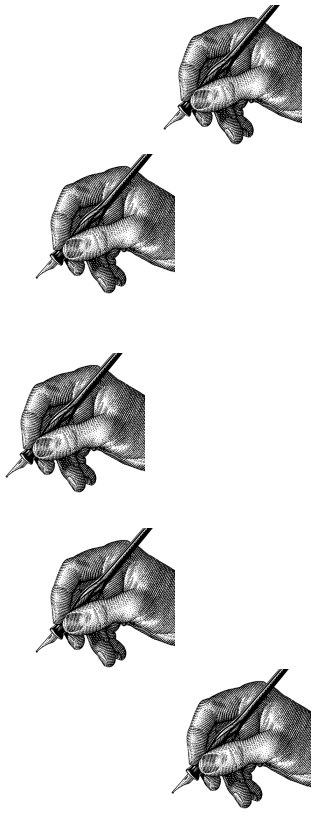
Graded Signatures

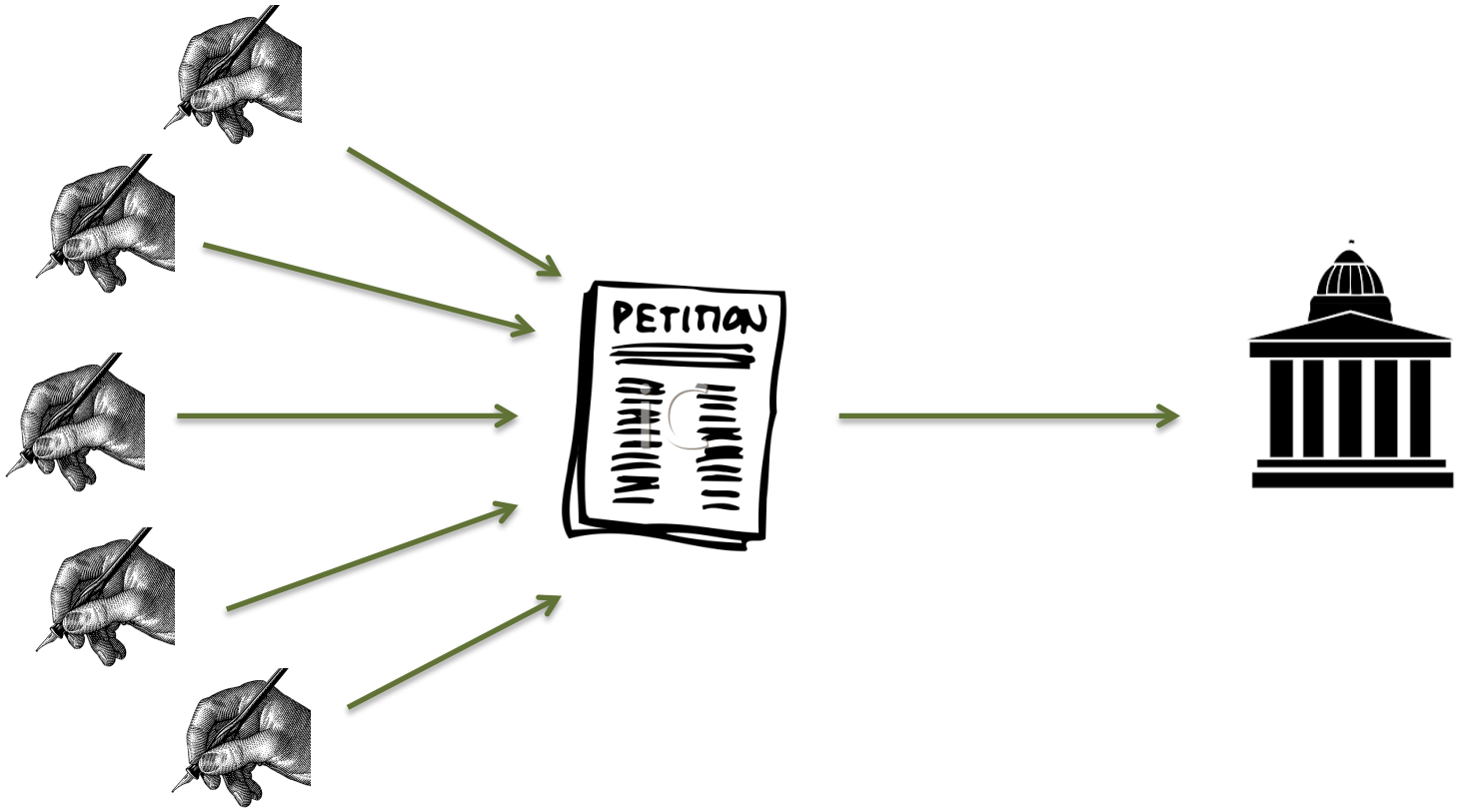
Murat Osmanoglu

joint work with Aggelos Kiayias and Qiang Tang

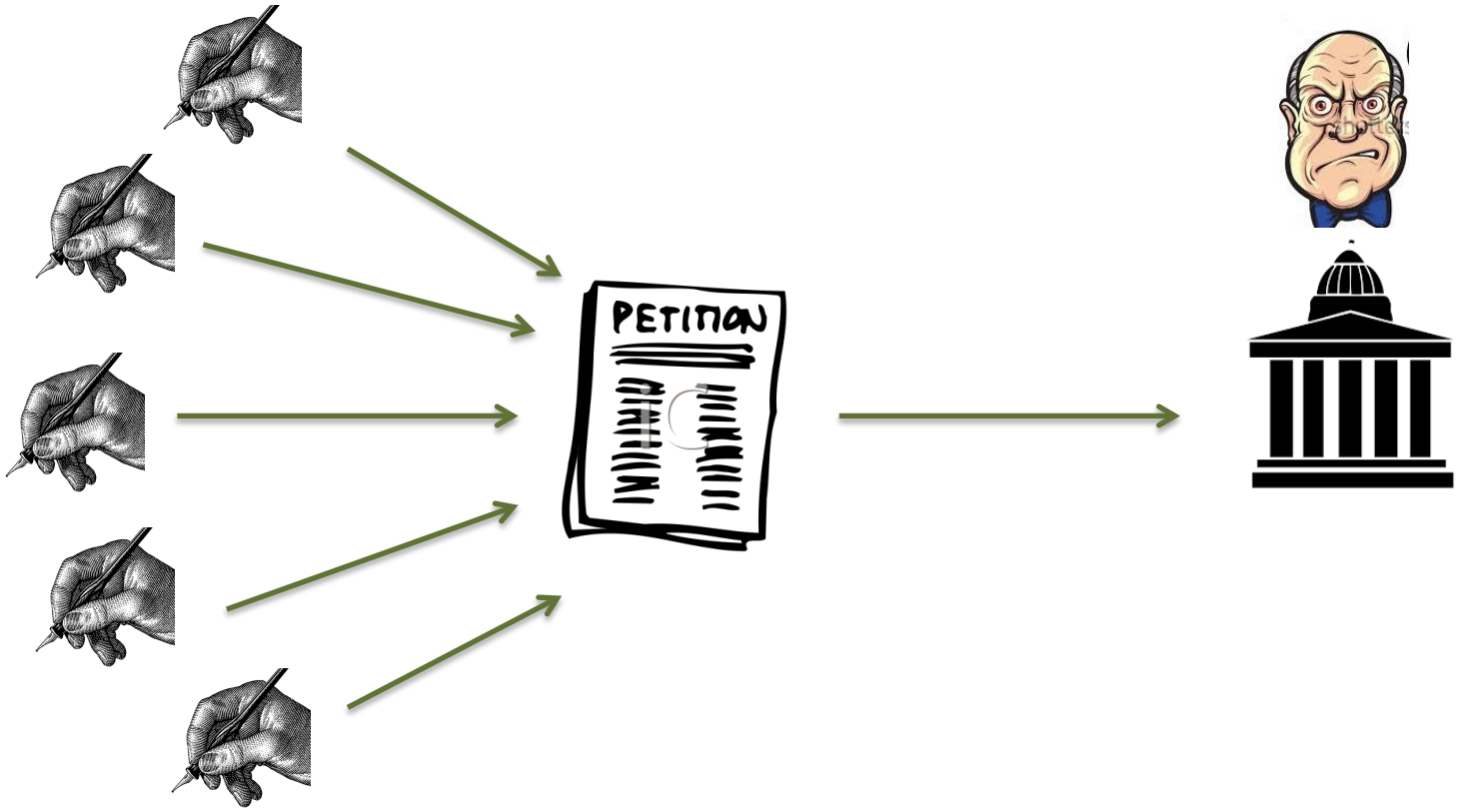
a petition system



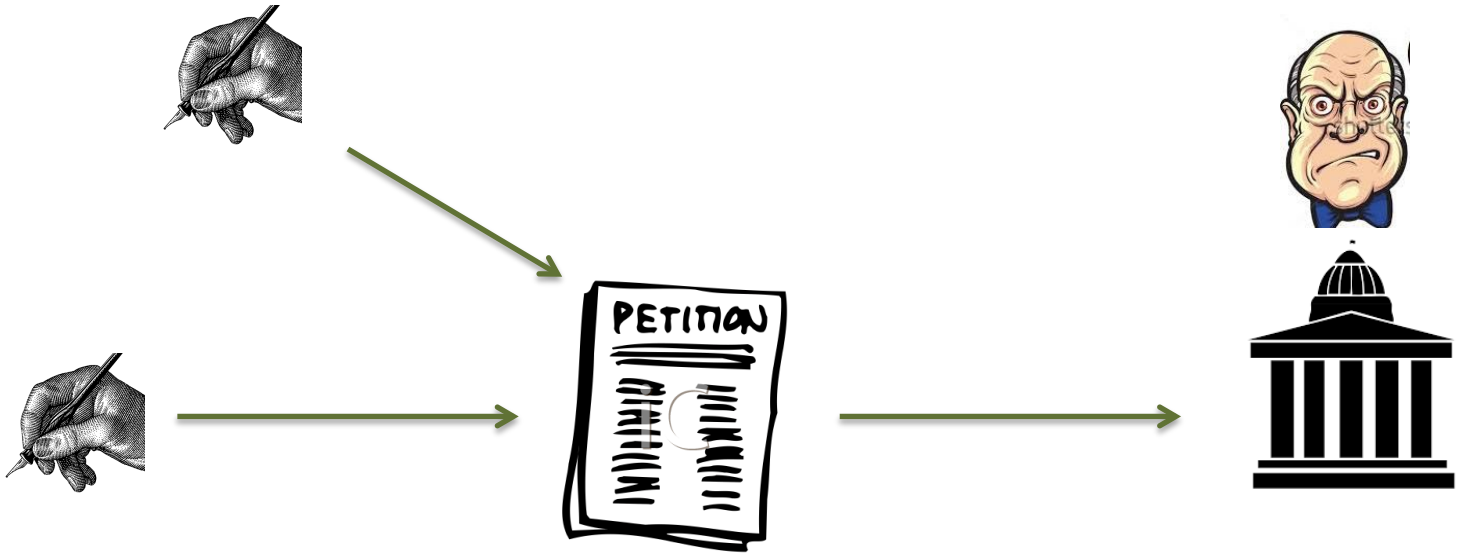
a petition system



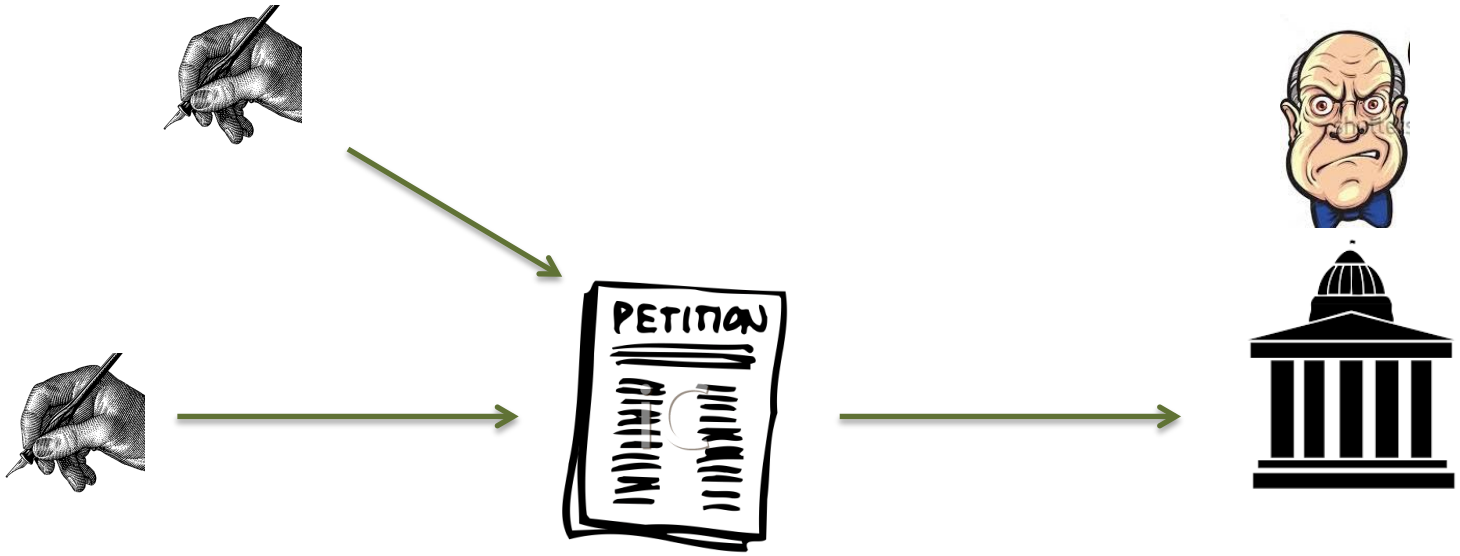
a petition system



a petition system

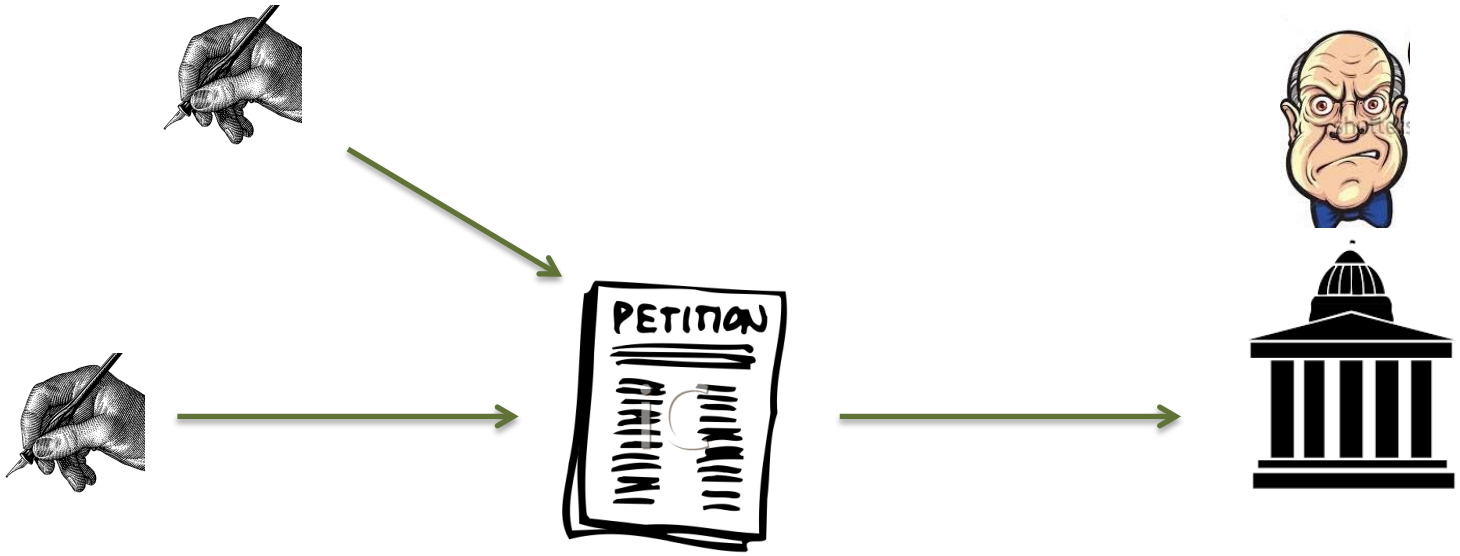


a petition system



- Privacy ?

a petition system

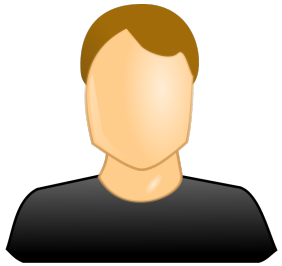


- Privacy ?
- Efficiency ?

Graded Signatures

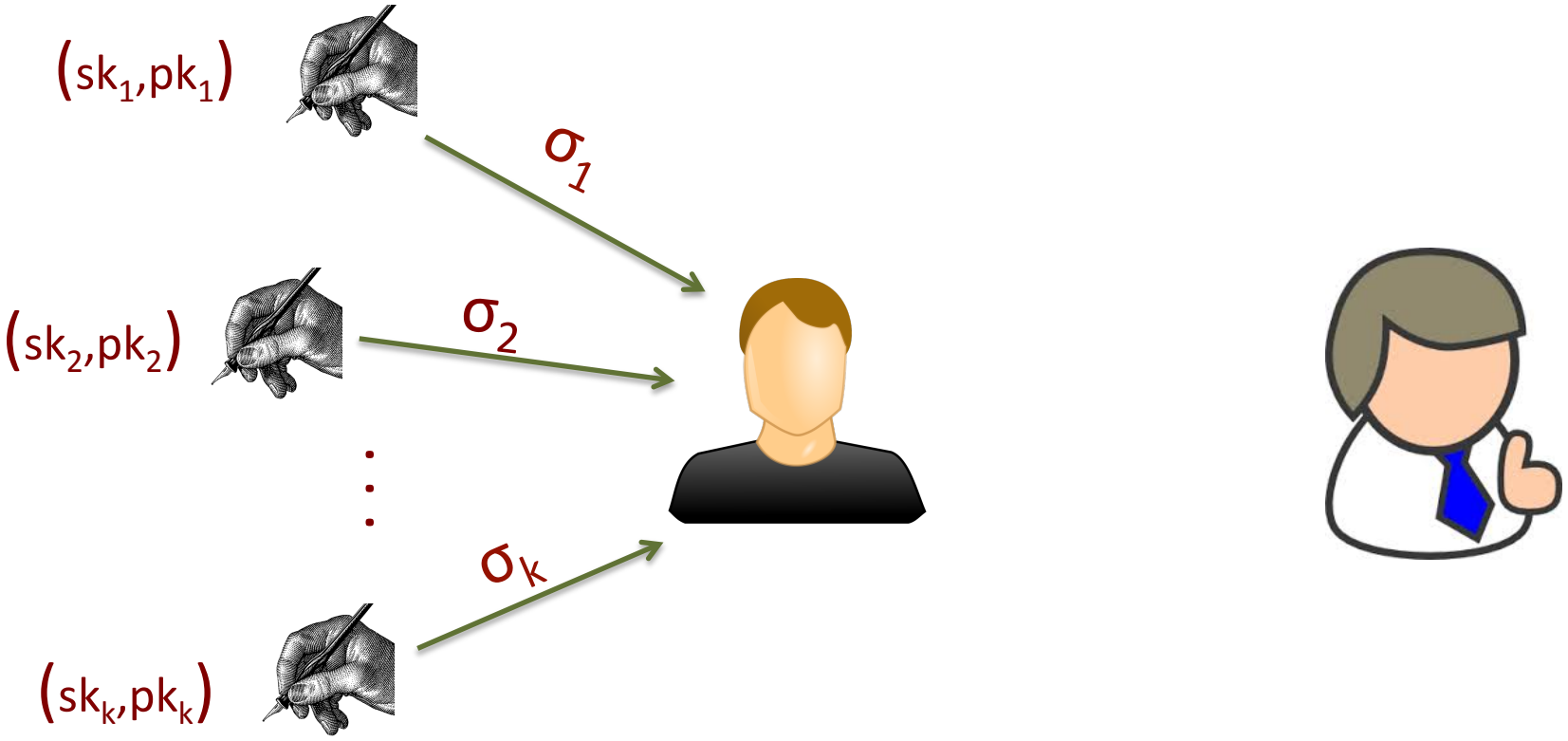
(sk_1, pk_1) 

(sk_2, pk_2) 

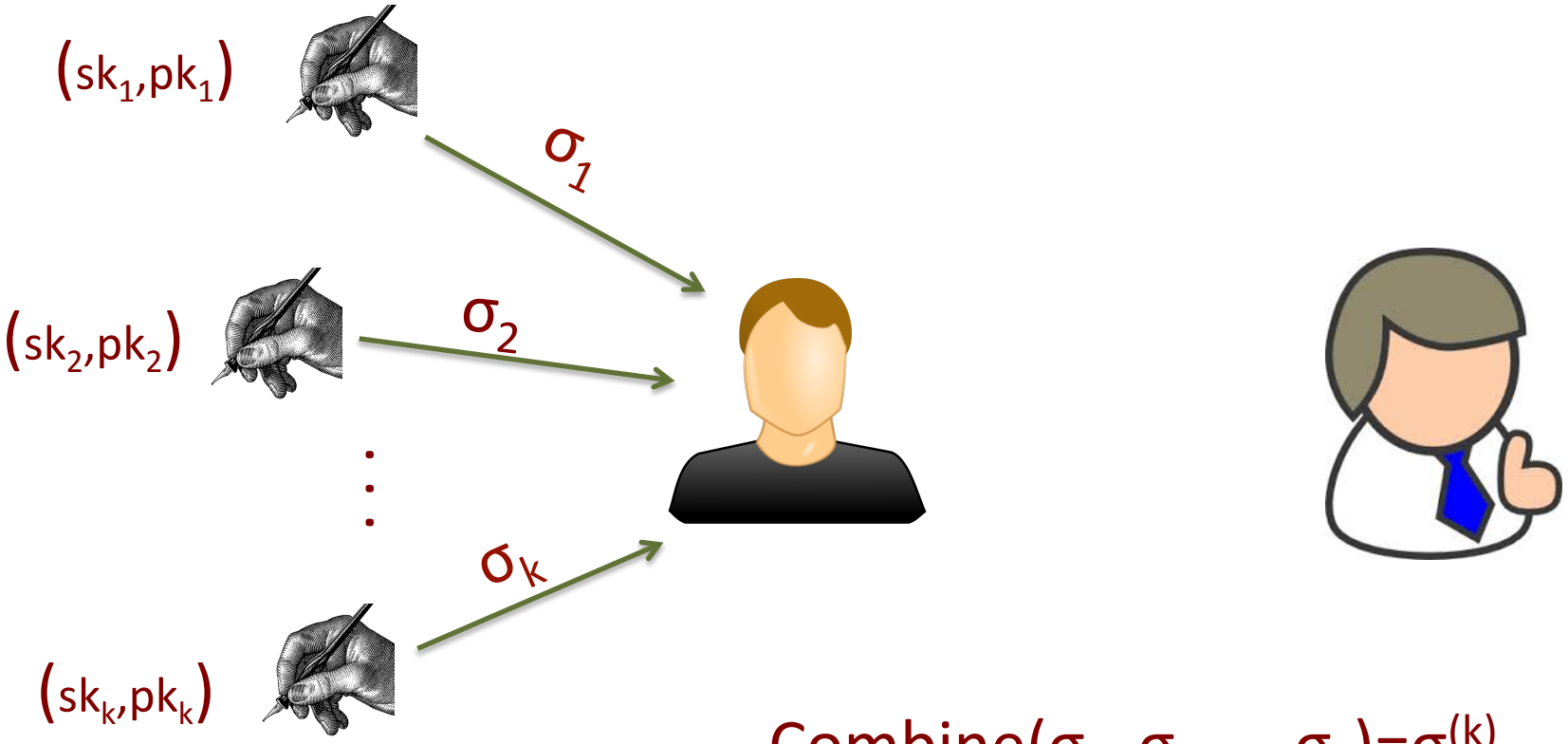


(sk_k, pk_k) 

Graded Signatures

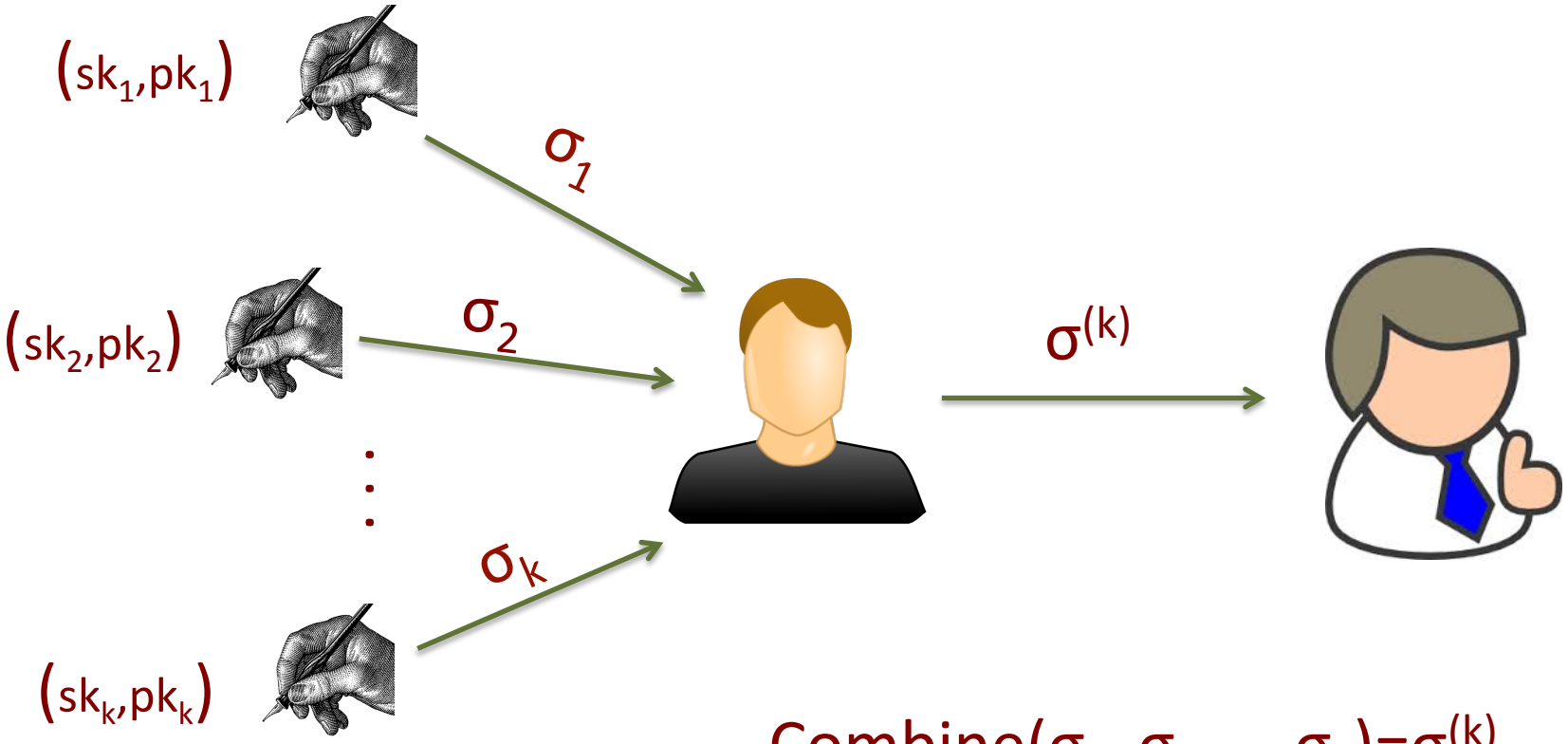


Graded Signatures



$$\text{Combine}(\sigma_1,\sigma_2,\ldots,\sigma_k)=\sigma^{(k)}$$

Graded Signatures



$\text{Combine}(\sigma_1,\sigma_2,\ldots,\sigma_k)=\sigma^{(k)}$

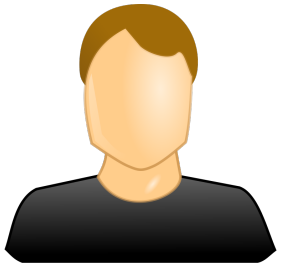
Graded Signatures

(sk_1, pk_1) 

(sk_2, pk_2) 

$\vdots$

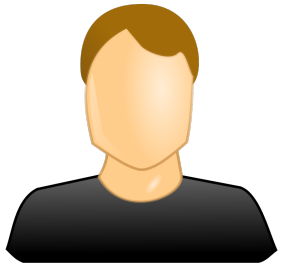
(sk_k, pk_k) 



Graded Signatures

(sk_1, pk_1) 

(sk_2, pk_2) 



(sk_k, pk_k) 

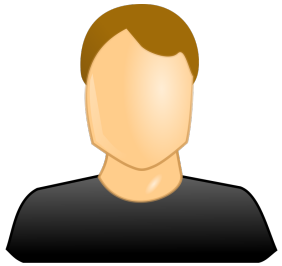
(gsk)

Setup(λ)=(gsk,gpk)

Graded Signatures

(sk_1,pk_1) 

(sk_2,pk_2) 



(sk_k,pk_k) 

pk_k

(gsk)

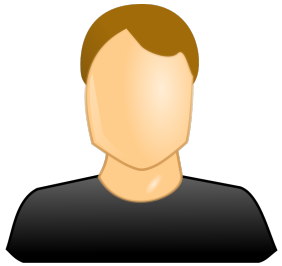
$Reg(pk_k,gsk)=cert_k$

$Setup(\lambda)=(gsk,gpk)$

Graded Signatures

(sk_1,pk_1)
$cert_1$

(sk_2,pk_2)
$cert_2$



(sk_k,pk_k)
$cert_k$

pk_k

$cert_k$

(gsk)

$Reg(pk_k,gsk)=cert_k$

$Setup(\lambda)=(gsk,gpk)$

Graded Signatures

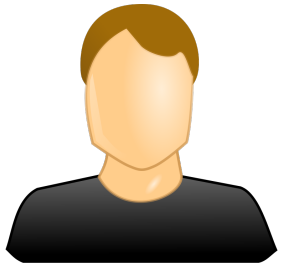
$\mathsf{Sign}(sk_1,m) = \sigma_1$

(sk_1,pk_1)

$cert_1$

(sk_2,pk_2)

$cert_2$



(sk_k,pk_k)

$cert_k$

pk_k

$cert_k$

$\mathsf{Reg}(pk_k,gsk)=cert_k$

(gsk)

$\mathsf{Setup}(\lambda)=(gsk,gpk)$

Graded Signatures

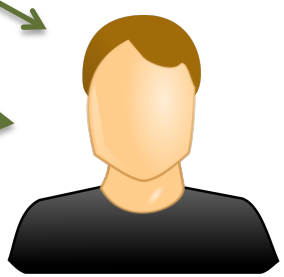
$\text{Sign}(sk_1, m) = \sigma_1$

(sk_1, pk_1)
$cert_1$

σ_1

(sk_2, pk_2)
$cert_2$

σ_2



σ_k

(sk_k, pk_k)
$cert_k$

pk_k

$cert_k$

(gsk)

$\text{Reg}(pk_k, gsk) = cert_k$

$\text{Combine}(m, gpk, \sigma_1, \sigma_2, \ldots, \sigma_k) = \sigma^{(k)}$

$\text{Setup}(\lambda) = (gsk, gpk)$

Graded Signatures

$\text{Sign}(sk_1, m) = \sigma_1$

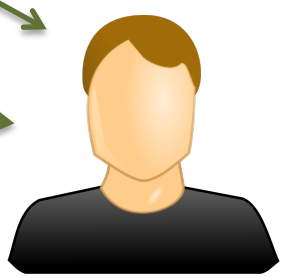
(sk_1, pk_1)
cert_1

σ_1

$\text{Verify}(gpk, \sigma^{(k)}, m, k) = 1 \text{ or } 0$

(sk_2, pk_2)
cert_2

σ_2



$\sigma^{(k)}$

σ_k

(sk_k, pk_k)
cert_k

$\text{Combine}(m, gpk, \sigma_1, \sigma_2, \ldots, \sigma_k) = \sigma^{(k)}$

pk_k

cert_k

(gsk)

$\text{Reg}(pk_k, gsk) = \text{cert}_k$

$\text{Setup}(\lambda) = (gsk, gpk)$

Graded Signatures

- *Correctness* : if the user combines k valid signatures σ_i on m under k different certified public keys using Combine alg. into the signature $\sigma^{(k)}$, then Verify alg outputs 1 on $\sigma^{(k)}$

Unforgeability of GS

gpk

Unforgeability of GS

gpk →

← $S = (i_1,\ldots,i_q)$

$(sk_{(i,1)},\ldots,sk_{(i,q)})$ →

Unforgeability of GS

gpk →

← $S = (i_1,\ldots,i_q)$

→ $(sk_{(i,1)},\ldots,sk_{(i,q)})$

← (i,m)

→ $(\sigma_i \text{ on } m)$

Unforgeability of GS

gpk →

← $S = (i_1,\ldots,i_q)$

→ $(sk_{(i,1)},\ldots,sk_{(i,q)})$

← (i,m)

→ $(\sigma_i \text{ on } m)$

← $(\sigma^{(k)},m^*,k)$

Unforgeability of GS

gpk →

← $S = (i_1,\ldots,i_q)$

← $(sk_{(i,1)},\ldots,sk_{(i,q)})$

← (i,m)

← $(\sigma_i \text{ on } m)$

← $(\sigma^{(k)},m^*,k)$

q' is # of queries (i, m^*) where i not in S

$q + q' < k$

Unforgeability of GS

gpk →

← $S = (i_1,\ldots,i_q)$

← $(sk_{(i,1)},\ldots,sk_{(i,q)})$

← (i,m)

← $(\sigma_i \text{ on } m)$

← $(\sigma^{(k)},m^*,k)$

q' is # of queries (i, m^*) where i not in S

$q + q' < k$

For any ppt adversary A, if the probability of A outputting a valid signature $\sigma^{(k)}$ is negligible function, then graded signature scheme is existentially unforgeable under adaptive corruption

Anonymity of GS

(gsk,gpk)

Anonymity of GS

(gsk,gpk)

(S_0,S_1,D_0,D_1,m,k)

- a message m,
- a grade k,
- two different sets of signers S_1 and S_0
- $D_0=\{\sigma_i\}$, $D_1=\{\sigma_j\}$.

Anonymity of GS

(gsk,gpk)

(S_0,S_1,D_0,D_1,m,k)

$(\sigma_b^{(k)},m,k)$

b'

- a message m,
- a grade k,
- two different sets of signers S_1 and S_0
- $D_0=\{\sigma_i\}$, $D_1=\{\sigma_j\}$.

Anonymity of GS

(gsk,gpk)

(S_0,S_1,D_0,D_1,m,k)

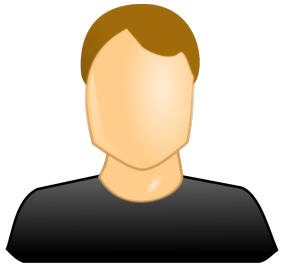
$(\sigma_b^{(k)},m,k)$

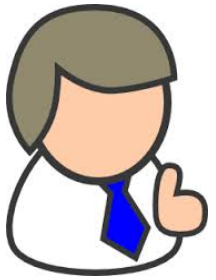
b'

- a message m,
- a grade k,
- two different sets of signers S_1 and S_0
- $D_0=\{\sigma_i\}$, $D_1=\{\sigma_j\}$.

For any ppt adversary A, if the probability of guessing bit correctly is negligibly close to ½, then graded signature scheme is fully anonymous.

construction for GS

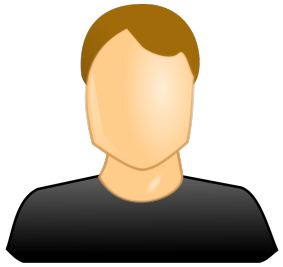


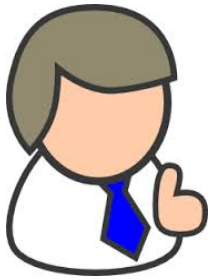


(sk_k, pk_k)

(gsk,gpk)

construction for GS



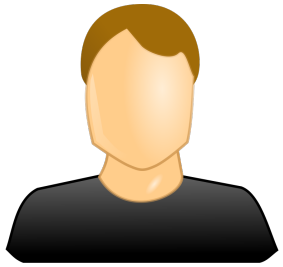


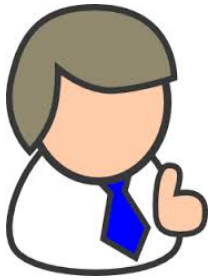
(sk_k, pk_k)

pk_k

(gsk,gpk)

construction for GS





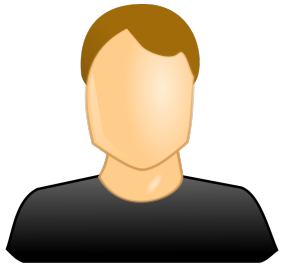
(sk_k, pk_k)

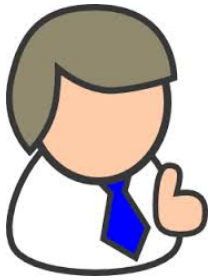
pk_k

(gsk,gpk)

$Sign(gsk, pk_k) = cert_k$

construction for GS





(sk_k, pk_k)

pk_k

$cert_k$

(gsk, gpk)

$Sign(gsk, pk_k) = cert_k$

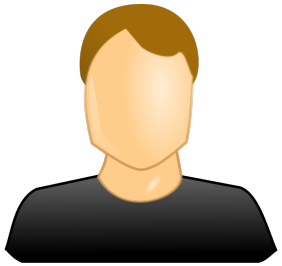
construction for GS

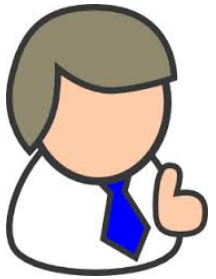
(sk_1,pk_1)

$cert_1$

(sk_2,pk_2)

$cert_2$





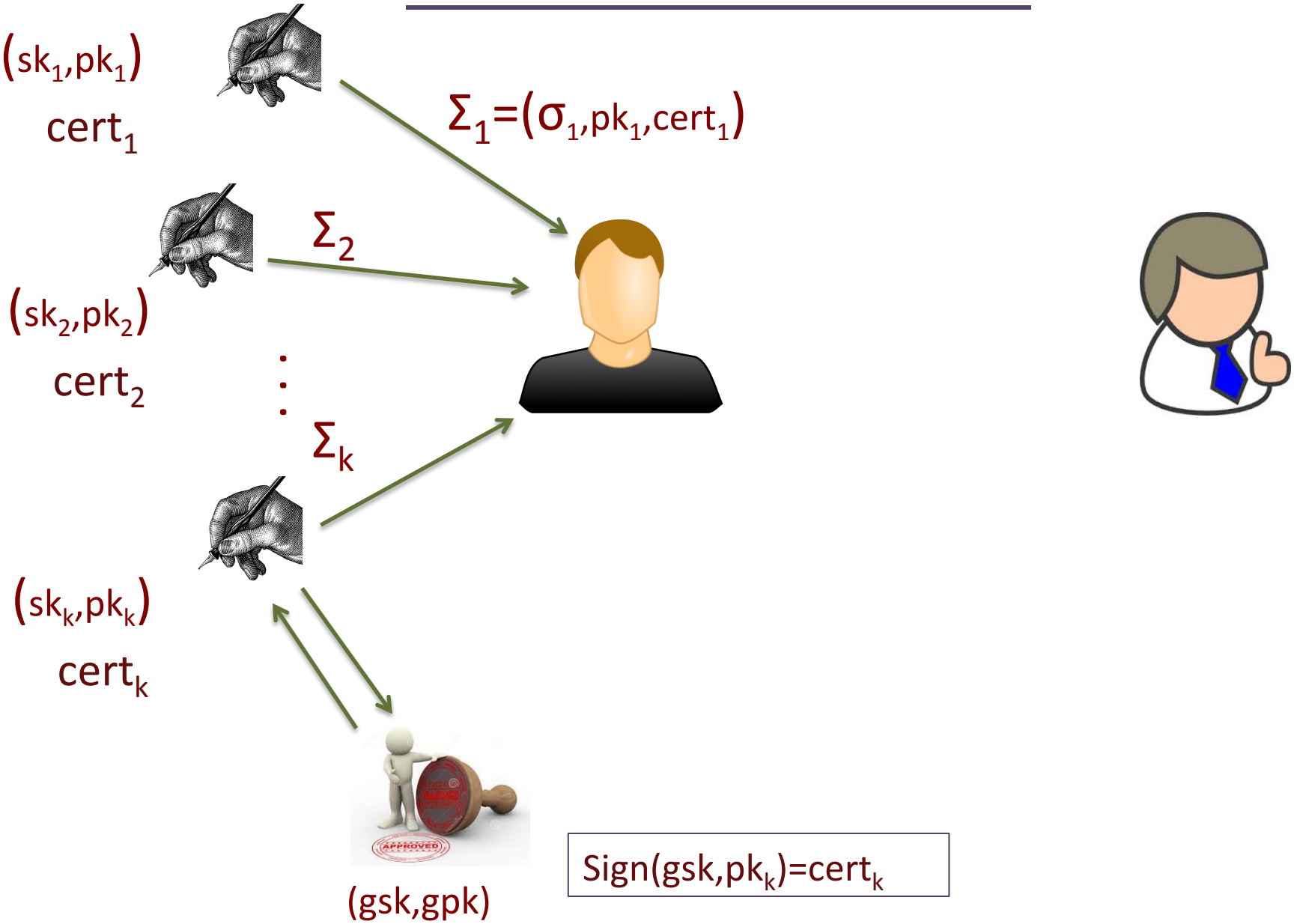
(sk_k,pk_k)

$cert_k$

(gsk,gpk)

$Sign(gsk,pk_k)=cert_k$

construction for GS



construction for GS

(sk_1,pk_1)

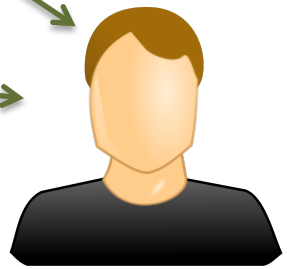
$cert_1$

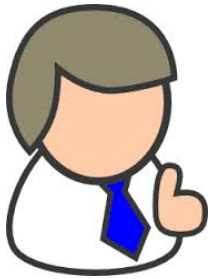
$\Sigma_1=(\sigma_1,pk_1,cert_1)$

Σ_2

(sk_2,pk_2)

$cert_2$





Σ_k

(sk_k,pk_k)

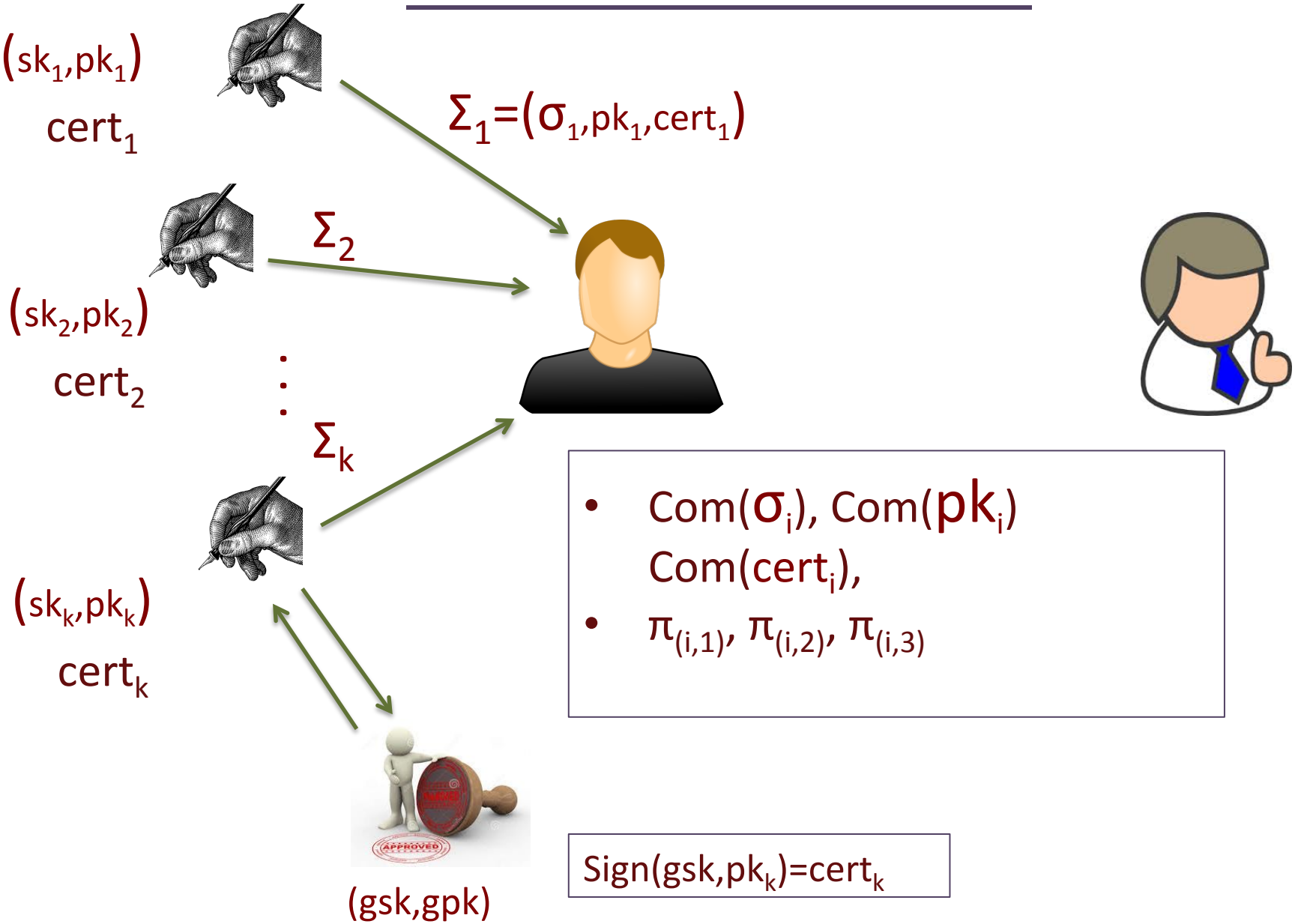
$cert_k$

- $Com(\sigma_i)$, $Com(pk_i)$ $Com(cert_i)$,

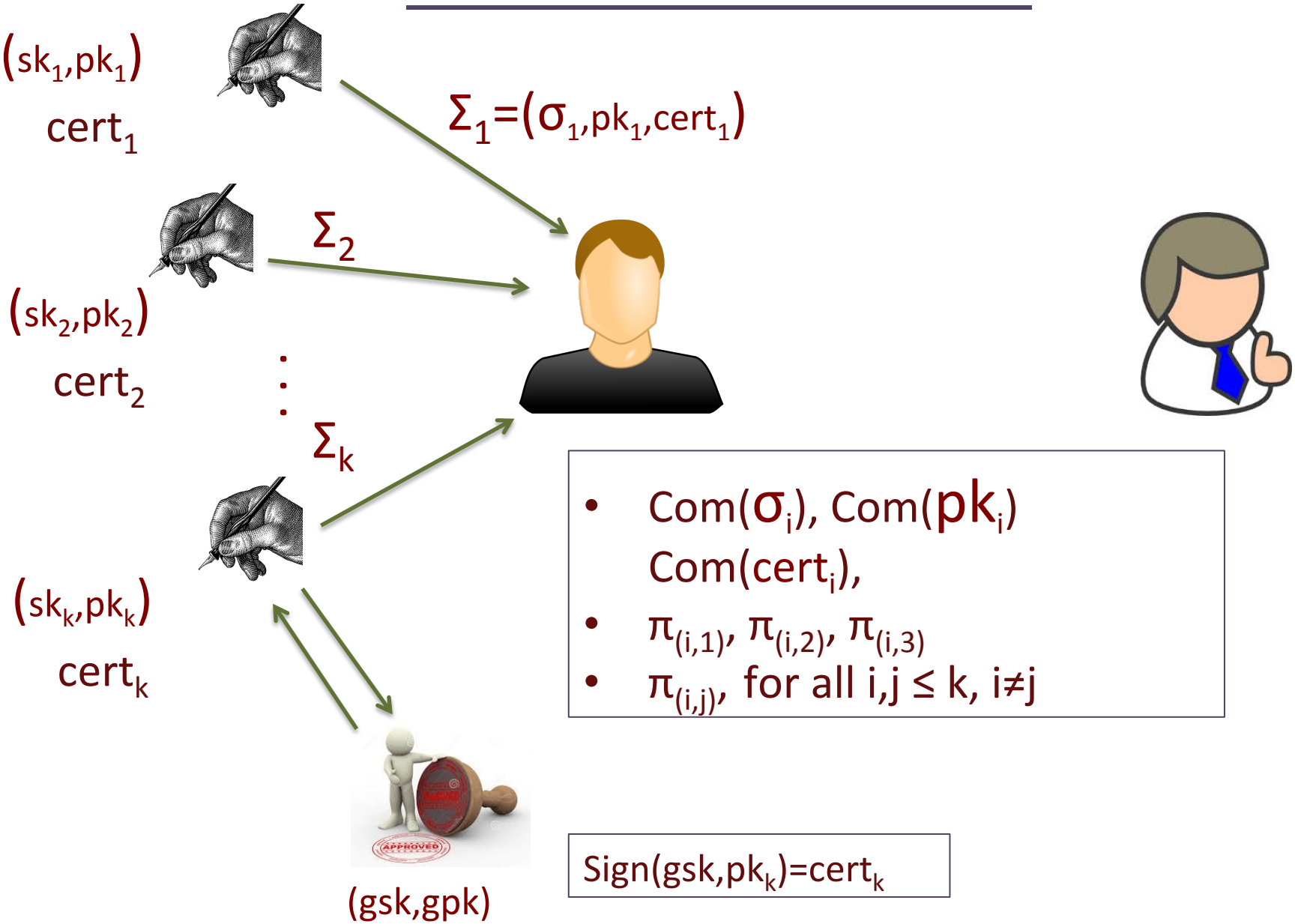
(gsk,gpk)

$Sign(gsk,pk_k)=cert_k$

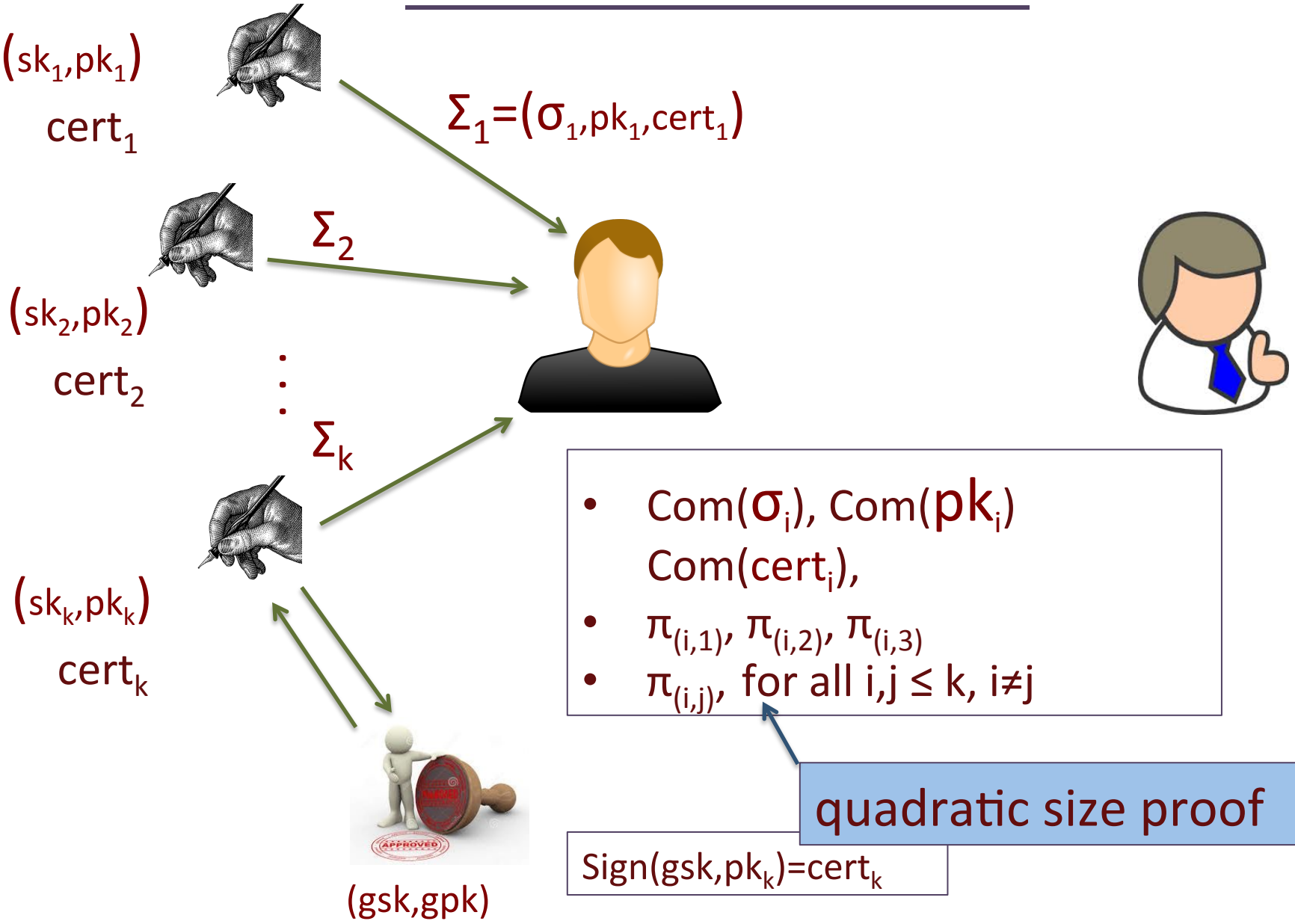
construction for GS



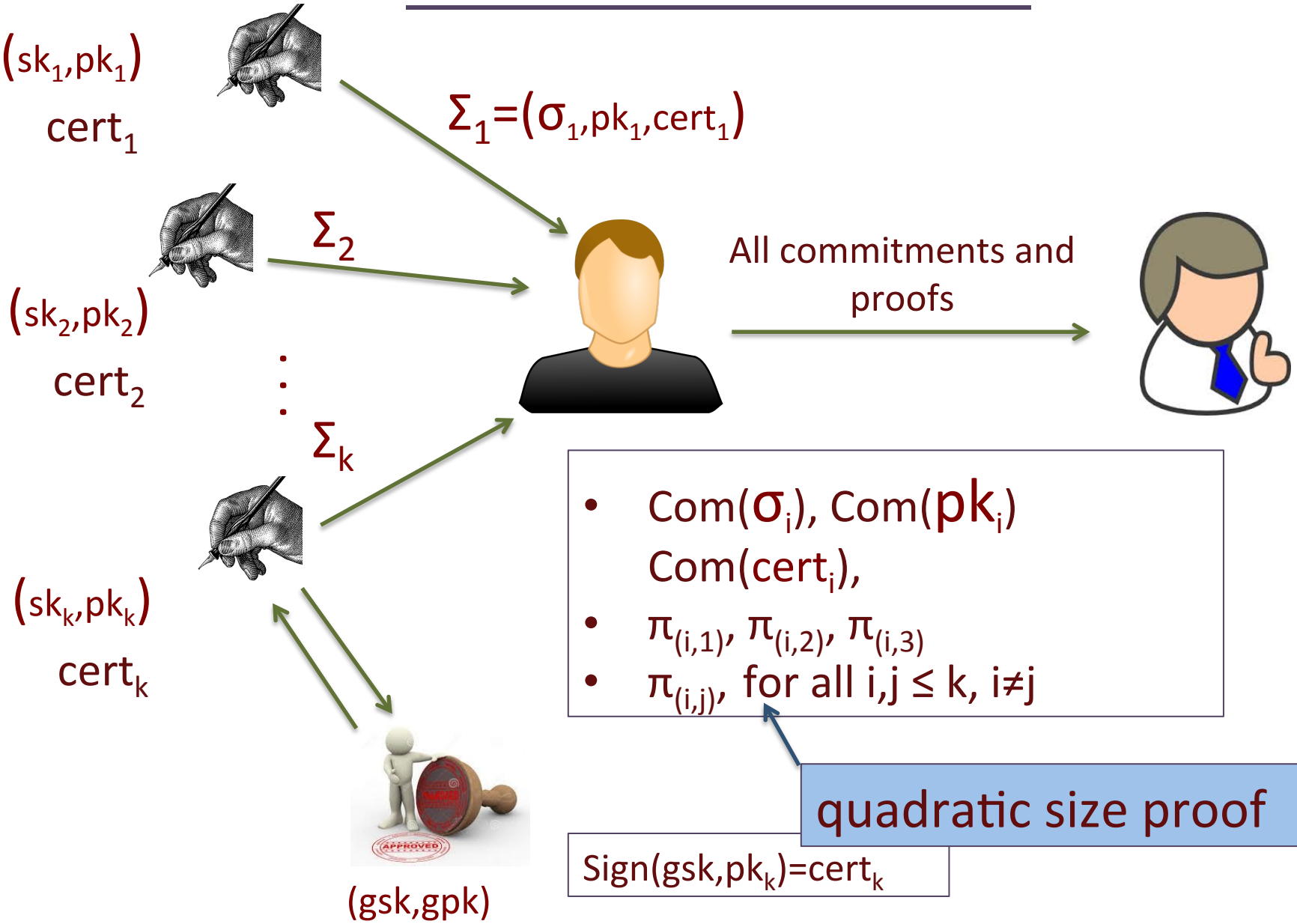
construction for GS



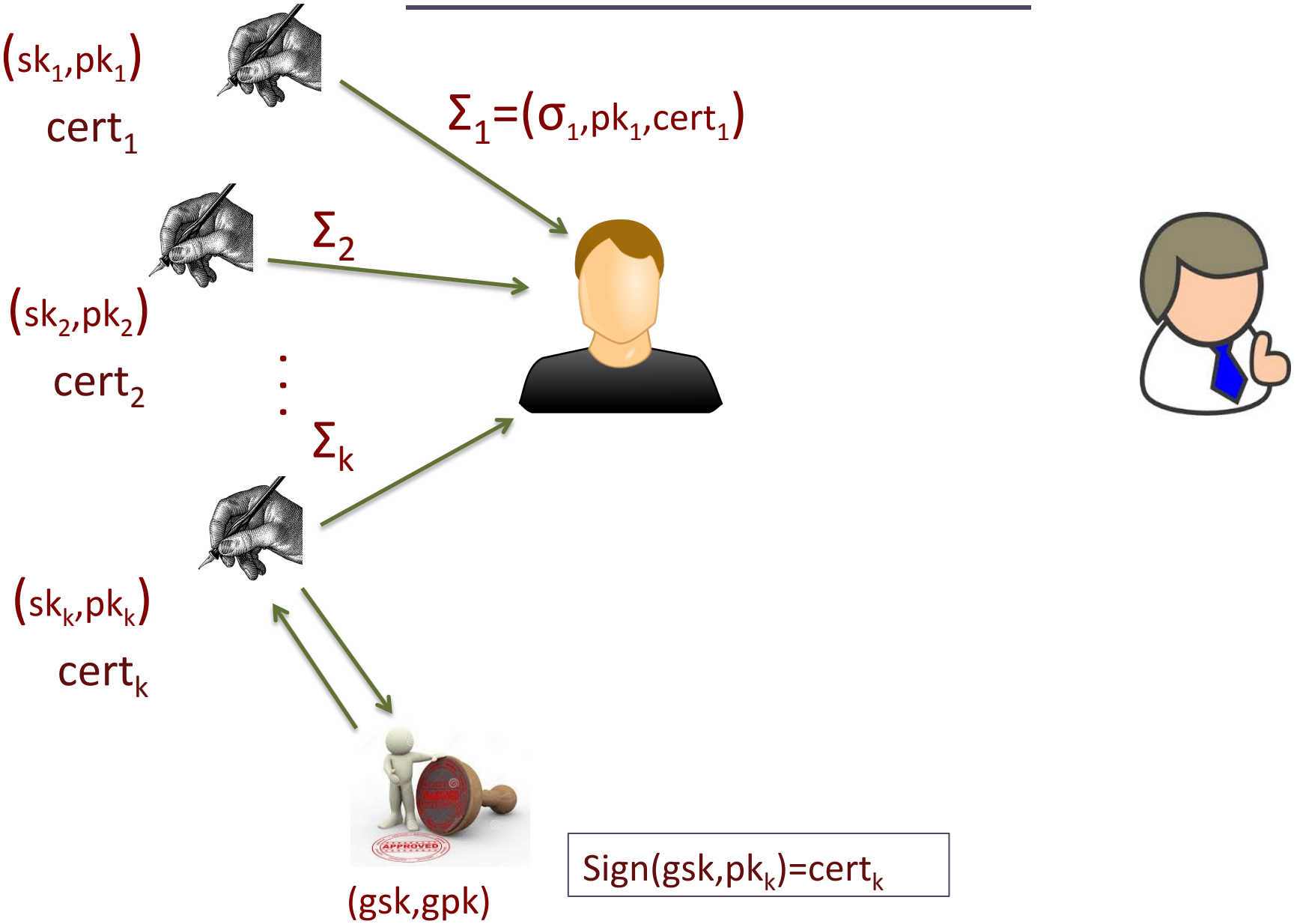
construction for GS



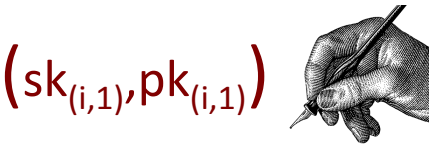
construction for GS



construction for GS



construction for GS



$(sk_{(i,1)},pk_{(i,1)})$

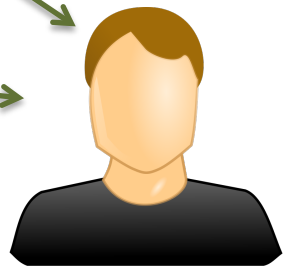
$cert_{(i,1)}$

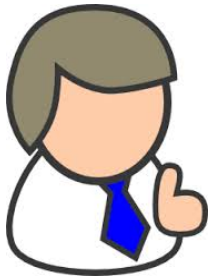
$\Sigma_{(i,1)}=(\sigma_{(i,1)},pk_{(i,1)},cert_{(i,1)},i_1)$

$\Sigma_{(i,2)}$

$(sk_{(i,2)},pk_{(i,2)})$

$cert_{(i,2)}$





$\Sigma_{(i,k)}$

$(sk_{(i,k)},pk_{(i,k)})$

$cert_{(i,k)}$

(gsk,gpk)

$Sign(gsk,(i_k,pk_{(i,k)}))=cert_{(i,k)}$, $1 \le i_k \le n$.

construction for GS

$(sk_{(i,1)},pk_{(i,1)})$

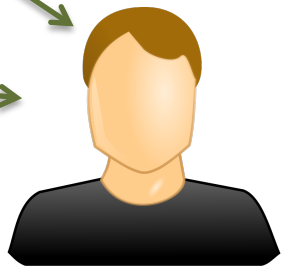
$cert_{(i,1)}$

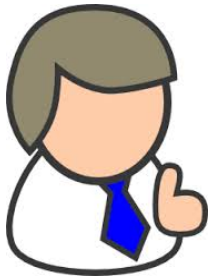
$\Sigma_{(i,1)}=(\sigma_{(i,1)},pk_{(i,1)},cert_{(i,1)},i_1)$

$\Sigma_{(i,2)}$

$(sk_{(i,2)},pk_{(i,2)})$

$cert_{(i,2)}$





$\Sigma_{(i,k)}$

$(sk_{(i,k)},pk_{(i,k)})$

$cert_{(i,k)}$

(gsk,gpk)

- Assume $i_1 > i_2 > \ldots > i_k$

$Sign(gsk,(i_k,pk_{(i,k)}))=cert_{(i,k)}$, $1 \le i_k \le n$.

construction for GS

$(sk_{(i,1)},pk_{(i,1)})$

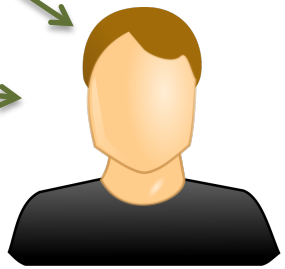
$cert_{(i,1)}$

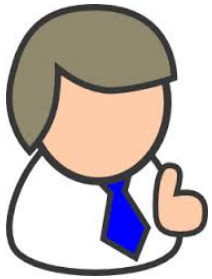
$\Sigma_{(i,1)}=(\sigma_{(i,1)},pk_{(i,1)},cert_{(i,1)},i_1)$

$\Sigma_{(i,2)}$

$(sk_{(i,2)},pk_{(i,2)})$

$cert_{(i,2)}$





$\Sigma_{(i,k)}$

$(sk_{(i,k)},pk_{(i,k)})$

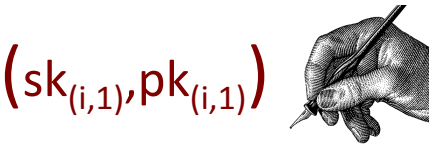
$cert_{(i,k)}$

(gsk,gpk)

- Assume $i_1 > i_2 > \ldots > i_k$
- $Com(\sigma_{(i,j)})$, $Com(pk_{(i,j)})$ $Com(cert_{(i,j)})$,

$Sign(gsk,(i_k,pk_{(i,k)}))=cert_{(i,k)}$, $1 \le i_k \le n$.

construction for GS



$(sk_{(i,1)}, pk_{(i,1)})$

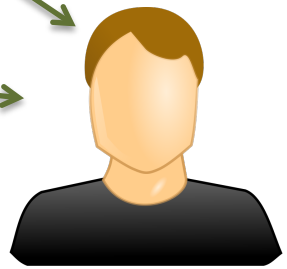
$cert_{(i,1)}$

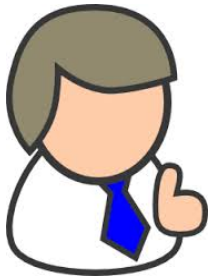
$\Sigma_{(i,1)}=(\sigma_{(i,1)}, pk_{(i,1)}, cert_{(i,1)}, i_1)$

$\Sigma_{(i,2)}$

$(sk_{(i,2)}, pk_{(i,2)})$

$cert_{(i,2)}$





$\Sigma_{(i,k)}$

$(sk_{(i,k)}, pk_{(i,k)})$

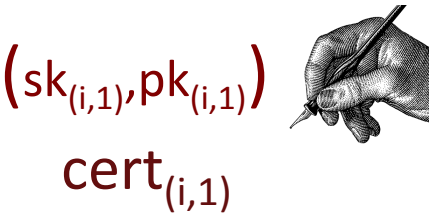
$cert_{(i,k)}$

(gsk,gpk)

- Assume $i_1 > i_2 > \ldots > i_k$
- $Com(\sigma_{(i,j)})$, $Com(pk_{(i,j)})$ $Com(cert_{(i,j)})$,
- $\pi_{(j,1)}$, $\pi_{(j,2)}$, $\pi_{(j,3)}$,

$Sign(gsk,(i_k, pk_{(i,k)}))=cert_{(i,k)}$, $1 \le i_k \le n$.

construction for GS



$(sk_{(i,1)}, pk_{(i,1)})$

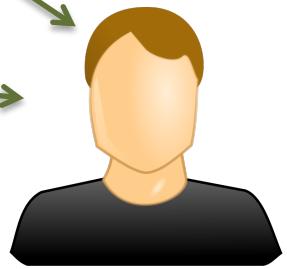
$cert_{(i,1)}$

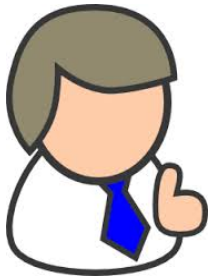
$\Sigma_{(i,1)}=(\sigma_{(i,1)}, pk_{(i,1)}, cert_{(i,1)}, i_1)$

$\Sigma_{(i,2)}$

$(sk_{(i,2)}, pk_{(i,2)})$

$cert_{(i,2)}$





$\Sigma_{(i,k)}$

$(sk_{(i,k)}, pk_{(i,k)})$

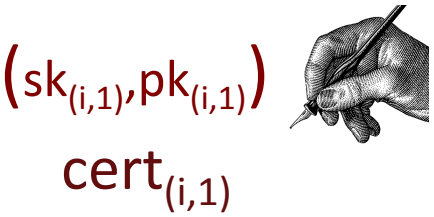
$cert_{(i,k)}$

(gsk,gpk)

- Assume $i_1 > i_2 > \ldots > i_k$
- $Com(\sigma_{(i,j)})$, $Com(pk_{(i,j)})$ $Com(cert_{(i,j)})$,
- $\pi_{(j,1)}$, $\pi_{(j,2)}$, $\pi_{(j,3)}$,
- $Com(i_j)$, $Com(i_{(j+1)}-i_j)$,

$Sign(gsk,(i_k, pk_{(i,k)}))=cert_{(i,k)}$, $1 \le i_k \le n$.

construction for GS



$(sk_{(i,1)}, pk_{(i,1)})$

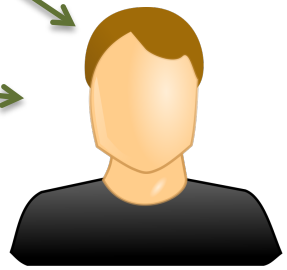
$cert_{(i,1)}$

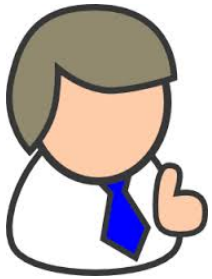
$\Sigma_{(i,1)}=(\sigma_{(i,1)}, pk_{(i,1)}, cert_{(i,1)}, i_1)$

$\Sigma_{(i,2)}$

$(sk_{(i,2)}, pk_{(i,2)})$

$cert_{(i,2)}$





$\Sigma_{(i,k)}$

$(sk_{(i,k)}, pk_{(i,k)})$

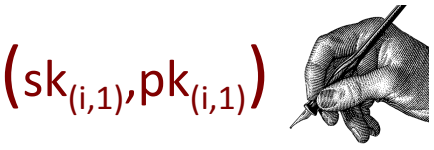
$cert_{(i,k)}$

(gsk,gpk)

- Assume $i_1 > i_2 > \ldots > i_k$
- $Com(\sigma_{(i,j)})$, $Com(pk_{(i,j)})$ $Com(cert_{(i,j)})$,
- $\pi_{(j,1)}$, $\pi_{(j,2)}$, $\pi_{(j,3)}$,
- $Com(i_j)$, $Com(i_{(j+1)}-i_j)$,
- $\pi_{(j,4)}$, $\pi_{(j,5)}$

$Sign(gsk,(i_k, pk_{(i,k)}))=cert_{(i,k)}$, $1 \le i_k \le n$.

construction for GS



$(sk_{(i,1)}, pk_{(i,1)})$

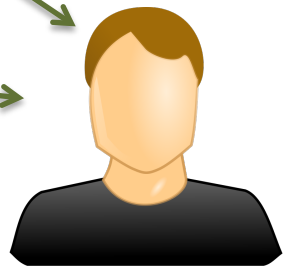
$cert_{(i,1)}$

$\Sigma_{(i,1)}=(\sigma_{(i,1)}, pk_{(i,1)}, cert_{(i,1)}, i_1)$

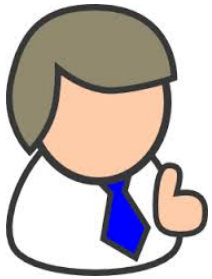
$\Sigma_{(i,2)}$

$(sk_{(i,2)}, pk_{(i,2)})$

$cert_{(i,2)}$



All commitments and proofs



$\Sigma_{(i,k)}$

$(sk_{(i,k)}, pk_{(i,k)})$

$cert_{(i,k)}$

(gsk,gpk)

- Assume $i_1 > i_2 > \ldots > i_k$
- $Com(\sigma_{(i,j)})$, $Com(pk_{(i,j)})$ $Com(cert_{(i,j)})$,
- $\pi_{(j,1)}$, $\pi_{(j,2)}$, $\pi_{(j,3)}$,
- $Com(i_j)$, $Com(i_{(j+1)}-i_j)$,
- $\pi_{(j,4)}$, $\pi_{(j,5)}$

$Sign(gsk,(i_k, pk_{(i,k)}))=cert_{(i,k)}$, $1 \le i_k \le n$.

extension of GS

$(sk_{(i,1)}, pk_{(i,1)})$

$cert_{(i,1)}$

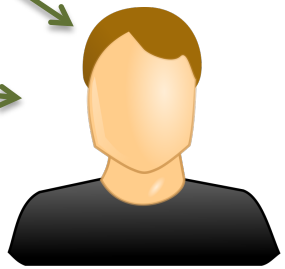
$\Sigma_{(i,1)}=(\sigma_{(i,1)}, pk_{(i,1)}, cert_{(i,1)}, i_1)$

RL : the set of indices of revoked users

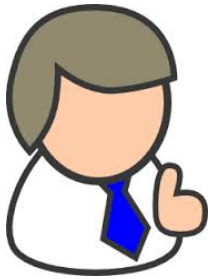
$\Sigma_{(i,2)}$

$(sk_{(i,2)}, pk_{(i,2)})$

$cert_{(i,2)}$



All commitments and proofs



$\Sigma_{(i,k)}$

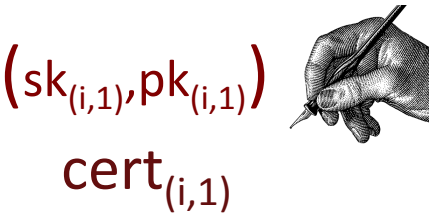
$(sk_{(i,k)}, pk_{(i,k)})$

$cert_{(i,k)}$

- Assume $i_1 > i_2 > \ldots > i_k$
- $Com(\sigma_{(i,j)})$, $Com(pk_{(i,j)})$ $Com(cert_{(i,j)})$,
- $\pi_{(j,1)}$, $\pi_{(j,2)}$, $\pi_{(j,3)}$,
- $Com(i_j)$, $Com(i_{(j+1)}-i_j)$,
- $\pi_{(j,4)}$, $\pi_{(j,5)}$

(gsk,gpk)

extension of GS



$(sk_{(i,1)}, pk_{(i,1)})$

$cert_{(i,1)}$

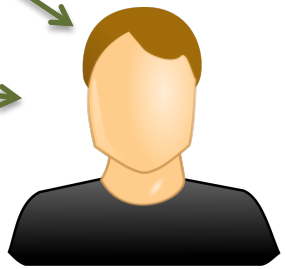
$\Sigma_{(i,1)}=(\sigma_{(i,1)}, pk_{(i,1)}, cert_{(i,1)}, i_1)$

RL : the set of indices of revoked users

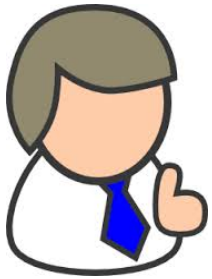
$\Sigma_{(i,2)}$

$(sk_{(i,2)}, pk_{(i,2)})$

$cert_{(i,2)}$



All commitments and proofs



$\Sigma_{(i,k)}$

$(sk_{(i,k)}, pk_{(i,k)})$

$cert_{(i,k)}$

(gsk,gpk)

- Assume $i_1 > i_2 > \ldots > i_k$
- $Com(\sigma_{(i,j)})$, $Com(pk_{(i,j)})$ $Com(cert_{(i,j)})$,
- $\pi_{(j,1)}$, $\pi_{(j,2)}$, $\pi_{(j,3)}$,
- $Com(i_j)$, $Com(i_{(j+1)}-i_j)$,
- $\pi_{(j,4)}$, $\pi_{(j,5)}$

- $\pi_{(j,6)}$: i_j does not belong to RL


THANK
YOU
GRACIAS
BÏYAN
SHUKRIA
DANKSCHEEN
TASHAKKUR ATU
YAQHAMYELAY
SUKSAMA
EKHMET
ARIGATO
SHUKURIA
GRAZIE
MEHRBANI
GOZAIMASHITA
EFCHARISTO
JUSPAXAR
BOLZÏN
MERCI