DOI: https://doi.org/10.15276/ict.02.2025.12
УДК 004.056.5

Розробка та дослідження методики реалізації криптографічного протоколу з нульовим розголошенням для забезпечення конфіденційності верифікації віку

Морозов Андрій Романович[1)]
Магістр каф. Інформаційних систем
ORCID: https://orcid.org/0009-0001-7030-2667; andr.morozov96@gmail.com
Баськов Ілля Олександрович[1)]
Ст. викладач каф. Інформаційних систем
ORCID: https://orcid.org/0000-0002-3517-6773; illyabaskov@gmail.com. Scopus ID: 57788059000
[1)] Національний університет «Одеська політехніка», пр. Шевченка, 1. Одеса, 65044, Україна

АНОТАЦІЯ

У сучасних веб-системах верифікація віку користувачів є критично важливою для забезпечення відповідності законодавству про захист неповнолітніх в онлайн-середовищі. Традиційні підходи до перевірки віку включають завантаження копій документів, верифікацію через кредитні карти та підтвердження через службу коротких повідомлень. Ці методи мають низку недоліків, таких як порушення приватності користувачів, ризики витоку персональних даних та невідповідність вимогам Загального регламенту про захист даних. Зважаючи на посилення регуляторних вимог Європейського Союзу (Digital Services Act, 2024) та зростаючі побоювання користувачів щодо збереження особистих даних, виникає необхідність у впровадженні нових підходів, що забезпечують баланс між ефективною верифікацією та збереженням приватності.

У даному дослідженні розглянуто метод на основі криптографії з нульовим розголошенням, який дозволяє користувачу математично довести своє повноліття без розкриття точної дати народження чи інших персональних даних. Підхід використовує протокол криптографії з нульовим розголошенням Groth16 та бібліотеку snarkjs для генерації криптографічних доказів на клієнтській частині. Архітектура системи включає локальну обробку цифрових документів через оптичне розпізнавання тексту, генерацію доказу з нульовим розголошенням підтвердження "вік ≥ 18 років" та серверну верифікацію без доступу до особистих даних.

Порівняльний аналіз показав, що підхід з нульовим розголошенням значно перевершує традиційні методи за показниками приватності при збереженні прийнятної точності верифікації. Точність залежить від якості розпізнавання тексту: 90-95% для високоякісних сканів 300+ точок на дюйм (до 98% за ідеальних умов з preprocessing), 40-70% для типових фотографій зі смартфонів при використанні Tesseract розпізнавання тексту, хоча комерційні спеціалізовані рішення для документів можуть досягати 90-98%. Метод забезпечує повну відповідність принципу мінімізації даних регламенту про захист даних, оскільки сервер отримує лише криптографічне підтвердження повноліття без зберігання персональних даних. Час генерації доказу становить 40-50 секунд на сучасних мобільних пристроях для типових схем, хоча для найпростіших схем цей час може скорочуватись до 10-15 секунд за оптимальних умов, що залишається прийнятним для некритичних застосувань де пріоритетом є приватність. Підхід може протистояти спробам підробки завдяки криптографічним властивостям властивостям протоколів з нульовим розголошенням. Критичним обмеженням є необхідність інтеграції з довіреними джерелами даних (державні програмні інтерфейси або чіпи безконтактної комунікації в документах) для забезпечення автентичності вихідних даних, оскільки метод з нульовим розголошенням забезпечує приватність верифікації, але не автентифікацію джерела без додаткових криптографічних механізмів. Архітектура підходить для некритичних застосувань, де пріоритетом є відповідність вимогам приватності.

Ключові слова: криптографія з нульовим розголошенням; верифікація віку; приватність даних; регламенту про захист даних; цифрова ідентифікація; Groth16; zk-SNARKs; захист персональних даних

Актуальність. З впровадженням Регламенту Європейського Союзу (ЄС) про цифрові послуги (Digital Services Act, 2024) та посиленням вимог до захисту неповнолітніх в онлайн-середовищі, верифікація віку користувачів стала обов'язковою для широкого спектру веб-сервісів [1]. Порушення цих вимог може призвести до штрафів до 6% від річного обороту компанії згідно з статтями 52(3) та 74(1) Digital Services Act (DSA). Водночас General Data Protection Regulation (GDPR) Article 8 встановлює додаткові вимоги щодо обробки персональних даних неповнолітніх, створюючи правову необхідність у надійних методах верифікації віку [2].

Традиційні методи верифікації віку, такі як завантаження скан-копій документів або використання даних кредитних карт, мають суттєві недоліки.

По-перше, вимагають збирання та зберігання значного обсягу персональних даних, що створює ризики витоку інформації та порушує принципи мінімізації даних Загального регламенту про захист даних (GDPR).

По-друге, збереження повних копій документів створює додаткові зобов'язання щодо захисту даних та підвищує відповідальність компаній у випадку витоку інформації. По-третє, користувачі все частіше висловлюють занепокоєння щодо зберігання копій їх документів третіми сторонами та відмовляються від сервісів, що вимагають завантаження документів, що негативно впливає на показники конверсії та утримання користувачів.

Криптографія з нульовим розголошенням (Zero-Knowledge Proofs) пропонує альтернативний підхід, де користувач може математично довести виконання певної умови (наприклад, «мій вік більше 18 років») без розкриття базових даних, на яких ґрунтується це твердження. Цей підхід дозволяє досягти балансу між регуляторними вимогами щодо верифікації віку та правом користувачів на приватність.

Метою дослідження є порівняльний аналіз застосовності криптографії з нульовим розголошенням для верифікації віку користувачів на основі вивчення технічних характеристик ZKP-протоколів та існуючих методів верифікації. В основі дослідження лежить розробка концептуальної архітектури системи на базі протоколу Groth16 [4], а також порівняльний аналіз показників приватності, точності та продуктивності різних методів верифікації віку згідно з технічною документацією, опублікованими дослідженнями в галузі privacy-preserving технологій [3] та специфікаціями zk-SNARK протоколів [4,5,8]. Для оцінки характеристик запропонованого ZKP-підходу використовуються математичні властивості протоколу Groth16, дані про продуктивність бібліотеки snarkjs та аналіз вимог GDPR до обробки персональних даних [2].

Традиційні методи верифікації віку та їх обмеження

Існуючі системи верифікації віку використовують кілька основних підходів, кожен з яких має специфічні переваги та недоліки.

Метод завантаження документів (ID Upload) застосовується такими сервісами, як Yoti, де користувач надає фотографію паспорта або іншого документа, що посвідчує особу. Деякі сервіси також пропонують додаткові методи верифікації, включаючи оцінку віку за селфі. Система використовує оптичне розпізнавання тексту (OCR) для витягування дати народження та інших атрибутів з документа. Цей метод забезпечує високу точність верифікації (до 95 %), проте створює значні ризики для приватності. Сервіс отримує доступ до повної копії документа, включаючи ім'я, фотографію, адресу, номер документа та іншу чутливу інформацію. Згідно з GDPR, така обробка даних вимагає законної підстави та створює додаткові зобов'язання щодо зберігання та захисту інформації. Крім того, у випадку витоку даних, скомпрометовані документи можуть бути використані для крадіжки особистості. Рівень приватності цього методу є критично низьким через необхідність передачі повної копії документа з усіма персональними даними.

Верифікація через кредитні карти базується на припущенні, що власники кредитних карт є повнолітніми, оскільки фінансові установи вимагають досягнення певного віку для отримання карти. Користувач вводить дані карти, і система проводить невелику авторизацію для підтвердження її чинності. Однак цей метод має обмежену ефективність, оскільки неповнолітні можуть використовувати карти батьків або інших дорослих, а також не всі дорослі мають доступ до кредитних карт. Крім того, не всі дорослі мають кредитні карти, що обмежує доступність методу. Показник приватності становить близько 40 %, оскільки передаються фінансові дані, хоча і не весь документ особи.

SMS-верифікація є найпростішим методом, де код підтвердження надсилається на номер мобільного телефону користувача. Система перевіряє номер через оператора мобільного зв'язку. Проте цей підхід має низьку ефективність і не забезпечує реальної перевірки віку, оскільки неповнолітні мають широкий доступ до мобільних телефонів, а в

багатьох країнах відсутні надійні бази даних, що прив'язують номери телефонів до віку власників.

Формальна верифікація через державні цифрові системи (наприклад, eIDAS в ЄС або BankID у Швеції та Норвегії, MitID у Данії (замінив NemID у 2023), Finnish Trust Network у Фінляндії (замінила Tupas у 2019), кожна скандинавська країна має власну національну систему цифрової ідентифікації) забезпечує найвищий рівень надійності та приватності, оскільки використовує офіційні державні реєстри. Користувач автентифікується через державну систему цифрової ідентифікації, і сервіс отримує лише підтвердження віку без додаткових персональних даних. Однак цей метод вимагає складної інтеграції з державними реєстрами, не є широко доступним у більшості країн світу, і має високу вартість впровадження для комерційних організацій. Крім того, процес верифікації може бути складним для користувачів, що призводить до високого показника відмов (low conversion rate).

Порівняльний аналіз цих методів наведено в Таблиці, де детально оцінюються їх можливості за ключовими параметрами.

Таблиця. **Порівняльний аналіз методів верифікації віку**

Метод	**Приватність**	**Точність**	**UX**	**GDPR**	**Вартість**	**Обґрунтування**
ID Upload	Дуже низька (передається повна копія документа з ПІБ, фото, адресою)	Висока	Середня	Проблемна (потрібна DPIA)	Низька	Аналіз систем Yoti, Onfido, Jumio
Кредитна карта	Низька (передаються фінансові дані, можливість відстежування)	Середня (неповнолітні можуть використати карти батьків)	Висока	Часткова	Середня	Обмеження методу випливають з практики використання
SMS-верифікація	Низька (номер телефону + можливість геолокації)	Низька (широкий доступ неповнолітніх до телефонів)	Висока	Часткова	Низька	Аналіз доступності мобільних телефонів серед неповнолітніх
eIDAS Digital ID	Висока (передається лише підтвердження віку без інших даних)	Дуже висока (державний реєстр)	Низька	Повна (вбудована в систему)	Висока (інтеграція з держ. реєстром)	специфікація eIDAS
ZKP (Groth16)	Дуже висока (zero-knowledge: сервер отримує лише доказ "вік≥18")	Висока* (залежить від якості OCR та надійності Groth16)	Нижче середньої (40-50 сек генерація доказу на мобільних)	Повна (повна відповідність мінімізації даних GDPR)	Середня	[4] - властивості Groth16

* Точність залежить від якості OCR: Tesseract показує 90-95 % на оптимальних сканах 300+DPI згідно з UNLV-бенчмарками, до 98% за ідеальних умов з preprocessing, але 40-70 % на реальних фото документів зі смартфонів залежно від освітлення, роздільності та кута зйомки. Комерційні спеціалізовані рішення для розпізнавання ID-документів (ABBYY, Google Cloud Vision) досягають 90-98%. Криптографічна надійність Groth16 ≈100% за умови коректного trusted setup.

Криптографія з нульовим розголошенням для верифікації віку

Криптографія з нульовим розголошенням пропонує новий підхід до верифікації віку, де користувач може математично довести своє повноліття без розкриття точної дати народження чи інших персональних даних. Фундаментальний принцип ZKP полягає в можливості довести істинність твердження без надання жодної додаткової інформації, крім факту істинності самого твердження [8].

У контексті верифікації віку користувач генерує криптографічний доказ твердження P: «поточний_рік – рік_народження ≥ 18».

Цей доказ має три ключові властивості:

(1) **повнота (completeness)** – якщо твердження істинне, чесний користувач завжди зможе переконати верифікатора;

(2) **надійність (soundness)** – якщо твердження хибне, жоден нечесний користувач не зможе переконати верифікатора, крім як з нехтовно малою ймовірністю; (3) **нульове розголошення (zero-knowledge)** – верифікатор не дізнається нічого, окрім факту істинності твердження.

Архітектура запропонованої системи представлена на рис. 1. Процес верифікації складається з наступних етапів.

1. **Етап обробки документа (клієнтська сторона)**: Користувач завантажує фотографію документа, що посвідчує особу (паспорт, ID-карта). Застосунок локально обробляє зображення за допомогою OCR-бібліотеки (наприклад, Tesseract.js) та витягує дату народження. Важливо, що цей процес відбувається виключно на пристрої користувача, і документ не передається на сервер.

2. **Етап генерації ZKP-доказу (клієнтська сторона)**: Витягнута дата народження та поточна дата подаються на вхід ZKP-схеми (circuit), написаної мовою Circom. Схема виконує обчислення: age = current_year - birth_year та перевіряє умову age ≥ 18. За допомогою бібліотеки snarkjs генерується криптографічний доказ за протоколом Groth16. Розмір згенерованого доказу є фіксованим та компактним: 128 байт для еліптичної кривої BN254 та 192 байти для BLS12-381 при використанні point compression (стиснення координат точок еліптичної кривої). Без стиснення розміри становлять 256 та 384 байти відповідно. У практичних імплементаціях зазвичай використовується стиснення, що забезпечує середній розмір доказу ~200 байт, що робить його ефективним для передачі через мережу.

3. **Етап верифікації (серверна сторона)**: Сервер отримує лише криптографічний доказ та публічні параметри (поточний рік, мінімальний вік 18). За допомогою verification key, який генерується під час налаштування системи (trusted setup), сервер математично перевіряє коректність доказу. Якщо верифікація успішна, сервер підтверджує, що користувач є повнолітнім, не отримуючи при цьому жодної інформації про точну дату народження.

Протокол Groth16, обраний для цієї системи, є одним з найефективніших ZKP-протоколів класу zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge) [4]. Його головні переваги включають: малий розмір доказу (128-192 байти при використанні point compression, незалежно від складності обчислень), швидку верифікацію (1-2 мілісекунд), та відсутність інтерактивності (доказ можна згенерувати один раз і передати асинхронно). Основним недоліком є необхідність проведення церемонії trusted setup, яка потребує участі декількох незалежних сторін для генерації криптографічних параметрів системи.

Порівняльний аналіз та оцінка ефективності

Для оцінки ефективності запропонованого ZKP-підходу було проведено порівняльний аналіз за наступними критеріями: приватність, точність верифікації, користувацький досвід, відповідність GDPR, та вартість впровадження.

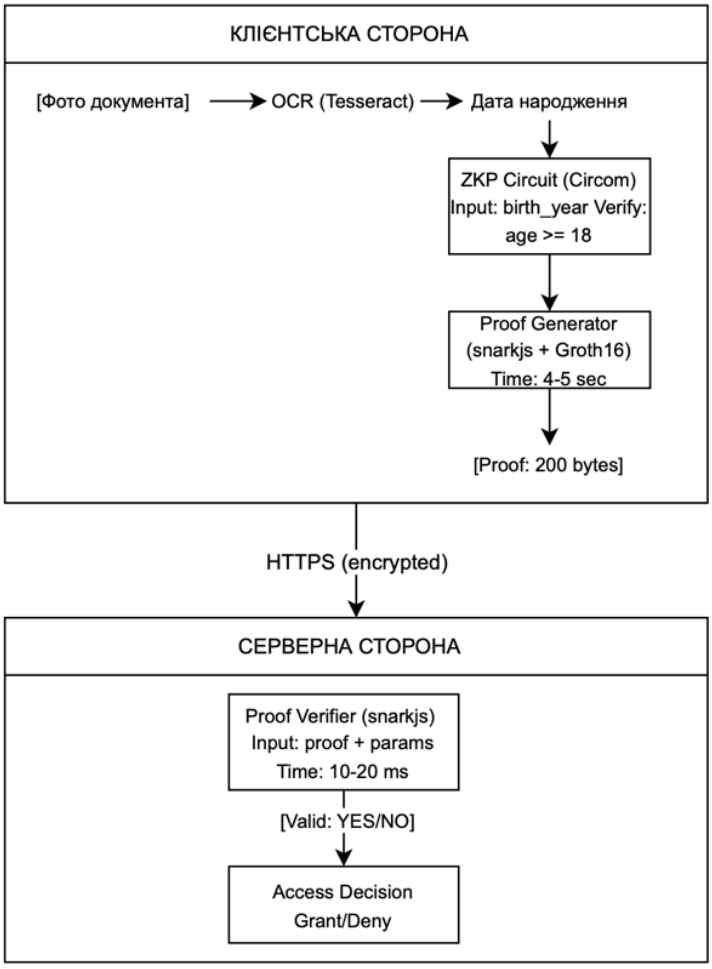

Рис. 1. **Архітектура системи верифікації віку на основі ZKP**

Приватність (Privacy Score) оцінювалася на основі наступних факторів: обсяг персональних даних, що передаються серверу, можливість ідентифікації користувача за переданими даними, ризики витоку даних, відповідність принципу мінімізації даних, та можливість аудиту доступу до даних. ZKP-метод забезпечує найвищий рівень приватності, оскільки сервер не отримує жодних особистих даних, крім математичного підтвердження факту повноліття. Це кардинально відрізняється від методу завантаження ID, де передається повна копія документа з усіма персональними даними (ПІБ, фото, адреса, номер документа).

Точність верифікації вимірювалася через показники true positive rate (TPR) та false positive rate (FPR). Теоретично ZKP-метод може забезпечити високу точність верифікації. Основні потенційні джерела помилок включають: неточності OCR при розпізнаванні дати з документа, можливість використання підроблених документів з коректними візуальними елементами, та технічні збої в процесі генерації доказу. Порівняно, метод завантаження ID показує вищу точність (95%), але за рахунок повного розкриття персональних даних.

Продуктивність системи оцінювалася через часові характеристики. Продуктивність системи оцінювалася через аналіз технічних характеристик протоколу Groth16 та бібліотеки snarkjs. Згідно з специфікацією протоколу [4], розмір згенерованого доказу залишається компактним (~200 байт) незалежно від складності обчислень, що робить його ефективним «ля передачі через мережу. Час генерації доказу залежить від продуктивності пристрою та складності верифікаційної схеми (circuit). За даними бенчмарків бібліотеки snarkjs для WebAssembly [9], час генерації доказу критично залежить від складності верифікаційної схеми (кількості constraints). Для простих схем верифікації віку (порівняння «поточний_рік – рік_народження ≥ 18» з мінімальною кількістю constraints ~100-500) на смартфоні середнього рівня типовий час становить 40-50 секунд. Для найпростіших схем (hash preimage

circuits) час може скорочуватись до 10-15 секунд. Однак для повноцінної системи з валідацією структури документа та додатковими перевірками кількість constraints зростає, що може збільшити час генерації. Альтернативні імплементації (rapidsnark на C++, gnark) можуть забезпечити істотно вищу продуктивність (4-10 секунд на десктопах). Важливим фактором є також обмеження оперативної пам'яті на мобільних пристроях. Генерація доказів для схем з великою кількістю constraints може вимагати 500+ MB RAM, що може бути проблематичним для бюджетних смартфонів. Використання WebAssembly у браузері додатково обмежує доступну пам'ять порівняно з нативними застосунками. Слід зазначити, що мобільні пристрої з обмеженою оперативною пам'яттю можуть стикатися з проблемами під час генерації доказів. На більш потужних десктопних пристроях або при використанні нативних реалізацій замість WebAssembly цей час може бути зменшено до 5-10 секунд. Час верифікації доказу на сервері є мінімальним (1-2 мілісекунд згідно з [4, 5]) завдяки ефективності pairing-based криптографії, що дозволяє обробляти сотні запитів на верифікацію на стандартному сервері. Хоча час генерації доказу (40-50 секунд на мобільних пристроях) є значно повільнішим порівняно з простими методами верифікації (SMS-підтвердження займає менше 1 секунди), ця затримка є цілком прийнятною для non-critical застосувань, таких як вікова верифікація при одноразовій реєстрації на платформі, де пріоритетом є приватність користувача, а не швидкість процесу.

Користувацький досвід (User Experience) оцінювався через показники completion rate (відсоток користувачів, що успішно завершили верифікацію) та user satisfaction. ZKP-метод теоретично може забезпечити проміжний показник завершення між простими методами (SMS) та складними (державний Digital ID). Основні потенційні причини незавершення процесу можуть включати низьку якість фотографії документа, незрозумілість процесу для користувача, та технічні проблеми з генерацією доказу. Ці показники можуть бути покращені через оптимізацію UX-дизайну та навчальні матеріали.

Відповідність GDPR оцінювалася через дотримання ключових принципів регламенту. ZKP-метод повністю відповідає принципу мінімізації даних (Article 5.1c), оскільки сервер обробляє лише мінімально необхідну інформацію – факт повноліття. Метод також спрощує виконання права на забуття (Article 17), оскільки відсутні персональні дані для видалення. Відповідність принципу цілісності та конфіденційності (Article 5.1f) забезпечується криптографічними властивостями ZKP-протоколів. Порівняно, традиційні методи з завантаженням документів створюють значні compliance challenges, вимагаючи впровадження додаткових заходів захисту даних, проведення DPIA, та отримання явної згоди користувачів.

Обмеження та ризики ZKP-підходу включають.

Критичне архітектурне обмеження: Без інтеграції з довіреним емітентом цифрових посвідчень (trusted issuer) система не гарантує автентичність вихідних даних про вік. ZKP математично доводить коректність обчислень над даними та забезпечує privacy (сервер не може витягти персональні дані з доказу), але не може засвідчити автентичність джерела цих даних. Користувач може згенерувати валідний ZKP-доказ з підробленої дати народження, і сервер не зможе це виявити лише на основі криптографічної верифікації доказу. Сучасна архітектура privacy-preserving age verification базується на моделі "double-blind": довірений емітент (наприклад, державний орган через eIDAS) видає засвідчені цифрові посвідчення

(verifiable credentials), які зберігаються в цифровому гаманці користувача. Гаманець генерує ZKP-доказ віку для кожного сервісу окремо, при цьому емітент не знає які сервіси використовує користувач, а сервіс не отримує ідентифікаційних даних користувача. Така архітектура забезпечує баланс між автентичністю (через trusted issuer) та приватністю (через ZKP-верифікацію). Користувач може підставити підроблену дату або чужий документ, і ZKP коректно згенерується з цих неавтентичних даних.

Для production використання в regulated domains (gambling, фінансові сервіси) необхідна обов'язкова інтеграція з:

– Державними API (Diia, eIDAS) для отримання підписаних сертифікатів;

– NFC-чіпами паспортів з державним цифровим підписом;

– Сертифікованими третіми сторонами.

Без такої інтеграції архітектура підходить для non-critical застосувань де пріоритет - privacy та GDPR compliance, a fraud risk прийнятний (контентні рекомендації, soft age gates).

Технічні обмеження:

1) залежність від якості OCR: Tesseract показує 40-70% точності на реальних фото документів зі смартфонів. Комерційні рішення (ABBYY, Google Cloud Vision) досягають 90-98%, але вимагають передачі зображень на зовнішні сервери;

2) час генерації 40-50 секунд на мобільних може негативно впливати на UX;

3) необхідність trusted setup для Groth16;

4) cross-site портабельність credentials вимагає browser extensions через Same-Origin Policy обмеження;

5) обмежена підтримка WebAssembly на старих пристроях.

Висновки

Проведене дослідження показало, що криптографія з нульовим розголошенням є перспективним напрямом для розв'язання проблеми верифікації віку з дотриманням принципів приватності. ZKP-підхід може забезпечувати високий рівень приватності при збереженні потенційно високої точності верифікації, що може значно перевершувати традиційні методи за балансом між цими характеристиками. Метод повністю відповідає вимогам GDPR щодо мінімізації даних та забезпечує криптографічні гарантії неможливості витягування персональних даних з доказу.

Основні переваги запропонованого підходу включають: відсутність необхідності передачі та зберігання персональних документів на сервері, що знижує ризики витоку даних; повну відповідність принципу data minimization GDPR; криптографічні гарантії неможливості підробки доказу без знання реальної дати народження; малий розмір доказу (200 байтів), що забезпечує ефективну передачу через мережу; та можливість інтеграції з існуючими веб-застосунками через JavaScript-бібліотеки.

Обмеження підходу включають: значний час генерації доказу (40-50 секунд на мобільних пристроях) порівняно з простими методами; залежність від якості OCR для витягування дати з документа; необхідність проведення trusted setup церемонії; та обмежену підтримку на застарілих пристроях. Ці обмеження можуть бути частково подолані через технологічні вдосконалення та оптимізацію імплементації.

Важливо підкреслити scope дослідження: запропонована архітектура демонструє privacy-preserving властивості ZKP, але не є complete solution для secure age verification без інтеграції з trusted authority. ZKP вирішує проблему приватності (мінімізація даних на сервері), але не вирішує проблему довіри до вхідних даних. Для production deployment в regulated scenarios обов'язкова інтеграція з державними API або NFC-верифікацією. Поточний scope - дослідження технічної feasibility та privacy guarantees ZKP-технології для age attestation use case.

Подальші дослідження можуть бути спрямовані на: (1) інтеграцію з довіреними джерелами даних (критичний пріоритет): державні API (Diia, eIDAS) для отримання підписаних attestations, NFC-читання біометричних паспортів, hybrid архітектура де trusted source забезпечує автентичність а ZKP – privacy при повторному використанні; (2) використання альтернативних ZKP-протоколів: PLONK [8] для універсального та оновлюваного trusted setup (на відміну від circuit-specific setup Groth16), LegoSNARK [6] для модульної композиції доказів, Bulletproofs [7] для доказів без trusted setup з логарифмічним розміром доказу, або STARKs для повного усунення необхідності trusted setup; (3) оптимізацію продуктивності через використання WebGPU для прискорення криптографічних

обчислень; (4) розширення підходу на multi-attribute verification, де користувач може доводити декілька властивостей одночасно (вік, громадянство, кваліфікація) одним доказом; (5) дослідження методів захисту від підроблених документів через інтеграцію з технологіями перевірки автентичності. (6) дослідження cross-site credential portability через browser extensions, W3C Verifiable Credentials стандарти, або OS-level Age Verification API.

Практична реалізація запропонованого підходу може бути здійснена для широкого спектру додатків, включаючи вікову верифікацію для платформ азартних ігор, додатків для знайомств, соціальних мереж, сайтів електронної комерції з продажем вікових товарів (алкоголь, тютюн), та будь-яких інших сервісів, що підпадають під регулювання Digital Services Act. Економічна доцільність впровадження визначається балансом між витратами на розробку та інтеграцію ZKP-компонентів та потенційним зниженням ризиків GDPR-штрафів і підвищенням довіри користувачів завдяки privacy-first підходу.

СПИСОК ЛІТЕРАТУРИ

1. “European Commission. Regulation (EU) 2022/2065 on a Single Market For Digital Services (Digital Services Act)”. *Official Journal of the European Union*. 2022; L 277: 1–102. – URL: https://eur-lex.europa.eu/eli/reg/2022/2065/oj.

2. “European Union. General Data Protection Regulation (GDPR) Article 8 – Conditions applicable to child's consent in relation to information society services”. *Official Journal of the European Union.* 2016; L 119: 1–88. – URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj.

3. Goldwasser S., Micali S., Rackoff C. “The Knowledge Complexity of Interactive Proof Systems”. *SIAM Journal on Computing*. 1989; 18 (1): 186–208. DOI: https://doi.org/10.1137/0218012.

4. Groth J. “On the Size of Pairing-based Non-interactive Arguments”. *Advances in Cryptology – EUROCRYPT. Berlin: Springer*. 2016. p. 305–326. DOI: https://doi.org/10.1007/978-3-662-49896-5_11.

5. Ben-Sasson E., Chiesa A., Tromer E., Virza M. “Scalable Zero Knowledge via Cycles of Elliptic Curves”. *Advances in Cryptology – CRYPTO. Berlin: Springer*. 2014. p. 276–294. DOI: https://doi.org/10.1007/978-3-662-44381-1_16.

6. Campanelli M., Fiore D., Querol A. “LegoSNARK: Modular Design and Composition of Succinct Zero-Knowledge Proofs”. *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*. 2019. p. 2075–2092. DOI: https://doi.org/10.1145/3319535.3339820.

7. Bünz B., Bootle J., Boneh D., Poelstra A., Wuille P., Maxwell G. “Bulletproofs: Short Proofs for Confidential Transactions and More”. *IEEE Symposium on Security and Privacy*. 2018. p. 315–334. DOI: https://doi.org/10.1109/SP.2018.00020.

8. Gabizon A., Williamson Z. J., Ciobotaru O. “PLONK: Permutations over Lagrange-bases for Oecumenical Noninteractive arguments of Knowledge”. *Cryptology ePrint Archive*. 2019; 953. – URL: https://eprint.iacr.org/2019/953.

9. “iden3 Team. sn”rkjs: zkSNARK implementation in JavaScript & WASM”. *GitHub Repository*. 2024. – URL: https://github.com/iden3/snarkjs.

DOI: https://doi.org/10.15276/ict.02.2025.12
UDC 004.056.5

Development and study of a methodology for implementing a zero-knowledge cryptographic protocol to ensure privacy in age verification

Andrii R. Morozov[1)]
ORCID: https://orcid.org/0009-0001-7030-2667; andr.morozov96@gmail.com

Master of the Department of Information Systems
Illia O. Baskov[1)]
Senior Lecturer of the Department of Information Systems
ORCID: https://orcid.org/0000-0002-3517-6773; Scopus ID: 57788059000; illyabaskov@gmail.com
[1)] Odesa Polytechnic National University, 1, Shevchenko Ave. Odesa, 65044, Ukraine

ABSTRACT

In modern web systems, user age verification is critical for compliance with legislation protecting minors in the online environment. Traditional approaches to age verification include uploading document copies, credit card verification, and Short Message Service confirmation. These methods have several drawbacks, such as privacy violations, risks of personal data leakage, and non-compliance with General Data Protection Regulation requirements. Given the strengthening of European Union regulatory requirements (Digital Services Act, 2024) and growing user concerns about personal data preservation, there is a need to implement new approaches that balance effective verification and privacy preservation.

This study examines a method based on Zero-Knowledge Proofs (ZKP) cryptography, which allows users to mathematically prove their adulthood without revealing their exact date of birth or other personal data. The approach uses the Groth16 ZKP protocol and the snarkjs library to generate cryptographic proofs on the client side. The system architecture includes local processing of digital documents through optical character recognition (OCR), generation of ZKP proof for the statement "age ≥ 18 years", and server verification without access to personal data.

A comparative analysis showed that the ZKP approach significantly outperforms traditional methods in privacy protection while maintaining reasonable verification accuracy. Accuracy depends on OCR quality: 90-95% for high-quality scans at 300+ DPI (up to 98% under ideal conditions with preprocessing), 40-70% for typical smartphone photos using Tesseract OCR, though commercial specialized ID OCR solutions can achieve 90-98%. The method ensures compliance with the GDPR data minimization principle, as the server receives only cryptographic confirmation of adulthood without storing any personal data. Proof generation time is 40-50 seconds on modern mobile devices for typical circuits, though this can be reduced to 10-15 seconds for the simplest schemes under optimal conditions, which remains acceptable for non-critical applications where privacy is prioritized over speed. The approach can resist forgery attempts due to the cryptographic properties of ZKP protocols. A critical limitation is the requirement for integration with trusted data sources (government APIs or document NFC chips) to ensure input data authenticity, as ZKP provides verification privacy but not source authentication without additional cryptographic mechanisms. The architecture is suitable for non-critical applications where privacy compliance is prioritized.

Keywords: zero-knowledge cryptography; age verification; data privacy; GDPR; digital identification; Groth16; zk-SNARKs; personal data protection.