Uniwersytet im. Adama Mickiewicza w Poznaniu

Wydział Matematyki i Informatyki
Uniwersytet im. Adama Mickiewicza w Poznaniu

Anna Izydorczyk, Mateusz Piątkowski, Jakub Pluciński

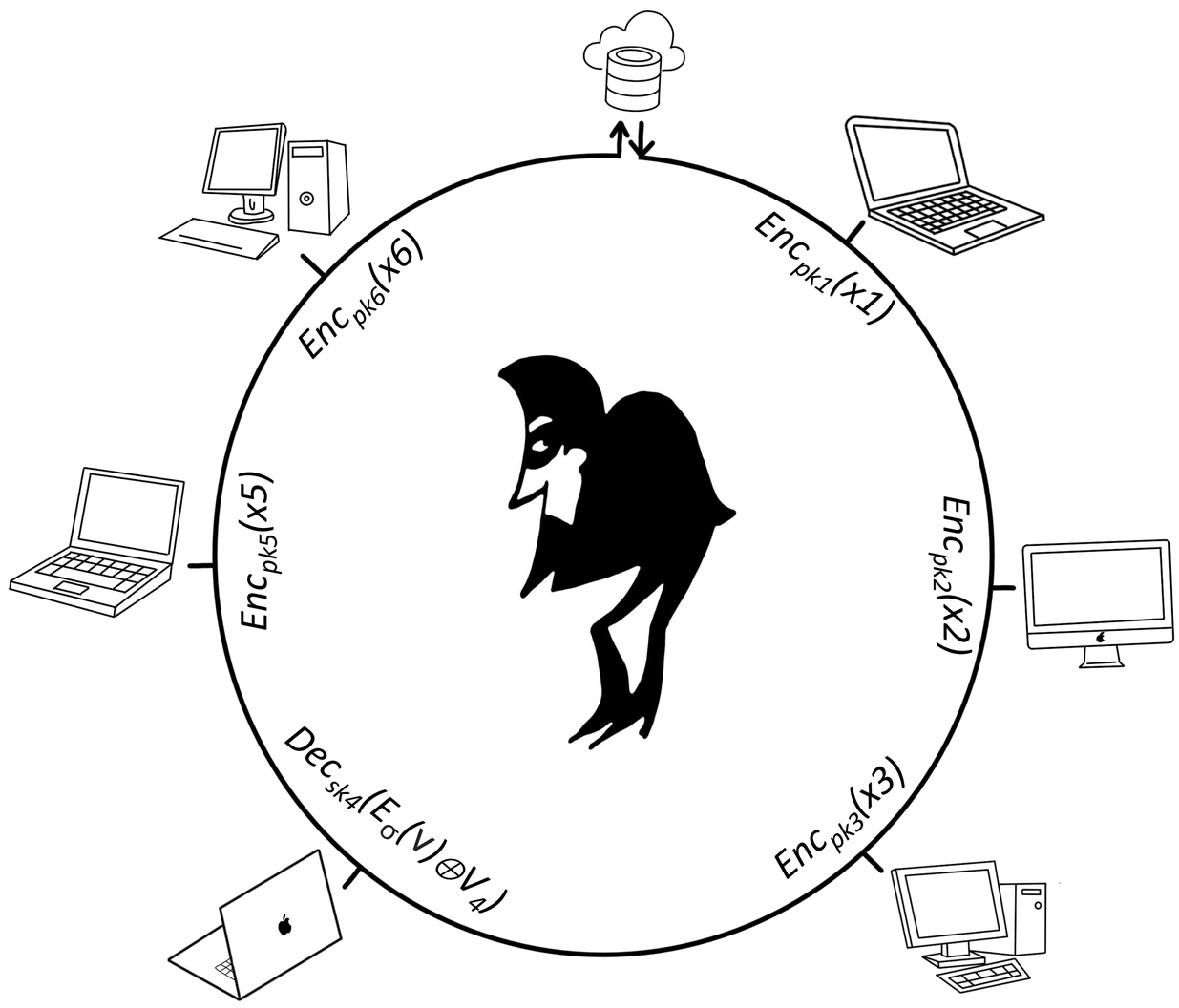
NoName1.0

Anonimowe ankiety kryptograficzne

Motywacja

- Anonimowość w systemach ankietujących oparta jest na obietnicy bez pokrycia.
- Osoby uczestniczące w ankiecie, z obawy przed konsekwencjami, mogą odpowiadać niezgodnie ze swoim przekonaniem.
- Ankieta może być wypełniona przez nieuprawnione osoby lub wypełniona wielokrotnie.

Schemat działania



Oczekiwanie

- Ankietę mogą wypełnić tylko uprawnieni użytkownicy.
- Osoba uprawniona może wypełnić ankietę tylko jeden raz.
- Osoba ewaluującą ankietę może zweryfikować, że wypełniła ją uprawniona osoba.
- Nie jest możliwe zidentyfikowanie osoby, która wypełniła daną ankietę.
- Matematyczny dowód prawdziwości obietnic.

Rozwiązanie

- Wykorzystanie podpisów pierścieniowych.
- Podpis musi należeć do członka ustalonej grupy.
- Brak możliwości ustalenia, do kogo z grupy należy podpis.
- Sprawdzenie podczas podpisywania, czy klucz prywatny użytkownika nie został już wykorzystany.

Opiekun projektu: prof. UAM dr hab. Maciej Grześkowiak

GPL Free Software
Free as in Freedom