University of Trento

Advanced Programming of Cryptographic Methods

Confidential But Genuine Feedback

Filippo De Grandi

Date: 21/11/2025

Contents

Description

A professor (or manager) collects feedback from students (or employees). Individuals must be free to express honest opinions while maintaining anonymity. At the same time, the professor or manager must verify that submissions come only from eligible participants.

An additional fairness requirement mandates that the system must detect when multiple messages originate from the same person, without revealing the person's identity.

The system must therefore support anonymous authentication, controlled pseudonymity and duplicate detection balancing privacy, authenticity, and fairness.

Requirements

Functional Requirements

FR 1 **Feedback Submission** : The submitters must be able to submit feedbacks

FR 2 **Feedbacks Access** : The receivers must be able to access the feedbacks

FR 3 **Duplicate Detection Mechanism** : The receiver must be able to distinguish if two feedbacks come from the same submitter

Security Requirements

SR 1 **Hidden Submitter Identity** : The receiver must not learn the identity of the submitter by the submitted feedbacks

SR 2 **Authorized Submission** : Only authorized submitters must be able to submit feedbacks

Non-Functional Requirements

NFR 1 **Privacy** : The system must comply with local privacy regulations and data protection laws to securely handle each user's data.The submitters must be aware of the inner functioning of the system

Technical Details

Architecture

Modules

1. Issuer Module: Managed by the professor/manager. This module verifies user eligibility (e.g. enrollment or employment status) and issues anonymous credentials or cryptographic tokens that allow secure, unlinkable participation while preventing unauthorized access.
2. User Module: Users authenticate to the issuer only once, obtain an anonymous credential, and then submit feedback using a GUI. Each submission is accompanied by a *linkable but anonymous* signature, derived from techniques such as Linkable Ring Signatures (LRS) [1] or group signatures with verifier-local revocation. This signature does not reveal the user's identity but generates a consistent pseudonym that allows detection of duplicate submissions.
3. Feedback Server: Receives feedback messages and verifies two aspects:
   1. The signature was produced by a legitimate credential holder.
   2. The submission's pseudonym has not been used before (if only one submission is allowed).

   The server aggregates feedback and provides results without learning the identity of any participant.
4. Cryptographic Layer: Employs privacy preserving authentication primitives such as anonymous credentials or linkable ring signatures. These provide anonymity, authenticity, and linkability. No user-identifying information is stored on the server.

Security Considerations

Anonymity

Users submit feedback with signatures that prove their eligibility without linking the message to their real-world identity.

Anonymous credentials ensure the issuer knows who is eligible but does not learn which participant produced which submission.

Authenticity

Only users who successfully obtained an anonymous credential can produce valid signatures. This ensures that all feedback originates from the authorized group.

Duplicate Detection

The linkable pseudonym generated by each user ensures that multiple submissions from the same participant can be detected. This pseudonym is stable across submissions but reveals no identifying information about the creator.

Integrity

Feedback cannot be modified or forged because signatures bind each message to a credentialed participant. Any tampering invalidates the signature.

Resistance to Impersonation

An attacker cannot impersonate a legitimate user, because anonymous credential systems enforce proof of knowledge of secret keys without revealing them.

Threat Model

Even if the feedback collector is curious or attempts to correlate messages, the cryptographic constructions prevent linking pseudonyms to identities. Network attackers cannot distinguish or clone submissions due to the use of secure channels and unforgeable anonymous signatures.

Bibliography

[1] Wikipedia, “Ring signature.” [Online]. Available: https://en.wikipedia.org/wiki/Ring_signature