Public keys of ring members {U_1; U_3, U_4, U_5}

User1: U_1; User3: U_3; User4: U_4; User5 : U_5.

$PuK_1=A_1$; **$PuK_3=A_3$**; **$PuK_4=A_4$**; **$PuK_5=A_5$**;

Alice is User2: U_2;

$PuK_A=a$-->$PuK_2=A_2$; **$PrK_2=z$**.

All ring members including Alice U_2:{U_1, U_2; U_3, U_4, U_5}$=R$

There are used 2 H-functions : $H(\ )$; $H_{EC}(\ )\rightarrow$ an EC point H.

$$H_{EC}(U_1||U_2||U_3||U_4||U_5)=H_{EC}(R)=H$$

1) $H(U_1||U_2||U_3||U_4||U_5)=h$

2) $H_{EC}(R)=h*G=H$

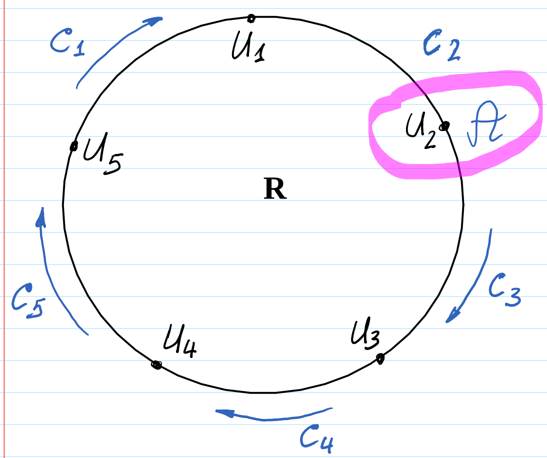
Verification key **V**

$$U_2:\ V=z*H_{EC}(U_1||U_2||U_3||U_4||U_5)=z*H_{EC}(R)=z*H$$

Ring of Users:

R = { **U_1,** **U_2,** **U_3,** **U_4,** **U_5 }**

$PuK_1=A_1$ **($PrK_2=z$, $PuK_2=A_2=z*G$)** **$PuK_3=A_3$** **$PuK_4=A_4$** **$PuK_5=A_5$**



U_2; computations

1) $\alpha\leftarrow randi(\mathbb{Z}_p)$; $\mathbb{Z}_p=\{0,1,2,\dots,p-1\}$.
$r_1, \ \vee, r_3, r_4, r_5\leftarrow randi(\mathbb{Z}_p)$)

2) M - message to be signed, then M is hashed by functions $H(\ )$; $H_{EC}(\ )$:
$H(M)=m$
$H_{EC}(R)=H_{EC}$

3) $c_3=H(R, V, m, \alpha*G, \alpha*H_{EC})$

4) $c_4=H(R, V, m, r_3*G+c_3*A_3, r_3*V+c_3*V)$

4) $c_4 = H(R, V, m, r_3*G + c_3*A_3, r_3*V + c_3*V)$

5) $c_5 = H(R, V, m, r_4*G + c_4*A_4, r_4*V + c_4*V)$

6) $c_1 = H(R, V, m, r_5*G + c_5*A_5, r_5*V + c_5*V)$

7) $c_2 = H(R, V, m, r_1*G + c_1 \cdot A_1, r_1*V + c_1*V)$

A computes: $r_2 = \alpha - z \cdot c_2 \bmod p$

$$Sign(M) = (c_1, r_1, r_2, r_3, r_4, r_5, V) = \sigma$$

Let ***u***, ***v*** are integers < ***p*** and ***P, Q*** are the points in EC.
Property 1: $(u + v)*P = u*P \boxplus v*P$ replacement to --> $(u + v)P = uP + vP$
Property 2: $(u)*(P \boxplus Q) = u*P \boxplus u*Q$ replacement to --> $u(P + Q) = uP + uQ$

Let ***t***, ***z***, ***c*** are integers.
Important identity used e.g. in Ring Signature:
$(t-z\cdot c)*G \boxplus c*A = t*G \boxplus (-z\cdot c)*G \boxplus c*A = t*G \boxplus (c*(-z)*G + A)) = t*G \boxplus c*(-A \boxplus A) = t*G \bmod p$.

Verification: $Ver(V, \sigma, m) \in \{T, F\}$

for $i = 1,2,3,4,5$ compute, replacing $5+1 \to 1$: $H_{EC}(R) = H$.

$q_1' = r_1*G + c_1*A_1$; $q_1'' = r_1*H_{EC} + c_1*V$;
$c_2' = H(R, V, m, q_1', q_1'')$.

$q_2' = r_2*G + c_2*A_2$; $q_2'' = r_1*H_{EC} + c_2*V$;
$c_3' = H(R, V, m, q_2', q_2'')$

— — — — —

$q_5' = r_5*G + c_5*A_5$; $q_5'' = r_5*H_{EC} + c_5*V$
$c_1' = H(R, V, m, q_5', q_5'')$

Signature is valid if: $c_1' = c_1$

Correctness: if $i \neq 2$, then c_{i+1} is defined as in signature algorithm.
if $i = 2$, then

$$q_2' = r_2 * G + c_2 * A_2 = (\alpha - z \cdot c_2) * G + c_2 * A_2$$
$$= \alpha * G - (c_2 \cdot z) * G + c_2 * A_2$$
$$= \alpha * G - c_2 * (z * G) + c_2 * A_2$$
$$= \alpha * G - \cancel{c_2 * A_2} + \cancel{c_2 * A_2} = \alpha * G$$

$$q_2'' = r_2 * H_{EC} + c_2 * V$$
$$= (\alpha - z \cdot c_2) * H_{EC} + c_2 * V$$
$$= \alpha * H_{EC} - (z \cdot c_2) * H_{EC} + c_2 * V$$
$$= \alpha * H_{EC} - c_2 * (z * H_{EC}(R)) + c_2 * V$$
$$= \alpha \cdot H_{EC} - \cancel{c_2 * V} + \cancel{c_2 * V} = \alpha * H_{EC}$$

$$c_2' = H(R, V, M, q_2', q_2'') = H(R, V, M, \underbrace{\alpha * G}, \underbrace{\alpha * H_{EC}})$$
$$c_2 = H(R, V, m, \overbrace{r_1 * G + c_1 \cdot A_1}, \overbrace{r_1 * V + c_1 * V})$$

$$c_2 = c_2'$$

Till this place

The purpose of blockchains is to furnish trust to operations between unrelated parties, without requiring the collaboration of a trusted third party.
Trust is attained through the use of cryptographic artifacts which cater for virtual immutability and non-falsi
ability of data registered in a readily accessible database | the blockchain. In
other words, a blockchain is a public distributed database, containing data whose legitimacy cannot be disputed by any party.
Cryptocurrencies store transactions in the blockchain. The latter acts as a public ledger of all the veri
ed currency operations. Most cryptocurrencies store transactions in clear text, to facilitate the veri
cation of transactions by the community.
Clearly, an open blockchain de
es any basic understanding of privacy, since it virtually publicizes complete transaction histories of its users.
To address the lack of privacy, users of cryptocurrencies such as Bitcoin can obfuscate transactions by using temporary intermediate addresses [16]. However, in spite of such measures, with appropriate tools it is possible to analyze
ows and to a large extent link true senders with
receivers [21, 8, 19].
In contrast, the cryptocurrency Monero, attempts to tackle the issue of privacy by storing only stealth, single-use addresses in a blockchain, and authenticating transactions with ring signatures. In this manner, there will be no e
ective way of linking senders with receivers nor

tracing the origins of funds [1].
Additionally, transaction amounts in the Monero blockchain are concealed behind cryptographic constructions, so as to complicate the task of inferringr currency
ows.
The result is a cryptocurrency with a high level of privacy.

The purpose of blockchains is to furnish trust to operations between unrelated parties, without requiring the collaboration of a trusted third party.
Trust is attained through the use of cryptographic artifacts which cater for virtual immutability and non-falsiability of data registered in a readily accessible database in the blockchain. In other words, a blockchain is a public distributed database, containing data whose legitimacy cannot be disputed by any party.
Cryptocurrencies store transactions in the blockchain. The latter acts as a public ledger of all the veri
ed currency operations. Most cryptocurrencies store transactions in clear text, to facilitate the veri
cation of transactions by the community.
Clearly, an open blockchain de
es any basic understanding of privacy, since it virtually publicizes complete transaction histories of its users.
To address the lack of privacy, users of cryptocurrencies such as Bitcoin can obfuscate transactions by using temporary intermediate addresses [16]. However, in spite of such measures, with appropriate tools it is possible to analyze
ows and to a large extent link true senders with receivers [21, 8, 19].
In contrast, the cryptocurrency Monero, attempts to tackle the issue of privacy by storing only stealth, single-use addresses in a blockchain, and authenticating transactions with ring signatures. In this manner, there will be no e
ective way of linking senders with receivers nor
tracing the origins of funds [1].
Additionally, transaction amounts in the Monero blockchain are concealed behind cryptographic constructions, so as to complicate the task of inferringr currency
ows.
The result is a cryptocurrency with a high level of privacy.

Correctness

We can convince ourselves that the algorithm works by observing the following:

If $i \neq \pi$ then c'_{i+1} is defined as in the signature algorithm.

If $i = \pi$ then

$$z'_i = r_i G + c_i K_i = (\alpha - k_\pi c_\pi)G + c_\pi K_\pi = \alpha G$$
$$z''_i = r_i \mathcal{H}_p(\mathcal{R}) + c_i \tilde{K} = (\alpha - k_\pi c_\pi)\mathcal{H}_p(\mathcal{R}) + c_\pi k_\pi \mathcal{H}_p(\mathcal{R}) = \alpha \tilde{K}$$

So even in this case the expression $c'_{i+1} = \mathcal{H}_n(\mathcal{R}, \tilde{K}, \mathfrak{m}, z_n{}', z_n{}'')$ will equal c_{i+1}

Linkability.
Given a fixed set of public keys PuK = {PuK_1, PuK_2, PuK_3, PuK_4, PuK_5}, and two valid signatures for different messages ***m*** and ***m'***,

$$\sigma = (c_1,\ r_1,\ r_2,\ r_3,\ r_4,\ r_5,\ V)$$

$$\sigma' = (c_1', r_1', r_2', r_3', r_4', r_5', V')'''''$$

If **V=V'** then clearly both signatures come from the same signing ring and private key.
In other words, the signature scheme yields mutually linkable signatures in the case a ring and a private key would be re-used.

Exculpability - Pateisinamumas.
At the same time, given that **V = x_2•H**, we can readily see that linkability would only apply if private key **x_2** were re-used.
Hence, no other group/ring member could be accused of signing twice.

3.4 Borromean Ring Signatures [Monero]
We will see in later sections of this report that it will be necessary to prove that transaction amounts are within expected ranges. This can be acomplished with ring signatures. However, to this particular end it is not necessary that signatures be linkable, which allows us to select more e cient algorithms in terms of space consumed.
In this context, and for the speci
c purpose of proving amount ranges, Monero uses a signature
scheme developed by G. Maxwell, which he described in [15]. We present here a simpli
ed
version of the scheme, in that we will assume that we have the same number of keys for any
value of the
rst index i.
In our case, range proofs will require exactly 2 keys for each digit, so this simpli
cation will not
have any negative impact.
Assume that we have a set of public keys fKi;jg for i 2 f1; 2; :::; ng and j 2 f1; 2; :::;mg.
Furthermore, we assume also that for each i there is an index   i such that signer knows the
private key ki; i corresponding to Ki; i .
In what follows we will use m for the hash of the message concatenated with keys fKi;jg.