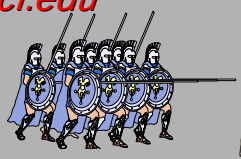
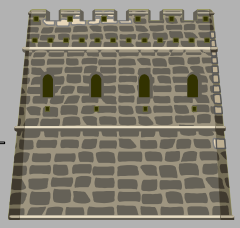


Certificate-based Admission Control in P2P Group Communications

Jeong H. Yi
UC, Irvine
jhyi@ics.uci.edu





1



Outline

Introduction

Admission Control Models

Signature Schemes for admission

Comparison

Future Study

System Demo



2

Group Communication Settings

One-to-Many

- Mailing list
- Cable/sat. TV broadcasting

Few-to-Many

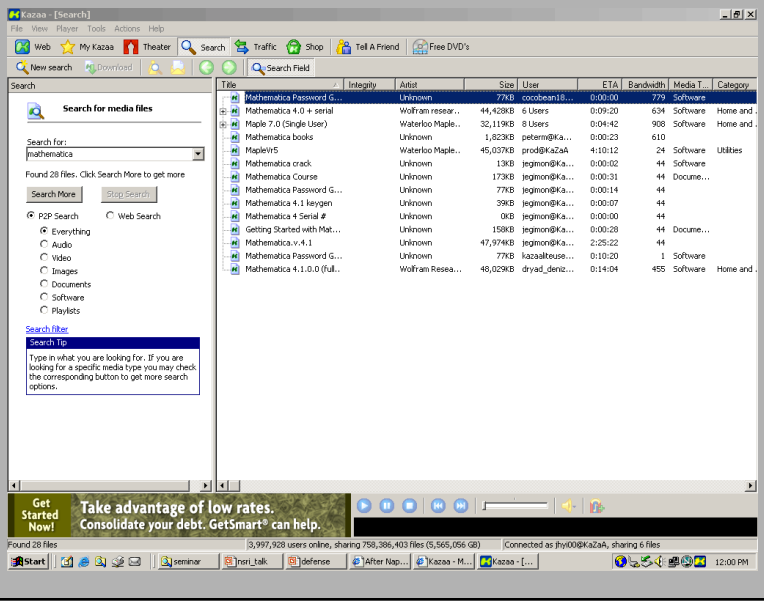
- Remote TV debates
- GPS

Any-to-Any

- Video/Audio conferencing
- Peer-to-peer file sharing
  - Napster, Kazaa, and so on
- Mobile ad-hoc networking

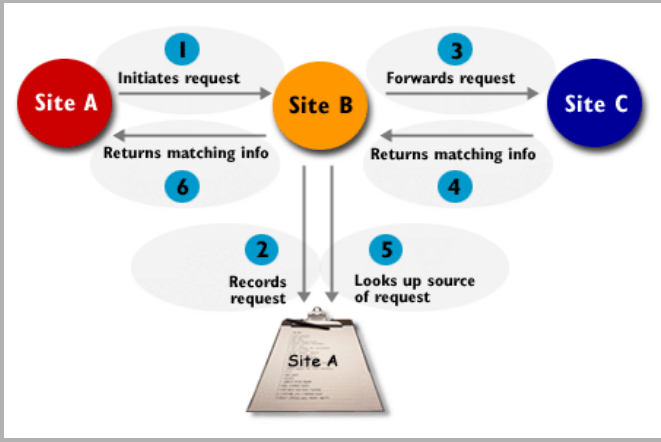
3

P2P File Sharing



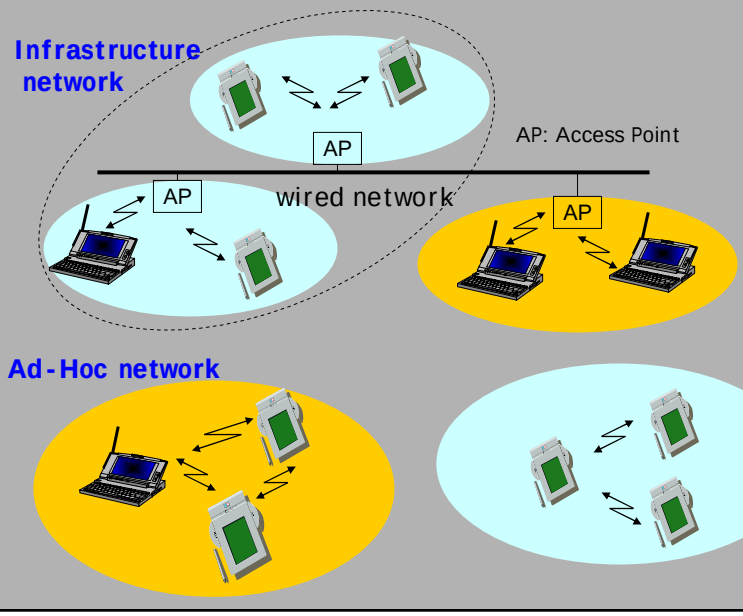
4

Gnutella Structure



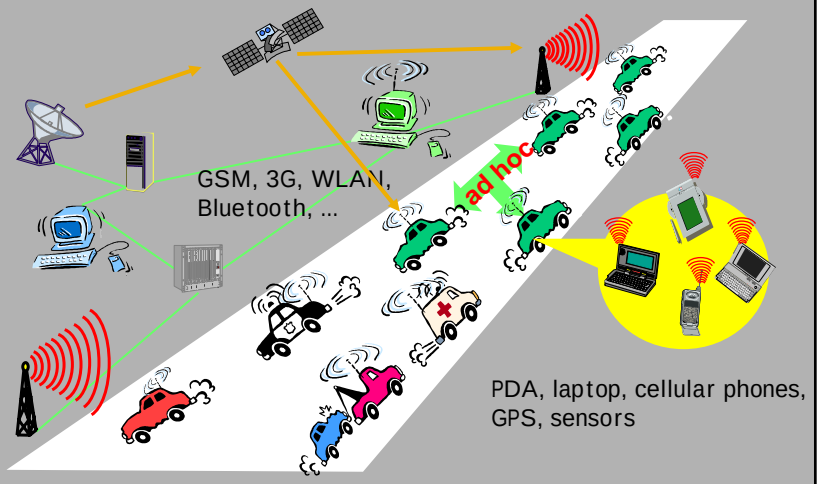
5

Wireless and Mobile Networks



6

Wireless Mobile Ad-Hoc Network



7

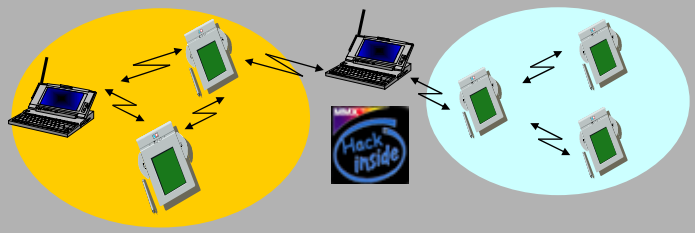
Ad-Hoc Routing

One-hop routing

- **IEEE 802.11: Station mode / Ad-hoc mode**
- **Just set operating mode = "Ad-hoc" mode**

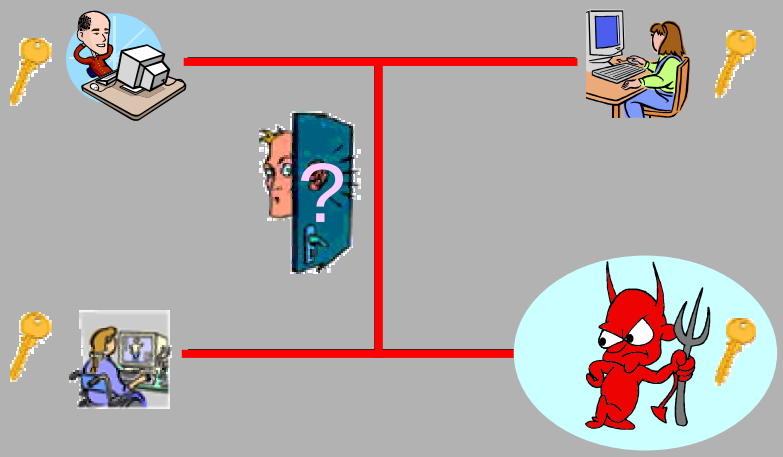
Multi-hop routing

- **Any device can take a role of router using one of following routing algorithms:**
  - AODV, DSR, OLSR, etc.
  - http://opensource.nus.edu.sg/projects/mobileip/links.html



8

Security in Group Communication



However…

9

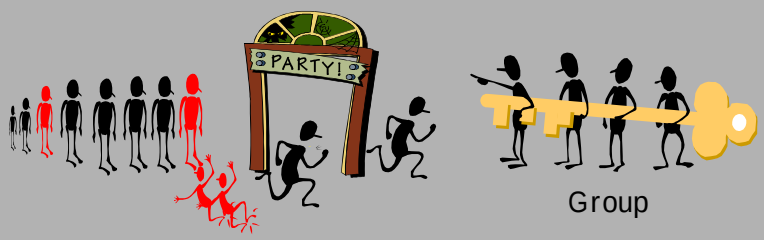
Motivation

Most research in peer group communication deals with key management.

Key management does not care about the eligibility of membership.

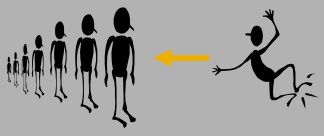
Without admission control, group key management alone is all but useless.

Question - Is access control list (ACL) good enough?

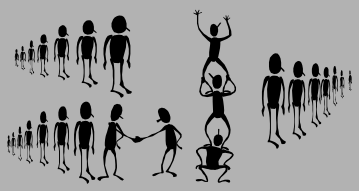


10

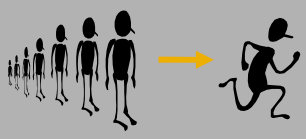
Membership Operations in Group



Member join



Group merge



Member leave



Group partition

11

Outline

Introduction

Admission Control Models

Signature Schemes for admission

Comparison

Future Study

System Demo

12

Terminologies

Group Charter
- issued by CA
- defines the group admission policies
  - Group Name
  - Group Authority Name
  - Admission Policy Type
  - Issuer Name
  - etc.



Group Membership Certificate (GMC)
- issued by GA



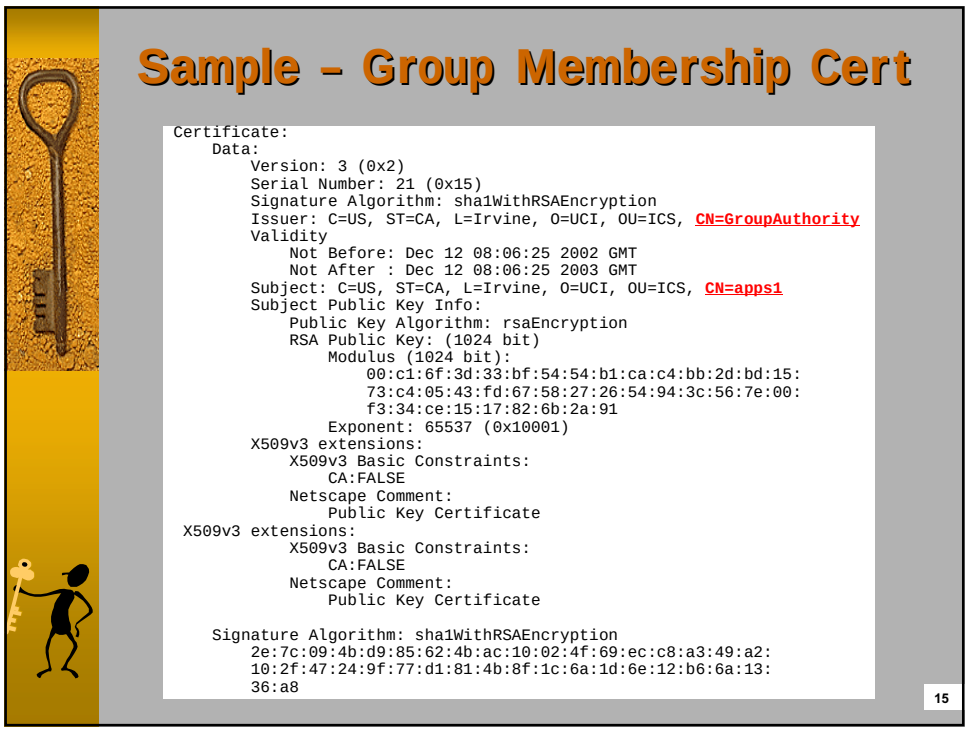
Group Authority (GA)
- the entity that certifies group admission
- who is eligible?
  - Group founder, CA or TTP

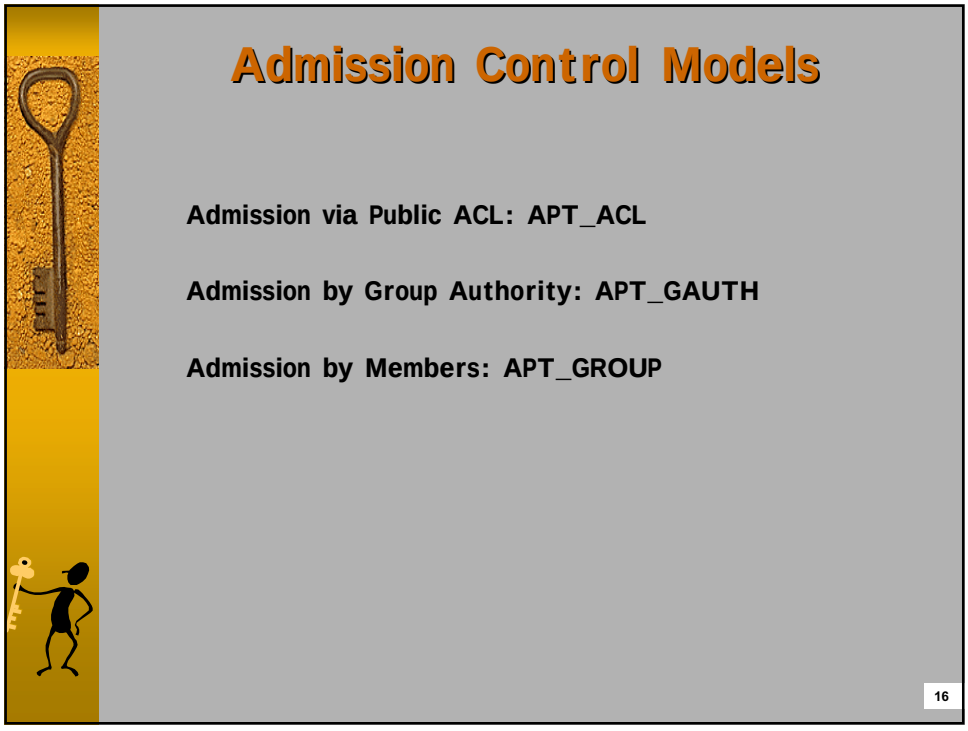
13

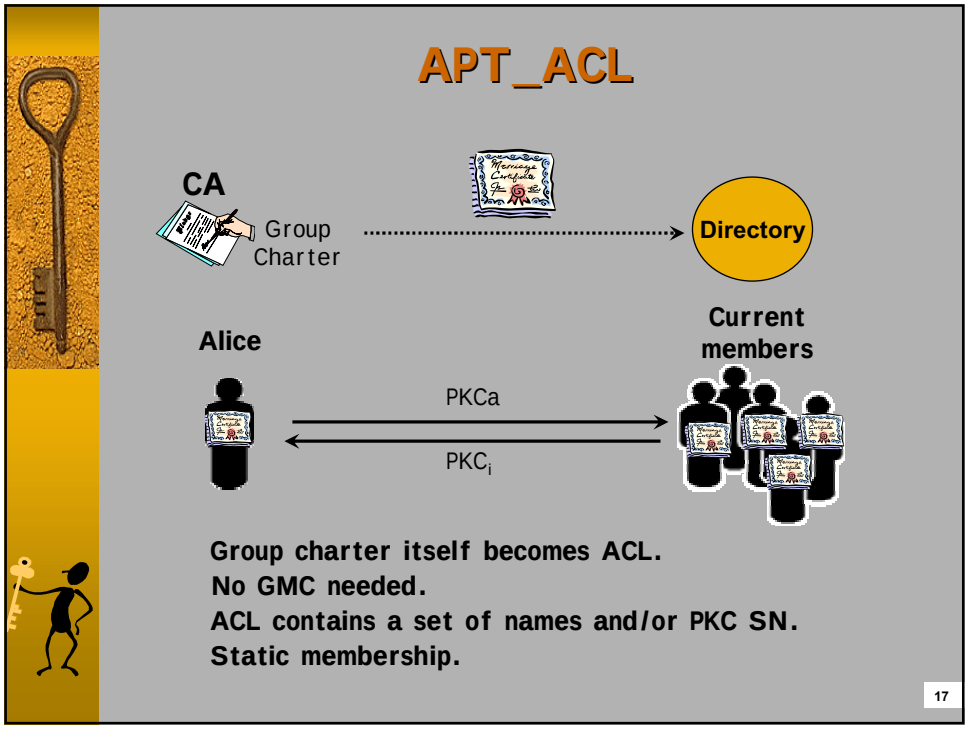
Sample – Group Charter

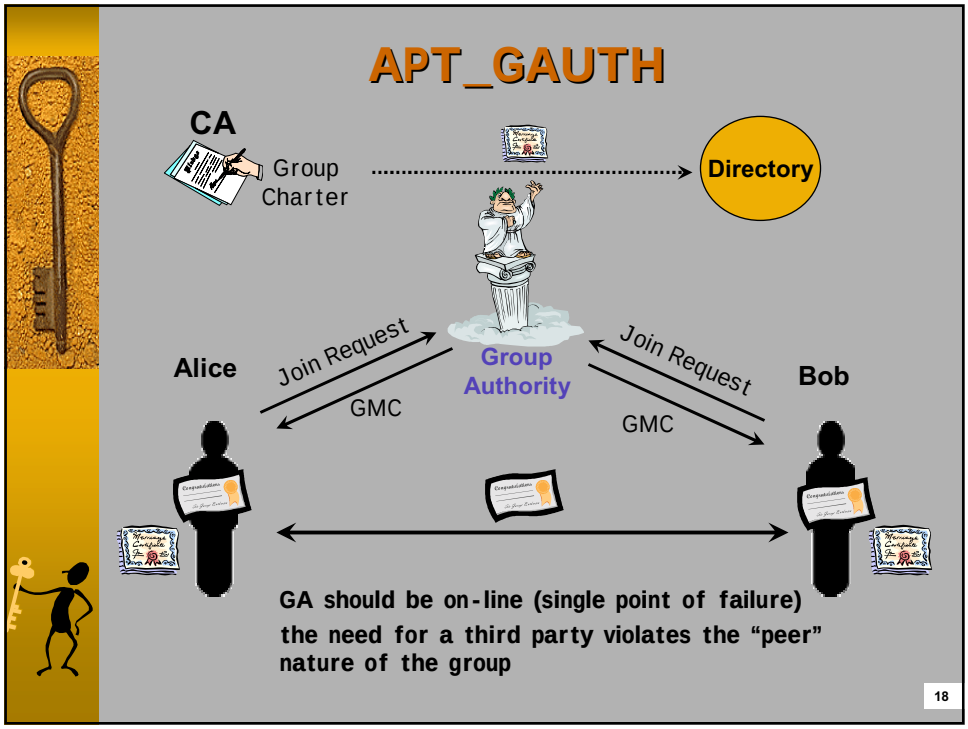
```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 19 (0x13)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=US, ST=CA, L=Irvine, O=UCI, OU=ICS, CN=CA
        Validity
            Not Before: Dec 12 08:05:38 2002 GMT
            Not After : Dec 12 08:05:38 2003 GMT
        Subject: C=US, ST=CA, L=Irvine, O=UCI, OU=ICS, CN=GroupAuthority
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:b0:65:b1:89:7b:f3:95:1b:70:1a:93:cb:33:c1:
                    8d:4c:40:7d:55:05:2c:3a:02:59:49:1e:43:75:64:
                    63:89:43:bf:6c:29:d4:45:ab
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL generated Group Charter
            Group Charter Threshold:
                1
            Group Charter Signature Type:
                4
    Signature Algorithm: sha1WithRSAEncryption
        15:d3:aa:48:8f:f1:93:83:b4:1e:57:a3:ab:0b:b7:f5:b3:da:
        28:46:3f:f4:22:22:88:89:68:dd:62:4c:24:f4:cd:11:73:dc:
        6c:de
```

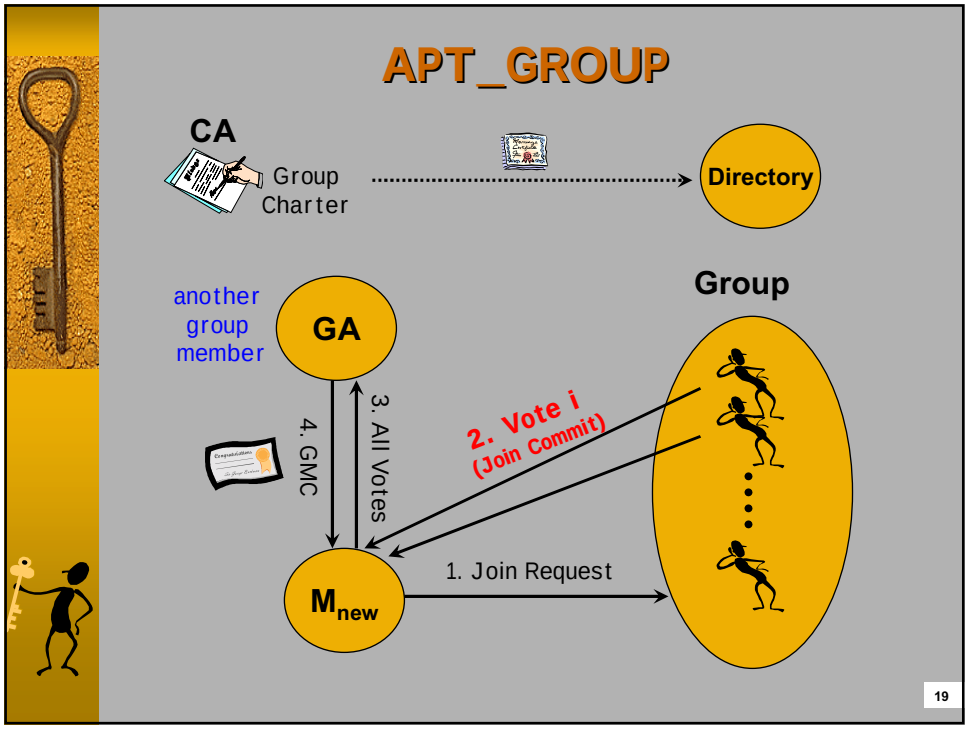
14

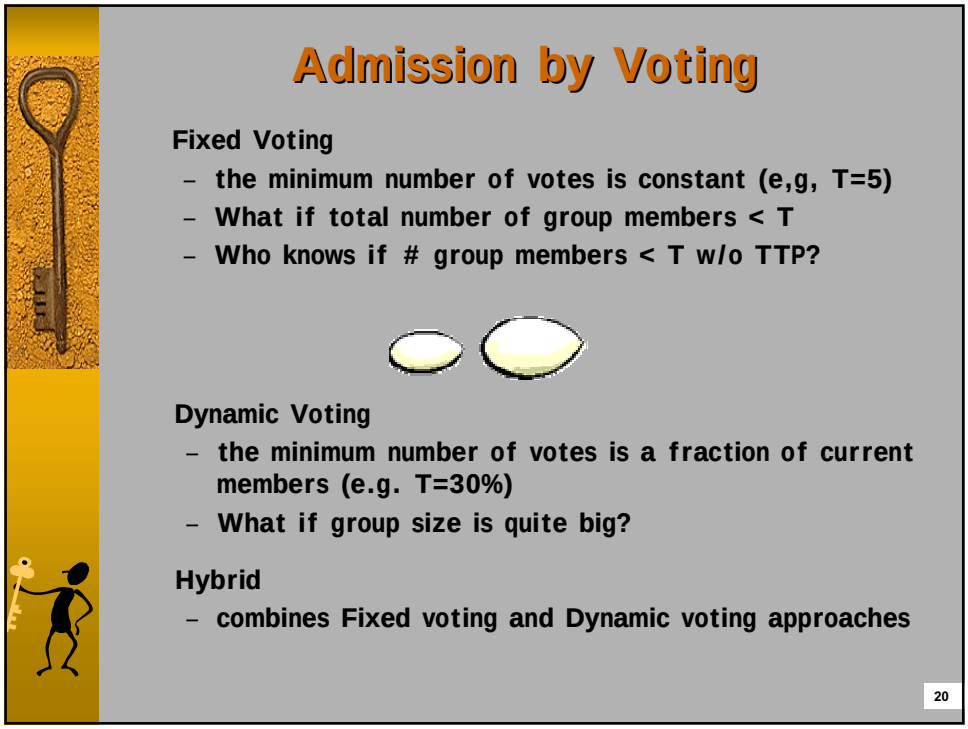

Sample – Group Membership Cert
Certificate:
Data:
Version: 3 (0x2)
Serial Number: 21 (0x15)
Signature Algorithm: sha1WithRSAEncryption
Issuer: C=US, ST=CA, L=Irvine, O=UCI, OU=ICS, CN=GroupAuthority
Validity
Not Before: Dec 12 08:06:25 2002 GMT
Not After : Dec 12 08:06:25 2003 GMT
Subject: C=US, ST=CA, L=Irvine, O=UCI, OU=ICS, CN=apps1
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public Key: (1024 bit)
Modulus (1024 bit):
00:c1:6f:3d:33:bf:54:54:b1:ca:c4:bb:2d:bd:15:
73:c4:05:43:fd:67:58:27:26:54:94:3c:56:7e:00:
f3:34:ce:15:17:82:6b:2a:91
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Basic Constraints:
CA:FALSE
Netscape Comment:
Public Key Certificate
X509v3 extensions:
X509v3 Basic Constraints:
CA:FALSE
Netscape Comment:
Public Key Certificate
Signature Algorithm: sha1WithRSAEncryption
2e:7c:09:4b:d9:85:62:4b:ac:10:02:4f:69:ec:c8:a3:49:a2:
10:2f:47:24:9f:77:d1:81:4b:8f:1c:6a:1d:6e:12:b6:6a:13:
36:a8
15

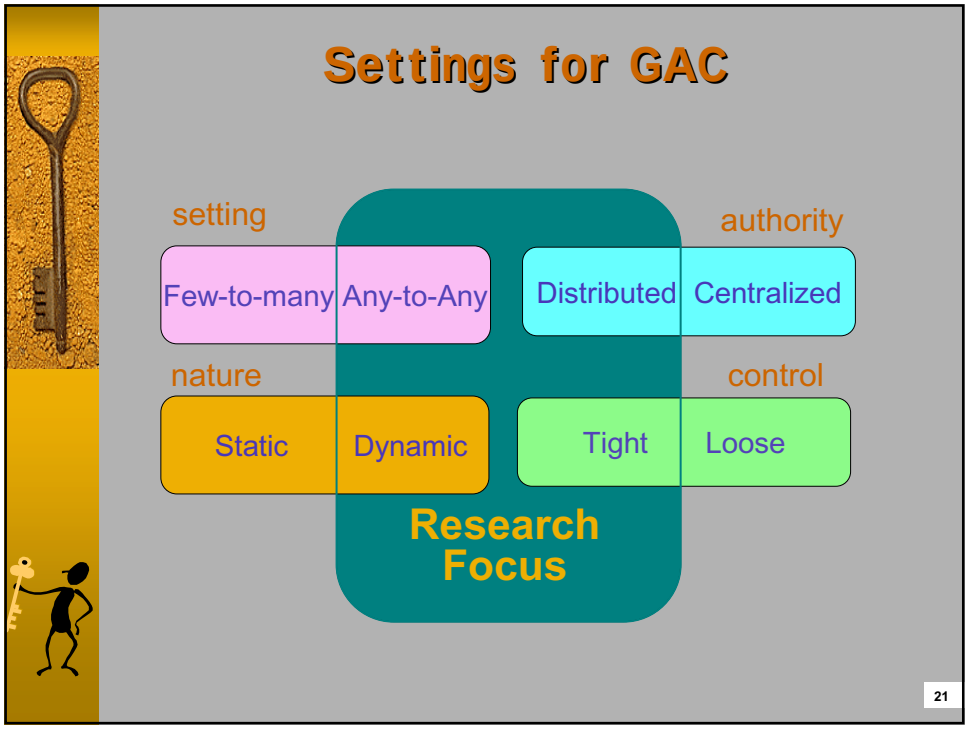

Admission Control Models
Admission via Public ACL: APT_ACL
Admission by Group Authority: APT_GAUTH
Admission by Members: APT_GROUP
16

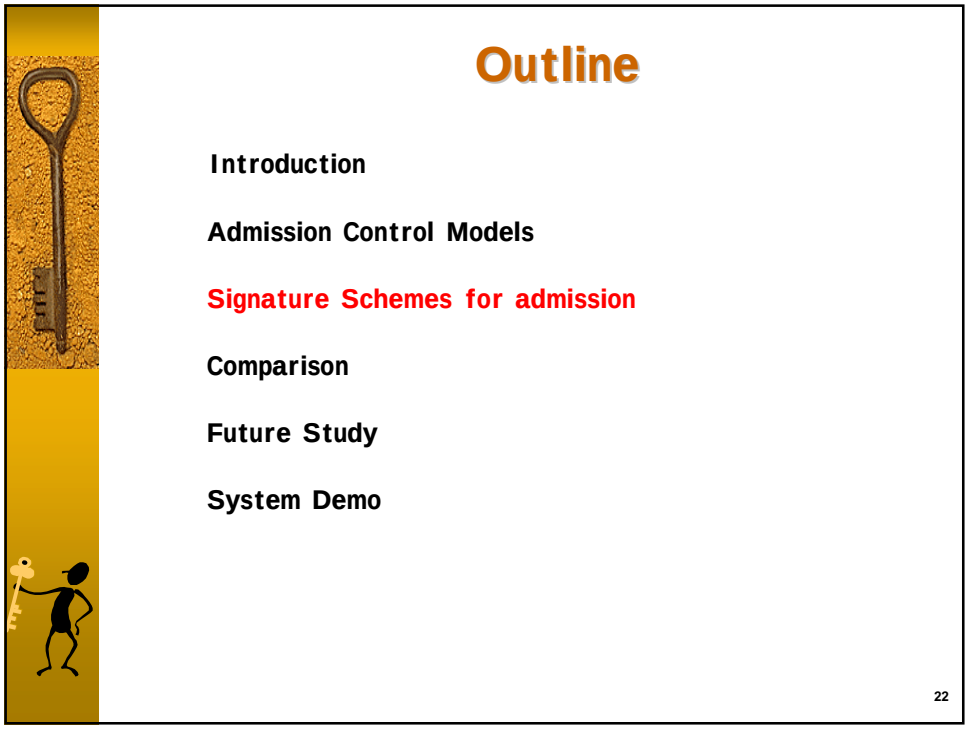

APT_ACL
CA
Group Charter
Directory
Alice
Current members
PKCa
PKC$_i$
Group charter itself becomes ACL.
No GMC needed.
ACL contains a set of names and/or PKC SN.
Static membership.
17

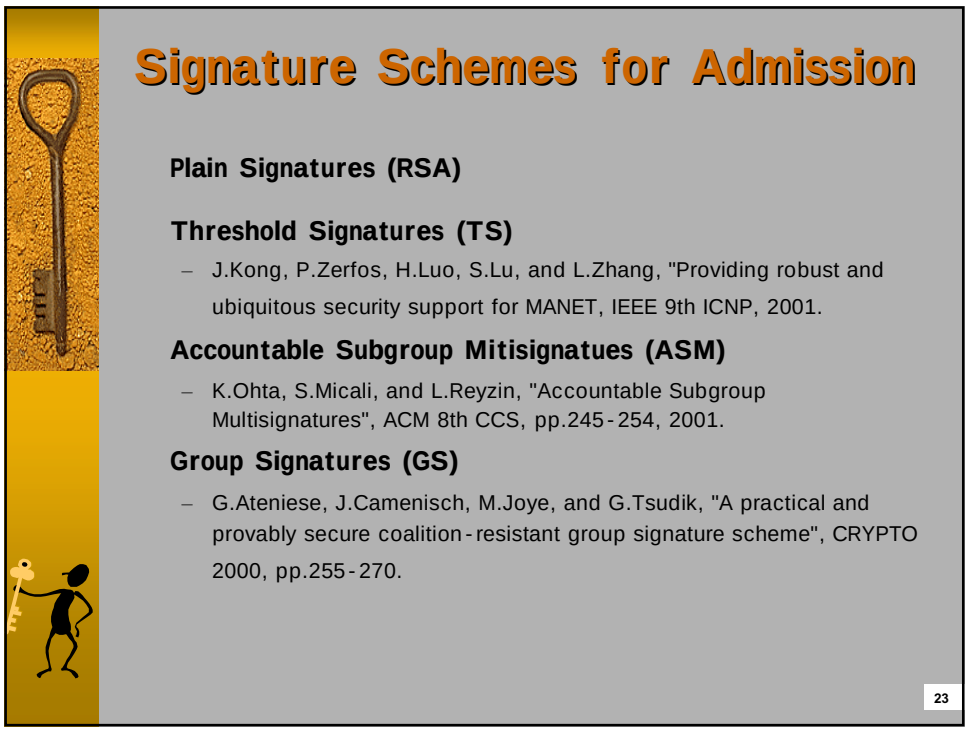

APT_GAUTH
CA
Group Charter
Directory
Alice
Join Request
GMC
Group Authority
Join Request
GMC
Bob
GA should be on-line (single point of failure)
the need for a third party violates the "peer" nature of the group
18

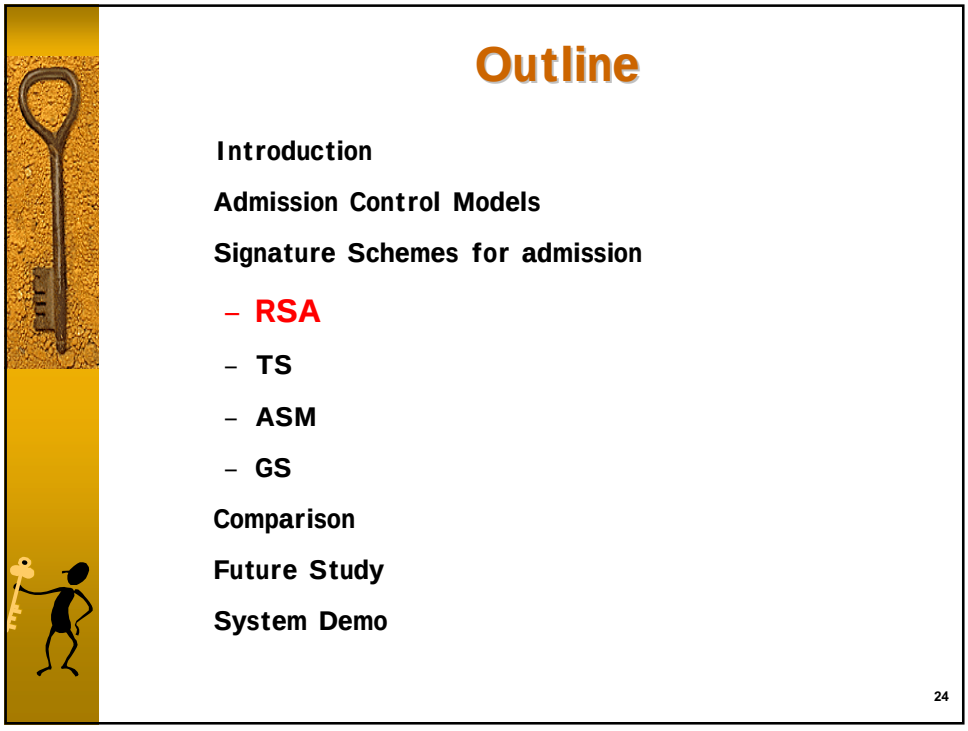

APT_GROUP
CA
Group
Charter
Directory
another
group
member
GA
Group
4. GMC
3. All Votes
2. Vote i
(Join Commit)
1. Join Request
M_{new}
19


Admission by Voting
Fixed Voting
– the minimum number of votes is constant (e,g, T=5)
– What if total number of group members < T
– Who knows if # group members < T w/o TTP?
Dynamic Voting
– the minimum number of votes is a fraction of current members (e.g. T=30%)
– What if group size is quite big?
Hybrid
– combines Fixed voting and Dynamic voting approaches
20


Settings for GAC
setting
Few-to-many
Any-to-Any
authority
Distributed
Centralized
nature
Static
Dynamic
control
Tight
Loose
Research Focus
21


Outline
Introduction
Admission Control Models
Signature Schemes for admission
Comparison
Future Study
System Demo
22


Signature Schemes for Admission
Plain Signatures (RSA)
Threshold Signatures (TS)
– J.Kong, P.Zerfos, H.Luo, S.Lu, and L.Zhang, "Providing robust and ubiquitous security support for MANET, IEEE 9th ICNP, 2001.
Accountable Subgroup Mitisignatues (ASM)
– K.Ohta, S.Micali, and L.Reyzin, "Accountable Subgroup Multisignatures", ACM 8th CCS, pp.245-254, 2001.
Group Signatures (GS)
– G.Ateniese, J.Camenisch, M.Joye, and G.Tsudik, "A practical and provably secure coalition-resistant group signature scheme", CRYPTO 2000, pp.255-270.
23


Outline
Introduction
Admission Control Models
Signature Schemes for admission
– RSA
– TS
– ASM
– GS
Comparison
Future Study
System Demo
24

Group Admission – RSA (1)

Setup process

- Generate RSA key pairs
  - generate primes p, q
  - d: secret, (e, n): public , where n=pq

Signing process

- $S = M^d \bmod n$

exponentiation: 1
time: 8 msec

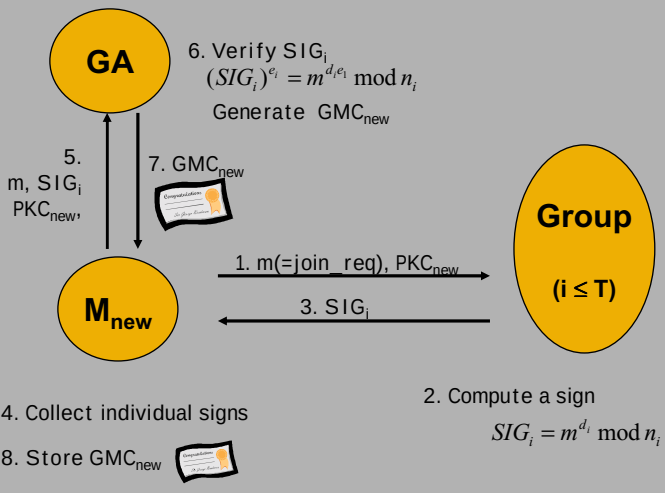
Verifying process

- $S^e = M^{de} \bmod n$, where $de = 1 \bmod \Phi(n)$

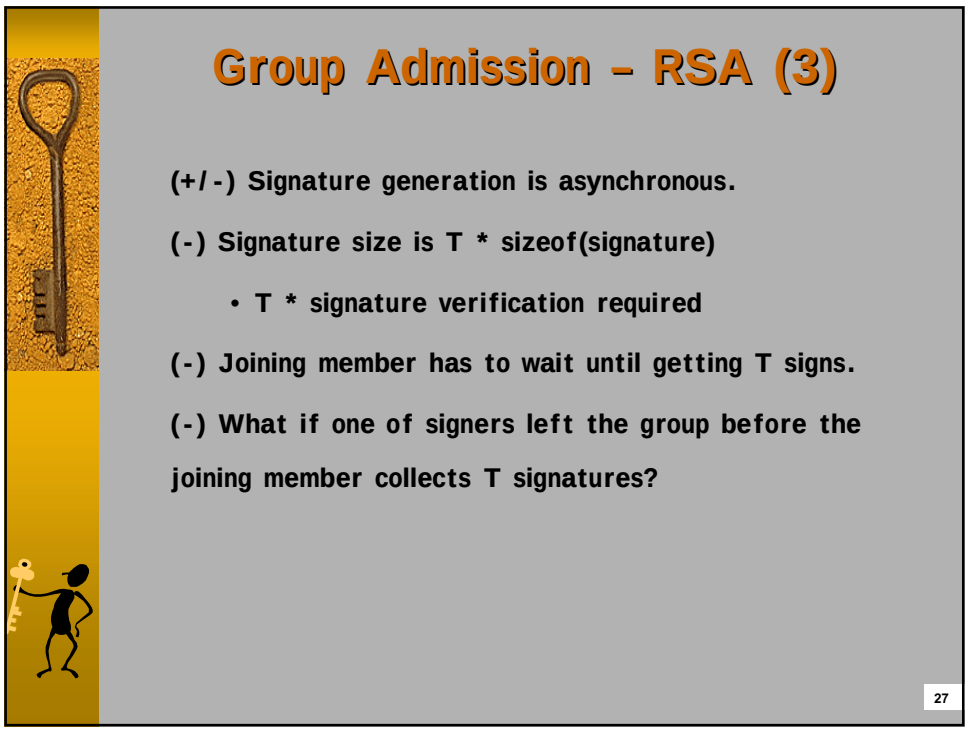
exponentiation: 1
time: 1 msec

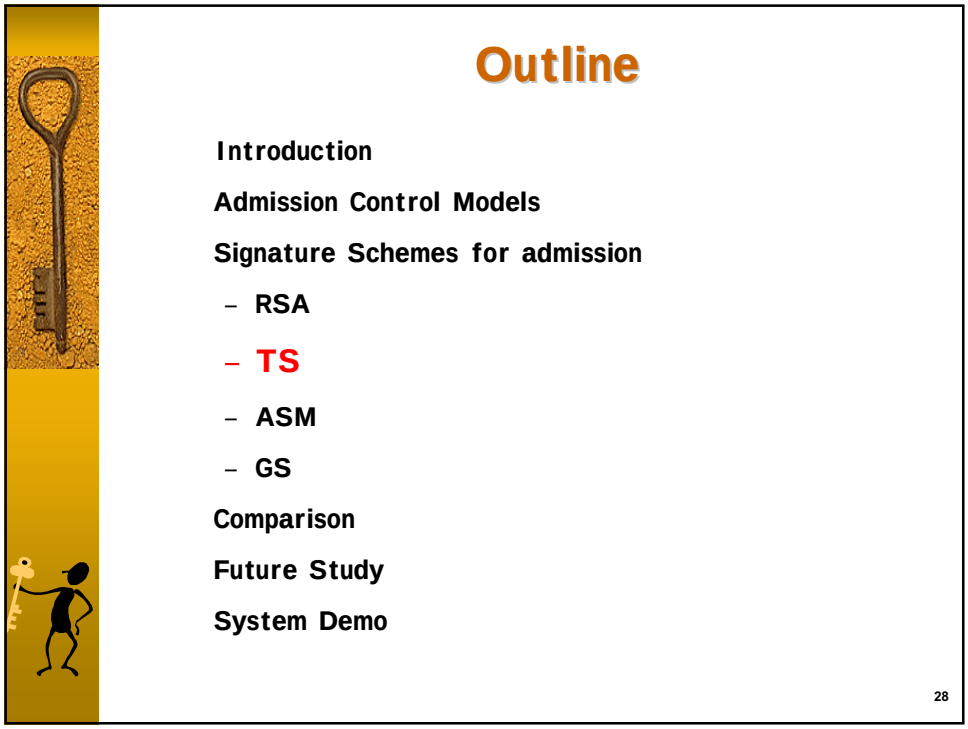
25

Group Admission – RSA (2)

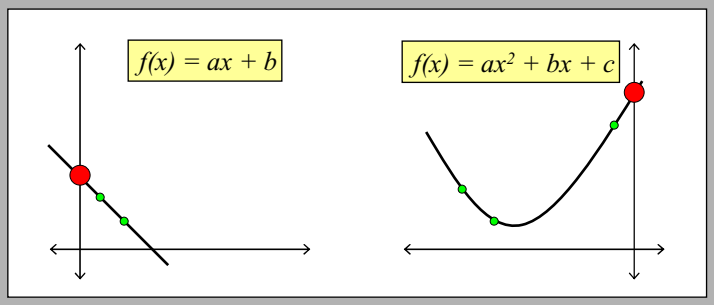


26


Group Admission – RSA (3)
(+/-) Signature generation is asynchronous.
(-) Signature size is T * sizeof(signature)
• T * signature verification required
(-) Joining member has to wait until getting T signs.
(-) What if one of signers left the group before the joining member collects T signatures?
27


Outline
Introduction
Admission Control Models
Signature Schemes for admission
– RSA
– TS
– ASM
– GS
Comparison
Future Study
System Demo
28

Threshold Secrets



Given *k* points in the plane, there is only one polynomial of degree *k-1* that intersects all *k* points

K-1 points do not suffice for interpolation

Threshold secrets: Given their (x_i, y_i) coordinates, *k* nodes can interpolate *f(0)*--the secret key

29

Dealing Secret Shares

Dealer obtains secret key *d*

Randomly selects polynomial *f(x)* of degree *k-1*

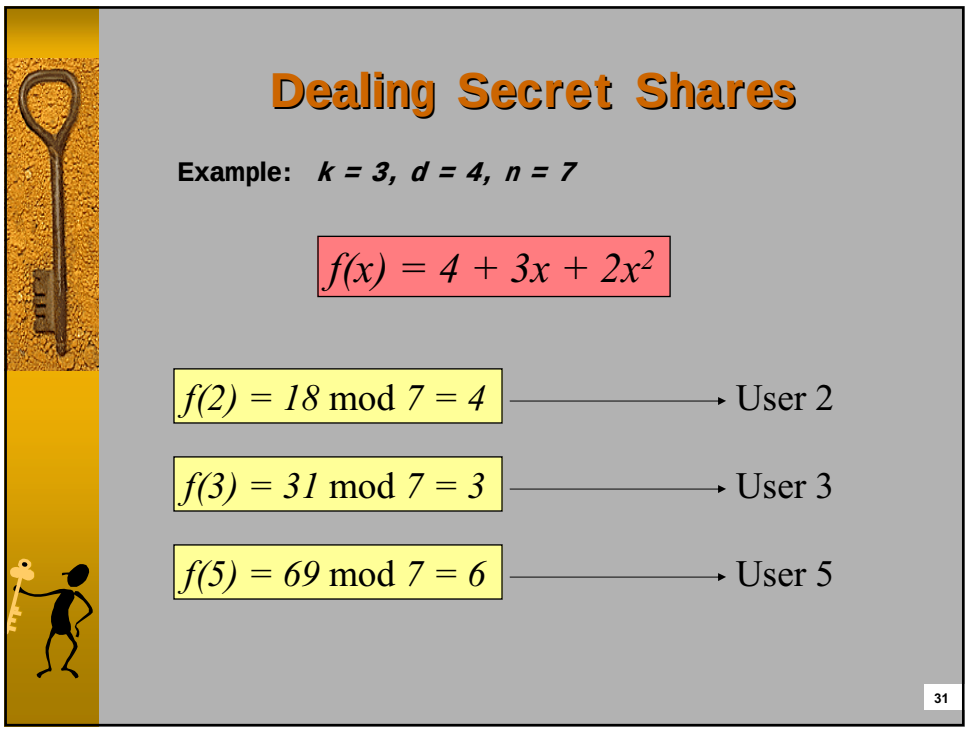
$$f(x) = d + a_1x + a_2x^2 + \ldots + a_{k-1}x^{k-1}$$

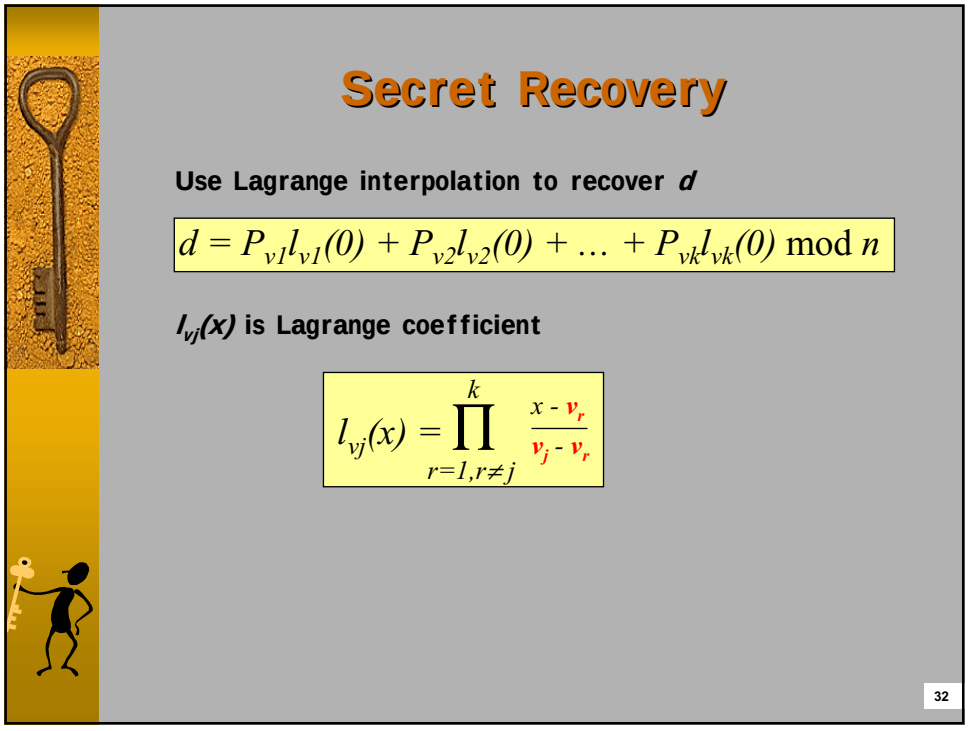
Note: *f(0) = d*

Dealer distributes secret shares to users

$$P_{vi} = f(v_i) \bmod n$$

30


Dealing Secret Shares
Example: k = 3, d = 4, n = 7
f(x) = 4 + 3x + 2x^2
f(2) = 18 mod 7 = 4
User 2
f(3) = 31 mod 7 = 3
User 3
f(5) = 69 mod 7 = 6
User 5
31


Secret Recovery
Use Lagrange interpolation to recover d
d = P_v1 l_v1(0) + P_v2 l_v2(0) + … + P_vk l_vk(0) mod n
l_vj(x) is Lagrange coefficient
l_vj(x) = ∏ (x - v_r)/(v_j - v_r), r=1, r≠j, k
32

Secret Recovery

From previous example:

$P_{v2} = 4$ $\quad l_{v2}(0) = \frac{-3}{2-3} \cdot \frac{-5}{2-5} = 5$

$P_{v3} = 3$ $\quad l_{v3}(0) = \frac{-2}{3-2} \cdot \frac{-5}{3-5} = -5$

$P_{v5} = 6$ $\quad l_{v5}(0) = \frac{-2}{5-2} \cdot \frac{-3}{5-3} = 1$

$$P_{v2}l_{v2}(0) + P_{v3}l_{v3}(0) + P_{v5}l_{v5}(0) \bmod 7 =$$
$$4 \cdot 5 \quad + 3 \cdot -5 \quad + 6 \cdot 1 \quad \bmod 7 = 4$$

$$f(x) = 4 + 3x + 2x^2$$

33

Group Admission – TS (1)

Setup process

- Generate RSA key pairs
  - d: group secret, (e, n): group public
- Trusted dealer(e.g., group founder) randomly selects polynomial $f(x)$ of degree $k-1$
  - $f(x) = d + a_1x + a_2x^2 + \ldots + a_{k-1}x^{k-1}$
  - Note: $f(0) = d$

GPC

Signing process

exponentiation: 1
time: 40 msec

- $M^{SK(i)} \bmod n$

where, $SK(i) = SS(i)l_i(0) \bmod n$, $l_i(x) = \prod_{j=1, j\neq i}^{k} \frac{x-j}{i-j}$

Constructing actual sign

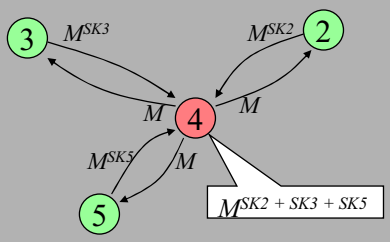
exponentiation: 1
time: 22 msec

$$M^d = \prod^{k} M^{SK(i)} \pmod{n}$$

34

Group Admission – TS (2)

Constructing actual sign (continued)



$$SK_i = P_{vi} l_{vi}(0) \bmod n$$

$$SK_2 + SK_3 + SK_5 \bmod n \equiv d$$

$$SK_2 + SK_3 + SK_5 = tn + d$$

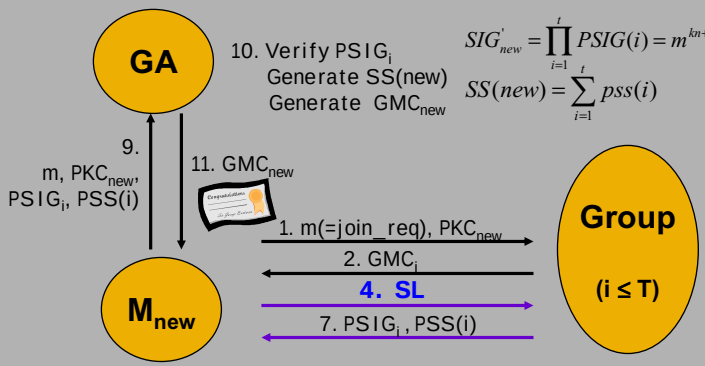
$$M^{SK2+SK3+SK5} = M^{tn+d} = M^{tn} M^{d}$$

```
for (i=0; i <= k; i++)  {
      Y = M^(tn+d) * M^(-ni)  mod n;
      if (Y^e = M  mod n)
            break;  }
return Y  (= M^d  mod n)
```

exponentiation: 1
time: 22 msec

35

Group Admission – TS (3)



3. Collect signers' list (SL)

8. Collect partial signs and partial shares

12. Store GMC$_{new}$

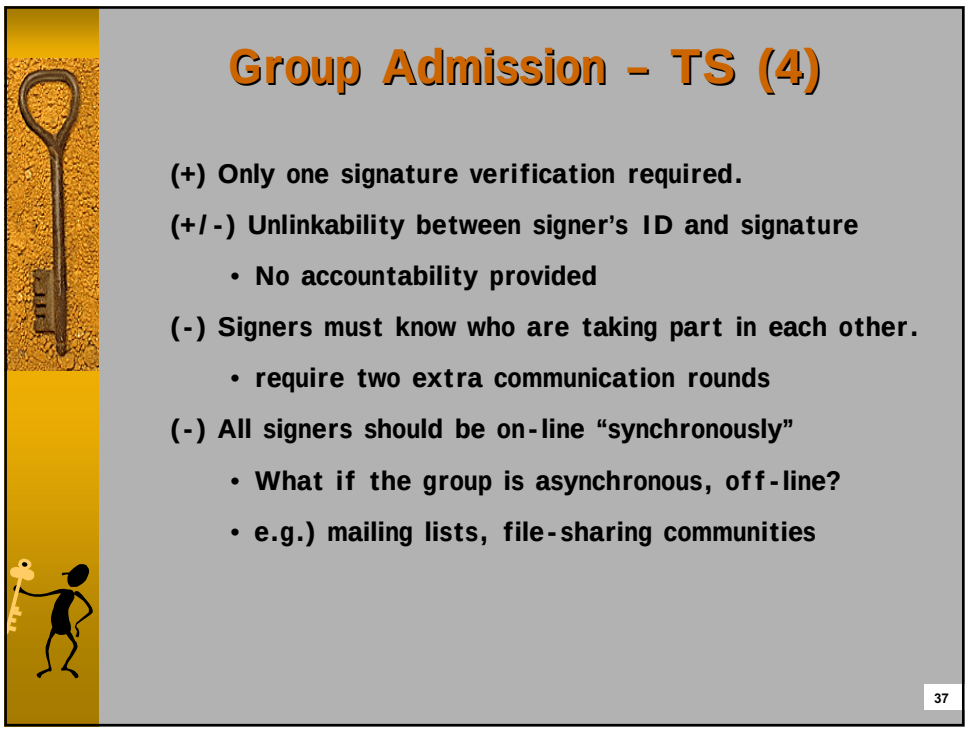
5. Compute a partial sign

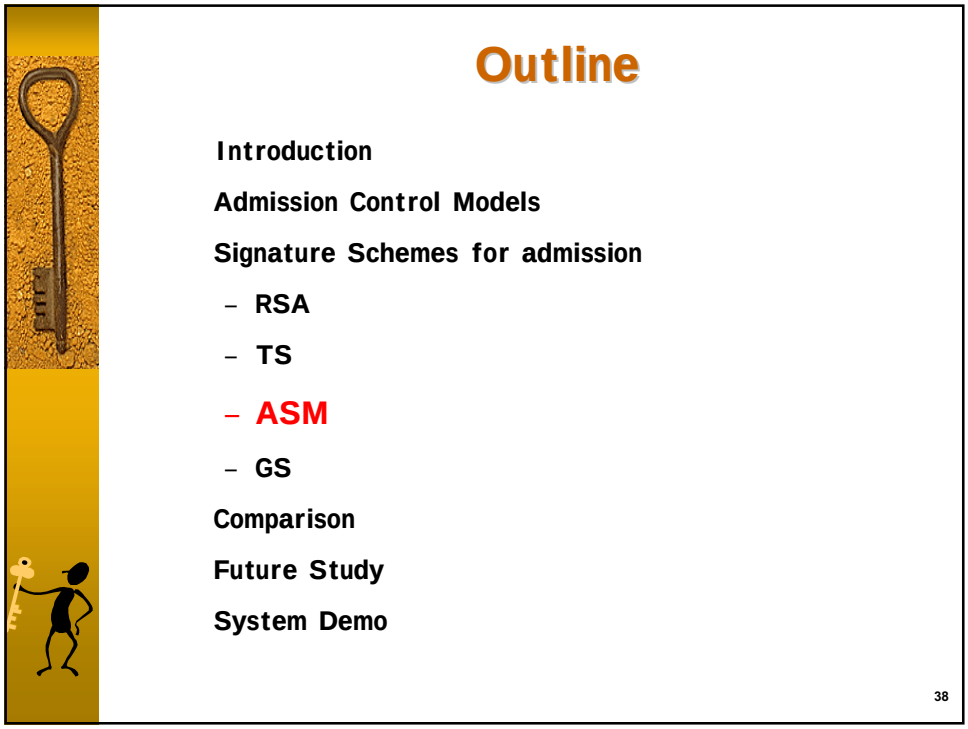
$$PSIG_i = m^{SS(i) l_i(0)}$$

6. Compute a partial secret share

$$PSS(i) = SS(i) \cdot l_i(ID_{new})$$

36


Group Admission – TS (4)
(+) Only one signature verification required.
(+/-) Unlinkability between signer's ID and signature
• No accountability provided
(-) Signers must know who are taking part in each other.
• require two extra communication rounds
(-) All signers should be on-line "synchronously"
• What if the group is asynchronous, off-line?
• e.g.) mailing lists, file-sharing communities
37


Outline
Introduction
Admission Control Models
Signature Schemes for admission
– RSA
– TS
– ASM
– GS
Comparison
Future Study
System Demo
38

Group Admission – ASM (1)

Based on Schnorr signatures

Setup process

$$g = b^{\frac{p-1}{q}} \bmod p$$

q=
91393660525024904359082805889697653376346777 2561

p=
11939328203597295838024350196951597430328245 6448271100115547869803212377630766000869655 2093497044434406317962812367019778641323190 5616974344199092135461044079250903138256737 0 9244702472866333159179400043468028439530383 1524791950728359107386772710088776371211306 5008960935756028735985287173153878077288805 95167651

g=
97901960952447623788172243961784046206554077 4352484547080919927687376930179633373755493 5214889818180397669138683817383357711083643 0574521858762016281481096166580921242916211 4420133746111292818039339689542639862640462 8 3621356452156356491497809289625641129122812 3427142599148138987727049367525047928224683 5912326

Singing process

- random x (x: secret)
- Generate $y = g^x \bmod p$ (y: public)
- random r
- Compute $c = g^r \bmod p$, $e=H(m, c)$, $s= (r+xe) \bmod q$
- Signature: (c, s)

Verifying process

- Compute $e' = H(m, c)$
- Compare $g^s = c\, y^{e'} \bmod p$

39

Group Admission – ASM (2)

Singing process

- random x_i (x_i: secret)
- Generate $y_i = g^{xi} \bmod p$
- Compute $Y = \prod y_i \pmod p$
- Select random $r_i \quad (1 \le r_i \le q-1)$

$$E = H(m, \prod g^{r_i}, SL) = H(m, g^{\sum r_i}, SL)$$

$$S = \sum s_i = \sum (r_i + x_i E) \pmod q$$

exponentiation: 1
time: 22 msec

- Signature: (C, S)

Verifying process

- Compute

$$E' = H(m, C, SL)$$

Accountable

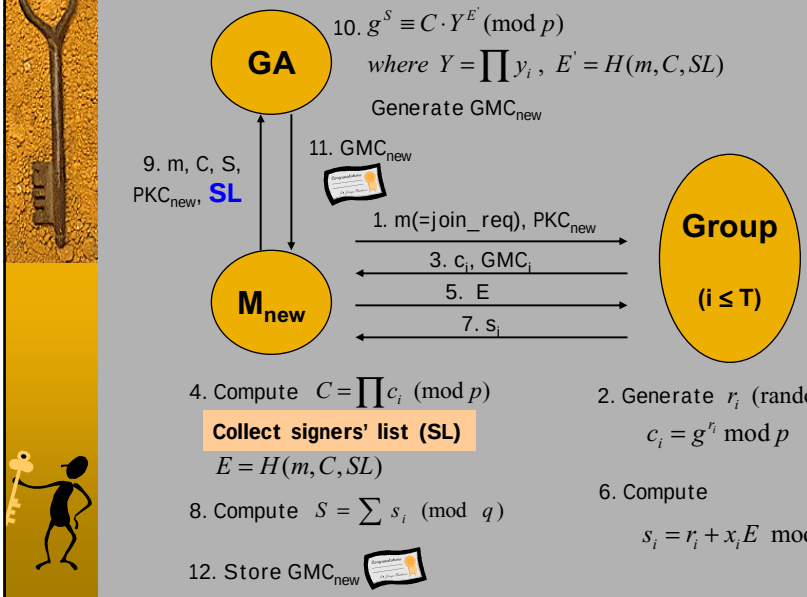
- Compare

$$g^S \equiv C \cdot Y^{E'} \pmod p$$

exponentiation: 2
time: 8 msec

40

Group Admission – ASM (3)



41

Group Admission – ASM (4)

(+/-) Full accountability of the signers is provided.

- **No unlinkability provided**

(-) All signers should be on-line "synchronously"

42



Outline

Introduction

Admission Control Models

Signature Schemes for admission

- RSA
- TS
- ASM
- GS

Comparison

Future Study

System Demo



43



Setting

Groups of entities (people, computers) who are part of a group

Any member can sign on behalf of a group

No one else can sign

Anyone can verify group signature

Signer is anonymous*

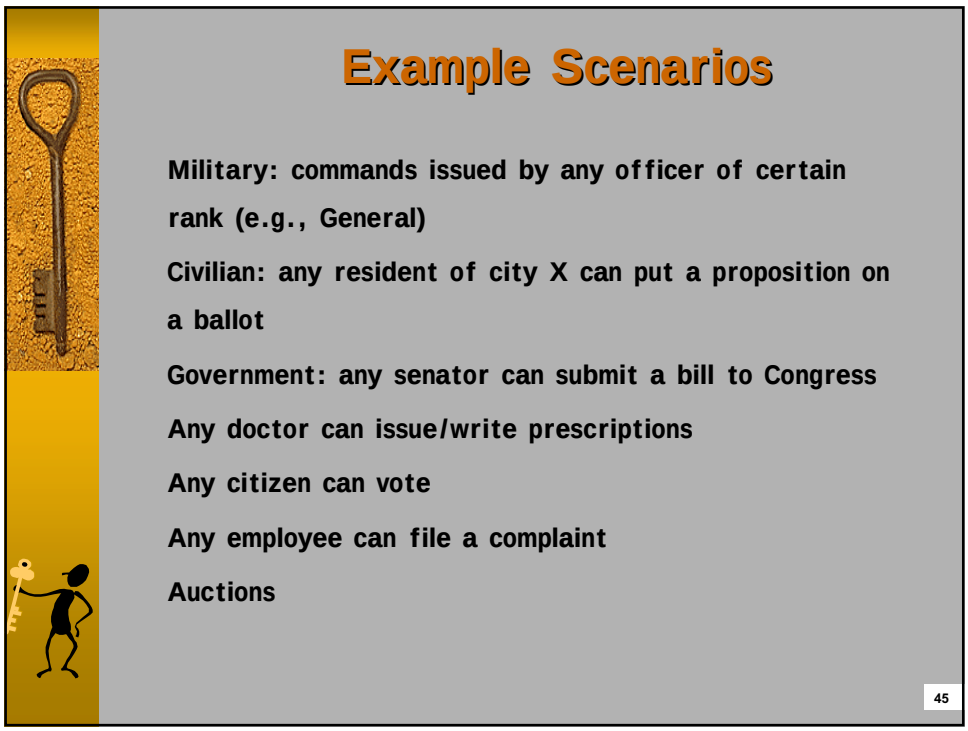
Signer is un-linkable*

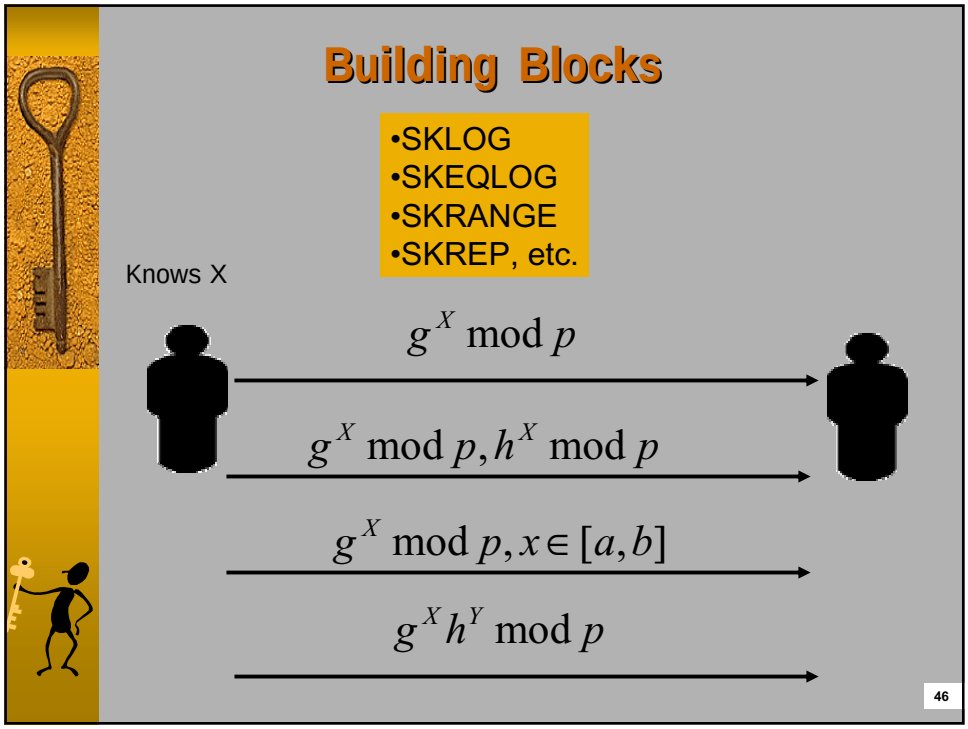
Signer is traceable by Group Manager

Signer cannot be “framed” by anyone



44


Example Scenarios
Military: commands issued by any officer of certain rank (e.g., General)
Civilian: any resident of city X can put a proposition on a ballot
Government: any senator can submit a bill to Congress
Any doctor can issue/write prescriptions
Any citizen can vote
Any employee can file a complaint
Auctions
45


Building Blocks
•SKLOG
•SKEQLOG
•SKRANGE
•SKREP, etc.
Knows X
$g^X \bmod p$
$g^X \bmod p, h^X \bmod p$
$g^X \bmod p, x \in [a,b]$
$g^X h^Y \bmod p$
46

Group Admission – GS (1)

Setup process

p', q' — time: 686 *2 msec

$p = 2p'+1,$

$q = 2q'+1$

$n = pq, QR(n)$

$a, a_0, g, h \in QR(n)$

$X \in Z^*_{p'q'}$

$y = g^X \bmod n$

Λ, Γ



$GPK = (n, a, a_0, g, h, y)$

GPC

p', q', X – group secret

47

Group Admission – GS (2)

Join process

$\breve{x}, \breve{r}$

$C1 = g^{\breve{x}} h^{\breve{r}} \bmod n$

α_i, β_i

$SKREP(g, h, \breve{x}, \breve{r}, C1)$

α_i, β_i

$x_i = (\alpha_i \breve{x}_i + \beta_i)$

$C2 = g^{x_i} \bmod n$

$C2, SKRANGE(a, x_i, C2, \Lambda), etc.$

e_i

time: 8551 msec

$e_i, \ A_i = (g^{X_i} a_0)^{d_i}$

member secret

member public

48

Group Admission – GS (3)

Signing process

$w - random$

$T_1 = A_i y^w$

$T_2 = g^w$

$T_3 = g^{e_i} h^w$

pre-computable

$r_1, r_2, r_3, r_4 - random$

$d_1 = T_1^{r_1} / (a^{r_2} y^{r_3})$

$d_2 = T_2^{r_1} / g^{r_3}$

$d_3 = g^{r_4}$

$d_4 = g^{r_1} h^{r_4}$

$c = (g \| h \| y \| a_0 \| a \| T_1 \| T_2 \| T_3 \| d_1 \| d_2 \| d_3 \| d_4 \| m)$

$s_1 = r_1 - c(e_i - 2^{\gamma_1})$

$s_2 = r_2 - c(x_i - 2^{\lambda_1})$

$s_3 = r_3 - c e_i w$

$s_4 = r_4 - cw$

exponentiation: 11
time: 108 msec

$SIG = \{c, s1, s2, s3, s4, T_1, T_2, T_3\}$

49

Group Admission – GS (4)

Verifying process

$SIG = \{c, s_1, s_2, s_3, s_4, T_1, T_2, T_3\}$ GPK

$d_1' = (a_0^c T_1^{s_1 - c2^{\gamma_1}}) / (a^{s_2 - c2^{\lambda_1}} y^{s_3})$

$d_2' = T_2^{s_1 - c2^{\gamma_1}} / g^{s_3}$

$d_3' = T_2^c g^{s_4}$

$d_4' = T_3^c g^{s_1 - 2^{\gamma_1}} h^{s_4}$

exponentiation: 11
time: 89 msec

$c' = (g \| h \| y \| a_0 \| a \| T_1 \| T_2 \| T_3 \| d_1' \| d_2' \| d_3' \| d_4' \| m)$

Compare c = c'

and

s_1, s_2, s_3, s_4

in correct ranges

50

Group Admission – GS (5)

Opening process

$$SIG = \{c, s_1, s_2, s_3, s_4, T_1, T_2, T_3\}$$

Verify SIG

group secret

$$A_i = T_1 / T_2^{X} \bmod n$$

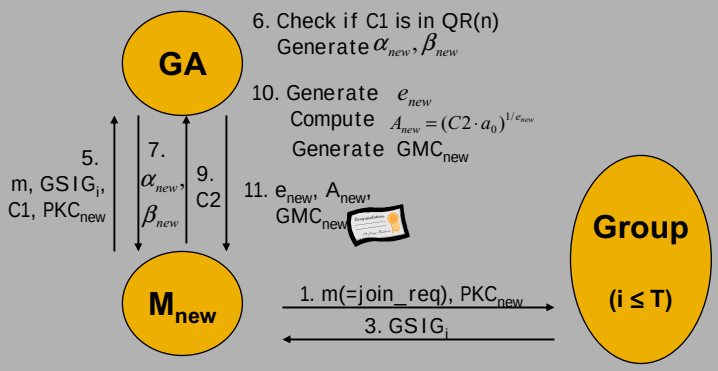
$$SKEQLOG\ (y, g, \frac{T_1}{A_i}, T_2)$$



exponentiation: 12
time: 106 msec

51

Group Admission – GS (6)



4. Generate $\breve{x}_{new}, \breve{r}$

$$C1 = g^{\breve{x}_{new}} h^{\breve{r}}$$

2. Compute GSIG$_i$

$$= \{c, s_1, s_2, s_3, s_4, T_1, T_2, T_3\}$$

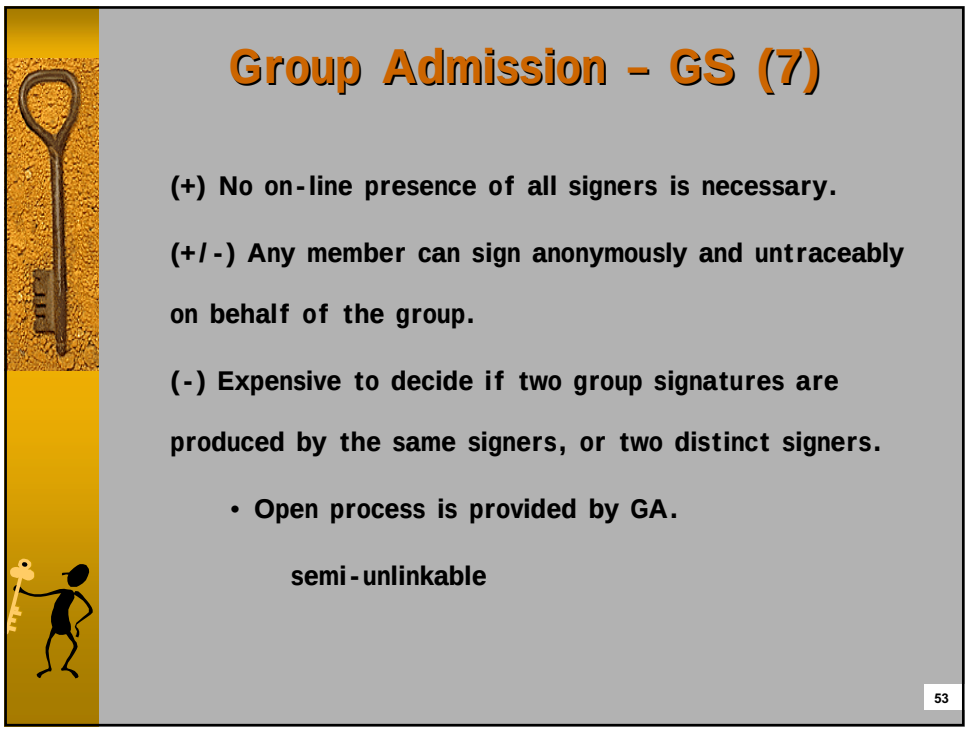
8. Compute

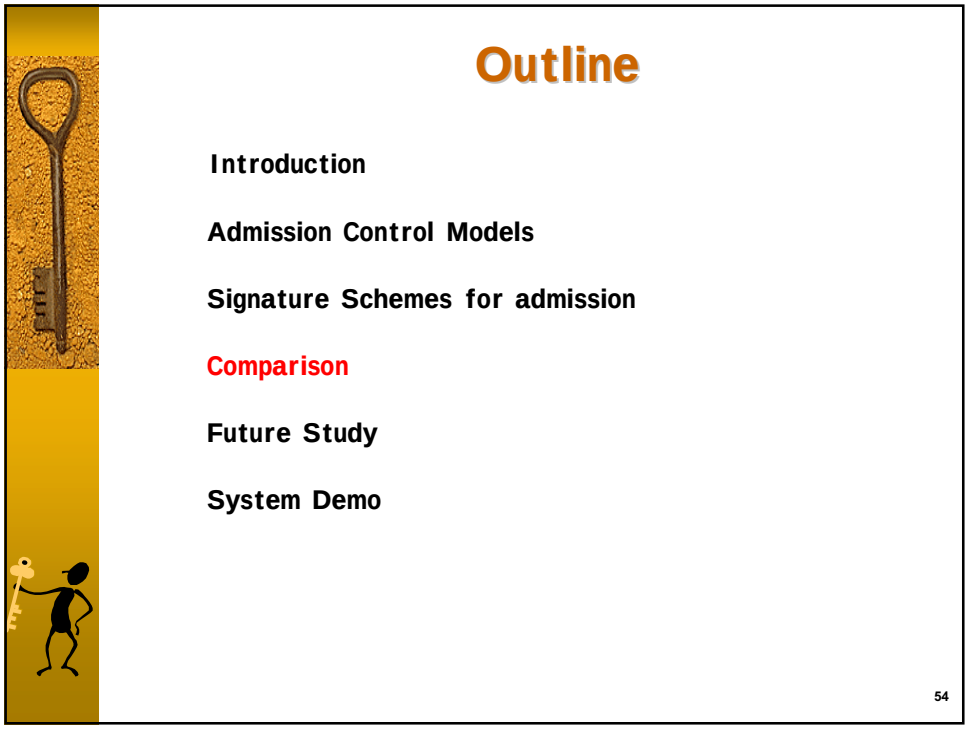
$$x_{new} = (\alpha_{new} \breve{x}_{new} + \beta_{new})$$

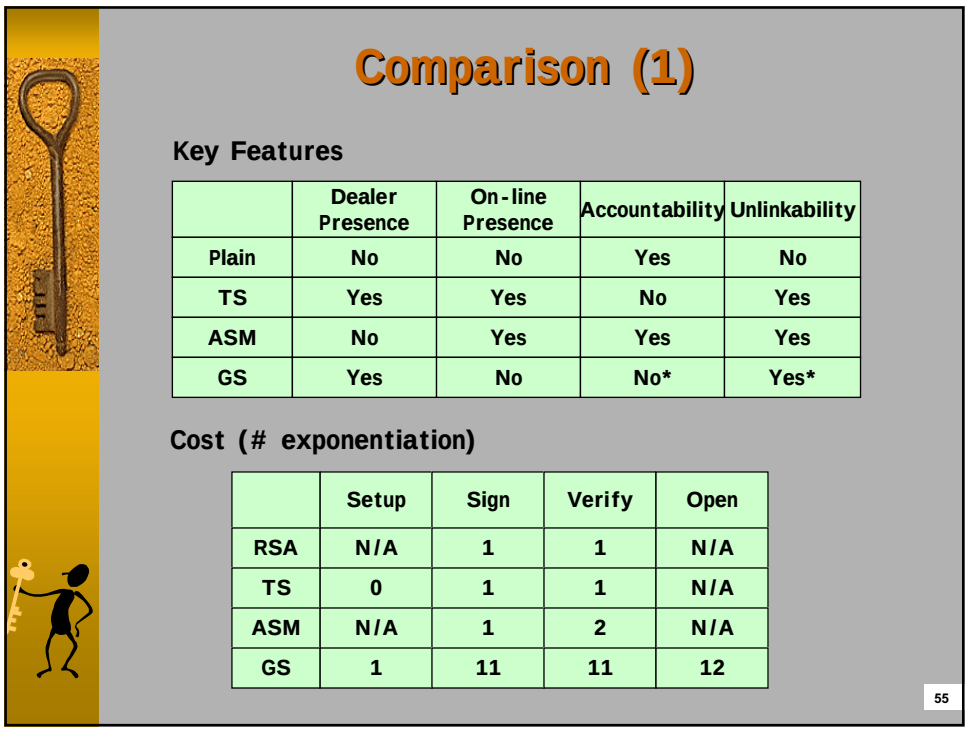
$$C2 = g^{x_{new}} \bmod n$$

12. Store e$_{new}$, A$_{new}$, GMC$_{new}$

52


Group Admission – GS (7)
(+) No on-line presence of all signers is necessary.
(+/-) Any member can sign anonymously and untraceably on behalf of the group.
(-) Expensive to decide if two group signatures are produced by the same signers, or two distinct signers.
• Open process is provided by GA.
semi-unlinkable
53


Outline
Introduction
Admission Control Models
Signature Schemes for admission
Comparison
Future Study
System Demo
54



Comparison (1)

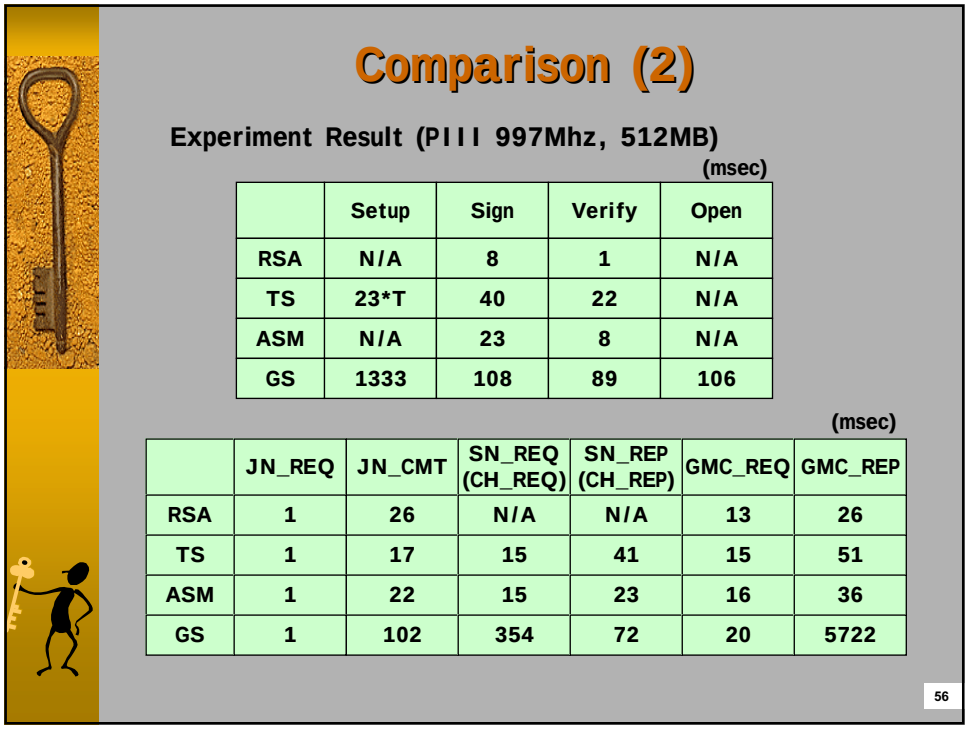
Key Features

	Dealer Presence	On-line Presence	Accountability	Unlinkability
Plain	No	No	Yes	No
TS	Yes	Yes	No	Yes
ASM	No	Yes	Yes	Yes
GS	Yes	No	No*	Yes*

Cost (# exponentiation)

	Setup	Sign	Verify	Open
RSA	N/A	1	1	N/A
TS	0	1	1	N/A
ASM	N/A	1	2	N/A
GS	1	11	11	12

55



Comparison (2)

Experiment Result (PIII 997Mhz, 512MB)

(msec)

	Setup	Sign	Verify	Open
RSA	N/A	8	1	N/A
TS	23*T	40	22	N/A
ASM	N/A	23	8	N/A
GS	1333	108	89	106

(msec)

	JN_REQ	JN_CMT	SN_REQ (CH_REQ)	SN_REP (CH_REP)	GMC_REQ	GMC_REP
RSA	1	26	N/A	N/A	13	26
TS	1	17	15	41	15	51
ASM	1	22	15	23	16	36
GS	1	102	354	72	20	5722

56



Comparison (3)

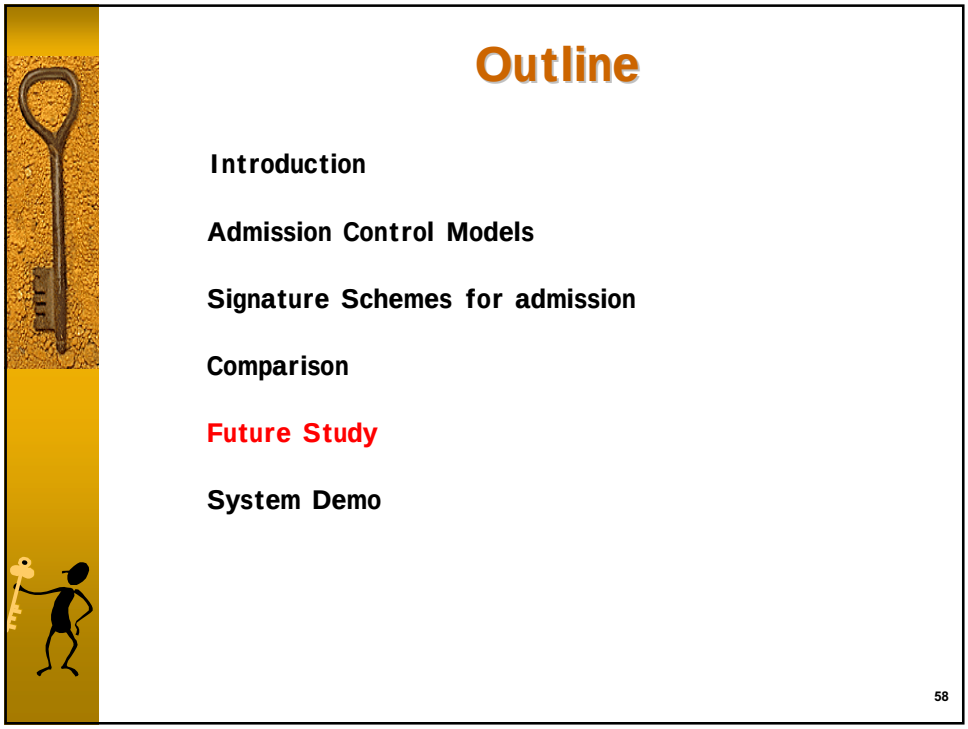
Estimated Join Cost

- RSA = JN_REQ + AVG(JN_CMT) + GMC_REQ + GMC_REP + (T-1) * Verify
- TS = JN_REQ + AVG(JN_CMT) + SN_REQ + AVG(SN_REP) + GMC_REQ + GMC_REP
- ASM = JN_REQ + AVG(JN_CMT) + SN_REQ + AVG(SN_REP) + GMC_REQ + GMC_REP
- GS = JN_REQ + AVG(JN_CMT) + CH_REQ + CH_REP + GMC_REQ + GMC_REP + (T-1) * Verify

(msec)

T	RSA	TS	ASM	GS
1	66	140	112	6272
3	69	140	112	6449
5	72	140	112	6627
10	79	140	112	7070
20	94	140	112	7957

57



Outline

Introduction

Admission Control Models

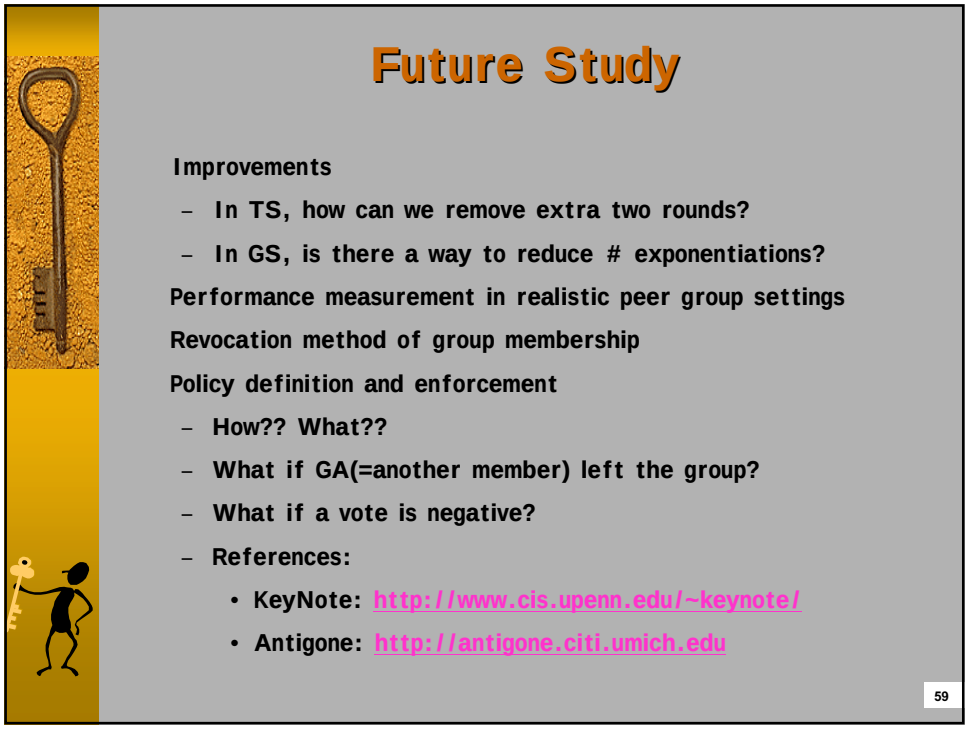
Signature Schemes for admission

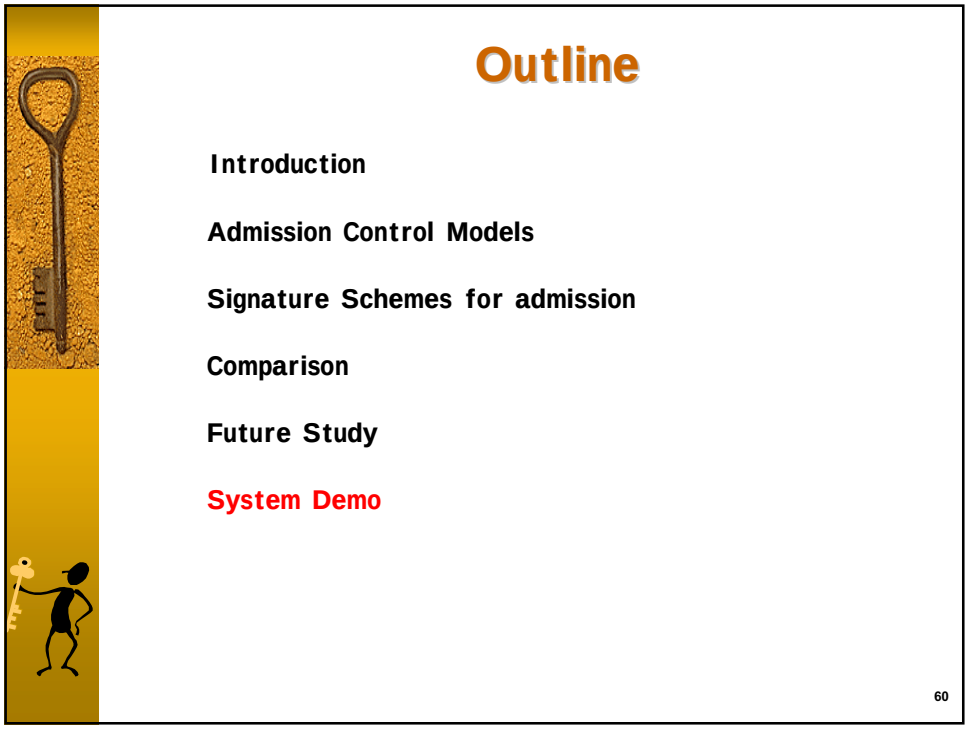
Comparison

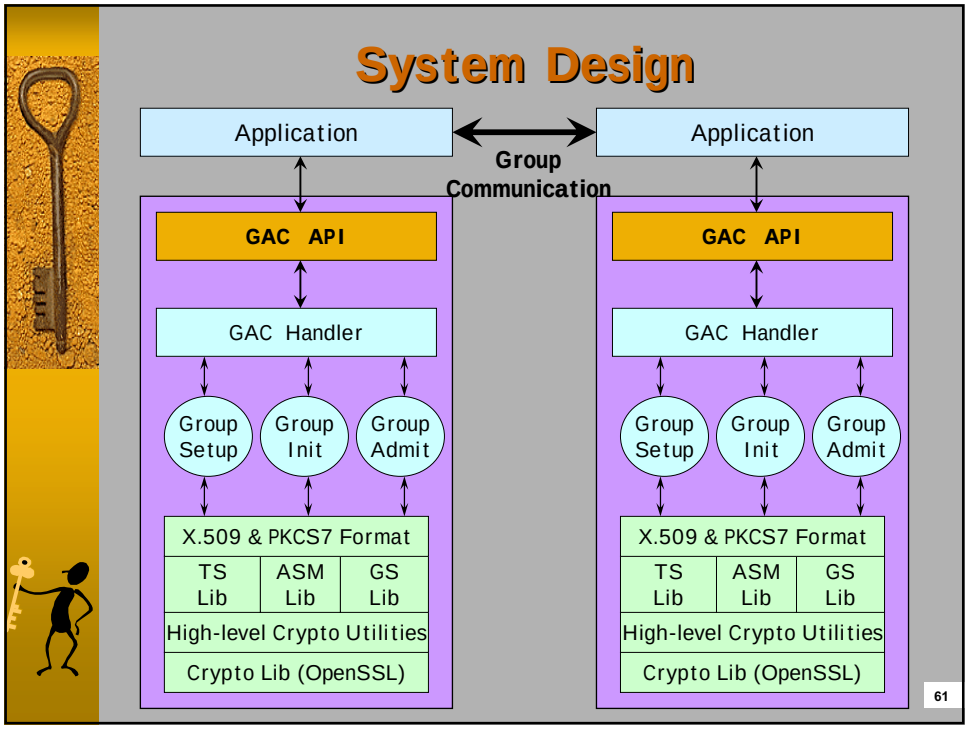
Future Study

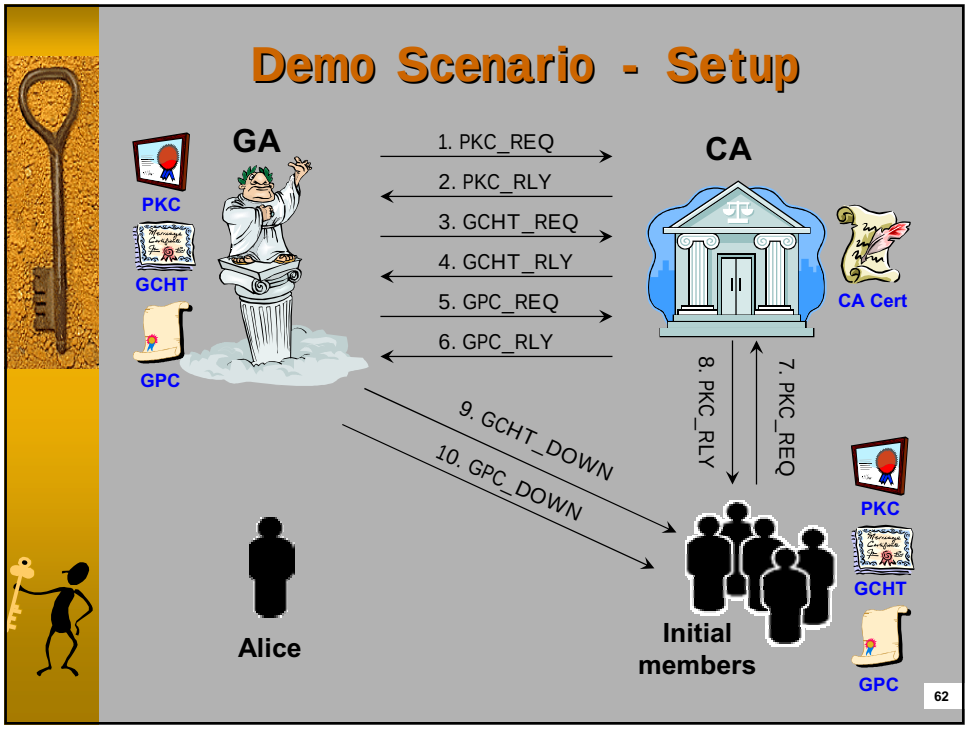
System Demo

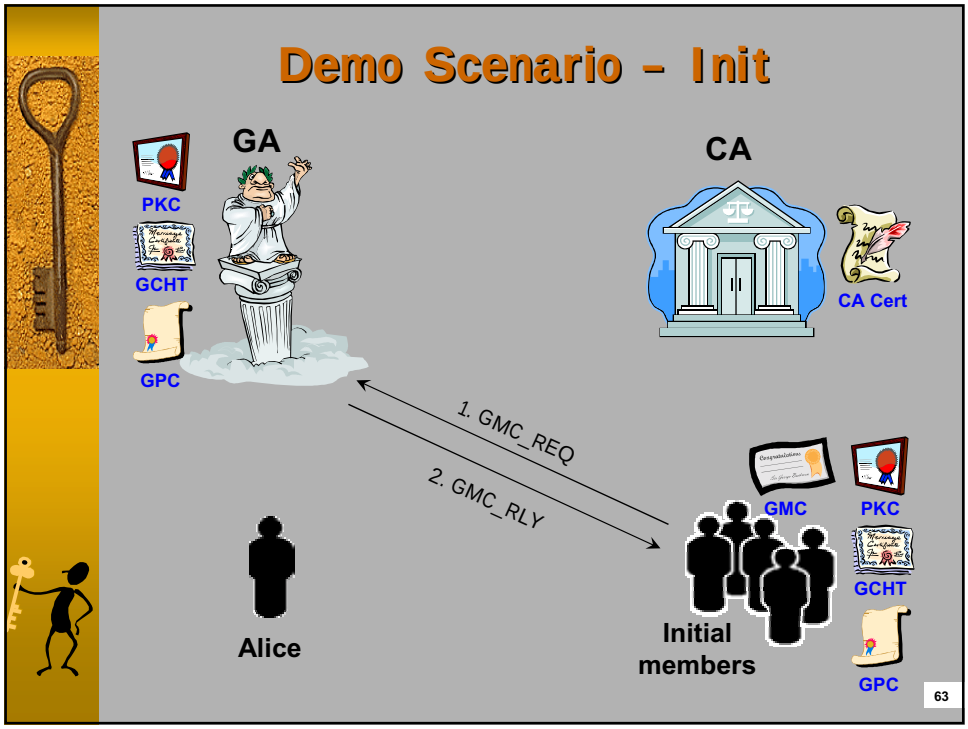
58

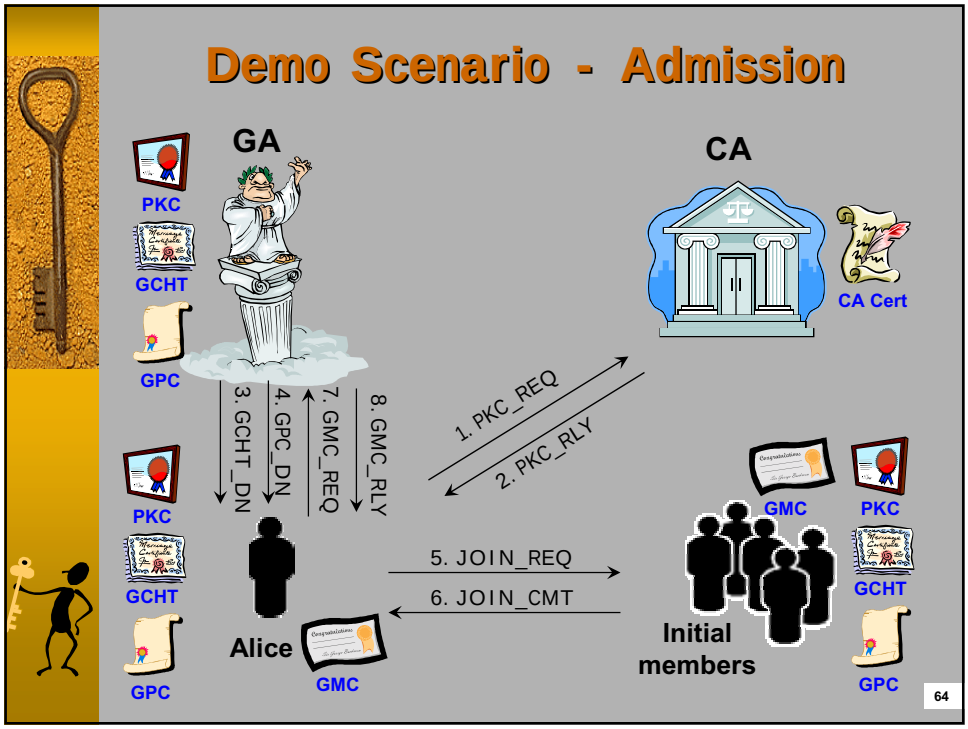

Future Study
Improvements
– In TS, how can we remove extra two rounds?
– In GS, is there a way to reduce # exponentiations?
Performance measurement in realistic peer group settings
Revocation method of group membership
Policy definition and enforcement
– How?? What??
– What if GA(=another member) left the group?
– What if a vote is negative?
– References:
• KeyNote: http://www.cis.upenn.edu/~keynote/
• Antigone: http://antigone.citi.umich.edu
59


Outline
Introduction
Admission Control Models
Signature Schemes for admission
Comparison
Future Study
System Demo
60


System Design
Application
Application
Group Communication
GAC API
GAC API
GAC Handler
GAC Handler
Group Setup
Group Init
Group Admit
Group Setup
Group Init
Group Admit
X.509 & PKCS7 Format
TS Lib
ASM Lib
GS Lib
High-level Crypto Utilities
Crypto Lib (OpenSSL)
X.509 & PKCS7 Format
TS Lib
ASM Lib
GS Lib
High-level Crypto Utilities
Crypto Lib (OpenSSL)
61


Demo Scenario - Setup
GA
CA
PKC
GCHT
GPC
1. PKC_REQ
2. PKC_RLY
3. GCHT_REQ
4. GCHT_RLY
5. GPC_REQ
6. GPC_RLY
CA Cert
8. PKC_RLY
7. PKC_REQ
9. GCHT_DOWN
10. GPC_DOWN
PKC
GCHT
GPC
Alice
Initial members
62


Demo Scenario – Init
GA
CA
PKC
GCHT
GPC
CA Cert
1. GMC_REQ
2. GMC_RLY
GMC
PKC
GCHT
GPC
Alice
Initial members
63


Demo Scenario - Admission
GA
CA
PKC
GCHT
GPC
CA Cert
3. GCHT_DN
4. GPC_DN
7. GMC_REQ
8. GMC_RLY
1. PKC_REQ
2. PKC_RLY
GMC
PKC
GCHT
GPC
5. JOIN_REQ
6. JOIN_CMT
Alice
GMC
Initial members
64


The END
65