ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

«Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ» КЕАҚ

Студенттер мен жас ғалымдардың
«ǴYLYM JÁNE BILIM - 2024»
XIX Халықаралық ғылыми конференциясының
БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ
XIX Международной научной конференции
студентов и молодых ученых
«ǴYLYM JÁNE BILIM - 2024»

PROCEEDINGS
of the XIX International Scientific Conference
for students and young scholars
«ǴYLYM JÁNE BILIM - 2024»

2024
Астана

УДК 001
ББК 72
G99

«ǴYLYM JÁNE BILIM – 2024» студенттер мен жас ғалымдардың XIX Халықаралық ғылыми конференциясы = XIX Международная научная конференция студентов и молодых ученых «ǴYLYM JÁNE BILIM – 2024» = The XIX International Scientific Conference for students and young scholars «ǴYLYM JÁNE BILIM – 2024». – Астана: – 7478 б. - қазақша, орысша, ағылшынша.

ISBN 978-601-7697-07-5

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.

В сборник вошли доклады студентов, магистрантов, докторантов имолодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 001
ББК 72
G99

ISBN 978-601-7697-07-5

2. Hassan, A., Shukur, Z., & Kamrul, M. (2020). An improved Time-Based One Time password authentication framework for electronic payments. International Journal of Advanced Computer Science and Applications, 11(11). https://doi.org/10.14569/ijacsa.2020.0111146

3. Mokalled, H., Catelli, R., Casola, V., Debertol, D., Meda, E., & Zunino, R. (2020). The guidelines to adopt an applicable SIEM solution. Journal of Information Security, 11(01), 46–70. https://doi.org/10.4236/jis.2020.111003

4. Arai, K. (2020). Adjacency effects of layered clouds by means of Monte Carlo ray tracing. International Journal of Advanced Computer Science and Applications, 11(1). https://doi.org/10.14569/ijacsa.2020.0110111

5. De Chérisey, É., Guilley, S., Rioul, O., & Jayasinghe, D. (2021). Information Theoretic Distinguishers for Timing Attacks with Partial Profiles: Solving the Empty Bin Issue. Journal of Information Security, 12(01), 1–33. https://doi.org/10.4236/jis.2021.121001

6. Dutson, J., Allen, D., Eggett, D. L., & Seamons, K. E. (2019). Don't Punish all of us: Measuring User Attitudes about Two-Factor Authentication. 2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), 119–128. https://doi.org/10.1109/eurospw.2019.00020

РАСШИФРОВКА ФАКТОРИЗАЦИИ - ВЫЗОВЫ КРИПТОГРАФИИ

Дурмагамбетов Асет[1], Дурмагамбетов Аслан[2]
[1]Преподаватель в ЕНУ имени Л.Н. Гумилёва
aset.durmagambetov@gmail.com
[2]Главный аналитик в Министерстве энергетики Республики Казахстан
tristesursi@gmail.com

Аннотация

В данной статье представлено описание нового метода решения проблемы факторизации, основанного на алгоритме градиентного спуска. Этот подход демонстрирует значительные улучшения в эффективности по сравнению с традиционными методами, предложенными в предыдущих исследованиях. В статье описывается новый метод решения проблемы факторизации на основе алгоритма градиентного спуска и демонстрируется переход от алгебраических методов к подходам, основанным на функциональном анализе. Предложенный подход не только повышает эффективность решения задачи, но также позволяет применять вычислительные алгоритмы функционального анализа, открывая новые возможности для исследований и оптимизации.

Ключевые слова: Дешифрование, проблема факторизации, алгоритм градиентного спуска, новый метод решения, переход от алгебраических методов к подходам, основанным на функциональном анализе.

Проблема факторизации, заключающаяся в поиске простых множителей составного числа, является одной из основополагающих задач в области криптографии и теории чисел. Эта проблема получила широкое распространение благодаря своему применению в алгоритме шифрования RSA, предложенном Rivest, Shamir и Adleman. Сложность задачи факторизации лежит в основе безопасности многих криптографических систем.

В последние годы было предложено несколько методов решения проблемы факторизации. К примеру, алгоритм квадратичного решета и метод поля чисел (1) демонстрируют высокую эффективность при работе с числами специфического размера. Однако, несмотря на их успех, они сталкиваются с серьезными вычислительными ограничениями при увеличении размера входных данных.

С развитием квантовых технологий возник новый интерес к алгоритмам факторизации, специально разработанным для квантовых компьютеров. Алгоритм Шора, предложенный в 1994 году, является одним из таких примеров, демонстрируя теоретическую возможность решения задачи факторизации за полиномиальное время на квантовом компьютере.

В данной работе мы предлагаем новаторский подход к проблеме факторизации, используя метод градиентного спуска, который, как мы надеемся, откроет новые горизонты в исследованиях данной области.

Результаты нашего исследования показывают, что применение градиентного спуска — метода, широко используемого в функциональном анализе, — к задаче факторизации не только возможно, но и приводит к значительному улучшению в эффективности по сравнению с традиционными алгебраическими подходами. Это открытие подтверждает значимость перехода к функциональным методам в изучении и решении проблемы факторизации Задача факторизации состоит в нахождении простых множителей заданного составного числа. Эта задача остается вычислительно сложной, особенно для больших чисел, что делает её одной из основных проблем в современной криптографии. Традиционно проблема факторизации чисел рассматривалась как чисто алгебраическая задача. В данной работе мы предлагаем новую формулировку для неё с помощью следующей функцииэ

$$f(x) = M/x - [M/x] \qquad (1)$$

где M составное письмо и тогда задача нахождения множителей прверащается в задачу поиска минимумов данной функции

Здесь мы рассмотрим метод градиентного спуска, который позволяет эффективно находить простые множители числа. Расмотрим функцию

$$f(x) = M/x - \left[\frac{M}{x}\right]$$

Теорема 1. Пусть M -целое составное число, тогда нули f(x) определяют сомножители числа M f(x)- бесконечно дифференцируемая функция на интервалах между локальными минимумами.

Доказательство следует из того, что при обнулении f(x) число

$$M/x = [M/x]$$

откуда следует

$$y = M/x$$

целое. А так как

$$y * x = M$$

то мы получаем целые сомножители числа M. Бесконечная дифференцируемость следует из бесконечной дифференцируемости функции $\{x\}$

Анализ данных и их визуализация

В этом разделе представлены основные численные методы, использованные для анализа задачи факторизации, а также визуализация полученных результатов. Важной частью исследования является применение метода градиентного спуска для нахождения локальных минимумов функции $f(x) = \frac{M}{x} - \lfloor\frac{M}{x}\rfloor$, что позволяет нам наглядно продемонстрировать эффективность предложенного подхода к факторизации.

Теорема 2. Если M — составное число, то для производной внутри интервалов гладкости справедливs

$$\frac{df(x)}{dx} = -\frac{M}{x^2} \qquad (2)$$

$$\frac{{x_0}^2}{M} < (x_1 - x_0) < \frac{{x_1}^2}{M} \qquad (3)$$

$$(x_1 - x_0) = \frac{{x_0}^2}{M} + O(\frac{{x_0}^3}{M}) \qquad (4)$$

Доказательство следует прямой проверкой внутри интервала гладкости. На графики видно, что расстояние между соседними нулями мало меняется при малых x, оценим более точно, вычислим разность значений функции в точке локального максимума x_0 и в точке локального минимумома е x_1 и воспользуемся Теоремой Лагранжва, что существеует точка $x_0 < \theta < x_1$ выполняется

$$1 - 0 = f(x_0) - f(x_1) = \frac{df(x)}{dx}|_\theta (x_1 - x_0) = -\frac{M}{\theta^2}(x_1 - x_0)$$

$$\frac{\theta^2}{M} = (x_1 - x_0)$$

$$\frac{{x_0}^2}{M} < (x_1 - x_0) < \frac{{x_1}^2}{M}$$

Второе уравнение следует при исследовании в разложении большего членов разложения

Теорема 3. Пусть $M = p * q$, p, q простые числа

$0 < \varepsilon < 1,\ \ i + k - p < \varepsilon * p/2,\quad i + m - p < \varepsilon * p/2\ \ ,\ \ x_i = \left\{\frac{M}{i}\right\}$

Тогда

простые числа (p,q) можно приближенно из определить последовательности x_i

Proof. Рассмотрим

$$x_i = \left\{\frac{M}{i}\right\}$$

Преобразуем

$$x_i = \left\{\frac{pq}{p + i - p}\right\} = \left\{\frac{pq}{p\left(1 + \frac{i-p}{p}\right)}\right\} =$$

$$x_i = \left\{\frac{pq}{p\left(1 + \frac{i-p}{p}\right)}\right\} = \left\{\frac{q}{\left(1 + \frac{i-p}{p}\right)}\right\} =$$

$$\left\{-\frac{q}{\left(1 + \frac{i-p}{p}\right)}\right\}$$

$$=$$

$$\left\{-\frac{q(i-p)}{p} + O\left(\frac{(i-p)^2}{p^2}\right)\right\}$$

Получим

$$x_{i+k} = \left\{1 - \frac{q(i+k-p)}{p} + \ O\left(\frac{(i+k-p)^2}{p^2}\right)\right\}$$

$$x_{i+m} = \left\{1 - \frac{q(i+m-p)}{p} + \ O\left(\frac{(i+m-p)^2}{p^2}\right)\right\}$$

Возьмем разность значений для k, m, получим

$$x_{i+k} - x_{i+m} = -\frac{q}{p}(k-m) + \ O\left(\frac{(i+m-p)^2}{p^2}\right) + O\left(\frac{(i+k-p)^2}{p^2}\right)$$

откуда имеем монотонно линейно убывающую последовательность. вычисляя угол наклона $\frac{q}{p}$ мы получим значение, в результате получили систему уравнений

$$pq = M,\quad \frac{p}{q} = C + O\left(\frac{(i+m-p)^2}{p^2}\right) + O\left(\frac{(i+k-p)^2}{p^2}\right)$$

откуда получим утверждение теоремы □

Ниже представлены графики 1,2 демонстрирующие анализируемую функцию и распределение расстояний между её локальными максимумами и минимумами.

Эти графики важны для визуализации поведения функции и подтверждения эффективности предложенного метода. Согласно Теореме 1 и Теореме 2 мы имеем возможность контролировать интервалы и строить быстрые алгоритмы вычисления локальных минимумов.

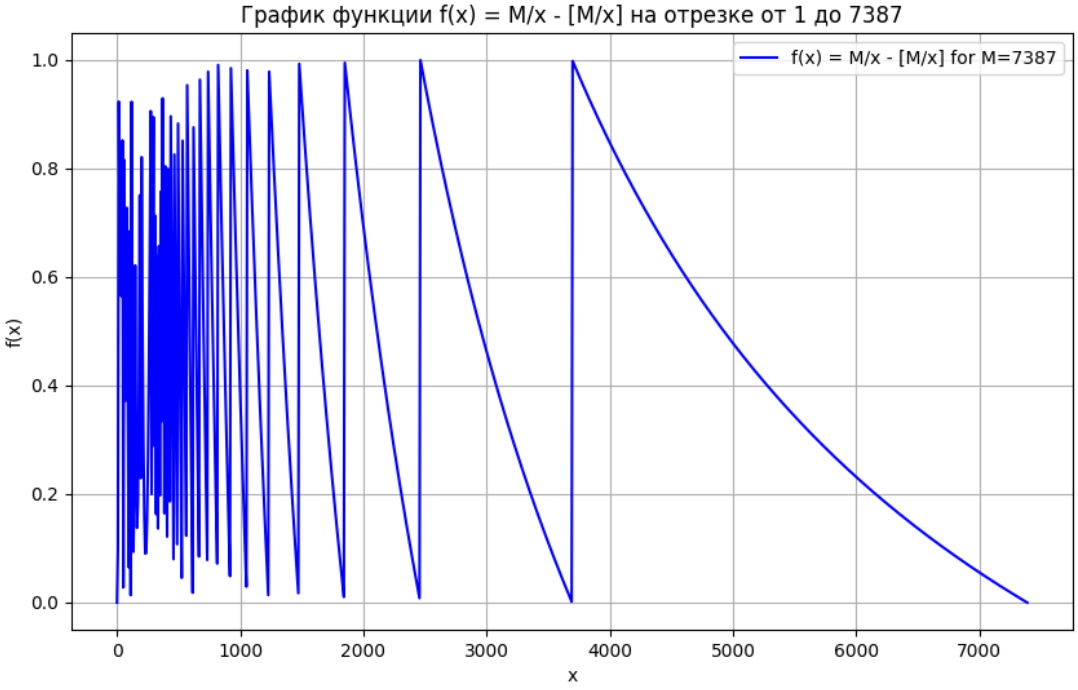

Рис.1: График функции $f(x)$ с выделением локальных максимумов и минимумов.

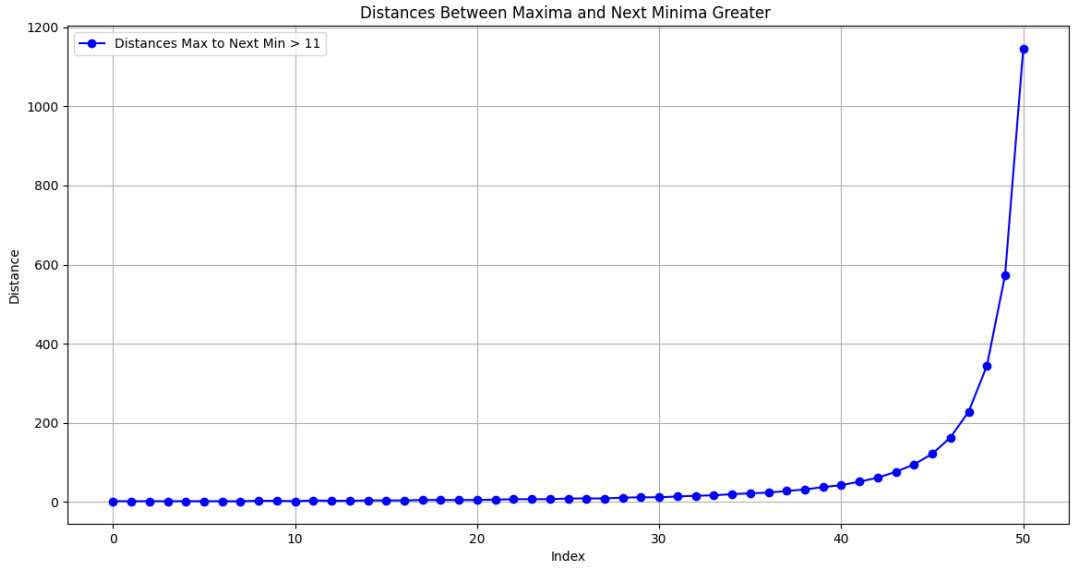

Рис. 2: Расстояния между максимумами и следующими за ними минимумами, больше заданного порога.

Заключение

В ходе данного исследования был произведён важный переход в осмыслении задачи факторизации: от традиционного алгебраического подхода к подходу, основанному на принципах дифференциального анализа. Этот сдвиг парадигмы позволил рассматривать задачу факторизации не просто как поиск численных решений, но как задачу оптимизации в многомерном функциональном пространстве. Такой подход открывает двери для использования мощных методов функционального анализа и сопутствующих вычислительных алгоритмов, что было успешно демонстрировано на примере применения метода градиентного спуска. В заключение, данный подход к факторизации через градиентный спуск и его осмысление в рамках дифференциального анализа открывают новые

горизонты для исследований и разработки в области математики, криптографии и вычислительной техники. Мы ожидаем, что наше исследование внесет значительный вклад в научное сообщество и стимулирует дальнейшие работы в этом направлении. Анализ данных и их визуализация являются ключевыми аспектами данного исследования, позволяя не только подтвердить теоретические предположения, но и наглядно продемонстрировать возможности предложенного метода.

Список использованных источников

1. Lenstra, A. K., Lenstra, H. W., Manasse, M. S., & Pollard, J. M. (1990). The number field sieve. Proceedings of the twenty-second annual ACM symposium on Theory of computing, 564-572.
2. Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. Proceedings 35th annual symposium on foundations of computer science, 124-134.
3. Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21(2), 120-126.

УДК 004.056.5

ФИШИНГТІК ВЕБ-САЙТТЫ АНЫҚТАУ ӘДІСТЕРІНЕ ЖҮЙЕЛІ ӘДЕБИЕТТІК ШОЛУ

Елеуов Батырхан Назымбекович
batyrkhan0808@gmail.com
Л.Н.Гумилев атындағы ЕҰУ «Ақпараттық технологиялар» факультетінің 1-курс магистранты, Астана, Қазақстан
Ғылыми жетекшісі – т. ғ. к., «Ақпараттық қауіпсіздік» кафедрасының доценті, К.М.Сагиндыков

Аннотация

Фишинг - бұл шабуылдаушы пайдаланушыдан құпия ақпарат алу үшін сенімді тұлға немесе ұйым ретінде өзін-өзі көрсететін алаяқтық әрекет. Бұл жүйелі әдебиеттерді зерттеу фишингті анықтаудың әртүрлі әдістерін, соның ішінде Тізімдерге Негізделген (Lists Based), Визуалды Ұқсастық (Visual Similarity), Эвристикалық, Машиналық Оқыту (Machine Learning) және Терең Оқыту (Deep Learning) әдістерін, олардың тиімділігін талдауды және салыстыруды зерттейді. Мақалада фишингтік веб-сайттар үшін көптеген алгоритмдері, деректер жиындары және анықтау әдістері мұқият зерттелді, сәйкесінше зерттеу сұрақтары жасалынды. Соңғы бес жыл ішінде ғылыми журналдарда, конференцияларда, семинарларда, зерттеушілердің тезистерінде, кітап тарауларында және беделді веб-сайттарда жарияланған 40 ғылыми мақалаларға жан-жақты шолу жасалды. Бұл зерттеу фишингті анықтау әдістемелерінің заманауи тенденцияларына баса назар аудара отырып, әдебиеттерге алдыңғы жүйелі шолуларға негізделген, оқырмандардың әртүрлі анықтау әдістері, деректер жиынын пайдалану және алгоритмдік өнімділікті салыстыру туралы түсінігін байытады. Айта кететін жайт, Машиналық Оқыту әдістері басым: зерттеу нәтижелеріне сәйкес, олар 28 зерттеуде қолданылған. Соның ішінде 15 зерттеуде Random Forest Classifier қолданылды. Айта кететін жайт, Convolutional Neural Network (CNN) фишингтік веб-сайттарды анықтауға арналған әртүрлі зерттеулерде ең жоғары дәлдікке қол жеткізді - 99,98%.

Кілт сөздер

Фишинг, Фишингті Анықтау, Киберқауіпсіздік, Машиналық Оқыту

1. Кіріспе

Фишинг, әлеуметтік инженерлік шабуыл, киберқылмыскерлер интернет пайдаланушысының жеке деректерін, соның ішінде банктік картасының деректерін, пайдаланушы аттары мен құпия сөздерді заңсыз алу үшін қолданатын негізгі әдіс ретінде кеңінен танылды. Кейде фишингтік шабуылдар зиянды бағдарламаларды желі ішінде тарату құралы ретінде қызмет етеді. Бұл шабуылдар әртүрлі формаларда көрінеді, соның ішінде