

Votopia will be continued...

1st Secure Internet Voting System
over the world

*To Choose the Most Valuable Player and the Best Goalkeeper
in 2002 FIFA World Cup Korea/JapanTM*

Kwangjo Kim

International Research Center for Information Security
Information and Communications Univ.

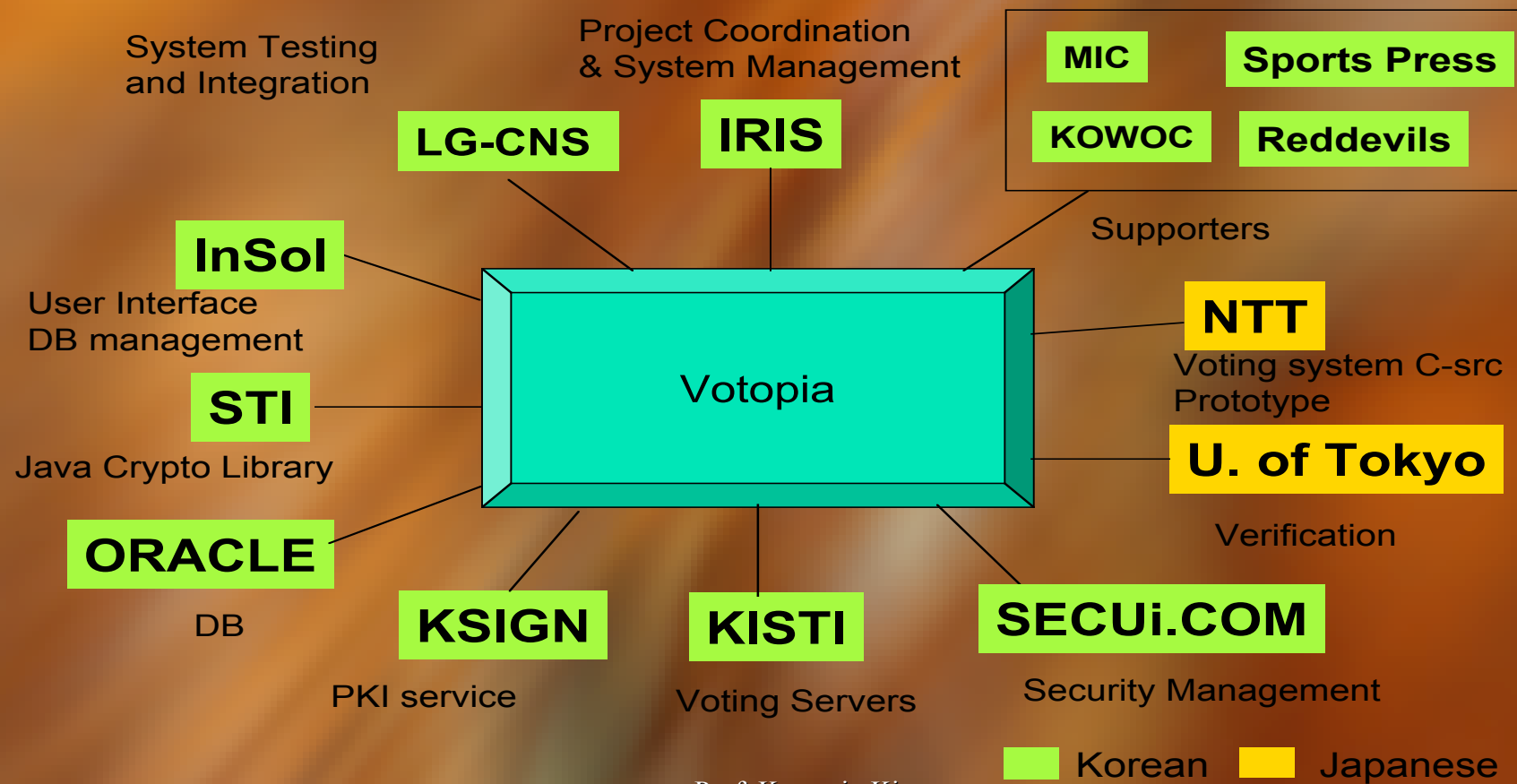


Prof. Kwangjo Kim
Votopia – A Secure Internet Voting System - © IRIS



Introduction

- » A project carried out by effective collaboration among some of the prominent Korean and Japanese IT firms and research institutes



Contributors

- ▶▶ **IRIS** : Kwangjo Kim, Byoungcheon Lee, Jinho Kim, Myoungsun Kim, Hyunrok Lee, Jaegwan Park, Manho Lee, Wooseok Ham, Jongseung Kim, Hyunggi Choi, Kyuseok Ham, Kukhwan Ahn, Vo Duc Liem, Xie Yan, Fangguo Zhang, etc
- ▶▶ **LG CNS** : Daehun Kim, Seung Pil Hong, Minhyung Kim, Jongyoon Choi
- ▶▶ **Insolsoft** : Sunjoo, Hyun, Mina Jung, Junghan Kim, YongJae Lee
- ▶▶ **KSIGN** : Ki-Yoong Hong, Jadong Ku, Eunsong Lee, Jinsoo Lim, Daesung Ku
- ▶▶ **STI** : Donnie Choi, Daeha Park, Seoungho Heo, Jung Cheol Yoon,
- ▶▶ **KISTI** : Younghwa Cho, Jungkwon Kim, Jun Woo, Okhwan Byun
- ▶▶ **SECUI.COM** : Kyongsoo Oh, Moonseok Seo, Wonkeun Hur, Hyunwon Ko
- ▶▶ **MIC** : Hyun Lee, Ee-Hwan Hwang
- ▶▶ **Korean Press** (Digital Times, Daily Econimics), Reddevils
- ▶▶ **U. of Tokyo** : Hideki Imai, Kazuguni Kobara
- ▶▶ **NTT** : Tatsuaki Okamoto, Atsushi Fujioka, Masayuki Abe, Koutarou Suzuki
- ▶▶ **ORACLE, SUN**

Cryptographic Req't

►► Basic

- ✓ 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

►► Advanced

- ✓ Walk-away : The voter need not to make any action after voting
- ✓ Robustness : The voting system should be successful regardless of partial failure of the system
- ✓ Universal verifiability : Anyone can verify the validity of vote
- ✓ Receipt-freeness : Voter should not be able to prove his or her vote to a buyer. (Voter does not have any receipt for the vote)

Security & Performance Req't

►► Server side

- Network and computer security
 - Anti-hacking such as DDOS attack, *etc*
- Large DB handling
- Fault-tolerance and high reliability
- Reasonable processing when registering and voting

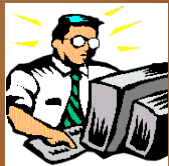
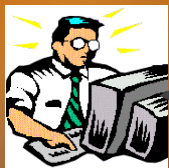
►► Client side

- Fast and easy, user-friendly web interface
- No tamper-proof device provided
- Various kinds of platforms, OS and browsers
- Keep the privacy of all voters at maximum

System Configuration

<http://mvp.worldcup2002.or.kr>

Voters



Internet

Firewall

G/100M

L4 SW

CA Server

SUN 6500 / 3000 SUN 880*2

Clustered Web Servers

**Admin Server
SUN 6500**

**DB Server
COMPAQ ES40**

**Counter Server
(COMPAQ ES40)**

Prof. Kwangjo Kim

Votopia – A Secure Internet Voting System - © IRIS

Implementation

▶▶ Client

- Java1.2, JLOCK+
- MS Explorer 4.0 on Windows98 /ME/XP/2000
- Korean, Japanese, English and Chinese

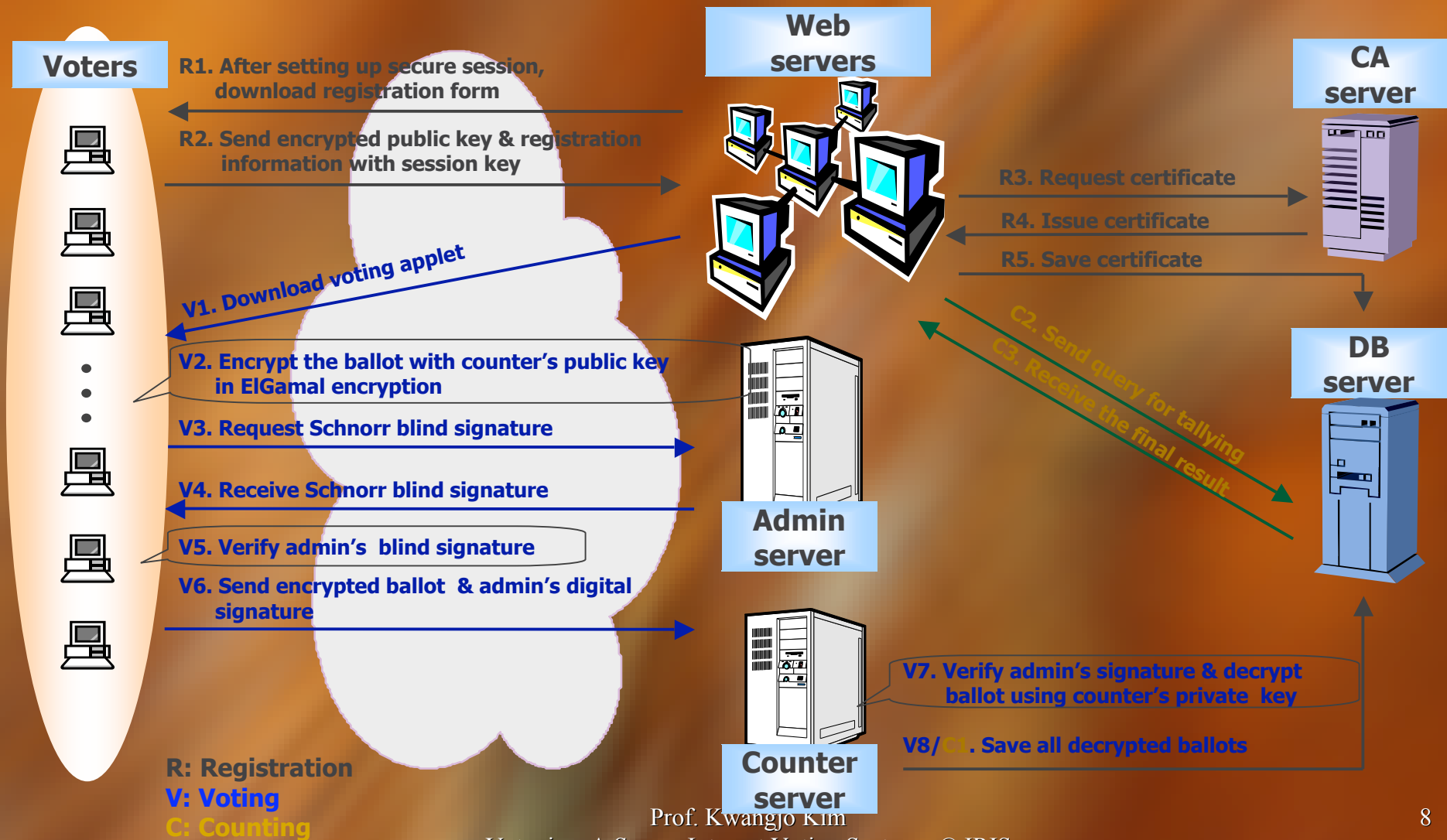
▶▶ Web, DB, Admin, and Counter Servers

- » Solaris 2.5.4 (SUN OS 5.8), Oracle DB 8.0.6 , JDBC
- » Tomcat3.1, Apache1.3.12, JSSWEB+

▶▶ Encryption and Certificate

- 512 bit ElGamal encryption and Schnorr (blind) signature
- Simplified X.509v3 certificate issued by CA server

Flow of 3 main stages



Home Page

(<http://mvp.worldcup2002.or.kr>)

The screenshot shows the homepage of the VOTOPIA voting system. The header features the text "Choose MVP 2002 FIFA World Cup Korea - Japan" and "Voting system" with a logo of a soccer ball. Below the header is a navigation bar with "Overview", "Organizations", and "Structure". On the left is a vertical menu with "INTRODUCTION", "VOTE" (highlighted with a mouse cursor), "About World Cup", "STATISTICS", "RESULT", "Q&A", "LINK", and "SITEMAP". At the bottom of the menu, it says "Today : 6" and "Total : 1689". The main content area has three sections: "Schedule" with voting periods and announcements, "Client Environments" with system requirements, and "Motivation" with reasons for the system. A map of Korea and Japan is on the right.

VOTOPIA

Choose MVP
2002 FIFA World Cup Korea - Japan™

Voting system

Overview Organizations Structure

INTRODUCTION
VOTE
About World Cup
STATISTICS
RESULT
Q&A
LINK
SITEMAP

Today : 6
Total : 1689

>> Schedule

- Select MVP and best Goal Keeper through the Internet
- Preliminary Voting
 - Period: Jun. 1 ~ 10, 2002
 - Announcement: Jun. 15, 2002
- Final Voting
 - Period: Jun. 16 ~ 26, 2002
 - Announcement: Jun. 30, 2002

>> Client Environments


- At least MS Windows 98 and MS Explorer 4.0 or higher

>> Motivation

- To celebrate the joint hosting of "2002 FIFA World Cup Korea/Japan (TM)" and to support this international festival by the volunteering parties from two hosting countries.
- To demonstrate that Korea/Japan are proud of having established the top-level IT infrastructure and to promulgate new cyber service to the world.
- To serve the first secure Internet voting that features the similar functionalities of the manual voting system to all the netizens all over


Korea Japan

Registration



[INTRODUCTION](#)[VOTE](#)[About World Cup](#)[STATISTICS](#)[RESULT](#)[Q&A](#)[LINK](#)[SITEMAP](#)

Today : 6
Total : 1689



Voting system

[Registration](#)[Vote](#)[Voting Procedure](#)

[Registration](#)

[Warning] For the registration and vote,
you must click **"Yes"** in the popping-up window.

ID(*)	<input type="text"/>	<input type="button" value="Check"/>
(4~10 English characters or numbers)		
Password (*)	<input type="text"/>	(within 4~8 characters)
Re-type Password(*)	<input type="text"/>	
Name	<input type="text"/>	
E-mail(*)	<input type="text"/>	
(Please give your correct e-mail address for further correspondence.)		
Country(*)	<input type="text"/>	
Gender(*)	<input type="text"/>	
Age(*)	<input type="text"/>	

(*) : Mandatory field

Voting

The screenshot shows the VOTOPIA voting interface for the 2002 FIFA World Cup Korea - Japan MVP. The header features the VOTOPIA logo, navigation links (Update Your Info., Registered Voter, Voting Procedure), and the title "Choose MVP 2002 FIFA World Cup Korea - Japan". A sidebar on the left contains links: INTRODUCTION, VOTE (highlighted), About World Cup, STATISTICS, RESULT, Q&A, LINK, and SITEMAP. The main content area displays a warning message, a voting form with dropdown menus for Country and Player, a "Process of voting" section, and "Ballot Casting" and "Log-out" buttons. The footer includes the copyright notice: Copyright(C) 2002 IRIS All rights Reserved.

Choose MVP
2002 FIFA World Cup Korea - Japan™

Voting system

Update Your Info. Registered Voter Voting Procedure

>> **Vote**

[Warning] For the registration and vote, you must click **"Yes"** in the popping-up window.

The period of preliminary voting.

	Country	Player
MVP	<input type="text"/>	<input type="text"/>
Best Goalkeeper	<input type="text"/>	<input type="text"/>

Process of voting

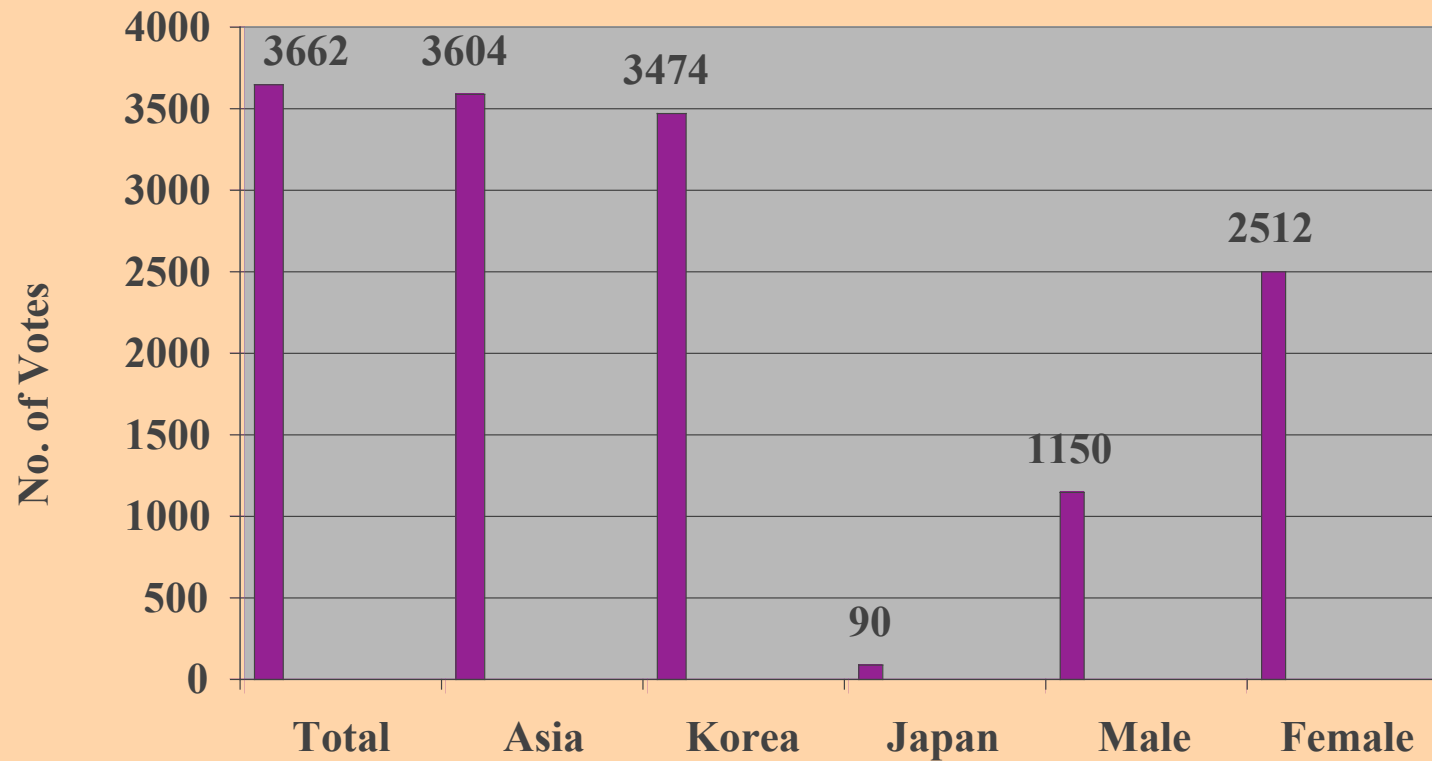
Ballot Casting

Log-out

Copyright(C) 2002 IRIS All rights Reserved.

**This page is for "vote-now". In case of "vote-later", you must give ID and passwd.*

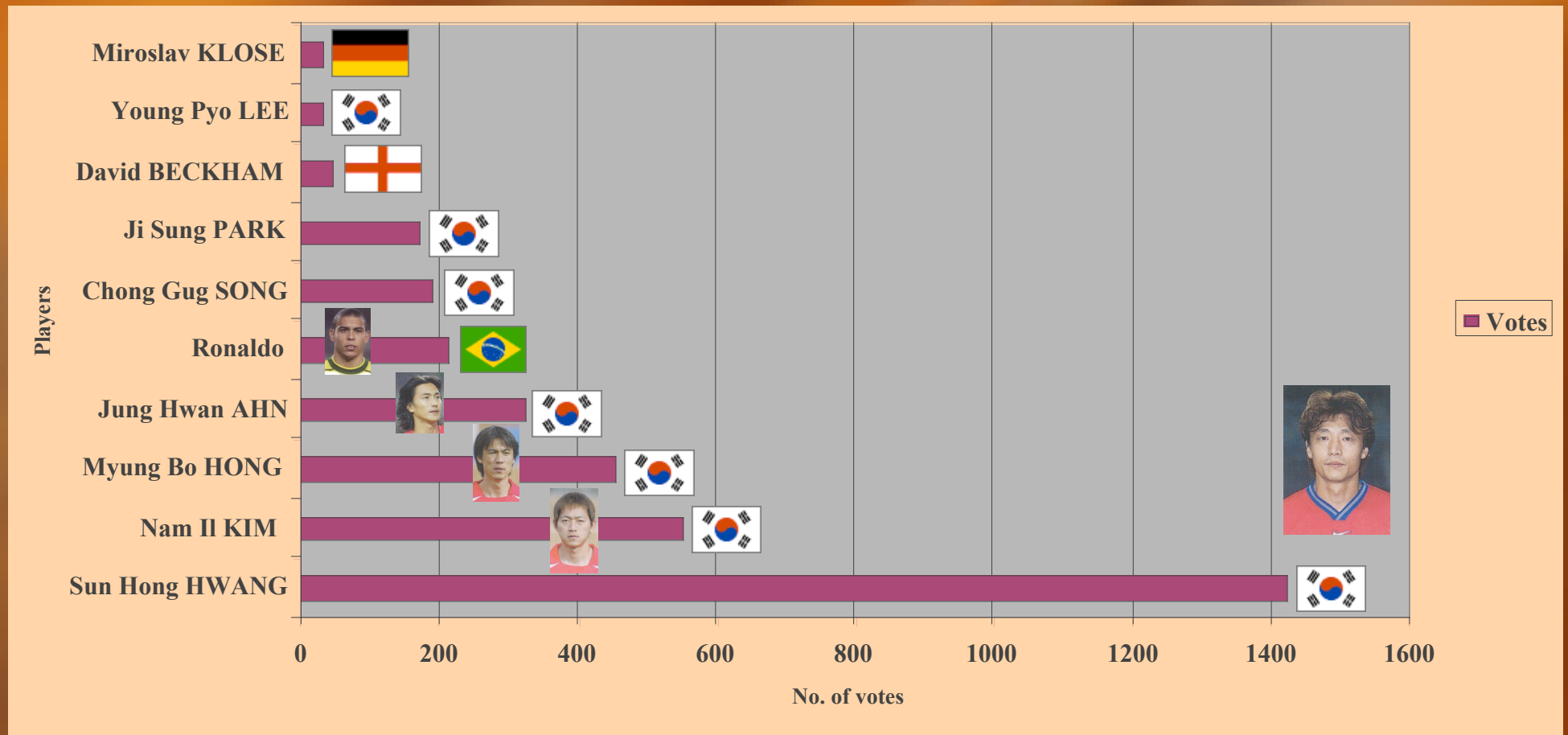
Statistics of main voting



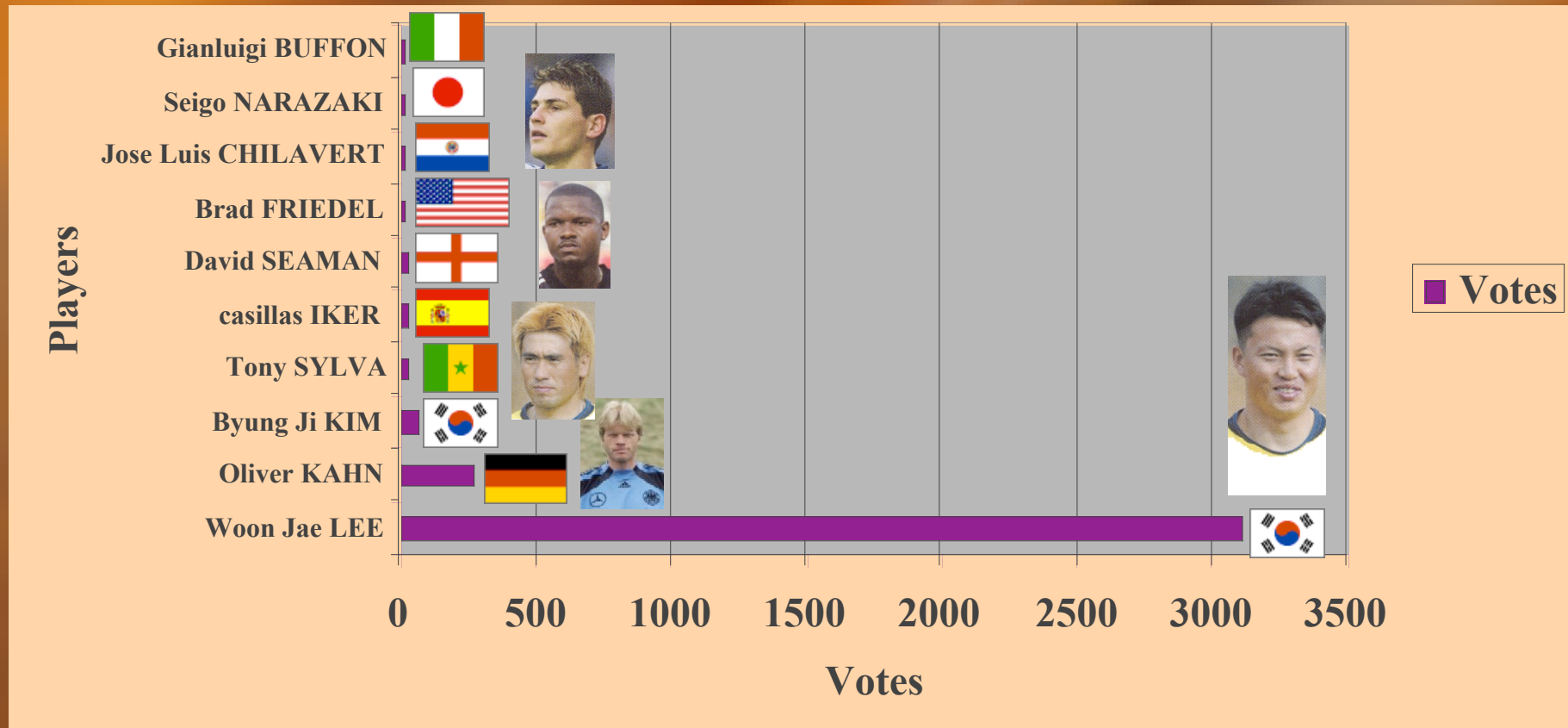
Preliminary : 903 votes

Voters

Top 10 MVP's



Top 10 Best Goalkeepers



Other Details

▶▶ 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.*

Highlights

- ▶▶ Registered netizen can cast his vote any where, any time
 - » Explorer 4.0 or higher on Windows 98/ME/2000/XP
 - » Min. 56 Kb/s Internet Speed
 - » Minimized personal information by ID/pwd identification
- ▶▶ Web Site Access
 - » About 100 votes and 1,000 hits in a day
- ▶▶ S/W Portability
 - » Platform independent by Java
- ▶▶ Double anti-hacking mechanism
 - » Firewall (H/W)
 - » Intrusion Detection System (S/W)

Concluding Remarks

▶▶ Successful Internet Voting

- ▶ Acceptable Performance on Client side
- ▶ Comfortable User Interface
- ▶ System Configuration and Daily Auditing

▶▶ Best practice of “*cryptography everywhere*” in 2002

- ▶ It works good but need some time for practical application depending on a number of factors.

▶▶ Further Works

- ▶ Authentication (bio-identification), Mobile Internet voting
- ▶ Trial voting for small society (e.g., IACR’s annual voting)
- ▶ Real voting replacements in isolated areas when natural disaster (e.g., heavy rain) happens.