Anonimowy egzamin.

Zagadnienie odwoływalnej anonimowości w schemacie dynamicznego podpisu grupowego.

Paweł Kaczorowski maj *2010*

Promotor: prof. dr hab. inż. Zbigniew Kotulski

Plan prezentacji

1. Przegląd rozwiązań.
2. Wprowadzenie (definicja, zastosowania podpisu grupowego).
3. Podstawy podpisu grupowego.
4. Protokół anonimowego egzaminu.
5. Architektura systemu.
6. Problemy do rozwiązania.
7. Kontrola uczciwości.

Anonimowość - definicja

Niemożność identyfikacji tożsamości jednostki pośród innych członków danej społeczności

Anonimowy egzamin – egzamin, dla którego niemożliwa jest identyfikacja tożsamości autora

Przegląd rozwiązań (1/2)

- matura (PESEL jako identyfikator)
- egzaminy papierowe (Exam ID, Chalmers University of Technology) – słaba skalowalność
- smart cards, PDA - Linkoping University

Przegląd rozwiązań (2/2)

Systemy e-learningowe:

- metody pośrednie:

  - kontrolowane środowisko egzaminacyjne, (College Level Examination Program)

  - Securexam Student software (Earle Mack School of Law, kroki: ściągnij egzamin, rozwiąż w MS Word, usuń dane identyfikujące, podpisz przydzielonym ID, wyślij, *"you should name the final version something unique"*)

- brak rozwiązań gwarantujących anonimowość

Wprowadzenie – podpis grupowy (1/2)

- podpis grupowy jest to schemat kryptograficzny, który pozwala na generację podpisu w imieniu grupy, bez ujawniania tożsamości podpisującego
- w szczególności istnieje możliwość ”otworzenia” tożsamości podpisującego przez uprawniony organ

Wprowadzenie - podpis grupowy (2/2)

Zastosowanie:

- Systemy głosowania: potwierdzenie prawa do głosowania poprzez należność do grupy, lecz bez ujawniania tożsamości głosującego
- Licytacje: tożsamość osoby, która wygrała licytacje jest znana po zakończeniu licytacji
- E-cash: transfery gotówkowe pomiędzy bankami, w sposób bezpieczny, lecz anonimowy, nienamierzalny
- Szeroko rozumiana ”Polityka Prywatności”

Podstawy podpisu grupowego (1/3)

Pierwsza koncepcja podpisu grupowego zaproponowana została przez Chaum 'a i Van Heyst'a w 1991 roku:

- jeden menadżer grupy (GM),
- GM posiada klucz prywatny, za pomocą którego może ”otworzyć” tożsamość podpisującego
- n członków grupy,
- ilość członków znana w czasie tworzenia grupy,
- każdy członek ma swój klucz prywatny, którym się podpisuje
- weryfikacja podpisu na podstawie publicznego klucza grupowego

Podstawy podpisu grupowego (2/3)

Cechy jakimi powinien się odznaczać schemat podpisu grupowego:

- Anonimowość (Anonymity) – nie można rozpoznać (wyśledzić) podpisującego za pomocą jego podpisu
- Traceability – nie można utowrzyć poprawnego podpisu, którego nie można wyśledzić (”otworzyć”)
- Niepodrabialność (Unforgeability) – jest obliczeniowo niemożliwe dla osoby nie posiadającej prywatnego podpisu grupowego do wygenerowania poprawnego podpisu σ wiadomości m
- Exculpability – nikt nie może wygenerować poprawnego podpisu w nieswoim imieniu

Podstawy podpisu grupowego (3/3)

Cechy jakimi powinien się odznaczać schemat podpisu grupowego c.d. :

- Odporność na koalicje (Coalition resistance) – użytkownicy w zmowie, nie mogą utworzyć podpisu, którego nie można wyśledzić (”otworzyć”)
- Framing – użytkownicy w zmowie nie mogą utworzyć podpisu składającego się z części własnych podpisów, który by był weryfikowany jako podpis innego członka grupy.
- Niemożność powiązania podpisów (Unlinkability) – podpisy tego samego użytkownika nie mogą służyć do jakiegokolwiek połączenia ich z użytkownikiem

Opis dotychczasowych schematów (1/5)

Schemat BMW (Mihir Bellare, Micciancio, Warinschi) 2003:

- Sformalizowanie schematu statycznego podpisu grupowego Chaum 'a i Van Heyst'a

Zdefiniowanie dwóch mocnych założeń, które są wypadkowymi założeń podstawowych:

- Full anonymity - Nikt poza managerem nie jest w stanie powiedzieć który członek grupy podpisał daną wiadomość,
- Full traceability – użytkownicy będący w zmowie nie mogą wygenerować poprawnego podpisu, który będzie przyporządkowany innemu członkowi grupy, nawet w przypadku znajomości sekretu menadżera grupy.

Opis dotychczasowych schematów (2/5)

W przypadku **dynamicznej grupy**, w momencie tworzenia nie jest znana liczba członkow oraz ich tożsamość. Strona zaufana jest odpowiedzialna za wygenerowanie klucza publicznego grupy oraz klucza dla organu zarządzającego (authority). Jednostka(osoba) może przyłączyć się do grupy i uzyskać klucz prywatny w dowolnym czasie, za pomocą protokołu dodawania wykonywanego z organem zarządzającym.

Opis dotychczasowych schematów (3/5)

Schemat BMW (Mihir Bellare, Micciancio, Warinschi) 2003 c.d. :

GS = (GKg ; GSig ; GVf ; Open)

GKg {k:N, n:N}-->{gpk, gmsk, **gsk**}
GSig {gsk[i], m}-->{σ}
GVf {gpk,m,σ}-->{0 v 1}
Open {gmsk, m, σ}-->{i}

Opis dotychczasowych schematów (4/5)

Mihir Bellare, Haixia Shi, Chong Zhang (BMW + Case of Dynamic Group) 2004

GS = (GKg ; UKg ; Join ; GSig ; GVf ; Open ; Judge)

GKg {k:N}-->{gpk, ik, ok}

UKg – odpowiednik PKI

Join – interaktywny protkoł pomiędzy użytkownikiem zarządzającym (posiadaczem klucza ik)

GSig –{gsk[i], m}-->{σ}

GVf – {gpk,m,σ}-->{0 v 1}

Open {ok, m, σ}-->{i,τ}

Judge {gpk, τ, upk[i],m,σ }-->{true,false}

Opis dotychczasowych schematów (5/5)

Schemat BMW (Mihir Bellare, Micciancio, Warinschi) oraz przypadek grupy dynamicznej:

Użyte prymitywy

- IND-CCA secure asymmetric encryption scheme;
- Zero-knowladge proofs;
- digital signature scheme (PKI);

Podpis grupowy - podsumowanie

- Schemat dynamiczny:

  - organ generujący podpis (gpk) nie zna kluczy prywatnych użytkowników

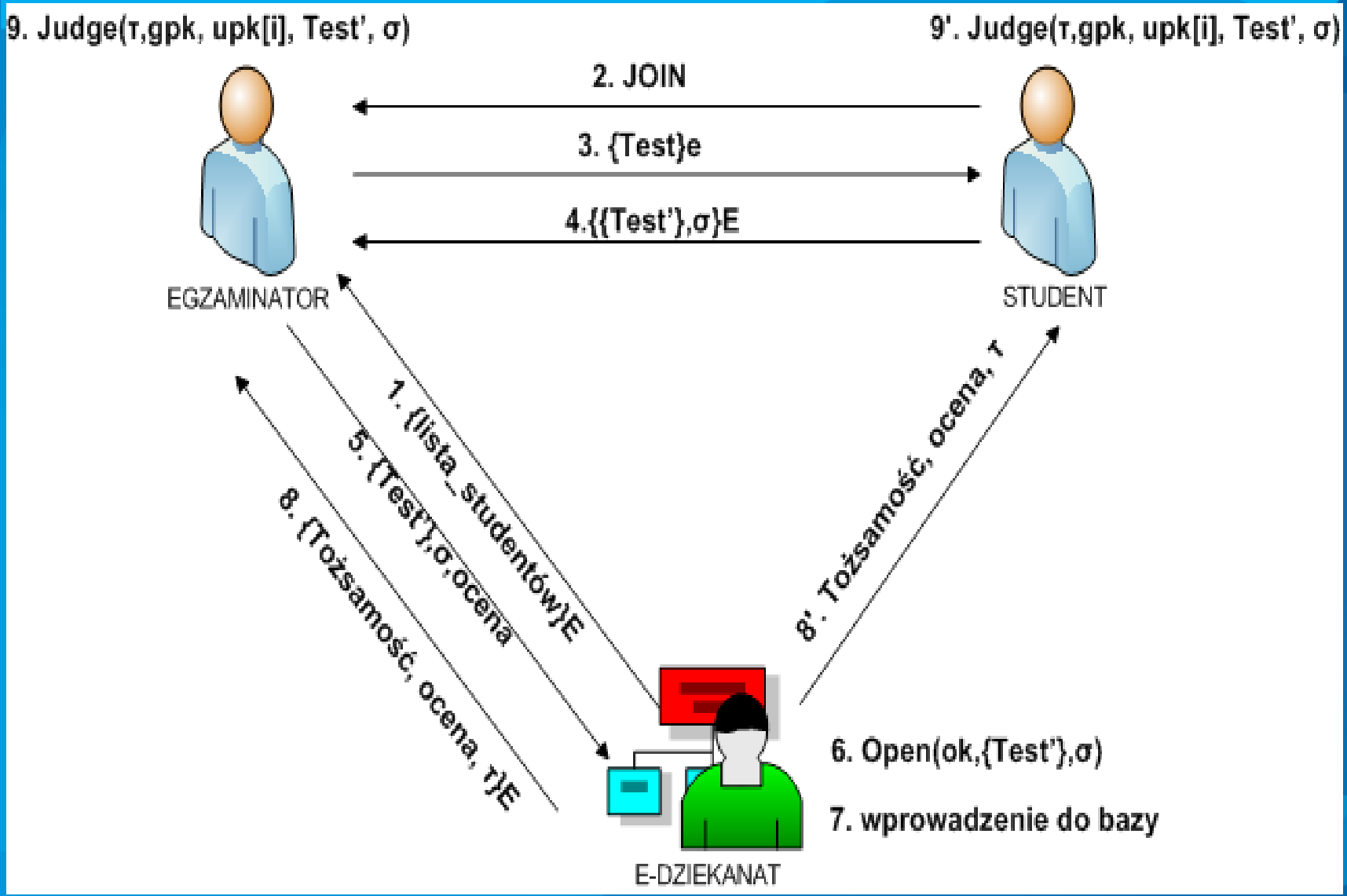
  - bezpieczny protokół dołączania do grupy

  - oddzielne organy *issuer* i *opener*

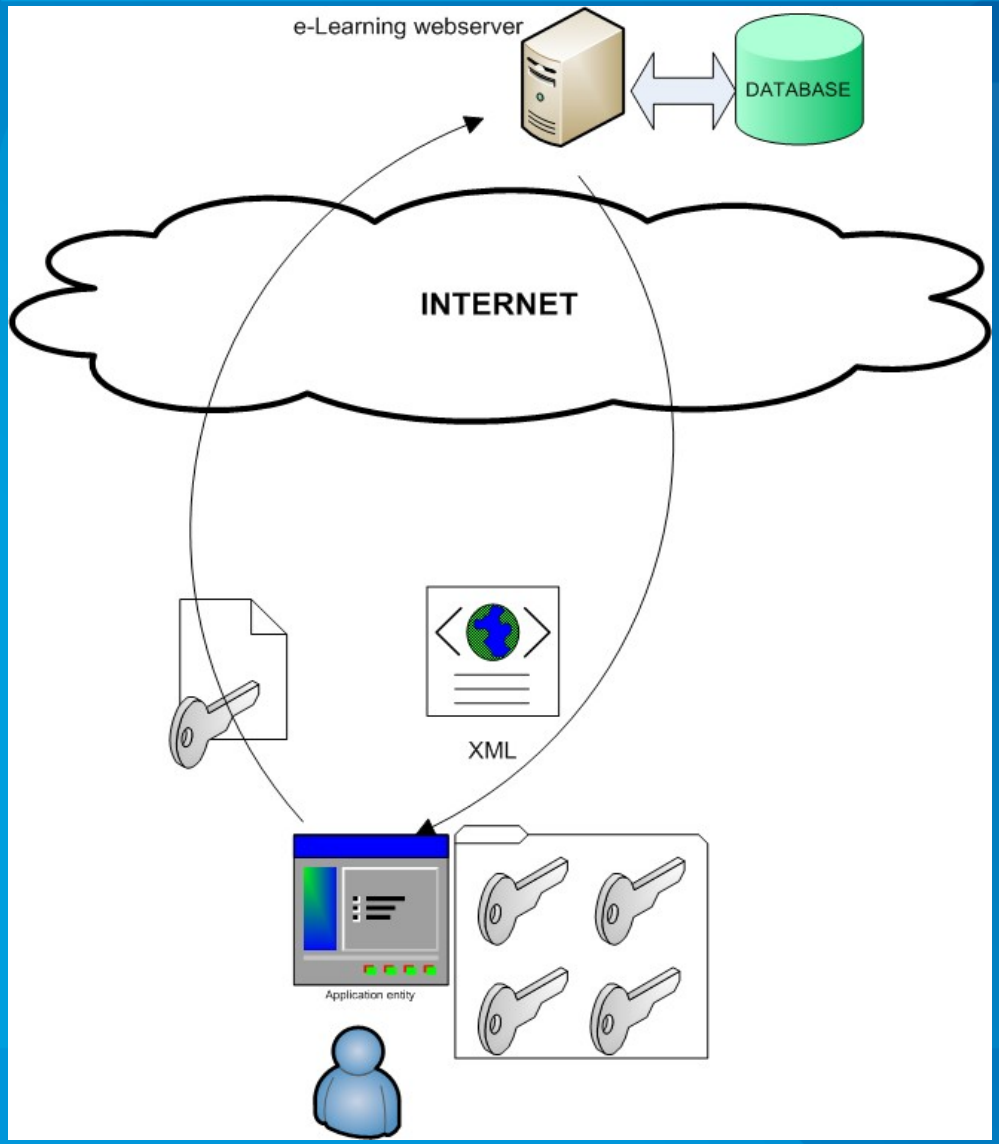
  - problem unieważniania podpisów

  - problem inicjalizacji (założenie, że jest bezpieczny)

Anonimowy egzamin - protokół



Architektura systemu



- ''Basen'' do wrzucania plików
- Egzaminy w formacie XML
- Bezpieczne uwierzytelnienie (SSL)
- Webservice + aplikacja kliencka

Problemy (1/2)

- pytania zamknięte (autogeneracja, sprawdzanie, wynik)

  W przypadku pytań zamkniętych możliwa jest eliminacja subiektywnej oceny egzaminatora.
- pytania otwarte (problem subiektywnej oceny)
- kontrola integralności danych

  Czy mój egzamin nie został zmieniony? Jak student ma zweryfikować poprawność dostarczonego egzaminy?

Problemy (2/2)

- przypadek unieważnienia klucza

  Co należy zrobić w przypadku niedopuszczenia studenta do egzaminu?
- format wysyłanej wiadomości

  Wiadomość wysyłana do systemu powinna być pozbawiona wszelkich danych, które mogą prowadzić do identyfikacji studenta. Odpowiedzialna jest za to aplikacja kliencka.
- ograniczenia interfejsu (prawdopodobnie ubogie GUI)

Kontrola uczciwości

- timeout

  Skończony czas na pisanie pracy
- aktywne okno czasowe (podwójna kontrola)

  Egzamin aktywny tylko o danej godzinie
- synchronizacja czasu (dostęp do internetu)
- mechanizm reklamacji

  Do momentu rozwiązania wszelkich reklamacji studentów, egzaminator nie może znać tożsamości autora egzaminu
- publikacja rozwiązań

Bibliografia

- CvH91 D. Chaum, E. van Heyst. Group signatures. In: EUROCRYPT'91, LNCS 547, pp. 257-265. Springer-Verlag, 1991.
- M. Bellare, D. Micciancio, and B. Warinschi. Foundations of Group Signatures: Formal Definitions, Simplified Requirements, and a Construction Based on General Assumptions. In: EUROCRYPT 2003, LNCS 2656, pp. 614-629. Berlin: Springer-Verlag, 2003.
- Mihir Bellare, Haixia Shi, Chong Zhang. Foundations of Group Signatures: The Case of Dynamic Groups. In: Topics in Cryptology - CT-RSA 2005, LNCS 3376, pp. 136-153. Springer-Verlag, 2005.

Dziękuję za uwagę.