Новосибирский Государственный Университет

Факультет Информационных Технологий

Защищенный калькулятор. Разработка клиентского компонента

Яковлев Михаил Олегович

Научный руководитель:
Кренделев Сергей Федорович

Цель исследования

Разработка криптосистемы **полностью гомоморфного шифрования**, т.е. системы шифрования, которая позволяет производить с зашифрованными данными математические операции, такие как:

- умножение
- сложение

Актуальность

Алгоритма полностью гомоморфного шифрования с приемлемой скоростью работы на данный момент не предложено.

Разработка такого алгоритма даст мощный толчок к развитию облачных сервисов, решив вопрос конфиденциальности обрабатываемой информации.

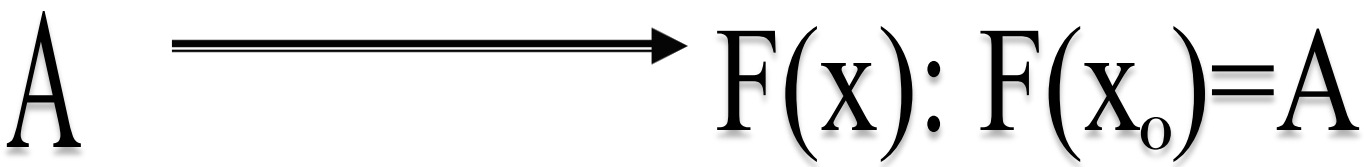
Задачи

- Разработка и совершенствование алгоритмов полностью гомоморфного шифрования
- Реализация алгоритмов в виде клиентского компонента приложения «Защищенный калькулятор»
- Исследование устойчивости алгоритмов к различным видам криптографических атак

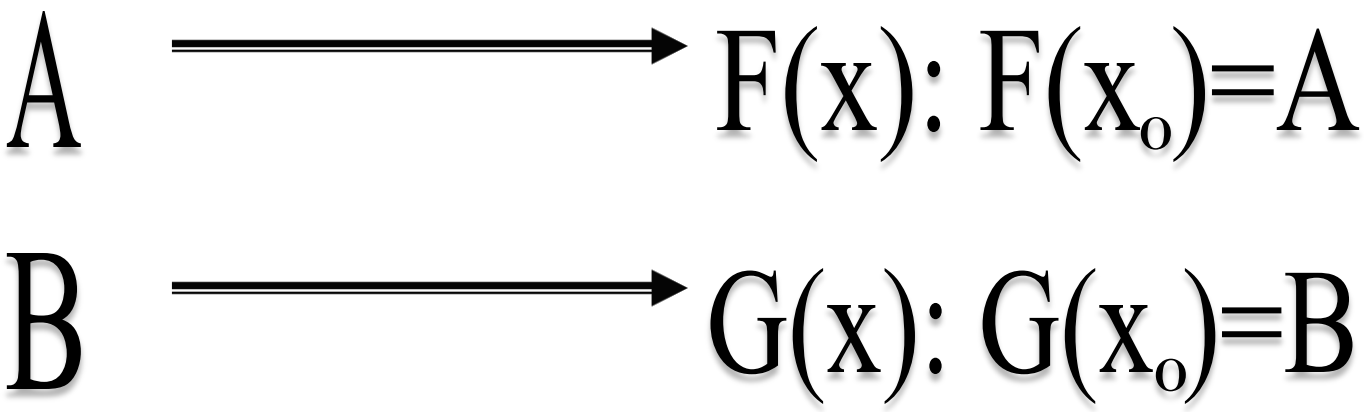
Алгоритм

A

Алгоритм



Алгоритм



Алгоритм

$$A \longrightarrow F(x):\ F(x_o)=A$$

$$B \longrightarrow G(x):\ G(x_o)=B$$

$$H_1(x)=F(x)+G(x);\ H_2(x)=F(x)G(x)$$

$$H_1(x_o)=F(x_o)+G(x_o)=A+B$$

Схема 1

$x_o = \frac{p}{q}$, p и q - целые

F(x) – полином степени n

$G(x) = q^n F(x) – q^n F(x_o) + z,$

где z – шифруемое число

Схема 2

$x_o \in A$;

$U(x)$ – полином, $U(x_o) = 0$;

$G(x) = F(x)U(x) + z$,

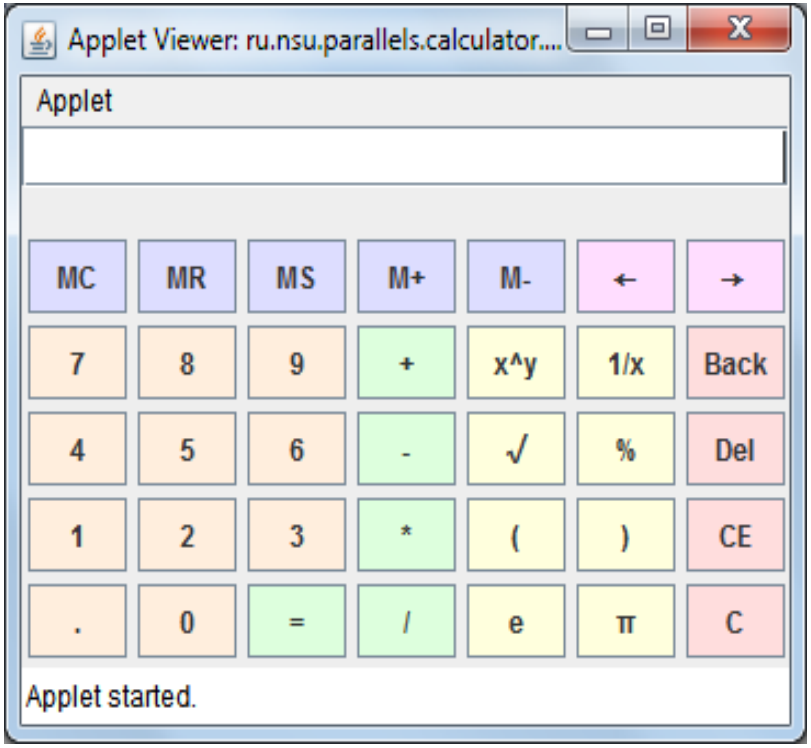
где z – шифруемое число

Защищенный калькулятор

Благодаря свойствам полностью гомоморфного шифрования:

$$f(c_1,.., c_n) = \varphi^{-1}(f(\varphi(c_1), .., \varphi(c_n)))$$

где
φ – функция шифровки,
φ^{-1} – функция дешифровки,
f – вычисляемая функция,
c_1 .. c_n – некоторые константы



Выводы

- Разработаны две схемы полностью гомоморфного шифрования
- Проверены работоспособность и быстродействие схем на практике в режиме реального времени
- Исследована устойчивость схем к криптографическим атакам
- Реализован клиентский компонент приложения «Защищенный калькулятор», выполняющий функции генерации секретного ключа, шифровки и дешифровки

Публикации

- Лихтанский Е.А., Усольцева М.А., Чеботарев С.Е., Яковлев М.О. Защищенный калькулятор // Наука, Технологии, Инновации. Всероссийская научная конференция молодых ученых, 2011 г.
- Лихтанский Е.А., Усольцева М.А., Чеботарев С.Е., Яковлев М.О. Защищенная база данных. Новосибирский государственный университет // 50-я юбилейная международная студенческая конференция «Студент и научно-технический прогресс», 2012 г.
- Защищенные облачные вычисления. Гомоморфное шифрование / С. Кренделев, О. Косырькова, А. Жиров, М. Усольцева, М. Яковлев. – Новосибирск: Лаборатория НГУ-Parallels, 2011. – 7 с.
- Усольцева М.А., Яковлев М.О. Защищенный калькулятор. Новосибирский государственный университет // 51-я международная студенческая конференция “Студент и научно-технический прогресс”, 2013 г.

Новосибирский Государственный Университет

Факультет Информационных Технологий

Защищенный калькулятор. Разработка клиентского компонента

Яковлев Михаил Олегович

Научный руководитель:
Кренделев Сергей Федорович