VOPRFs with public metadata

draft-iyengar-cfrg-voprfmetadata-00

Subodh Iyengar
Ananth Raghunathan
Chris Wood
Motivation: Bind public data to VOPRF evaluation

Privacy Pass requirement: https://github.com/ietf-wg-privacypass/base-drafts/issues/63

Rate limiting requests

Expiring evaluations
Binding metadata to public key generation

main_priv_key, main_pub_key
Binding metadata to public key generation

\[
\text{main\_priv\_key, main\_pub\_key}
\]

\[
\text{Attr1 = \{0, 0, 0, 1\}}
\]

\[
\text{Attr2 = \{0, 0, 1, 0\}}
\]

\[
\text{Attr3 = \{0, 0, 1, 1\}}
\]

\[
\text{attr1\_priv\_key, attr1\_public\_key}
\]

\[
\text{attr2\_priv\_key, attr2\_public\_key}
\]

\[
\text{attr3\_priv\_key, attr3\_public\_key}
\]

draft-irtf-cfrg-voprf

VOPRF(priv_key, data)
Binding metadata to public key generation

Attr1 = {0, 0, 0, 1}

attr1_priv_key, attr1_public_key

main_priv_key, main_pub_key

is attr1_public_key correctly derived from main_pub_key?
AB-VOPRF

Pairing-free

Naor-Reingold inspired VOPRF with sequential DLEQ proofs

16 bits: 1.6 ms with proof 0.2ms without proof

Key derivation can be done offline

Asking for proof can be done offline
Attribute based VOPRFs

master_key(n) = (a₀, a₁, …, aₙ), for ai in GF(p)

master_public_key(n) = (G, g, h, P₀ = gᵃ₀, h₁ = hᵃ₁, …, hₙ = hᵃₙ)

attr_msk(t) = a₀ * ∏ aᵢᵗᵢ
attr_pub(t) = g^{attr_msk(t)}

πᵢ = DLEQ-π(h, hᵢᵗ[i], Pᵢ₋₁, Pᵢ)
Pᵢ = g^{A(t)ᵢ}
A(t)ᵢ = a₀ * ∏ⱼ<i (aⱼ)ᵗ[j]
Comparison

\(N=\text{size of attribute set}\)
\(n=\log(N)\)
\(q_A=\text{# of different attributes queried}\)

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Dependencies</td>
<td>None</td>
<td>pairings</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Public key size</td>
<td>(O(N))</td>
<td>(O(1))</td>
<td>(O(\log N))</td>
<td>(O(1))</td>
<td>(O(1))</td>
</tr>
<tr>
<td>Public key compute</td>
<td>(O(N))</td>
<td>(O(1))</td>
<td>(O(\log N)) (offline)</td>
<td>(O(1))</td>
<td>(O(N)) (offline)</td>
</tr>
<tr>
<td>Proof transmission size</td>
<td>No proof</td>
<td>No proof</td>
<td>(O(\log N)) (can be offline)</td>
<td>None</td>
<td>(O(\log N)) (can be offline)</td>
</tr>
<tr>
<td>Compatible with irtf-cfrg-voprf</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No*</td>
<td>Yes</td>
</tr>
<tr>
<td>Hardness assumption</td>
<td>DDH</td>
<td>Bilinear DDH</td>
<td>n-Diffie Hellman Exponent</td>
<td>q_A-Diffie Hellman Inversion</td>
<td>DDH + collision resistance</td>
</tr>
</tbody>
</table>

[4] https://mailarchive.ietf.org/arch/msg/privacy-pass/BS7Fg3Ui2VtAmgtIJ1y5MI_D5dw/
Questions

Is there RG interest in a VOPRF variant with public metadata?

What are the criteria for applications that need public metadata? Is (offline) logarithmic proof size acceptable?

Are the hardness assumptions stable enough to standardize now?

Since this work naturally extends [draft-irtf-cfrg-voprf](draft-irtf-cfrg-voprf) without modification, should the RG adopt this now?