КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ
ПРОФИ

КАК ОБЕЗОПАСИТЬ ОБЛАЧНЫЕ ВЫЧИСЛЕНИЯ?

Евгений ОСЕТРИН
Университет Иннополис

Развитие облачных решений

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ПРОФИ

Проблемы безопасности облаков

- Отсутствие видимости и контроля
- Теневое ИТ
- Вероятность случайной публикации данных
- Злоумышленная утечка данных
- Искажение или потеря критичных данных
- Несоответствие требованиям регуляторов
- Присутствие облачных вредоносных программ
- Вероятность распространения вредоносного ПО на всю сеть

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
ПРОФИ

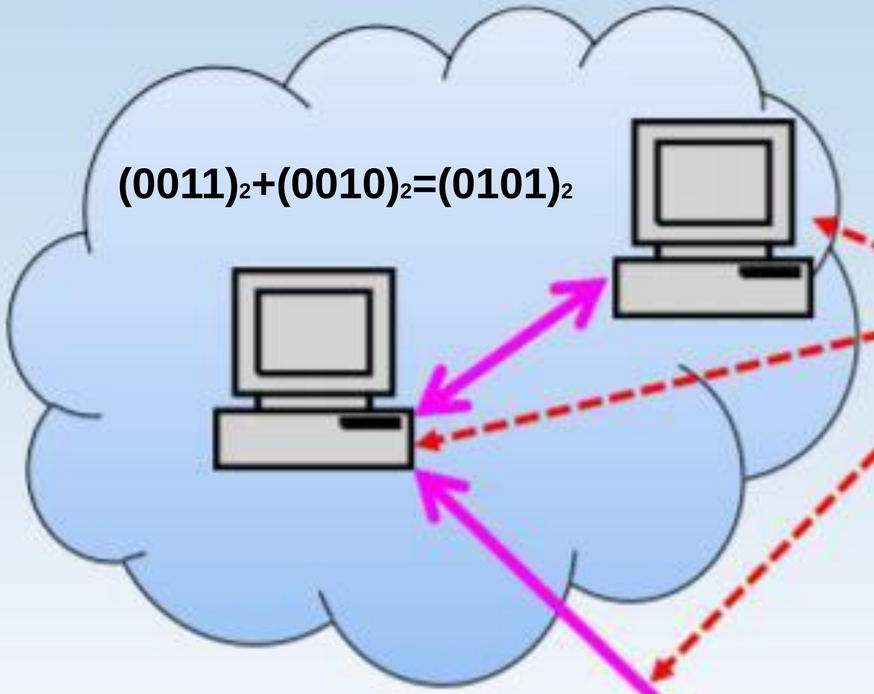
Решения по защите угроз безопасности

Шифрование

Аутентификация
токены

Использование виртуальных
сетей (VPN)

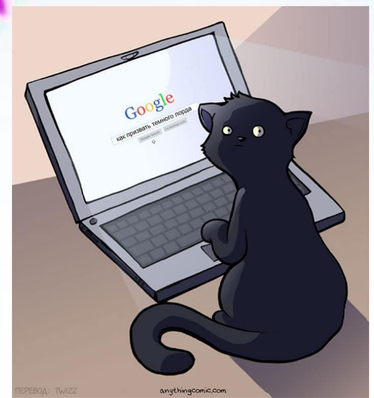
Облачные вычисления



Злоумышленник

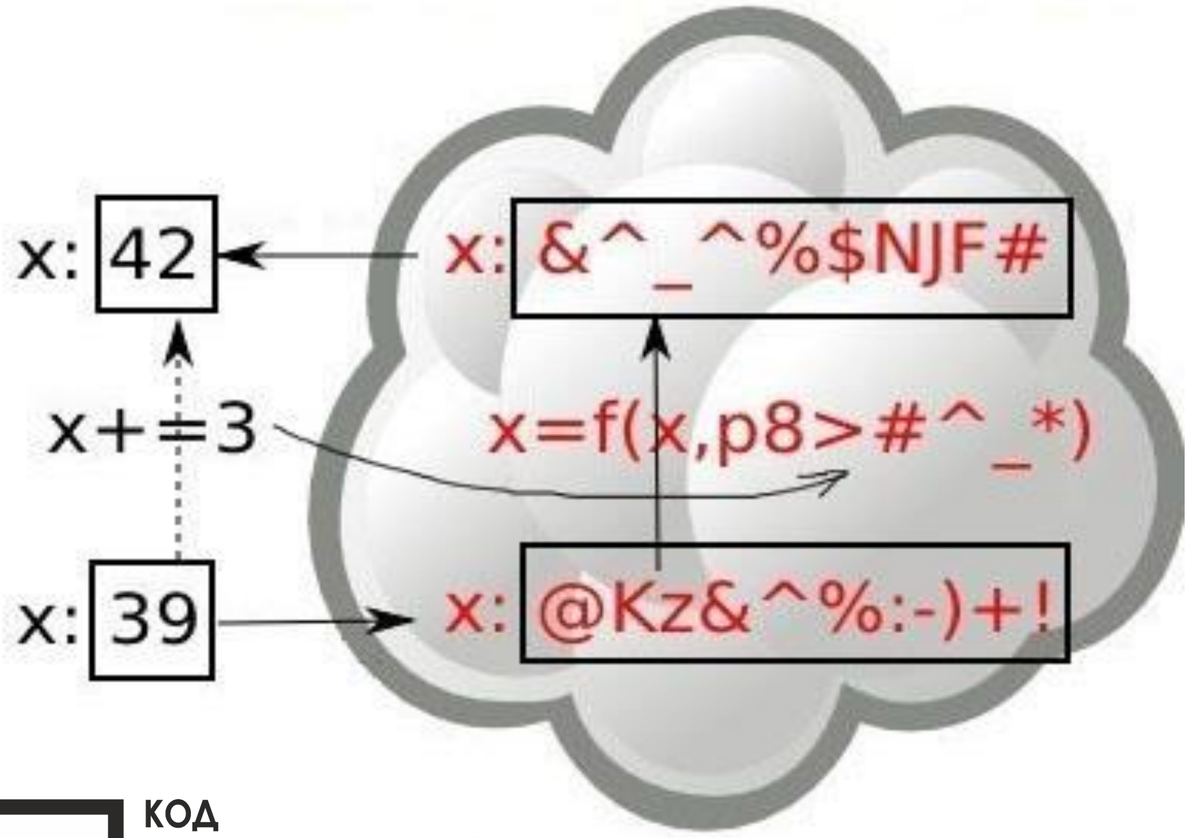
Вот это да!
У кота ИБ 5 лимонов!
Надо его навестить.

$(0011)_2+(0010)_2$



КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
ПРОФИ

Гомоморфное шифрование



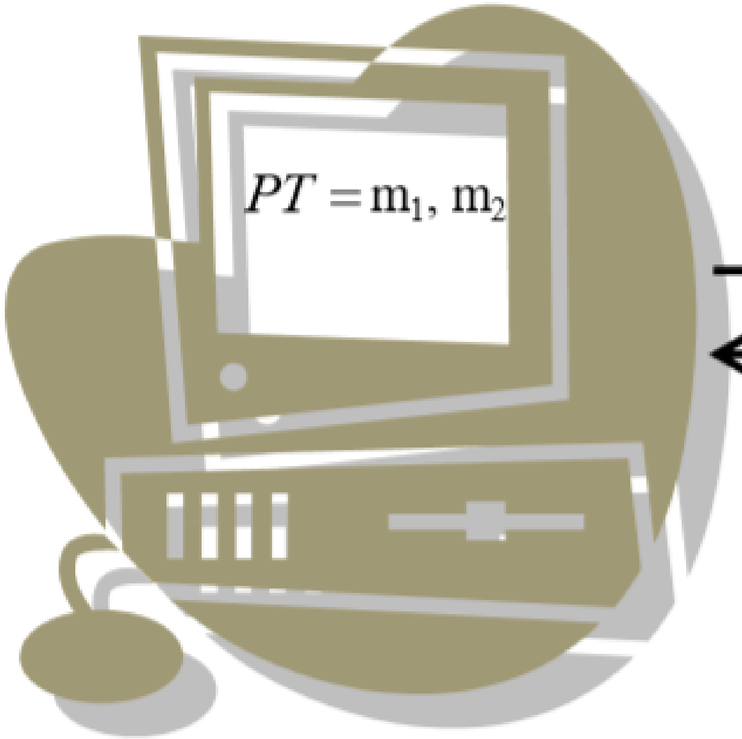
- Это форма шифрования, позволяющая производить математические действия с зашифрованным текстом и получать зашифрованный результат, который при расшифровании равен результату операций, выполненных с открытым текстом

Гомоморфизм – это отображение алгебраической системы, сохраняющее основные операции.

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРОФИ

Генерация ключей

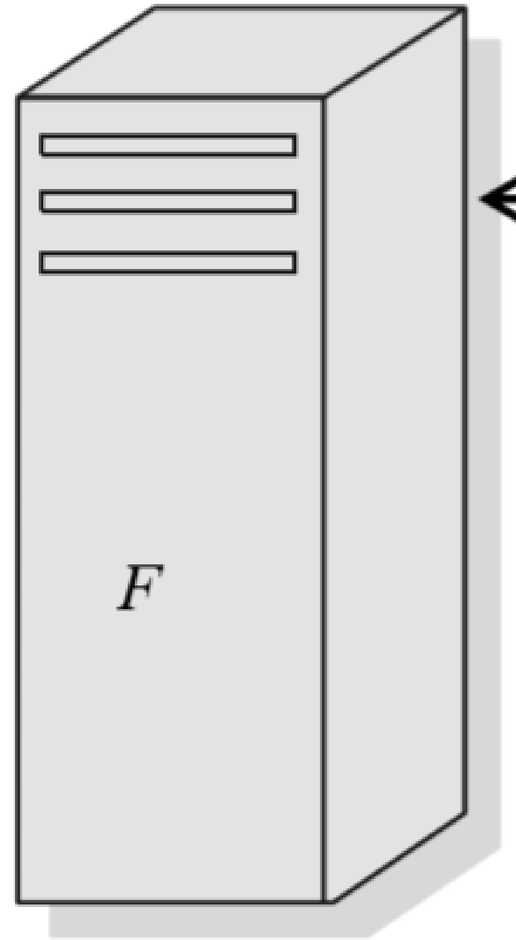
Генерация sk и pk



Шифрование

$(E_{sk}(m_1), E_{sk}(m_2), pk)$

$Y = E(m_1 + m_2)$



Хранилище (база) зашифрованных данных

Дешифрование

$D_{sk}(Y)$

Вычисление

$Eval_{pk}(F, E_{sk}(m_1), E_{sk}(m_2))$

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРОФИ

Результат $D_{sk}(Eval_{pk}(F, E_{sk}(m_1), E_{sk}(m_2)))$

Виды гомоморфного шифрования

Частично гомоморфные схемы

Полностью гомоморфные схемы

$$D(E(m1) \cdot E(m2)) = m1 \cdot m2$$

$$D(E(m1) + E(m2)) = m1 + m2$$

Детерминированные

Вероятностные

Крейг Джентри

Первая возможная конструкция для полностью гомоморфной криптосистемы впервые была предложена в 2009 году.

Схема Джентри поддерживает операции сложения и умножения над шифротекстом

Недостатки схемы Джентри

- наличие возрастающей ошибки в шифрованном тексте

- рост размера шифрованного текста

- трудно реализуема

Известные системы гомоморфного шифрования

- Криптосистема RSA (1977)
- Криптосистема Эль-Гамаля (1985)
- Криптосистема Пэйе (1999)
- Схема Джентри (2009)
- Криптосистема на основе матричных полиномов (2015)

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРОФИ

Оценка производительности криптосистемы на матричных полиномах с использованием параллельных вычислений

Параметр λ	Шифрование	Дешифрование	Умножение шифртекстов
16	4 мс	13мс	8 мс
24	79 мс	13 мс	15 мс
32	1,5 с	14 мс	22 мс
64	2 мин	20 мс	1 с

Оценка производительности модифицированной криптосистемы Джентри

Параметр λ	Шифрование	Дешифрование	Умножение шифртекстов
16	2 мс	6мс	5 мс
24	40 мс	11 мс	12 мс
32	1 с	15 мс	50 мс
64	5 мин	200 мс	10 с

Области применения гомоморфного шифрования

Облачные вычисления

Возможность сохранения целостности, доступности и конфиденциальности данных при их обработке в облачных системах.

Электронное голосование

Система сможет зашифровать голоса избирателей и провести расчеты над зашифрованными данными, сохраняя анонимность избирателей.

Защищенный поиск информации

Сервисы смогут получать и обрабатывать запросы, а также выдавать результаты обработки, не анализируя и не фиксируя их реальное содержание.

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРОФИ

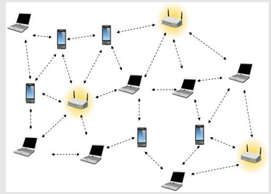
Области применения гомоморфного шифрования

Аутсорсинговые услуги для смарт-карт

Использование внешних устройств хранения и внешних процессоров, более мощных, чем на карте.

Обфускация программ

Возможность гомоморфно зашифровать целиком всю программу так, что она сохранит свою функциональность.

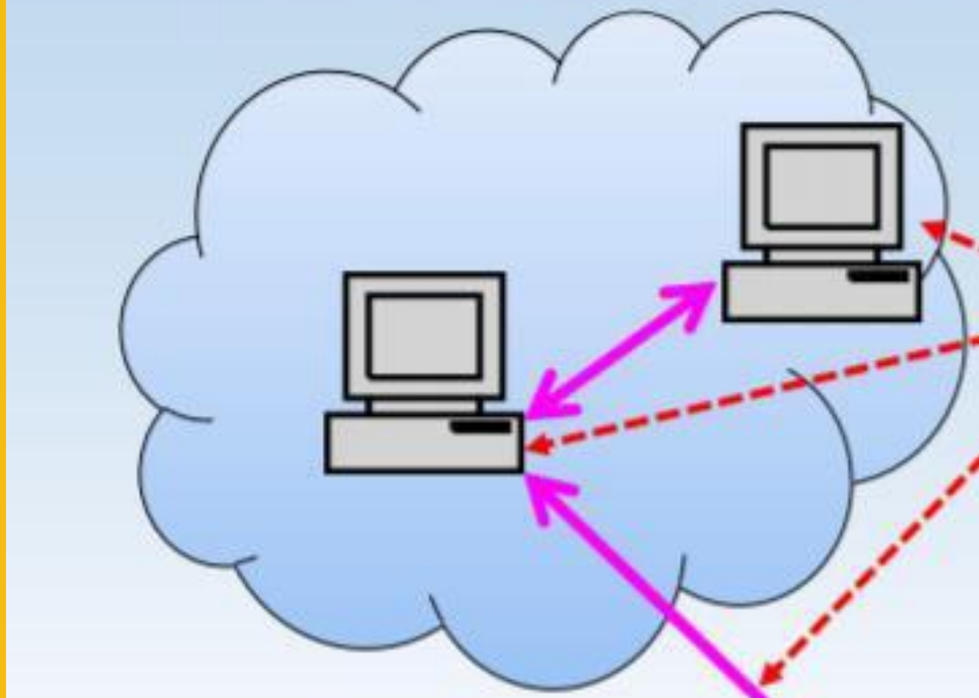


Защита беспроводных децентрализованных сетей связи.

Наличие гомоморфного шифрования не позволяет злоумышленнику найти связь между сообщениями, входящими в узел и выходящими из узла.

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРОФИ

Облачные вычисления



c_1+c_2

(1010110)+(0100011)

Злоумышленник

Ничего не понимаю!
Без секретного ключа не расшифровать.

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ПРОФИ

В заключение

Переход на гомоморфные схемы шифрования поставит на новый уровень защиту облачных вычислений и не только…

#CODEIB

СПАСИБО ЗА ВНИМАНИЕ

e.osetrin@innopolis.ru