Реєстраційна картка технології (РКТ)

5436. Державний реєстраційний номер: 0623U000076

5517. № Держреєстрації НДДКР: 0120U102607

5256. Особливі позначки: 5

9000. Походження технології: С

9159. Договір: немає

Відомості про заявника технології

2459. Код ЄДРПОУ (або реєстраційний номер облікової картки платника податків для фізичних осіб): 05390336

2151. Повне найменування юридичної особи (або П.І.Б.)

1 - українською мовою

Черкаський державний технологічний університет

2 - англійською мовою

Cherkasy State Technological University

2358. Скорочене найменування юридичної особи: ЧДТУ

2655. Місцезнаходження: бульвар Шевченка, буд. 460, м. Черкаси, Черкаський р-н., Черкаська обл., 18006, Україна

2934. Телефон / Факс: 380472434481; 380472513672

2394. Адреса електронної пошти/веб-сайт: chdtu@chdtu.edu.ua; https://chdtu.edu.ua/

1333. Форма власності, сфера управління: Міністерство освіти і науки України

Відомості про власника технології

2458. Код ЄДРПОУ (або реєстраційний номер облікової картки платника податків для фізичних осіб): 05390336

2152. Повне найменування юридичної особи (або П.І.Б.)

1 - українською мовою

Черкаський державний технологічний університет

3 - англійською мовою

Cherkasy State Technological University

2360. Скорочене найменування юридичної особи: ЧДТУ

2656. Місцезнаходження: бульвар Шевченка, буд. 460, м. Черкаси, Черкаський р-н., Черкаська обл., 18006, Україна

2935. Телефон / Факс: 380472434481; 380472513672

2395. Адреса електронної пошти/веб-сайт: chdtu@chdtu.edu.ua; https://chdtu.edu.ua/

1332. Форма власності, сфера управління: Міністерство освіти і науки України

Джерела, напрями та обсяги фінансування

7700. КПКВК: 2201040

7201. Напрям фінансування: 2.2 - прикладні дослідження і розробки

Код джерела фінансування	Обсяг фінансування, тис. грн.
7711	150,00
7713	150,00

Терміни виконання роботи

7553. Початок виконання НДДКР: 01.2020

7362. Закінчення виконання НДДКР: 12.2022

Відомості про технологію

9027. Назва технології

1 - українською мовою

Трьохетапний криптографічний протокол на основі перестановок

3 - англійською мовою

Three-pass protocol on permutations

9125.Опис технології

1. Мета, для досягнення якої розроблено чи придбано технологію

Підвищення захищеності інформаційного обміну на основі трьохетапного криптографічного протоколу.

2. Основна суть технології

Трьохетапний криптографічний протокол за рахунок виконання операцій над перестановками чисел, зокрема їх множення, піднесення до степенів їхніх непересічних циклів, а також пошуку спряженої перестановки дозволяє підвищити стійкість криптографічного перетворення інформації.

3. Анотований зміст

Трьохетапний криптографічний протокол на основі перестановок базується на складності факторизації перестановки та складності реалізації перетворень, які є зворотними до нелінійних операцій на основі ідентичної циклової структури спряжених перестановок.

4. Проблеми, які технологія дає змогу вирішувати

Інші відомі трьохетапні криптографічні протоколи використовують шифр піднесення до степеня та є нестійкими до атак з використанням гіпотетичних квантових комп'ютерів. Розроблений трьохетапний криптографічний протокол використовує операції над перестановками, а його стійкість визначається як складністю факторизації перестановок, так і складністю зворотних перетворень над спряженими перестановками, враховуючи їх структурні особливості.

5. Ознаки новизни технології

Вперше для реалізації трьохетапного криптографічного протоколу застосовано перестановки, їх розкладання в добутки непересічних циклів, спряжені перестановки.

6. Складові технології

Формування спільної перестановки, формування таємних ключів учасників обміну, перетворення повідомлення.

Опис технології англійською мовою

Three-pass protocol on permutations use multiplication of permutations, raising to the power of their disjoint cycles, as well as the operation of finding the conjugate permutation. This avoids the problems associated with discrete logarithms, which can increase the cryptographic strength of the proposed protocol.

9127. Технічні характеристики

Трьохетапний криптографічний протокол може бути реалізовано в різноманітних пристроях зв'язку, в тому числі засобами малоресурсної криптографії. Для коректної роботи трьохетапного протоколу необхідно забезпечувати відсутність помилок у перестановці після її отримання з каналу зв'язку. Протокол розроблено для систем передавання інформації, що використовують нероздільне факторіальне кодування, проте може бути адаптований і для традиційних

систем, що не використовують факторіальний код. У останньому випадку до протоколу передавання даних необхідно додатково включити процедуру бієктивного відображення інформаційного блоку в перестановку.

9128. Техніко-економічний чи соціальний ефект

Трьохетапний криптографічний протокол на основі перестановок дозволяє обійти проблеми, пов'язані з дискретним логарифмуванням, і підвищити криптографічну стійкість протоколу.

5490. Об'єкти інтелектуальної власності

немає

9156. Основні переваги порівняно з існуючими технологіями

Трьохетапні протоколи на основі шифру піднесення до степеня не захищені від атак з використанням гіпотетичних квантових комп'ютерів. Операціями криптографічної трансформації запропонованого протоколу є операції множення перестановок, піднесення до степенів їх непересічних циклів, а також операція пошуку спряжених перестановок. Стійкість перетворення ґрунтується не лише на складності факторизації перестановок, а й на складності реалізації перетворень, зворотних до нелінійних операцій на основі однакової циклової структури спряжених перестановок.

9155. Галузь застосування

Комунікаційні системи захищеного зв'язку. Телекомунікаційні системи та мережі. Системи захисту інформації. Потенційні споживачі технології - виробники комунікаційного обладнання.

9158. Інформація щодо потенційних ринків збуту технології

Проведені дослідження маркетингового характеру свідчать, що потенційними споживачами отриманих науково-технічних результатів є розробники та виробники комунікаційного обладнання та систем. Рекомендації щодо застосування трьохетапного криптографічного протоколу на основі перестановок потенційно можуть представляти інтерес для Міжнародного консультаційного комітету з телефонії та телеграфії ITU-T, Національного інституту стандартів і технологій NIST, а також співтовариств Інституту інженерів з електротехніки та електроніки IEEE.

9160. Інформація щодо потенційних ринків збуту продукції, виробленої з використанням технології

Трьохетапний криптографічний протокол на основі перестановок може бути використано для створення програмно-апаратних комплексів захищеного обміну інформацією та реалізовано на глобальному ринку комунікаційних послуг.

9157. Ступінь відпрацювання технології

– 9157/TRL4 - перевірено прототип в лабораторії, технологію перевірено в лабораторії

5535. Умови поширення в Україні

53 - за договірною ціною

5211. Умови передачі зарубіжним країнам

63 - за договірною ціною

6012. Орієнтовна вартість технології та витрат на впровадження: 100 тис. грн.

6013. Особливі умови впровадження технології

немає

Підсумкові відомості

5634. Індекс УДК: 004.7, 004.056

5616. Коди тематичних рубрик НТІ: 50.37.23

6111. Керівник юридичної особи: Григор Олег Олександрович

6210. Науковий ступінь, вчене звання керівника юридичної особи: (д. політ. н., професор)

6120. Керівник НДДКР

1 - українською мовою

Фауре Еміль Віталійович

2 - англійською мовою

Faure Emil V.

6228. Науковий ступінь, вчене звання керівника НДДКР: (д. т. н., професор)

6140. Керівник структурного підрозділу МОН України: Чайка Дар'я Юріївна

Тел.: +38 (044) 287-82-55
Email.: chayka@mon.gov.ua

6142. Реєстратор: Іванов Олексій Васильович