Biblioteka PARI/GP w zastosowaniu do systemu ćwiczeń laboratoryjnych

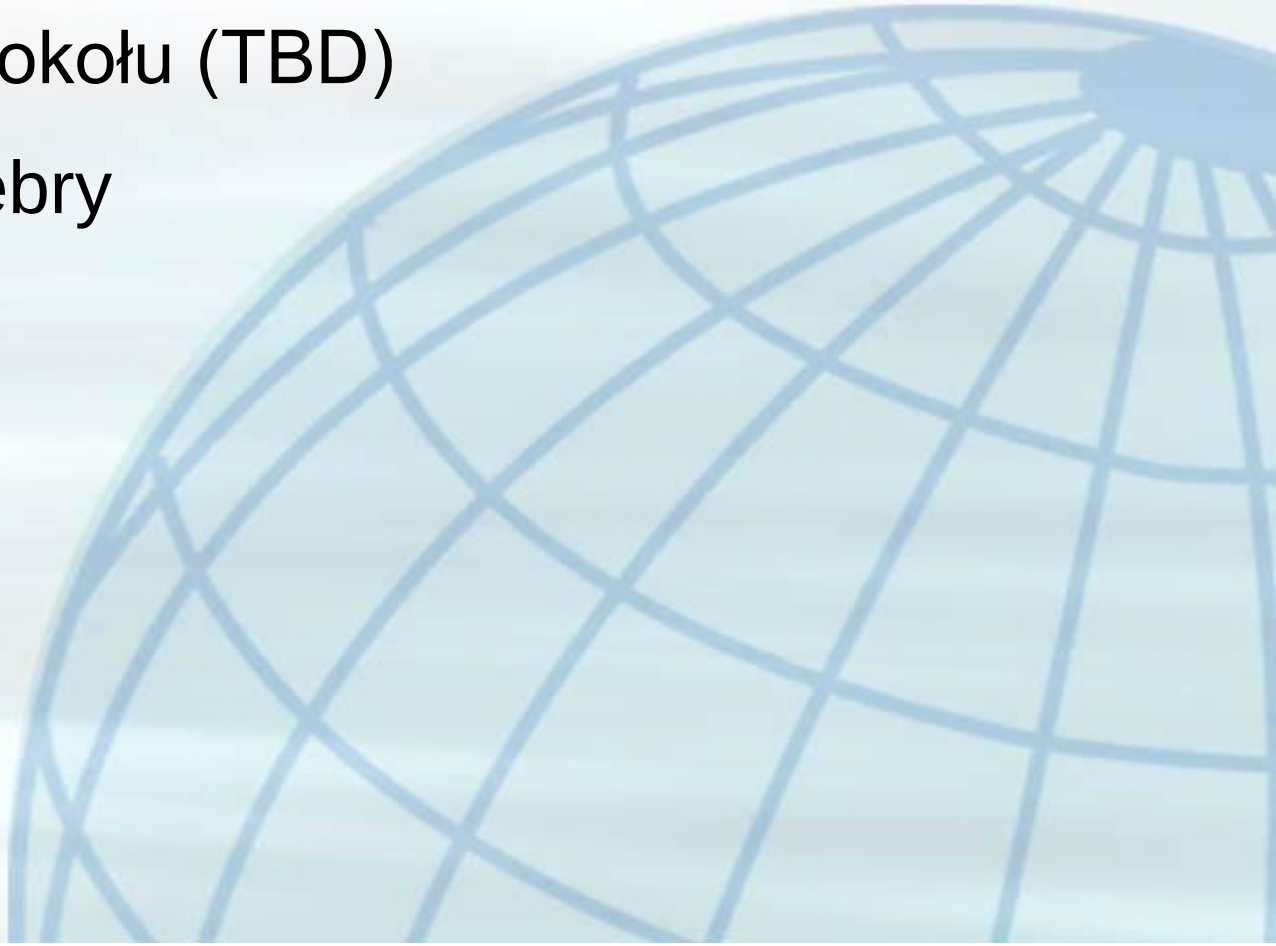
Bartosz Dzirba

Gabriel Kujawski

opiekun: prof. dr hab. Zbigniew Kotulski

Plan prezentacji

- Ćwiczenie laboratoryjne
- Przykład protokołu (TBD)
- Systemy algebry
- PARI/GP
  - wstęp
  - problemy…
  - biblioteka



Ćwiczenie laboratoryjne
wstęp

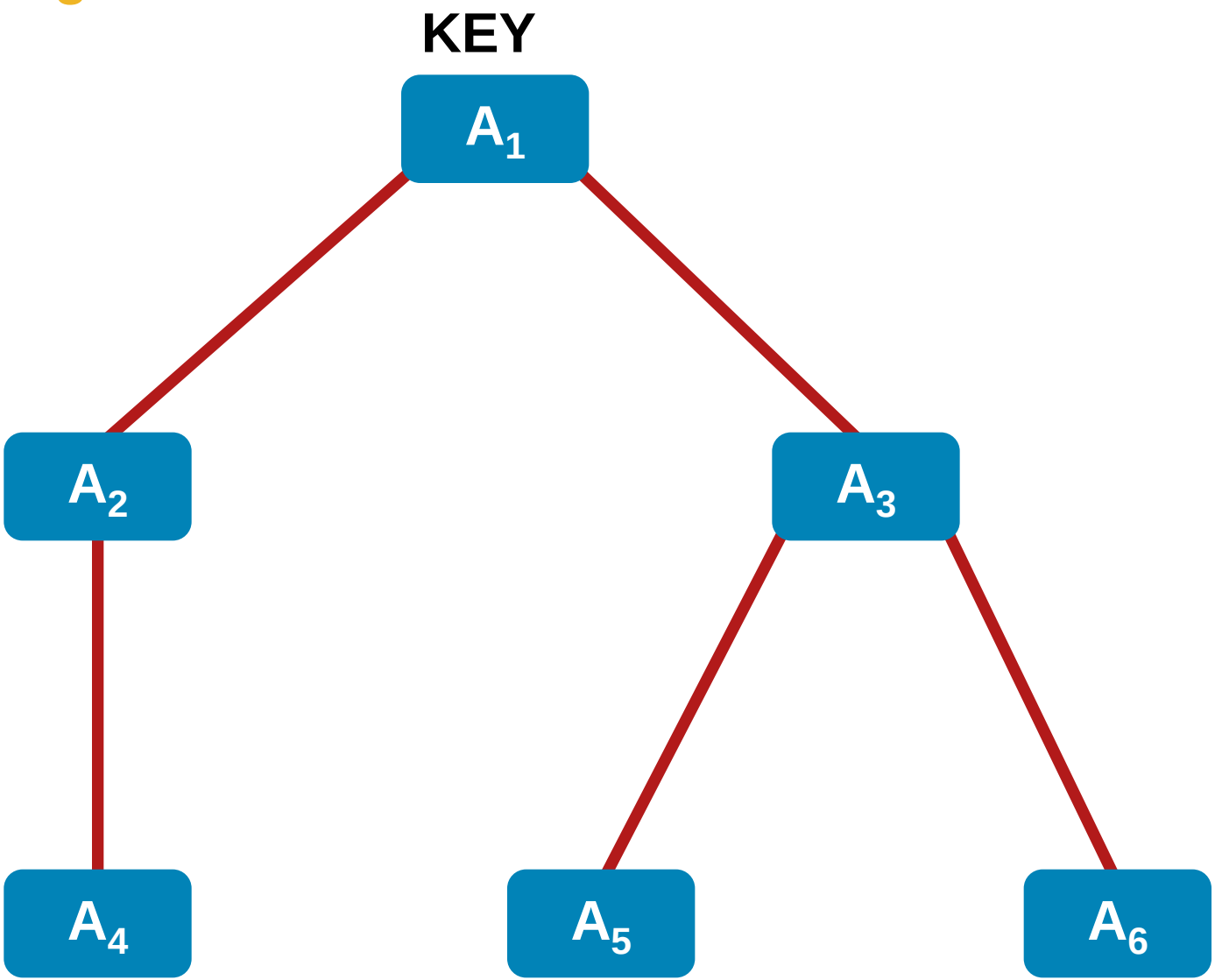
- Tematyka:
  - Kolektywne uzgadnianie klucza
- Założenia:
  - Praktyczne zapoznanie studenta z protokołami uzgadniania klucza
  - Wykonanie wybranych protokołów
  - Możliwość łatwej rozbudowy
  - Działanie w laboratorium komputerowym
- Potrzebne elementy:
  - Aplikacja
  - Biblioteki protokołów
  - System algebry

Ćwiczenie laboratoryjne
efekt pracy

- Aplikacja sieciowa *KUK*
- Zaimplementowane protokoły
  - dwustronne
  - grupowe (różne topologie)
- Scenariusze z atakami
  - MitM
  - kontrola klucza
- Realne testy dla kilkunastu uczestników
- Przykładowy skrypt ćwiczenia

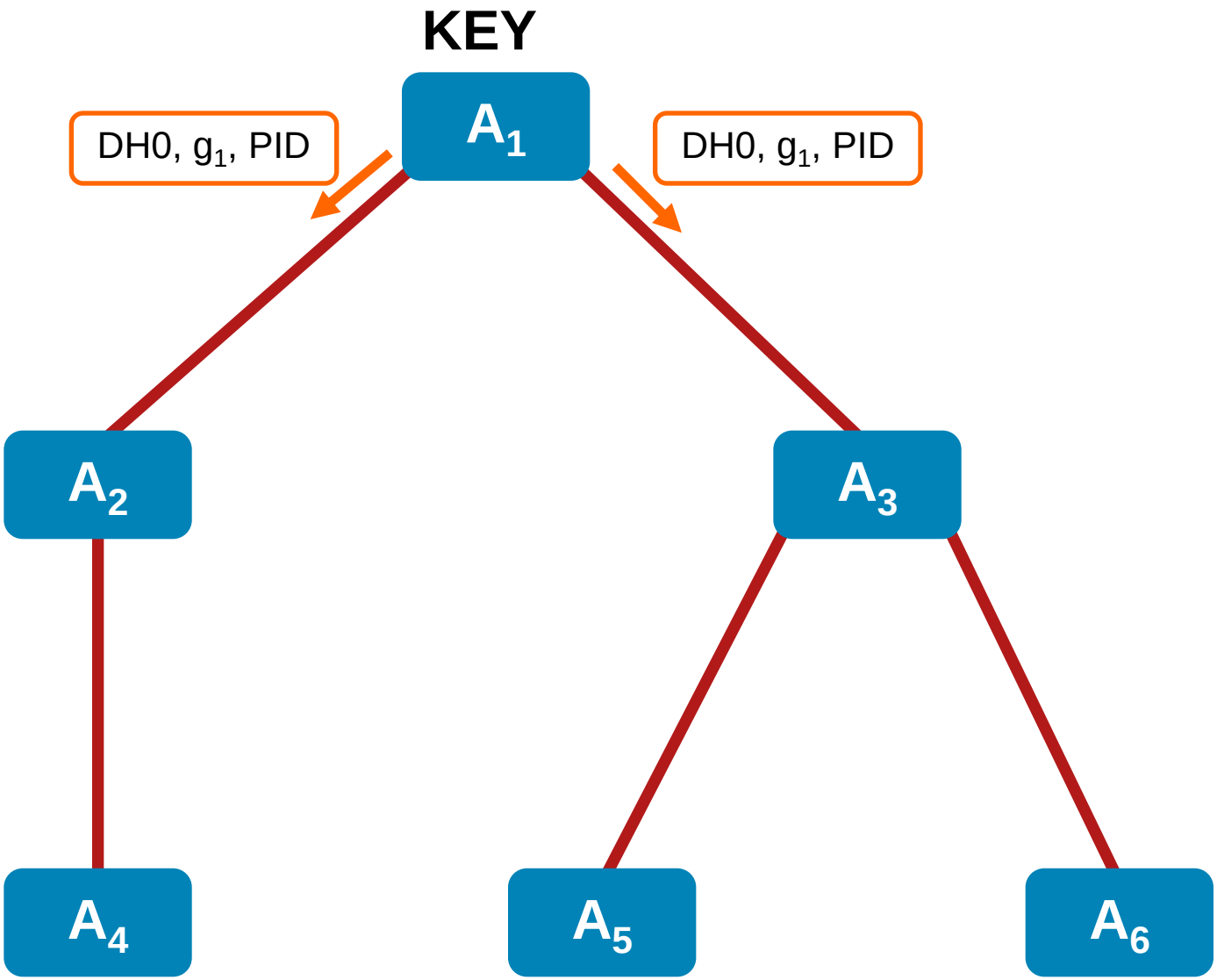
Tree-based Burmester Desmedt

topologia



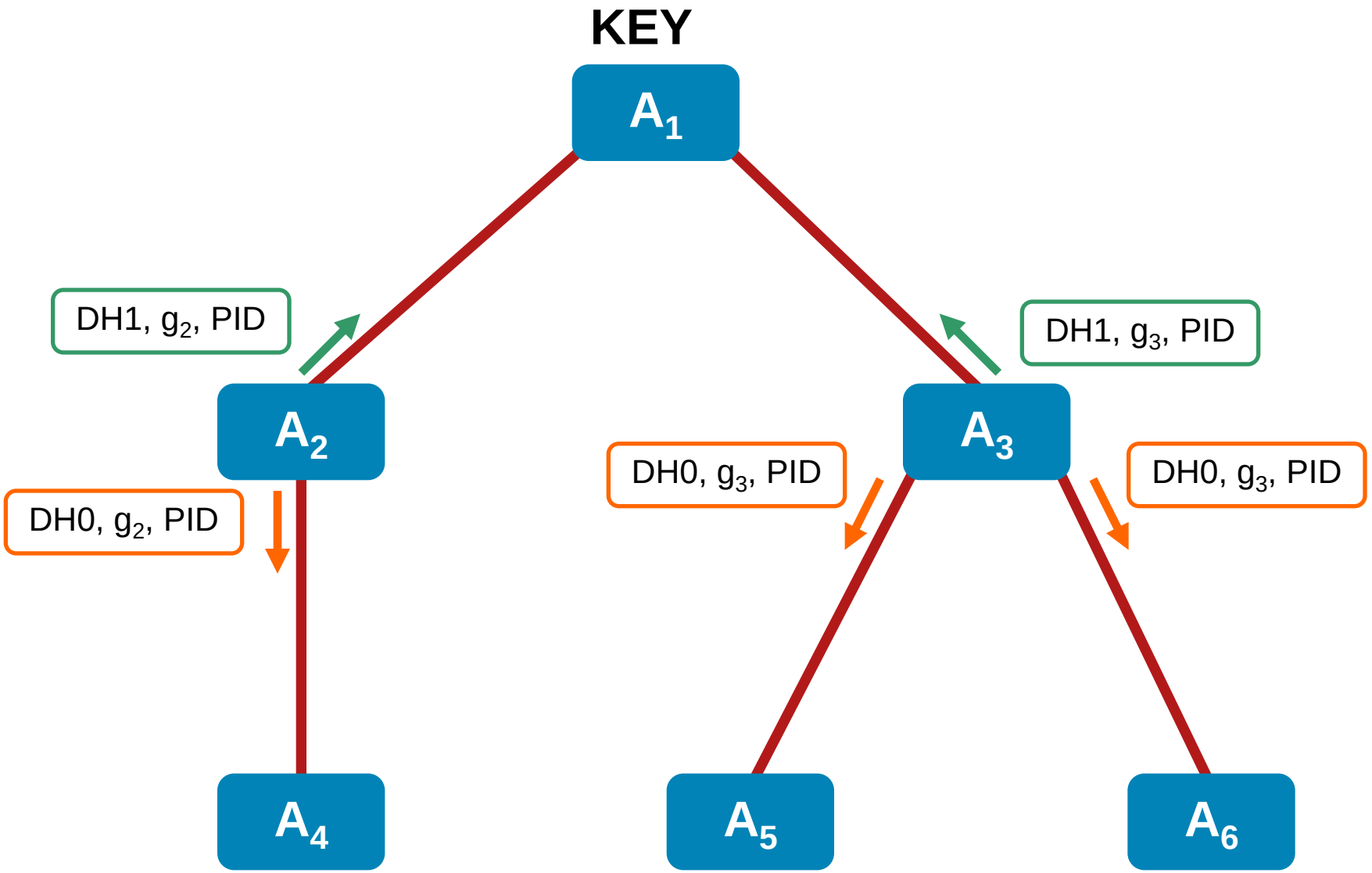
Tree-based Burmester Desmedt

runda 1



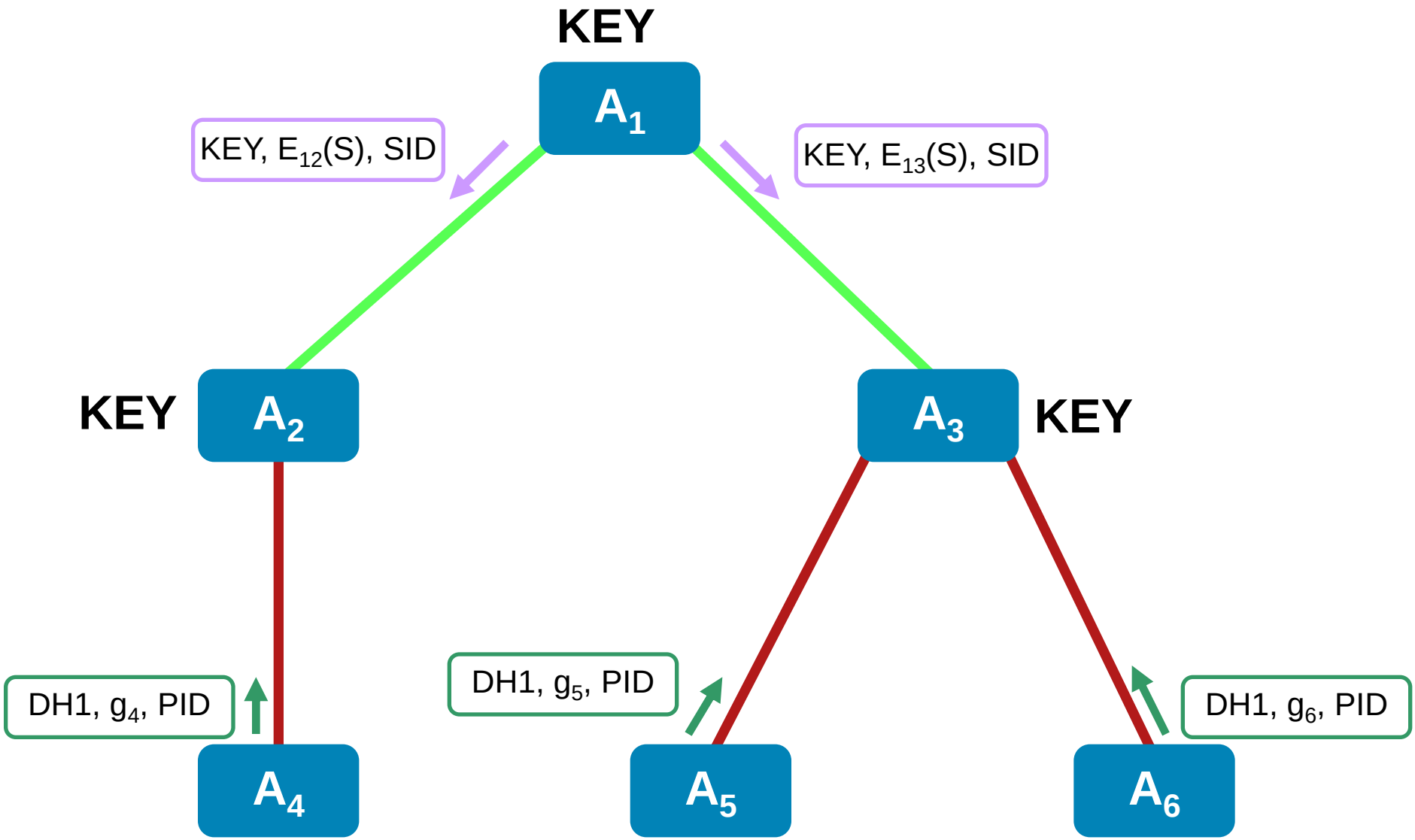
Tree-based Burmester Desmedt

runda 2



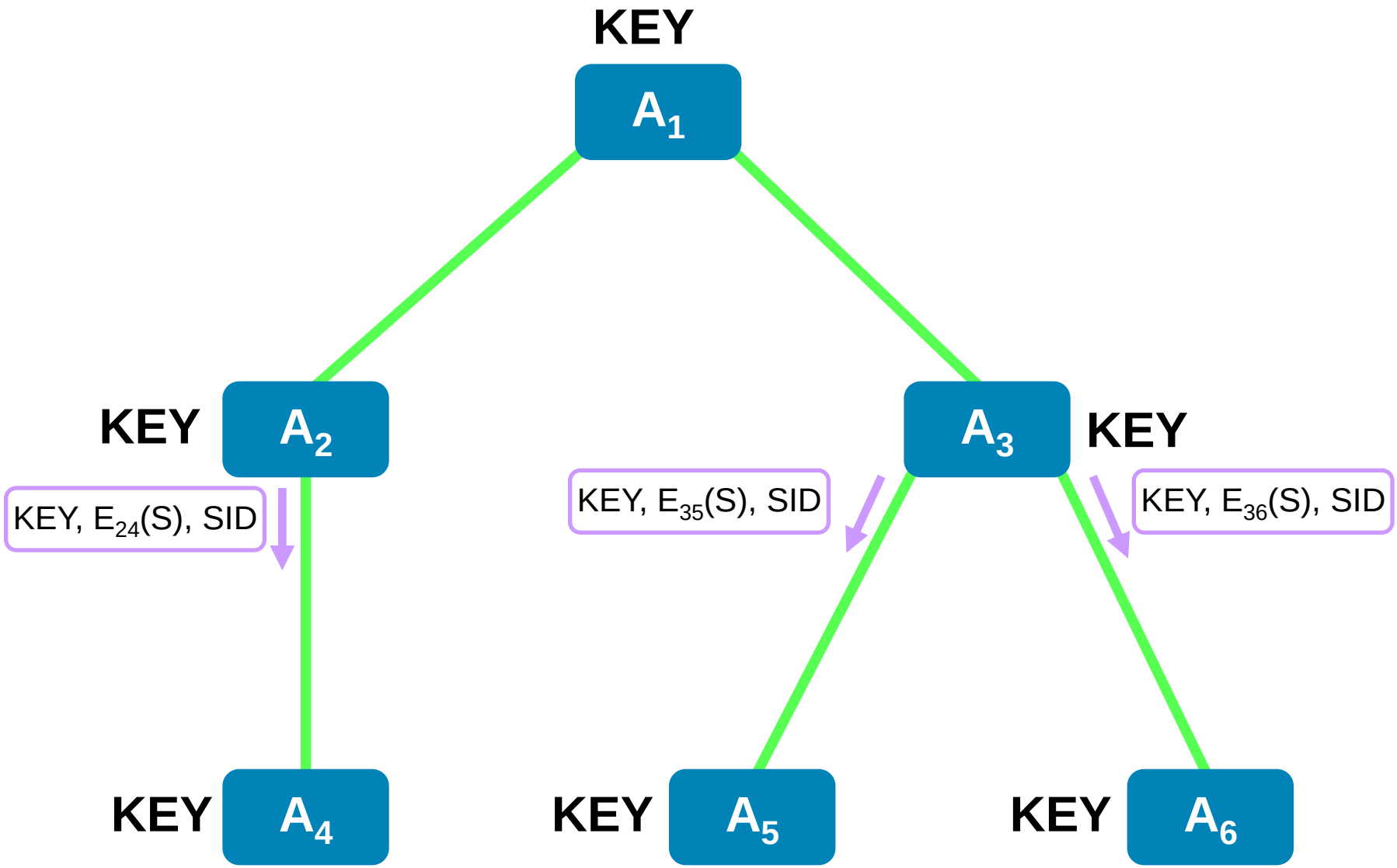
Tree-based Burmester Desmedt

runda 3



Tree-based Burmester Desmedt

runda 4



Systemy algebry
wstęp

- Potrzeby:
  - obsługa dużych liczb
  - operacje modulo p
  - znajdowanie generatora grupy
  - znajdowanie elementu odwrotnego modulo p
  - znajdowanie liczb pierwszych
  - możliwość wykorzystania w MS VC++ .NET 2008
- Możliwe podejścia:
  - wykorzystanie gotowego systemu
  - napisanie własnej biblioteki

Systemy algebry
dostępne możliwości

Crypto++

Yacas

OpenSSL

PARI/GP

cryptlib

Maxima

MathCAD

Axiom

Maple

PARI/GP
wstęp

- Dostępny pod adresem: http://pari.math.u-bordeaux.fr/
- Możliwości:
  - Operacje na liczbach całkowitych i rzeczywistych
  - Wsparcie podstawowych operacji matematycznych jak i na wektorach oraz macierzach
  - Generatory liczb losowych i pierwszych
  - Praca z teoretycznie dowolnie dużymi liczbami
- Źródła i binaria (GP)
- Licencja GPL
- Wydajność – czołówka wśród darmowych

PARI/GP
problemy

- Dokumentacja, głównie do GP
- Biblioteka dedykowana dla systemów Unix/Linux

  Brak oficjalnego wsparcia dla Windowsa

  Binaria pod Windows (GP, Cygwin)

  C/C++ to nie to samo co Microsoft .NET VC++
- Działało z VC 6 / Win 9x (1998r.)

PARI/GP
pomysły

- Wykorzystanie GP
  - opcja 1: lokalny proces aplikacji (stdin/stdout)
  - opcja 2: demon sieciowy
  - zalety: prosta metoda
  - wady: dostęp do wybranych funkcji
- Bezpośrednie wykorzystanie w aplikacji
  - zalety: pełna integracja
  - wady: niekompatybilność z MS VC++
- Niezależna biblioteka DLL
  - zalety: pełna integracja
  - wady: brak

PARI/GP
biblioteka

- Out-of-box… nie działa
- Uruchomienie zajęło 2 tyg.
- Efekt: biblioteka DLL oferująca wymagane funkcje dla aplikacji
- PARI FAQ

Pytania?
Dziękujemy.

Bartosz Dzirba

Gabriel Kujawski

opiekun: prof. dr hab. inż. Zbigniew Kotulski