Verifiable Member and Order Queries on a List in Zero Knowledge

Esha Ghosh

Brown University

Joint work with:
Olga Ohrimenko, Microsoft Research
Roberto Tamassia, Brown University

August 19, 2014
<table>
<thead>
<tr>
<th>Vaccine</th>
<th>Date given (mm/dd/yyyy)</th>
<th>Administered by</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hepatitis B</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Diptheria, Tetanus</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Haemophilus influenzae type b</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Polio</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rotavirus</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Measles, Mumps and Rubella</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Varicella</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hepatitis A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Meningococcal</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Human papillomavirus</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Selectively revealing health record [BB12]
Model - Privacy Preserving Authenticated List (PPAL)

**SERVER** (MALICIOUS)

List L + Server Digest

**CLIENT** (MALICIOUS)

Query on L

Answer: {X,Z,Y}

Query: {Z,Y,X}

Answer + Proof

**OWNER** (TRUSTED)

X

Z

Y

**Server Digest**

1 2 3 4 5 6 7

**List L**

1 2 3 4 5 6 7

**Client Digest**

X

Z

Y

Esha Ghosh (Brown)

Rump-CRYPTO 2014

August 19, 2014 3 / 10
Security Properties - PPAL

Completeness: Honestly generated proofs are always accepted by the client.

Soundness: Proofs forged by the server for incorrect answers to queries do not pass the verification.

Zero-Knowledge: Proofs do not reveal anything beyond the answers, i.e., the proofs are simulatable.
Solution 1: Zero-Knowledge List (ZKL)

**PHASE 1:**
- Linearly Ordered List (L)
- "Commitment" made public
- Query (Member + Order) on L

**PHASE 2:**
- Answer + Proof
- Revealing anything more?
- Consistent with "commitment"?
Solution 2: Direct Privacy-Preserving Authenticated List (PPAL) Construction

**Diagram**

- **OWNER** (TRUSTED)
- **SERVER** (MALICIOUS)
- **CLIENT** (MALICIOUS)

Linearly Ordered List (L)

1 2 3 4 5 6 7

Server Digest

Client Digest

Order Query on L

Answer + Proof

Revealing anything more?

Authentic?
### Efficiency Comparison:

#### Notations:

- \( n \) = List size
- \( m \) = Query size
- \( k \) = Security parameter

<table>
<thead>
<tr>
<th></th>
<th>Time Complexity via ZKL</th>
<th>PPAL</th>
<th>Space Complexity via ZKL</th>
<th>PPAL</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Owner (Setup)</strong></td>
<td>( O(kn) )</td>
<td>( O(n) )</td>
<td>( O(kn) )</td>
<td>( O(n) )</td>
</tr>
<tr>
<td><strong>Server (Query)</strong></td>
<td>( O(km) )</td>
<td>( O(\min{m \log n, n}) )^1</td>
<td>( O(kn) )</td>
<td>( O(n) )</td>
</tr>
<tr>
<td><strong>Client (Verify)</strong></td>
<td>( O(km) )</td>
<td>( O(m) )</td>
<td>( O(km) )</td>
<td>( O(m) )</td>
</tr>
</tbody>
</table>

^1With preprocessing time \( O(n) \)
How we compare

<table>
<thead>
<tr>
<th></th>
<th>[SBZ01]</th>
<th>[JMSW02]</th>
<th>[CLX09]</th>
<th>[BBD+10]</th>
<th>[SPB+12]</th>
<th>[PSPDM12]</th>
<th>[KAB12]</th>
<th>This Work</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zero-Knowledge</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Setup time</td>
<td>$n \log n$</td>
<td>$n$</td>
<td>$n$</td>
<td>$n^2$</td>
<td>$n^2$</td>
<td>$n$</td>
<td>$n^2$</td>
<td>$n$</td>
</tr>
<tr>
<td>Space</td>
<td>$n$</td>
<td>$n$</td>
<td>$n$</td>
<td>$n^2$</td>
<td>$n^2$</td>
<td>$n$</td>
<td>$n^2$</td>
<td>$n$</td>
</tr>
<tr>
<td>Query time</td>
<td>$m$</td>
<td>$n \log n$</td>
<td>$n$</td>
<td>$mn$</td>
<td>$m$</td>
<td>$n$</td>
<td>$n$</td>
<td>$\min(m \log n, n)$</td>
</tr>
<tr>
<td>Verification time</td>
<td>$m \log n \log m$</td>
<td>$m \log n$</td>
<td>$n^2$</td>
<td>$m^2$</td>
<td>$m^2$</td>
<td>$m$</td>
<td>$m$</td>
<td>$m$</td>
</tr>
<tr>
<td>Proof size</td>
<td>$m$</td>
<td>$m \log n$</td>
<td>$n$</td>
<td>$m^2$</td>
<td>$m^2$</td>
<td>$m$</td>
<td>$n$</td>
<td>$m$</td>
</tr>
<tr>
<td>Assumption</td>
<td>RSA</td>
<td>RSA</td>
<td>SRSA, Division</td>
<td>EUCMA</td>
<td>ROH, nEAE</td>
<td>AnAHF</td>
<td>ROH, RSA</td>
<td>ROH, nBDHI</td>
</tr>
</tbody>
</table>

**Table:** Comparison of our construction of a privacy-preserving authenticated list with previous work. All the time and space complexities are asymptotic. Notation: $n$ is the number of elements of the list, $m$ is the number of elements in the query. Acronyms for the assumptions: Associative non-abelian hash function (AnAHF); Bilinear Diffie Hellman Inversion Assumption (BDHI) $n$-Bilinear Diffie Hellman Inversion Assumption and $n$-weak Bilinear Diffie Hellman Inversion Assumption (Decisinal) (nBDHI); $n$-Element Aggregate Extraction Assumption (nEAE); Existential Unforgeability under Chosen Message Attack (EUCMA) of the underlying signature scheme; Random Oracle Hypothesis (ROH); Strong RSA Assumption (SRSA);
References

Jordan Brown and Douglas M. Blough.
Verifiable and redactable medical documents.

Ron Steinfeld, Laurence Bull, and Yuliang Zheng.
Content extraction signatures.

Robert Johnson, David Molnar, Dawn Xiaodong Song, and David Wagner.
Homomorphic signature schemes.

Ee-Chien Chang, Chee Liang Lim, and Jia Xu.
Short redactable signatures using random trees.

Christina Brzuska, Heike Busch, Ouzgur Dagdelen, Marc Fischlin, Martin Franz, Stefan Katzenbeisser, Mark Manulis, Cristina Onete, Andreas Peter, Bertram Poettering, and Dominique Schröder.
Redactable signatures for tree-structured data: Definitions and constructions.

Kai Samelin, Henrich C. Poehls, Arne Bilzhaus, Joachim Posegga, and Hermann De Meer.
Redactable signatures for independent removal of structure and content.

Henrich C. Poehls, Kai Samelin, Joachim Posegga, and Hermann De Meer.
Length-hiding redactable signatures from one-way accumulators in $O(n)$.
Technical Report MIP-1201, Faculty of Computer Science and Mathematics (FIM), University of Passau, 2012.

Ashish Kundu, Mikhail J. Atallah, and Elisa Bertino.
Leakage-free redactable signatures.

Dan Boneh, Craig Gentry, Ben Lynn, and Hovav Shacham.
Aggregate and verifiably encrypted signatures from bilinear maps.

Dan Boneh and Xavier Boyen.
Efficient selective-id secure identity based encryption without random oracles.

Dan Boneh, Xavier Boyen, and Eu-Jin Goh.
Hierarchical identity based encryption with constant size ciphertext.

Thank you!