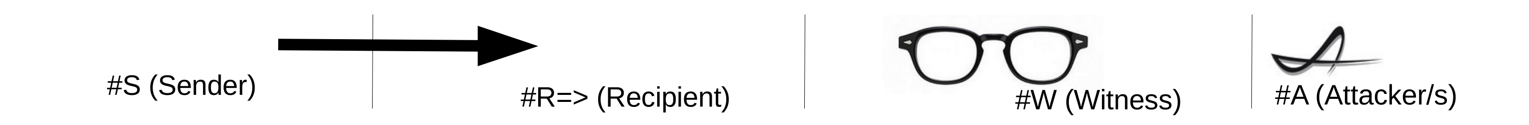
The Inner Identifier and Outer Mask (IIaOM) protocol for producing reputation and transaction records based on public hashed picture, private map and picture of sender, transactions and transferred objects.

Feature: peer to peer means of registration with scalable anonymity, usable for scaling to onion the problem of equality (in democracy) and accountability (for any morality in representation) being invalidated by anonymity.

Author: Namzezam, Erez Elul. http://namzezam.wikidot.com/blog:12

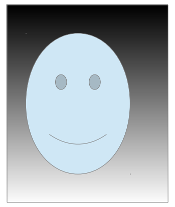
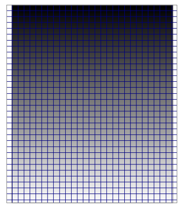
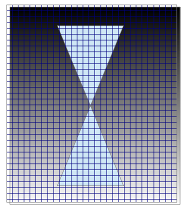
To anon: please improve this + Why let the state the monopoly over identities bind with transactions?

players

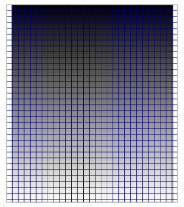


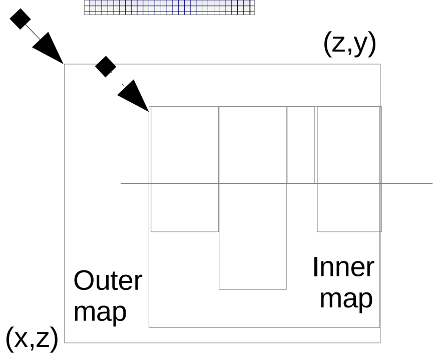
#S (Sender) → #R=> (Recipient) | #W (Witness) | #A (Attacker/s)

Elements

Privately: meet(#S) in person or online	Private: picture(#S)	Private: Map(picture(#S))	Public: H(picture(#S))	Encrypted for xy	Signed by xy
				🔒 xy	✓ xy

Creating the H(picture(#S)) and publicly using it:

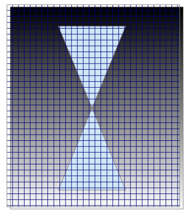




Forming n maps, each is an ordered set of side by side rectangles over a picture, by starting from the inner to the outer and having the locating point of the inner in its outer after ending the inner one, while using stream of pair of random numbers, each defines a rectangle, where

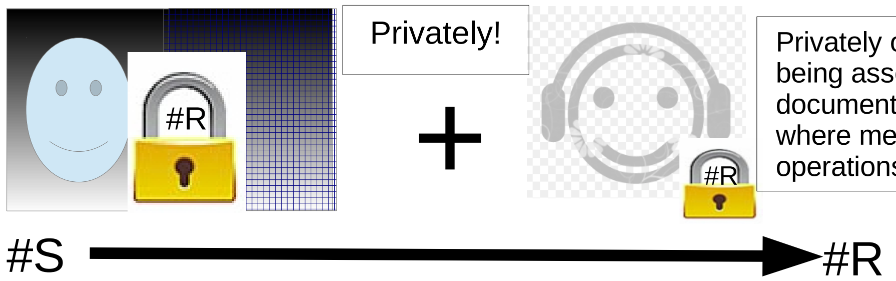
- at each corner the rectangle is re-defined to exclude the minimum height/width after walking vertically/horizontally;
- the data in the rectangle is hashed (eg. by SHA-3); and
- hash is put into array which is finally hashed to produce the H(picture), such that, each map is defined when one of the pairs number equals z,
  - either as x=z, so that the x axis of the map ends in this pair and the y axis is the number on pairs to use to complete the map while walking in the clock or the vertical returning direction, or
  - as y=z so that the y axis of the map ends in this pair and the x axis is the number on pairs to use to complete the map while walking the clock reverse or the horizontal returning direction,
  - and where any another found z defines a switch between the clock or returning methods in the next corner.

Conventions: z=zero=0, starting-point=TopLeftCorner,MaxNumber=256.



#S shows the public link having her/his H(picture(#S)) and #R gets it.

From here we get localized for requiring #A, the attacker, to interact with each victim in addition to any accessing data :



Privately or in crypto party fashion done, but without being associated with any governmental document/data. This is the most sensitive part, where meet(#S) could be made separated. Bulk operations by #A are harder to be made.

Object - the subject being transferred, such as a coin, money , ownership, delivery or document of accountability etc.

And now, the event is distribute encrypted for each of #w, the witness/es, being a community member or their operator/s:

#S → #W

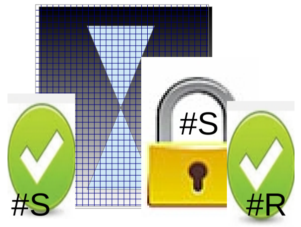
{^o , ^t(object), password, secret }

Objects(^o -> {H(^t), symmetrically-encrypted-for-#S(secret)})

#S sends ^o (the id of the object), the ^t(id of the last transaction of this object) and both: the secret and the password by which the secret is reviled, where the secret may also be a different password and where both are generated per each object or transaction separately.

For the prove of privilege of being #S: #R keeps the ^t(object) and the password of the secret.

For hiding correlation, objects are verified and updated immediately (including creating new ^t secret and password by #R), while logs are updated at once and periodically, only after passing the confirmation process, (including having the existing hash been successfully checked and the secret being unlocked by password, by each #W), for proving #S being the privileged for transferring each of those object!



#R → #W

The stamped(#S&#R) is sent to both logs

- Reputation(^r(#S)->stamped(#S&#R)),
  - where the Reputation is of #S;
- Transactions(^t->stamped(#S&#R)),
  - where hash of ^t is stored in the transferred object.

stamped(#S&#R) = sign_by#S_and#R(encrypted-for-#S(H(picture(#S)))).
#S should sign to prevent #A from pretending to be #R and signing false stamp.