Лекция 5. Криптографические примитивы: гомоморфное шифрование

Косолапов Ю.В.

ЮФУ

29 сентября 2020 г.

Содержание

Что-то вроде определения

«Определение»

Гомоморфное шифрование – это такое преобразование данных, которое позволяет *анализировать* зашифрованные данные или/и выполнять над ними *арифметические действия* так, как если бы анализировались незашифрованные данные или выполнялись арифметические действия над незашифрованными данными.

Что-то вроде определения

«Определение»

Гомоморфное шифрование – это такое преобразование данных, которое позволяет *анализировать* зашифрованные данные или/и выполнять над ними *арифметические действия* так, как если бы анализировались незашифрованные данные или выполнялись арифметические действия над незашифрованными данными.

- **Анализировать** — например, производить поиск данных в **шифртексте**

Что-то вроде определения

«Определение»

Гомоморфное шифрование – это такое преобразование данных, которое позволяет *анализировать* зашифрованные данные или/и выполнять над ними *арифметические действия* так, как если бы анализировались незашифрованные данные или выполнялись арифметические действия над незашифрованными данными.

- **Анализировать** — например, производить поиск данных в **шифртексте**
- **Арифметические действия** — складывать, умножать **шифртекст**

Для чего это нужно?

Пример 1[1]

[1] https://searchsecurity.techtarget.com/definition/homomorphic-encryption

Для чего это нужно?

Пример 1[1]

- Компания X имеет очень секретные данные $A = 10$ и $B = 20$.

[1] https://searchsecurity.techtarget.com/definition/homomorphic-encryption

Для чего это нужно?

Пример 1[1]

- Компания X имеет очень секретные данные $A = 10$ и $B = 20$.
- Компания X не может сама эти данные обрабатывать и хранить, поэтому решила передать хранение и обработку в облако O;

[1] https://searchsecurity.techtarget.com/definition/homomorphic-encryption

Для чего это нужно?

Пример 1[1]

- Компания X имеет очень секретные данные $A = 10$ и $B = 20$.
- Компания X не может сама эти данные обрабатывать и хранить, поэтому решила передать хранение и обработку в облако O;
- Но так как данные секретные, то предварительно данные зашифровала, умножив каждое из чисел на $K = 2$. Таким образом, в обдаке будут храниться два шифртекста: $C_A = 20$ и $C_B = 40$.

[1] https://searchsecurity.techtarget.com/definition/homomorphic-encryption

Для чего это нужно?

Пример 1[1]

- Компания X имеет очень секретные данные $A = 10$ и $B = 20$.
- Компания X не может сама эти данные обрабатывать и хранить, поэтому решила передать хранение и обработку в облако O;
- Но так как данные секретные, то предварительно данные зашифровала, умножив каждое из чисел на $K = 2$. Таким образом, в обдаке будут храниться два шифртекста: $C_A = 20$ и $C_B = 40$.
- Через год контролирующее агентство Y запросило у X сумму $A + B$ для проверки деятельности компании.

[1] https://searchsecurity.techtarget.com/definition/homomorphic-encryption

Для чего это нужно?

Пример 1[1]

- Компания X имеет очень секретные данные $A = 10$ и $B = 20$.
- Компания X не может сама эти данные обрабатывать и хранить, поэтому решила передать хранение и обработку в облако O;
- Но так как данные секретные, то предварительно данные зашифровала, умножив каждое из чисел на $K = 2$. Таким образом, в обдаке будут храниться два шифртекста: $C_A = 20$ и $C_B = 40$.
- Через год контролирующее агентство Y запросило у X сумму $A + B$ для проверки деятельности компании.
- Компания X сама не может выполнить эту операцию (не хватает вычислительных ресурсов), поэтому просит сделать это облако O.

[1] https://searchsecurity.techtarget.com/definition/homomorphic-encryption

Для чего это нужно?

Пример 1[1]

- Компания X имеет очень секретные данные $A = 10$ и $B = 20$.
- Компания X не может сама эти данные обрабатывать и хранить, поэтому решила передать хранение и обработку в облако O;
- Но так как данные секретные, то предварительно данные зашифровала, умножив каждое из чисел на $K = 2$. Таким образом, в обдаке будут храниться два шифртекста: $C_A = 20$ и $C_B = 40$.
- Через год контролирующее агентство Y запросило у X сумму $A + B$ для проверки деятельности компании.
- Компания X сама не может выполнить эту операцию (не хватает вычислительных ресурсов), поэтому просит сделать это облако O.
- Облако O вычисляет $C_A + C_B = 60$ и возвращает это число компании X;

[1] https://searchsecurity.techtarget.com/definition/homomorphic-encryption

Для чего это нужно?

Пример 1[1]

- Компания X имеет очень секретные данные $A = 10$ и $B = 20$.
- Компания X не может сама эти данные обрабатывать и хранить, поэтому решила передать хранение и обработку в облако O;
- Но так как данные секретные, то предварительно данные зашифровала, умножив каждое из чисел на $K = 2$. Таким образом, в обдаке будут храниться два шифртекста: $C_A = 20$ и $C_B = 40$.
- Через год контролирующее агентство Y запросило у X сумму $A + B$ для проверки деятельности компании.
- Компания X сама не может выполнить эту операцию (не хватает вычислительных ресурсов), поэтому просит сделать это облако O.
- Облако O вычисляет $C_A + C_B = 60$ и возвращает это число компании X;
- Компания X делит полученное число на $K = 2$ и передает полученное значение 30 агентству Y.

[1] https://searchsecurity.techtarget.com/definition/homomorphic-encryption

Для чего это нужно?

Пример 2 [2]

[2] Graepel T., Lauter K., Naehrig M. (2013) ML Confidential: Machine Learning on Encrypted Data. In: Kwon T., Lee MK., Kwon D. (eds) Information Security and Cryptology – ICISC 2012. ICISC 2012. Lecture Notes in Computer Science, vol 7839. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-37682-5_1

Для чего это нужно?

Пример 2 [2]

- Облачный сервис X имеет возможность по набору характеристик (возраст, город проживания, заработная плата, образование и т.п.) физического лица определить, вернет ли этот клиент кредит (0 – вернет, 1 – не вернет).

[2] Graepel T., Lauter K., Naehrig M. (2013) ML Confidential: Machine Learning on Encrypted Data. In: Kwon T., Lee MK., Kwon D. (eds) Information Security and Cryptology – ICISC 2012. ICISC 2012. Lecture Notes in Computer Science, vol 7839. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-37682-5_1

Для чего это нужно?

Пример 2 [2]

- Облачный сервис X имеет возможность по набору характеристик (возраст, город проживания, заработная плата, образование и т.п.) физического лица определить, вернет ли этот клиент кредит (0 – вернет, 1 – не вернет).
- Решение принимается путем *вычисления математической функции* $F()$, зависящей от набора признаков-характеристик.

[2] Graepel T., Lauter K., Naehrig M. (2013) ML Confidential: Machine Learning on Encrypted Data. In: Kwon T., Lee MK., Kwon D. (eds) Information Security and Cryptology – ICISC 2012. ICISC 2012. Lecture Notes in Computer Science, vol 7839. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-37682-5_1

Для чего это нужно?

Пример 2 [2]

- Облачный сервис X имеет возможность по набору характеристик (возраст, город проживания, заработная плата, образование и т.п.) физического лица определить, вернет ли этот клиент кредит (0 – вернет, 1 – не вернет).
- Решение принимается путем *вычисления математической функции* $F()$, зависящей от набора признаков-характеристик.
- Владельцы сервиса X (банк B) потратили много средств, чтобы добиться высокой точности предсказания.

[2] Graepel T., Lauter K., Naehrig M. (2013) ML Confidential: Machine Learning on Encrypted Data. In: Kwon T., Lee MK., Kwon D. (eds) Information Security and Cryptology – ICISC 2012. ICISC 2012. Lecture Notes in Computer Science, vol 7839. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-37682-5_1

Для чего это нужно?

Пример 2 [2]

- Облачный сервис X имеет возможность по набору характеристик (возраст, город проживания, заработная плата, образование и т.п.) физического лица определить, вернет ли этот клиент кредит (0 – вернет, 1 – не вернет).
- Решение принимается путем *вычисления математической функции* $F()$, зависящей от набора признаков-характеристик.
- Владельцы сервиса X (банк B) потратили много средств, чтобы добиться высокой точности предсказания.
- Потенциальный клиент хочет проверить, выдаст ли ему банк кредит. Для этого он может воспользоваться сервисом X, передав вектор своих характеристик $\mathbf{a}$.

[2] Graepel T., Lauter K., Naehrig M. (2013) ML Confidential: Machine Learning on Encrypted Data. In: Kwon T., Lee MK., Kwon D. (eds) Information Security and Cryptology – ICISC 2012. ICISC 2012. Lecture Notes in Computer Science, vol 7839. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-37682-5_1

Для чего это нужно?

Пример 2 [2]

- Облачный сервис X имеет возможность по набору характеристик (возраст, город проживания, заработная плата, образование и т.п.) физического лица определить, вернет ли этот клиент кредит (0 – вернет, 1 – не вернет).
- Решение принимается путем *вычисления математической функции* $F()$, зависящей от набора признаков-характеристик.
- Владельцы сервиса X (банк B) потратили много средств, чтобы добиться высокой точности предсказания.
- Потенциальный клиент хочет проверить, выдаст ли ему банк кредит. Для этого он может воспользоваться сервисом X, передав вектор своих характеристик $\mathbf{a}$.
- Но клиент не хочет передавать свои данные банку в открытом виде, поэтому он шифрует вектор своих данных $\mathbf{a}$ в $\mathbf{c}_a$ и передает $\mathbf{c}_a$ сервису.

[2] Graepel T., Lauter K., Naehrig M. (2013) ML Confidential: Machine Learning on Encrypted Data. In: Kwon T., Lee MK., Kwon D. (eds) Information Security and Cryptology – ICISC 2012. ICISC 2012. Lecture Notes in Computer Science, vol 7839. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-37682-5_1

Для чего это нужно?

Пример 2 [2]

- Облачный сервис X имеет возможность по набору характеристик (возраст, город проживания, заработная плата, образование и т.п.) физического лица определить, вернет ли этот клиент кредит (0 – вернет, 1 – не вернет).
- Решение принимается путем *вычисления математической функции* $F()$, зависящей от набора признаков-характеристик.
- Владельцы сервиса X (банк B) потратили много средств, чтобы добиться высокой точности предсказания.
- Потенциальный клиент хочет проверить, выдаст ли ему банк кредит. Для этого он может воспользоваться сервисом X, передав вектор своих характеристик $\mathbf{a}$.
- Но клиент не хочет передавать свои данные банку в открытом виде, поэтому он шифрует вектор своих данных $\mathbf{a}$ в $\mathbf{c}_a$ и передает $\mathbf{c}_a$ сервису.
- Сервис X должен уметь работать с зашифрованными данными. Он вычисляет $F(\mathbf{c}_a) = C$.

[2] Graepel T., Lauter K., Naehrig M. (2013) ML Confidential: Machine Learning on Encrypted Data. In: Kwon T., Lee MK., Kwon D. (eds) Information Security and Cryptology – ICISC 2012. ICISC 2012. Lecture Notes in Computer Science, vol 7839. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-37682-5_1

Для чего это нужно?

Пример 2 [2]

- Облачный сервис X имеет возможность по набору характеристик (возраст, город проживания, заработная плата, образование и т.п.) физического лица определить, вернет ли этот клиент кредит (0 – вернет, 1 – не вернет).
- Решение принимается путем *вычисления математической функции* $F()$, зависящей от набора признаков-характеристик.
- Владельцы сервиса X (банк B) потратили много средств, чтобы добиться высокой точности предсказания.
- Потенциальный клиент хочет проверить, выдаст ли ему банк кредит. Для этого он может воспользоваться сервисом X, передав вектор своих характеристик $\mathbf{a}$.
- Но клиент не хочет передавать свои данные банку в открытом виде, поэтому он шифрует вектор своих данных $\mathbf{a}$ в $\mathbf{c}_a$ и передает $\mathbf{c}_a$ сервису.
- Сервис X должен уметь работать с зашифрованными данными. Он вычисляет $F(\mathbf{c}_a) = C$.
- Клиент расшифровывает C и проверяет, что получилось: 0 или 1.

[2] Graepel T., Lauter K., Naehrig M. (2013) ML Confidential: Machine Learning on Encrypted Data. In: Kwon T., Lee MK., Kwon D. (eds) Information Security and Cryptology – ICISC 2012. ICISC 2012. Lecture Notes in Computer Science, vol 7839. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-37682-5_1

Почти строгое определение

Почти строгое определение

Первый способ:

$$E_k(a \cdot b) \sim E_k(a) \bullet E_k(b),$$

$$E_k(a + b) \sim E_k(a) \uplus E_k(b)$$

Почти строгое определение

Первый способ:

$$E_k(a \cdot b) \sim E_k(a) \bullet E_k(b),$$

$$E_k(a + b) \sim E_k(a) \uplus E_k(b)$$

Второй способ:

$$D_k(c_1 \bullet c_2) \sim D_k(c_1) \cdot D_k(c_2),$$

$$D_k(c_1 \uplus c_2) \sim D_k(c_1) + D_k(c_2)$$

Почти строгое определение

Первый способ:

$$E_k(a \cdot b) \sim E_k(a) \bullet E_k(b),$$

$$E_k(a + b) \sim E_k(a) \uplus E_k(b)$$

Второй способ:

$$D_k(c_1 \bullet c_2) \sim D_k(c_1) \cdot D_k(c_2),$$

$$D_k(c_1 \uplus c_2) \sim D_k(c_1) + D_k(c_2)$$

Важно! (1)

Операции $+$ и $\cdot$ — это обычные арифметические операции, а $\bullet$ и $\uplus$ — это соответствующие операции над шифртекстом (иногда они другие!). Например, операция $\bullet$ может реализовываться путем тензорного умножения шифрограмм с последующей проекцией вектора на заданное множество.

Почти строгое определение

Первый способ:

$$E_k(a \cdot b) \sim E_k(a) \bullet E_k(b),$$

$$E_k(a + b) \sim E_k(a) \uplus E_k(b)$$

Второй способ:

$$D_k(c_1 \bullet c_2) \sim D_k(c_1) \cdot D_k(c_2),$$

$$D_k(c_1 \uplus c_2) \sim D_k(c_1) + D_k(c_2)$$

Важно! (1)

Операции $+$ и $\cdot$ — это обычные арифметические операции, а $\bullet$ и $\uplus$ — это соответствующие операции над шифртекстом (иногда они другие!). Например, операция $\bullet$ может реализовываться путем тензорного умножения шифрограмм с последующей проекцией вектора на заданное множество.

Важно! (2)

Вместо $+$ может быть, например, операция побитового сложения $\oplus$ (xor)

DEMO

Пример симметричного гомоморфного шифрования [3]

[3] несколько модифицированная версия van Dijk M., Gentry C., Halevi S., Vaikuntanathan V. (2010) Fully Homomorphic Encryption over the Integers. In: Gilbert H. (eds) Advances in Cryptology – EUROCRYPT 2010. EUROCRYPT 2010. Lecture Notes in Computer Science, vol 6110. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-13190-5_2

Пример симметричного гомоморфного шифрования [3]

- Корреспонденты A и B договариваются об общем секретном ключе $k \in 2\mathbb{N} + 1$ (нечетные числа, большие 1).

[3] несколько модифицированная версия van Dijk M., Gentry C., Halevi S., Vaikuntanathan V. (2010) Fully Homomorphic Encryption over the Integers. In: Gilbert H. (eds) Advances in Cryptology – EUROCRYPT 2010. EUROCRYPT 2010. Lecture Notes in Computer Science, vol 6110. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-13190-5_2

Пример симметричного гомоморфного шифрования [3]

- Корреспонденты A и B договариваются об общем секретном ключе $k \in 2\mathbb{N} + 1$ (нечетные числа, большие 1).
- Сообщение: $m \in \{0, 1\}$ (один бит).

[3] несколько модифицированная версия van Dijk M., Gentry C., Halevi S., Vaikuntanathan V. (2010) Fully Homomorphic Encryption over the Integers. In: Gilbert H. (eds) Advances in Cryptology – EUROCRYPT 2010. EUROCRYPT 2010. Lecture Notes in Computer Science, vol 6110. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-13190-5_2

Пример симметричного гомоморфного шифрования [3]

- Корреспонденты A и B договариваются об общем секретном ключе $k \in 2\mathbb{N} + 1$ (нечетные числа, большие 1).
- Сообщение: $m \in \{0, 1\}$ (один бит).
- Шифрование:

[3] несколько модифицированная версия van Dijk M., Gentry C., Halevi S., Vaikuntanathan V. (2010) Fully Homomorphic Encryption over the Integers. In: Gilbert H. (eds) Advances in Cryptology – EUROCRYPT 2010. EUROCRYPT 2010. Lecture Notes in Computer Science, vol 6110. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-13190-5_2

Пример симметричного гомоморфного шифрования [3]

- Корреспонденты A и B договариваются об общем секретном ключе $k \in 2\mathbb{N} + 1$ (нечетные числа, большие 1).
- Сообщение: $m \in \{0, 1\}$ (один бит).
- Шифрование:
  - Случайным образом выбираются параметры $q, r (\in \mathbb{Z})$ такие, что $|r| < \lfloor \sqrt{k-1}/2 \rfloor - 1$, число r еще называется «шумом».

[3] несколько модифицированная версия van Dijk M., Gentry C., Halevi S., Vaikuntanathan V. (2010) Fully Homomorphic Encryption over the Integers. In: Gilbert H. (eds) Advances in Cryptology – EUROCRYPT 2010. EUROCRYPT 2010. Lecture Notes in Computer Science, vol 6110. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-13190-5_2

Пример симметричного гомоморфного шифрования [3]

- Корреспонденты A и B договариваются об общем секретном ключе $k \in 2\mathbb{N} + 1$ (нечетные числа, большие 1).
- Сообщение: $m \in \{0, 1\}$ (один бит).
- Шифрование:
  - Случайным образом выбираются параметры $q, r (\in \mathbb{Z})$ такие, что $|r| < \lfloor \sqrt{k-1}/2 \rfloor - 1$, число r еще называется «шумом».
  - Зашифрованное сообщение:

$$c = m + q \cdot k + 2 \cdot r.$$

- Расшифрование:

[3] несколько модифицированная версия van Dijk M., Gentry C., Halevi S., Vaikuntanathan V. (2010) Fully Homomorphic Encryption over the Integers. In: Gilbert H. (eds) Advances in Cryptology – EUROCRYPT 2010. EUROCRYPT 2010. Lecture Notes in Computer Science, vol 6110. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-13190-5_2

Пример симметричного гомоморфного шифрования [3]

- Корреспонденты A и B договариваются об общем секретном ключе $k \in 2\mathbb{N}+1$ (нечетные числа, большие 1).
- Сообщение: $m \in \{0,1\}$ (один бит).
- Шифрование:
  - Случайным образом выбираются параметры $q, r(\in \mathbb{Z})$ такие, что $|r| < \lfloor \sqrt{k-1}/2 \rfloor - 1$, число r еще называется «шумом».
  - Зашифрованное сообщение:

$$c = m + q \cdot k + 2 \cdot r.$$

- Расшифрование:
  - Находится представитель $\tilde{m} = c(\mathrm{mod} k)$, $\tilde{m} \in \{0, ..., k-1\}$;

[3] несколько модифицированная версия van Dijk M., Gentry C., Halevi S., Vaikuntanathan V. (2010) Fully Homomorphic Encryption over the Integers. In: Gilbert H. (eds) Advances in Cryptology – EUROCRYPT 2010. EUROCRYPT 2010. Lecture Notes in Computer Science, vol 6110. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-13190-5_2

Пример симметричного гомоморфного шифрования [3]

- Корреспонденты A и B договариваются об общем секретном ключе $k \in 2\mathbb{N}+1$ (нечетные числа, большие 1).
- Сообщение: $m \in \{0,1\}$ (один бит).
- Шифрование:
  - Случайным образом выбираются параметры $q, r(\in \mathbb{Z})$ такие, что $|r| < \lfloor\sqrt{k-1}/2\rfloor - 1$, число r еще называется «шумом».
  - Зашифрованное сообщение:

$$c = m + q \cdot k + 2 \cdot r.$$

- Расшифрование:
  - Находится представитель $\tilde{m} = c(\mathrm{mod} k)$, $\tilde{m} \in \{0, ..., k-1\}$;
  - Находится $m = \tilde{m}(\mathrm{mod} 2)$:

$$m = (c(\mathrm{mod} k))(\mathrm{mod} 2).$$

[3] несколько модифицированная версия van Dijk M., Gentry C., Halevi S., Vaikuntanathan V. (2010) Fully Homomorphic Encryption over the Integers. In: Gilbert H. (eds) Advances in Cryptology – EUROCRYPT 2010. EUROCRYPT 2010. Lecture Notes in Computer Science, vol 6110. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-13190-5_2

Пример симметричного гомоморфного шифрования [3]

- Корреспонденты A и B договариваются об общем секретном ключе $k \in 2\mathbb{N}+1$ (нечетные числа, большие 1).
- Сообщение: $m \in \{0,1\}$ (один бит).
- Шифрование:
  - Случайным образом выбираются параметры $q, r(\in \mathbb{Z})$ такие, что $|r| < \lfloor\sqrt{k-1}/2\rfloor - 1$, число r еще называется «шумом».
  - Зашифрованное сообщение:

$$c = m + q \cdot k + 2 \cdot r.$$

- Расшифрование:
  - Находится представитель $\tilde{m} = c(\mathrm{mod} k)$, $\tilde{m} \in \{0, ..., k-1\}$;
  - Находится $m = \tilde{m}(\mathrm{mod} 2)$:

$$m = (c(\mathrm{mod} k))(\mathrm{mod} 2).$$

Вопрос

Почему число k выбирается нечетным?

[3] несколько модифицированная версия van Dijk M., Gentry C., Halevi S., Vaikuntanathan V. (2010) Fully Homomorphic Encryption over the Integers. In: Gilbert H. (eds) Advances in Cryptology – EUROCRYPT 2010. EUROCRYPT 2010. Lecture Notes in Computer Science, vol 6110. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-13190-5_2

Проверка гомоморфности сложения и умножения

Проверка гомоморфности сложения и умножения

- Сложение:

$$\begin{aligned} c_1 + c_2 &= (m_1 + q_1 \cdot k + 2 \cdot r_1) + (m_2 + q_2 \cdot k + 2 \cdot r_2) \\ &= (m_1 + m_2) + (q_1 + q_2) \cdot k + 2 \cdot (r_1 + r_2) \end{aligned}$$

Проверка гомоморфности сложения и умножения

- Сложение:

$$\begin{aligned} c_1 + c_2 &= (m_1 + q_1 \cdot k + 2 \cdot r_1) + (m_2 + q_2 \cdot k + 2 \cdot r_2) \\ &= (m_1 + m_2) + (q_1 + q_2) \cdot k + 2 \cdot (r_1 + r_2) \end{aligned}$$

(помним, что $|r| < \lfloor \sqrt{k-1}/2 \rfloor - 1$)

Проверка гомоморфности сложения и умножения

- Сложение:

$$\begin{aligned} c_1 + c_2 &= (m_1 + q_1 \cdot k + 2 \cdot r_1) + (m_2 + q_2 \cdot k + 2 \cdot r_2) \\ &= (m_1 + m_2) + (q_1 + q_2) \cdot k + 2 \cdot (r_1 + r_2) \end{aligned}$$

(помним, что $|r| < \lfloor \sqrt{k-1}/2 \rfloor - 1$)

- Умножение:

$$\begin{aligned} c_1 \cdot c_2 &= (m_1 + q_1 \cdot k + 2 \cdot r_1) \cdot (m_2 + q_2 \cdot k + 2 \cdot r_2) \\ &= (m_1 \cdot m_2) + (m_2 q_1 + q_2 m_1 + k q_1 q_2 + 2 q_1 r_2 + 2 r_1 q_1) \cdot k + \\ &+ 2 \cdot (r_1 m_2 + r_2 m_1 + 2 r_1 \cdot r_2) \end{aligned}$$

Проверка гомоморфности сложения и умножения

- Сложение:

$$\begin{aligned} c_1 + c_2 &= (m_1 + q_1 \cdot k + 2 \cdot r_1) + (m_2 + q_2 \cdot k + 2 \cdot r_2) \\ &= (m_1 + m_2) + (q_1 + q_2) \cdot k + 2 \cdot (r_1 + r_2) \end{aligned}$$

(помним, что $|r| < \lfloor \sqrt{k-1}/2 \rfloor - 1$)

- Умножение:

$$\begin{aligned} c_1 \cdot c_2 &= (m_1 + q_1 \cdot k + 2 \cdot r_1) \cdot (m_2 + q_2 \cdot k + 2 \cdot r_2) \\ &= (m_1 \cdot m_2) + (m_2 q_1 + q_2 m_1 + k q_1 q_2 + 2 q_1 r_2 + 2 r_1 q_1) \cdot k + \\ &+ 2 \cdot (r_1 m_2 + r_2 m_1 + 2 r_1 \cdot r_2) \end{aligned}$$

(снова помним, что $|r| < \lfloor \sqrt{k-1}/2 \rfloor - 1$)

Пример реализации

Пример реализации

- $k = 11,\ m_1 = 1,\ m_2 = 0$

Пример реализации

- $k = 11,\ m_1 = 1,\ m_2 = 0$
- Шифрование

$$c_1 = 1 + 123 \cdot 11 + 2 \cdot 1 = 1356 (q_1 = 123, r_1 = 1)$$
$$c_2 = 0 - 15 \cdot 11 + 2 \cdot 2 = -161 (q_2 = -15, r_2 = 2)$$

Пример реализации

- $k = 11,\ m_1 = 1,\ m_2 = 0$
- Шифрование

$$c_1 = 1 + 123 \cdot 11 + 2 \cdot 1 = 1356 (q_1 = 123, r_1 = 1)$$
$$c_2 = 0 - 15 \cdot 11 + 2 \cdot 2 = -161 (q_2 = -15, r_2 = 2)$$

- Сложение:

$$c_1 \cdot c_2 = 1356 - 161 = 1195$$
$$(1195(\mathrm{mod}11))(\mathrm{mod}2) = 7(\mathrm{mod}2) = 1$$

Пример реализации

- $k = 11,\ m_1 = 1,\ m_2 = 0$
- Шифрование

$$c_1 = 1 + 123 \cdot 11 + 2 \cdot 1 = 1356 (q_1 = 123, r_1 = 1)$$
$$c_2 = 0 - 15 \cdot 11 + 2 \cdot 2 = -161 (q_2 = -15, r_2 = 2)$$

- Сложение:

$$c_1 \cdot c_2 = 1356 - 161 = 1195$$
$$(1195(\mathrm{mod}11))(\mathrm{mod}2) = 7(\mathrm{mod}2) = 1$$

$$D_k(c_1 + c_2) = m_1 + m_2 => \mathrm{true}$$

Пример реализации

- $k = 11,\ m_1 = 1,\ m_2 = 0$
- Шифрование

$$c_1 = 1 + 123 \cdot 11 + 2 \cdot 1 = 1356 (q_1 = 123, r_1 = 1)$$
$$c_2 = 0 - 15 \cdot 11 + 2 \cdot 2 = -161 (q_2 = -15, r_2 = 2)$$

- Сложение:

$$c_1 \cdot c_2 = 1356 - 161 = 1195$$
$$(1195(\mathrm{mod}11))(\mathrm{mod}2) = 7(\mathrm{mod}2) = 1$$

$$D_k(c_1 + c_2) = m_1 + m_2 => \mathrm{true}$$

- Умножение:

$$c_1 \cdot c_2 = 1356 \cdot (-161) = -218316$$
$$(-218316(\mathrm{mod}11))(\mathrm{mod}2) = -10(\mathrm{mod}2) = 1(\mathrm{mod}2) = 1$$

Пример реализации

- $k = 11,\ m_1 = 1,\ m_2 = 0$
- Шифрование

$$c_1 = 1 + 123 \cdot 11 + 2 \cdot 1 = 1356 (q_1 = 123, r_1 = 1)$$
$$c_2 = 0 - 15 \cdot 11 + 2 \cdot 2 = -161 (q_2 = -15, r_2 = 2)$$

- Сложение:

$$c_1 \cdot c_2 = 1356 - 161 = 1195$$
$$(1195(\mathrm{mod}11))(\mathrm{mod}2) = 7(\mathrm{mod}2) = 1$$

$$D_k(c_1 + c_2) = m_1 + m_2 => \mathrm{true}$$

- Умножение:

$$c_1 \cdot c_2 = 1356 \cdot (-161) = -218316$$
$$(-218316(\mathrm{mod}11))(\mathrm{mod}2) = -10(\mathrm{mod}2) = 1(\mathrm{mod}2) = 1$$

$$D_k(c_1 \cdot c_2) = m_1 \cdot m_2 => \mathrm{false}$$

Почему?

Давайте разбираться

- Вспомним операцию умножения:

$$\begin{aligned} c_1 \cdot c_2 &= (m_1 + q_1 \cdot k + 2 \cdot r_1) \cdot (m_2 + q_2 \cdot k + 2 \cdot r_2) \\ &= (m_1 \cdot m_2) + (m_2 q_1 + q_2 m_1 + k q_1 q_2 + 2 q_1 r_2 + 2 r_1 q_1) \cdot k + \\ &+ 2 \cdot (r_1 m_2 + r_2 m_1 + 2 r_1 \cdot r_2) \end{aligned}$$

Давайте разбираться

- Вспомним операцию умножения:

$$\begin{aligned} c_1 \cdot c_2 &= (m_1 + q_1 \cdot k + 2 \cdot r_1) \cdot (m_2 + q_2 \cdot k + 2 \cdot r_2) \\ &= (m_1 \cdot m_2) + (m_2 q_1 + q_2 m_1 + k q_1 q_2 + 2 q_1 r_2 + 2 r_1 q_1) \cdot k + \\ &+ 2 \cdot (r_1 m_2 + r_2 m_1 + 2 r_1 \cdot r_2) \end{aligned}$$

$$|r| < \lfloor \sqrt{k-1}/2 \rfloor - 1$$

Давайте разбираться

- Вспомним операцию умножения:

$$\begin{aligned} c_1 \cdot c_2 &= (m_1 + q_1 \cdot k + 2 \cdot r_1) \cdot (m_2 + q_2 \cdot k + 2 \cdot r_2) \\ &= (m_1 \cdot m_2) + (m_2 q_1 + q_2 m_1 + k q_1 q_2 + 2 q_1 r_2 + 2 r_1 q_1) \cdot k + \\ &+ 2 \cdot (r_1 m_2 + r_2 m_1 + 2 r_1 \cdot r_2) \end{aligned}$$

$$|r| < \lfloor \sqrt{k-1}/2 \rfloor - 1$$

- Это условие не выполняется для обеих шифрограмм c_1 и c_2, поэтому получаем:

$$\begin{aligned} c_1 \cdot c_2 &= 1356 \cdot (-161) = (1 \cdot 0) + (\ldots) \cdot k + 2 \cdot (1 \cdot 2 + 0 \cdot 1 + 2 \cdot (1 \cdot 2)) \\ &= (1 \cdot 0) + (\ldots) \cdot 11 + 12 = (1 \cdot 0) + (\ldots) \cdot 11 + 11 + 1. \end{aligned}$$

Давайте разбираться

- Вспомним операцию умножения:

$$\begin{aligned} c_1 \cdot c_2 &= (m_1 + q_1 \cdot k + 2 \cdot r_1) \cdot (m_2 + q_2 \cdot k + 2 \cdot r_2) \\ &= (m_1 \cdot m_2) + (m_2 q_1 + q_2 m_1 + k q_1 q_2 + 2 q_1 r_2 + 2 r_1 q_1) \cdot k + \\ &+ 2 \cdot (r_1 m_2 + r_2 m_1 + 2 r_1 \cdot r_2) \end{aligned}$$

$$|r| < \lfloor \sqrt{k-1}/2 \rfloor - 1$$

- Это условие не выполняется для обеих шифрограмм c_1 и c_2, поэтому получаем:

$$\begin{aligned} c_1 \cdot c_2 &= 1356 \cdot (-161) = (1 \cdot 0) + (\ldots) \cdot k + 2 \cdot (1 \cdot 2 + 0 \cdot 1 + 2 \cdot (1 \cdot 2)) \\ &= (1 \cdot 0) + (\ldots) \cdot 11 + 12 = (1 \cdot 0) + (\ldots) \cdot 11 + 11 + 1. \end{aligned}$$

Вывод

Уровень «шума» в шифрограмме превысил допустимые пределы.

Пример с правильными параметрами

DESK

Вопросы на засыпку (для рассматриваемого шифра)

Вопросы на засыпку (для рассматриваемого шифра)

- Пусть параметры шифрования выбраны так, что

$$D_k(c_1 \cdot c_2) = D_k(1) \cdot D_k(2)$$

$$D_k(c_1 + c_2) = D_k(1) + D_k(2)$$

Вопросы на засыпку (для рассматриваемого шифра)

- Пусть параметры шифрования выбраны так, что

$$D_k(c_1 \cdot c_2) = D_k(1) \cdot D_k(2)$$

$$D_k(c_1 + c_2) = D_k(1) + D_k(2)$$

- Будут ли выполняться равенства:

Вопросы на засыпку (для рассматриваемого шифра)

- Пусть параметры шифрования выбраны так, что

$$D_k(c_1 \cdot c_2) = D_k(1) \cdot D_k(2)$$

$$D_k(c_1 + c_2) = D_k(1) + D_k(2)$$

- Будут ли выполняться равенства:

$$D_k((c_1 \cdot c_2) \cdot (c_1 \cdot c_2)) = D_k(c_1 \cdot c_2) \cdot D_k(c_1 \cdot c_2)$$

Вопросы на засыпку (для рассматриваемого шифра)

- Пусть параметры шифрования выбраны так, что

$$D_k(c_1 \cdot c_2) = D_k(1) \cdot D_k(2)$$

$$D_k(c_1 + c_2) = D_k(1) + D_k(2)$$

- Будут ли выполняться равенства:

$$D_k((c_1 \cdot c_2) \cdot (c_1 \cdot c_2)) = D_k(c_1 \cdot c_2) \cdot D_k(c_1 \cdot c_2)$$

$$D_k((c_1 + c_2) \cdot (c_1 + c_2)) = D_k(c_1 + c_2) \cdot D_k(c_1 + c_2)$$

Вопросы на засыпку (для рассматриваемого шифра)

- Пусть параметры шифрования выбраны так, что

$$D_k(c_1 \cdot c_2) = D_k(1) \cdot D_k(2)$$

$$D_k(c_1 + c_2) = D_k(1) + D_k(2)$$

- Будут ли выполняться равенства:

$$D_k((c_1 \cdot c_2) \cdot (c_1 \cdot c_2)) = D_k(c_1 \cdot c_2) \cdot D_k(c_1 \cdot c_2)$$

$$D_k((c_1 + c_2) \cdot (c_1 + c_2)) = D_k(c_1 + c_2) \cdot D_k(c_1 + c_2)$$

$$D_k((c_1 \cdot c_2) \cdot (c_1 + c_2)) = D_k(c_1 \cdot c_2) \cdot D_k(c_1 + c_2)$$

Вопросы на засыпку (для рассматриваемого шифра)

- Пусть параметры шифрования выбраны так, что

$$D_k(c_1 \cdot c_2) = D_k(1) \cdot D_k(2)$$

$$D_k(c_1 + c_2) = D_k(1) + D_k(2)$$

- Будут ли выполняться равенства:

$$D_k((c_1 \cdot c_2) \cdot (c_1 \cdot c_2)) = D_k(c_1 \cdot c_2) \cdot D_k(c_1 \cdot c_2)$$

$$D_k((c_1 + c_2) \cdot (c_1 + c_2)) = D_k(c_1 + c_2) \cdot D_k(c_1 + c_2)$$

$$D_k((c_1 \cdot c_2) \cdot (c_1 + c_2)) = D_k(c_1 \cdot c_2) \cdot D_k(c_1 + c_2)$$

$$D_k((c_1 \cdot c_2) + (c_1 + c_2)) = D_k(c_1 \cdot c_2) + D_k(c_1 + c_2)$$

Заключение

Спасибо за внимание!