НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

# МОДЕЛІ І МЕТОДИ КОНТРОЛЮ ЦІЛІСНОСТІ ТА АВТЕНТИЧНОСТІ НА ОСНОВІ КАСКАДНОГО АЛГОРИТМУ UMAC

**Дисертація на здобуття наукового ступеня доктора філософії**
**за спеціальністю 125 – Кібербезпека та захист інформації**

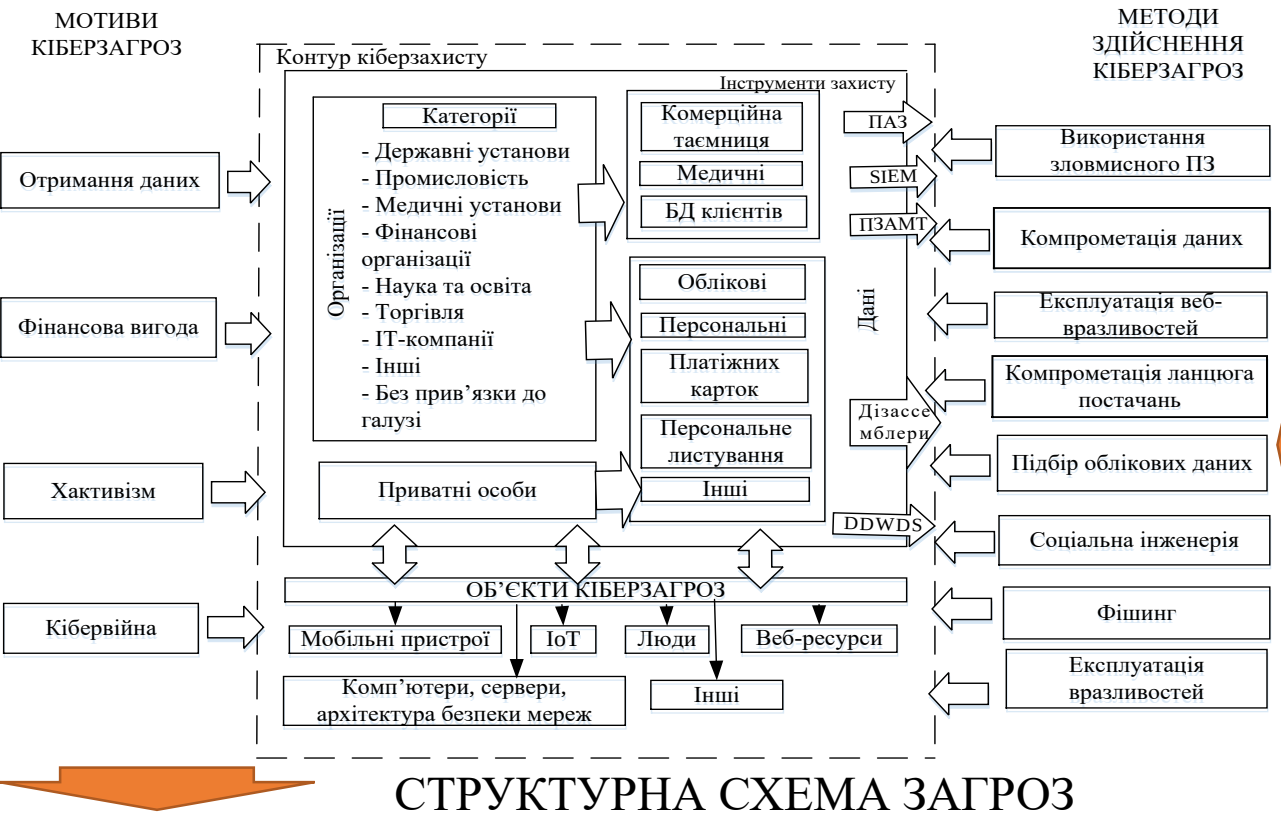
**Здобувач:** аспірантка кафедри безпеки інформаційних технологій
Національний авіаційний університет
**ГАВРИЛОВА Алла Андріївна**

**Науковий керівник**: кандидат технічних наук, доцент,
**ХОХЛАЧОВА Юлія Євгеніївна**

Київ - 2023

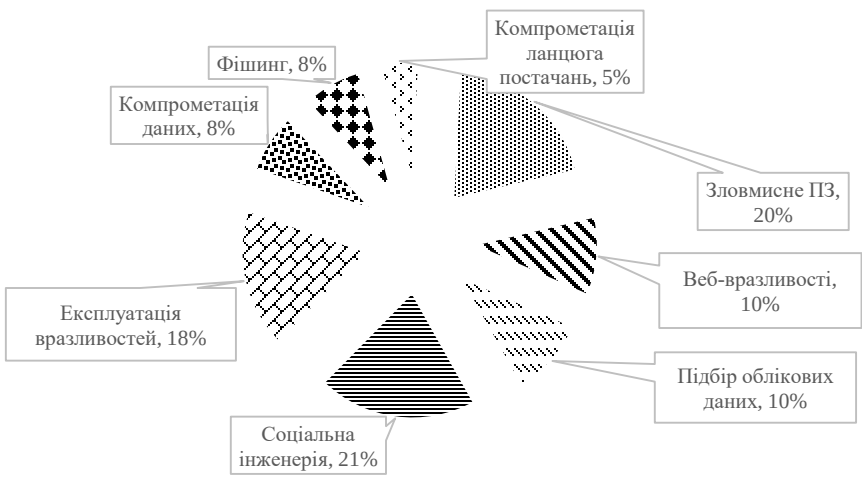
# АКТУАЛЬНІСТЬ ТЕМИ

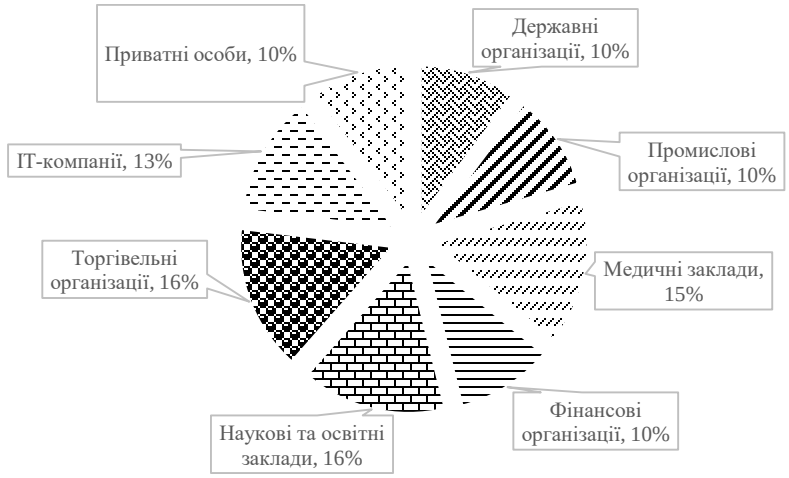





розроблення нових та удосконалення існуючих моделей і методів забезпечення цілісності та автентичності інформації, яка циркулює в кіберпросторі

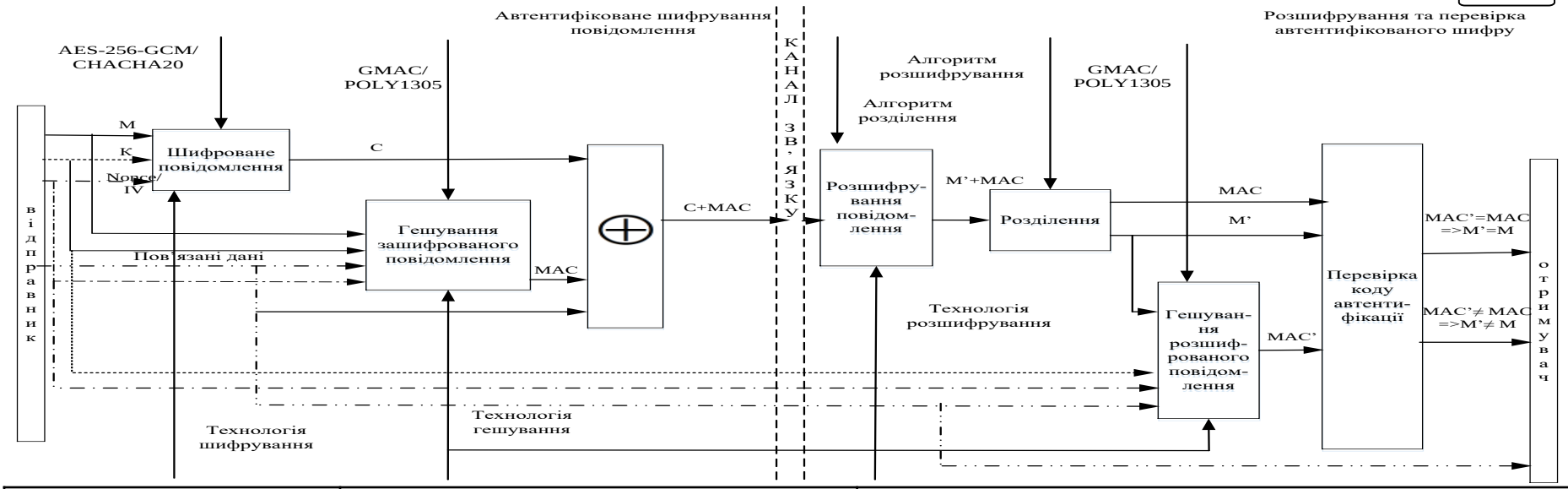
## СТРУКТУРНА СХЕМА ЗАГРОЗ




## РЕАЛІЗАЦІЯ ЗАГРОЗ

# АКТУАЛЬНІСТЬ ТЕМИ




| Характеристики | SSL | TLS |
|---|---|---|
| означає | рівень захищених сокетів | протокол безпеки транспортного рівня |
| версії | - розвивався до версій 1.0, 2.0 та 3.0;<br>- замінюється на TLS | - оновлена версія SSL;<br>- розвивався до версій 1.0, 1.1, 1.2 та 1.3 |
| активність | усі версії застаріли | активно використовуються версії TLS 1.2 та 1.3 |
| оповіщення | - є два типи оповіщень;<br>- оповіщення не шифруються | - є більше двох типів оповіщень;<br>- оповіщення шифруються |
| автентифікація повідомлень | використовує MAC | використовує HMAC |
| набори шифрів | підтримує старі алгоритми з відомими уразливістю безпеки | використовує найсучасніші алгоритми шифрування |
| рукостискання | складне і повільне | - складається з меншої кількості кроків;<br>- забезпечує більш швидке з'єднання |

# ЗВ’ЯЗОК ТЕМИ З ОСВІТНЬОЮ ПРОГРАМОЮ

## Кібербезпека

### Основний фокус ОНП:

формування у здобувачів вищої освіти (аспірантів) **здатності розв’язувати комплексні проблеми професійної та / або дослідницько-інноваційної діяльності в області кібербезпеки**, що передбачає **розробку нових, удосконалення або подальшого розвитку існуючих розробок та досліджень**.

### Напрям досліджень:

**ФКЗ –** дослідження теоретичних, науково-технічних і технологічних проблем, пов’язаних із організацією, створенням методів та засобів забезпечення захисту інформації та/або кібербезпеки при її зберіганні, обробці й передачі з використанням сучасних математичних методів, інформаційних технологій та технічних засобів.

# МЕТА, ОБ'ЄКТ, ПРЕДМЕТ ТА МЕТОДИ ДОСЛІДЖЕННЯ



**Метою дисертаційної роботи є**

розробка вдосконаленого алгоритму гешування UMAC на основі крипто-кодових конструкцій.

**Об'єкт дослідження –**

процес забезпечення цілісності та автентичності в системах безпеки на основі алгоритму UMAC

**Предмет дослідження**

моделі і методи контролю цілісності та автентичності на основі каскадного алгоритму UMAC

**Методи дослідження:**

теорії завадостійкого кодування,
теорії захисту інформації,
теорії криптографії,
теорії кодування,
теорії кінцевих полів Галуа,
теорії ймовірностей і математичної статистики,
теорія автентифікації,
процесний підхід

# ЧАСТКОВІ ЗАВДАННЯ ДОСЛІДЖЕННЯ

**Актуальність задачі**

В умовах бурхливого зростання обчислювальних можливостей щодо зламу криптографічних алгоритмів, виникає необхідність у розробці та практичної реалізації алгоритмів щодо забезпечення послуг безпеки – цілісності та автентичності

**Науково-прикладна завдання**

дослідження присвячене актуальним питанням розроблення нових та удосконалення існуючих моделей і методів забезпечення цілісності та автентичності інформації, яка циркулює в кіберпросторі в умовах постквантового періоду

**ОСНОВНІ ЗАВДАННЯ ДОСЛІДЖЕННЯ**

**Завдання 1.** Проведення аналізу використання і обгрунтування напрямків вдосконалення методів автентифікації в інформаційно-комунікаційних системах

- виконати аналіз безпеки інформації в сучасних ІКСМ
- виконати аналіз методів автентичності SSL, TLS
- виконати аналіз методів побудови кодів контролю цілісності та автентичності на основі алгоритму UMAC

**Завдання 2.** Розробити методи контролю цілісності та автентичності даних на основі алгоритму UMAC на крипто-кодових конструкціях

- Визначити методи побудови безпечних сучасних ІКСМ
- Провести дослідження каскадного ключового гешування
- Побудувати алгоритм UMAC на ССС
- Розробити метод алгоритму UMAC на ССС Мак-Еліса з ЕС

**Завдання 3.** Розробити математичні моделі UMAC на модифікованих ССС

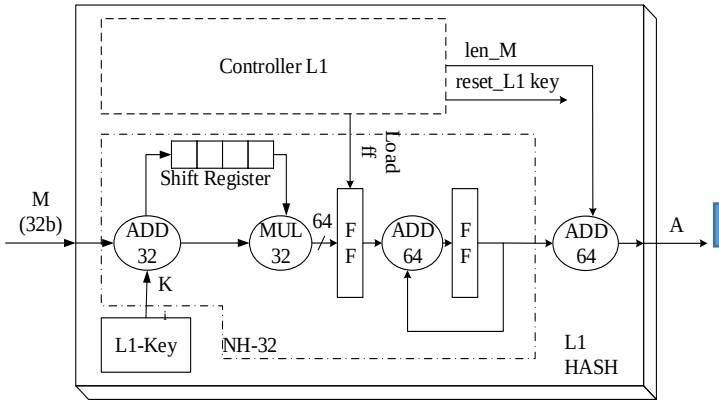
- Розробити математичну модель та метод формування алгоритму UMAC на ССС МЕС
- Розробити математичну модель та метод формування алгоритму UMAC на НССС DC
- Дослідити каскадний UMAC на ССС з МЕС та DC

**Завдання 4.** Розробити практичні рекомендації використання алгоритму UMAC у протоколі SSL/TLS

- Розробити додаток для вдосконаленого алгоритму UMAC
- Розробити комплексовані алгоритми ССС/ UMAC
- Вдосконалити протокол SSL/TLS на основі алгоритмів ССС/UMAC
- Дослідити стійкість та продуктивність алгоритмів ССС/ UMAC

**Мета:** дослідження вдосконаленого алгоритму гешування UMAC на основі крипто-кодових конструкцій

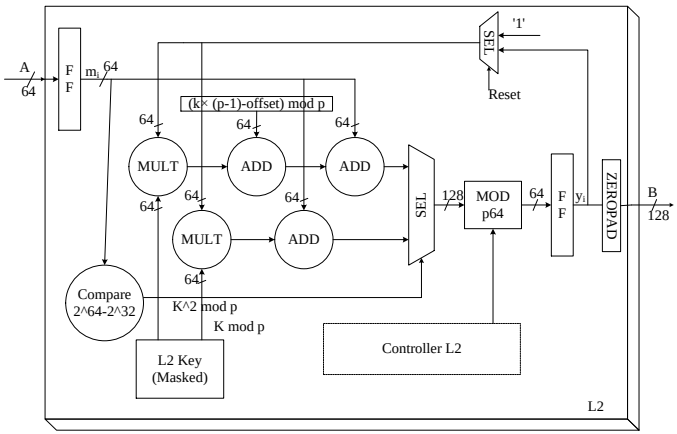
# МЕТОД КОНТРОЛЮ ЦІЛІСНОСТІ ТА АВТЕНТИЧНОСТІ ДАНИХ НА ОСНОВІ АЛГОРИТМУ UMAC НА ККК




На **першому шарі** алгоритму UMAC використовується значення функції UHASH-hash

UHASH-hash

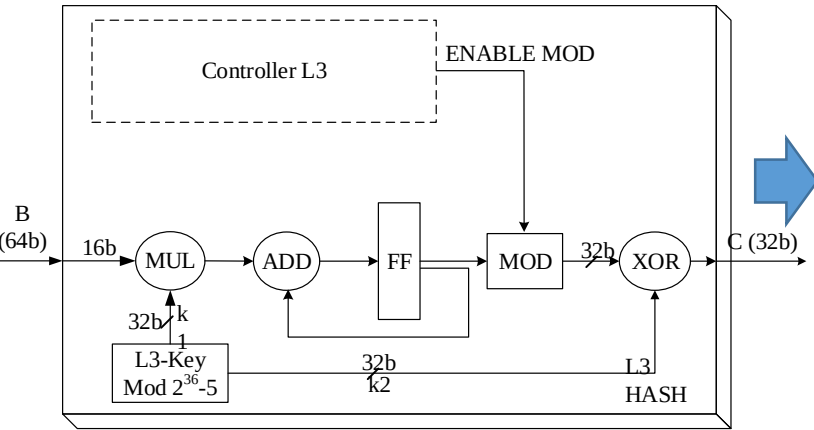
$$Y_{L1}=Hash_{L1}(K_{L1},M)$$




На **другому шарі** алгоритму UMAC використовується значення функції POLY-hash

POLY-hash

$$Y_{L2}=Hash_{L2}(K_{L2},Y_{L1})$$




На **третьому шарі** алгоритму UMAC використовується значення функції Carter-Wegman-hash

Carter-Wegman-hash

$$Y_{L3}=Hash_{L3}(K_{L31},K_{L32},Y_{L2})$$

# РЕЗУЛЬТАТИ ОЦІНКИ МЕТОДІВ АВТЕНТИФІКАЦІЇ ДЛЯ ФОРМУВАННЯ ПСЕВДОВИПАДКОВОЇ ПІДКЛАДКИ

| показники | алгоритми формування псевдовипадкової підкладки Pad | | | | |
|---|---|---|---|---|---|
| | UMAC+ MASH-1 | UMAC+ MASH-2 | POLY1305-AES | AES GCM | UMAC+ AES |
| універсальність | + | + | – | + | – |
| стійкість до постквантових зломів | – | + | – | – | – |
| оперативність формування | – | – | – | – | + |
| незалежність від обчислювальних потужностей | – | – | + | + | – |

# ВИЗНАЧЕННЯ УНІВЕРСАЛЬНОГО ГЕШУВАННЯ

***Універсальне гешування*** полягає у визначенні такого набору елементів конечного множини *H* геш-функцій *h: A→B*, $|A| = a$, $|B| = b$, щоб випадкове обрання функції $h \in H$ забезпечувало б низьку ймовірність колізії, тобто для будь-яких різних входів $x_1$ та $x_2$ ймовірність того, що $h(x_1) = h(x_2)$ (ймовірність колізії, зіткнення) не повинна перевищувати деякого заздалегідь заданого значення $\varepsilon$:

$$P_{кол} = P(h(x_1) = h(x_2)) \le \varepsilon, \quad P_{кол} = \frac{\delta_H(x_1, x_2)}{|H|}$$

де $\delta_H(x_1, x_2)$ - кількість таких геш-функцій в *H*, при яких $x_1, x_2 \in A$, $x_1 \neq x_2$ викликають колізію, тобто $h(x_1) = h(x_2)$ .

**Визначення 1.** Нехай $0 < \varepsilon < 1$. *H* є $\varepsilon$ - *універсальним геш-класом,* якщо для $x_1, x_2 \in A, x_1 \neq x_2$ існує не більше ніж $H \times \varepsilon$ функцій $f \in H$ таких, що $h(x_1) = h(x_2)$, якщо $\delta_H(x_1, x_2) \le \varepsilon |H|$ для всіх $x_1, x_2 \in A, x_1 \neq x_2$ .

**Визначення 2.** Нехай $0 < \varepsilon < 1$. *H* є $\varepsilon$ - *суворо універсальним геш-класом*, якщо виконуються наступні умови:

- для кожного $x_1 \in A$ та для кожного $y_1 \in B$ , $|\{h \in H : h(x_1) = y_1\}| = |H|/|B|$;
- для кожних $x_1, x_2 \in A, x_1 \neq x_2$ та для кожного $y_1, y_2 \in B$,

$$|\{h \in H : h(x_1) = y_1, h(x_2) = y_2\}| \le \varepsilon |H|.$$

***Геш-функція є універсальною, якщо виконуються обмеження за кількістю ключових даних, для яких виконуються відповідні рівності визначень 1 та 2,*** які використовуються у якості критеріїв дослідження колізійних властивостей алгоритму mini-UMAC запропонованого математичного апарату

# КЛАСИФІКАЦІЯ КРИПТО-КОДОВИХ КОНСТРУКЦІЙ

КРИПТО-КОДОВІ КОНСТРУКЦІЇ

**СИМЕТРИЧНІ** (ц, ~~к~~, д)

Недоліки:
- складність реалізації ($2^{13}$)
- недоліки БСШ

Переваги:
- висока швидкість шифрування (порівнянна з БСШ)
- інтегрований механізм забезпечення Д + К
- модель доказовою стійкості

**НЕСИМЕТРИЧНІ** (ц, к, д)

Недоліки:
- складність реалізації ($2^{10} – 2^{13}$)
- схильні до атаки Сидельникова

Схема Рао-Нама на кодах Гоппе 1986-89 р.

Схеми задані через многочлен Гоппе, коди Гоппе 1989 – 95 р.

Схема на скорочених кодах Гоппе 1995 – 98 р.

– лінійність кодових перетворень

ККК на узагальнених кодах РС 1995-2002 р.

ККК Нідеррайтера на кодах БЧХ, Гопа 1986 р.

ККК Мак-Еліса на кодах Гопа 1978 р.

ККК на кодах БЧХ, РС, узагальнених кодах РС 1989 – 2002 р.

Переваги:
- стійкість до атаки Сидельникова
- збільшення криптостійкості
- зменшення ключових даних
- інтегрований механізм забезпечення Д + К + Ц
- модель доказової стійкості

ККК на АГК, згортальних кодах 2002 – 2006 р.

ККК на модифікованих АГК, еліптичних кривих 2007 р.

ГККК Мак-Еліса на збиткових кодах+МЕС, 2017 р.

ГККК Нідерратера на збиткових кодах+МЕС, 2020 р.

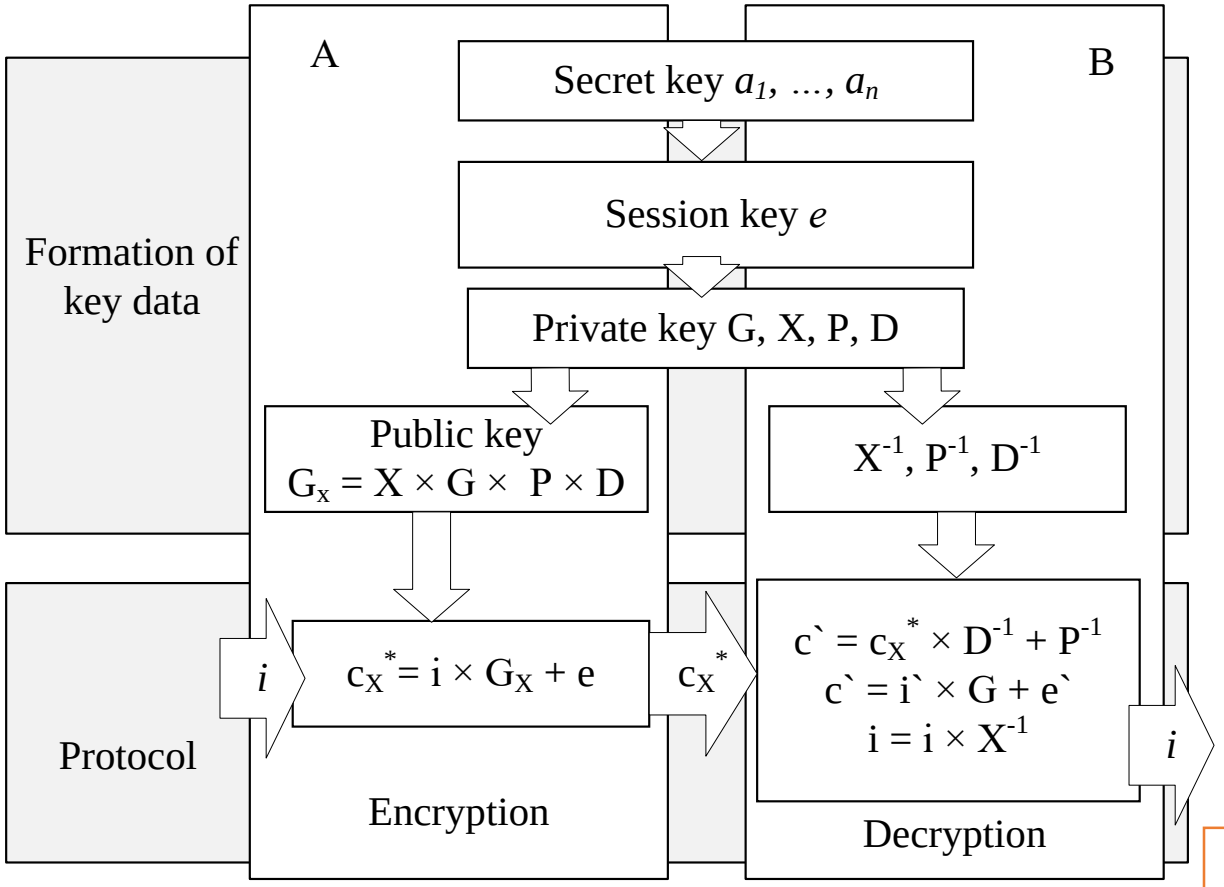
Ц – цілісність
К – конфіденційність
Д – достовірність

ККК – крипто-кодові конструкції
НККК – несиметричні ККС
СККК – симетричні ККС
ГККК – гібридні крипто-кодві конструкції

АГК – алгеброгеометричні коди

# СТРУКТУРНА СХЕМА ККК МАК-ЕЛІСА НА ЕС






**Закритий ключ – матриці *X, P та D.***

X – невироджена k×k матриця над GF(q),
P – перестановочна n×n матриця над GF(q),
D – діагональна n×n матриця над GF(q),
$G^{EC}$ – породжувальна k×n матриця на еліптичних кодах над GF(q),

**Відкритий ключ – матриця**

$$G_X^{EC} = X \times G^{EC} \times P \times D$$

**Закрита інформацій (кодограма)**

$$c_X^* = i \times G_X^{EC} + e,$$

$e$ – випадковий вектор помилки$\leq t$

*Еліптична крива (EC)* в афінному просторі $\boldsymbol{A^2}$ над полем *GF(q)* є лінейною кривою, що задається рівнянням

$\boldsymbol{y^2+a_1xy+a_3y=x^3+a_2x^2+a_4xy+a_6}$,

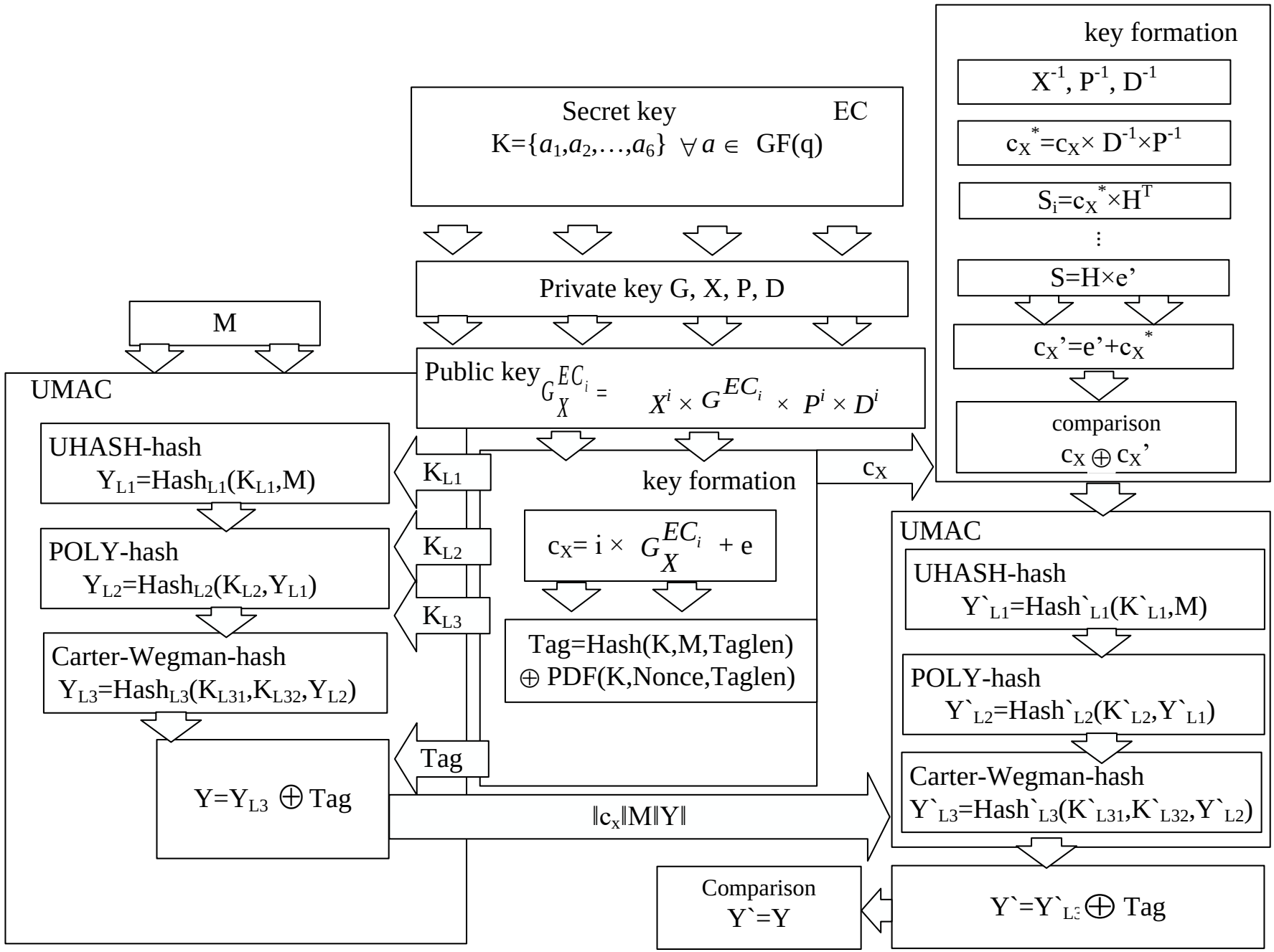
*або* $\boldsymbol{P^2}$ *задається однорідним рівнянням*

$\boldsymbol{y^2z+a_1xyz+a_3yz^2=x^3+a_2x^2z+a_4xyz+a_6z^3}$,

$a_i \in GF(q)$, рід кривої $g=1$.

# СТРУКТУРНА СХЕМА МЕТОДУ UMAC НА ККК МАК-ЕЛІСА



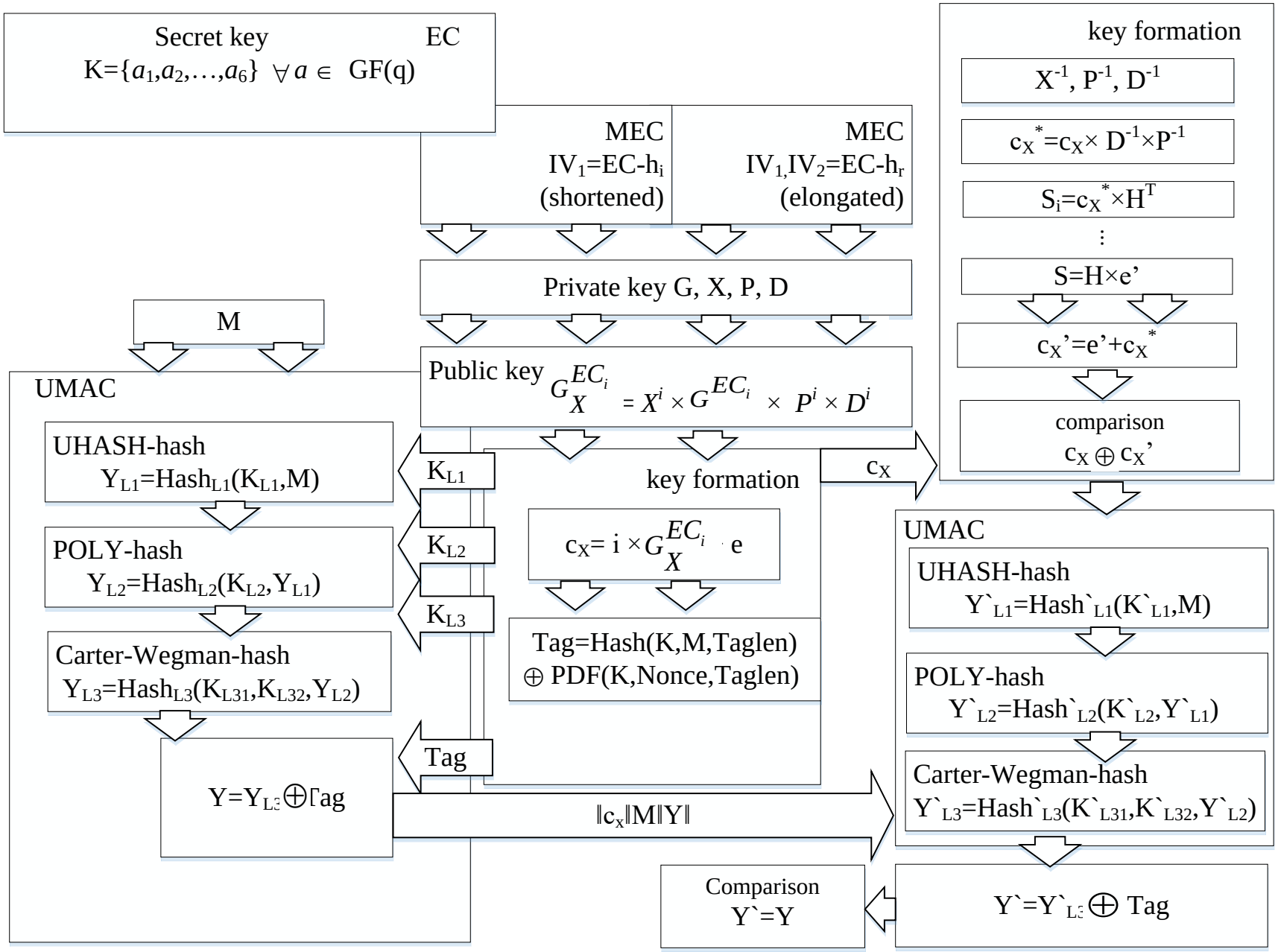


# ПЕРШИЙ НАУКОВИЙ РЕЗУЛЬТАТ

***Вперше запропоновано метод забезпечення автентичності та цілісності на основі каскадного алгоритма UMAC на крипто-кодових конструкціях Мак-Еліса з еліптичними кодами*** – дозволяє забезпечити його використання в постквантовий криптоперіод.

# СТРУКТУРНА СХЕМА МЕТОДУ UMAC НА ККК МАК-ЕЛІСА НА МОДИФІКОВАНИХ (УКОРОЧЕНИХ/ПОДОВЖЕНИХ) ЕС



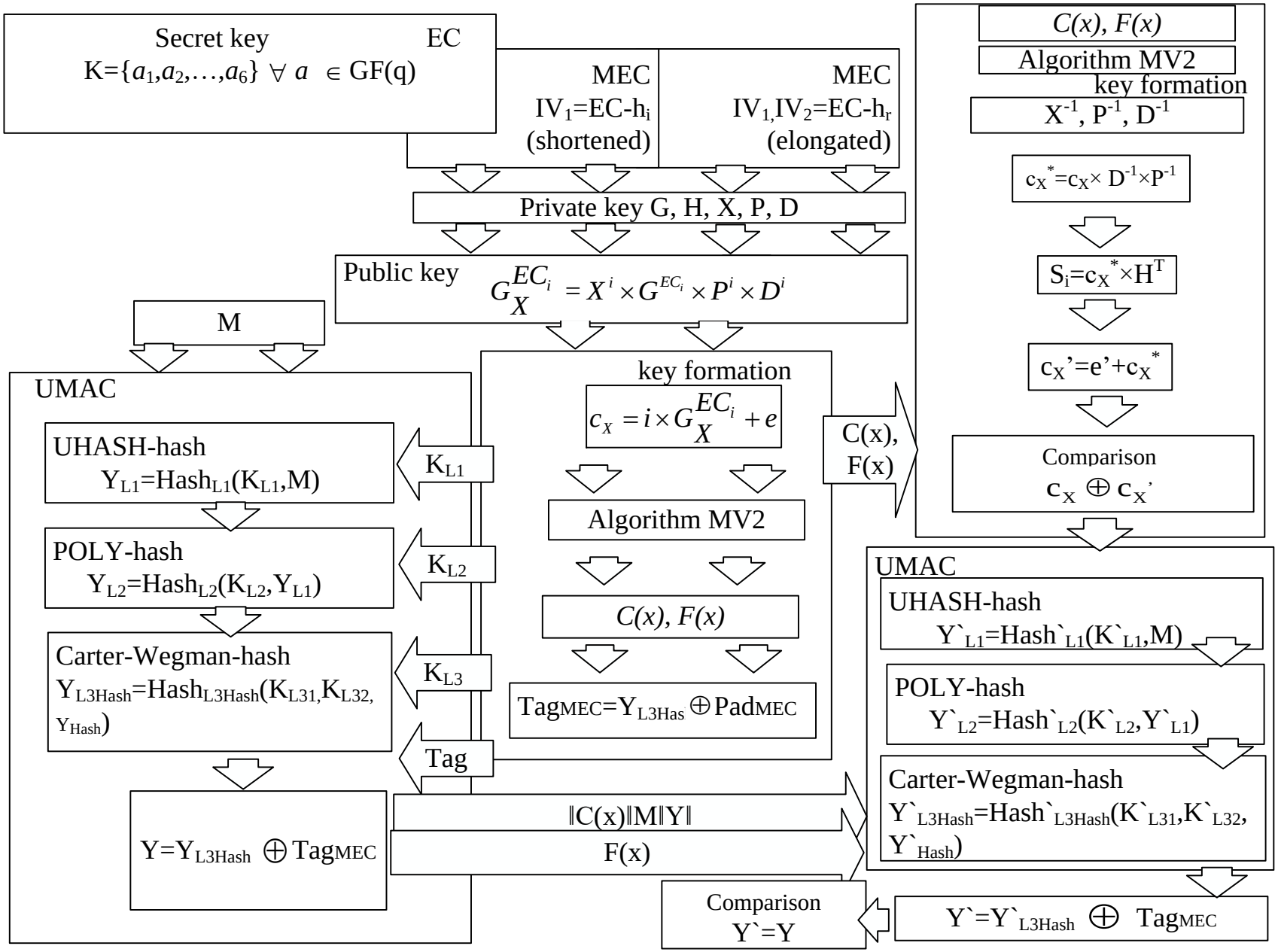


# ДРУГИЙ НАУКОВИЙ РЕЗУЛЬТАТ

***Вперше запропоновано метод забезпечення автентичності та цілісності на основі каскадного алгоритму UMAC на крипто-кодових конструкціях Мак-Еліса з модифікованими*** *(укороченими та/або подовженими)* ***еліптичними кодами*** – дозволяє забезпечити зменшення обчислювальної ємності та зберегти стійкість до зламу.

# СТРУКТУРНА СХЕМА АЛГОРИТМУ UMAC НА ГККК МАК-ЕЛІСА НА ЗБИТКОВИХ КОДАХ





# ТРЕТІЙ НАУКОВИЙ РЕЗУЛЬТАТ

***Вперше запропоновано метод забезпечення автентичності та цілісності на основі каскадного алгоритма UMAC на гібридних крипто-кодових конструкціях Мак-Еліса на збиткових кодах*** – дозволяє забезпечити практичне використання в смарт-технологіях з обмеженими обчислювальними ресурсами.

# РОЗРОБКА МАТЕМАТИЧНИХ МОДЕЛЕЙ UMAC НА ККК



## *Перший рівень геш-коду.*

$$Y_{L1} = Hash_{L1}(K_{L1}, M) = NH(K_{L1}, M_0) \| NH(K_{L1}, M_1) \| ... \| NH(K_{L1}, M_{n-1})$$

де $n = \left\lceil \frac{Length(M)}{1024} \right\rceil$, $[x]$ – ціла частина числа $x$,

$Length(M)$ – байтовая довжина інформаційного повідомлення

$$M_i = M_{i_1} \| M_{i_2} \| ... \| M_{i_t} \qquad K_{L1} = K_{L1_1} \| K_{L1_2} \| ... \| K_{L1_t}$$

$$Hash_{L1_i} = Hash_{L1_i} +_{64} ((M_{i_{j+0}} +_{32} K_{L1_{j+0}}) \times_{64} (M_{i_{j+4}} +_{32} K_{L1_{j+4}})),$$

$$Hash_{L1_i} = Hash_{L1_i} +_{64} ((M_{i_{j+1}} +_{32} K_{L1_{j+1}}) \times_{64} (M_{i_{j+5}} +_{32} K_{L1_{j+5}})),$$

$$Hash_{L1_i} = Hash_{L1_i} +_{64} ((M_{i_{j+2}} +_{32} K_{L1_{j+2}}) \times_{64} (M_{i_{j+6}} +_{32} K_{L1_{j+6}})),$$

$$Hash_{L1_i} = Hash_{L1_i} +_{64} ((M_{i_{j+3}} +_{32} K_{L1_{j+3}}) \times_{64} (M_{i_{j+7}} +_{32} K_{L1_{j+7}})).$$

## *Другий рівень геш-коду.*

$$Y_{L2} = Hash_{L2}(K_{L2}, Y_{L1}) = Poly(Wordbits, Maxwordrange, k, M_P)$$

$$M_P = M_{P_1} \| M_{P_2} \| ... \| M_{P_n}$$

$$Y_{L2} = \left(M_{P_n} + kM_{P_{n-1}} + ... + k^{n-1}M_{P_1} + k^n\right) \bmod(p)$$

$$Poly_i = \left(kPoly_{i-1} + M_{P_i}\right) \bmod(p), Poly_0 = 1, p = prime(Wordbits)$$

$$M_{P_n} + kM_{P_{n-1}} + ... + k^{n-1}M_{P_1} + k^n = (((k + M_{P_1})k + M_{P_2})k + ... + M_{P_{n-1}})k + M_{P_n}$$

*При укорочені* вектор ініціалізації:

$IV_1 = a_{11}\, a_{12}\, a_{13}\, a_{14}\, a_{15}\, a_{16}\, a_{17}\, a_{18}$

початкова кодограма

$C_{Хукороч} = c_{11}\, c_{12}\, 0\, c_{14}\, c_{15}\, c_{16}\, c_{17}\, c_{18}.$

## *Третій рівень геш-коду.*

$$Y_{L3Hash} = Hash_{L3Hash}(K_{L31}, K_{L32}, Y_{Hash}).$$

*При подовжені* вектор ініціалізації:

$IV_2 = b_{11}\, b_{12}\, b_{13}\, b_{14}\, b_{15}\, b_{16}\, b_{17}\, b_{18}.$

початкова кодограма

$C_{Худлин} = c_{11}\, c_{12}\, 1\, 0\, c_{14}\, c_{15}\, c_{16}\, c_{17}\, c_{18}.$

$\oplus$

## Псевдовипадкова підкладка

$$Pad_{EC} = PDF(C_X, Nonce, Taglen) \qquad Pad_{MEC} = PDF(C_{Хукороч} / C_{Хподовж}, Nonce, Taglen)$$

## Код автентичності повідомлення

$$Tag_{MEC} = Y_{L3Hash} \oplus Pad_{MEC}$$

# МАТЕМАТИЧНА МОДЕЛЬ ФОРМУВАННЯ ПСЕВДОВИПАДКОВОЇ ПІДКЛАДКИ НА ССС МАК-ЕЛІСА НА ЕС

Крок 1. Формування відкритого тексту M $M_i = \{I_0, I_{h_1}, .. I_{h_j}, I_{k-1}\}$

Крок 2. Формування закритого тексту $C = \{C_1, C_2, ..., C_{q^k}\}$

Крок 3. Формування множини прямих відображень
$\phi = \{\phi_1, \phi_2, ... \phi_s\}$

Крок 4. Формування множини зворотних відображень
$\phi^{-1} = \{\phi_1^{-1}, \phi_2^{-1}, ..., \phi_s^{-1}\}$

Крок 5. Формування відкритого ключа
$K_{a_i} = \{K_{1_{a_i}}, K_{2_{a_i}}, ..., K_{s_{a_i}}\} = \{G_X^{EC_1}{}_{a_i}, G_X^{EC_2}{}_{a_i}, ..., G_X^{ECs}{}_{a_i}\}$
$\phi_i : M \xrightarrow{K_{ia_i}} C_k$

Крок 6. Формування закритого ключа
$K^* = \{K_1^*, K_2^*, ..., K_s^*\} = \{\{X, P, D\}_1, \{X, P, D\}_2, ..., \{X, P, D\}_s\}$
$\{X, P, D\}_i = \{X^i, P^i, D^i\}$
$\phi_i^{-1} : C \xrightarrow{K_i} M$

Крок 7. Формування випадкового (n, k, d)-коду
$G_X^{ECu} = X^u \times G^{EC} \times P^u \times D^u,\ u \in \{1, 2, ..., s\}$

Крок 8. Формування закритого тексту (n, k, d)-коду
$C_j = \phi_u\left(M_i, G_X^{ECu}{}_{a_i}\right) = M_i \times \left(G_X^{ECu}{}_{a_i}\right)^T + e$

$Pad_{EC} = PDF(i \times G_X^{EC_i} + e, Nonce, Taglen)$

# МАТЕМАТИЧНА МОДЕЛЬ ФОРМУВАННЯ ПСЕВДОВИПАДКОВОЇ ПІДКЛАДКИ PAD НА ССС МАК-ЕЛІСА НА МЕС

Крок 1. Формування відкритого тексту M

*укорочення* $M_i = \{I_0, I_{h_1}, .. I_{h_j}, I_{k-1}\}$

*подовження* $M_i = \{I_0, I_{h_{r_1}}, .. I_{h_{r_j}}, I_{k-1}\}$

Крок 2. Формування закритого тексту

*укорочення* $C_i = (c^*_{X_0}, c^*_{h_1}, ..., c^*_{h_j}, c^*_{X_{n-1}})$

*подовження* $C_i = (c^*_{X_0}, c^*_{h_{r1}}, ..., c^*_{h_{r_j}}, c^*_{X_{n-1}})$

Крок 3. Формування безлічі прямих відображень $\phi = \{\phi_1, \phi_2, ... \phi_s\}$

*укорочення* $\phi_i : M \to C_{k-h_j}$

*подовження* $\varphi_i : M \to C_{h_r}$

Крок 4. Формування безлічі зворотних відображень $\phi^{-1} = \{\phi_1^{-1}, \phi_2^{-1}, ... \phi_s^{-1}\}$

*укорочення* $\phi_i^{-1} : C_{k-h_j} \to M$

*подовження* $\varphi_i^{-1} : C_{h_r} \to M$

Крок 5. Формування відкритого ключа

$K_{a_i} = \{K_{1_{a_i}}, K_{2_{a_i}}, ..., K_{s_{a_i}}\} = \{G_X^{EC_1}{}_{a_i}, G_X^{EC_2}{}_{a_i}, ..., G_X^{ECs}{}_{a_i}\}$

*укорочення* $\phi_i : M \xrightarrow{K_{ia_i}} C_{k-h_j}$

*подовження* $\varphi_i : M \xrightarrow{K_{ia_i}} C_{h_r}$

Крок 6. Формування закритого ключа

$K^* = \{K_1^*, K_2^*, ..., K_s^*\} = \{\{X, P, D\}_1, \{X, P, D\}_2, ..., \{X, P, D\}_s\}$

$\{X, P, D\}_i = \{X^i, P^i, D^i\}$

$\phi_i^{-1} : C \xrightarrow{K_i^*} M$

Крок 7. Формування випадкового (n, k, d)-коду $G_X^{ECu} = X^u \times G^{EC} \times P^u \times D^u,\ u \in \{1, 2, ..., s\}$

Крок 8. Формування закритого тексту (n, k, d)-коду

$$C_j = \phi_u\left(M_i, G_X^{ECu}{}_{a_i}\right) = M_i \times \left(G_X^{ECu}{}_{a_i}\right)^T + e$$

$$Pad_{\text{MEC}} = PDF(i \times G_X^{EC_i} + e + IV_{1/2}, Nonce, Taglen)$$

# ЧЕТВЕРТИЙ НАУКОВИЙ РЕЗУЛЬТАТ

***Вперше*** **розроблено модель формування псевдовипадкової підкладки каскадного алгоритму UMAC на основі крипто-кодових конструкцій Мак-Еліса на алгеброгеометричних кодах** – дозволяє забезпечити рівень безпеки (безпечний час – $T_Б$> 200 р., стійкість до криптоаналізу $P_К$ <$10^{25}$ - $10^{35}$ групових операцій), а також в умовах кібератак підвищити рівень захищеності послуг безпеки в постквантовий криптоперіод.

# МАТЕМАТИЧНА МОДЕЛЬ ФОРМУВАННЯ ПСЕВДОВИПАДКОВОЇ ПІДКЛАДКИ PAD НА ГККК МАК-ЕЛІСА НА ЗБИТКОВИХ КОДАХ

Крок 1. Формування відкритого тексту M

*укорочення* $M_i = \{I_0, I_{h_1}, .. I_{h_j}, I_{k-1}\}$

*подовження* $M_i = \{I_0, I_{h_{r1}}, .. I_{h_{r_j}}, I_{k-1}\}$

Крок 2. Формування закритого тексту

*укорочення* $C_i = (c^*_{X_0}, c^*_{h_1}, ..., c^*_{h_j}, c^*_{X_{n-1}})$

*подовження* $C_i = (c^*_{X_0}, c^*_{h_{r1}}, ..., c^*_{h_{r_j}}, c^*_{X_{n-1}})$

Крок 3. Формування безлічі прямих відображень $\phi = \{\phi_1, \phi_2, ... \phi_s\}$

*укорочення* $\phi_i : M \to C_{k-h_j}$

*подовження* $\varphi_i : M \to C_{h_r}$

Крок 4. Формування безлічі зворотних відображень $\phi^{-1} = \{\phi_1^{-1}, \phi_2^{-1}, ... \phi_s^{-1}\}$

*укорочення* $\phi_i^{-1} : C_{k-h_j} \to M$

*подовження* $\varphi_i^{-1} : C_{h_r} \to M$

Крок 5. Формування відкритого ключа $K_{a_i} = \{K_{1_{a_i}}, K_{2_{a_i}}, ..., K_{s_{a_i}}\} = \{G_X^{EC_1}{}_{a_i}, G_X^{EC_2}{}_{a_i}, ..., G_X^{ECs}{}_{a_i}\}$

*укорочення* $\phi_i : M \xrightarrow{K_{ia_i}} C_{k-h_j}$

*подовження* $\varphi_i : M \xrightarrow{K_{ia_i}} C_{h_r}$

Крок 6. Формування закритого ключа $K^* = \{K_1^*, K_2^*, ..., K_s^*\} = \{\{X, P, D\}_1, \{X, P, D\}_2, ..., \{X, P, D\}_s\}$

$\{X, P, D\}_{i^*} = \{X^i, P^i, D^i\}$

$\phi_i^{-1} : C \xrightarrow{K_i} M$

Крок 6. Формування залишку та збитку

$C_j^* = C_j - C_{k-h_j}$, $E_{K_{MV2}} : C_j^* \to \left\| f(x)_i \right\| + \left\| C(x)_i \right\|$

$C_j^* = C_{h_r}$, $E_{K_{MV2}} : C_j^* \to \left\| f(x)_i \right\| + \left\| C(x)_i \right\|$.

Крок 7. Формування випадкового (n, k, d)-коду $G_X^{ECu} = X^u \times G^{EC} \times P^u \times D^u$, $u \in \{1, 2, ..., s\}$

Крок 8. Формування закритого тексту (n, k, d)-коду

$C_j = \phi_u\left(M_i, G_X^{ECu}{}_{a_i}\right) = M_i \times \left(G_X^{ECu}{}_{a_i}\right)^T + e$

$$Pad_{\text{MEC\_DC}} = PDF(i \times G_X^{EC_i} + e + IV_{1/2}, Nonce, Taglen)$$

# П’ЯТИЙ НАУКОВИЙ РЕЗУЛЬТАТ

***Вперше*** **розроблено модель формування псевдовипадкової підкладки каскадного алгоритму UMAC на основі крипто-кодових конструкцій Мак-Еліса на збиткових кодах** – дозволяє забезпечити практичне використання в смарт-технологіях з обмеженими обчислювальними ресурсами.

# МАТЕМАТИЧНИЙ АПАРАТ ДОСЛІДЖЕННЯ КОЛІЗІЙНИХ ВЛАСТИВОСТЕЙ UMAC

**Введені наступні позначення**:

$$n_1(x_1, x_2) = \left|\left\{h \in H : h(x_1) = h(x_2)\right\}\right|, \; x_1, x_2 \in A, \; x_1 \neq x_2; \quad (1)$$

$$n_2(x_1, y_1) = \left|\left\{h \in H : h(x_1) = y_1\right\}\right|, \; x_1 \in A, \; y_1 \in B; \quad (2)$$

$$n_3(x_1, x_2, y_1, y_2) = \left|\left\{h \in H : h(x_1) = y_1, h(x_2) = y_2\right\}\right|, \; x_1, x_2 \in A, \; x_1 \neq x_2, \; y_1, y_2 \in B. \quad (3)$$

*Статистичні показники оцінки колізійних властивостей*:

- математичні очікування $m(n_1), m(n_2), m(n_3)$ максимумів кількості правил гешування, при яких виконуються рівняння у визначеннях 1, 2;

- дисперсії $D(n_1), D(n_2), D(n_3)$ , характеризують розкид значень максимумів кількості правил гешування, відносно їх математичних очікувань.

У якості ***статистичної оцінки*** математичного очікування та дисперсії випадкової величини будемо використовувати:

$$\tilde{m} = \frac{1}{N}\sum_{i=1}^{N} X_i, \;\; \tilde{D} = \frac{1}{N-1}\sum_{i=1}^{N} (X_i - \tilde{m})^2.$$

При більших *N* середнє арифметичне буде мати розподіл, близький до нормального с математичним очікуванням $m[\tilde{m}] \approx \tilde{m}$ та ВКО $\sigma[\tilde{m}] \approx \sigma / \sqrt{N}$ .

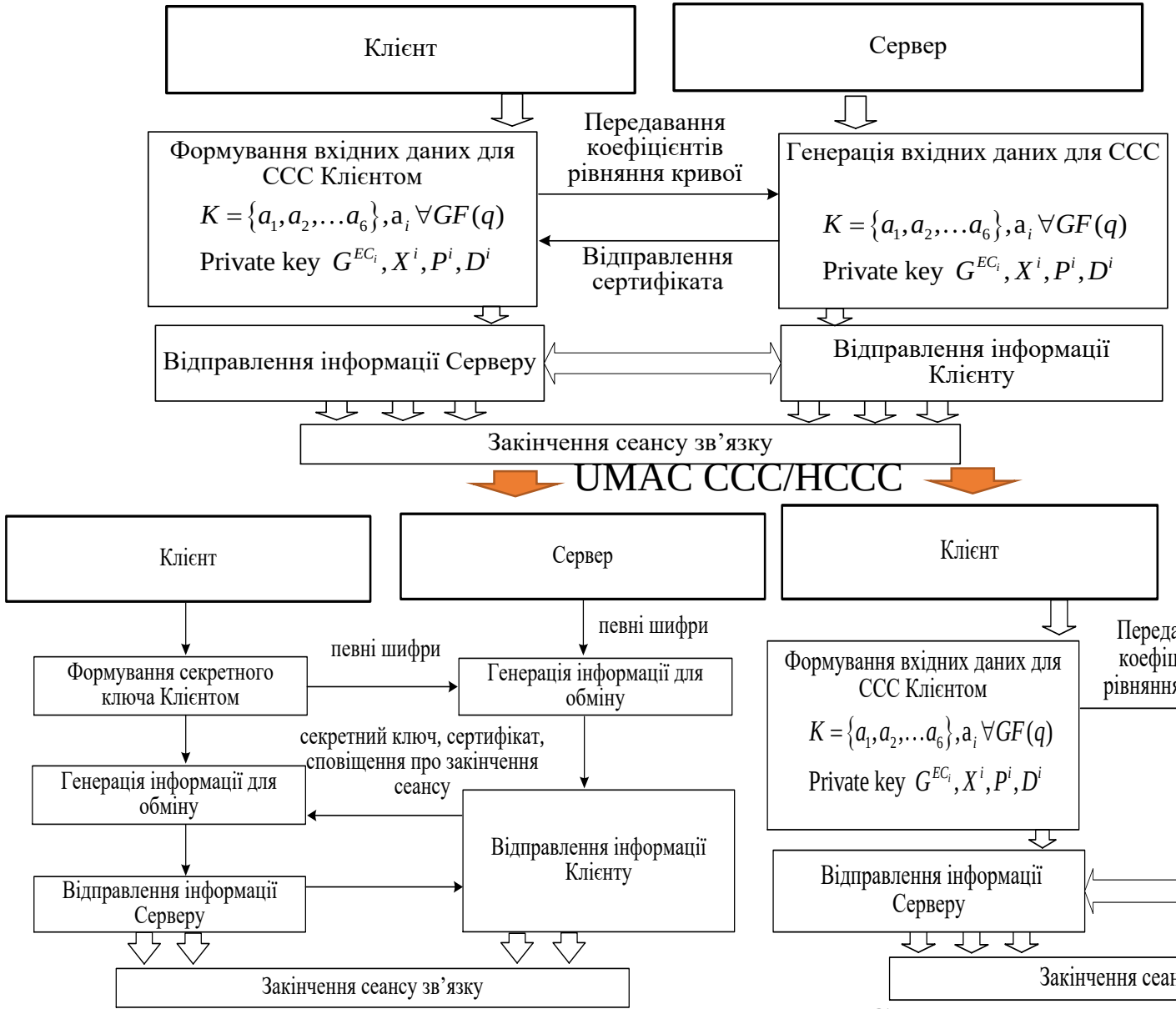
***Довірча ймовірність:*** $P(|\tilde{m} - m| < \varepsilon) \approx 2\Phi\left(\frac{\varepsilon}{\sigma[\tilde{m}]}\right), \quad \Phi(x) = \frac{1}{\sqrt{2\pi}}\int_0^x e^{-\frac{t^2}{2}} dt.$

***Довірчий інтервал*** (для заданої) $P_д$ $\tilde{m} - t_\rho \cdot \sigma[\tilde{m}] < m < \tilde{m} + t_\rho \cdot \sigma[\tilde{m}], \quad 2\Phi(t_\rho) = P_д$

# РЕЗУЛЬТАТИ ПЕРЕВІРКИ ГЕШ-КОДІВ UMAC+CCC НА КОЛІЗІЙНІ ВЛАСТИВОСТІ

| **Статистичні характеристики експерименту** | **MASH-1** | **MASH-2** | **mini-UMAC MASH-1** | **mini-UMAC MASH-2** | **mini-UMAC AES** | **mini-UMAC** ККК |
|---|---|---|---|---|---|---|
| $m(n_1)$ | ***7,09**** | ***7,14**** | 1,965 | 1,968 | 1,096 | 1,166 |
| $D(n_1)$ | 1,69 | 1,56 | 0,123 | 0,120 | 0,094 | 0,599 |
| $m(n_1)-\varepsilon_1$ | 7,061 | 7,111 | 1,957 | 1,961 | 1,088 | 1,148 |
| $m(n_1)+\varepsilon_1$ | 7,122 | 7,169 | 1,973 | 1,977 | 1,103 | 1,184 |
| $m(n_2)$ | 1,013 | 1,014 | ***2,629**** | ***2,64**** | 1,532 | 1,161 |
| $D(n_2)$ | 0,013 | 0,014 | 0,349 | 0,355 | 0,36 | 0,67 |
| $m(n_2)-\varepsilon_2$ | 1,01 | 1,011 | 2,62 | 2,63 | 1,52 | 1,14 |
| $m(n_2)+\varepsilon_2$ | 1,02 | 1,017 | 2,64 | 2,65 | 1,55 | 1,18 |
| $m(n_3)$ | 1,0008 | 1,0002 | ***0,237**** | ***0,224**** | ***0,0005**** | ***0**** |
| $D(n_3)$ | $9993\cdot10^{-8}$ | $9999\cdot10^{-8}$ | 0,184 | 0,177 | $499\cdot10^{-6}$ | 0 |
| $m(n_3)-\varepsilon_3$ | 1,00006 | 0,9994 | 0,227 | 0,214 | -2,087 | 0 |
| $m(n_3)+\varepsilon_3$ | 1,002 | 1,0009 | 0,247 | 0,234 | 0,001 | 0 |

# МОДИФІКОВАНИЙ ПРОТОКОЛ SSL/TLS НА CCC/UMAC




Структурна схема вдосконаленого протоколу SSL/TLS

Структурна схема вдосконаленого протоколу SSL/TLS в режимі 0-RTT

# ШОСТИЙ НАУКОВИЙ РЕЗУЛЬТАТ

***Удосконалено протокол SSL/TLS на основі комплексованих алгоритмів – крипто-кодових конструкцій Мак-Еліса на модифікованих та/або збиткових кодах з удосконаленим каскадним алгоритмом UMAC*** – забезпечує необхідний рівень безпеки в постквантовий криптоперіод, обчислювальних та енергоємнісних вимог до використання в кіберфізичних системах на основі смарт-технологій.

# РЕЗУЛЬТАТИ СТАТИСТИЧНОЇ БЕЗПЕКИ АЛГОРИТМА UMAC НА ККК МАК-ЕЛІСА

| Криптосистеми | Кількість тестів, у яких тестування пройшло понад 99% послідовностей | Кількість тестів, у яких тестування пройшло понад 96% послідовностей | Кількість тестів, у яких тестування пройшло менше ніж 96% послідовностей |
|---|---|---|---|
| UMAC+CCC Мак-Еліса на *EC* | 149 (78,83%) | 189 (100%) | 0 (0%) |
| UMAC+CCC Мак-Еліса на укорочених *MEC* | 151 (79,89%) | 189 (100%) | 0 (0%) |
| UMAC+CCC Мак-Еліса на подовжених *MEC* | 152 (80,42%) | 189 (100%) | 0 (0%) |
| UMAC+HCCC Мак-Еліса на подовжених *MEC* | **153** (80,95%) | 189 (100%) | 0 (0%) |
| UMAC+HCCC Мак-Еліса на укорочених *MEC* | **155** (82 %) | 189 (100%) | 0 (0%) |

# РЕЗУЛЬТАТИ ПОРІВНЯЛЬНОГО АНАЛІЗУ ФУНКЦІЙ ГЕШУВАННЯ

| Геш-функція | Довжина геш-коду, біт | Перетворення, що застосовуються | Швидкість формування геш-коду, біт/с | Модель безпеки (за NESSIE) |
|---|---|---|---|---|
| UMAC+ MASH-1 | розмірність модуля перетворень | Модулярне піднесення до квадрата | $10^5..10^6$ | Доведена безпека (“Provable” Security) |
| UMAC+ MASH-2 | розмірність модуля перетворень | Модулярне піднесення до степеня $2^8+1 = 257$ | $10^4..10^5$ | Доведена безпека (“Provable” Security) |
| POLY1305-AES | 128 | В кінцевих полях Галуа | $10^6..10^7$ | Практична секретність (Practical Security) |
| AES GCM | 128<br>256 | В кінцевих полях Галуа | $10^7..10^8$ | Практична секретність (Practical Security) |
| UMAC+ AES | 128<br>256 | В кінцевих полях Галуа | $10^8 ..10^9$ | Практична секретність (Practical Security) |
| UMAC+ CCC/HCCC | 16...96 | На еліптичних кривих | $10^8 ..10^9$ | Практична секретність (Practical Security) |

# РЕЗУЛЬТАТИ ЯКІСНОЇ ОЦІНКИ АНАЛІЗУ ІСНУЮЧИХ МЕТОДІВ



| показники | алгоритми формування псевдовипадкової підкладки Pad | | | | | |
|---|---|---|---|---|---|---|
| | UMAC+ MASH-1 | UMAC+ MASH-2 | POLY1305-AES | AES GCM | UMAC+ AES | UMAC+ CCC |
| універсальність | + | + | – | + | – | + |
| стійкість до постквантових зломів | – | + | – | – | – | + |
| оперативність формування | – | – | – | – | + | + |
| незалежність від обчислювальних потужностей | – | – | + | + | – | + |

# ВИСНОВКИ: ОСНОВНІ НАУКОВІ ТА ПРАКТИЧНІ РЕЗУЛЬТАТИ

**У дисертації вирішені теоретичне узагальнення та розв'язання актуальної задачі розроблення нових та удосконалення існуючих моделей і методів забезпечення цілісності та автентичності інформації, яка циркулює в кіберпросторі в умовах постквантового періоду. Розроблені моделі та методи** забезпечать необхідний рівень безпеки на рівні симетричних алгоритмів шифрування, що дає змогу підтримувати необхідний рівень швидкодії криптоперетворень і практичної реалізації для використання в кіберфізичних системах.

***Вперше*** **розроблено модель формування псевдовипадкової підкладки каскадного алгоритму UMAC на основі крипто-кодових конструкцій Мак-Еліса на алгеброгеометричних кодах**, що дозволяє забезпечити рівень безпеки (безпечний час – $T_Б$> 200 р., стійкість до криптоаналізу $P_K$ <$10^{25}$ групових операцій), а також в умовах кібератак підвищити рівень захищеності послуг безпеки в постквантовий криптоперіод.

***Вперше*** **розроблено модель формування псевдовипадкової підкладки каскадного алгоритму UMAC на основі крипто-кодових конструкцій Мак-Еліса на збиткових кодах**, що дозволяє забезпечити практичне використання в смарт-технологіях з обмеженими обчислювальними ресурсами.

***Вперше*** **запропоновано метод забезпечення автентичності та цілісності на основі каскадного алгоритма UMAC на основі крипто-кодових конструкцій Мак-Еліса з еліптичними кодами**, що дозволяє забезпечити його використання в постквантовий криптоперіод

***Вперше*** **запропоновано метод забезпечення автентичності та цілісності на основі каскадного алгоритма UMAC на основі крипто-кодових конструкцій Мак-Еліса з модифікованими (укороченими та/або подовженими) еліптичними кодами**, що дозволяє забезпечити зменшення обчислювальної ємності та зберегти стійкість до зламу

***Вперше*** **запропоновано метод забезпечення автентичності та цілісності на основі каскадного алгоритма UMAC на гібридних крипто-кодових конструкціях Мак-Еліса на збиткових кодах**, що дозволяє забезпечити практичне використання в смарт-технологіях з обмеженими обчислювальними ресурсами.

***Удосконалено*** **протокол SSL/TLS на основі комплексованих алгоритмів – крипто-кодових конструкцій Мак-Еліса на модифікованих (збиткових) кодах з удосконаленим каскадним алгоритмом UMAC**, що забезпечує необхідний рівень безпеки в постквантовий криптоперіод, обчислювальних та енергоємнісних вимог до використання в кіберфізичних системах на основі смарт-технологій

# ПУБЛІКАЦІЇ, АПРОБАЦІЯ ТА РЕАЛІЗАЦІЯ РЕЗУЛЬТАТІВ ДИСЕРТАЦІЇ

## ПУБЛІКАЦІЇ

Основні положення дисертації опубліковано у **27** наукових працях з яких:

<u>в співавторстві</u>:

- ❑ **3** монографії (**1** – Scopus, **1** – закордонне, **1** – вітчизняне фахові наукові видання );
- ❑ **3** наукові статті у міжнародних рецензованих виданнях, що входять до баз даних *Scopus*;
- ❑ **9** наукових статей (**3** – закордонні видання та **6** у вітчизняних фахових наукових журналах, які входять до інших міжнародних наукометричних баз даних;
- ❑ **12** матеріалів і тез доповідей на міжнародних конференціях.

<u>без співавторів</u> – опубліковано **1** наукову статтю.

## РЕАЛІЗАЦІЇ

Результати впроваджено у діяльність:

- ➢ ТОВ “Сайфер ІТ” (№ 22/23 від 05.01.2023);
- ➢ отримано 2 патенти на корисну модель.

# ДЯКУЮ ЗА УВАГУ!