Private location verification with incentivization

in-progress

Vadym Fedyukovych

https://platin.io/

May 18, 2018

Abstract

We design an interactive proof system for "location is close enough" statement, in the form of specification for further implementation.

1 Definitions

Node proves the statement "distance is within a threshold" (less or equal) for node coordinates (x_n, y_n, z_n), given location (x_l, y_l, z_l), and some threshold d (all integers):

$$d^2 - ((x_n - x_l)^2 + (y_n - y_l)^2 + (z_n - z_l)^2) = a_1^2 + a_2^2 + a_3^2 + a_4^2 \quad (1)$$

We rely on 4-squares Lagrange theorem to prove equality statement (Lipmaa). Proofs for integer relations are possible in hidden group order setup (Camenisch-Stadler).

2 Proof setup

Let g be a generator of a proper group of a hidden order, and h be a group element (Pedersen commitment scheme). We use multiplicative group of invertible residue classes modulo a composite n such that $n = pq$, $p = 2p' + 1$, $q = 2q' + 1$ and p, q, p', q' primes (Idemix).

3 Signals harvesting

Node picks random (r_x, r_y, r_z), creates commitment (s_x, s_y, s_z) to it's coordinates

$$s_x = g^{x_n} h^{r_x}, \qquad s_y = g^{y_n} h^{r_y}, \qquad s_z = g^{z_n} h^{r_z} \tag{2}$$

and keeps coordinates-randoms pairs (x_n, y_n, z_n), (r_x, r_y, r_z) private.

4 Proof

Sigma-protocol with 3 messages. Public information is node location commitment, given location, threshold, proof parameters. Private information is node location and randomness to commitment.

1. Prover (node) picks random $\alpha_j, \beta_x, \beta_y, \beta_z, \rho_0, \rho_1, \eta_x, \eta_y, \eta_z$ and computes initial commitments b_0, b_1, t_x, t_y, t_z
   (f_0 and f_1 explained at Background section)

$$b_0 = g^{f_0} h^{\rho_0}, \qquad b_1 = g^{f_1} h^{\rho_1} \tag{3}$$

$$t_x = g^{\beta_x} h^{\eta_x}, \qquad t_y = g^{\beta_y} h^{\eta_y}, \qquad t_z = g^{\beta_z} h^{\eta_z} \tag{4}$$

2. Challenge c
3. Prover computes responses

$$X_n = cx_n + \beta_x, \quad Y_n = cy_n + \beta_y, \quad Z_n = cz_n + \beta_z \tag{5}$$

$$R_x = cr_x + \eta_x, \quad R_y = cr_y + \eta_y, \quad R_z = cr_z + \eta_z \tag{6}$$

$$A_j = ca_j + \alpha_j, \; j = 1..4 \tag{7}$$

$$R_a = c\rho_1 + \rho_0 \tag{8}$$

4. Proof verification

$$g^{c^2 d - ((X_n - cx_l)^2 + (Y_n - cy_l)^2 + (Z_n - cz_l)^2) - (A_1^2 + A_2^2 + A_3^2 + A_4^2)} h^{R_a} = b_1^c b_0 \tag{9}$$

$$g^{X_n} h^{R_x} s_x^{-c} = t_x, \quad g^{Y_n} h^{R_y} s_y^{-c} = t_y, \quad g^{Z_n} h^{R_z} s_z^{-c} = t_z \tag{10}$$

5 Background

Consider quadratic (degree 2 in v) polynomial

$$\begin{aligned} &f_V(v) = f_2 v^2 + f_1 v + f_0 = \\ &v^2 d - (((vx_n + \beta_x) - vx_l)^2 + ((vy_n + \beta_y) - vy_l)^2 + ((vz_n + \beta_z) - vz_l)^2) \\ &\qquad - ((va_1 + \alpha_1)^2 + (va_2 + \alpha_2)^2 + (va_3 + \alpha_3)^2 + (va_4 + \alpha_4)^2) \end{aligned} \tag{11}$$

This polynomial is actually linear ($f_2 = 0$, degree-one in v) if, and only if statement about distance (1) holds for node coordinates that are hidden from verifier. We evaluate this polynomial at a random point chosen as the challenge of verifier. It follows, distance verification equation (9) only needs constant b_0 and degree-one b_1^c components.

$$f_0 = -\beta_x^2 - \beta_y^2 - \beta_z^2 - \alpha_1^2 - \alpha_2^2 - \alpha_3^2 - \alpha_4^2 \tag{12}$$

$$\begin{aligned} f_1 = -2(x_n - x_l)\beta_x - 2(y_n - y_l)\beta_y - 2(z_n - z_l)\beta_z \\ - 2a_1\alpha_1 - 2a_2\alpha_2 - 2a_3\alpha_3 - 2a_4\alpha_4 \end{aligned} \tag{13}$$

Prover calculates b_0, b_1 from f_0, f_1.

6 Private incentivization

To engage users, verifier (map service) is giving tokens in exchange for verifying location proofs. To keep privacy of users, proof verification and token issuance are separated with intermediate tokens. Intermediate tokens should unlink locations that users were confirming.

Intermediate token is a Schnorr proof instance, non-interactive variant (Fiat-Shamir), in another group of a known prime order q generated by g_i. Issuing (private) key x_i and public key X_i of map service.

A new blinded intermediate token is sent to user on each successful location verification. Users unblind their intermediate tokens and periodically exchange them for Platin tokens.

1. Issuer (map service) chooses random γ and sends $\tilde{w}$ to Recipient

$$\tilde{w} = g_i^\gamma \tag{14}$$

2. Recipient (node) chooses random blinding (δ, μ), produces blinded challenge $\tilde{c}_i$ and sends it to Issuer

$$w = \tilde{w} g_i^{-\delta} X_i^\mu \tag{15}$$

$$\tilde{c}_i = H(w) + \mu \pmod{q} \tag{16}$$

3. Issuer produces blinded response $\tilde{r}_i$ and sends it to Recipient

$$\tilde{r}_i = \tilde{c}_i x_i + \gamma \pmod{q} \tag{17}$$

4. Recipient verifies validity of response received and unblinds challenge and response

$$\tilde{c}_i = H(g_i^{\tilde{r}_i} X_i^{-\tilde{c}_i}) \tag{18}$$

$$c_i = \tilde{c}_i - \mu \pmod q \tag{19}$$

$$r_i = \tilde{r}_i - \delta \pmod q \tag{20}$$

   Intermediate token is (c_i, r_i).

5. Intermediate token verification (while exchange for Platin tokens)

$$c_i = H(g_i^{r_i} X_i^{-c_i}) \tag{21}$$

7 Intermediate token properties

Both components of intermediate token are statistically (unconditionally) independent from blinded intermediate token.

Consider an Adversary trying to distinguish two pairs of unblinded intermediate tokens (c_1, r_1) and (c_2, r_2), matching them to issuing session identified with $\tilde{w}$. View of Issuer is $(\tilde{c}_i, \tilde{r}_i, c_j, r_j)$ for $j = 1, 2$.

$$g_i^{r_j} X_i^{-c_i} \stackrel{?}{=} \tilde{w} g_i^{-\delta_j} X_i^{\mu_j} = \tilde{w} g_i^{r_j - \tilde{r}_i} X_i^{\tilde{c}_i - c_j} = (\tilde{w} g_i^{-\tilde{r}_i} X_i^{\tilde{c}_i})(g_i^{r_j} X_i^{-c_j}) \tag{22}$$

It could be seen that the only possible relation does not depend on issuing session identifier $\tilde{w}$, resulting in unconditional privacy for intermediate tokens.

8 Todo

Specify ranges for random numbers.
Introduce accumulator for a set of time-locations.
Design enforcement for “just one single location at a time”.
Add references (bibliography).