Literature Report

Zachary Zerafa

University of Technology Sydney, Sydney, Australia
zachary.c.zerafa@student.uts.edu.au

September 27, 2024

Table of Contents

Contents

List of Figures

1 Introduction

1.1 Context

Computer networking is the crux of the majority of relied upon technologies of the modern age, notably the internet. As of August 2023 (Cooke, 2014) (note that 2014 is the publication of the site article, that is continuously updated), ISPs in Australia was a 6.5 billion dollar industry, alluding to its high usage in modern society. Consequently, databases interacting on such networks become susceptible to attacks and confidential and proprietary information is put in potential jeopardy of being disclosed to undesired parties.

The 2014 Sony a data breach conducted by the North Korean intelligence group 'the Lazarus group' exposed roughly 30 million files worth of salacious content, private emails between executives and celebrities (Mills et al., 2018) to the public, resulting in an estimated loss of billions of dollars in revenue. However the most noteworthy example is the 2013 and 2014 Yahoo! data breaches occurring due to inadequate hashing procedures and susceptibility to phishing schemes orchestrated by the Russian FSB (Daswani et al., 2021). These resulted in the public disclosure of 500 million user's credentials and affected all 3 billion users of Yahoo!'s services.

In response, mathematicians and computer scientists alike have developed a corpus of literature discussing the optimization of mathematical methods in the context of such data breaches, with breakthrough results, notably in cryptography through number theory and group theory, as well as anomaly detection through probability theory and AI.

Despite considerable progress, there exist knowledge gaps in the current state of literature relating to unknown or unrefined solutions that have practical shortcomings. With the resurgence of AI and the repertoire of modern tools recently introduced, anomaly detection has the potential to be greatly improved, especially when contrasted to Bayesian-based techniques. On the converse, developments in computing are constantly placing cryptography in jeopardy of being computationally feasible to break (such as the MD5 hashing system); particularly in the light of quantum computing, demanding alternatives or refinements to uphold the breakthroughs of cryptography achieved by research.

Few articles provide relation of vulnerabilities with previous case studies of data breaches, which plays a crucial role in demonstrating the utility of mathematical research outcomes (which can appear abstract on first introduction) and their capability of being employed to protect the data relied upon by organizations and the general public.

1.2 Report objective, question and aim

The scope of this literature report concentrates on literature relating to fields of applied mathematics (specifically cryptography and anomaly detection) within the specific context of data breach prevention; hence articles relating to data breach history or have a mathematical nature with applications in cybersecurity will form the basis upon all points of discussion. Due to the specific nature of applied mathematics, the overwhelming majority of articles focus on a single field of applied mathematics such as cryptography or anomaly detection. The remaining articles represent data, studies, and surface-level cause explanations for actual data breaches that have occurred; the findings in these articles are enriched through a technical understanding of how these mathematical models are used or exploited, which are explained in the former category of articles. This unique scope of literature allows for key knowledge gaps to become prevalent, such as the lack of a directly reported relation between theoretical ideas and real data breaches in an article.

The aim of the research topic is to advance knowledge in fields of applied mathematics and convey such research findings to organisations for the prevention of their databases being breaches. Essentially, the aim can be decomposed into two distinct, yet related parts:

- Advancing research in applied mathematics
- Promoting use of this research in data breach prevention

Deriving from these aims, various research questions arise relating to the methodology and philosophies in which this is achieved, a notable example prompted by Bernstein et al. (2017), which will be discussed in greater depth, includes question such as whether to empower existing models or to develop new ones.

1.3 Report Structure

This report will synthesise an initial critical analysis concentrated on two outstanding articles related to the topic, drawing constant comparisons with a metric to evaluate the level of topic relevance, reliability, accuracy, potential for bias, timeliness and completeness exhibited by each article.

Additionally, a cohesive literature review will depict the broader state of the focus' corpus, discussing how recent research has contributed to the optimization of mathematical methods for data breach prevention, and highlighting critical knowledge gaps whose satisfaction will motivate the advancement of cybersecurity research.

A conclusion will summarise the key ideas representing the literary corpus and allude to the direction in which the progression of data breach prevention research may take considering the observations in literature.

2 Critical Evaluation of Two Sources

Justifying the validity of current literature since current literature is an imperative component for all literature reviews as subsequent literature is predominantly built upon previous research conducted. Developing malformed or obsolete concepts degrades the quality of literature and contradicts the research aims to provide accurate mathematical advancements towards modern age data breach prevention.

By challenging the background and content of employed sources, one can have assurance that the direction of research is of a sound basis and has high relevance in working towards satisfying research objectives.

This section will systematically review two sources and their context according to relevance, accuracy, bias potential, timeliness and completeness as a metric. Such details affecting these qualities includes the date, source citation count, diversity in referencing, and the quality and validity of the article's content when cross references. Finally a general evaluation will be formulated on the following questions:

- Is the article of sound basis for future research?
- How relevant and complete is this article within the scope of the research objectives?

2.1 Machine learning for email spam filtering: review, approaches and open research problems

The article (Dada et al., 2019) discusses the history of anomaly detection for spam filters and phishing prevention from Bayesian based techniques to a machine learning applications. An ideal machine learning based model is proposed and its efficacy is measured and compared to alternative solutions.

The structured search to find (see Figure 1 in appendix) this article was '"spam filter*" AND "Machine learning" AND "anomaly"', with heady use of the 'AND' boolean operator to find a specific article that dealt with the extremely specific topic. Spam filtering is often associated with emails, which is a large social component that contributes to data breaches.

2.1.1 Relevance

The article's topic on Machine Learning (ML) techniques for spam filtering in email systems has a concentrated relevance to the use of mathematical models for data breach prevention, focusing specifically on phishing instances in the context of email. Though narrow in scope, its relevance to data breach prevention cannot be understated; email phishing was one of the major proponents in

the 2014 Yahoo! breach (Daswani et al., 2021) where an enhanced anomaly detection model could have assisted in preventing such spam from reaching internal users. It discusses the use of Naive Bayesian filters and ML models such as Support Vector Machines (SVM) and Neural Networks, which may fulfil research aims by lowering the chance of a data breach occurring.

2.1.2 Reliability

The paper's appearance in the peer-reviewed, open-access journal Heliyon by Elsevier, adds to its credibility. In addition, the work is a collaborative approach from individuals representing multiple universities in Nigeria, suggesting that various professional perspectives and inputs refined the paper, and the very discussion on a broad range of various ML techniques exhibits comprehensive knowledge among the group.

References to universally known datasets like SpamAssassin and links to an extensive body of spam filtering experiments with various different models further augment to the paper's reliability, particularly since a brief evaluation of limitations and capabilities for each are listed in a table. The ability of the authors to evaluate other models and prudently select sources demonstrates their comprehensive knowledge of AI, not to mention their ability to explain a wide range of various machine learning techniques.

2.1.3 Accuracy

The paper's survey of ML techniques for spam filtering is largely in line with existing literature, offering a fairly accurate review of widely known algorithms like Naive Bayesian filtering, SVM, Neural Networks, and decision trees. The paper references spam trends and data primarily up to 2018, which might not reflect the latest developments in cybersecurity and AI. For instance, while it acknowledges the use of deep learning in spam filtering, it does not explore the more advanced techniques like hybrid models that combine ML with encryption for data breach prevention. Elmrabit et al. (2020) shows anomaly detection experiments with a slight super set of the models included in the article, demonstrating accuracy by showing that the article is in consensus with the main body of literature.

2.1.4 Bias potential

The article has minimal bias in its writing style and diverse referencing. Due to the article's high level of completeness, it discusses both the advantages and limitations of the majority of employed methods of spam filtering and offers an unbiased depiction of the state of anomaly detection for spam filtering. One instance in which the article manifests an equal consideration of models is when analysing the strong efficacy of Support Vector Machines (SVM) in classifying spam, while simultaneously recognising its computational limitations in handling large-scale data. The article references conventionally accepted sources and datasets, suggesting an objective approach to spam filtering.

Despite this, the affiliation of contributors with Nigerian institutions may limit the discussion to challenges or solutions more relevant to developing countries, possibly overlooking the quality discrepancy of accuracy that may be more obvious in more developed regions, which may confront different threats.

2.1.5 Timeliness and Completeness

The paper was published in 2019 and references literature mainly up to 2018. While it provides an extensive survey of ML algorithms up to that point, as mentioned before, is unable to discuss methods inaccessible at the time of publication. The swift progression of AI is therefore the pivotal detriment to the completeness of the paper.

The article lacks recent advancements such as advanced adversarial networks or privacy-preserving machine learning, reinforcement learning or advanced adversarial networks, or more specific and older technologies such as Residual Neural Networks (ResNN), which have clear applications in data breach prevention and are gradually becoming commonplace technologies. Disregarding the fast paced nature of AI however, the paper is quite complete in its coverage relative to its date of publication, with discussion of the aforementioned statistical and ML techniques.

2.1.6 General evaluation

Dada et al. (2019) encapsulates the history of spam filtering by anomaly detection with sufficient depth and completion as a base from which to inspire further research. It strongly represents the bridge from Bayesian to ML methods, offering the understanding required to relate knowledge of computer science to solve issues related to the efficacy and timeliness of such systems.

The article is closely aligned with the research aims due to its ML applications in spam filtering, which is a common medium through which employee error is abused for the motive of stealing data from a business or organisation (Daswani et al. 2021). It primarily serves as a compendium of essential knowledge of anomaly detection applied to spam filters from which researchers may use as a reference for when developing more advanced systems to resolve knowledge gaps.

2.2 Post-quantum RSA

The following article (Bernstein et al., 2017) delves into a solution to the potential dangers that post-quantum computing may pose towards the RSA cryptographic scheme by restricting the prime numbers used in key generation such that Shor's algorithm and other such quantum factorisation algorithms require infeasible time complexities to return a product of primes.

The structured search to find (see Figure 1 in appendix) this article was '"Post-quantum" AND "RSA"', since the preconception was that a strong general article would mention both key words since they are so intrinsically important to crypyography. In retrospect, a query using 'OR' may have been useful to discover more results, and words such as '"breach*"' could potentially return articles that even make direct reference to cryptography in the context of data breaches, which is quite a rare find in an article.

2.2.1 Relevance

The article holds high relevance in regards to the cryptographic side of data breach prevention by addressing solutions to issues that will arise from post-quantum cryptography. Such research is not transcends relevance by laying the foundations of how possible targets of data breaches will secure their data in a post-quantum world.

As Shor's algorithm is expected to threaten current cryptographic frameworks given sufficient quantum computing power becomes available (Shor, 1994), post-quantum-resistant RSA parameters could potentially extend the relevance of the heavily relied upon RSA cryptography framework, proving highly relevant for the advancement of data breach protection in parallel with an ever-evolving nature of cryptography.

There is a lack of mention of the explicit link between the article and data breach prevention due to the theoretical focus and nonexistance of quantum-based databreaches, however this article's relevance to the topic can be interpreted through anticipation for the future direction that data breach prevention will take. Therefore though postquantum cryptography is hardly a factor manifested in previous data breaches, it is surely a major component that will have to be considered in data breach prevention in the future.

2.2.2 Reliability

The paper's primary author is by Daniel J. Bernstein, a prominent figure in cryptography with a strong reputation. The article's publication in the Cryptology ePrint Archive and presentation at the PQCrypto event in 2017 validates its legitimacy of information.

Furthermore, the paper has undergone peer review and has been cited in 21 other articles as a source of trusted information on the nature of the post-quantum problem, such as Sun et al. (2021) who attempt to apply this result to the future of voting systems. The use of the result by other researchers certifies the article's reputability.

Bernstein's work has historically been well-regarded in the cryptographic community, lending credibility to this research. The article makes reference to and is heavily inspired by the renown result of Shor's algorithm for quantum computing, further adding to its reliability by association to such a prominent and fundamental motivator for the post-quantum problem.

2.2.3 Accuracy

An accuracy comparison to other such related literature (Khalid et al., 2019) distinguishes this article by its unique concept of prolonging the RSA framework to be resistant to quantum algorithms, as opposed to the common conception of distancing future algorithms from that of RSA due to its vulnerability to Shor's algorithm.

Since the article deals with the optimisation of RSA rather than alternatives, this calls into question the accuracy of the article as it is at odds with publications of Bernstein's peers. The article is aware of such a juxtaposition to the current state of literature, however validates its claims using sound mathematical arguments

While the majority of research suggests that fully abandoning RSA might be more secure, the compelling argument proposed by the article to enhance the RSA process is still within the scope of research and has high legitimacy as an accurate approach to post-quantum cryptography.

2.2.4 Bias potential

As manifested in most mathematical articles, the article's style is predominantly technical and neutral. However, bias in this work can be seen from its unusual philosophy of maintaining RSA through the quantum era.

Bernstein's research has a history of focusing on RSA, hence this article may portray an overly optimistic outlook on RSA's future, while it may be more beneficial to follow the researchers who are advocating for entirely new cryptographic systems to supersede this possibly vulnerable framework.

Bias is however mitigated by the diversity of referencing, drawing inspiration from articles of classical and quantum cryptography alike.

2.2.5 Timeliness and Completeness

The article's publication in 2017 finds itself in the context post-quantum cryptography gaining significant attention from researchers. Despite being a relatively recent article, it fails to recognise newer advancements in lattice-based and multivariate cryptosystems due not only to the fact that some such techniques were developed after 2017, but also due to the intense focus on RSA, affecting its completeness.

However, such topics including RSA as well as the research problem of mitigating the adversarial effects of quantum-computing on cryptography are currently relevant, and the article is quite complete in the scope of its extensive review of the RSA protocol and its related problem by discussing both theoretical and practical aspects, including implementation results, which add to its robustness.

It should be noted that such an article could be reviewed in light of recent advancements in quantum computing and how effective such extensions to RSA are in contrast to these, reevaluating the possibilities of practical implementation.

2.2.6 General evaluation

Overall, the article offers a valuable contribution to cryptographic research in the quantum era, worthy as a basis for further study, however researchers should be aware that although it proposes legitimate mathematics to upgrade the RSA algorithm, the uncertainty and lack of ability to experiment with quantum computing should encourage researchers to also consider articles that embrace the idea of creating new cryptosystems that differ from the integer factorisation problem, such as lattice or block cipher algorithms; this allows for an open minded approach to an ambiguous dilemma.

Bernstein et al. (2017) is well within the confines of the research objectives as it proposes a unique idea to be developed to revive current public key cryptography into the quantum era. Although the topic of post-quantum cryptography is seldom related to current industries attempting to protect data from being tampered to disclosed, it will eventually become a field that will become the fundamental basis for future cryptography and hence quantum algorithms that can

crack hashes containing sensitive information or intercept and break encrypted messages could cause countless data breaches and retro-cede from any progress towards the research goals.

3 Literature Review

To further understand the state of research, it is necessary to review a variety of related articles spanning the history of the related field to best understand the context of certain ideas. Following this, the direction of future research is calculated by identifying knowledge gaps in the current literature and consider the effect of their fulfilment on the research objectives.

Mathematical disciplines employed for data breach prevention are quite active due to the heavy reliance of secure data for businesses and universities, who fund industry and academic research respectively. The papers reviewed focus primarily on cryptography and anomaly detection, addressing prominent knowledge gaps of the past and providing a concoction of theoretical and experimental results that advance the quintessential technologies for data breach prevention.

Each sub-discipline will be dealt with separately, commencing with an overview describing the history and state of current literature, referencing the key insights and articles that form the basis of current literature. Subsequently, a critique of the state of literature will be conducted by cross-referencing sources as well as by proposing original insights.

3.1 Anomaly detection

3.1.1 Overview

Statistics dictate that 95% of all data breaches involve an element of human error (Daswani et al., 2021), and persistent threats engineer phishing methods to abuse human error in leaking sensitive data. Such instances have been recorded, for example during the Ubiquiti data breach being caused by a phishing email impersonating a cloud provider (Nadeem et al., 2023). As Artificial Intelligence (AI) experiences the plateau of productivity, AI has been a major tool in advanced automation, leading many researchers to question its role in automatic surveillance of computing systems. Such problems fall under anomaly detection; mathematical methods for detecting, flagging, and removing malicious network traffic.

Originally, statistical models were the basis for all research in anomaly detection, a major proponent of which being Bayesian models as demonstrated by Marchal et al. (2014), which made keen observations on how accuracy relates to the amount of keywords recognised by the filter. Eventually the field gained significant attention in the 2000s when the application of ML techniques was employed to monitor for unusual behavior in network traffic and user activity (Sommer & Paxson, 2010). In the past decade, such techniques have evolved immensely in terms of accuracy and efficiency, and hence could effectively classify and cluster the identification of unknown threats, eventually overtaking signature-based detection methods that could flag previously known attacks only (Chandola et al., 2009).

Deep learning techniques such as autoencoders, recurrent neural networks, and generative adversarial networks (GANs) have had wide success in identifying complex threats in a range of contexts (Buczak & Guven, 2016). The research in such innovations can refine systems to intervene between potential threats before any damage is inflicted on an organisation's data, aiding in achieving the research objective.

3.1.2 Research gaps

Anomaly detection is fundamentally based on data analysis, statistics, and decision making, making it susceptible to false positives and false negatives, or in statistics terminology, type I and II error respectively. Many detection systems (especially purely statistical ones) tend to classify legitimate activities as anomalies and worse, illegitimate activities as normal activity. Such an issue often arises in unsupervised learning models where the confidence intervals are not adequately parameterised. Papers such as Daswani et al. (2019) have expressed caution of model errors and it remains a major knowledge gap that remains on the frontier of research.

The frenetic pace at which new AI techniques are being created provides ample potential for research gaps to be filled with regards to creating stronger anomaly detection models. An

overview of Elmrabit et al. (2020) and Dada et al. (2019) suggest that there exists a delay between the discovery and implementation of results, since both articles have a similar age and absence of more advanced models and training techniques, such as ResNN and the notable use of adversarial attacks through GANs.

While anomaly detection models are designed to detect attacks, they themselves are vulnerable to adversarial attacks through GANs are a key instrument for training anomaly detection models with generated data, intentionally manipulating input data to deceive the model. Persistent threats may craft requests in such a manner to bypass standard anomaly detection systems, which stresses the importance of filling knowledge gaps related to adaptability.

The use of adversarial machine learning for anomaly detection is in its infancy, and according to previous experiments, significant challenge lies in enhancing robustness of models such that its training is resistant to outliers, while keeping performance consistent (Guo et al., 2021; Hu & Tan, 2017).

Furthermore, research in applying explainable AI (XAI) techniques for anomaly detection is another knowledge gap of literature that could boast improvements as insights into the model's reasoning would facilitate further research in the field. Anomaly detection is often an easy task computationally for a human (on a smaller scale), hence rather than treating anomaly detection systems as 'black-boxes', an effective collaboration between humans and machines in preventing data breaches can be conducted for more fruitful results (Zhang et al., 2022).

Anomaly detection requires a timely response to be effective in true data breach prevention; as well as the question of inaccuracy, delayed results can prove just as counterproductive since this offers persistent threats a time window to plan a data leak around (Toledano et al., 2017). Many models in often rely on batch processing or lack implementation to handle instantaneous data, where data is analyzed at constant intervals. This is incompatible with the research aim to provide practical models as real-time detection is essential to mitigate threats in the instant that they occur. Reviewing practical considerations, large organisations may require immense amount of processing power due to the scale of data, which summons the need for quick, concurrent algorithms that can handle continuous data streams dynamically without sacrificing accuracy in the process.

3.2 Cryptography

3.2.1 Overview

Cryptography has historically been an essential component in data security and by extension, data breach prevention, predating even the scene of computer based systems. Appropriate hashing algorithms protect sensitive credentials from being exposed in data leaks and secure encryption protocols prevents persistent threats from potentially eavesdropping on information facilitating unauthorised access of sensitive data. Strengthening knowledge and research of cryptography techniques gives organisations the capabilities to fulfil the research aim by adequately preparing data such that its utility to adversarial parties is abysmal, hence in the case of a partial system penetration there is no data that can be leaked.

Much literature in cryptography relates to discoveries and results that may be decades old, for instance, Shor (1997) published a landmark article that proposed the possible ramifications of quantum computing's potential to undermine the most commonly employed cryptographic techniques at the time, and was still referenced recently by Bernstein et al. (2017). Furthermore, the technologies commonly employed by organisations for the safeguarding of data are based on decade old ideas, such as the RSA cryptosystem discussed in Rivest et al. (1978) and the MD5 hashing algorithm proposed by Rivest (1992). The primary observation is that the timeless articles within the field are often the points of discussion for subsequent decades of articles, and are often continuously validated and compared to modern innovations, such as by Rachmawati et al. (2018) which conducts a research experiment of comparing MD5 to SHA-256.

Many articles furnish these pioneering concepts with modifications to further prolong the longevity of relevance and efficacy of these concepts. Notable examples include Bernstein et al. (2017) who propose optimisations for RSA prime selections for quantum algorithm resistance, and Pallier & Pointcheval (1999) who extends the number theoretic approach of RSA to propose

additive homomorphic encryption systems.

However, there are articles that demonstrate the weaknesses of the current state of cryptography, including Wang et al. (2005), further supplemented by Black et al. (2006), which demonstrate a vulnerability in the collision resistance of the MD5 hashing algorithm. Despite such an article being released in 2005, the Yahoo! breach of 2014 reportedly employed MD5 hashing for credentials 9 years after literature dismissed their practical usage (Daswani et al., 2021), suggesting that articles in cryptography may not relate its result's impact on data breach prevention strongly enough, or perhaps that security researchers may be ignorant to the state of cryptographic literature, even when there is high relevance.

3.2.2 Research gaps

Needless to say, research in cryptography is quite active and there are a variety of questions posed that have practical implications in addition to concepts that have been seldom developed and related to an actual application.

Perhaps the most significant knowledge gaps lie in quantum-resistant cryptography, due to its future potential to enforce major changes in the ways that researchers approach cryptography. The severity of the threat that Shor's algorithm poses to current cryptographic methods such as RSA and Elliptic Curve Cryptography (ECC) has been a frequent mention in this report, and the need for countermeasures has been linked towards the research aim. Currently, various solutions with conflicts in philosophy have been posed, and the metrics to determine the success of such solutions are supported only by theoretical claims. An obvious contributing factor to this incompleteness and confusion within literature stems from the fact that quantum computing is still a novel field of research and such computers that can feasibly execute Shor's algorithm are not yet available.

Experimenting with lattice-based, hash-based, and code-based cryptographic algorithms (Khalid et al., 2019) have been conducted in attempt to construct quantum-safe frameworks, however their high computational complexity when run on a quantum Turing machine distances them from being a practical solution.

Like with classical cryptography, the pioneering methods of post-quantum cryptography must be standardised if the base of literature is to be sound, since the implementation of inferior or unreliable systems induce financial and chronological cost for entities that aim to prevent data breaches.

Homomorphic encryption allows functions to be performed on encrypted data without the need to decrypt said data beforehand. This allows manipulation of data between trusted parties in such a way that provides less of an attack vector for persistent threats to capture and leak sensitive information. This solution can boost productivity alongside data security, however the computational complexity required for fully homomorphic encryption may render the practice infeasible to be applied in a true data breach prevention situation. Bezuglova and Kucherov (2023) discusses a range of encryption schemes that obey homomorphism on basic operations such as addition and multiplication and extends these to fully homomorphic encryption schemes, covering a wide range of the algorithms and their properties and even software implementations of these schemes, but also mentions caveats leading to higher time complexity such as the increasing dimension in the multiplication within thew CKKS scheme. Gong et al. (2024) discuss hardware optimisation and techniques to diminish time complexity such as the use of relinearisation to keep the dimension of CKKS homomorphic multiplication constant.

Similarly to the scavenge for quantum resistent cryptographic algorithms, the novelty of fully homomorphic encryption is the root of the gaps in knowledge. On the contrary, homomorphic encryption is much easier to conduct practical experiments with than quantum algorithms, therefore research may be advanced by integrating homomorphic encryption with existing infrastructures and services and conducting extensive analysis to best understand the contexts in which fully homomorphic encryption struggled to prove beneficial, and subsequently propose modifications to perpetually reduce the time complexity and provide a feasible solution for industries to transfer and process data in a secure manner.

4 Conclusion

The state of literature for applied mathematics for data breach prevention has had immense developments in the past half century, however clear knowledge gaps for both anomaly detection and cryptography alike. This report's analysis by evaluating the quality of articles by use of a metric and criticising them through comparison has brought to light a strong direction for future research; the significant role of machine learning for ameliorating anomaly detection models and the importance of evolving cryptographic techniques to secure data in a post-quantum world are two initial vectors that will bring research closer to the stated research aims. The resolution of such gaps are imperative measures that must be taken to ensure the protection of sensitive data in a data driven society. Addressing these gaps through innovative research will enhance data breach prevention, benefiting organizations and individuals alike.

5 Reference

References

Bernstein, D. J., Heninger, N., Lou, P., & Valenta, L. (2017). Post-quantum rsa. *Post-Quantum Cryptography*, *10346*, 311–329. https://doi.org/10.1007/978-3-319-59879-6_18

Bezuglova, E., & Kucherov, N. (2023). An overview of modern fully homomorphic encryption schemes. *Lecture Notes in Networks and Systems*, *702*, 300–311. https://doi.org/10.1007/978-3-031-34127-4_29

Black, J., Cochran, M., & Highland, T. (2006). A study of the md5 attacks: Insights and improvements. *Fast Software Encryption. FSE 2006. Lecture Notes in Computer Science*, *4047*, 262–277. https://doi.org/10.1007/11799313_17

Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications Surveys & Tutorials*, *18*, 1153–1176. https://doi.org/10.1109/comst.2015.2494502

Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. *ACM Computing Surveys*, *41*, 1–58. https://doi.org/10.1145/1541880.1541882

Cooke, J. (2014). Ibisworld - industry market research, reports, and statistics. *IBISWorld*. https://www.ibisworld.com/au/industry/cybersecurity-software-services/14771/

Dada, E. G., Bassi, J. S., Chiroma, H., Abdulhamid, S. M., Adetunmbi, A. O., & Ajibuwa, O. E. (2019). Machine learning for email spam filtering: Review, approaches and open research problems. *Heliyon*, *5*, e01802. https://doi.org/10.1016/j.heliyon.2019.e01802

Daswani, N., & Elbayadi, M. (2021). *Big breaches : Cybersecurity lessons for everyone*. Apress.

Deshpande, V. P., Erbacher, R. F., & Harris, C. (2007). An evaluation of naïve bayesian anti-spam filtering techniques. *2007 IEEE SMC Information Assurance and Security Workshop*, 333–340. https://doi.org/10.1109/IAW.2007.381951

Elmrabit, N., Zhou, F., Li, F., & Zhou, H. (2020). Evaluation of machine learning algorithms for anomaly detection. *IEEE Xplore*. https://doi.org/10.1109/CyberSecurity49315.2020.9138871

Gong, Y., Chang, X., Mišić, J., Mišić, V. B., Wang, J., & Zhu, H. (2024). Practical solutions in fully homomorphic encryption: A survey analyzing existing acceleration methods. *Cybersecurity*, *7*. https://doi.org/10.1186/s42400-023-00187-4

Guo, S., Zhao, J., Li, X., Duan, J., Mu, D., & Jing, X. (2021). A black-box attack method against machine-learning-based anomaly network flow detection models (Q. Yang, Ed.). *Security and Communication Networks*, *2021*, 1–13. https://doi.org/10.1155/2021/5578335

Hu, W., & Tan, Y. (2017). On the robustness of machine learning based malware detection algorithms. *Proceedings of the IEEE 2017 International Joint Conference on Neural Networks (IJCNN)*, 1435–1441. https://doi.org/10.1109/ijcnn.2017.7966021

Khalid, A., McCarthy, S., O'Neill, M., & Liu, W. (2019, June). Lattice-based cryptography for iot in a quantum world: Are we ready? *IEEE Xplore*. https://doi.org/10.1109/IWASI.2019.8791343

Marchal, S., Francois, J., State, R., & Engel, T. (2014). Phishscore: Hacking phishers' minds. *HAL (Le Centre pour la Communication Scientifique Directe)*. https://doi.org/10.1109/cnsm.2014.7014140

Nadeem, M., Zahra, S. W., Abbasi, M. N., & Arshad, A. (2023). Phishing attack, its detections and prevention techniques. *International Journal of Wireless Information Networks*, *12*, 18–25. https://doi.org/10.37591/IJWSN

Paillier, P., & Pointcheval, D. (1999). Efficient public-key cryptosystems provably secure against active adversaries, 165–179. https://doi.org/10.1007/978-3-540-48000-6_14

Rachmawati, D., Tarigan, J. T., & Ginting, A. B. C. (2018). A comparative study of message digest 5(md5) and sha256 algorithm. *Journal of Physics: Conference Series*, *978*, 012116. https://doi.org/10.1088/1742-6596/978/1/012116

Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, *21*, 120–126. https://doi.org/10.1145/359340.359342

Shor, P. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. *Proceedings 35th Annual Symposium on Foundations of Computer Science*. https://doi.org/10.1109/sfcs.1994.365700

Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. *2010 IEEE Symposium on Security and Privacy*. https://doi.org/10.1109/sp.2010.25

Toledano, M., Cohen, I., Ben-Simhon, Y., & Tadeski, I. (2018). Real-time anomaly detection system for time series at scale. *Knowledge Discovery and Data Mining*, 56–65.

Wang, X., Lai, X., Feng, D., Chen, H., & Yu, X. (2005). Cryptanalysis of the hash functions md4 and ripemd. *Lecture Notes in Computer Science*, *3494*, 1–18. https://doi.org/10.1007/11426639_1

Zhang, Z., Hamadi, H. A., Damiani, E., Yeun, C. Y., & Taher, F. (2022). Explainable artificial intelligence applications in cyber security: State-of-the-art in research. *IEEE Access*, *10*, 93104–93139. https://doi.org/10.1109/access.2022.3204051

6 Appendix

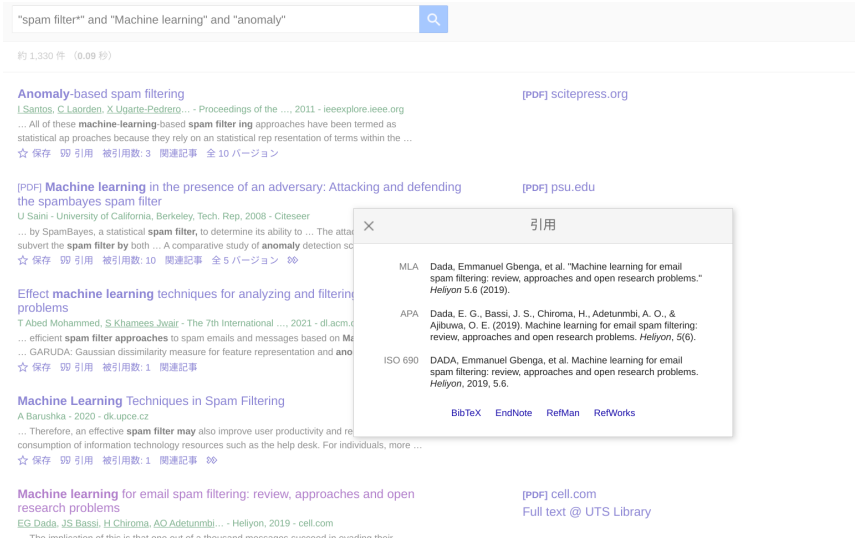

Figure 1: the search query ‘”spam filter*” AND ”Machine learning” AND ”anomaly”‘ lead to the discovery of Dada et al. (2019)

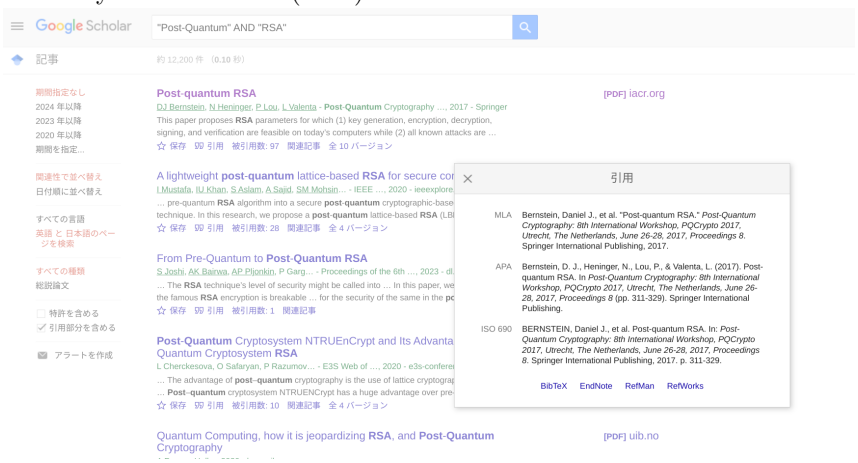

Figure 2: the search query ‘”Post-quantum” AND ”RSA”‘ lead to the discovery of Bernstein et al. (2017)

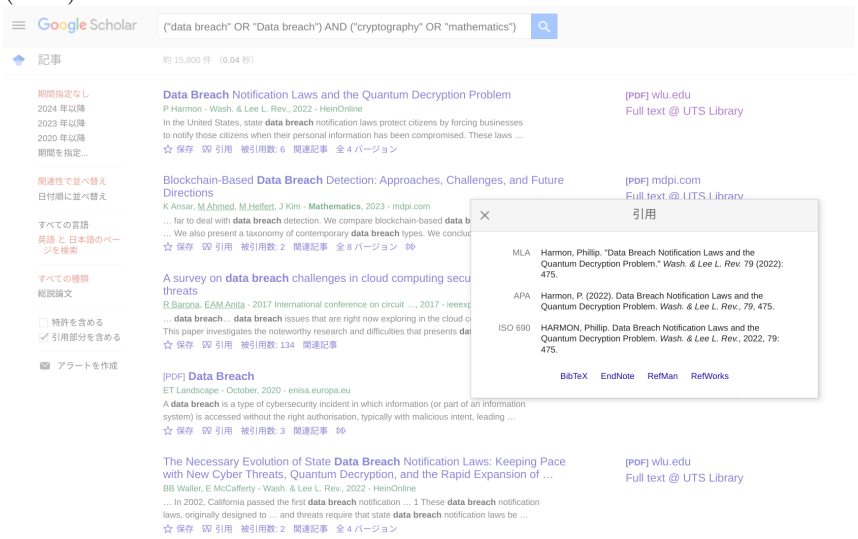

Figure 3: the search query ‘”Data breach” OR ”cryptography”‘ lead to the discovery of Mills et al. (2018).