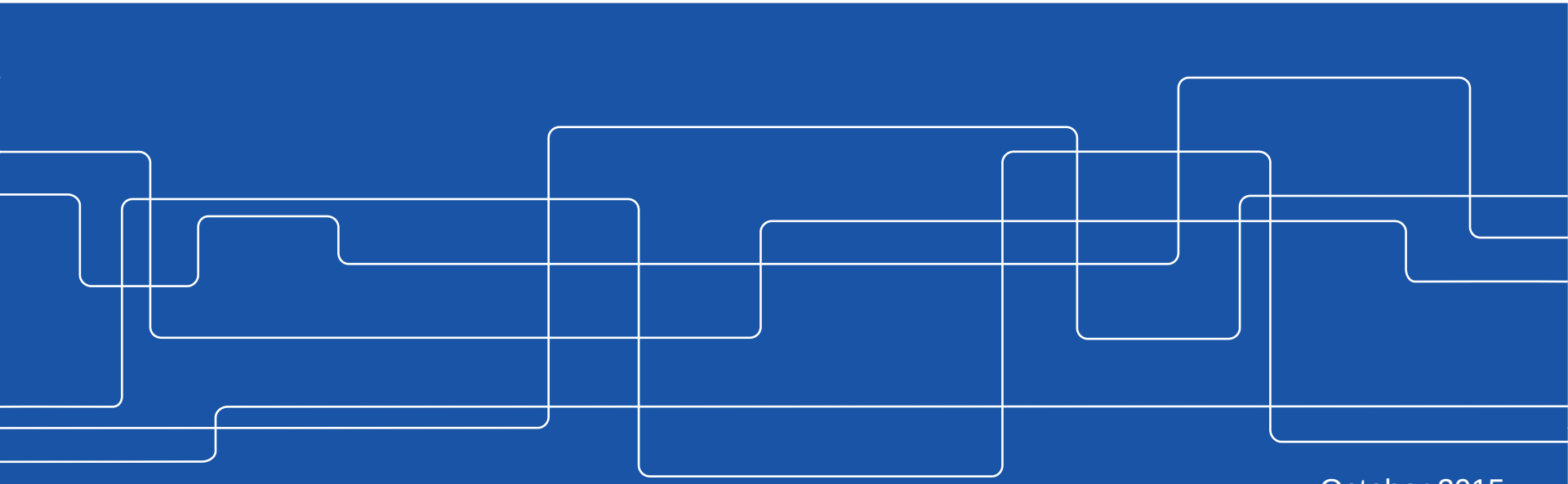
NordSec15 · 20th Nordic Conference on Secure IT Systems
KTH ROYAL INSTITUTE OF TECHNOLOGY · STOCKHOLM · SWEDEN

Design of a Privacy-preserving Document Submission and Grading System

Benjamin Greschbach, Guillermo Rodríguez-Cano, Tomas Ericsson, Sonja Buchegger
KTH Royal Institute of Technology



October 2015

Outline

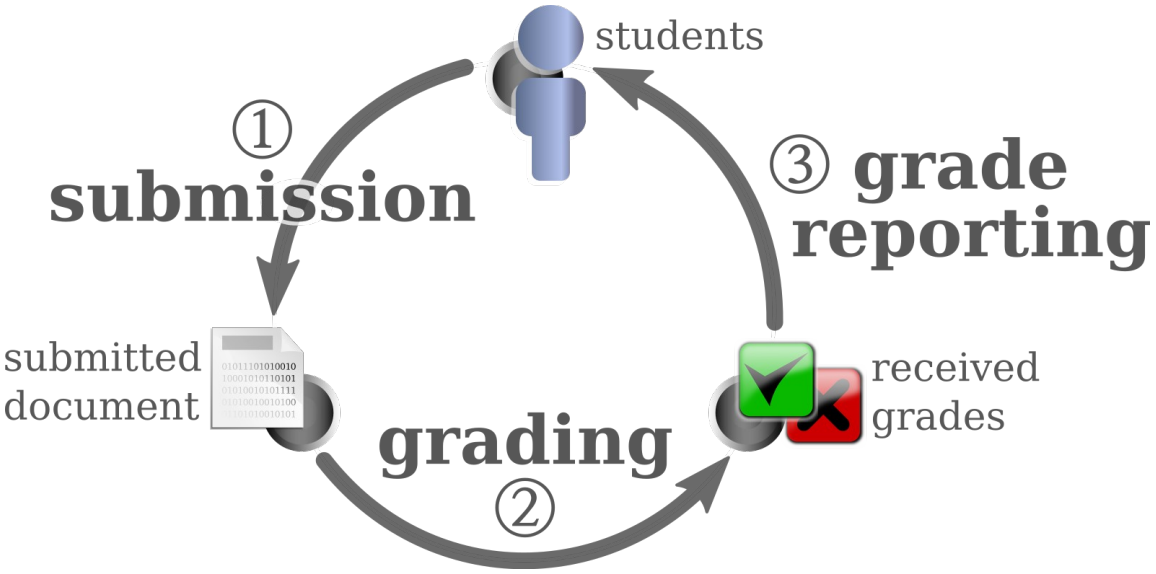
Problem Statement and System Model

Required Properties

Protocol

Discussion of Attacks and Limitations

Problem Statement and System Model

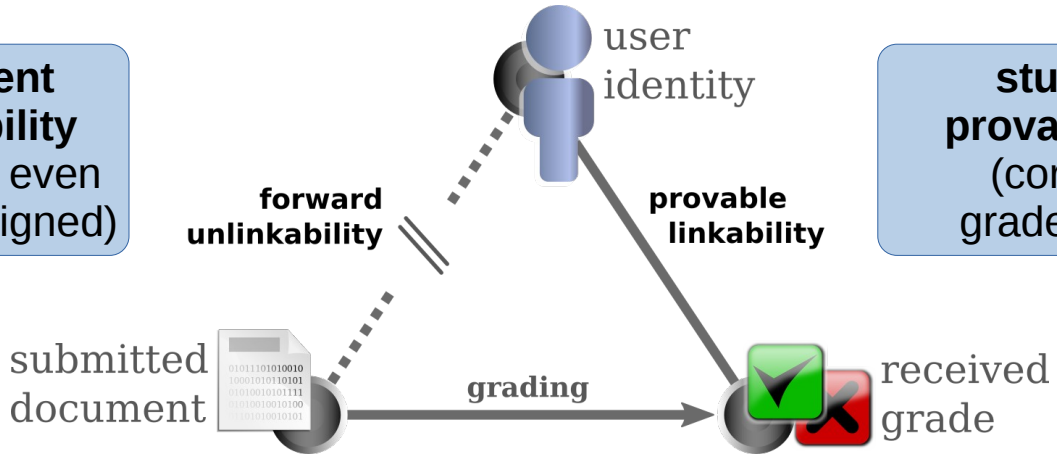


- Document submission and grading system

  e.g. university context: students handing in a written assignment, teacher grading with pass/fail

Required Properties

student-document forward unlinkability (anonymity remains even after grades are assigned)



student-grade provable linkability (correctness of grade-assignment)

- Anonymity: forward unlinkability of documents and identities
- Why? Biased grading, data minimization!
- Different from voting/whistle-blowing/Tor

Blind Signatures (Chaum 1982)

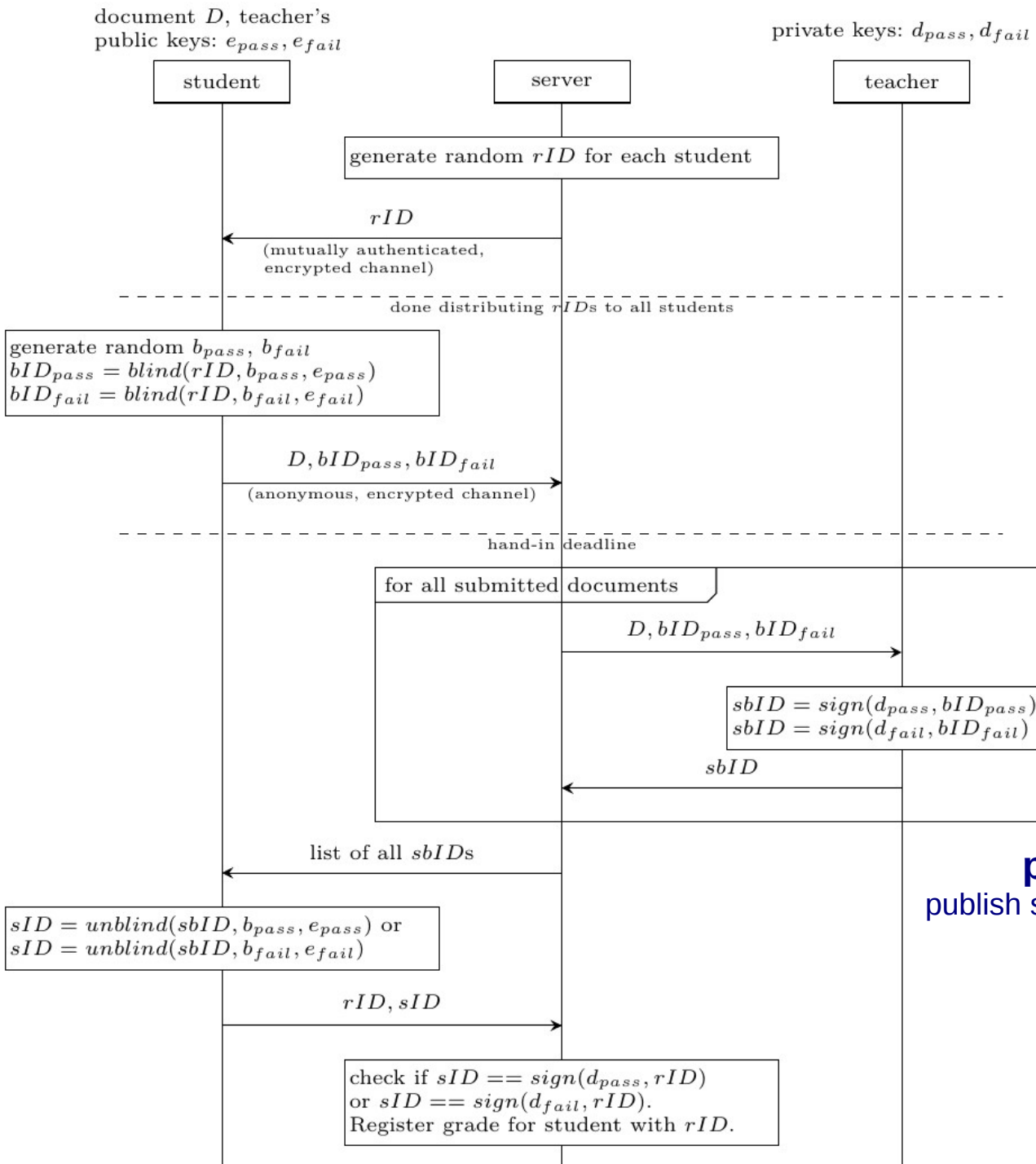
- Four functions: sign, verify, blind, unblind
- Desired property: **unblind(sign(blind(m))) = sign(m)**
- blind(message, blinding-factor, target-public-key)
  blindig-factor needed for unblinding
- RSA-based blind signature (implemented in GNU libcrypt):

  blind(m,b,e) = m·b^e = x

  sign(x,d) = x^d = (m·b^e)^d = (m^d)·b = y

  unblind(y,b) = y/b = m^d = sign(m,d)

Protocol



setup
distribute random identifiers (rID)

submission
hand in document and blinded rID

grading
teacher signs blinded rIDs

publish grades
publish signed, blinded rIDs

claim grades
submit unblinded signatures

Discussion: Required Properties

- **Anonymity (student - document forward unlinkability)**
  setup: rID -- studentID
  submission: document -- blinded rID
  grading: blinded rID -- grade
  claiming grades: rID/studentID -- grade
  ► k-anonymity among those with same grade
- **Correctness (student - grade provable linkability)**
  sound (students cannot cheat), and
  complete (students can claim grade)

Discussion: Attacks

- **Timing and correlation attacks**
  submission not before rID distribution
  publish grades as complete list (no fetch single entries)
  end-to-end traffic correlation (Tor deanonymization)
- **Impersonation and replay attacks**
  rID instead of public identifier (e.g. e-mail address)
  ghost-writing general limitation
- **Crypto primitives implementation**
  importance of different blinding-factors for each grade
- **General system implementation attacks**
  cross-site-scripting on webinterface, etc.

Discussion: Limitations and Extensions

- **Anonymity**
  no plagiarism/cheating punishment beyond grading as fail
  not more information than the grade for the teacher (about individual students)
- **Students can choose not to claim their grade**
  possible extension: additional commit phase
- **Unfair grading**
  students can give up their anonymity in order to complain
- **Submission acknowledgements**
  proof that you submitted before deadline (even in case of technical failure later)
- **More finegrained grading scales**
  straightforward (one additional key per grade), but reduces anonymity sets
- **more...**
  several teachers, additional text-feedback/comments

Summary

- Anonymous (forward unlinkable) Document Submission and Grading
- Protocol using Blind Signatures (+ prototype implementation using GNU libcrypt)
- Achieves k-anonymity for students with same grade and correctness for teachers
- Limitations and Extensions