# Симетрична схема частково-гомоморфного шифрування над кільцем цілих чисел

Богдан Кулинич

17 квітня 2015

# Асиметричне шифрування

Схема асиметричного шифрування $\mathcal{E}$:

- $\mathsf{KeyGen}_{\mathcal{E}}(1^{\lambda}) \to (\mathbf{pk}, \mathbf{sk})$
- $\mathsf{Encrypt}_{\mathcal{E}}(\mathbf{pk}, m \in \{0, 1\}) \to c \in \mathcal{C}$.
- $\mathsf{Decrypt}_{\mathcal{E}}(\mathbf{sk}, c \in \mathcal{C}) \to m \in \{0, 1\}$

# Гомоморфне шифрування

Схема асиметричного гомоморфного шифрування $\mathcal{E}$:

- $\mathsf{KeyGen}_{\mathcal{E}}(1^{\lambda}) \to (\mathbf{pk}, \mathbf{sk})$
- $\mathsf{Encrypt}_{\mathcal{E}}(\mathbf{pk}, m \in \{0,1\}) \to c \in \mathcal{C}.$
- $\mathsf{Decrypt}_{\mathcal{E}}(\mathbf{sk}, c \in \mathcal{C}) \to m \in \{0,1\}$
- $\mathsf{Add}_{\mathcal{E}}(\mathbf{pk}, c_1 \in \mathcal{C},\ \ c_2 \in \mathcal{C})$
- $\mathsf{Mult}_{\mathcal{E}}(\mathbf{pk}, c_1 \in \mathcal{C},\ \ c_2 \in \mathcal{C})$

# Гомоморфне шифрування

**Означення.** Позначимо шифрування біта $m$ як $\hat{m}$:

$$\mathsf{Decrypt}_{\mathcal{E}}(\mathbf{pk}, \hat{m}) = m$$

для відомого контексту $(\mathbf{pk}, \mathbf{sk})$ і схеми $\mathcal{E}$. Нехай також:

(Гомоморфне додавання) $\hat{m}_1 \oplus \hat{m}_2 = \mathsf{Add}_{\mathcal{E}}(\mathbf{pk}, \hat{m}_1, \hat{m}_2)$

(Гомоморфне множення) $\hat{m}_1 \otimes \hat{m}_2 = \mathsf{Mult}_{\mathcal{E}}(\mathbf{pk}, \hat{m}_1, \hat{m}_2)$

# Повне гомоморфне шифрування

Гомоморфна схема шифрування $\mathcal{E}$ *коректна* і *повна*, якщо для будь-яких $m_1, m_2 \in \{0, 1\}$ і будь-яких $\hat{m}_1, \hat{m}_2 \in \mathcal{C}$:

- $\mathsf{Decrypt}_{\mathcal{E}}(\mathbf{sk}, \hat{m}_1 \oplus \hat{m}_2)) = m_1 + m_2 \mod 2$
- $\mathsf{Decrypt}_{\mathcal{E}}(\mathbf{sk}, \hat{m}_1 \otimes \hat{m}_2)) = m_1 \cdot m_2 \mod 2$

# Повне гомоморфне шифрування

Схеми гомоморфного шифрування першого покоління (2009—2010):

- Перша схема на базі ідеальних решіток [Gen09]
- На базі цілих чисел [DGHV10]

- Шифрування (симетричне) біта $m$ з приватним ключем $\mathbf{sk} = p$

$$c = q \cdot p + m + 2r$$

- Шифрування біта $m$ з публічним ключем $\mathbf{pk}$

$$c = \left[ m + 2r + 2 \sum_{i \in S} x_i \right]_{x_0}$$

- Публічний ключ $\mathbf{pk}$ — набір шифрувань нуля

$$x_i = q_i \cdot p + r_i$$

- $x_0 = q_0 \cdot p -$ елемент без шуму
- Розшифрування $c$

$$m = [c \bmod p]_2$$

# Схема DGHV над цілими числами

## Симетричний варіант з публічним елементом без шуму $x_0$

- Шифрування (симетричне) біта $m$ з приватним ключем $\mathbf{sk} = p$

$$c = [q \cdot p + m + 2r]_{x_0}$$

- $x_0 = q_0 \cdot p$ – публічний елемент без шуму
- Розшифрування $c$

$$m = [c \bmod p]_2$$

- Гомоморфне додавання

$$c_1 \oplus c_2 = [c_1 + c_2]_{x_0}$$

- Гомоморфне множення

$$c_1 \otimes c_2 = [c_1 \cdot c_2]_{x_0}$$

# Схема DGHV над цілими числами

## Симетричний варіант з публічним елементом без шуму $x_0$

- Шифрування (симетричне) біта $m$ з приватним ключем $\mathbf{sk} = p$

$$c = [q \cdot p + m + 2r]_{x_0}$$

- $x_0 = q_0 \cdot p$ – публічний елемент без шуму
- Розшифрування $c$

$$m = [c \bmod p]_2$$

- Гомоморфне додавання

$$c_1 \oplus c_2 = [c_1 + c_2]_{x_0}$$

- Гомоморфне множення

$$c_1 \otimes c_2 = [c_1 \cdot c_2]_{x_0}$$

# Властивості симетричного варіанту DGHV I

- Схема частково-гомоморфна:

$$\begin{aligned}\hat{m}_1 \oplus \hat{m}_2 &= [m_1 + m_2 + (q_1 + q_2)p + 2(r_1 + r_2)]_{x_0} \\ &= [m_1 + m_2 + q' \cdot p + 2r']_{x_0} \\ \hat{m}_1 \otimes \hat{m}_2 &= [m_1 \cdot m_2 + (q_1 q_2 p + q_1 m_2 + q_2 m_1 + 2q_1 r_2 + 2q_2 r_1)p \\ &\quad + 2(m_1 r_2 + m_2 r_1 + 2r_1 r_2)]_{x_0} \\ &= [m_1 \cdot m_2 + q' \cdot p + 2r']_{x_0}\end{aligned}$$

  Зі збільшенням кількості виконаних операцій, шум $2r$ зростає. Коли перевищує $p - m$, $c$ розшифровується некоректно.

- Техніка бутстрапінгу використовується, щоб зменшити шум в $c$ [DGHV10, Gen09]

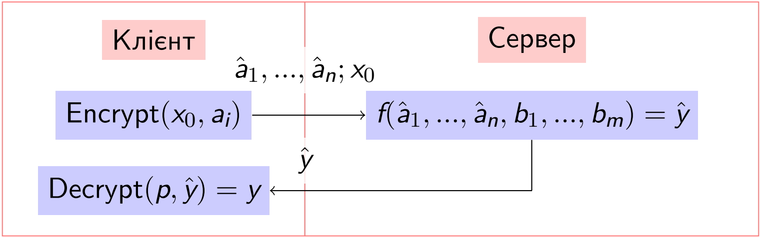
# Властивості симетричного варіанту DGHV II

- Схема підтримує змішані операції:

$$\hat{m} \oplus \hat{1} = [\hat{m} + 1]_{x_0}$$
$$\hat{m} \oplus \hat{0} = [\hat{m} + 0]_{x_0} = \hat{m}$$
$$\hat{m} \otimes \hat{1} = [\hat{m} \cdot 1]_{x_0} = \hat{m}$$
$$\hat{m} \otimes \hat{0} = [\hat{m} \cdot 0]_{x_0} = 0$$

  При цьому шум зростає тільки при виконанні додавання одиниці.

# Висновки




- Виконання змішаних операцій дозволяє не шифрувати *всі* входи функції, що виконується гомоморфно
- Зникає необхідність передавати публічний ключ, що зменшує розмір передаваних даних
- Потрібно підбирати параметри схеми, щоб $f$ виконувалась коректно (без перевищень шуму).
- В [YKPB13] параметри схеми підібрані неправильно.

# Посилання


Marten van Dijk, Craig Gentry, Shai Halevi, and Vinod Vaikuntanathan.
Fully Homomorphic Encryption over the Integers.
In Henri Gilbert, editor, *EUROCRYPT*, volume 6110 of *Lecture Notes in Computer Science*, pages 24--43. Springer, 2010.

Craig Gentry.
*A fully homomorphic encryption scheme*.
PhD thesis, Stanford University, 2009.

Xun Yi, Md. Golam Kaosar, Russell Paulet, and Elisa Bertino.
Single-Database Private Information Retrieval from Fully Homomorphic Encryption.
*IEEE Trans. Knowl. Data Eng.*, 25(5):1125--1134, 2013.