SMARTINCRYPTO

ПРИВАТНІСТЬ ДЛЯ ВАШОГО РОЗУМНОГО БУДИНКУ

01

МЕТА ПРОЕКТУ

Створення програмно-апаратного комплексу для криптографічного захисту кіберфізичних систем «розумний дім»

02

ЗАВДАННЯ ПРОЕКТУ

Забезпечити послуги безпеки даних у системі «розумний дім» на основі використання постквантових криптосистем
Забезпечити безпеку у постквантовий період на основі багатоконтурних систем безпеки

Проблема

ПРОБЛЕМА 1

Проблема захисту будь-яких каналів зв'язку значно загостриться у найближчому майбутньому з винаходом повномасштабного квантового комп'ютера

ПРОБЛЕМА 2

Використовуючи його потужність можна досить швидко зламувати атакою грубої сили симетричні та несиметричні криптосистеми

ПРОБЛЕМА 3

Зламування системи безпеки призведе до руйнування безперервності бізнес-процесів, що забезпечують прибуток та/або роботу виробництва

Рішення

✓ **РІШЕННЯ 1**

Ми пропонуємо «закрити» канал зв'язку за допомогою програмно-апаратного комплексу, що ґрунтується на використанні запатентованої нами технології постквантових криптосистем.

✓ **РІШЕННЯ 2**

Технологія забезпечить необхідний рівень безпеки у постквантовий період

✓ **РІШЕННЯ 3**

Дозволить уникнути хаосу та відсутності послуг безпеки у сучасних інформаційно-комунікаційних технологіях, збитки можуть обчислюватися мільйонами та мільярдами доларів.

НДДКР

Результати досліджень опубліковано в українських та міжнародних виданнях, що входять до наукометричної бази Scopus (2015-2023 рр.), а також отримано патенти на корисну модель (Україна)

Експериментальні випробування проведено в Україні (в організаціях ТОВ «Сайфер БІС», ТОВ «ТАНТАРІУМ», ТОВ «Мікрокрипт Текнолоджіс», ВАТ «МЕГАБАНК»)

Запропонована технологія дозволить забезпечити безпеку в постквантовий період будь-якого каналу зв'язку та гарантує:

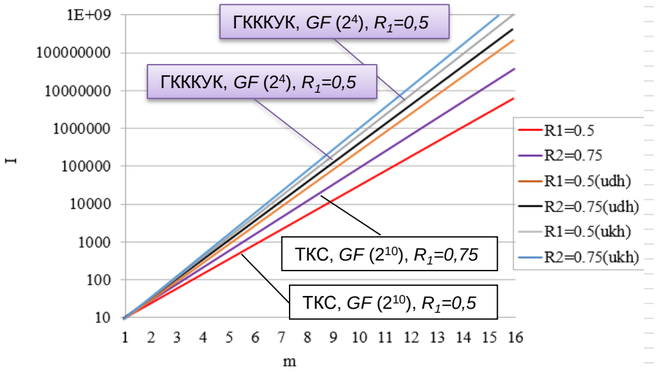
- високий рівень захисту від злому – 82% пройдених тестів NIST STS 822 з ймовірністю 99%. (Традиційна криптосистема - 78,83%);
- зниження складності кодування (у 12 разів) та розкодування кодограми (криптограми) (у 20 разів) порівняно з класичною схемою Мак-Еліса

Частина дослідження базується на завершених НДР 2016-2021 (Україна):
№ 36Б115 "Розробка методів синтезу тестових моделей поведінки програмних об'єктів, підвищення оперативності передачі та захисту інформації в телекомунікаційних системах" (**№ 0115U003103**)
"Розробка алгоритмів несиметричного шифрування для мобільних засобів зв'язку" (**№ 0116U005696**)
"Розробка методу підвищення конфіденційності та ймовірності банківської інформації в автоматизованих банківських системах" (**№. 0117U000136**)
№ 15/2016-2017
"Методологія побудови системи забезпечення безпеки банківської інформації: аналіз проблеми та синтез нових рішень" **(№. 0117U001628**)

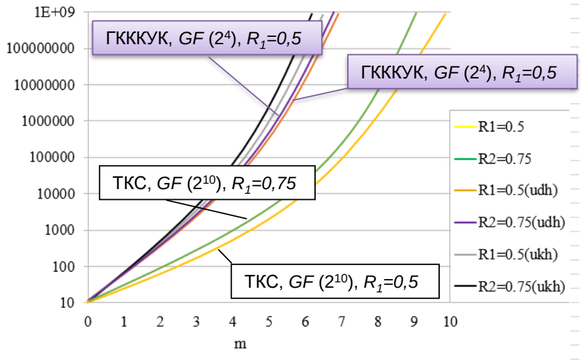
НДДКР

Наукова новизна: вперше розроблено технологію забезпечення конфіденційності та цілісності інформаційних ресурсів на основі **крипто-кодових конструкцій з алгеброгеометричними та/або неповноцінними кодами,** що дозволяє підвищити рівень конфіденційності, цілісності та достовірності інформаційних ресурсів в умовах дії APT-загроз.

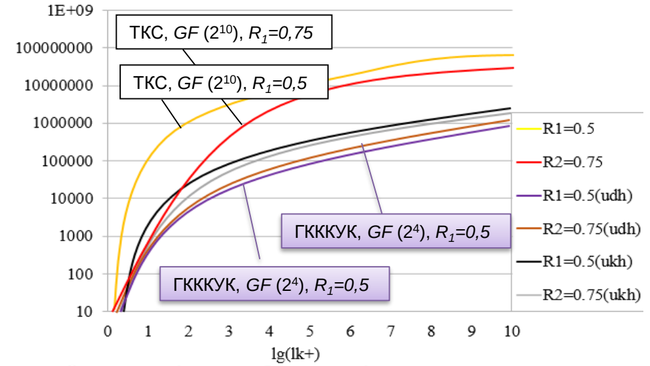
ВЕРИФІКАЦІЯ ВЛАСТИВОСТЕЙ ГККККУК



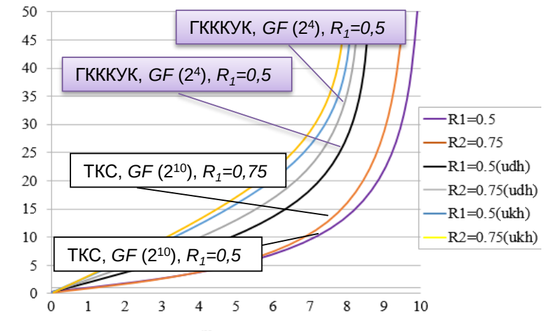
Залежність складності формування криптограми в різних GF (2^m)



Залежність складності розкодування криптограми в різних GF (2^m)



Залежність обсягу відкритих ключових даних



Залежність складності злому

Результати дослідження статистичної безпеки (NIST STS 822)

Криптосистеми	Кількість тестів, у яких тестування пройшли понад 99% послідовностей	Кількість тестів, у яких тестування пройшли понад 96% послідовностей	Кількість тестів, у яких тестування пройшли менше 96% послідовностей
НККС McEliece	149 (78,83%)	189 (100%)	0 (0%)
МНККС McEliece на скорочених МЕС	151 (79,89%)	189 (100%)	0 (0%)
МНККС McEliece на подовжених МЕС	152 (80,42%)	189 (100%)	0 (0%)
ГККККЗК на подовжених МЕС	153 (80,95%)	189 (100%)	0 (0%)
ГККККЗК на скорочених МЕС	155 (82 %)	189 (100%)	0 (0%)

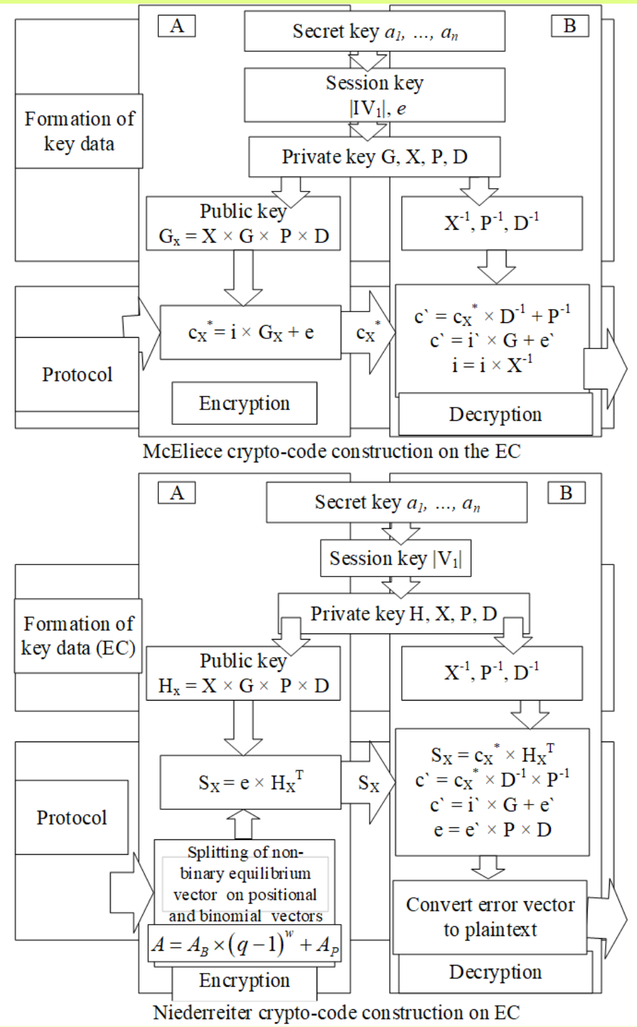
Залежність швидкості програмної реалізації від потужності поля

Криптосистеми	$GF(q^m)$						
	2^4	2^5	2^6	2^7	2^8	2^9	2^{10}
МНККС Мак-Элиса на скорочених МЕС	8293075	10007947	**17787431**	28595014	44079433	61974253	79554764
МНККС Мак-Элиса на подовжених МЕС	8506422	11156138	**18561228**	33210708	48297112	65171690	84051337
ГККККУК подовжених МЕС	**5612316**	7900315	14892945	25565274	42279183	58963778	76564173
ГККККУК скорочених МЕС	**5942627**	7905257	14682411	25595014	42116327	58468143	75474764

Технологія Smart Incrypto

Конкурентна перевага:

- вартість
- незалежні від моделей систем «розумний будинок» чи провайдерів зв'язку
- підвищення рівня безпеки систем «розумний дім»



Результати за проектом

STEP 3

близько 4-х місяців

Впровадження технології в інших галузях

STEP 2

близько 3-х місяців

Створення готового продукту для продажу ліцензії

STEP 1

6-9 місяців

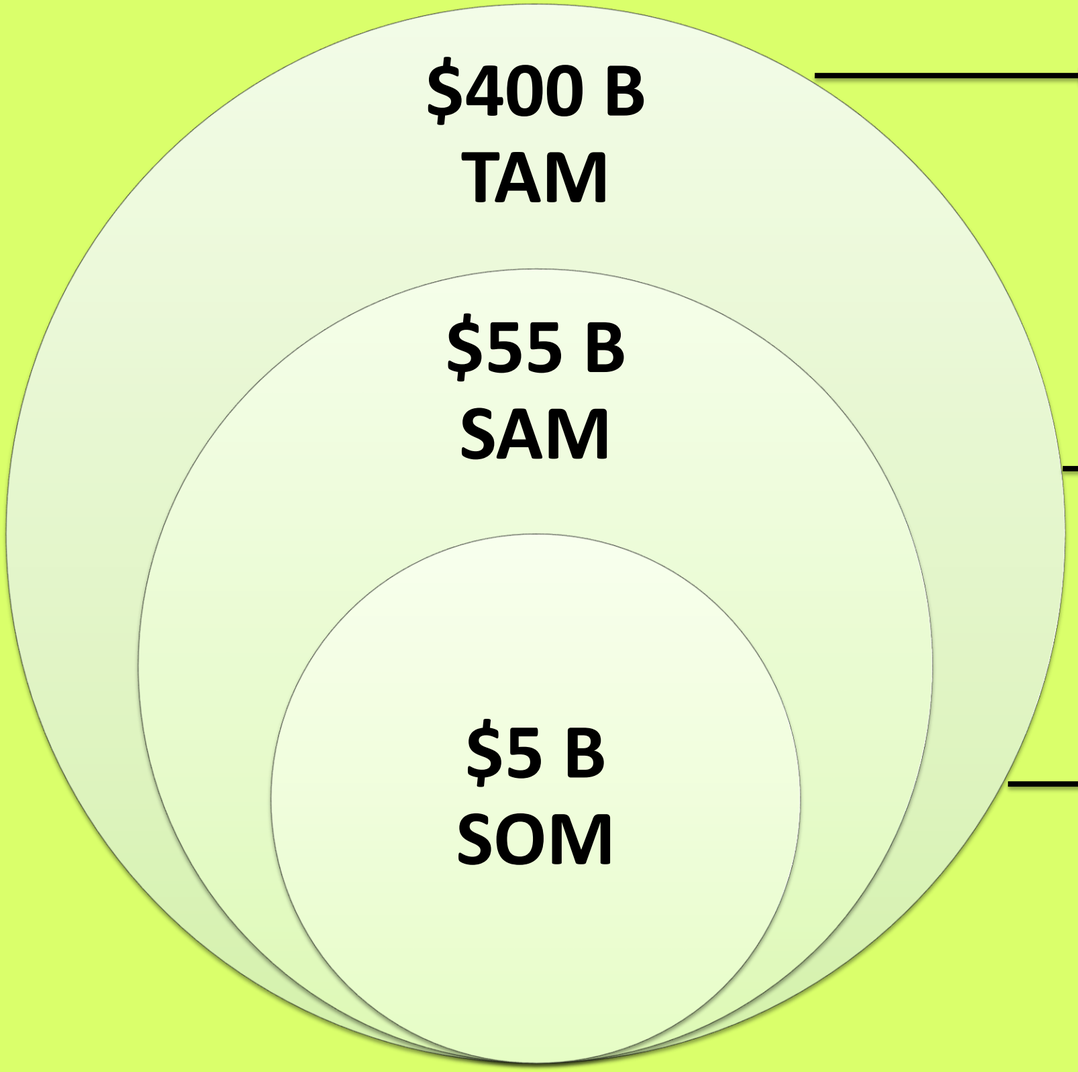
Створення MVP

Для побудови системи закриття будь-яких каналів зв'язку розроблено:

- ❑сервер генерації ключів,
- ❑мобільний додаток,
- ❑чіпсет із прошитым шифратором

Прототип розроблений та функціонує

Обсяг ринку



Розмір глобального ринку IoT
400 млрд доларів США

Безпека "розумних" пристроїв для дому та офісу
55 млрд доларів США

Досяжний обсяг ринку програмного забезпечення для захисту IoT
5 млрд. доларів США

Конкуренти

Компанія	Веб-сайт
Armis	https://www.armis.com/
Claroty	https://claroty.com/
Finite State	https://finitestate.io/
Forescout	https://www.forescout.com/
Ordr	https://ordr.net/
Palo Alto Networks	https://www.paloaltonetworks.com/
Phosphorus Cybersecurity	https://inbound.aexus.com/
Shield-IoT	https://inbound.aexus.com/
TXOne Networks	https://www.txone.com/
Xage Security	https://xage.com/

Нашими конкурентами є виробники захищених IoT-систем на основі смарт-технологій

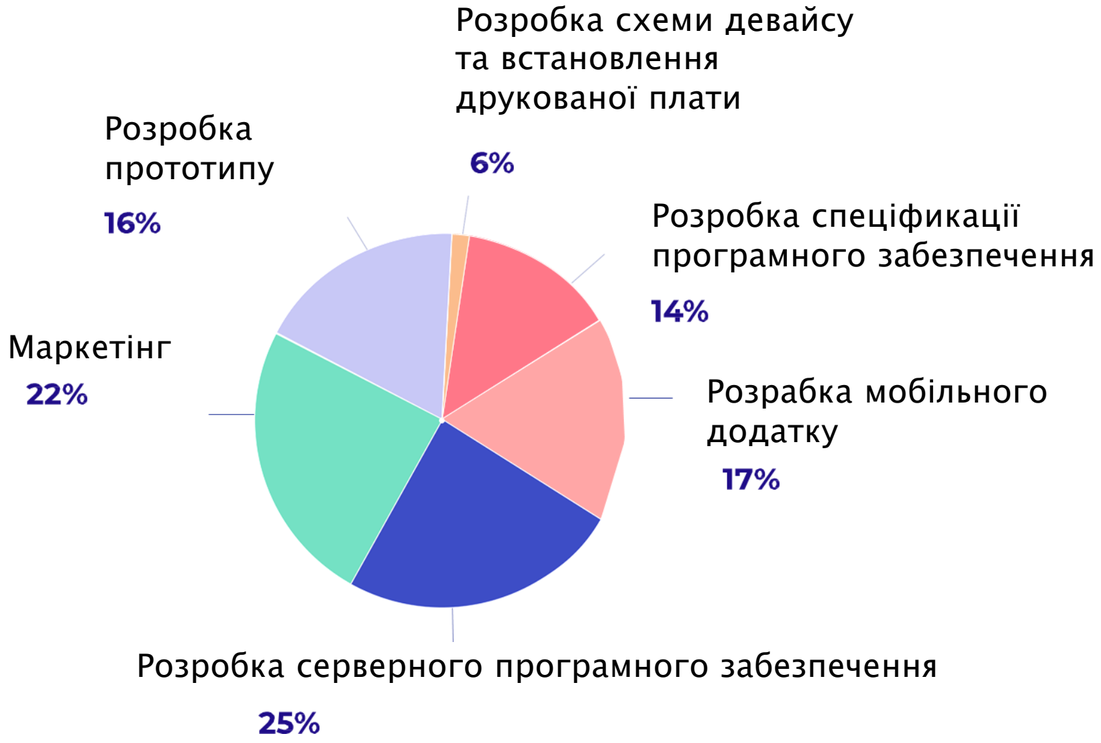
Наш продукт має меншу вартість, не залежить від моделей систем «розумний дім» або провайдерів комунікацій і дозволяє підвищити рівень безпеки систем «розумний дім» на основі постквантових крипто-систем – крипто-кодових конструкцій на алгеброгеометричних кодах.

Бізнес модель

Потенційними клієнтами є виробники систем безпеки «Розумного дому» та всі зацікавлені особи

Бізнес-модель: (**B2B** продаж ліцензії)
$50,000 – паушальний платіж
$25 від кожного проданого комплекту – роялті
Для створення MVP необхідно близько **$260,000** на витрати за напрямками на діаграмі –Ці кошти окупляться вже після продажу **6-ти ліцензій.**

Бізнес-моделлю стартапу є **B2B**, а саме, продаж ліцензії компаніям виробникам систем безпеки для «Розумного дому» на використання технології стартапу в їхніх продуктах



Команда проекту

Serhii Yevseiev
CEO/Technology development

Vladyslav Khvostenko
Business planning

Anna Strelnikova
Research

Roman Korolyov
Technology development

Serhii Pohasii
Device development

Serhii Dunaev
IT development

Stanislav Milevskyi
Information-communication support

Andrii Kopp
Communication

ПРОПОЗИЦІЯ ДЛЯ СПІВПРАЦІ

Комерційна пропозиція для потенційного бізнес-партнера

- Ми хочемо запропонувати виробникам систем «розумний дім» ліцензію на використання нашої технології криптографічного захисту каналів зв'язку у постквантовий період
- У ліцензію входить: користування програмним забезпеченням для програматора чіпсетів та сервером для генерації ключів
- Ця ліцензія дозволить вам випустити нову лінійку вашої продукції, яка надаватиме можливість забезпечити послуги безпеки даних приватного життя клієнтів
- Ми також готові розглянути будь-які способи співпраці та відкриті для діалогу
- Пропонуємо організувати онлайн-зустріч для обговорення деталей нашої пропозиції

Контакты

Serhii Yevseiev

Сергій Євсеєв

PHONE NUMBER

+ 38 (095) 360-66-13

EMAIL

serhii.yevseiev@gmail.com

WEBSITE

http://smart.incrypto.ltd/

SMARTINCRYPTO