Multiparty Cryptographic Protocols

(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 $P_i$.
(Correctness) any $P_j$ can know the value of $f$.

$m$-party Cryptographic Protocol

*(Ex.)
$f() = x_1 + x_2 + ... + x_n$ or
$= x_1 \oplus x_2 \oplus ... \oplus x_n$ or
$= \max\{x_1, x_2, ..., x_n\}$
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: \[1 \ 0 \ 0 \ 1 \ 0 \ \quad 1 \ 1 \ 0 \ 0 \ 1\]

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

(w,t) Secret Sharing(I)

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

\[h(x)=a_0 +a_1x+a_2x^2+ ... +a_{t-1}x^{t-1} \mod p\]

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

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

\[h(x)=\sum_{s=1}^{t}K_i \prod_{j=1,j\neq s}^{t}(x-x_j)/(x_i-x_j) \mod p\]
(w,t) Secret Sharing (II)

(Parameters) t=3, w=5, p=17, a_0=13
(Polynomial) h(x) = \(2x^2 + 10x + 13\) mod 17
(Secret sharing) 5 shadows, K_1=h(1)=25 mod 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,

\[
h(x) = \frac{8(x-3)(x-5)}{(1-3)(1-5)} + \frac{10(x-1)(x-5)}{(3-1)(3-5)} + \frac{11(x-1)(x-3)}{(5-1)(5-3)} \mod 17
\]

\[
= \{8*\text{inv}(8,17)^* (x-3)(x-5) + 10*\text{inv}(-4,17)^* (x-1)(x-5) + 11 \mod 17
\]

\[
= 8*15(x-3)(x-5) + 10*4*(x-1)(x-5) \mod 17
\]

\[
= 19x^2 - 92x + 81 \mod 17
\]

(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
- Lipton/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
- Crepeau('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

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 \((E_B(m))\) into the deck.
(Step 2) A selects 5 cards in the deck and sends them to B. B decrypts \((D_A(E_A(m))=m)\) 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 \((E_A(E_B(m)))\) and sends them to B.
(Step 4) B decrypts 5 cards using his secret key and send \((E_A(m))\) to A
(Step 5) Using his secret key \(D_A\), A decrypts \(E_A(m)\) 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
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 \( T = x_1 + x_2 + ... + x_n \)
  - 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

- **Blind Signature**
- **Anonymous Channel**
- **r-th residue cryptosystem**
- **OT**
- **BC**
- **VSS**
- **Secret Sharing**
- **Homomorphism**
- **Fault-tolerant**
- **multi-party protocol**

Cryptographic Basics
- Cryptoalgorithms, hash ft, probabilistic encryption, RNG, Secret Sharing, ECC, ZKIP
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.

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
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

- **Registration**
  - Poll list
  - Voting office
  - Voters

- **Voting at Booth**
  - Observer/Administrator
  - Identification by poll list
  - Secret voting
  - Voting Sheet

- **Counting**
  - Tallying
  - # slip
Internet Voting

1. After setting up secure session, download registration form
2. Send encrypted public key & registration information with session key
3. Request certificate
4. Issue certificate
5. Save certificate
6. Save certificate
7. Save all decrypted ballots

Registration Stage

1. After setting up secure session
2. Download registration form
3. Fill out the registration form
4. Generate private/public key pair
5. Save private key in safe
6. Encrypt the registration information & public key with session key
7. Send encrypted message (public key & registration information)
8. Issue certificate
9. Save registration information & certificate
10. Save all decrypted ballots
Voting Stage

V1. Download voting applet
V2. Encrypt the ballot with counter's public key in ElGamal encryption
V3-1. Request Schnorr blinding factor
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
V3-2. Save Schnorr blinding factor

Counter server

DB server

Admin server

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
V5. Verify admin's blind signature
V6. Send encrypted ballot & admin's digital signature

Web servers

V3-10. Verify admin's digital signature
V7-2. Decrypt the ballot using counter's private key
V7-1. Verify admin's digital signature
V8. Save all decrypted ballots

V7. Verify admin's digital signature

Counting Stage

C1. Save all decrypted ballots
C2. Send query for tallying
C2.1. Ballot counting
C3-2. Receive the final result
C3. Post the final result

C3. Look up the final result

Voters

DB server

Web servers

Voters

DB server
Configuration of Servers (1)

http://mvp.worldcup2002.or.kr

KISTI Backbone Network
Cisco 6506/opal

Firewall SECU.Wall
Compaq Proliant ML310

L4 Switch
CSS 11800

VLAN 1

GbE

VLAN10

GbE

mvp01  mvp02  mvp03  mvp04  mvperv
SUN V880  SUN V880  SUN Enterprise 3000  SUN Enterprise 6500  Compaq

Web Servers  ADMIN Servers  DB Server

Configuration of Servers (2)
Implementation

- **Client**
  - Java 1.2, JLOCK+
  - MS Explorer 4.0 on Windows 98/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
  - Tomcat 3.1, Apache 1.3.12, JSSWEB+

- **Encryption and Certificate**
  - ElGamal encryption & Schnorr (blind) signature
  - Simplified X.509v3 certificate issued by CA server

---

Homepage([http://mvp.worldcup2002.or.kr](http://mvp.worldcup2002.or.kr))
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: 9fa840a6974fco4810db89b73461bb8d561a20bd

Security Parameters:

\[ p = \text{c16bad34d475ec5396695d694bc8bc47e598e23b5a9d7c5cec82ed5b6827d4e953784} \]
\[ q = \text{b7b810b58c0934f642878f360b96yb67dce26b53e4d} \]
\[ g = \text{4c537266d2hbb6a549d7e7319396c93a869aa275db17ba3c3ac589d7b3e003fa735f290} \]
\[ \text{e0d7a3e1f0f3515ff12af7033aaf7b6a5211a103318fb444e9718} \]

**Admin’s public key**

Public Key y: coace9838c4346b99b54e96505f9d72ba25d6764c16fb9f293cbc47402f

Security Parameters:

\[ p = \text{f668a94f0ce284e0ce284e30776b59b31efc12ba069d1055649fe2bdoeb42f} \]
\[ q = \text{e3109ecfd13e8d676c39e6coabe9dfcoae69df} \]
\[ g = \text{a7688634018f161c62de5014ca99e83759fbaf67b757b54b51d32392177a40} \]
Sample Vote (2)

Counter's public key

Public Key $y$: b6fbabc9259a1267fde3a82e6b067581e040db7ca4e07837fb86b1054207fb

Security Parameters:

- $p$: e2043679a6b62fe446b62fe440c0bfe0122398d982b6a6b1093962b94d502d21
- $q$: ad9c0a5de1d2224400a47599d24de66b0ddad67
- $g$: 3294730de55ef79b94f9684140166e610dbdd3eb7d090aecdbef310411

Message from Admin1 ($\tilde{A}$):

Vote: 0000001431000000160
Tag: 4277bb955f69f86

Encoded vote ($vi$): 3130303030303134333103030303136304277bb955f69f86

Message for ElGamal encryption:

Random number $k$ for ElGamal encryption:

G($y^k$ mod $p$): 316aafb99ed1a7565e09d795a4c4bcb884f5069b3e3af12e61976bd929cd35
M($m(y^k)$ mod $p$): 9f88bcf0128500c218c8f88bde13a21ca8ae432ca458a933998e3a5eaa79489d

Encrypted $vi$($ev$):

440020988bcf0128500c218c8f88bde13a21ca8ae432ca458a933998e3a5eaa79489d0d020316afbb959d1e7665e09d795a4c4bcb884f5069b3e3af12e61976bd929cd35

Blinding encrypted $vi$

Random commitment $\tilde{A}$ for blinding given by signer

440c5f693b20aad4574a0621eb80d6e20ed79639f755cd9e4de14593f69f86

Message to be blinded:

440020988bcf0128500c218c8f88bde13a21ca8ae432ca458a933998e3a5eaa79489d0d020316afbb959d1e7665e09d795a4c4bcb884f5069b3e3af12e61976bd929cd35

Sample Vote (3)

Random number $k$ for ElGamal encryption:

G($y^k$ mod $p$): 316aafb99ed1a7565e09d795a4c4bcb884f5069b3e3af12e61976bd929cd35
M($m(y^k)$ mod $p$): 9f88bcf0128500c218c8f88bde13a21ca8ae432ca458a933998e3a5eaa79489d

Encrypted $vi$($ev$):

440020988bcf0128500c218c8f88bde13a21ca8ae432ca458a933998e3a5eaa79489d0d020316afbb959d1e7665e09d795a4c4bcb884f5069b3e3af12e61976bd929cd35

Blinding encrypted $vi$

Random commitment $\tilde{A}$ for blinding given by signer

440c5f693b20aad4574a0621eb80d6e20ed79639f755cd9e4de14593f69f86

Message to be blinded:

440020988bcf0128500c218c8f88bde13a21ca8ae432ca458a933998e3a5eaa79489d0d020316afbb959d1e7665e09d795a4c4bcb884f5069b3e3af12e61976bd929cd35
Sample Vote (4)

Blinding factor \( u \): 1a35c441697df3cde24885a6179ad3c50ea7
Blinding factor \( v \): e1b254df36ad3344d92e75c752242f0977b717992

\[ r'(=\tilde{A}^u g^u y^v) \]
\[ e'(=\text{hash}(r',\text{msg}) \mod q) \]
\[ e (= e'-v \mod q) \]

Blinded ev(\(\tilde{t}l.d.C=e\)):

Message for Schnorr Sig.: 2e6c534078edaf0f47edc4523fbb296f0f40d8
random factor \( k \) of Schnorr Sig.: b09bd1ea81f8f91c2ec9cc8a05b4150ced8b537
\[ r(=g^k \mod p) \]
\[ e (= \text{hash}(r,\text{msg}) \mod q) \]
\[ s (= k - e*x \mod q) \]

Message to admin2 (\(eai=(s,e)|\tilde{t}l.d.A\)):

Unblinding
Admin's blind sig. factor \( s (= \omega-e*x \mod q) \):
Admin's sig. factor \( e (= e'-v \mod q) \):
Message to Bubo (\(esev=bs||ev\)):

Vote Result: 10000001431000000160

Sample Vote (5)

Message to admin3 (\(eai=(s,e)|\tilde{t}l.d.C|\tilde{t}l.d.A\)):

Unblinding
Admin's blind sig. factor \( s (= \omega-e*x \mod q) \):
Admin's sig. factor \( e (= e'-v \mod q) \):
Message to Bubo (\(esev=bs||ev\)):

Vote Result: 10000001431000000160
Daily Access Record

<table>
<thead>
<tr>
<th>Date</th>
<th>Value1</th>
<th>Value2</th>
<th>Value3</th>
</tr>
</thead>
<tbody>
<tr>
<td>27-May</td>
<td>11521</td>
<td>829</td>
<td>58</td>
</tr>
<tr>
<td>28-May</td>
<td>954</td>
<td>80</td>
<td>0</td>
</tr>
<tr>
<td>29-May</td>
<td>592</td>
<td>60</td>
<td>0</td>
</tr>
<tr>
<td>30-May</td>
<td>524</td>
<td>50</td>
<td>0</td>
</tr>
<tr>
<td>31-May</td>
<td>448</td>
<td>50</td>
<td>0</td>
</tr>
<tr>
<td>1-Jun</td>
<td>202</td>
<td>59</td>
<td>34</td>
</tr>
<tr>
<td>2-Jun</td>
<td>190</td>
<td>40</td>
<td>16</td>
</tr>
<tr>
<td>3-Jun</td>
<td>665</td>
<td>210</td>
<td>30</td>
</tr>
<tr>
<td>4-Jun</td>
<td>302</td>
<td>70</td>
<td>52</td>
</tr>
<tr>
<td>5-Jun</td>
<td>198</td>
<td>165</td>
<td>152</td>
</tr>
<tr>
<td>6-Jun</td>
<td>476</td>
<td>22</td>
<td>20</td>
</tr>
<tr>
<td>7-Jun</td>
<td>622</td>
<td>38</td>
<td>32</td>
</tr>
<tr>
<td>8-Jun</td>
<td>453</td>
<td>10</td>
<td>17</td>
</tr>
<tr>
<td>9-Jun</td>
<td>304</td>
<td>45</td>
<td>49</td>
</tr>
<tr>
<td>10-Jun</td>
<td>77</td>
<td>41</td>
<td>69</td>
</tr>
<tr>
<td>11-Jun</td>
<td>707</td>
<td>34</td>
<td>309</td>
</tr>
<tr>
<td>12-Jun</td>
<td>117</td>
<td>172</td>
<td>101</td>
</tr>
<tr>
<td>13-Jun</td>
<td>453</td>
<td>20</td>
<td>43</td>
</tr>
<tr>
<td>14-Jun</td>
<td>525</td>
<td>104</td>
<td>103</td>
</tr>
<tr>
<td>15-Jun</td>
<td>897</td>
<td>95</td>
<td>100</td>
</tr>
<tr>
<td>16-Jun</td>
<td>506</td>
<td>340</td>
<td>885</td>
</tr>
<tr>
<td>17-Jun</td>
<td>1765</td>
<td>782</td>
<td>782</td>
</tr>
<tr>
<td>18-Jun</td>
<td>748</td>
<td>87</td>
<td>87</td>
</tr>
<tr>
<td>19-Jun</td>
<td>648</td>
<td>66</td>
<td>66</td>
</tr>
<tr>
<td>20-Jun</td>
<td>795</td>
<td>77</td>
<td>77</td>
</tr>
<tr>
<td>21-Jun</td>
<td>1400</td>
<td>115</td>
<td>101</td>
</tr>
<tr>
<td>22-Jun</td>
<td>1347</td>
<td>247</td>
<td>256</td>
</tr>
<tr>
<td>23-Jun</td>
<td>1250</td>
<td>132</td>
<td>105</td>
</tr>
<tr>
<td>24-Jun</td>
<td>1107</td>
<td>270</td>
<td>273</td>
</tr>
<tr>
<td>25-Jun</td>
<td>1001</td>
<td>194</td>
<td>151</td>
</tr>
<tr>
<td>26-Jun</td>
<td>785</td>
<td>93</td>
<td>94</td>
</tr>
<tr>
<td>Total</td>
<td>25.680</td>
<td>55.985</td>
<td>30.69</td>
</tr>
</tbody>
</table>

# of Typical Hacking (Filtered by IDS)(1)

<table>
<thead>
<tr>
<th>Type of Hacking</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
<th>14</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# of Typical Hacking (Filtered by IDS)(2)

- 73%
- 20%
- 6%
- 1%

Packet Control(by Firewall)(1)

- Allowed Packet (Jun. 7th, 2002)

<table>
<thead>
<tr>
<th>Allowed Rule ID</th>
<th># of Allowed Packet</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>37234</td>
</tr>
<tr>
<td>5</td>
<td>25371</td>
</tr>
<tr>
<td>9</td>
<td>284195</td>
</tr>
<tr>
<td>10</td>
<td>0</td>
</tr>
<tr>
<td>12</td>
<td>2515</td>
</tr>
<tr>
<td>13</td>
<td>0</td>
</tr>
<tr>
<td>17</td>
<td>2034</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Disallowed Rule ID</th>
<th># of Disallowed Packet</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>79840</td>
</tr>
</tbody>
</table>

Total Packet | Allowed Packet | Disallowed Packet | Unit |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>610853</td>
<td>530813</td>
<td>79840</td>
<td>[req]</td>
</tr>
</tbody>
</table>

Allowed Packet
Packet Control (by Firewall) (2)

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

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

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 (0.1%), Africa: 3 (0.1%)

- **List of nations more than 5 voters:**
  - Korea: 3,612, Japan: 90, Vietnam: 18, China: 14, Canada: 8, USA: 7, India: 6, Australia: 6, France: 5, Netherlands: 3, Brazil: 3, Denmark: 3, England: 3, Germany: 3, Russia: 3, Taiwan: 3, Indonesia: 3, Finland: 3, Spain: 3, etc.
Top 10 MVP’s

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 for IACR2010 Election
Voting after Pre-registration

Voting
Confirmation and Encryption

Voter’s Qualification and Getting Receipt