DWUDZIESTE TRZECIE FORUM TELEINFORMATYKI®

Ukrywanie danych i obliczeń w chmurze na potrzeby administracji publicznej

Aleksandra Dolot[1], Daniel Waszkiewicz[1], Piotr Sapiecha[1], Michał Andrzejczak[2]

[1] Politechnika Warszawska, WEiTI
[2] Wojskowa Akademia Techniczna, WCY

Szyrowanie homomorficzne

- poufne przetwarzanie danych

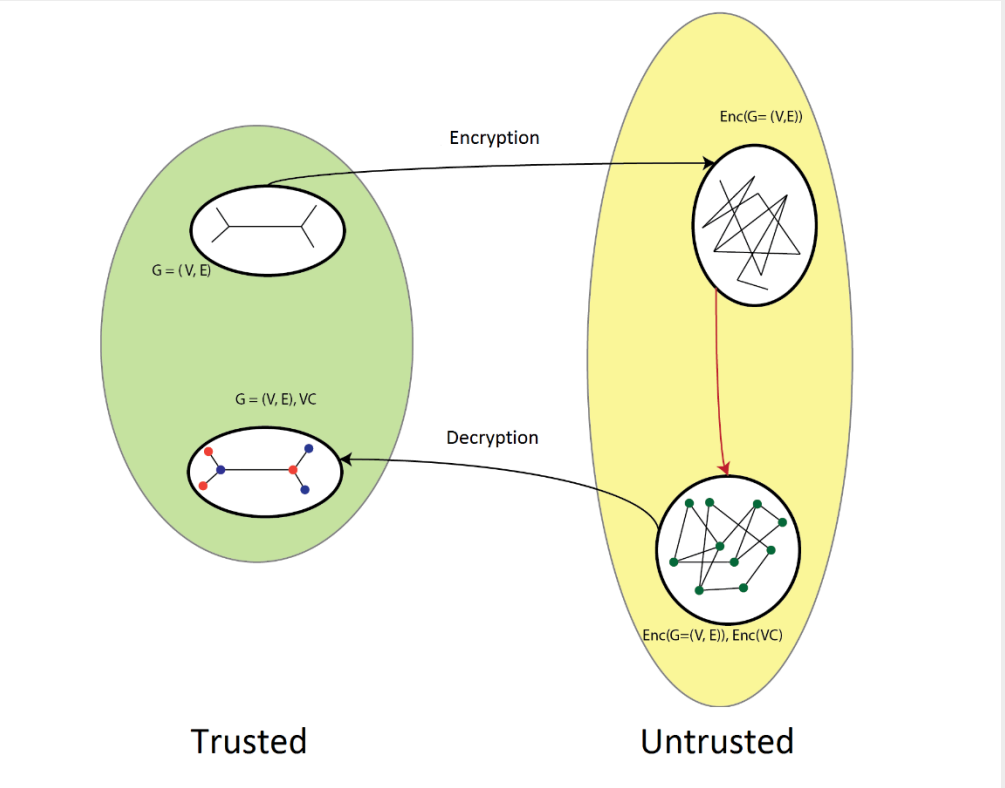
- Rozwój od 2007 roku (systemy fully homomorphic)
- Bazujące na kratach teorioliczbowych
- Kryptosystemy: Fan-Vercauteren, BGV, Regev's LWE
- Dostępne biblioteki: HElib, FV-NFLlib, SEAL
- Badania głównie w kierunku algorytmów grafowych oraz algorytmów szyfrujących

Szyrowanie homomorficzne
- poufne przetwarzanie danych

Schemat działania

Szyfrowanie homomorficzne
jest sposobem szyfrowania umożliwiającym dalsze operacje na uzyskanym szyfrogramie, takie jak dodawanie i mnożenie.

Standardowe algorytmy implementowane są za pomocą kryptosystemów homomorficznych.

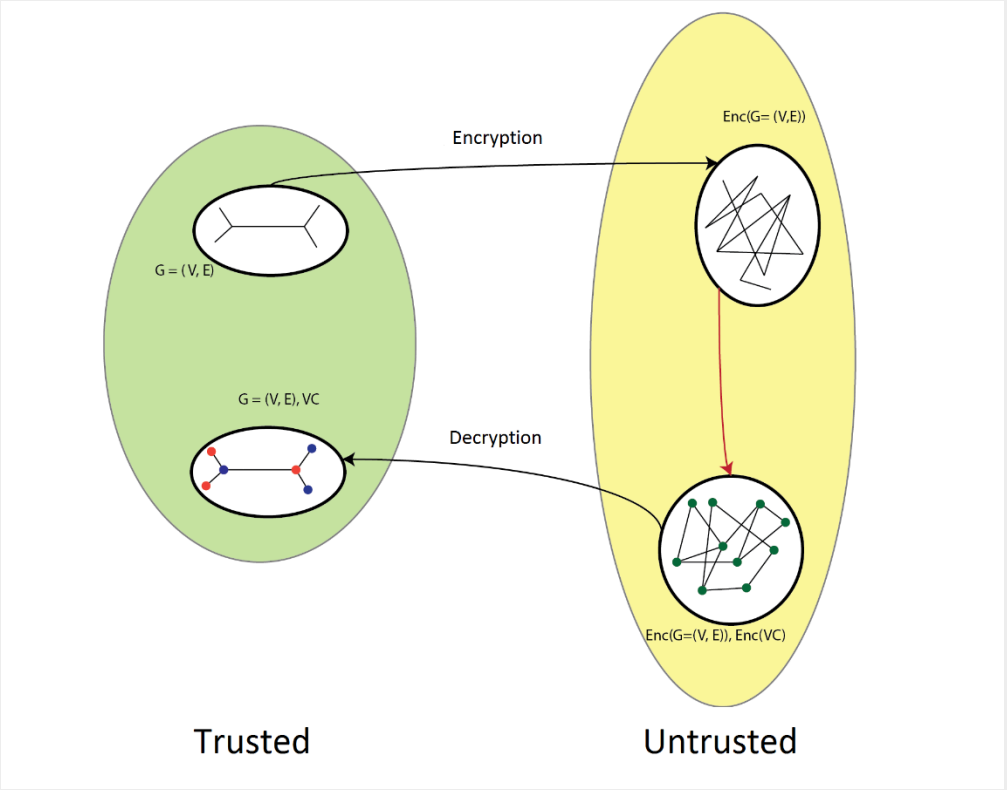


Szyrowanie homomorficzne
- poufne przetwarzanie danych

Schemat wykorzystania

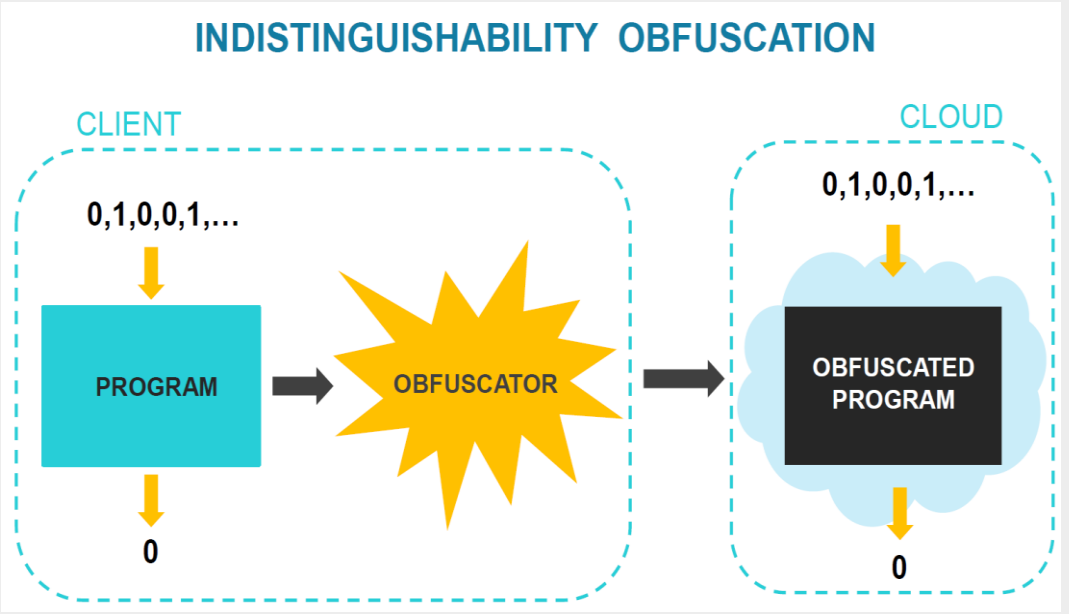
Wykorzystanie
szyfrowania homomorficznego
pozwala wykonywać obliczenia
w niezaufanym środowisku,
bez narażania danych na kompromitację.

Przez niezaufane środowisko można
rozumieć usługi firm zewnętrznych
np. chmury obliczeniowe.



Obfuskacja kryptograficzna
- zaciemnianie obliczeń

- Rozpoczęcie badań ok. 2013 roku
- Bazujące na m. in. kratach teorioliczbowych, mapach wieloliniowych
- Główna idea to ukrycie wykonywanych obliczeń



Obfuskacja kryptograficzna
- zaciemnianie obliczeń

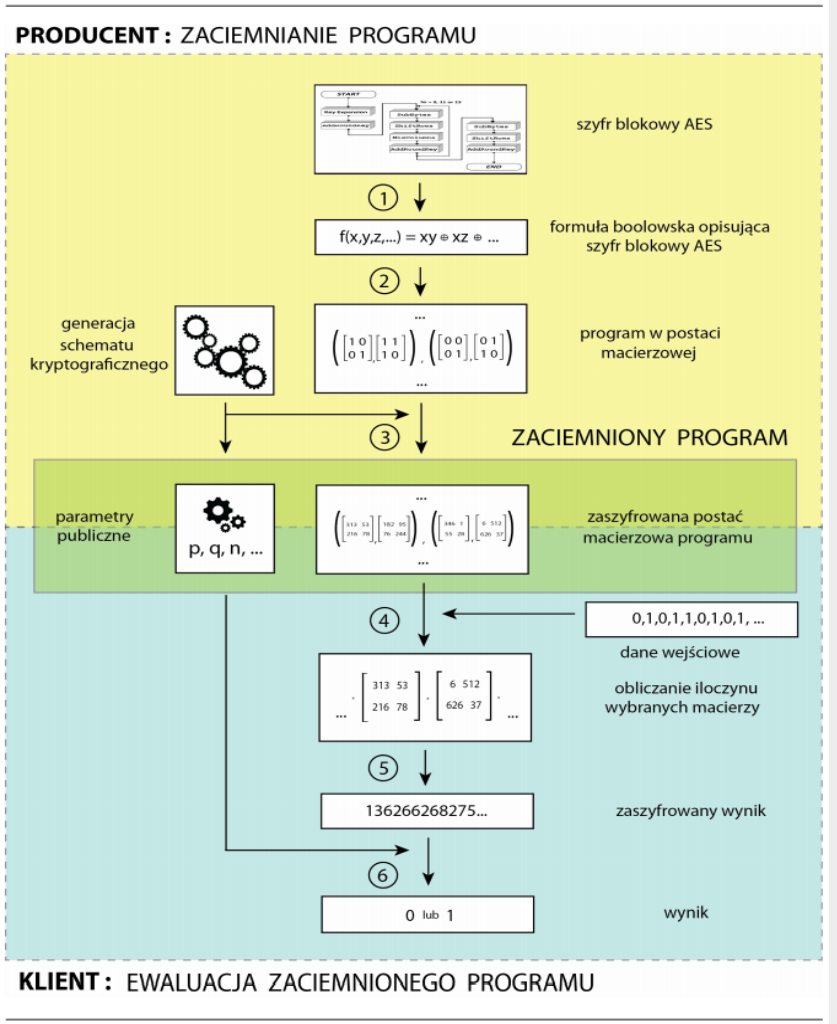
Schemat działania

Obfuskację kryptograficzną wykonuje się w kilku krokach:

1. Przedstawienie programu w postaci formuł boolowskich
2. Przedstawienie formuł w postaci macierzowej
3. Zaszyfrowanie macierzy

Wykonanie programu:
- Obliczanie iloczynu wybranych macierzy,

Zależnych od danych wejściowych
- Odszyfrowanie wyniku

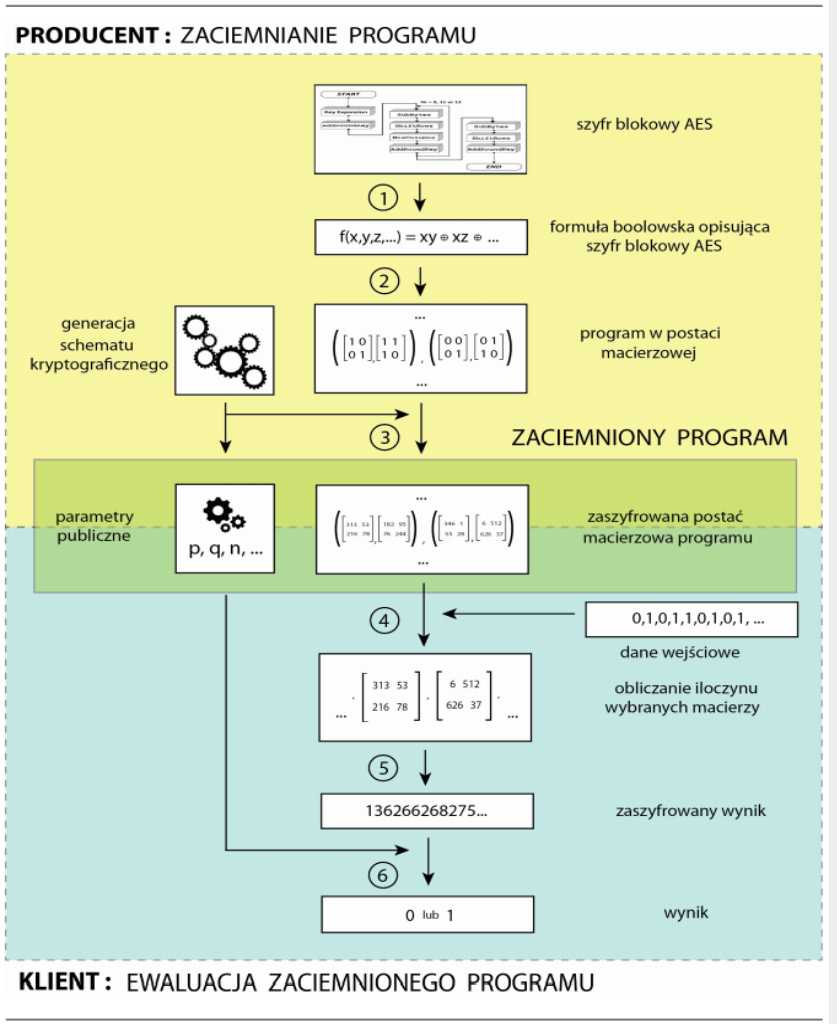


Obfuskacja kryptograficzna
- zaciemnianie obliczeń

Schemat wykorzystania

Wykorzystanie obfuskacji pozwala wykonywać obliczenia na dostępnych danych bez ujawniania samego programu i natury obliczeń, chroniąc tajemnicę przedsiębiorstwa
(np. opracowane i wykorzystywane algorytmy)

Istnieje możliwość zakodowania poufnych danych w ciele programu, bez narażenia na ich ujawnienie (klucze, parametry).

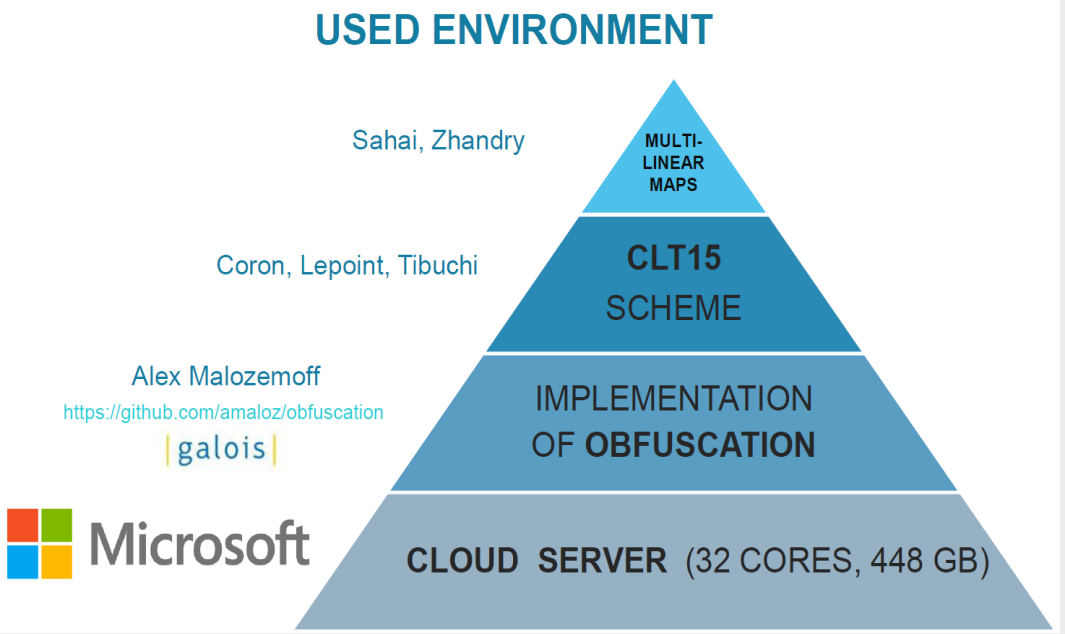


Zastosowanie w administracji publicznej:

Ochrona danych:
- system podatkowy
- dane osobowe
- zarządzanie kryzysowe
- dane publiczne
- dane biomedyczne

Ochrona obliczeń:
- symulacje zagrożeń (klęski, ataki)
- bezpieczna komunikacja

Pierwsze prace:
- Wykorzystanie szyfrowania homomorficznego do poufnego algorytmu pokrycia wierzchołkowego
- Obfuskacja algorytmu szyfrowania mini-AES



Dalsze prace:
- optymalizacja obfuskacji
- implementacja kolejnych algorytmów wykorzystując szyfrowanie homomorficzne

OBFUSCATED MINIAES CIPHER

on security level: 2^6

2 ROUNDS OF MINIAES CIPHER:	WHITEBOX INTERNAL KEY:	WHITEBOX EXTERNAL KEY:	BLACKBOX EXTERNAL KEY:
SIZE OF OBFUSCATED PROGRAM [kB]	11 000	557 000	$\sim 35,7 \cdot 2^{16}$
EVALUATION TIME [s]	11	3 557	$\sim 13\,466 \cdot 2^{16}$
MULTIPLICATIVE COMPLEXITY	9	81	289

Dziękujemy za uwagę!

WYDZIAŁ ELEKTRONIKI
I TECHNIK INFORMACYJNYCH

WYDZIAŁ CYBERNETYKI WAT