

Рішення
разової спеціалізованої вченої ради
про присудження ступеня доктора філософії

Здобувач ступеня доктора філософії Андрій СЕВЕРІН, 1997 року народження, громадянин України, освіта вища: закінчив у 2020 році Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського» за спеціальністю Інженерія програмного забезпечення, є аспірантом кафедри програмного забезпечення комп'ютерних систем в Національному технічному університеті України «Київський політехнічний інститут імені Ігоря Сікорського» Міністерства освіти і науки України, м. Київ, виконав акредитовану освітньо-наукову програму Інженерія програмного забезпечення.

Разова спеціалізована вчена рада ДФ 26.002.140, утворена наказом Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського» від «12» квітня 2024 року № НСВС/37/24, у складі:

Голови разової

спеціалізованої вченої ради - Олександра КОВАЛЯ, доктора технічних наук, професора, завідувача кафедри інженерії програмного забезпечення в енергетиці Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського»;

Рецензентів -

Анатолія ДОРОШЕНКА, доктора фізико-математичних наук, професора, професора кафедри інформаційних систем та технологій Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського»;

Ярослава КЛЯТЧЕНКА, кандидата технічних наук, доцента, доцента кафедри системного програмування і спеціалізованих комп'ютерних систем Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського»;

Офіційних опонентів -

Сергія СУББОТІНА, доктора технічних наук, професора, завідувача кафедри програмних засобів Національного університету «Запорізька політехніка»;

Олега ЗОЛОТУХІНА, кандидата технічних наук, доцента, доцента кафедри штучного інтелекту Харківського національного університету радіоелектроніки,

на засіданні «24» червня 2024 року прийняла рішення про присудження ступеня доктора філософії з галузі знань 12 Інформаційні технології Андрію Северіну

на підставі публічного захисту дисертації «Алгоритмічне та програмне забезпечення захисту приватних наборів даних у задачах класифікації» за спеціальністю 121 Інженерія програмного забезпечення.

Дисертацію виконано у Національному технічному університеті України «Київський політехнічний інститут імені Ігоря Сікорського» Міністерства освіти і науки України, м. Київ.

Науковий керівник Микола ОНАЙ, кандидат технічних наук, доцент, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», доцент кафедри програмного забезпечення комп'ютерних систем.

Дисертацію подано у вигляді спеціально підготовленого рукопису українською мовою, який повністю відповідає вимогам до оформлення дисертації, затвердженим Наказом МОН України від 12.01.2017 р., № 40.

Наукова новизна полягає в наступному:

1. Уперше запропоновано архітектуру програмної системи для вирішення задачі класифікації на основі приватних даних, характерною особливістю якої є захист приватних наборів даних, шляхом функціонального шифрування, що відбувається на стороні клієнта, і дозволяє збільшити кількість наборів даних для навчання загальнодоступних систем аналізу даних і штучного інтелекту.
2. Уперше запропоновано модифікацію програмної моделі шифрування даних, яка відрізняється від існуючої використанням двовимірних згорткових нейронних мереж, замість одновимірних, і дозволяє застосовувати модель шифрування з використанням нейронних мереж до даних, що представлені набором пікселів, з яких складається зображення.
3. Уперше розроблено алгоритмічно-програмний метод функціонального шифрування наборів даних, особливістю якого є можливість використання приватних наборів даних в загальнодоступних системах аналізу даних та штучного інтелекту шляхом зменшення їх розмірності й функціонального шифрування отриманих даних з використанням приватного ключа.
4. Уперше розроблено алгоритмічно-програмний метод пошуку нормальних поліномів серед незвідних, який відрізняється від існуючого використанням простих чисел у десятковому представленні замість поліномів, що дозволяє зменшити обчислювальні витрати алгоритму пошуку незвідних многочленів з $O(n^3)$ до $O(n \log(\log n))$ і, як наслідок, спростити міжбазисні перетворення у бінарних скінченних полях з метою пришвидшення виконання операцій над елементами поля у методах гомоморфного шифрування даних.
5. Уперше розроблено модифікований спосіб побудови матриці переходу між поліноміальним та нормальним базисами скінченного поля, який полягає у використанні рекурентної формули $\alpha_{i+1} = t^{p^{i+1}} = t^{p^i \cdot p} = (\alpha_i)^p$ замість обчислення остачі від ділення елемента $t^{p^{i+1}}$ на незвідний

поліном, що дозволяє зменшити кількість використовуваної пам'яті з n^{p^i} до $n \cdot p$, а також обчислювальну складність з $O(m^{p^i})$ до $O(m^p)$.

Здобувач має 7 наукових публікацій за темою дисертації, з них 2 статті у наукових виданнях, включених на дату опублікування до переліку наукових фахових видань України; 2 статті у періодичних наукових виданнях, проіндексованих у базах даних Web of Science Core Collection та Scopus, з яких 1 статтю у виданні, віднесеному до третього квартилю (Q3) відповідно до класифікації SCImago Journal and Country Rank; 3 тези доповідей на наукових конференціях:

1. Modified Change-of-Basis Conversion Method in $GF(2^m)$ / I. A. Dychka, V. P. Legeza, M. V. Onai, A. I. Severin. // Radio Electronics, Computer Science, Control. — 2020. — №2. — С. 117–128.
2. Method of Performing Operations on the Elements of $GF(2^m)$ Using a Sparse Table / I. Dychka, M. Onai, A. Severin, C. Hu. // International Journal of Computer Network and Information Security (IJCNIS). — 2024. — Vol. 16, №1. — pp. 61-72.
3. A. Severin. Architecture of a software system for solving the classification problem based on private data. / M. Onai, A. Severin // Herald of Khmelnytskyi national university. Technical Sciences. — 2024. — №1. — pp. 244-247.

У дискусії взяли участь голова, рецензенти, офіційні опоненти, без зауважень.

Результати відкритого голосування:

«За» 5 членів ради,

«Проти» немає членів ради.

На підставі результатів відкритого голосування разова спеціалізована вчена рада присуджує Андрію Северіну ступінь доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 121 Інженерія програмного забезпечення.

Відеозапис трансляції захисту дисертації додається.

Голова разової спеціалізованої
вченої ради



Олександр КОВАЛЬ

Учений секретар
КПІ ім. Ігоря Сікорського



Валерія ХОЛЯВКО