VOPRFs with public metadata

draft-iyengar-cfrg-voprfmetadata-00

Subodh Iyengar
Ananth Raghunathan
Chris Wood

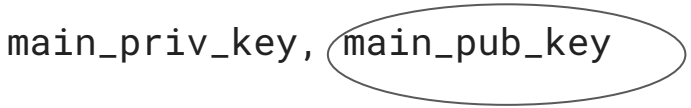
Motivation: Bind public data to VOPRF evaluation

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

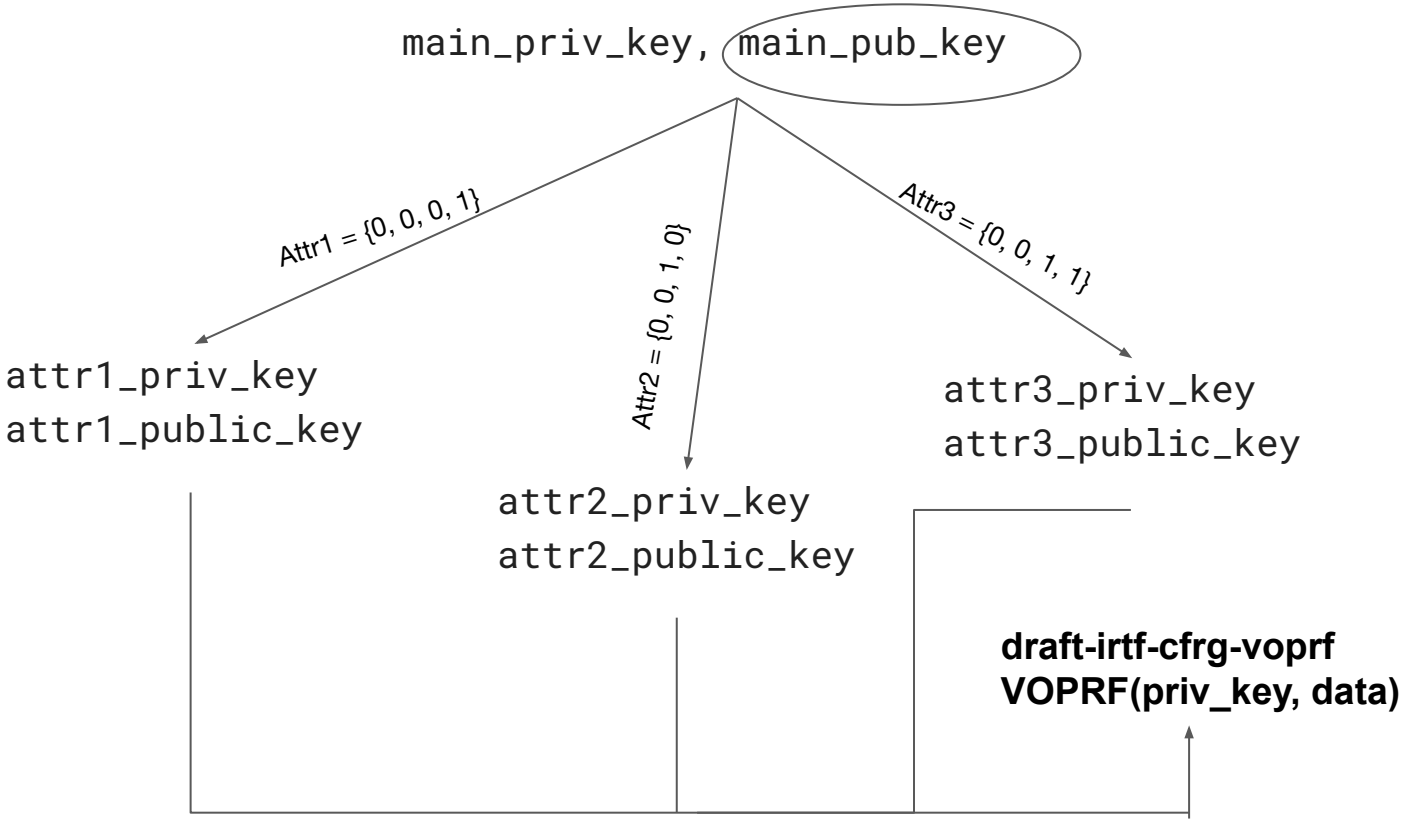
Rate limiting requests

Expiring evaluations

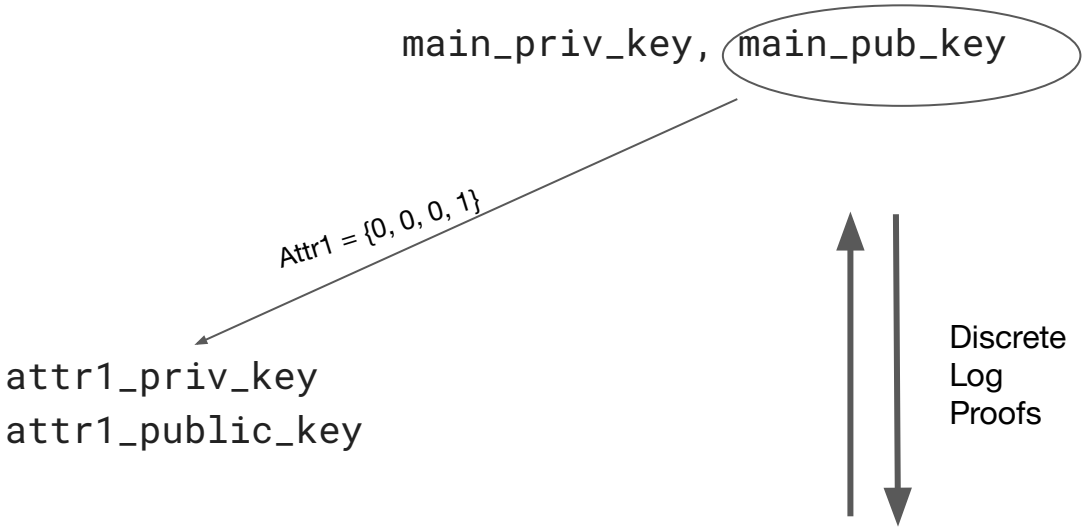
Binding metadata to public key generation



Binding metadata to public key generation



Binding metadata to public key generation



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

$$\text{master\_key}(n) = (a_0, a_1, \ldots, a_n), \text{ for } ai \text{ in } GF(p)$$

$$\text{master\_public\_key}(n) = (G, g, h, P_0 = g^{a0}, h_1 = h^{a1}, \ldots, h_n = h^{an})$$

$$\text{attr\_msk}(t) = a_0 * \prod a_i^{ti}$$
$$\text{attr\_pub}(t) = g^{\text{attr\_msk}(t)}$$

$$\pi_i = \text{DLEQ-}\pi(h, h_i^{t[i]}, P_{i-1}, P_i)$$
$$P_i = g^{A(t)i}$$
$$A(t)_i = a_0 \cdot \prod_{j<i} (a_j)^{t[j]}$$

Comparison

N = size of attribute set
n = log(N)
q_A = # of different attributes queried

Method	Naive (key per metadata)	Pythia [1]	AB-VOPRF [2]	DY-PRF [3]	Merkle Tree [4]
Dependencies	None	pairings	None	None	None
Public key size	O(N)	O(1)	O(log N)	O(1)	O(1)
Public key compute	O(N)	O(1)	O(log N) (offline)	O(1)	O(N) (offline)
Proof transmission size	No proof	No proof	O(log N) (can be offline)	None	O(log N) (can be offline)
Compatible with irtf-cfrg-voprf	Yes	No	Yes	No*	Yes
Hardness assumption	DDH	Bilinear DDH	n-Diffie Hellman Exponent	q_A-Diffie Hellman Inversion	DDH + collision resistance

[1] https://eprint.iacr.org/2015/644.pdf
[2] https://research.fb.com/privatestats
[3] https://eprint.iacr.org/2021/203
[4] https://mailarchive.ietf.org/arch/msg/privacy-pass/BS7Fg3Ui2VtAmgtlJ1y5MI_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 without modification, should the RG adopt this now?