Sapling binding signature

$(\oplus, \ominus)$

- jubjub curve points (diamonds in the Sapling spec, couldn't find the right symbols)

$(\boxplus, \boxminus)$

- scalar field operators

$(+, -)$

- real world operators
- $a + b \mod{n} = a \boxplus b$

Pedersen Commitment

- $Com(v, rcv) = [v]V \oplus [rcv]R$

Notice:

- $Com(0, rcv) = [rcv]R$
- $Com(v, 0) = [v]V$

Setup

- $v= \sum_i v_i^{old} - \sum_j v_j^{new}$

net value of spend transfers minus net value of output transfers

- We have n

spend desc: $cv_i^{old} =Com(v_i^{old}, rcv_i^{old})= [v_i^{old}]V \oplus [rcv_i^{new}]R$

- And m

output desc: $cv_j^{new} =Com(v_j^{new}, rcv_j^{new})= [v_j^{new}]V \oplus [rcv_j^{new}]R$

Binding signature

An honest signer computes bsk

as:

$bsk = (\boxplus_i^n rcv_i^{old}) \boxminus (\boxplus_j^m rcv_j^{new})$

And bvk

is computed as

$(\bigoplus_i^n cv_i^{old}) \ominus (\bigoplus_j^m cv_j^{new}) \ominus Com(v, 0) =(\bigoplus_i^n cv_i^{old}) \ominus (\bigoplus_j^m cv_j^{new}) \ominus ([v]V \oplus [0]R)=$

$(\bigoplus_i^n cv_i^{old}) \ominus (\bigoplus_j^m cv_j^{new}) \ominus [v]V$

Now, let's do some math magic with the expression for bvk

here. Replace cvs with expressions:

1. $(\bigoplus_i^n ([v_i^{old}]V \oplus [rcv_i^{old}]R)) \ominus (\bigoplus_j^m ([v_j^{new}]V \oplus [rcv_j^{new}]R)) \ominus [v]V=$

Open the parentheses:

1. $(\bigoplus_i^n [v_i^{old}]V \oplus \bigoplus_i^n[rcv_i^{old}]R) \ominus (\bigoplus_j^m [v_j^{new}]V \oplus \bigoplus_j^m[rcv_j^{new}]R) \ominus [v]V=$
2. $(\bigoplus_i^n [v_i^{old}]V) \oplus (\bigoplus_i^n[rcv_i^{old}]R) \ominus (\bigoplus_j^m [v_j^{new}]V) \ominus (\bigoplus_j^m[rcv_j^{new}]R) \ominus [v]V=$

Now group by the generator (V or R):

1. ((\bigoplus_i^n [v_i^{old}]V) \ominus(\bigoplus_j^m [v_j^{new}]V)) \oplus
2. ((\bigoplus_i^n[rcv_i^{old}]R) \ominus (\bigoplus_j^m[rcv_j^{new}]R)) \ominus [v]V=

Now factor out the generators (here we change the operators because they aren't curve points anymore, they are scalars):

1. [\boxplus_i^n v_i^{old}]V \ominus [\boxplus_j^m v_j^{new}]V) \oplus

[\boxplus_i^nrcv_i^{old}]R \ominus [\boxplus_j^m rcv_j^{new}]R \ominus [v]V=

And merge (keep switching to scalar operations):

1. [\boxplus_i^n v_i^{old} \boxminus \boxplus_j^m v_j^{new}]V) \oplus [\boxplus_i^n rcv_i^{old} \boxminus \boxplus_j^m rcv_j^{new}]R) \ominus [v]V=

Here we can see that one of the expressions corresponds to bsk

:

1. [\boxplus_i^n v_i^{old} \boxminus \boxplus_j^m v_j^{new}]V) \oplus [bsk]R \ominus [v]V=

Rearrange and factor V out again:

1. [\boxplus_i^n v_i^{old} \boxminus \boxplus_j^m v_j^{new} \boxminus v]V) \oplus [bsk]R =

And if v \mod{r_J} = \boxplus_i^n [v_i^{old}] \boxminus \boxplus_j^m [v_j^{new}]

(r_j

– Jubjub scalar field):

1. [v]V \oplus [bsk]R \ominus [v]V=
2. [bsk]R = Com(0, bsk)

If the signature is valid with the validating key bvk

, it proves the signer's knowledge of bsk

with relation to bvk

: bvk = [bsk]R = [0]V \oplus [bsk]R = Com(0, bsk)

(because when a signature is correct it makes us believe that the signer knows the secret key, the general idea of signatures).

Wrong balance attack

Let v* = \sum_i v_i^{old} - \sum_j v_j^{new} - v

If v* \neq 0 \mod{r_J}

(the balance field v

in the tx doesn't represent the actual balance change) then bvk = Com(v*, bsk)

:

- from the line 10 above: (\boxplus_i^n [v_i^{old}] \boxminus \boxplus_j^m [v_j^{new}] \boxminus v)V) \oplus [bsk]R = [v]V \oplus [bsk]R = Com(v, bsk)

If the adversary can find bsk'

s.t. bvk = [bsk']R

(has to be done to pass the signature check) then

bvk = Com(0, bsk') = Com(v*, bsk)

which is impossible because of the binding property of the commitment scheme