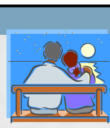
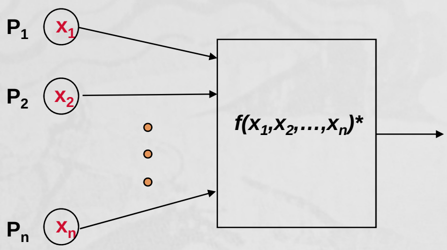
Multiparty Cryptographic Protocols

m-party Cryptographic Protocol



(Def.) **While keeping individual's information x_i secret, everyone can learn the result of *f()*.**
Even if arbitrary subset *S* which is less than the half of an input set behave maliciously, (If *t* malicious players exist, we say *t-secure* protocol)

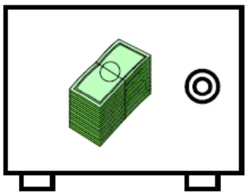
(Privacy) Other honest players except *S* can't know secret x_i of P_j.
(Correctness) any P_j can know the value of *f()*.



*(Ex.)
$f() = x_1 + x_2 + \ldots + x_n$ or
$= x_1 \oplus x_2 \oplus \ldots \oplus x_n$ or
$= \max\{x_1,x_2,\ldots,x_n\}$

Secret Sharing

The "classical" way that two crooks (or two bank vice presidents), who do not trust one another, can share a secret.



The **secret**: 1 0 0 1 0 1 1 0 0 1

The **shares** 1 0 0 1 0 | 1 1 0 0 1

(Note) VSS(Verifiable SS) = SS + ZKIP !!

(w,t) Secret Sharing(I)

(Step 1) A dealer selects a secret, a_0 (< p : prime) as a constant term and t-1 degree random polynomial with arbitrary coefficients as :

$h(x)=a_0 + a_1x + a_2x^2 + \ldots + a_{k-1}x^{t-1}$ mod p

(Step 2) Distributes $h(x_i)$ $(i=1,\ldots,w)$ to a share holder.

(Step 3) When t shadows $K_1, K_2,\ldots,K_t$ among w are given, recover a_0 by using the Lagrange Interpolation

$h(x)= \Sigma_{s=1}^{t} K_i \Pi_{j=1,j\neq s}^{t} (x - x_j)/(x_j - x_s)$ mod p

(w,t) Secret Sharing(II)

(Parameter) $t=3$, $w=5$, $p=17$, $a_0=13$

(Polynomial) $h(x) = (2x^2 + 10x + 13) \bmod 17$

(Secret sharing) 5 shadows, $K_1=h(1)=25 \bmod 17=8$, $K_2=h(2)=7$, $K_3=h(3)=10$, $K_4=h(4)=0$, $K_5=h(5)=11$

(Recover secret) By using $K_1=8$, $K_3=10$, and $K_5=11$,

$h(x) =\{8(x-3)(x-5)/(1-3)(1-5) +10(x-1)(x-5)/(3-1)(3-5) + 11(x-1)(x-3)/(5-1)(5-3)\} \bmod 17$

$= \{8*inv(8,17)*(x-3)(x-5) + 10 *inv(-4,17)(x-1)(x-5) +11 *inv(8,17)*(x-1)(x-3)\} \bmod 17$

$=8*15(x-3)(x-5) +10*4*(x-1)(x-5)\ 11*15*(x-1)(x-3) \bmod 17$

$= 19x^2 - 92x +81 \bmod 17 = 2x^2 + 10x + 13 \bmod 17$

(Original secret) $h(0)=13$

Mental Poker from Wiki

- **Mental poker** is the common name for a set of cryptographic problems that concerns playing a fair game over distance without the need for a trusted third party. The term is also applied to the theories surrounding these problems and their possible solutions. The name stems from the card game poker which is one of the games to which this kind of problem applies. A similar problem is flipping a coin over a distance.

Mental Poker(Def.)

- Non face-to-face digital poker over communication channel like the Internet.
- Assumption
  - No trust each other.
  - During setting up protocol, information must be transferred in an unbiased and fair manner. After transfer is completed, validation must be made correctly.
- Expandability from *2* players to *n* players.

History of Mental Poker

- SRA('79) : Using RSA
- Liption/Coppersmith('81) : Using Jacobian value
- GM('82) : Using probabilistic encryption
- Barany & Furedi ('83) : Over 3 players
- Fortune & Merrit('84) : Solve player's compromise
- Crepeau ('85) : Game without trusted dealer
- Crepaeu('86) : ZKIP without revealing strategy
- Kurosawa('90) : Using *r*-th residue cryptosystems
- Park('95) : Using fault-tolerant scheme
- etc.

Basic Method

- Player A shuffles the card and post them into the deck
- Player B selects 5 cards from the deck
- (Problem)
  - A can know B's selection
  - A is in advantage position than B
- (Solution)

  Use cryptographic protocols

9

Mental Poker 1 by RSA (I)

(Preparation) A and B prepare public keys (E_A, E_B) and secret keys (D_A,D_B) of RSA cryptosystem.

(Step 1) Using B's public key E_B , B posts all 52 encrypted cards ($E_B(m_i)$) into the deck.

(Step 2) A selects 5 cards in the deck and sends them to B. B decrypts ($D_A(E_A(m_i))=m_i$) using his secret key and keep them as his own cards.

(step 3) A selects 5 cards from the remaining 47 cards and encrypts using his public key ($E_A(E_B(m_j))$) and sends them to B.

(step 4) B decrypt 5 cards using his secret key and send ($E_A(m_j)$) to A

(step 5) Using his secret key D_A, A decrypts $E_A(m_j)$ and keeps them as his cards.

Note that RSA is commutative PKC.

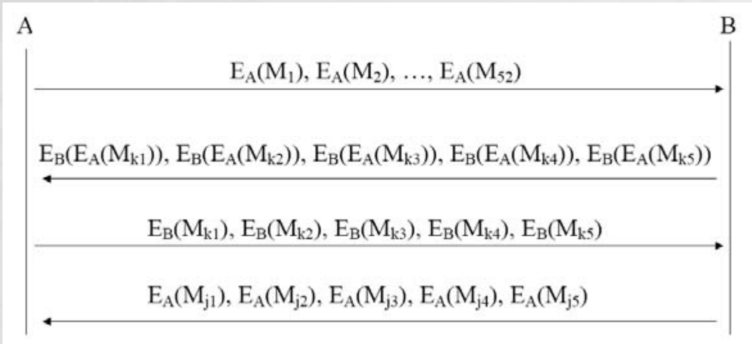
(Victory or defeat) Reveal his own cards to counterparts and decides

(Validation) Reveal his secret card to counterpart

10

Mental Poker 2 by RSA(II)

- Require commutative cryptosystem



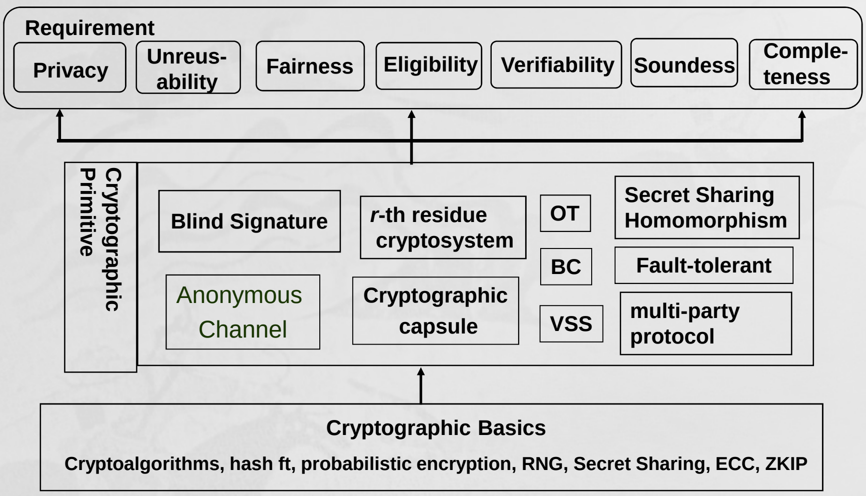
Electronic Vote

- Yes-No Vote
  - While keeping each voter's vote secret (x_i), compute only total sum $(T=x_1+x_2+\ldots+x_n)$
  - Malicious t $(< n)$ players among n exist
    - t-secure multiparty protocol
  - Basic tool
    - Blind signature
    - VSS (Verifiable Secret Sharing)
    - OT (Oblivious Transfer)

Security Requirements of E-vote

- *Privacy : keeping each vote secret*
- *Unreusability : prevent double voting*
- *Fairness : if interruption occurs during voting process, it doesn't affect remaining voting*
- *Eligibility : only eligible voter can vote*
- *Verifiability : can't modify voting result*
- *Soundness : preventing malicious acts*
- *Completeness : exact computation*

Cryptographic tool for e-vote



Votopia

Introduction (1)

- A project “VOTOPIA” carried out by effective collaboration among some of the prominent Korean and Japanese IT firms and research institutes
  - Korea: IRIS, KISTI, KSIGN, LG CNS, SECUi.COM, STI, VOCOTECH
  - Japan: NTT, University of Tokyo
- IRIS, affiliated to ICU, Korea - initiated, managed, and coordinated the project

Introduction (2)

- **Korea/Japan teams initiated the idea of VOTOPIA(*) in 2000, in order to show their strong support to the most prestigious mega event "2002 FIFA World Cup Korea/Japan(TM)".**
- **Korea PKI**
  - 10M broadband Internet users at home
  - 3M certificate holders for Internet banking, e-auction, *etc*.
- **Verify secure Internet system using cryptographic primitives and show its usefulness as replacement of paper voting.**

* VOTOPIA is in no way associated with FIFA and does not intend to violate international legal issues and digital copy rights.

❑*17*

System Design (1)

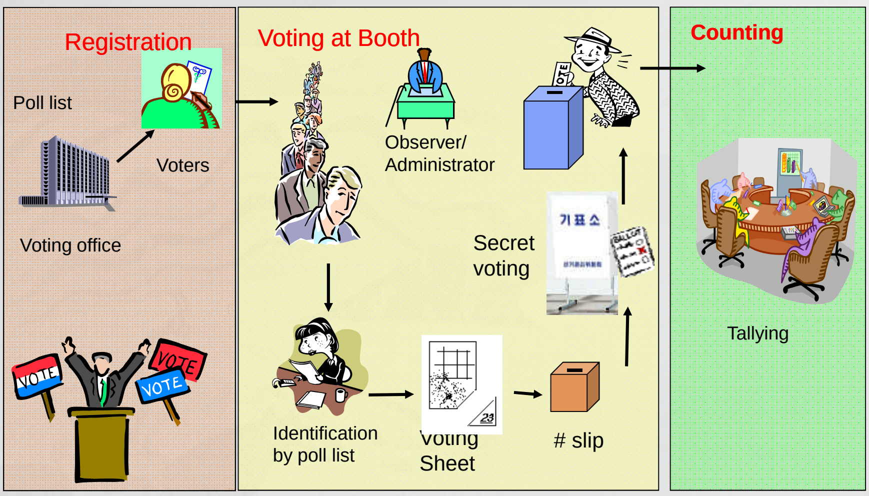
- **Remote Internet voting based on blind signature under PKI for large scale election**
- **Anyone registered once can cast a vote**
- **2 times voting to select MVP and Best GK**
  - Preliminary vote (period. candidates, notification) : (Jun. 1 ~14, 32 teams, June 15 10 AM)
  - Main vote(period. candidates, notification) : (Jun. 16 ~ 30, 16 teams, June 30 12 PM)
  - one team has 20 players and 3 GKs
- **Meet basic cryptographic requirements**
  - ✓ Privacy : All votes must be secret
  - ✓ Completeness : All valid votes are counted correctly
  - ✓ Soundness : The dishonest voter cannot disrupt the voting
  - ✓ Unreusability : No voter can vote twice
  - ✓ Eligibility : No one who isn't allowed to vote can vote
  - ✓ Fairness : Nothing can affect the voting

❑*18*

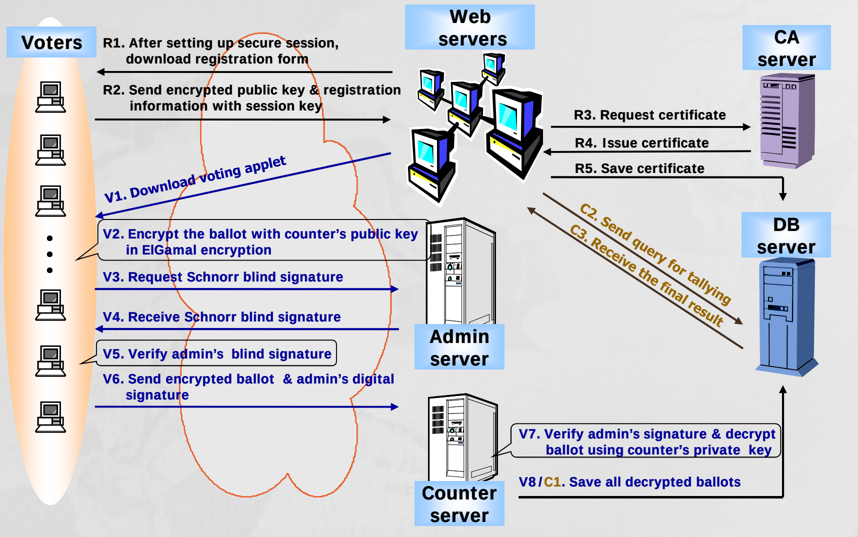
System Design (2)

- **Client side**
  - Fast and easy, user-friendly web interface
  - No tamper-proof device provided
  - Consider various kinds of platforms, OS browsers, and Internet speed
  - Allow as many voters can cast
- **Server side**
  - Highly secure network and computer system
    - Anti-hacking such as DOS attack, *etc*
  - Large DB handling
  - Fault-tolerance and high reliability
  - Reasonable processing when registering and voting

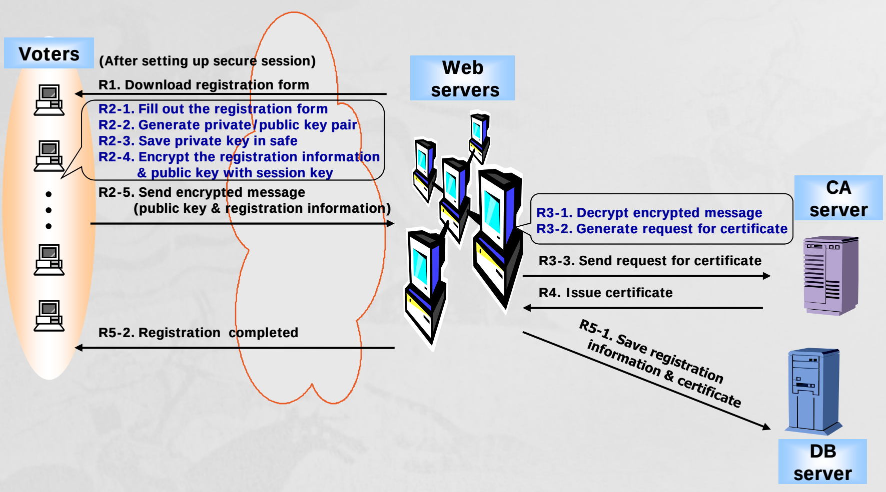
Paper Voting

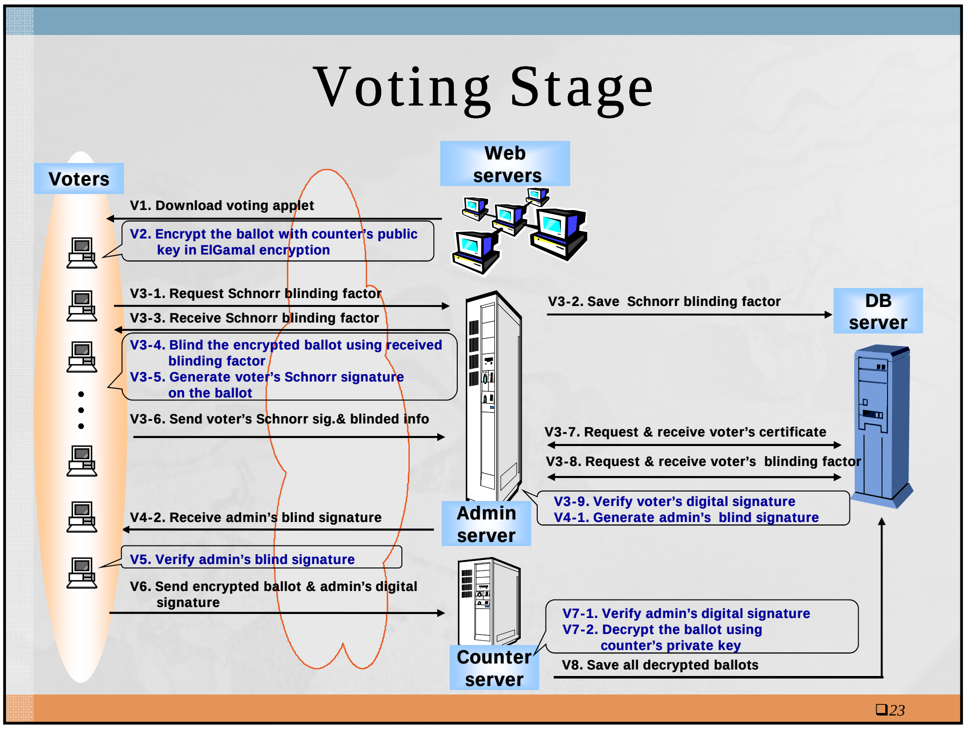


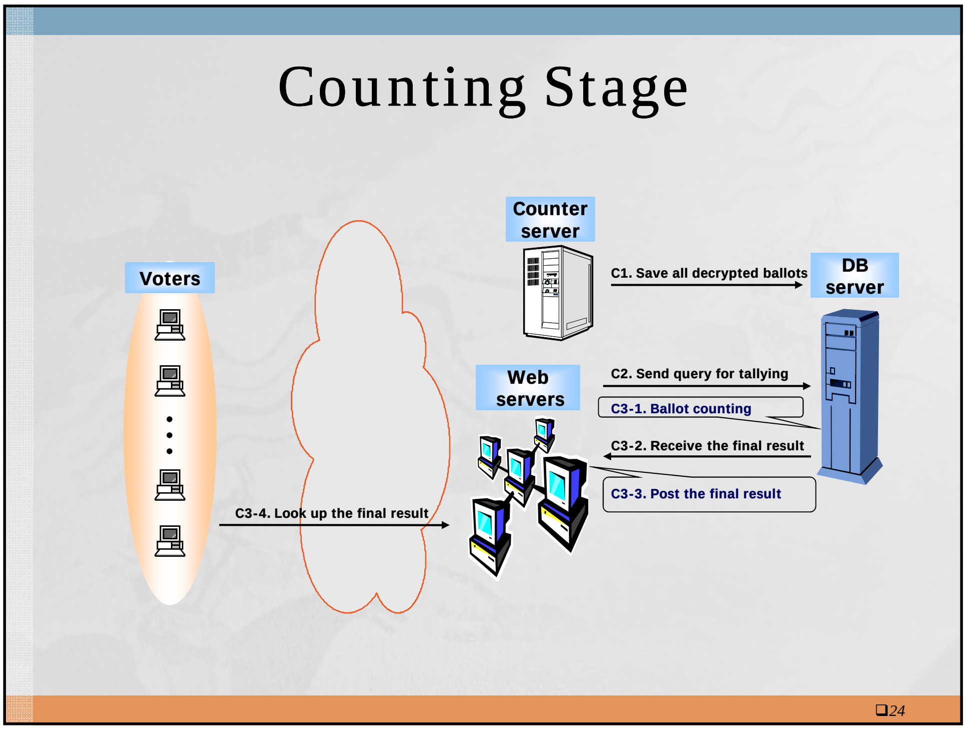
Internet Voting



Registration Stage

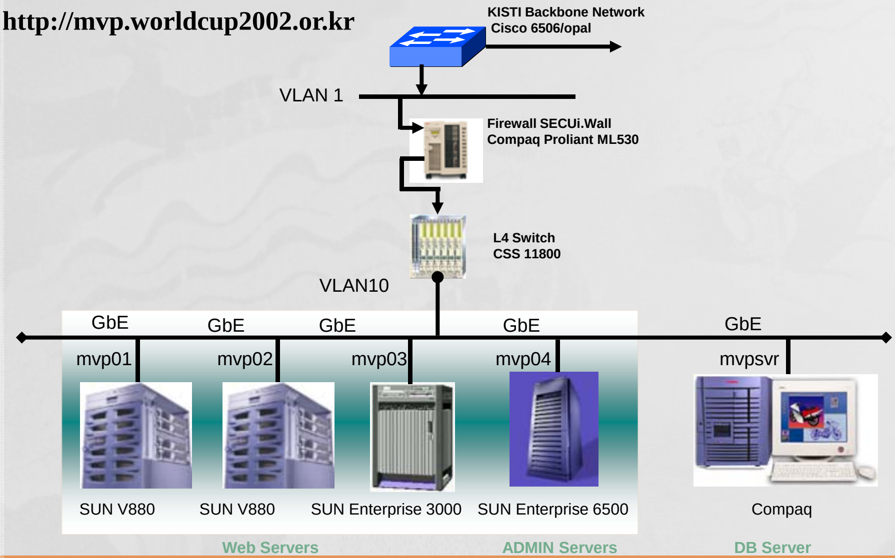



Voting Stage
Web servers
Voters
V1. Download voting applet
V2. Encrypt the ballot with counter's public key in ElGamal encryption
V3-1. Request Schnorr blinding factor
V3-2. Save Schnorr blinding factor
DB server
V3-3. Receive Schnorr blinding factor
V3-4. Blind the encrypted ballot using received blinding factor
V3-5. Generate voter's Schnorr signature on the ballot
V3-6. Send voter's Schnorr sig.& blinded info
V3-7. Request & receive voter's certificate
V3-8. Request & receive voter's blinding factor
V3-9. Verify voter's digital signature
V4-1. Generate admin's blind signature
V4-2. Receive admin's blind signature
Admin server
V5. Verify admin's blind signature
V6. Send encrypted ballot & admin's digital signature
V7-1. Verify admin's digital signature
V7-2. Decrypt the ballot using counter's private key
Counter server
V8. Save all decrypted ballots
23


Counting Stage
Counter server
C1. Save all decrypted ballots
DB server
Voters
Web servers
C2. Send query for tallying
C3-1. Ballot counting
C3-2. Receive the final result
C3-3. Post the final result
C3-4. Look up the final result
24

Configuration of Servers (1)

http://mvp.worldcup2002.or.kr

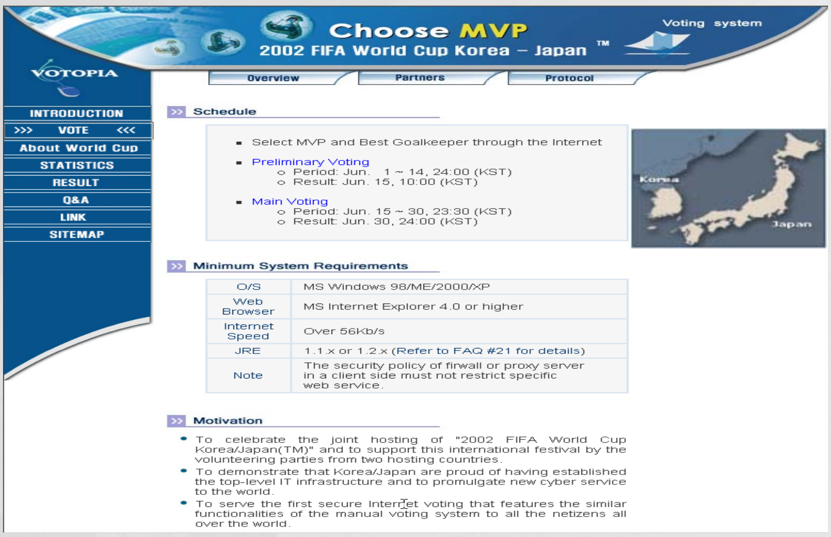


Configuration of Servers (2)

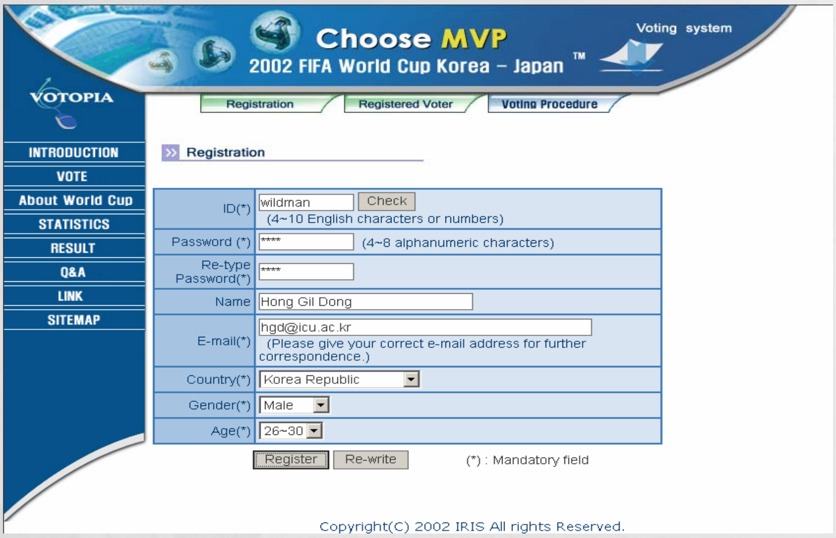
Implementation

- **Client**
  - Java1.2, JLOCK+
  - MS Explorer 4.0 on Windows98 /ME/XP/2000
  - Korean, Japanese, English and Chinese
- **Web, DB, Admin, and Counter Servers**
  - Solaris 2.5.4 (SUN OS 5.8), Oracle DB 8.0.6 , JDBC
  - Tomcat3.1, Apache1.3.12, JSSWEB+
- **Encryption and Certificate**
  - ElGamal encryption & Schnorr (blind) signature
  - Simplified X.509v3 certificate issued by CA server

Homepage(http://mvp.worldcup2002.or.kr)

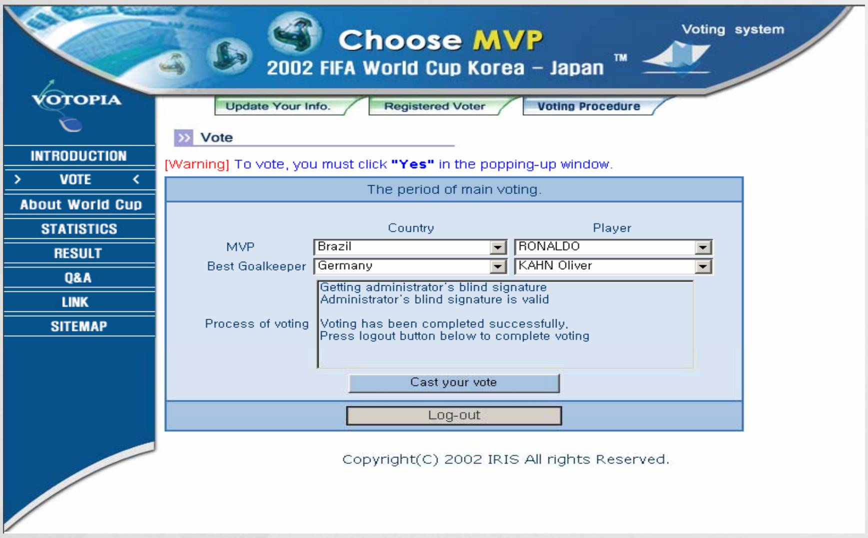


Registration Page



29

Voting Page



30

Data Size & Voting Time

- Data Size
  - Applet for SSL Connection at *R1*
    - 207 KB
  - Voting Client Applet at *V1*
    - 215 KB
  - Voter's Registration Information at *R2-1*
    - Avg 50 Bytes
  - Key Size : Security / Performance Trade-off
    - Voter : 256 bit ElGamal Encryption & 512bit Schnorr Signature
    - Administrator : 256 bit Schnorr Blind Signature & 512bit Schnorr Verification
    - Counter : 256 bit ElGamal Decryption
- Voting Time (*V1* - *V6*)
  - Avg 2 (or 3) min. under Pentium III 100M LAN (or 56K modem)
  - Including Admin's & Counter's Server Computation Time : avg 195 msec

Sample Vote(1)

Voter's ID : tank02
tank02's private key
Private Key *x*: 9fa840a6974fc04810db89b73461bb8d561a20bd
Security Parameters:
p :
c16cbad34d475ec5396695d694bc8bc47e598e23b5a9d7c5cec82d65b6827d44e953784
84730c0bff1f4cb56f47c6e51054be89200f30d43dc4fef9624d4665b
q : b7b810b58c0934f642878f360b96d7cc26b53e4d
g :
4c53c726bdbfbba6549d7e731939c6c93a869a27c5db17ba3cac589d7b3e003fa735f290
cfd07a3ef10f35155f1a2ef70335af7b6a5211a1103518fba44e9718

Admin's public key
Public Key *y*: c0ace983c8c4346b99b54e96505f94b7b2ba25d6764c16fcb9f239cbc447402f
Security Parameters:
p : f668a94f0ce284e30ce284e30776b59b319fec12ba069d10c56498e2bd0cb42f
q : e3109c1fd13c8d637f6c39e6c0a6e9dfc0a6e9df
g : a7688634018f161c62de5014ca99e983759fb4f67b575bbc4b51d32392177a40

Sample Vote (2)

Counter's public key

Public Key *y*: b6fbabc9259a1267fcde3a82ebc060781c9404b7caf4c07837fb86b1054207fb
Security Parameters:
p : e204679a6b62fe446b62fe440c0bfea01223d98b7b65a6b1095962b41d502d21
q : ad9c0afead1c2e24900e4799ddcade6bddcade6b
g : 329d730dea5e5cff79b9a46968414e16ec610dbdd3e1b7d090aec0bdef310411

Message from Admin1(*tildeA*):
2004d4c5ff693b20ad4574a062c1eb80d6e2e0d79639f755cd9e4de14593f9ceec

Vote : 10000001431000000160
Tag : 4277bb955fad5f86

Encoded vote(*vi*) : 3130303030303031343331303030303030313630427 7bb955fad5f86

Message for ElGamal encryption :
31303030303030313433313030303030303136304277bb955fad5f86

Sample Vote (3)

Random number k for ElGamal encryption :
4af1c2911bd5f59789307fd12366436e68dbd0ae

G(=*g^k mod p*) :
316aafb99ed1a7565e09d795a1c4bc1bc884f5069b3e3af12c61976bd929cd35
M(=*m*(y^k) mod p*) :
9f88bcf0128a500c218c8fbde13a21ca8eae32caa58ac9339d8c3a5eaa79489d

Encrypted *vi(ev)* :
4400209f88bcf0128a500c218c8fbde13a21ca8eae32caa58ac9339d8c3a5eaa79489d0
020316aafb99ed1a7565e09d795a1c4bc1bc884f5069b3e3af12c61976bd929cd35

Blinding encrypted *vi*
Random commitment *tildeA* for blinding given by signer
4d4c5ff693b20ad4574a062c1eb80d6e2e0d79639f755cd9e4de14593f9ceec

Message to be blinded
4400209f88bcf0128a500c218c8fbde13a21ca8eae32caa58ac9339d8c3a5eaa79489d0020
316aafb99ed1a7565e09d795a1c4bc1bc884f5069b3e3af12c61976bd929cd35

Sample Vote (4)

Blinding factor *u* : 1a35c544169b7df3cde2488f5ae6179ad3c50ea7
Blinding factor *v* : e1254df36ad334dc92e7f5c75224f2b77b179924

*r'(=tildeA * g^u * y^v)* :
8ac9e4f8917d0961a017b0706bb2cc9145161dab9b01322849ce97878ffb67d5
e'(=hash(r',msg)mod q) : 2c81051411f5826f47fa9825b579bb6eb97bf01d
e (= e'-v mod q) : 2e6c5340785edaf6347edc4523fbb296ff0b40d8

Blinded *ev(tildeC=e)* : 2e6c5340785edaf6347edc4523fbb296ff0b40d8

Message for Schnorr Sig. : 2e6c5340785edaf6347edc4523fbb296ff0b40d8
random factor *k* of Schnorr Sig. : b09bd1ea81f8f91c2ec9cc8a805b4150ced8bf37
r(=g^k mod p) :
a04164bfc61f673d77d29aae45fb503394823bbf96bb1407acdbbf2a76069313204ae1cf
8e9fc8862f3d07c27ac2f6dc529d47d5e06f2450715a1a5034c996ff

voter's sig. (s,e) of message *tildeC*
Schnorr Sig. factor *e (= hash(r,msg) mod q)* :
3b6226900a5333f29f8c0ca99b1c0c5aeee5a1c7
Schnorr Sig. factor *s (= k - e*x mod q)* : 12ed689be782fbcae8d8f823226997769fc469d0

Sample Vote (5)

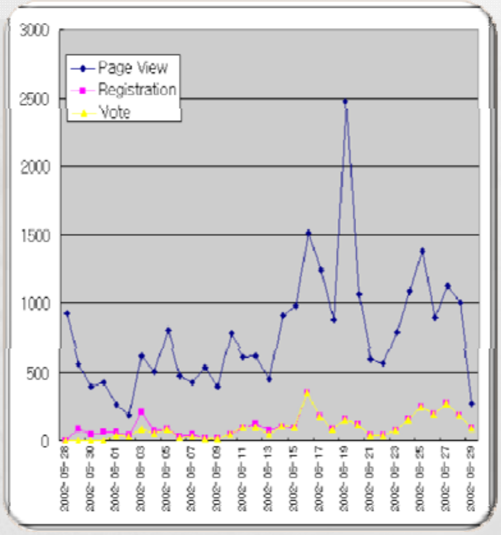
Message to admin2 (*eai=(s,e)|tildeC|tildeA*) :
8e0054001e00066b6d616e3232001490a9ab12dc8f91be844dc57575ff741f6565bab300320030002e0
502001412ed689be782fbcae8d8f823226997769fc469d000143b6226900a5333f29f8c0ca99b1c0c5ae
ee5a1c700142e6c5340785edaf6347edc4523fbb296ff0b40d8002004d4c5ff693b20ad4574a062c1eb8
0d6e2e0d79639f755cd9e4de14593f9ceec
Message from admin2, that is, admin's blind signature (*ezc*) :
53001d000561646d696e001411cc6504f02e79e6811c8046cf13ebb47d4f6e6600320030002e0502001
48bcd80bd228501354422eacf5032171ee491725000142e6c5340785edaf6347edc4523fbb296ff0b40d
8

Unblinding
Admin's blind sig. factor *s (= omega-e*x mod q)* : 8bcd80bd228501354422eacf5032171ee4917250
Admin's sig. factor *s' (= s+u mod q)* : a603460139207f291205335eab182eb9b85680f7
Admin's sig. factor *e' (= e+v)* : 2c81051411f5826f47fa9825b579bb6eb97bf01d
Unblinded admin sig.(*bs*) :
2e05020014a603460139207f291205335eab182eb9b85680f700142c81051411f5826f47fa9825b579bb
6eb97bf01d
Message to Bubo(*esev=bs||ev*)
76002e05020014a603460139207f291205335eab182eb9b85680f700142c81051411f5826f47fa9825b5
79bb6eb97bf01d004400209f88bcf0128a500c218c8fbde13a21ca8eae32caa58ac9339d8c3a5eaa79489
d0020316aafb99ed1a7565e09d795a1c4bc1bc884f5069b3e3af12c61976bd929cd35

Vote Result : 10000001431000000160

Daily Access Record

	Page View	Registration	Vote
27-May	1137	209	0
28-May	925	0	0
29-May	559	85	0
30-May	394	50	0
31-May	428	59	0
1-Jun	263	59	39
2-Jun	186	42	34
3-Jun	622	210	89
4-Jun	502	70	57
5-Jun	798	85	82
6-Jun	476	33	25
7-Jun	423	44	32
8-Jun	533	19	17
9-Jun	393	14	15
10-Jun	772	47	48
11-Jun	610	94	99
12-Jun	617	124	102
13-Jun	453	80	48
14-Jun	910	104	105
15-Jun	973	92	100
16-Jun	1508	346	346
17-Jun	1240	180	180
18-Jun	878	82	82
19-Jun	2474	154	154
20-Jun	1060	113	113
21-Jun	597	38	37
22-Jun	588	39	39
23-Jun	784	77	78
24-Jun	1086	154	155
25-Jun	1380	247	246
26-Jun	889	194	194
27-Jun	1125	270	271
28-Jun	1002	188	187
29-Jun	275	93	94
Total	26840	3695	3068



of Typical Hacking (Filtered by IDS)(1)

Type of Hacking

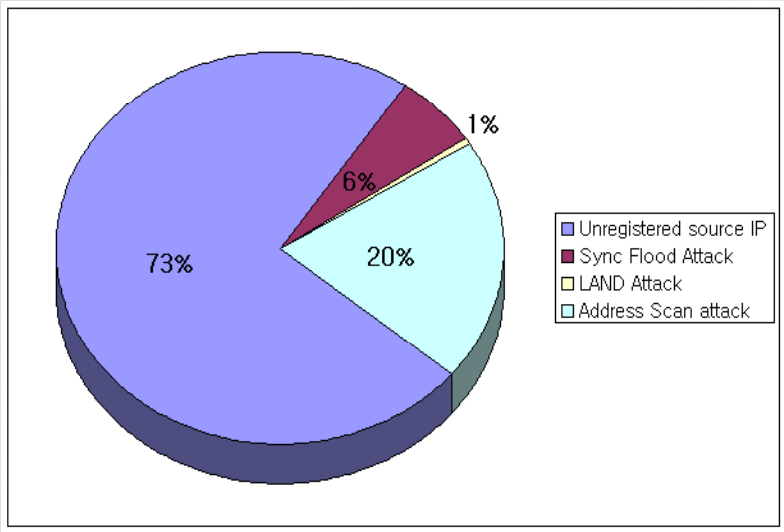
Date

	1	2	3	4	5	6	7	8	9	10	11	12	13	14
28-May	0	0	0	10	0	0	1	0	0	0	0	4	0	0
29-May	0	0	0	7	0	0	1	0	0	0	0	3	0	0
30-May	0	0	0	6	0	0	0	0	0	0	0	4	0	0
31-May	0	0	0	1	0	0	0	0	0	0	0	2	0	0
1-Jun	0	0	0	5	0	0	1	0	0	0	0	3	0	0
2-Jun	0	0	0	3	0	0	0	0	0	0	0	3	0	0
3-Jun	0	0	0	8	0	0	0	0	0	0	0	3	0	0
4-Jun	0	0	0	3	0	0	0	0	0	0	0	1	0	0
5-Jun	0	0	0	3	0	0	0	0	0	0	0	2	0	0
6-Jun	0	0	0	3	0	0	0	0	0	0	0	6	0	0
7-Jun	0	0	0	1	0	0	0	0	0	0	0	4	0	0
8-Jun	0	0	0	3	0	0	0	0	0	0	0	0	0	0
9-Jun	0	0	0	4	0	0	0	0	0	0	0	3	0	0
10-Jun	0	0	0	2	0	0	0	0	0	0	0	4	0	0
11-Jun	0	0	0	7	0	0	0	0	0	0	0	2	0	0
12-Jun	0	0	0	17	0	0	4	0	0	0	0	11	0	0
13-Jun	0	0	0	9	0	0	0	0	0	0	0	1	0	0
14-Jun	0	0	0	13	0	0	0	0	0	0	0	1	0	0
15-Jun	0	0	0	11	0	0	1	0	0	0	0	3	0	0
16-Jun	0	0	0	31	0	0	0	0	0	0	0	1	0	0
17-Jun	0	0	0	17	0	0	2	0	0	0	0	7	0	0
18-Jun	0	0	0	14	0	0	1	0	0	0	0	2	0	0
19-Jun	0	0	0	16	0	0	2	1	0	0	0	1	0	0
20-Jun	0	0	0	23	0	0	3	0	0	0	0	4	0	0
21-Jun	0	0	0	6	0	0	0	0	0	0	0	3	0	0
22-Jun	0	0	0	6	0	0	0	0	0	0	0	1	0	0
23-Jun	0	0	0	11	0	0	4	0	0	0	0	2	0	0
24-Jun	0	0	0	9	0	0	1	1	0	0	0	1	0	0
25-Jun	0	0	0	11	0	0	1	0	0	0	0	2	0	0
26-Jun	0	0	0	16	0	0	0	0	0	0	0	2	0	0
27-Jun	0	0	0	12	0	0	3	0	0	0	0	2	0	0
28-Jun	0	0	0	35	0	0	3	0	0	0	0	1	0	0
29-Jun	0	0	0	8	0	0	0	1	0	0	0	1	0	0
Total	0	0	0	331	0	0	28	3	0	0	0	90	0	0

Type of Hacking

1. Mail Bomb Attack
2. PORT Scan attack
3. Internal source IP
4. Unregistered source IP
5. Unsolicited ICMP reply
6. Inconsitent fragmentation
7. Sync Flood Attack
8. LAND attack
9. Ping of death packet
10. ICMP unreachable packet
11. Source route option
12. Address Scan attack
13. TargaNewTear Nestea attack
14. UDP flood attack

of Typical Hacking (Filtered by IDS)(2)



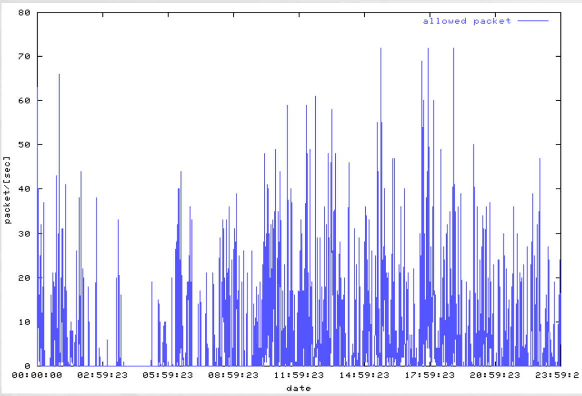
Packet Control(by Firewall)(1)

- Allowed Packet (Jun. 7th , 2002)

Allowed Rule ID	# of Allowed Packet
3	37334
5	205078
9	284195
10	0
12	2175
13	0
17	2031

Disallowed Rule ID	# of Disallowed Packet
1	79840

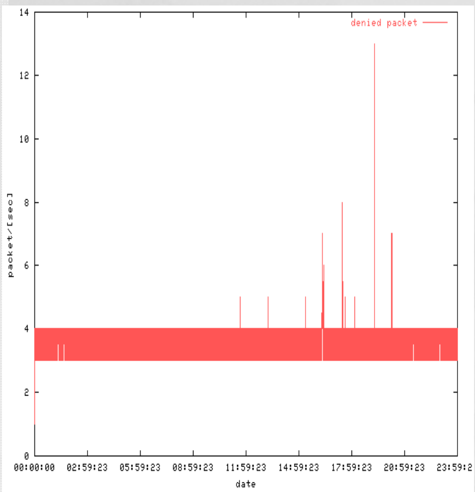
Total Packet	Allowed Packet	Disallowed Packet	Unit
610653	530813	79840	[ea]



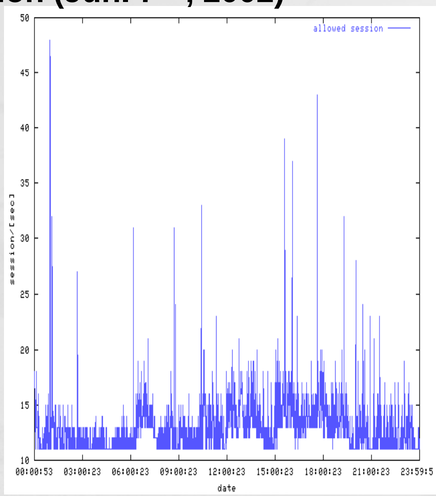
Allowed Packet

Packet Control(by Firewall) (2)

- Disallowed Packet & Session (Jun. 7th , 2002)

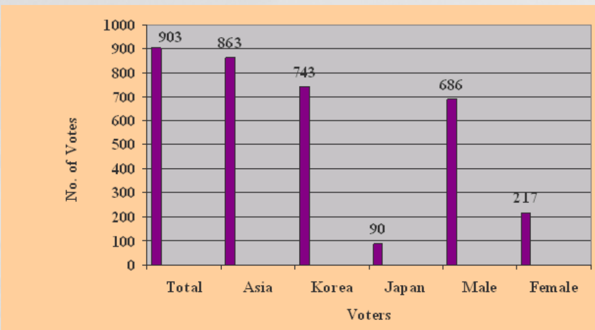


Disallowed Packet



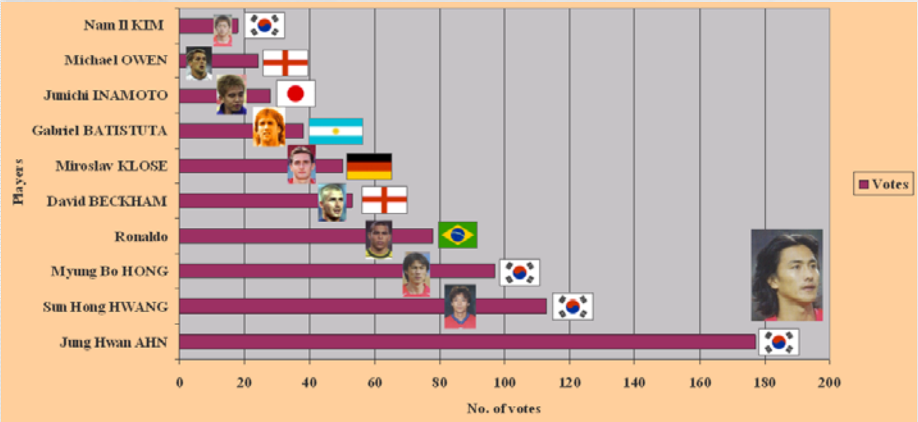
Allowed Session

Statistics of Preliminary voting



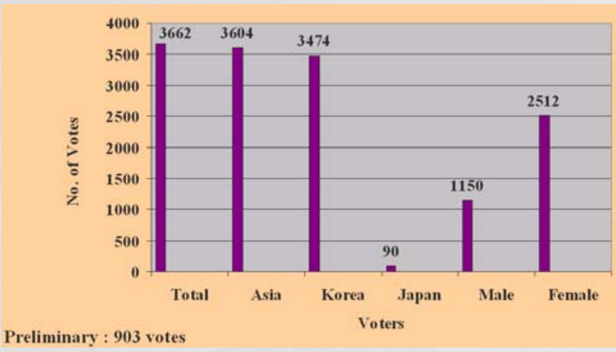
- **Age:**
  - Below 10 yrs: 9 (1.0%), 11~ 20 yrs: 200 (22.1%), 21~30 yrs: 454 (50.3%), 31~40 yrs: 176 (19.5%), 41~50 yrs: 49 (5.4%), 51~60 yrs: 7 (0.8%), Above 61 yrs: 8 (0.9%)
- **Continents:**
  - Asia: 863 (95.6%), Europe: 16 (1.8%), North America: 10 (1.1%), Oceania: 4 (0.4%), South America: 6 (0.7%), Africa: 4 (0.4%)

Top 10 MVP's after Preliminary Voting



43

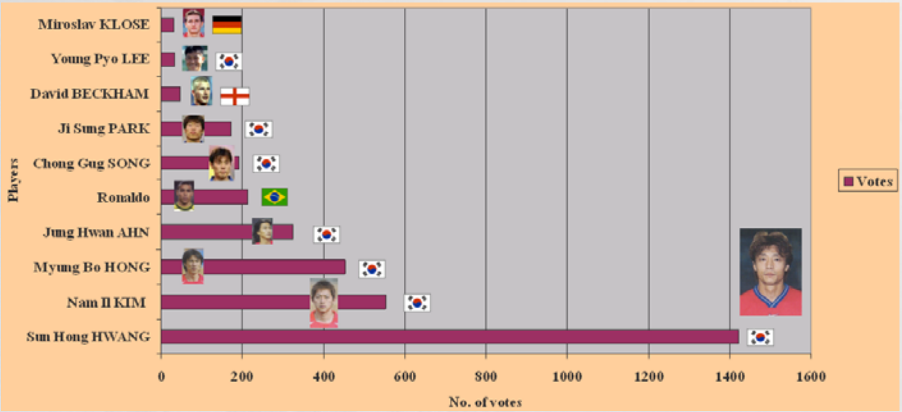
Statistics of Main Voting



- **Age:**
  - Below 10 yrs: 13 (0.4%), 11~ 20 yrs: 1,725 (47.1%), 21~30 yrs: 1,551 (42.4%), 31~40 yrs: 270 (7.4%), 41~50 yrs: 85 (2.3%), 51~60 yrs: 13 (0.4%), Above 61 yrs: 5 (0.1%)
- **Continents:**
  - Asia: 3,604 (98.4%), Europe: 23 (0.6%), North America: 20 (0.5%), Oceania: 8 (0.2%), South America: 4 (0.2%), Africa: 3 (0.1%),
- **List of nations more than 5 voters :**
  - Korea: 3,474 . Japan: 90, Vietnam: 18. China: 14, Canada: 8, USA: 7, India: 6 ,Australia: 6,France: 5,Netherlands, Brazil, Denmark, England, Germany, Russia, Peru, Taiwan, Indonesia, Finland, Spain, *etc.*

44

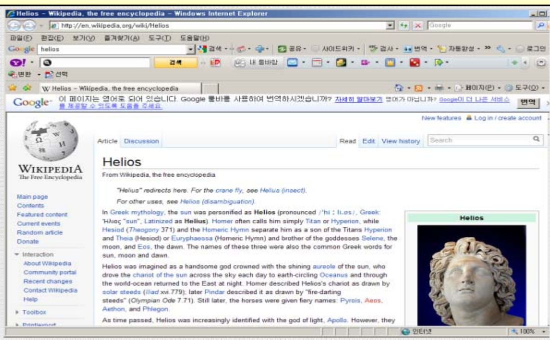
Top 10 MVP's



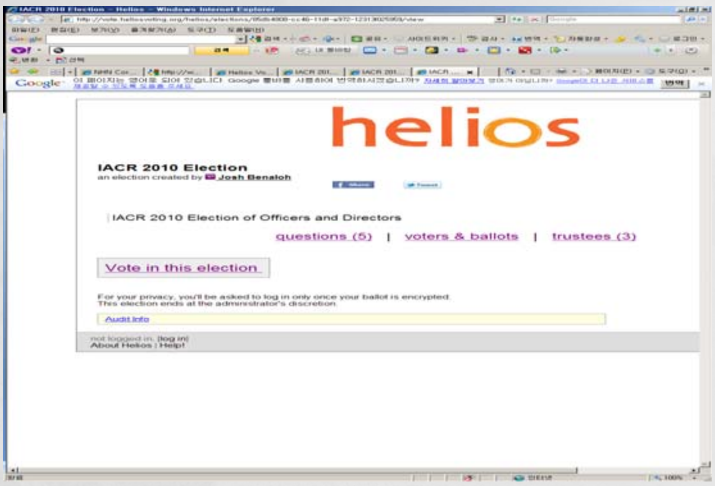
Concluding Remarks

- Lessons we learned
  - Need Performance/Security Trade-off
  - Proper anti-Hacking mechanisms due to double screening
    - Firewall (H/W) , Intrusion Detection System(S/W)
  - S/W Portability
    - Platform independent by Java
  - Impossible to meet all the security requirements
  - Multiple voting by different ID's due to weak identification
- Further Works
  - More secure and practical Internet voting system to FIFA WorldCup2006™ in Germany shared with our code
    - Against DDOS
  - Extensions
    - Strong authentication (bio-identification), Mobile Internet voting
    - Absence voting, I-polling Trial
  - Overcome Non-technical Problems(Digital Divide, Political Consensus, legal issue, *etc.*)

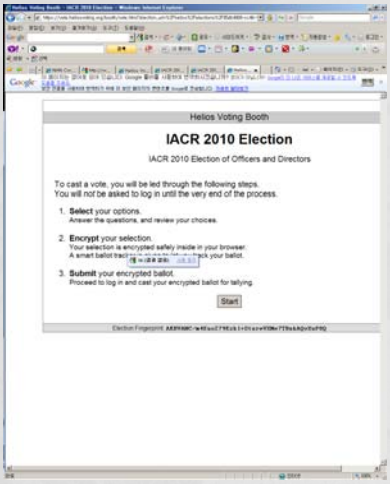
Helios

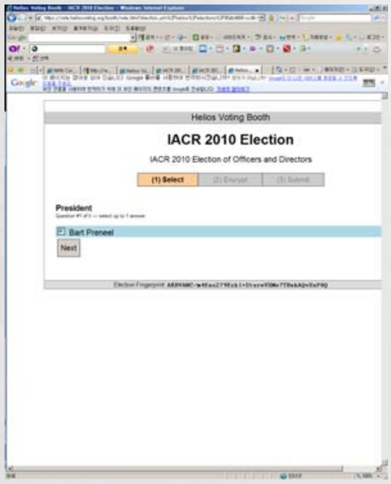


Helios for IACR2010 Election

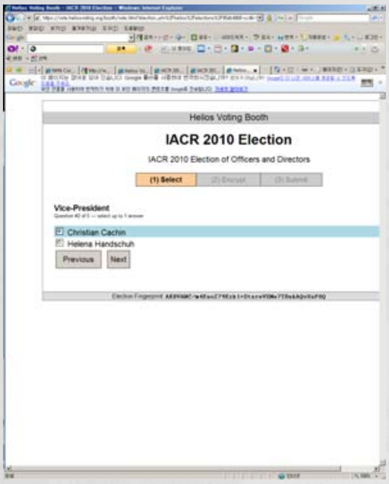


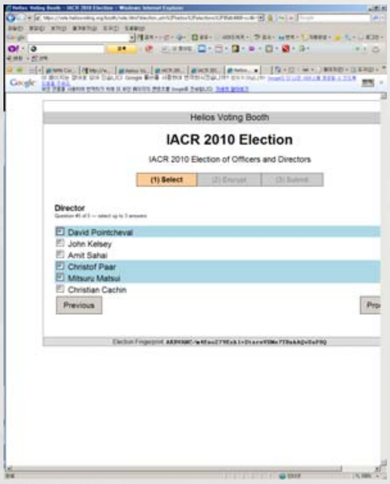
Voting after Pre-registration



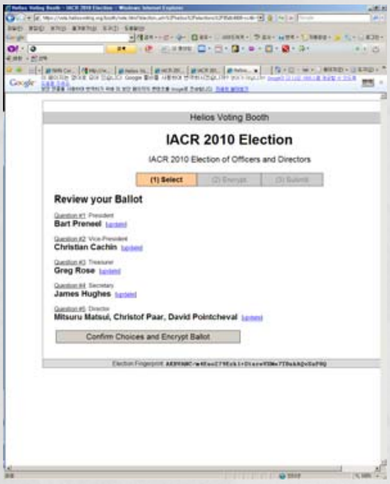


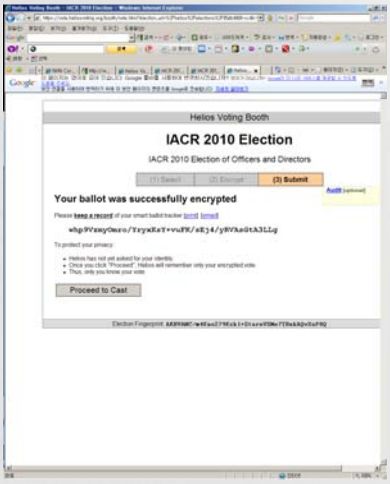
Voting





Confirmation and Encryption





Voter's Qualification and Getting Receipt