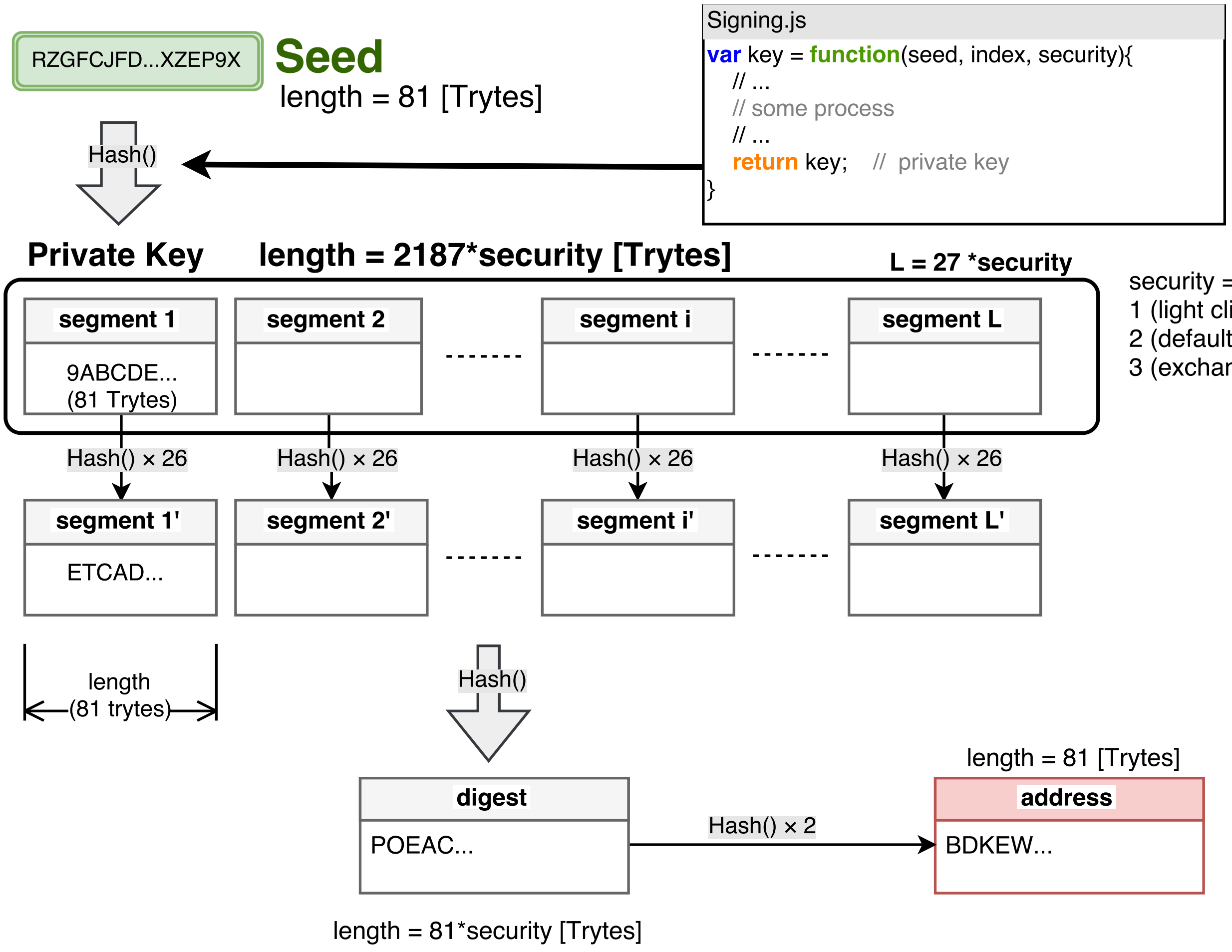
IOTA Address Generation Cheat Sheet ver.1

@abmushi



RZGFCJFD...XZEP9X

Seed
length = 81 [Trytes]

Signing.js

```
var key = function(seed, index, security){
   // ...
   // some process
   // ...
   return key;   //  private key
}
```

seed（81 Trytes）
index（>=0）、
security（>0）

Hash()

Private Key **length = 2187*security [Trytes]**

L = 27 *security

security =
1 (light client)
2 (default wallet)
3 (exchange level security)

segment 1
9ABCDE...
(81 Trytes)

segment 2

----

segment i

----

segment L

Hash() × 26

Hash() × 26

Hash() × 26

Hash() × 26

segment 1'
ETCAD...

segment 2'

----

segment i'

----

segment L'

length
(81 trytes)

Hash()

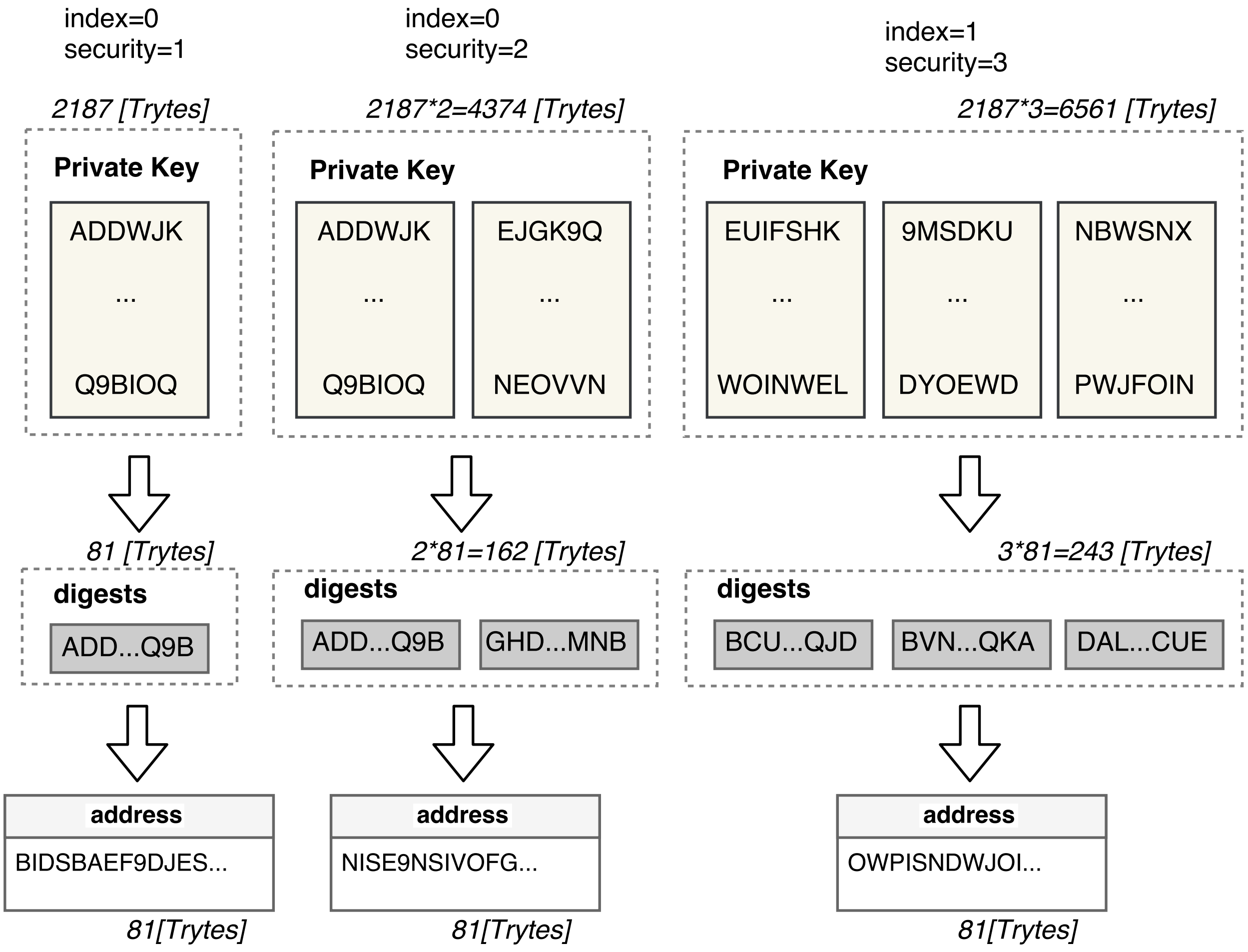
digest
POEAC...

length = 81*security [Trytes]

Hash() × 2

length = 81 [Trytes]

address
BDKEW...



index=0
security=1

2187 [Trytes]

Private Key

ADDWJK
...
Q9BIOQ

81 [Trytes]

digests

ADD...Q9B

address
BIDSBAEF9DJES...

81[Trytes]

index=0
security=2

*2187*2=4374 [Trytes]*

Private Key

ADDWJK
...
Q9BIOQ

EJGK9Q
...
NEOVVN

*2*81=162 [Trytes]*

digests

ADD...Q9B

GHD...MNB

address
NISE9NSIVOFG...

81[Trytes]

index=1
security=3

*2187*3=6561 [Trytes]*

Private Key

EUIFSHK
...
WOINWEL

9MSDKU
...
DYOEWD

NBWSNX
...
PWJFOIN

*3*81=243 [Trytes]*

digests

BCU...QJD

BVN...QKA

DAL...CUE

address
OWPISNDWJOI...

81[Trytes]