Short, Undeniable Signatures for Android 2.x

Master Semester Project

Sebastien Duc

EPFL

June 15, 2012

Outline

Outline

Outline

Outline

Outline

Introduction (1)

Introduction (1)

- MOVA is an undeniable signature scheme.

Introduction (1)

- MOVA is an undeniable signature scheme.
- It can achieve very small signatures.

Introduction (1)

- MOVA is an undeniable signature scheme.
- It can achieve very small signatures.
- Shortness of signatures is very convenient in mobile applications.

Introduction (1)

- MOVA is an undeniable signature scheme.
- It can achieve very small signatures.
- Shortness of signatures is very convenient in mobile applications.
- The aim of the project was to design an application for Android using MOVA.

Introduction (2)

Introduction (2)

- Today there exists a lot of application for classical signatures.

Introduction (2)

- Today there exists a lot of application for classical signatures.
- It is not the case for undeniable signatures (and MOVA).

Introduction (2)

- Today there exists a lot of application for classical signatures.
- It is not the case for undeniable signatures (and MOVA).
- We tried to find an application where undeniable signatures can bring something.

Outline

Outline

Specifications

Specifications

- Undeniable Signatures are not universally verifiable.

Specifications

- Undeniable Signatures are not universally verifiable.
- The verifier must run an interactive protocol with the signer

Definition

Consider two participants S and V.
We define

Definition

Consider two participants S and V.
We define

Setup $(k_p^S, k_s^S) \leftarrow \mathrm{Setup}^S(1^n)$ and
$(k_p^V, k_s^V) \leftarrow \mathrm{Setup}^V(1^n)$.

Definition

Consider two participants S and V.
We define

Setup $(k_p^S, k_s^S) \leftarrow \mathrm{Setup}^S(1^n)$ and
$(k_p^V, k_s^V) \leftarrow \mathrm{Setup}^V(1^n)$.

Sign $\sigma \leftarrow \mathrm{Sign}(m, k_s^S)$

Definition

Consider two participants S and V.
We define

Setup $(k_p^S, k_s^S) \leftarrow \mathrm{Setup}^S(1^n)$ and
$(k_p^V, k_s^V) \leftarrow \mathrm{Setup}^V(1^n)$.

Sign $\sigma \leftarrow \mathrm{Sign}(m, k_s^S)$

Confirm Interactive protocol between S and V to confirm the validity of (m, σ).

Definition

Consider two participants S and V.
We define

Setup $(k_p^S, k_s^S) \leftarrow \mathrm{Setup}^S(1^n)$ and
$(k_p^V, k_s^V) \leftarrow \mathrm{Setup}^V(1^n)$.

Sign $\sigma \leftarrow \mathrm{Sign}(m, k_s^S)$

Confirm Interactive protocol between S and V to confirm the validity of (m, σ).

Deny Interactive protocol between S and V to deny the validity of (m, σ').

Outline

MOVA Signature Scheme

MOVA Signature Scheme

- MOVA is a scheme for undeniable, short signatures.

MOVA Signature Scheme

- MOVA is a scheme for undeniable, short signatures.
- Provides batch verification.

MOVA Signature Scheme

- MOVA is a scheme for undeniable, short signatures.
- Provides batch verification.
- Scheme based on group homomorphism.

Setup

Consider a pseudo-random generator $GenK$.

Setup

Consider a pseudo-random generator $GenK$.

1. choose two groups G, H.
2. choose a homomorphism $h : G \to H$
3. Generate $Xkeys \leftarrow GenK(seedK)$, $Xkeys \in G^{Lkey}$.
4. Compute $Ykeys = h^{Lkey}(Xkeys)$.

Setup

Consider a pseudo-random generator $GenK$.

1. choose two groups G, H.
2. choose a homomorphism $h : G \to H$
3. Generate $Xkeys \leftarrow GenK(seedK)$, $Xkeys \in G^{Lkey}$.
4. Compute $Ykeys = h^{Lkey}(Xkeys)$.

Public key: $(G, H, |H|, seedK, Ykeys)$
Secret key: h

Signature

Consider a message $m \in \{0,1\}^*$ and the pseudo-random generator $GenS$.

Signature

Consider a message $m \in \{0,1\}^*$ and the pseudo-random generator $GenS$.

1. Generate $Xsigs \leftarrow GenS(m)$, where $Xsigs \in G^{Lsig}$
2. Compute $Ysigs = h^{Lsig}(Xsigs)$.

Signature

Consider a message $m \in \{0,1\}^*$ and the pseudo-random generator $GenS$.

1. Generate $Xsigs \leftarrow GenS(m)$, where $Xsigs \in G^{Lsig}$
2. Compute $Ysigs = h^{Lsig}(Xsigs)$.

Signature: $Ysigs$

Group Interpolation

Definition

We say the $S \subseteq G \times H$ interpolates in a group homomorphism if $\exists$ a homomorphism h st. $h(x) = y \ \forall (x, y) \in S$.

Note: In MOVA we consider sets S that interpolates in a unique group homomorphism.

Verification

The verification is an interactive protocol between S and V.

Verification

The verification is an interactive protocol between S and V.

The prover convinces the verifier that

$$\{(Xkey_i, Ykey_i) | i = 1, ..., Lkey\} \cup \{(Xsig_i, Ysig_i) | i = 1, ..., Lsig\}$$

interpolates in a group homomorphism.

Batch Verification

Batch Verification

- Used to verify multiple signature.

Batch Verification

- Used to verify multiple signature.
- Signatures must be issued from same key pair.

Batch Verification

- Used to verify multiple signature.
- Signatures must be issued from same key pair.
- Verify all the signatures in only one protocol call.

Outline

Motivation

Motivation

- The application is a University Contest

Motivation

- The application is a University Contest
- The concept is similar to the University Challenge in the UK, but using phones.

Outline

Overview (1)

Overview (1)

- Universities are providing quizzes to teams in other universities.

Overview (1)

- Universities are providing quizzes to teams in other universities.
- Teams win points by answering quizzes correctly and this increased the final score of their university.

Overview (1)

- Universities are providing quizzes to teams in other universities.
- Teams win points by answering quizzes correctly and this increased the final score of their university.
- The university with the highest score wins the contest.

Overview (2)

Overview (2)

- Quizzes are uniquely assigned to the teams.

Overview (2)

- Quizzes are uniquely assigned to the teams.
- When subscribing, teams choose a password for future authentication.

Overview (2)

- Quizzes are uniquely assigned to the teams.
- When subscribing, teams choose a password for future authentication.
- Quizzes can contain normal or multiple choice questions.

Overview (2)

- Quizzes are uniquely assigned to the teams.
- When subscribing, teams choose a password for future authentication.
- Quizzes can contain normal or multiple choice questions.
- Correction and scoring is done manually by the server manager.

Setup

Consider two universities U_1, U_2 and a team T_i in university U_2.

Setup

Consider two universities U_1, U_2 and a team T_i in university U_2.

1. Server S_1 of U_1 provides quizzes to T_i with a MOVA signature.

Setup

Consider two universities U_1, U_2 and a team T_i in university U_2.

1. Server S_1 of U_1 provides quizzes to T_i with a MOVA signature.
2. When filled-in, the quiz is sent to server S_2 of U_2.

Setup

Consider two universities U_1, U_2 and a team T_i in university U_2.

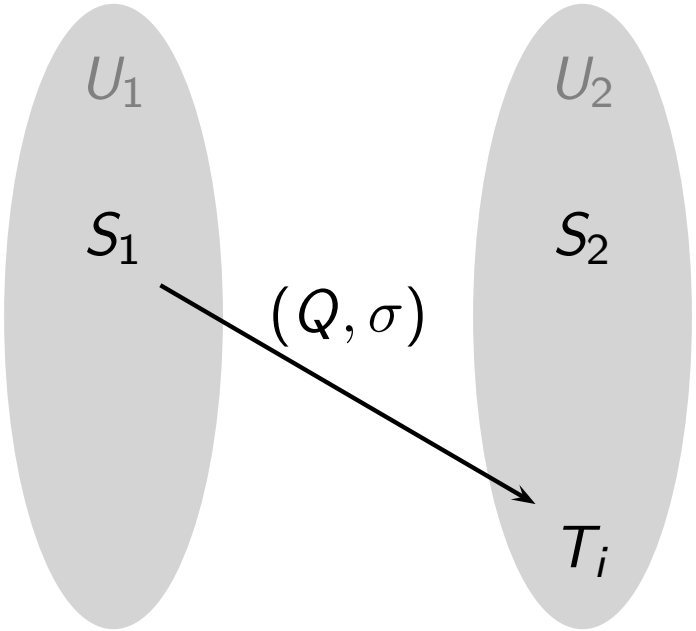
1. Server S_1 of U_1 provides quizzes to T_i with a MOVA signature.
2. When filled-in, the quiz is sent to server S_2 of U_2.
3. S_2 signs it and send it back to T_i with the signature.

Setup

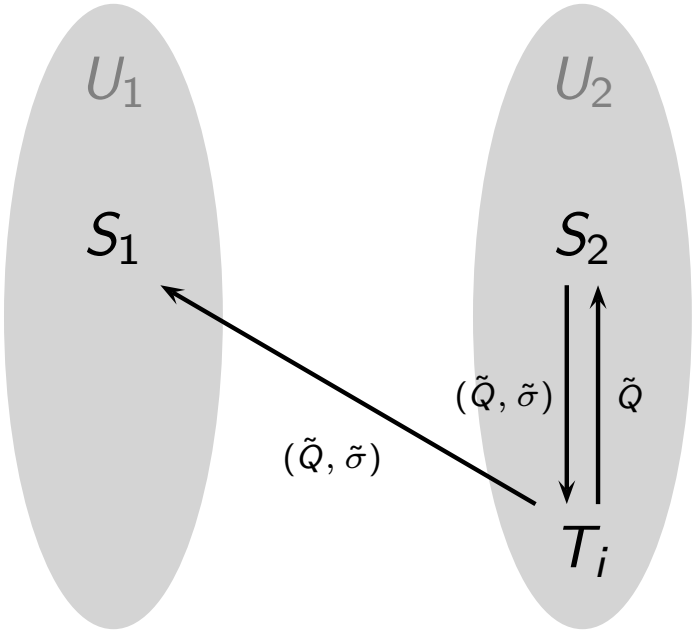
Consider two universities U_1, U_2 and a team T_i in university U_2.

1. Server S_1 of U_1 provides quizzes to T_i with a MOVA signature.
2. When filled-in, the quiz is sent to server S_2 of U_2.
3. S_2 signs it and send it back to T_i with the signature.
4. T_i can verify the signature and send it to S_1 with the signature.

Sending Quiz



Sending Quiz Back



Security

Security

- Every signature is done with MOVA.

Security

- Every signature is done with MOVA.
- Quizzes are signed so that teams are ensured not to have a fake one.

Security

- Every signature is done with MOVA.
- Quizzes are signed so that teams are ensured not to have a fake one.
- Servers use batch verification.

Security

- Every signature is done with MOVA.
- Quizzes are signed so that teams are ensured not to have a fake one.
- Servers use batch verification.
- Teams are authenticated to their respective university server when sending the quizzes back.

Security

- Every signature is done with MOVA.
- Quizzes are signed so that teams are ensured not to have a fake one.
- Servers use batch verification.
- Teams are authenticated to their respective university server when sending the quizzes back.
- Authentication is done using a simple challenge-response protocol.

Threat Model

An adversary could try the following

Threat Model

An adversary could try the following

- Forge fake quizzes. Hence the signature when sending quizzes.

Threat Model

An adversary could try the following

- Forge fake quizzes. Hence the signature when sending quizzes.
- Fill in the quizzes of another team. Not possible by construction.

Threat Model

An adversary could try the following

- Forge fake quizzes. Hence the signature when sending quizzes.
- Fill in the quizzes of another team. Not possible by construction.
- Modify the answers in a filled-in quiz. Hence the signature when sending back.

Implementation of MOVA

Implementation of MOVA

- $G = (\mathbb{Z}/n\mathbb{Z})^*$ where $n = pq$ is the product of two large primes.

Implementation of MOVA

- $G = (\mathbb{Z}/n\mathbb{Z})^*$ where $n = pq$ is the product of two large primes.
- $H = \{-1, 1\}$.

Implementation of MOVA

- $G = (\mathbb{Z}/n\mathbb{Z})^*$ where $n = pq$ is the product of two large primes.
- $H = \{-1, 1\}$.
- The homomorphism can be either $\left(\frac{\cdot}{p}\right)$ or $\left(\frac{\cdot}{q}\right)$.

Outline

Client

Android Application. It has three main activities.

Client

Android Application. It has three main activities.

ChallengeActivity To get the latest quiz. Answer to questions and send it back.

Client

Android Application. It has three main activities.

ChallengeActivity To get the latest quiz. Answer to questions and send it back.

UniversityScoreActivity To get the score of all participating universities.

Client

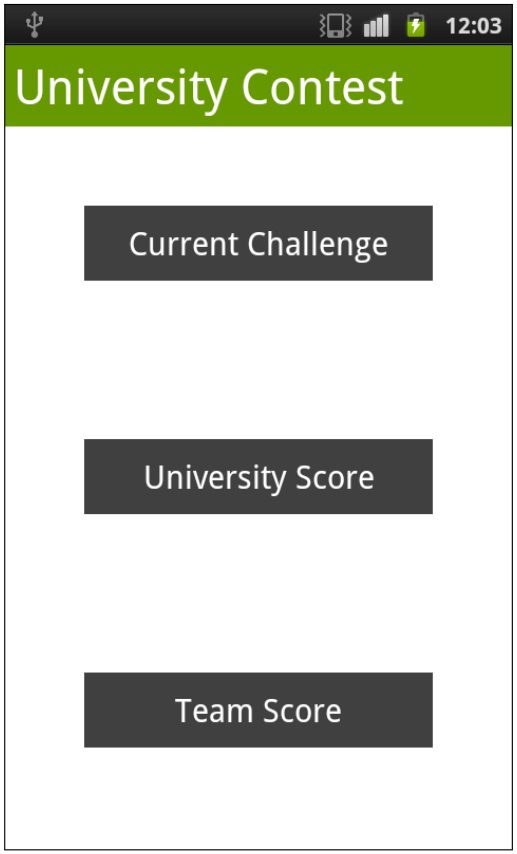
Android Application. It has three main activities.

ChallengeActivity To get the latest quiz. Answer to questions and send it back.

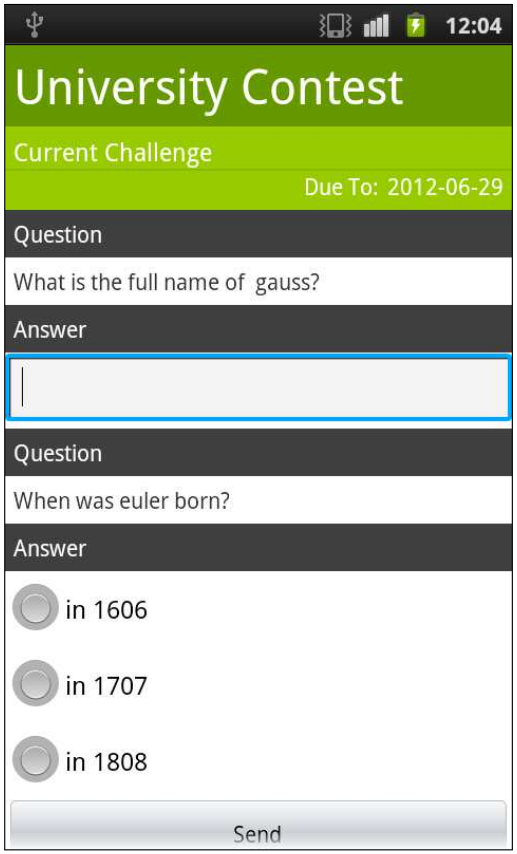
UniversityScoreActivity To get the score of all participating universities.

TeamScoreActivity To get his team score and the results of the quizzes.

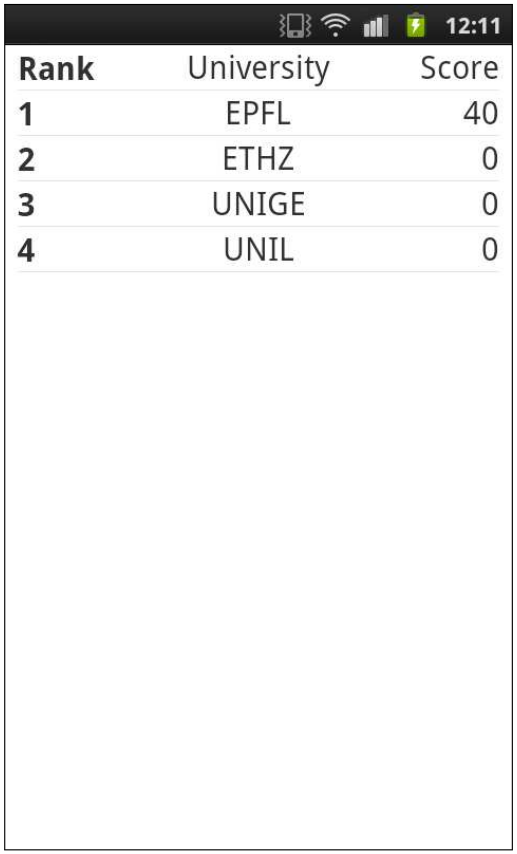
Main Menu


12:03
University Contest
Current Challenge
University Score
Team Score

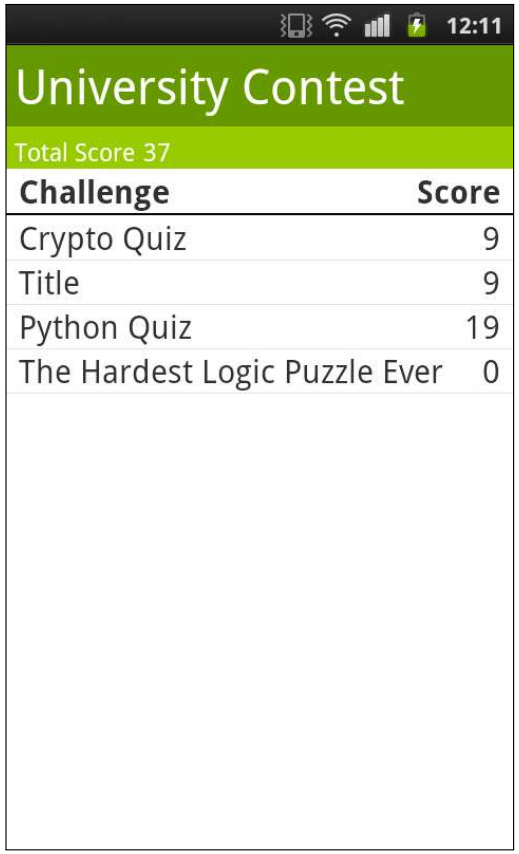
ChallengeActivity

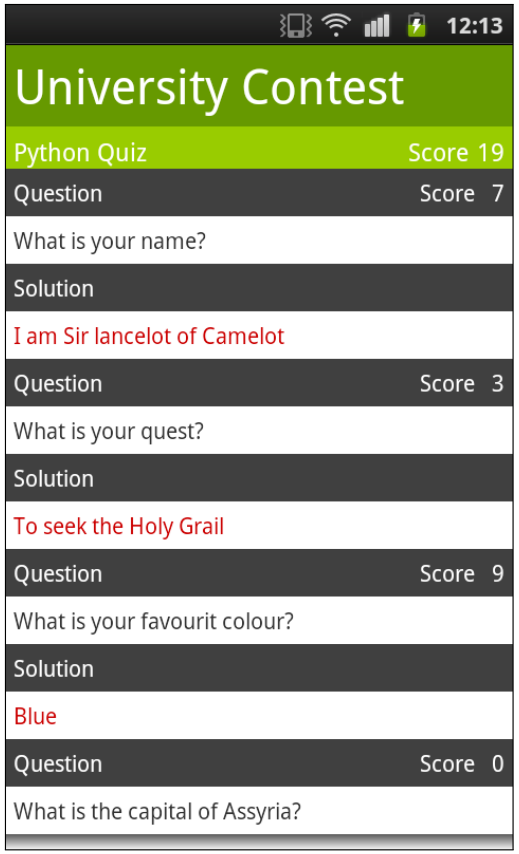


UniversityScoreActivity



TeamScoreActivity





Server

Two Java applications and a MySQL database.

Server

Two Java applications and a MySQL database.

Query Handler Process A constantly alive thread listening to a specified port and answering to queries.

Server

Two Java applications and a MySQL database.

Query Handler Process A constantly alive thread listening to a specified port and answering to queries.

Server Manager An application used to manage the server. Manage quizzes, teams and universities.

Server

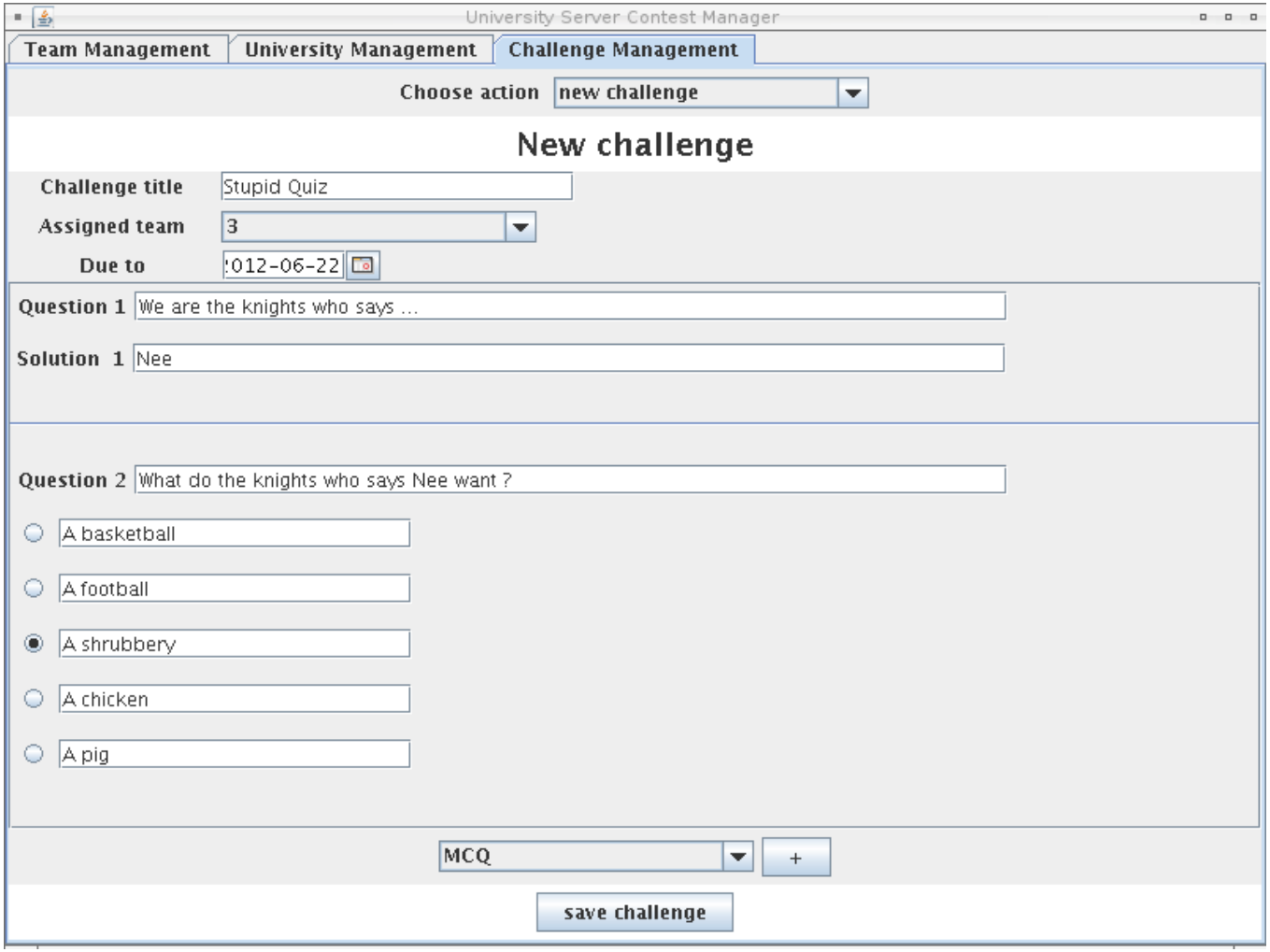
Two Java applications and a MySQL database.

Query Handler Process A constantly alive thread listening to a specified port and answering to queries.

Server Manager An application used to manage the server. Manage quizzes, teams and universities.

unicontest The database consisting of three tables (team,challenge and university).

Challenge Manager



Outline

Conclusion

- We have designed an application for android using MOVA.
- MOVA serves such real-life mobile apps.: e.g., by its shortness and by the batch verification.

Conclusion

- We have designed an application for android using MOVA.
- MOVA serves such real-life mobile apps.: e.g., by its shortness and by the batch verification.

Future Work: Find other applications using MOVA which look a bit less artificial.

Thanks for your attention !