
Detailed Construction of VST\(_G\) Generation

\[
\begin{align*}
C^{i}_{ID_j} &= \text{ASE.Enc}(k_{RA}, |ID_j|) \\
vp^{i}_{ID_j} &= H_1(vp^{i}_{ID_j} || C^{i}_{ID_j} || i)
\end{align*}
\]

Locally generated TOTP instances
Detailed Construction of VST\(_G\) Generation

**Bloom Filter** \(BF = vst_G\)

\[
\begin{array}{cccccccc}
1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\
\end{array}
\]

\[\hat{vp}_{ID_1}^1, \hat{vp}_{ID_2}^2, \hat{vp}_{ID_2}^1, \hat{vp}_{ID_2}^2, \hat{vp}_{ID_3}^1, \hat{vp}_{ID_3}^2, \hat{vp}_{ID_4}^1, \hat{vp}_{ID_4}^2\]

\[\hat{vp}_{ID_1}^1, \hat{vp}_{ID_2}^2, \hat{vp}_{ID_2}^1, \hat{vp}_{ID_2}^2, \hat{vp}_{ID_3}^1, \hat{vp}_{ID_3}^2, \hat{vp}_{ID_4}^1, \hat{vp}_{ID_4}^2\]

\[C_{ID_j}^i = ASE.Enc(k_{RA}, ID_j)\]

\[\hat{vp}_{ID_j}^i := H_1(vp_{ID_j}^i || C_{ID_j}^i || i)\]

Merkle trees

Locally generated TOTP instances

Shuffled Leaves
Detailed Construction of $VST_G$ Generation

$\text{Bloom Filter} \quad BF = vst_G$

$\begin{array}{cccccccc}
1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1
\end{array}$

$\text{Aux}_i = \text{Merkle Proof for } \text{ID}_i$

$C_{\text{ID}_j} = \text{ASE.Enc}(k_{RA}, |\text{ID}_j|)$

$\hat{v}_p^{i \text{ID}_j} := H_1(v_{p^{i \text{ID}_j}} || C_{\text{ID}_j} || i)$

$\text{Locally generated TOTP instances}$

$\text{Shuffled Leaves}$

$\text{Merkle trees}$
Privacy-Preserving Proof of Location
Privacy-Preserving Proof of Location

• **Goal**: user proves where she/he was
  • allows users to record authenticated location data at times of their choice by presenting a fraud-proof location claim, without revealing the identities of protocol participants
Privacy-Preserving Proof of Location

• **Goal**: user proves where she/he was
  • allows users to record authenticated location data at times of their choice by presenting a fraud-proof location claim, without revealing the identities of protocol participants

• **Parties**:
  • **Registration Authority**: register for prover and witnesses
  • **Prover**: prove she/he was at a location at time $T$
  • **Witness**: testify the location of the prover based on its own location
  • **Verifier**: verify the location proofs
  • **Public Ledger**: record the location proofs and incentivize the witnesses
Privacy-Preserving Proof of Location

• **Goal**: user proves where she/he was
  • allows users to record authenticated location data at times of their choice by presenting a fraud-proof location claim, without revealing the identities of protocol participants

• **Parties**:
  • **Registration Authority**: register for prover and witnesses
  • **Prover**: prove she/he was at a location at time T
  • **Witness**: testify the location of the prover based on its own location
  • **Verifier**: verify the location proofs
  • **Public Ledger**: record the location proofs and incentivize the witnesses

• **Additional Building blocks**:
  • Commitment Scheme
  • Privacy-Preserving Location Proximity (PPLP) Scheme
Privacy-Preserving Proof of Location

1. A prover broadcasts its GTOTP password and privacy-preserving location proximity (PPLP) request to nearby witnesses via a short-range communication channel.

2. Witnesses who can testify for the prover will respond with both message and location commitments regarding the PPLP responses.

3. Witnesses and prover exchange the password for verifying the message commitment.

4. The prover finally assembles the location proof based on the gathered proofs and publishes it to Public Ledger.

5. The verifier can obtain the location proof from either the Public Ledger or the prover.
Performance Evaluation

- Prover/witness: RPi3
- Verifier: PC with i7 CPU and 2GB RAM
- More detailed breakdown analysis in the paper

<table>
<thead>
<tr>
<th>M</th>
<th>Prover</th>
<th>Witness</th>
<th>Total</th>
<th>Verify</th>
<th>PfSize (KB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>0.116/0.133</td>
<td>0.089/0.098</td>
<td>0.205/0.231</td>
<td>0.00065</td>
<td>1.16</td>
</tr>
<tr>
<td>10</td>
<td>0.237/0.276</td>
<td>0.089/0.098</td>
<td>0.326/0.347</td>
<td>0.0011</td>
<td>2.17</td>
</tr>
<tr>
<td>15</td>
<td>0.331/0.382</td>
<td>0.089/0.098</td>
<td>0.42/0.48</td>
<td>0.0018</td>
<td>3.19</td>
</tr>
</tbody>
</table>
Performance Evaluation

- Prover/witness: RPi3
- Verifier: PC with i7 CPU and 2GB RAM
- More detailed breakdown analysis in the paper

<table>
<thead>
<tr>
<th>M</th>
<th>Computation time (s)</th>
<th>PfSize (KB)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>PfGen</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Prover</td>
<td>Witness</td>
</tr>
<tr>
<td>5</td>
<td>0.116/0.133</td>
<td>0.089/0.098</td>
</tr>
<tr>
<td>10</td>
<td>0.237/0.276</td>
<td>0.089/0.098</td>
</tr>
<tr>
<td>15</td>
<td>0.331/0.382</td>
<td>0.089/0.098</td>
</tr>
</tbody>
</table>
Performance Evaluation

- Prover/witness: RPi3
- Verifier: PC with i7 CPU and 2GB RAM
- More detailed breakdown analysis in the paper

```
<table>
<thead>
<tr>
<th>M</th>
<th>PfGen</th>
<th>PFSIZE (KB)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Prover</td>
<td>Witness</td>
</tr>
<tr>
<td>5</td>
<td>0.116/0.133</td>
<td>0.089/0.098</td>
</tr>
<tr>
<td>10</td>
<td>0.237/0.276</td>
<td>0.089/0.098</td>
</tr>
<tr>
<td>15</td>
<td>0.331/0.382</td>
<td>0.089/0.098</td>
</tr>
</tbody>
</table>
```
Summary
Summary

• Extend traditional TOTP to a group setting
Summary

- Extend traditional TOTP to a group setting
- Propose an efficient GTOTP construction
Summary

• Extend traditional TOTP to a group setting
• Propose an efficient GTOTP construction
• Demonstrate an application of GTOTP in privacy-preserving proof of location
Summary

• Extend traditional TOTP to a group setting
• Propose an efficient GTOTP construction
• Demonstrate an application of GTOTP in privacy-preserving proof of location

• Open question:
  • Dynamic group management