Rusk: Dusk genesis circuits

Dusk Network

Victor Lopez <victor@dusk.network>

March 14, 2022

Contents

1. Elements

- Let $\mathbb{B}$ be a boolean set $\{false, true\}$.
- Let $\mathbb{F}_q$ be a finite field with order q.
- Let $\mathbb{F}_r$ be a finite field with order r.
- Let $\mathbb{J}$ be an elliptic-curve over $\mathbb{F}_q$ with a subgroup of prime order r.
- Let I be the identity point of $\mathbb{J}$.
- Let G and G' be two random generators of $\mathbb{J}$.
- Let $\mathbb{Q}$ be the set of efficient functions in the space.
- Let $\Re_r$ be a random number generator in $\mathbb{F}_r$.

2. Functions

2.1. H - Cryptographic hash

H is a cryptographically secure hash function.

Definition

$$\mathbb{H} : \mathbb{F}_q \mapsto \mathbb{F}_q \tag{1}$$

$$\mathbb{H}_r : \mathbb{F}_q \mapsto \mathbb{F}_r \tag{2}$$

Properties

$$\nexists F \in \mathbb{Q} : F(H(x)) = x \tag{3}$$

$$\nexists F \in \mathbb{Q} : F(H(x)) = y \wedge H(y) = H(x) \wedge x \neq y \tag{4}$$

$$\nexists F \in \mathbb{Q} : F(H_r(x)) = x \tag{5}$$

$$\nexists F \in \mathbb{Q} : F(H_r(x)) = y \wedge H_r(y) = H_r(x) \wedge x \neq y \tag{6}$$

2.2. U - Select pair

U selects either $\mathbb{J}^2$ or $\{I, I\}$, depending on a bit.

Definition

$$U : \mathbb{B} \times \mathbb{J}^2 \mapsto \mathbb{J}^4 \tag{7}$$

Properties

$$U(x, A, B) = \begin{cases} (A, B, I, I), \text{if } x = true. \\ (I, I, A, B), \text{if } x = false. \end{cases} \tag{8}$$

2.3. C - Commitment opening

C is a Pedersen Commitment with range check for 2^{64}.

Definition

$$\mathrm{C} : \mathbb{F}_q \times \mathbb{F}_r \mapsto \mathbb{J} \tag{9}$$

$$C_v : \mathbb{J} \times \mathbb{F}_q \times \mathbb{F}_r \mapsto \mathbb{B} \tag{10}$$

Properties

$$C(v, b) = T(v) \cdot G + b \cdot G' \tag{11}$$

$$C_v(P, v, b) \rightarrow v < 2^{64} \tag{12}$$

$$C(P, v, b) \rightarrow P = C(v, b) \tag{13}$$

2.4. T - Truncate Fq to Fr

T truncate $\mathbb{F}_q$ to the bits of $\mathbb{F}_r$.

Definition

$$\mathbb{H} : \mathbb{F}_q \mapsto \mathbb{F}_r \tag{14}$$

2.5. A - Stealth address

A is a stealth address for Phoenix notes.

Definition

$$A : \mathbb{F}_r^3 \mapsto \mathbb{F}_r \tag{15}$$

$$A_{sk_r} : \mathbb{F}_r^2 \times \mathbb{J} \mapsto \mathbb{F}_r \tag{16}$$

$$A_o : \mathbb{F}_r \times \mathbb{J}^3 \mapsto \mathbb{B} \tag{17}$$

Properties

$$A(r, a, b) = H_r(r \cdot a \cdot G) + b \tag{18}$$

$$A_{sk_r}(a, b, R) = H_r(a \cdot R) + b \tag{19}$$

$$\begin{aligned} A_o(a, B, R, X) \rightarrow B &= b \cdot G \wedge \\ R &= r \cdot G \wedge \\ X &= A(r, a, b) \cdot G \end{aligned} \tag{20}$$

2.6. E - Data encryption

O is a data encryption function with secret over $\mathbb{F}_r$.

Definition

$$E : \mathbb{J} \times \mathbb{F}_q^4 \mapsto \mathbb{F}_q^3 \tag{21}$$

$$E_d : \mathbb{J} \times \mathbb{F}_q^4 \mapsto \mathbb{F}_q^3 \tag{22}$$

Properties

$$\mathbf{m} = E_d(S, n, \psi) \rightarrow \psi = E(S, n, \mathbf{m}) \tag{23}$$

2.7. L - Discrete logarithm

L is a discrete logarithm function.

Definition

$$L : \mathbb{J} \mapsto \mathbb{F}_r \tag{24}$$

Properties

$$(P), P = L(P) \cdot G \tag{25}$$

$$L \notin \mathbb{Q} \tag{26}$$

2.8. S - Schnorr signature

S is a Schnorr signature function.

Definition

$$S : \mathbb{F}_r^2 \times \mathbb{F}_q \mapsto \mathbb{F}_r \times \mathbb{J} \tag{27}$$

$$S_v : \mathbb{F}_r \times \mathbb{F}_q \times \mathbb{J}_q^2 \mapsto \mathbb{B} \tag{28}$$

Computations

$$\begin{aligned} R &= r \cdot G \\ c &= H_r(R \| m) \\ u &= r - c \cdot s \end{aligned} \tag{29}$$

Properties

$$\begin{aligned} S(s, r, m) = (u, R) \rightarrow S_v(u, m, R, s \cdot G) \\ R = u \cdot G + c \cdot s \cdot G \end{aligned} \tag{30}$$

$$\begin{aligned} \nexists F \in \mathbb{Q} : F(u, R) = s \\ u = r - c \cdot s \\ s = (L(R) - u)/c \therefore true^{[1]} \end{aligned} \tag{31}$$

2.9. O - Merkle opening

O is a Merkle tree opening function.

Types

1. T Merkle tree over H.
2. O_y Merkle root for T.
3. O_p Merkle opening for leaf indexed by p over T.

[1] Discrete logarithm problem, check [2.7.26].

Definition

$$O : T \times \mathbb{F}_q \mapsto O_p \tag{32}$$

$$O_v : \mathbb{F}_q^2 \times O_p \mapsto \mathbb{B} \tag{33}$$

Properties

$$h, o = O(T, p) \to O_v(O_y, o, h) \wedge O_{p[last]} = h \tag{34}$$

2.10. P - Schnorr proof

P is a Schnorr proof function.

Definition

$$P : \mathbb{F}_r^2 \times \mathbb{F}_q \mapsto \mathbb{F}_r \times \mathbb{J}^2 \tag{35}$$

$$P_v : \mathbb{F}_r \times \mathbb{F}_q \times \mathbb{J}_q^4 \mapsto \mathbb{B} \tag{36}$$

Computations

$$\begin{aligned} R &= r \cdot G \\ R' &= r \cdot G' \\ c &= H_r(R \| R' \| m) \\ u &= r - c \cdot s \end{aligned} \tag{37}$$

Properties

$$\begin{aligned} P(s, r, m) = (u, R, R') \to P_v(u, m, R, R', s \cdot G, s \cdot G') \\ R = u \cdot G + c \cdot s \cdot G \\ R' = u \cdot G' + c \cdot s \cdot G' \end{aligned} \tag{38}$$

$$\begin{aligned} \nexists F \in \mathbb{Q} : F(u, R, R') &= s \\ u &= r - c \cdot s \\ s &= (L(R) - u)/c \therefore true^{[2]} \end{aligned} \tag{39}$$

[2] Discrete logarithm problem, check [2.7.26].

3. Execute

3.1. Precomputation

1. Fetch the hash m of the transaction skeleton
2. Fetch a Merkle tree of Phoenix notes T
3. Fetch the anchor y of T
4. Fetch $\mathbb{I}$ of input notes that exists in T

   t Note type
   C Value commitment
   R Stealth address entropy
   K Stealth address
   p Merkle tree index
   n Encryption nonce
   ψ Encryption cipher
   s Secret spend key in $\mathbb{F}_r^2$

5. Define the crossover value V_v
6. Define the gas $g = g_{limit} \cdot g_{price}$
7. Define [3] the set of outputs $\mathbb{O}$

   v Value

8. $\forall I : (t, C, R, K, p, n, \psi, s) \in \mathbb{I}$
   (a) $(I_v, I_b, \_) = E_d(s_a \cdot R, n, \psi)$
   (b) $sk_r = A_{sk_r}(s_a, s_b, R)$
   (c) $I_{K'} = sk_r \cdot G'$
   (d) $z \leftarrow \Re_r$
   (e) $I_\lambda = P(sk_r, z, m)$
   (f) $I_h = H(\{t, C, n, K, R, p, \psi\}$
   (g) $I_o = \mathbb{O}(T, p)$
   (h) $I_x = H(I_{k'} \| p)$
9. $\forall O : (v) \in \mathbb{O}$
   (a) $O_b \leftarrow \Re_r$
   (b) $O_c = v \cdot G + O_b \cdot G'$
10. $V_b \leftarrow \Re_r$
11. $V_c = C(V_v, V_b)$

[3] Add a change note to satisfy $\sum(o_v \in \mathbb{O}) = \sum(i_v \in \mathbb{I}) - V_v - g$

3.2. Witness arguments

V : (V_v, V_b) Crossover value and blinder

$I \in \mathbb{I}$: $(t, v, b, C, K, K', \lambda, R, p, n, \psi, h, o)$ Input notes

$O \in \mathbb{O}$: (v, b) Output value and blinder

3.3. Public arguments

V : (V_C) Crossover value commitment

y Merkle tree anchor

g Gas reserved

$I \in \mathbb{I}$: (x) Nullifiers of $\mathbb{I}$

$O \in \mathbb{O}$: (C) Value commitment of $\mathbb{O}$

m Hash of the transaction skeleton

3.4. Circuit

1. $\forall I \in \mathbb{I} : (t, v, b, C, K, K', \lambda, R, p, n, \psi, h, o, x)$
   (a) $O_v(y, o)$[4]
   (b) $h = H(t, C, n, K, R, p, \psi)$[5]
   (c) $P_v(\lambda_u, m, K, K', \lambda_R, \lambda_{R'})$[6]
   (d) $x = H(K', p)$[7]
   (e) $C(C, v, b)$
2. $C(V_C, V_v, V_b)$
3. $\forall O \in \mathbb{O} : (v, b, C)$
   (a) $C(C, v, b)$
4. $\sum(i_v \in \mathbb{I}) - \sum(o_v \in \mathbb{O}) - V_v - g = 0$[8]

[4] Ensure I_h exists as leaf of T and has a valid branch to root y. [2.9.34]

[5] Binds I_h to all public attributes of the input note via hash pre-image. [2.1.4]

[6] Enforce $K = sk_r \cdot G \wedge K' = sk_r \cdot G'$. A valid Schnorr proof can be produced only by one who knows sk_r because there is one, and only one, solution to this circuit. [2.10.38]

[7] Considering $K' = sk_r \cdot G'$ is constrained by the Schnorr proof, the pre-image guarantees that only the owner of sk_r can produce this nullifier. [2.1.4]

[8] All values are checked with the crossover opening. The range check protects against overflow attacks. [2.3.12]

4. Send to contract transparent

4.1. Precomputation

1. Define a destination address $a \in \mathbb{F}_q$
2. Define a value $v \in \mathbb{F}_q | v < 2^{64}$
3. Define a crossover encryption nonce $V_n \in \mathbb{F}_q$
4. Define a key $k = (a, b) | (a, b) \in \mathbb{F}_r^2$
5. $V_b \leftarrow \Re_r$
6. $V_C = C(v, V_b)$
7. $r \leftarrow \Re_r$
8. $R = r \cdot G$
9. $V_\psi = E(k_a \cdot R, V_n, \{v, V_b, \varnothing\}$
10. $sk_r = A_{sk_r}(k_a, k_b, R)$[9]
11. $T = sk_r \cdot G$
12. $m = H(V_C, V_n, V_\psi, v, a)$
13. $z \leftarrow \Re_r$
14. $\sigma = S(sk_r, z, m)$

4.2. Witness arguments

V : (V_b, V_n, V_ψ) Crossover blinder, nonce and cipher

σ Schnorr signature

a Contract address

4.3. Public arguments

V_C Crossover commitment

v Value

T Stealth address

m Schnorr message

[9] The stealth address is specified in [2.5.19]

4.4. Circuit

1. $C(V_C, V_v, V_b)$
2. $m = H(V_C, V_n, V_\psi, v, a)$
3. $S_v(\sigma_u, m, \sigma_R, T)$

5. Send to contract obfuscated

5.1. Precomputation

1. Define a destination address $a \in \mathbb{F}_q$
2. Define a value $v \in \mathbb{F}_q | v < 2^{64}$
3. Define a crossover encryption nonce $V_n \in \mathbb{F}_q$
4. Define a message encryption nonce $M_n \in \mathbb{F}_q$
5. Define a crossover key $k = (a, b) | (a, b) \in \mathbb{F}_r^2$
6. Define a message key $l = (a, b) | (a, b) \in \mathbb{F}_r^2$
7. Define in $f \in \mathbb{B}$ if message derive key is public.
8. $V_b \leftarrow \Re_r$
9. $V_C = C(v, V_b)$
10. $r \leftarrow \Re_r$
11. $R = r \cdot G$
12. $V_\psi = E(k_a \cdot R, V_n, \{v, V_b, \varnothing\}$
13. $V_T = A_{sk_r}(k_a, k_b, R) \cdot G$
14. $sk_r = A_{sk_r}(l_a, l_b, R)$[10]
15. $M_T = sk_r \cdot G$
16. $M_b \leftarrow \Re_r$
17. $M_C = C(v, M_b)$
18. $s \leftarrow \Re_r$
19. $M_\psi = E(l_a \cdot R, M_n, \{v, M_b, \varnothing\})$
20. $p = H(V_C, V_n, V_\psi, M_C, M_n, M_\psi, v, a)$
21. $z \leftarrow \Re_r$
22. $\sigma = S(sk_r, z, p)$
23. $\theta = U(f, l_a \cdot G, l_b \cdot G)$

[10]The stealth address is specified in [2.5.19]

5.2. Witness arguments

v Value

V_b Crossover blinder

M : $(M_s, M_b, f, \theta_0, \theta_1)$ Message entropy, blinder, flag, secret derive key

5.3. Public arguments

V : (V_C, V_T, V_n, V_ψ) Crossover commitment, stealth address, nonce and cipher

M : $(M_C, \theta_2, \theta_3, M_T, M_n, M_\psi)$ Message commitment, public derive key, stealth address, nonce and cipher

a Contract address

σ Schnorr signature

5.4. Circuit

1. $C(V_C, v, V_b)$
2. $C(M_C, v, M_b)$
3. $\gamma = U(f, \theta_0, \theta_1, \theta_2, \theta_3)$
4. $\alpha = \theta_0 + \theta_2$
5. $\beta = \theta_1 + \theta_3$
6. $A_o(M_s, \alpha, \beta, M_T)$
7. $M_\psi = E(M_s \cdot \alpha, M_n, \{v, M_b, \varnothing\})$
8. $p = H(V_C, V_n, V_\psi, M_C, M_n, M_\psi, v, a)$
9. $S_v(\sigma_u, p, \sigma_R, V_T)$

6. Withdraw from transparent

6.1. Precomputation

1. Define a value $v \in \mathbb{F}_q | v < 2^{64}$
2. $b \leftarrow \Re_r$
3. $C = C(v, b)$
4. Generate a note with (C, v, b)

6.2. Witness arguments

b Blinder

6.3. Public arguments

v Value

C Commitment

6.4. Circuit

1. $C(C, v, b)$

7. Withdraw from obfuscated

7.1. Precomputation

1. Fetch a message key $k = (a, b) | (a, b) \in \mathbb{F}_r^2$
2. Fetch an unspent message $M : (C, n, \psi, S)$ generated with k
3. Define a value $v \in \mathbb{F}_q | v < 2^{64}$ for the output note
4. Define a change message key $l = (a, b) | (a, b) \in \mathbb{F}_r^2$
5. Define a change message encryption nonce $G_n \in \mathbb{F}_q$
6. Define in $f \in \mathbb{B}$ if change message derive key is public.
7. $(M_v, M_b, \_) = E_d(k_a \cdot M_S, M_n, M_\psi)$
8. $b \leftarrow \Re_r$
9. $C = C(v, b)$
10. $G_v = M_v - v$
11. $G_r \leftarrow Re_r$
12. $G_R = G_r \cdot G$
13. $G_b \leftarrow Re_b$
14. $G_C = C(G_v, G_b)$
15. $G_T = A_{sk_r}(l_a, l_b, G_R) \cdot G$
16. $\theta = U(f, l_a \cdot G, l_b \cdot G)$
17. $G_\psi = E(l_a \cdot G_R, G_n, \{G_v, G_b, \varnothing\})$

7.2. Witness arguments

M : (M_v, M_b) Message value and blinder

G : $(G_v, G_b, G_r, f, \theta_0, \theta_1)$ Change value, blinder, entropy, flag, secret derive key

v Value

b Blinder

7.3. Public arguments

M_C Message value commitment

G : $(G_C, \theta_2, \theta_3, G_T, G_n, G_\psi)$ Change message commitment, public derive key, stealth address, nonce and cipher

C Value commitment

7.4. Circuit

1. $C(M_C, M_v, M_b)$
2. $C(G_C, G_v, G_b)$
3. $C(C, v, b)$
4. $\gamma = U(f, \theta_0, \theta_1, \theta_2, \theta_3)$
5. $\alpha = \theta_0 + \theta_2$
6. $\beta = \theta_1 + \theta_3$
7. $A_o(G_r, \alpha, \beta, G_T)$
8. $G_\psi = E(G_r \cdot \alpha, G_n, \{G_v, G_b, \varnothing\})$
9. $M_v - G_v - v = 0$