Blind Digital Signatures, Group Digital Signatures and Revocable Anonymity

Vijay Gabale
Ashutosh Dhekne
Sagar Bijwe
Nishant Burte
MTech 1st Year, CSE Dept.,
IIT Bombay

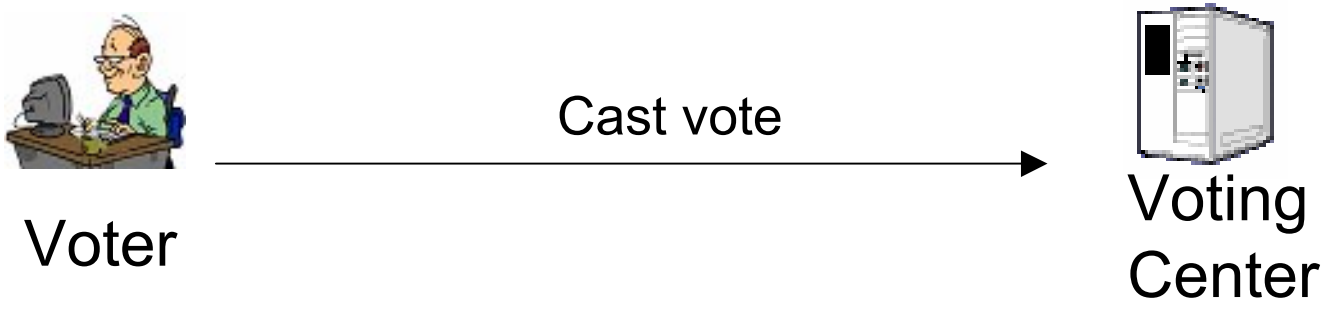
Network Security Project Presentation,
CSE Department, IIT Bombay

Blind Signatures

What are blind digital signatures?

- Signer signs the document without actually looking at its contents

The need for blind signatures



Voting Scheme

Check credentials, curb duplicates

Election Authority

Authentication, Blinded vote

sign on blinded vote

Verification using public key

Unblind vote, retain signature

Voter

Cast vote

Voting Center

Blinding Using RSA

Election Authority

Check credentials,
Sign(B)=B^d

B = H(m).r^e
authentication, B

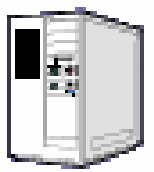
Sign(B) = (H(m).r^e)^d
Sign(B) = H(m)^d.r

(Sign(m))^e = H(m)

Sign(m) =
Sign(B)/r

Voter

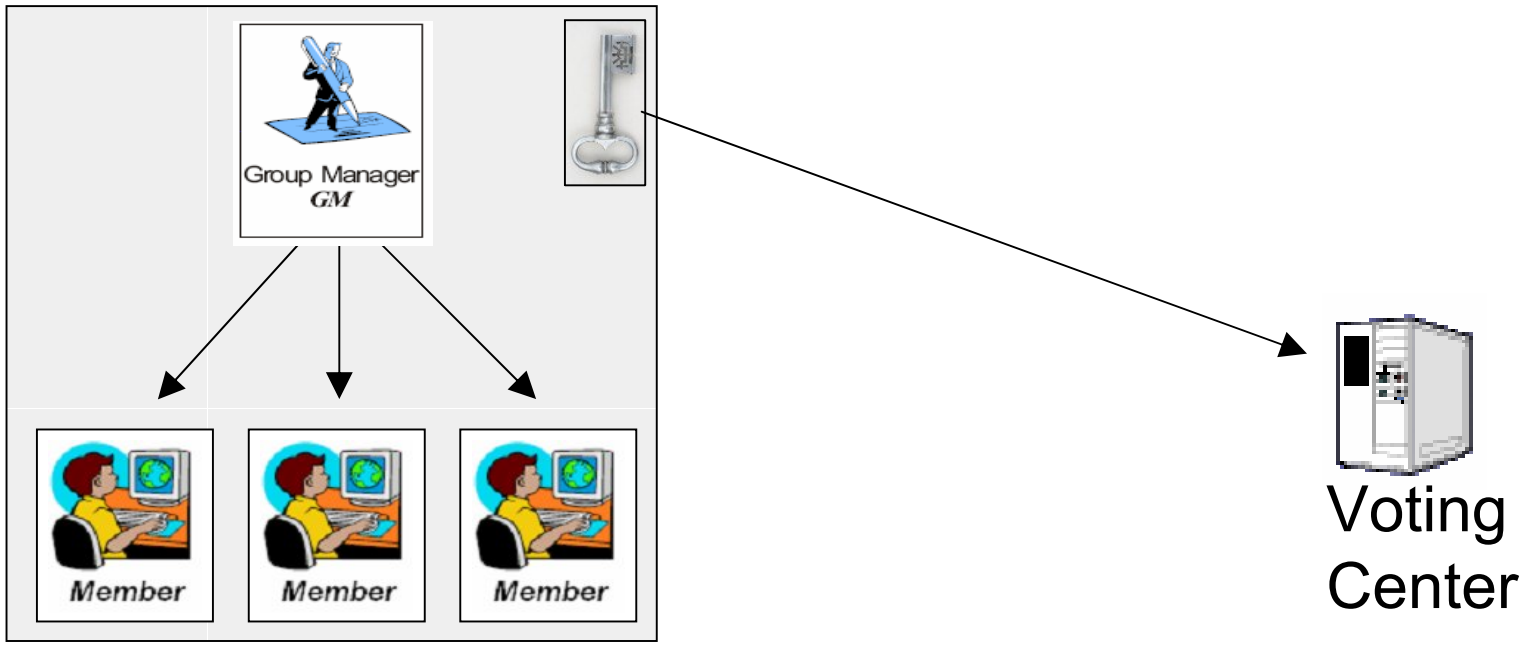
Cast vote <m, Sign(m)>



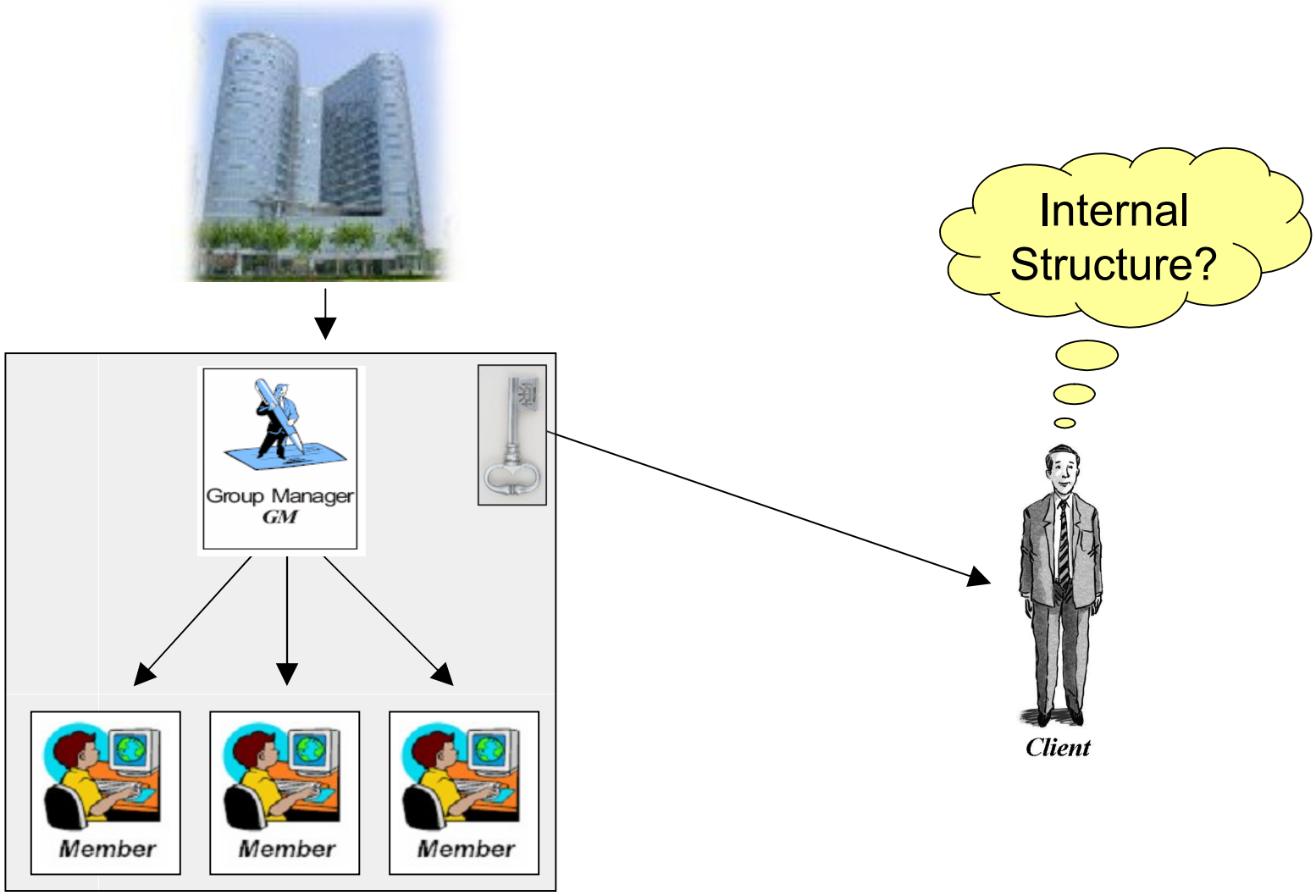
Voting Center

Need for grouping

- Multiple election authorities
- One public key for the voting center to verify



Group Digital Signature



Security Wishlist

- Unforgeability
  - No one other than group members should be able to produce a valid signature
- Conditional Signer Anonymity
  - No one but the Group Manager should be able to determine which member issued the signature
- Undeniable Signer Identity
  - Identity when revoked should be provable to an external law enforcement authority

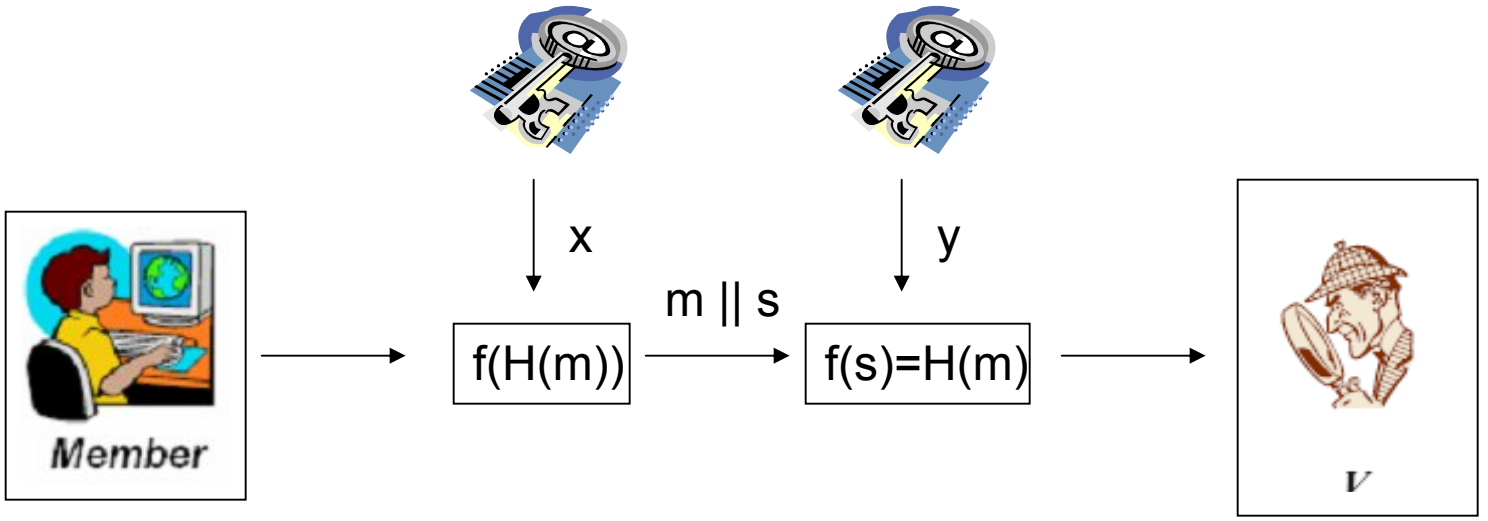
Security Wishlist Continued…

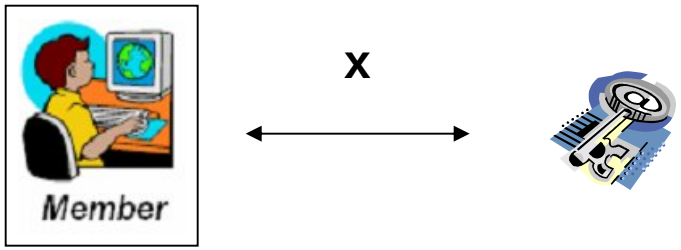
- Unlinkability
  - Determining if two different signatures were issued by the same member is infeasible
- Security against Framing Attacks
  - A group member not be able to produce signatures which give someone else's identity
- Coalition Resistant
  - Members colluding to produce irrevocable keys should be infeasible

Setup Phase

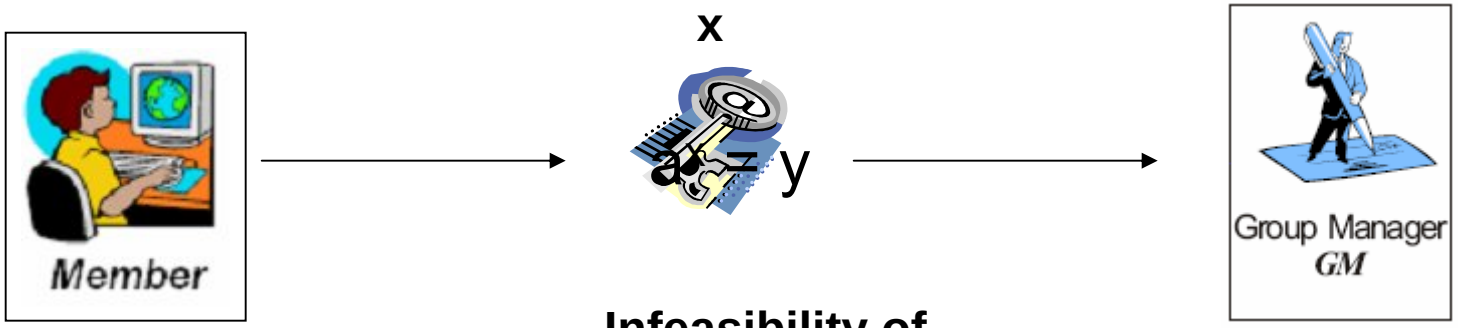
- Two large prime numbers p &q
- RSA public key (n,e), private key (n,d)
- Group G :
  - |G|=n
  - Cyclic subgroup of Z_{p2}^{*} such that n divides p2-1
  - Primitive root : $g^{(p2-1)/pi} \neq 1 \mod p2$
- Group Public key : Y =(n,e,G,g,a,λ, μ)

Digital Signatures





Requirements : Anonymity, Revocation

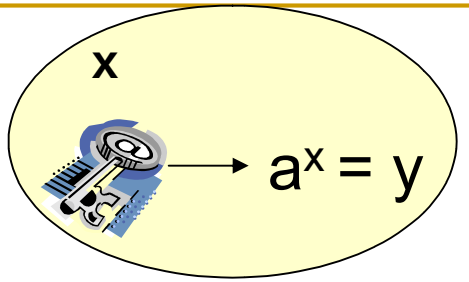


Infeasibility of Calculating Discrete log

Digital Signatures	**A New Scheme**
PR key x	PR key x
PB key y	?? ??? ?

Signature of Knowledge

Signature of Knowledge



Digital Signature
Hash
Sign

m || sign

$r_{i(1 \text{ to } |c|)} \longrightarrow P_i = a^{r_i}$

$C = H (m, y, P_i)$

$S_i = r_i$ if $c [i] = 0$

$S_i = r_i - x$ if $c [i] = 1$

m || (c,s,y)

PB

Verification

$C = H(m, y, P_i) \rightarrow (C, S, y)$

$P_i = a^{r_i}$

Group Public Key

$P_i = a^{S_i}$ if $c[i] = 0$

$P_i = a^{S_i} y$ if $c[i] = 1$

$\longleftrightarrow$

$S_i = r_i$ if $c[i] = 0$

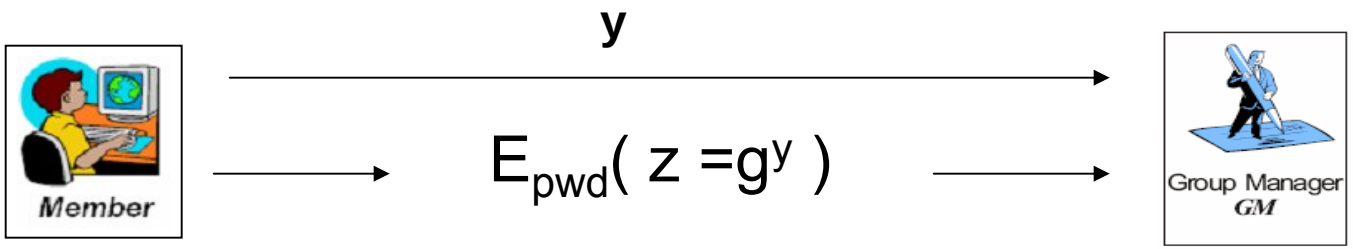
$S_i = r_i - x$ if $c[i] = 1$

x

m || (c,s,y)

Group Public Key

Revocation



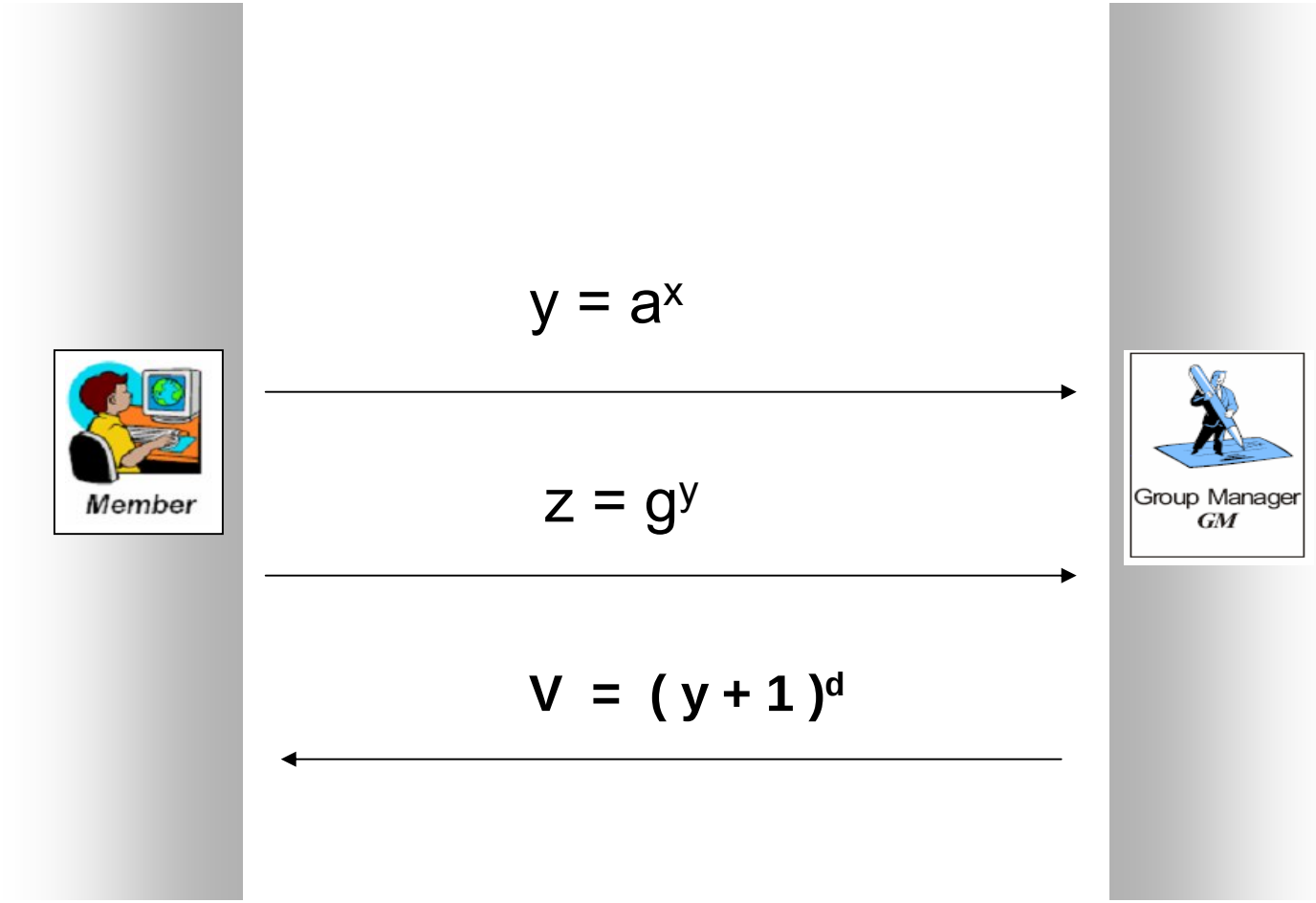
Signature : (g~,z~, C, S)

Is $g^{\sim y'} = z^{\sim}$?

Group Member

y	ID
y_1	ID1

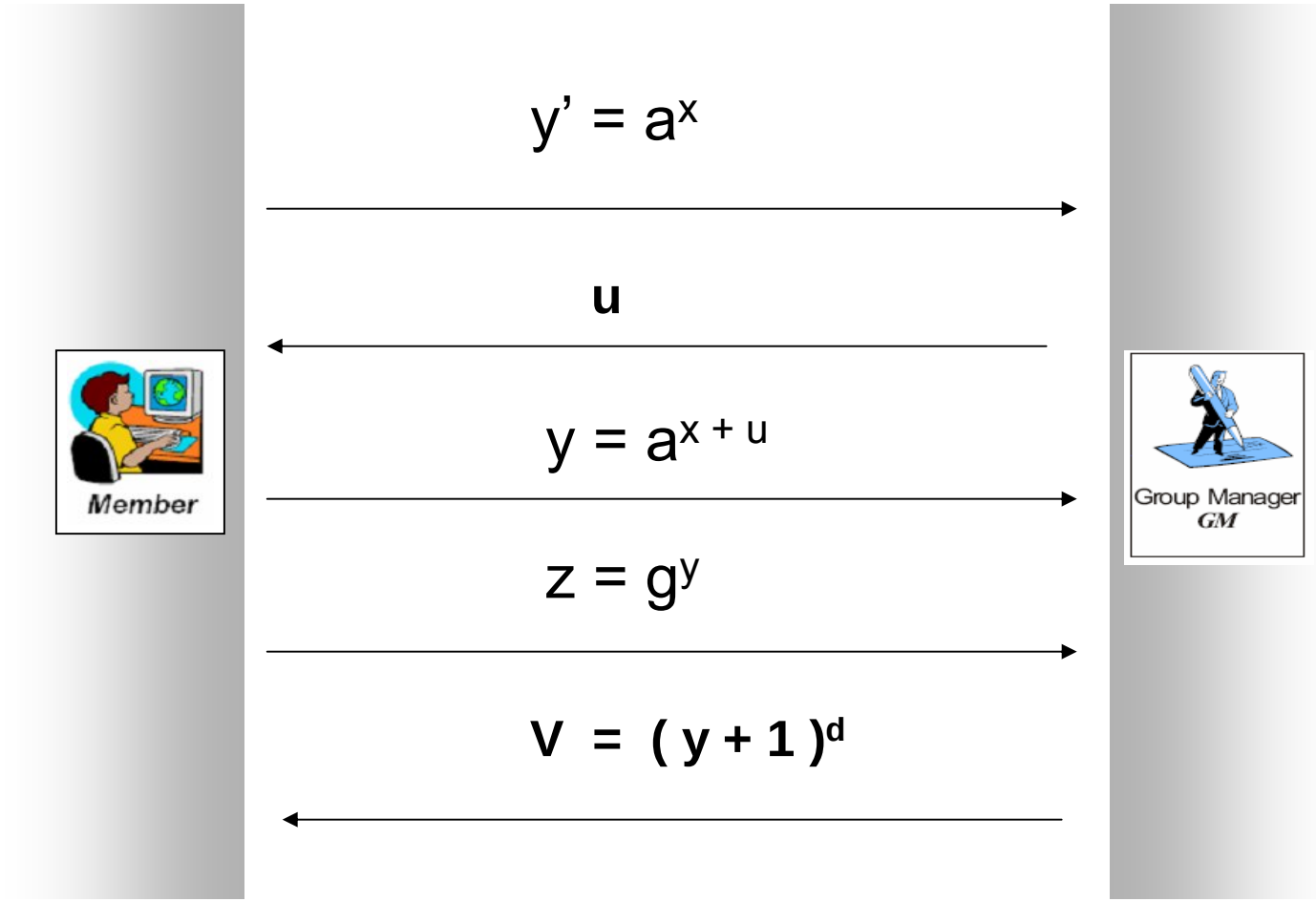
Join Protocol - Revisited



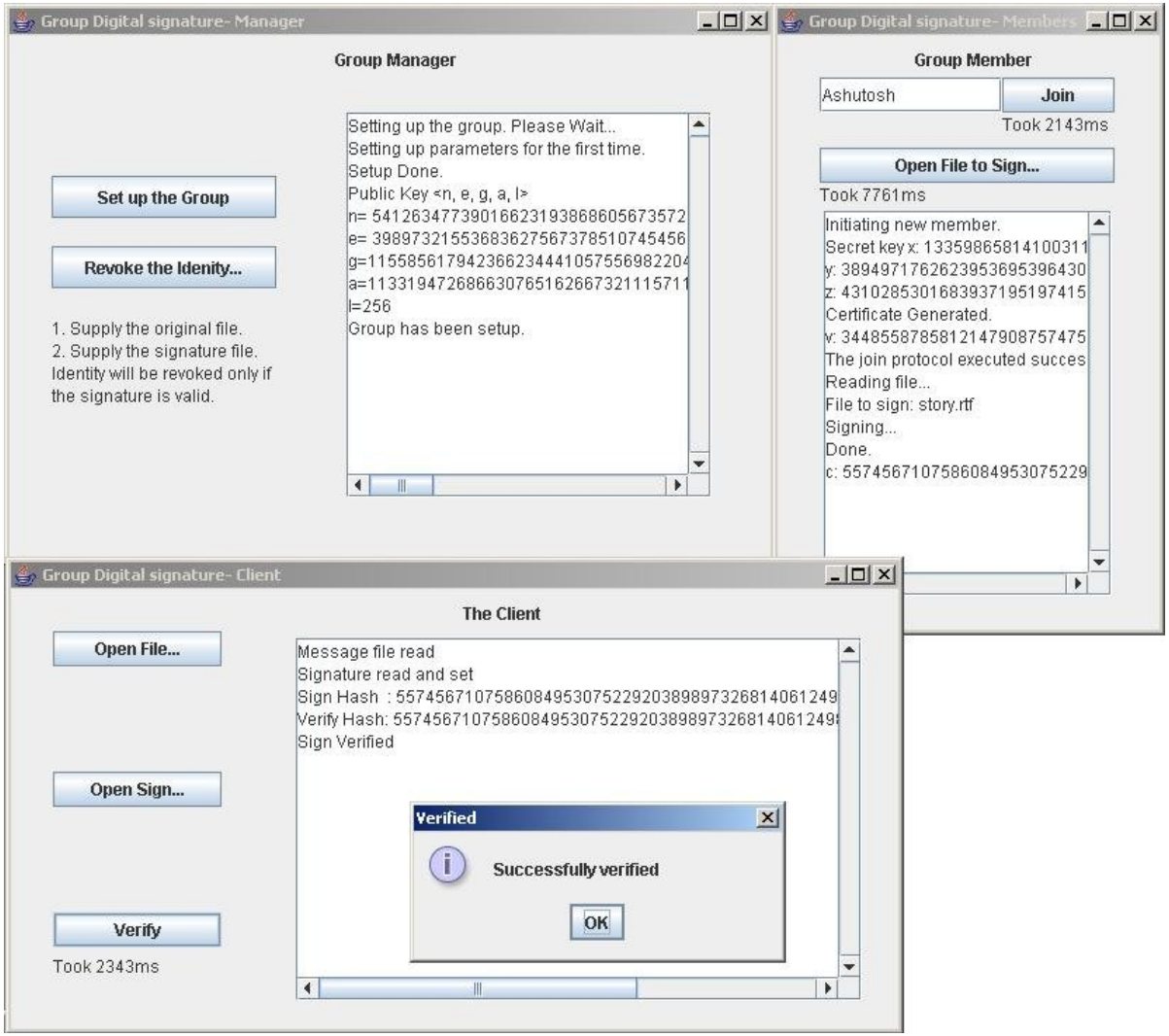
Quasi-Coalition Attack

Private Key	Certificate
x	$A=(a^{x}+1)^{d}$ $=a^{xd}(1+a^{-x})^{d}$
-x	$B=(a^{-x}+1)^{d}$
rx	$C=(a^{rx}+1)^{d}$
-rx	$C\,(A\,B^{-1})^{-r}$

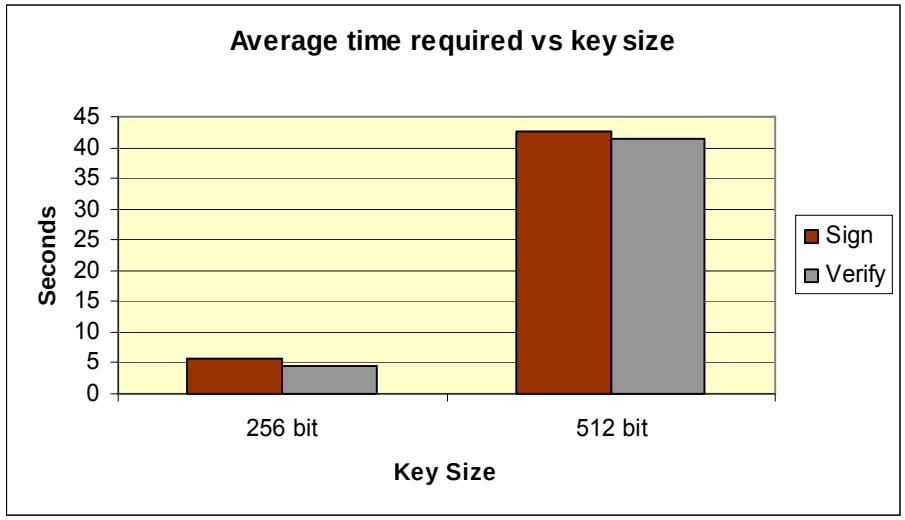
Modified Join Protocol

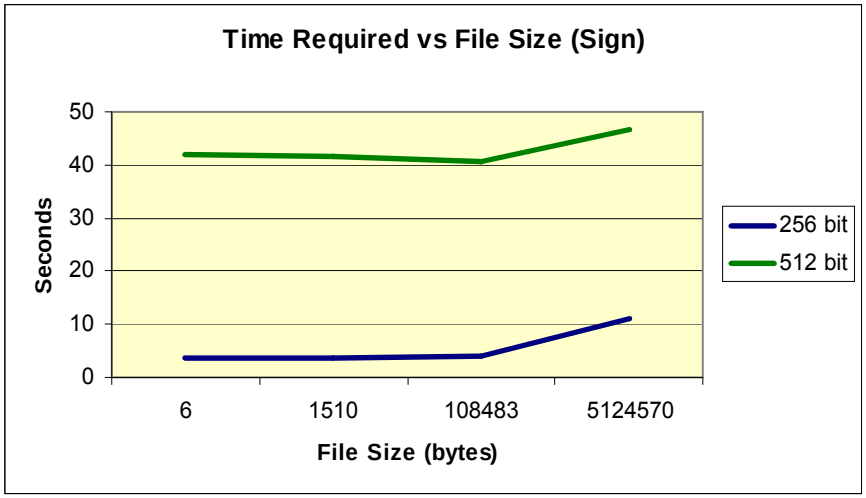


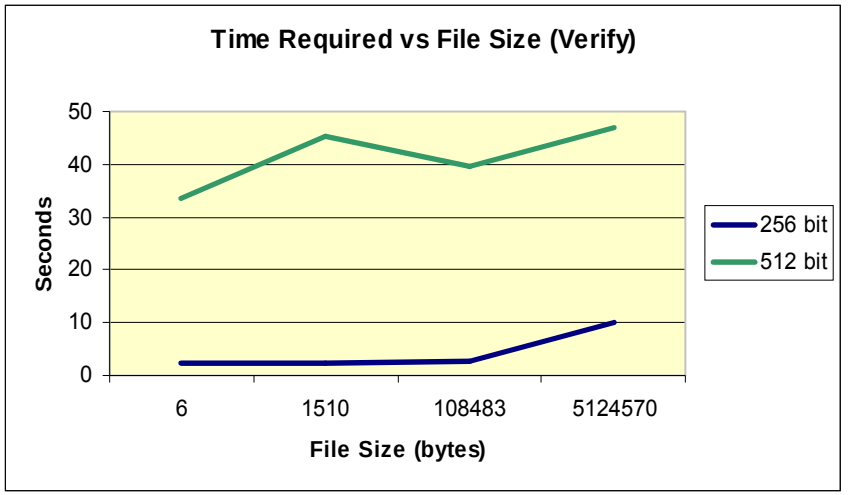
Demo


Group Digital signature- Manager
Group Manager
Set up the Group
Revoke the Idenity...
1. Supply the original file.
2. Supply the signature file.
Identity will be revoked only if
the signature is valid.
Setting up the group. Please Wait...
Setting up parameters for the first time.
Setup Done.
Public Key <n, e, g, a, l>
n= 541263477390166231938686056735 72
e= 398973215536836275673785107454 56
g=115585617942366234441057556982 204
a=113319472686630765162667321115 711
l=256
Group has been setup.
Group Digital signature- Members
Group Member
Ashutosh
Join
Took 2143ms
Open File to Sign...
Took 7761ms
Initiating new member.
Secret key x: 13359865814100311
y: 38949717626239536953964 30
z: 43102853016839371951974 15
Certificate Generated.
v: 34485587858121479087574 75
The join protocol executed succes
Reading file...
File to sign: story.rtf
Signing...
Done.
c: 55745671075860849530752 29
Group Digital signature- Client
The Client
Open File...
Open Sign...
Verify
Took 2343ms
Message file read
Signature read and set
Sign Hash : 55745671075860849530752292038989732681406124 9
Verify Hash: 55745671075860849530752292038989732681406124 9
Sign Verified
Verified
Successfully verified
OK

Timing Analysis







Additional Applications

- Applying for Patents (Blind Signatures)
- Insurance Company (Group Digital Signatures)
- e-Banking (Group Blind Digital Signatures)

Conclusion

- Anonymity & revocation features of Group Signatures are suitable in current scenarios like organization hierarchy
- Added advantage of reducing the burden off PKI & CA employing a single Group Public key for verification

References

- Z.A. Ramzan, Group Blind Digital Signatures: Theory and Applications, Master of Science, MIT, 1999. http://citeseer.ist.psu.edu/ramzan99group.html

- David Chaum, Blind signatures for untraceable payments. In *Proc. CRYPTO 82*, pages 199-203, New York, 1983. Plenum Press.

- Jan Camenisch and Markus Stadler, Efficient group signatures for large groups. In *Proc. CRYPTO 97*, pages 410-424. Springer-Verlag, 1997. Lecture Notes in Computer Science No. 1294.

- S. Kopsell, R. Wendolsky, H. Federrath, Revocable Anonymity. In *Proc. ETRICS 2006, pages* 206-220, LNCS 3995, Springer-Verlag, Heidelberg 2006

Questions

Thank you