Zero-Knowledge Proofs: Emerging Opportunities for the Insurance Industry

October | 2023

SOA Research INSTITUTE

Zero-Knowledge Proofs

Emerging Opportunities for the Insurance Industry

AUTHORS Stefano Chiaradonna (Ph.D. Candidate)

Petar Jevtić, Ph.D. (PI)

Dragan Boscovic, Ph.D. (Co-PI)

SPONSOR Actuarial Innovation and Technology Strategic Research Program Steering Committee

CONTENTS

Zero-Knowledge Proofs

Emerging Opportunities for the Insurance Industry

Executive Summary

Zero-Knowledge Proofs (ZKPs) represent an innovative suite of cryptographic algorithms that empower various parties, especially the insurance community, to validate the accuracy of sensitive information without revealing the actual information itself. When implemented, it could help the insurance industry authenticate policyholders and beneficiaries more efficiently, faster and, with fraud prevention mechanisms, it could facilitate communication with distribution channels, reinsurers or other stakeholders. Industry standards have not yet emerged and various technological solutions offer various tradeoffs. Thus, this report introduces the diverse applications and emerging opportunities that ZKPs offer to the insurance community, especially in the health insurance space.

Section 1: Introduction

Within the intricate landscape of insurance, health insurance providers operate amidst a complex web of regulations. A prominent example of these regulations is the Health Insurance Portability and Accountability Act (HIPAA) in the United States, which mandates stringent measures to protect individuals' health information. Failure to comply with these regulatory standards not only exposes insurers to substantial financial penalties, but also erodes trust among policyholders and can lead to further financial losses. For example, in 2018, health insurer, Anthem Inc., incurred a $16 million fine due to HIPAA violations related to privacy breaches to customer data.[1] These exacting regulatory standards are not confined to the U.S., as evidenced by a similar scenario in China in July 2023, where companies failing to adhere to consumer protection and corporate governance standards could face fines approaching $1 billion.[2]

Amidst this challenging regulatory environment, insurers must invest strategically to protect sensitive data and ensure compliance with evolving privacy regulations. Measures include robust data protection, advanced encryption technologies, and the implementation of stringent privacy policies. Compliance efforts should align with evolving privacy regulations, such as the General Data Protection Regulation (GDPR), regulations outlined by the China Banking and Insurance Regulatory Commission (CBIRC), and guidelines established by the National Association of Insurance Commissioners (NAIC). Achieving these goals often requires substantial resource allocation, including the creation of dedicated compliance teams and the adoption of novel software solutions. Furthermore, this alarming financial toll underscores the pressing need for the insurance industry to expedite its modernization efforts in compliance procedures, considering the persistent and substantial risk of insurance fraud.

In fact, every year, health insurance fraud inflicts a staggering toll of around $260 billion on insurers and policyholders worldwide.[3] This expansive aftermath encompasses a broad spectrum of deceptive practices, spanning from inflating claims and purposeful harm infliction to fabricating reports and making multiple submissions.[4] These fraudulent behaviors have a wide-reaching impact, affecting diverse sectors of insurance providers, ranging from property and casualty to workers' compensation and life and health insurance. For example, every year in the U.S., the financial loss attributed to life insurance fraud alone reaches $74.7 billion, followed by $68.7 billion in Medicare fraud, and trailed by $34 billion in workers' compensation fraud along with numerous other cases, culminating in a collective loss of nearly $308 billion.[5] Such substantial losses are seen elsewhere across the globe. For example, every year, India loses nearly $6 billion to health insurance fraud[6], and Canada over $500 million in personal injury fraud[7]. These alarming losses reveal the global scale of the insurance fraud problem, transcending borders and affecting economies worldwide. Such substantial financial losses underscore the urgency for comprehensive anti-fraud strategies and heightened vigilance within the insurance industry, necessitating a closer examination of existing regulations and their effectiveness.

Nonetheless, despite insurers' rigorous adherence to stringent regulations and anti-fraud strategies, they may face obstacles that still impede their competitive edge. A clear example is the issue of insurance-based discrimination, where individuals encounter unjust treatment from healthcare providers based on their insurance coverage or its absence. For instance, physicians may segregate patients according to their insurance status, resulting in unequal care for those with public insurance compared to others.[8] In such situations, a patient's perception that their insurance

[1] U.S. Department of Health and Human Services, 2018.
[2] Chang and Cooban, 2023.
[3] Lu, et al. 2023.
[4] Derrig, 2002.
[5] National Association of Insurance Commissioners, 2022.
[6] Khanna, 2023.
[7] Corporate Research and Investigations Group, 2021.
[8] Han, et al., 2015

status influences the quality of care they receive can undermine their trust in the insurer's ability to advocate for their well-being.

To address these compounding issues, emerging technological advancements, known as zero-knowledge proofs (ZKPs), provide some relief to the insurance industry. By highlighting the capabilities of this innovative technology, this report not only extends an opportunity to a diverse array of insurers, but also to businesses seeking to safeguard and verify sensitive data. The ultimate goal of this endeavor is to empower professionals within the insurance industry, allowing them to envision novel insurance applications and garner valuable insights into the realm of this groundbreaking technology. To this end, a comprehensive exploration of ZKPs is offered, serving as a foundation for a broader understanding and informed decision-making. While the implementation of ZKPs is out of the scope of this work, there are resources available[9,10,11]. Equipped with ZKP technology, insurers have a compelling opportunity to leapfrog their competitors by building, from scratch, an operating model that harnesses analytics and automation and runs on a flexible architecture, which allows insurers to integrate new business and regulatory requirements quickly.

[9] https://codethechange.stanford.edu/guides/guide_zk.html
[10] https://zksk.readthedocs.io/en/latest/usage.html
[11] https://github.com/matter-labs/awesome-zero-knowledge-proofs

Section 2: Understanding Zero-Knowledge Proofs (ZKPs)

2.1 BACKGROUND

At their core, *zero-knowledge proofs (*ZKPs*)* are cryptographic protocols that enable a provider to verify the validity of a statement to a verifier without disclosing any additional information beyond the statement's truthfulness (Midha, Gupta, and Mathur, 2021). In other words, zero-knowledge methods are probabilistic evaluations, which means they do not establish something as conclusively as just releasing all the information would. Instead, they give unlinkable data that might be used to demonstrate that the assertion's validity is likely. This concept of ZKPs originated in the 1980s with Shafi Goldwasser, Charles Rackoff, and Silvio Micali's introduction of "knowledge complexity" (Goldwasser, Micali, and Rackoff, 1989).

Fundamentally, ZKPs represent a technological advancement that bolsters privacy by reducing the need for extensive information exchange between users. Beyond this, ZKPs also offer scalability, expediting the verification process by excluding exhaustive information for non-private systems. The adaptability and confidentiality inherent in ZKPs position them as invaluable assets within contemporary cryptography, effectively addressing pressing security and privacy considerations across a spectrum of applications (Chen, et al. 2023). Underlining their significance, in 2021, a report from McKinsey & Company designated ZKPs as a pivotal technology poised to spearhead business transformations over the next decade (Fong, et al. 2021). Moreover, this innovation is expected to profoundly shape the competitive landscape of the financial sector, showcasing its potential to revolutionize industry dynamics.

At present, some notable corporations using ZKP technology include Alibaba Group, IBM, Toyota, Microsoft, and Accenture (Retail Banker International, 2022). As a recent testament, in 2022 alone, the Mina Foundation, a corporate leader in ZKP technology development, received over $92 million in investments from multi-billion-dollar asset management companies, such as Brevan Howard and Pantera Capital (Thurman, 2022). According to the foundation's latest survey in 2022 (Mina Foundation, 2022), interest and acceptance of ZKPs, especially within the finance industry, have become increasingly widespread, drawing the involvement of many other companies such as Bank of America, State Farm, Visa, and Mastercard. In fact, some corporations have already leveraged ZKP technology as part of their verification process. For example, in 2017, the financial services corporation, ING Group, incorporated ZKPs as a means for mortgage applicants to prove their salary without revealing the exact salary amount (ING Group, 2017). This provided enhanced efficiency and accurate data collection while maintaining the privacy of their applicants. Following suit, in 2019, JPMorgan Chase implemented ZKPs to improve the processing speed of syndicated loans while reducing administrative costs (Allison, 2021). Similarly, in 2022, Ernst & Young deployed ZKP technology to help corporations verify, track, and ultimately manage their supply chains (Haig, 2022). The same year, American Express Travel Related Services Company became invested in ZKP technology by provisioning a cutting-edge payment process to improve the efficiency of transactions between businesses and consumers (Ferenczi, 2022). Thus, in these instances, and increasingly many others, ZKPs provide enhanced verification and operational efficiency processes while also contributing to novel product development.

2.2 WHY USE ZKPS?

Every day, all types of insurers handle and process sensitive data, but also need to verify the data is accurate. For example, in life insurance claims processing, a beneficiary can prove their claim with an insurer and quickly collect their benefit without the need to order and share a death certificate, which includes sensitive information, with the insurer. In addition to streamlined claims processing, the insurer gains confidence that the ZKP claim is legitimate and needs to spend less time validating that the death certificate is real and not counterfeit. Similarly, in health insurance, the verification of medical conditions, such as diabetes, within an applicant's medical history for underwriting purposes ensures individual privacy protection by refraining from revealing explicit medical details. This upholds non-discriminatory underwriting practices that adhere to HIPAA compliance and underscores the insurer's commitment to fair policy assessment. Another advantage of ZKP technology arises in the verification of an applicant's participation

in a particular pension or employee healthcare plan, ensuring expedited group benefit communication without requiring the disclosure of personal identities. This versatility of ZKPs enables insurers to validate identities or documentation without the need to share sensitive credentials, bolstering security and privacy.

Beyond the insurance domain, ZKPs have found a diverse range of applications. For example, consider the case of international travelers carrying vaccination passports. These documents, whether in digital or paper form, serve as evidence of an individual's COVID-19 vaccination status, granting them access to various activities, travel opportunities, or venues with reduced health and safety restrictions (Vasconcelos Barros, Schardong, and Felipe Custódio, 2022). This concept can be further extended to verifying one's geographic location, such as confirming European Union (EU) citizenship, without the need to divulge specific nationalities. An interesting example of this is the World ID[12], a digital passport that allows users to establish their uniqueness and authenticity while maintaining anonymity. This innovation incorporates an ingenious fusion of ZKPs and machine learning, resulting in the emergence of a new extension of ZKP-technology known as Zero-Knowledge Machine Learning (ZKML).[13]

In the financial sector, ZKPs play a vital role in Know Your Customer (KYC) processes for companies, facilitating the verification and comprehension of their customers' identities (Pauwels, 2021). Furthermore, financial institutions can enhance their services by offering portfolio reporting to clients, enabling them to securely review their investment holdings and performance. Through the integration of ZKPs, clients can validate the accuracy of their portfolio information without exposing specific asset details or account balances. This preserves their financial privacy while ensuring the integrity of the reporting.

Furthermore, ZKPs find various scale applications in emerging domains leveraging blockchain technologies (Burger, et al. 2022; Xiao, et al. 2020; Wang, Zhao, and Wang, 2020; Wan, et al. 2019). Some examples include patient management systems in healthcare (Sharma, Halder, and Singh, 2020; Bai, et al. 2022), personalized car insurance (Huang, 2022), anti-fraud healthcare insurance (Liu, et al. 2019), insurance for car-sharing services (Huang, et al. 2020) and much more[14]. Collectively, the merits of ZKPs reside in their capacity to safeguard privacy, enhance security, and cultivate confidence across diverse fields. These attributes position them as essential cornerstones for the evolution of privacy and trust assurance (Chen, et al. 2023).

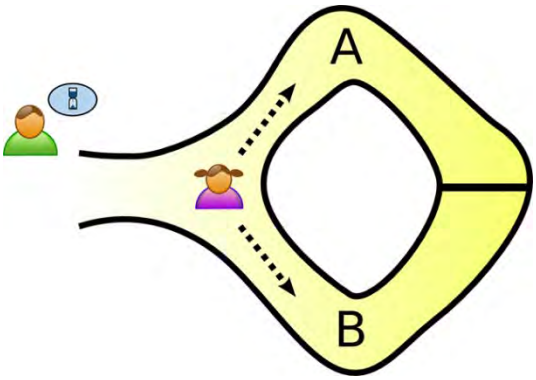
2.3 ILLUSTRATIVE EXAMPLE OF THE ZKP PROCESS

A ZKP typically follows a three-step process consisting of a witness, a challenge, and a response via a series of questions. In this cryptographic protocol, there are two key participants: the prover, responsible for demonstrating knowledge of a certain secret without revealing it, and the verifier, tasked with confirming the prover's claim without learning any sensitive information. One of the most common examples to describe the ZKP process is known as the *Ali Baba Cave* example (see Mohr, 2007), which provides a non-technical overview of the ZKP process. The ZKP process unfolds as follows:

Witness. In this scenario, Peggy takes on the role of the prover, while Victor assumes the position of the verifier. Within the narrative, a cave assumes the form of a ring, featuring an entrance on the left and a door obstructing the right side. Peggy's objective is to demonstrate her knowledge of the secret word required to unlock the door to Victor, all while safeguarding the secrecy of the word itself.

[12] https://docs.worldcoin.org/world-idl
[13] https://worldcoin.org/blog/engineering/intro-to-zkml
[14] https://blockchain.asu.edu/ More available information, by request, at dragan.boscovic@asu.edu

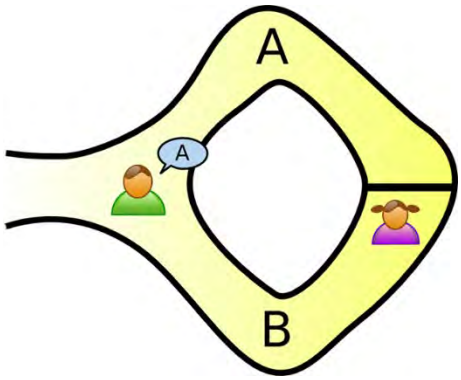
Figure 1
WITNESS PHASE: PEGGY RANDOMLY TAKES EITHER PATH A OR B, WHILE VICTOR WAITS OUTSIDE



Credit: https://en.wikipedia.org/wiki/Zero-knowledge_proof (CC BY 2.5; no changes made)

Challenge. To prove that Peggy knows the secret word, they designate the paths from the cave entrance as A and B. Victor remains outside the cave while Peggy ventures inside. Concealed from Victor's view, Peggy traverses either path A or B. Victor subsequently enters the cave and vocalizes the name of the chosen path—A or B—that he wants Peggy to retrace. Since Peggy possesses the actual knowledge of the secret, she can effortlessly unlock the door if necessary and retrace the designated path chosen by Victor, returning to the entrance.

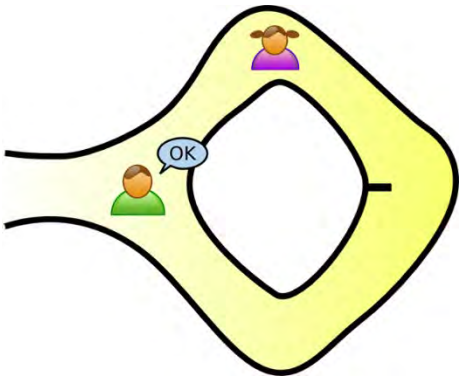
Figure 2
CHALLENGE PHASE: VICTOR CHOOSES AN EXIT PATH



Credit: https://en.wikipedia.org/wiki/Zero-knowledge_proof (CC BY 2.5; no changes made)

Response. Peggy returns using the path Victor shouted. In case Peggy does now know the secret word, she returns the same way she came in. This back-and-forth process is repeated numerous times to prove that Peggy knows the secret word.

Figure 3
RESPONSE PHASE: PEGGY RELIABLY APPEARS AT THE EXIT VICTOR NAMES



Credit: https://en.wikipedia.org/wiki/Zero-knowledge_proof (CC BY 2.5; no changes made)

The aforementioned process can be applied to the insurance domain. For example, a scenario where an insurance policyholder (Peggy) needs to prove to the insurer (Victor) that she has visited a primary care doctor last year, a prerequisite for coverage eligibility. Through this process, the policyholder can convincingly demonstrate that she indeed had a medical appointment without exposing the exact diagnosis or any other confidential health data. ZKP ensures that insurers can assess claims, while respecting the privacy rights of their policyholders, striking a delicate balance between privacy and necessary verification in the insurance sector. This is only one application of a ZKP, see Berentsen, Lenzi, and Nyffenegger (2023) for additional examples.

2.3 ZKP TECHNOLOGY

When compared to conventional password-based methods and public key infrastructure (PKI), ZKP offers two key advantages. The first benefit centers around its zero-knowledge capabilities, enabling anonymous communications and thwarting potential threats such as forgery and password-based breaches. The second advantage lies in its efficiency, resulting in decreased network congestion. Zero-knowledge authentication leads to reduced computational complexity and shorter proof lengths in contrast to alternative techniques such as the Merkle tree (Chen, et al. 2023).

To delve deeper into the realm of ZKPs, there are three fundamental properties that these proofs need to satisfy[15]:

1. **Completeness**: The ZKP should be valid and accurate, meaning that if the statement being proven is true, the verifier should be convinced of its truth after interacting with the prover. The proof must hold when both parties follow the protocol correctly and honestly.

If the completeness property is violated or incomplete, it means that a dishonest prover, such as an insured, can convince the verifier, the insurer, falsely. This could happen if the protocol lacks a proper verification step or if the prover does not provide sufficient information for verification. An example is non-interactive zero-knowledge proof with a missing verification step.

[15] See (Chen, et al. 2023; Sharma, Halder, and Singh, 2020; Gaba, et al. 2022; Sun, et al. 2021).

2. **Soundness**: The ZKP should provide a high level of confidence that the statement being proven is indeed true. If the statement is false, the probability of the prover being able to convince the verifier of its truth should be negligible. This property ensures that the proof cannot be used to deceive the verifier.

A protocol, such as an interactive zero-knowledge proof, may fail to meet soundness if the implementation of the cryptographic design is flawed, allowing dishonest provers to cheat and convince the verifier of fraudulent statements.

3. **Zero-knowledge Property**: The most critical aspect of ZKPs is that they should not reveal any information about the statement being proven beyond its truthfulness. Even after observing multiple interactions between the prover and verifier, the verifier should gain no knowledge of the underlying information or data related to the claim. In other words, the proof should be "zero-knowledge" in that it imparts no insight into the confidential or private aspects of the statement.

An interactive proof system without the zero-knowledge property may inadvertently leak information about the prover's secret or make it possible for the verifier to gain more knowledge than necessary to determine the statement's truth.

Section 3: Emerging Opportunities for Insurers

Within the insurance sector, the versatility of ZKP technology goes far beyond its primary function of deterring fraudulent endeavors. Its capabilities span a wide array of operations, encompassing tasks that range from optimizing operational effectiveness and ensuring meticulous data authentication, such as the verification of coverage, to facilitating the inception of novel and alluring insurance products. In this section, we delve into a collection of emerging prospects where insurers can harness the inherent potential of ZKPs to their advantage.

3.1 HANDLING SENSITIVE DATA IN CLAIMS PROCESSING

ZKPs offer a compelling solution to bolster the confidentiality and security of data, all while maintaining the ability to accurately verify assertions. This is especially pertinent within the realm of healthcare-related claims. The sensitive nature of medical records and treatment specifics demands rigorous privacy safeguards. With ZKPs, individuals can lodge medical claims without exposing their entire medical history. Notably, a significant portion of scholarly research concerning ZKPs revolves around their application to healthcare-related claims. The emphasis lies in ensuring the legitimacy and privacy of transactions between patients and insurance entities (Zheng, et al. 2022; Wan, et al. 2019). These studies seek to facilitate the secure sharing of medical data while preserving data integrity, offering a dependable means of data access that maintains confidentiality (Al-Aswad, et al. 2021; Chondrogiannis, et al. 2022).

Furthermore, ZKPs empower insurers to confirm the precision of claims, including details like treatment type or prescribed medication, without the need to delve into individuals' health data (Al-Aswad, et al. 2019). For instance, in life insurance, a beneficiary could prove the legitimacy of their claim by demonstrating the policy's active status and coverage amount without revealing intricate medical or personal information about the insured individual. This method adeptly maintains an equilibrium between streamlined claims processing and the preservation of medical confidentiality, thereby fostering a sense of trust between policyholders and insurers (Sharma, et al. 2020).

Expanding beyond healthcare, ZKPs hold promise for a wide range and various scales of property and casualty claims, as well. For instance, ZKPs could expedite the resolution of vehicle insurance claims (Chen, et al. 2019) by having drivers create cryptographic proof that validates their accounts of an accident without revealing sensitive details. Similarly, ZKPs can help verify the extent of damage to a property after an incident, such as a natural disaster or fire, without disclosing personal property details. For instance, after a hurricane, the property owner could use a ZKP to prove to their insurance company that a certain portion of the property has been damaged, and the insurance company could verify the claim without investing more resources in accessing information about the property's layout, valuables, or other private details. This efficiency may yield significant administrative cost savings.

3.2 REGULATORY COMPLIANCE

Increasingly, ZKPs have emerged as a powerful tool to enhance regulatory compliance, especially concerning data protection laws and data sharing agreements. ZKPs hold promise to support the highest confidentiality standards and regulations, such as the Health Insurance Portability and Accountability Act (HIPAA) in the U.S. (Wan, et al. 2019; Sharma, et al. 2020; Zhang, et al. 2021).

Similarly, within the European Union (E.U.), ZKPs hold a pivotal role in addressing the intricacies of regulatory compliance. In 2019, a European Parliament report underscored the potential of zk-SNARKs as a mechanism to align with the data protection provisions delineated in the General Data Protection Regulation (GDPR) (European Parliamentary Research Service, 2019). This acknowledgment highlights the utility of ZKPs in enabling data-sharing processes that adhere to stringent privacy guidelines, while fostering efficient collaboration among insurers, policyholders, and other stakeholders. As the E.U. continues to navigate the complexities of data protection, ZKPs offer a compelling solution that not only ensures compliance, but also instills confidence in the secure exchange of information within the insurance ecosystem. Therefore, ZKPs can improve compliance with data protection laws and

data-sharing agreements because they enable parties to interact and transact without sharing protected or confidential information.

3.3 UNDERWRITING AND RISK ASSESSMENT

Shifting the landscape of assessing potential policyholders, ZKPs present insurers with a robust instrument to enhance their underwriting and risk evaluation methodologies. A case in point is the computation of a credit score, which quantifies an individual's creditworthiness or credit risk. This pivotal metric is integral to the considerations of financial and banking institutions, as well as various entities, such as when procuring insurance policies or applying for rental properties. The outcomes of such deliberations, including the approval of policy purchases or the determination of premium rates, are significantly influenced by this metric (Lin, et al. 2021). Through ZKPs, insureds can provide verifiable and accurate information about their financial situations or other pertinent factors, without revealing sensitive personal details. Doing so may provide insurers with more accurate premium calculations that are both authenticated and protective of privacy (Wan, et al. 2022).

Via ZKPs, insurers can meticulously assess risk profiles and confirm coverage eligibility, all while rigorously safeguarding the utmost level of data privacy. For example, a healthcare insurance bill inspection service detects any forgery or tampering in reimbursement claims, effectively mitigating instances of health insurance fraud (Liu, et al. 2019). Moreover, there have been other recent developments in automating the underwriting process of parametric insurance policies, such as for fire insurance (Hao, et al. 2023). In doing so, ZKPs quickly provide risk assessment so insurers can quickly verify that the triggering conditions have been met, enabling prompt compensation to policyholders while potentially reducing the time insurers spend on each claim.

3.4 DATA SHARING AND IDENTITY VERIFICATION

From a broader perspective, insurance providers can establish the legitimacy of an individual's identity without necessitating the disclosure of sensitive personal information. Through the utilization of ZKPs, policyholders can substantiate their eligibility for coverage and benefit from various insurance services, all while maintaining a robust level of privacy and security. This technological innovation empowers insurers to verify critical details, such as age or medical history, without the need for direct transmission of raw data (Al-Aswad, et al. 2019). For instance, Bai, et al. (2022) devised an identity management system grounded in ZKP, allowing for identity verification that remains encrypted and only viewable during the authentication process. This not only ensures the privacy of patient data, but also enables patients to transparently and securely authenticate their identities across diverse healthcare domains, thereby promoting interaction between identity management providers and patients. This concept could also extend into other insurance subdomains, like long-term care insurance (Zhang, et al. 2021), bolstering privacy protection for data sharing (Al-Aswad, et al. 2021), and offering potential benefits in billing and health insurance communications.

In summary, ZKPs present the insurance industry with versatile and enduring solutions that span various scopes. ZKPs have the potential to significantly elevate data integrity, confidentiality, anonymity, and protection against substantial threats, including those cyber-related during data-sharing processes (Gaba, et al. 2022).

Section 4: Types of Zero-Knowledge Proofs

In this and the following sections, we dive into the more technical details of ZKPs. In particular, there are two primary variants of zero-knowledge proofs: interactive zero-knowledge proofs (iZKPs) and non-interactive zero-knowledge proofs (NIZKPs) (Bai, et al. 2022; Diro, et al. 2023).

Table 1
COMPARING IZKPS AND NIZKPS

Characteristic	Interactive Zero-Knowledge Proofs (IZKPs)	Non-Interactive Zero-Knowledge Proofs (NIZKPs)
Definition	Requires multiple rounds of interaction between the prover and verifier	Can be computed by the prover without verifier interaction. The prover generates a proof that can be verified in a single step.
Advantages	Direct verifier involvement enhances security	Reduced communication complexity
	Prover and verifier collaborate to establish the truth	Faster due to the elimination of interaction steps
	Potential for more adaptable protocols	Better scalability for large-scale systems
	Established security models for interactive proofs	Strong privacy preservation with minimal interaction
	Applicable in scenarios with feasible interaction	Suitable for scenarios with limited interaction
Computational Efficiency	Generally slower due to multiple rounds of interaction	Generally faster due to the elimination of iterative communication
Set-up Complexity	Relatively simpler set-up process	Set-up process can be complex
Privacy and Security	Direct interaction adds security but may be prone to attacks	Stronger privacy assurances from the elimination of iterative communication

4.1 INTERACTIVE

Interactive zero-knowledge proofs (iZKPs) are attainable by engaging in an interactive exchange protocol, encompassing a sequence of challenge-response interactions between the verifier and the prover (see section 2.3 for an illustration). Throughout each step of an iZKP, the prover showcases the correctness of the secrets to the verifier, while safeguarding the confidentiality of private keys (Fiat and Shamir, 1986; Diro, et al. 2023).

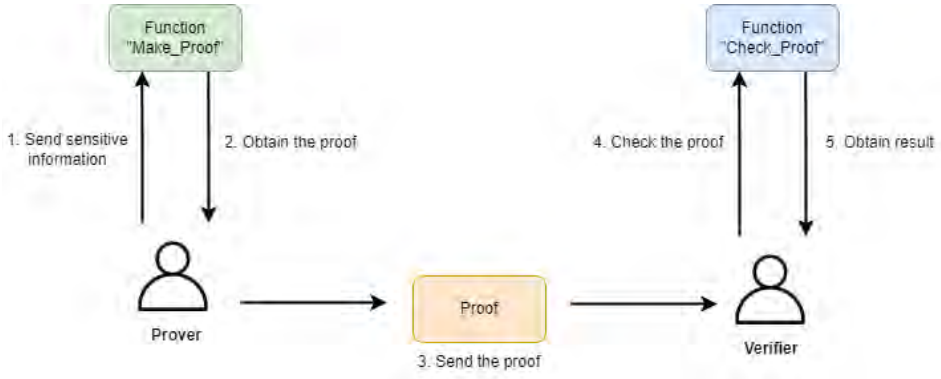
Moreover, iZKPs enable efficient fraud detection mechanisms. Insurance companies can request clients to provide evidence of specific conditions or damages without revealing all personal information. By employing zero-knowledge proofs, the policyholder can demonstrate the existence of relevant data or documents without disclosing unnecessary private data, thereby safeguarding sensitive details. This trust-building process ensures that insurance companies can process claims swiftly and accurately, while maintaining the utmost confidentiality and privacy for their clients, resulting in a more secure and reliable insurance environment. The main advantage of iZKPs is their simplicity and ease of implementation, especially when dealing with complex statements.

4.2 NON-INTERACTIVE

Non-interactive zero-knowledge proofs (NIZKPs) enable the prover to validate shared information with the verifier without the need for back-and-forth communication between the parties involved (Sasson, et al. 2014). In NIZKPs, the prover generates a proof comprising a collection of mathematical statements along with a corresponding set of proof objects. These proof objects enable the verifier to authenticate the proof without the need for any direct interaction with the prover (see figure 2). This characteristic renders NIZKPs suitable for use in asynchronous scenarios, enhancing their adaptability for situations where real-time interaction is unfeasible. For example, NIZKPs are showing promise in

the recent emergence of usage-based insurance for vehicles, where insurance costs are determined based on the actual usage and driving conduct of the insured vehicle (Qi, et al. 2020). Another emerging domain, particularly within healthcare, involves identity management systems designed to preserve the confidentiality of sensitive data, including medical records (Chin, et al. 2023), or provide insurance compensation for medical claims (Cao, et al. 2022).

Figure 4
PROCESS OF A NON-INTERACTIVE ZERO-KNOWLEDGE PROOF



Within the field of NIZKPs, there are two main types: Zero-Knowledge Succinct Non-Interactive Argument of Knowledge (ZK-SNARKs) and Zero-Knowledge Scalable Transparent Arguments of Knowledge (ZK-STARKs).

Zero-Knowledge Succinct Non-Interactive Argument of Knowledge (ZK-SNARKs) is a cryptographic protocol that allows one party to prove the validity of a statement without revealing any specific information about the statement itself (Ben-Sasson, et al. 2014). ZK-SNARKs generate concise proofs that can be swiftly verified, all without requiring iterative communication between the prover and verifier. The most notable feature of ZK-SNARKs is their succinctness, as the proof size remains constant regardless of the complexity of the statement being proven, making them highly efficient and ideal for resource-constrained environments. It was first applied in Zcash, a cryptocurrency centered on privacy, to allow users to verify transaction validity without compromising the confidentiality of the sender, recipient, or transaction value (Sasson, et al. 2014; Diro, et al. 2023). Moreover, ZK-SNARKs hold promise for other diverse applications such as robust voting systems (ElSheikh and Youssef, 2022), protocols for decentralized identity (Lee, et al. 2021), and much more. However, a significant disadvantage of ZK-SNARKs pertains to the necessity for a trusted set-up involving both the prover and verifier. This situation poses challenges in identifying any potential compromise of the trusted set-up and makes them less resistant to quantum computing attacks (Kassaras and Maglaras, 2020; Babel and Sedlmeir, 2023).

Zero-Knowledge Scalable Transparent Arguments of Knowledge (ZK-STARKs) are cryptographic protocols that allow for efficient and secure verification of large computations (Ben-Sasson, et al. 2018; Diro, et al. 2023). Much like ZK-SNARKs, these mechanisms allow one party to prove to another that a computation has been executed accurately, without revealing any extra information beyond the validation of the correct computation. However, unlike ZK-SNARKs, ZK-STARKs do not rely on a trusted set-up, making them more resilient to potential attacks arising from a malicious set-up (Diro, et al. 2023; Babel and Sedlmeir, 2023). They achieve transparency by generating proofs that can be easily verified with publicly available information, removing the need for a secret key or cryptographic parameters during verification. Additionally, ZK-STARKs are scalable and allow for proofs that are logarithmic in size, resulting in much smaller proof sizes compared to ZK-SNARKs, which maintain a constant proof size. This makes ZK-STARKs highly attractive for applications where efficiency and security are paramount (Diro, et al. 2023). Furthermore, ZK-STARKs are also resistant to quantum computing attacks due to their more complex mathematical properties (Harikrishnan and Lakshmy, 2019).

Table 2
COMPARING ZK-SNARKS AND ZK-STARKS

Characteristic	ZK-SNARKS	ZK-STARKS
Advantages	Well-established, widely used in blockchain applications	Emerging technology that offers higher scalability
	Efficient proofs suitable for insurance documents	Scalable for processing large amounts of insurance data
	Efficient verification for policy claims	No trusted set-up is required for transparent audits
Potential Applications	Privacy-preserving claims processing	Large-scale fraud detection and prevention
	Premium calculation while preserving privacy	Transparent verifiable underwriting
	Smart contract-based parametric insurance	Trustless telematics data verification
Set-up Complexity	Requires a trusted set-up	No trusted set-up required
Scalability	Limited scalability for large-scale data	Higher scalability
Privacy and Security	Vulnerable if trusted set-up is compromised	Strong security, resistant to quantum attacks

Overall, both interactive and non-interactive zero-knowledge proofs can be used to protect sensitive policyholder information, ensure the validity of claims, and maintain the confidentiality of insurance-related transactions. The choice between these two approaches depends on the specific use case, required security level, and performance constraints. iZKPs may be employed in situations where additional assurance or context-dependent proofs are needed. For example, an iZKP can be applied when a policyholder is required to demonstrate their adherence to particular safety protocols following an accident, furnishing context-dependent verification. In contrast, for scenarios where real-time processing and lower communication overhead are critical, NIZKPs might be favored. One such example is an insurer quickly verifying a policyholder's eligibility for a specific coverage. Regardless of the approach or insurance need, ZKPs offer a transformative solution that enhances the security and efficiency of the claims process, empowering insurers with effective fraud mitigation capabilities.

Section 5: Complementary Privacy Enhancing Technologies

5.1 CHALLENGES OF ZKP IMPLEMENTATION

Despite the significant advantages of preserving privacy and ensuring secure authentication, ZKPs face inherent challenges:

- Risk of improper implementation: ZKPs require high code quality, data integrity, and robust technology security. During implementation, potential risks, such as circuit design, data, code, or calculation errors must be addressed. To mitigate these risks effectively, it is crucial to conduct thorough testing, oversight, and verification, including rigorous mathematical verification (Marleau, et al. 2015). While third-party audits and open-source development can boost implementation confidence, security, intellectual property, and regulatory concerns may also arise.

- Quantum threats: Similar to other cryptographic methods, ZKPs are susceptible to quantum computing attacks. However, efforts are underway to enhance their resilience against quantum threats, reflecting their critical role in various industries, including insurance (Niraula, et al. 2022; Baum, et al. 2018; Chiesa, Ojha, and Spooner, 2020; Wen, et al. 2022; Chi, Lu, and Guan, 2023).

- Lack of standardization: The absence of a universally applicable approach for ZKPs due to different models' unique advantages introduces complexity and a lack of uniformity, requiring careful consideration for specific use cases (Sun, et al. 2021).

- Computational complexity: ZKPs involve complex mathematical and cryptographic techniques, which can lead to significant computational demands, such as ZK-SNARKs in Zerocash, relying on trusted third parties for system initialization. Although removing this trusted third party can enhance ZKP security, it may impact efficiency (Sun, et al. 2021), underscoring the need for a careful equilibrium between strong security and practical execution within feasible timeframes.

- Trusted set-up: Certain ZKP methodologies require a trusted set-up phase, emphasizing the importance of accurate and secure execution by trusted entities to prevent potential security vulnerabilities (Sun, et al. 2021).

Hence, it is important to recognize that ZKPs alone do not provide an end-all solution for privacy assurance and complete cryptographic security. Instead, the true power of ZKPs lies in their ability to seamlessly integrate with a myriad of privacy-enhancing technologies, creating an enticing avenue to fortify data security and maintain the utmost confidentiality, particularly within the intricacies of the insurance domain.

In the remainder of this section, we provide examples of complementary cryptographic algorithms synergizing with the ZKP technology.

Table 3
VARIOUS PRIVACY ENHANCING TECHNOLOGIES

Technology	Pros	Cons
Homomorphic Encryption	Enables computation on encrypted data	High computational overhead
Differential Privacy	Strong privacy guarantees	Trade-off between privacy and utility
Secure Multi-Party Computation	Supports collaborative computations	Complex set-up and high computational costs
Proxy Re-Encryption	Facilitates controlled data sharing	Limited use cases and key complexity

5.2 HOMOMORPHIC ENCRYPTION

Homomorphic encryption is a cryptographic technique that allows computations to be performed directly on encrypted data, without the need for decryption (Rivest, Adleman, and Dertouzos, 1978; Xiao, et al. 2020). In traditional encryption schemes, data must be decrypted before any operations can be executed, potentially exposing it to security risks. However, in homomorphic encryption, the encrypted data retains its confidentiality while supporting mathematical operations, such as addition, multiplication, and more, on the encrypted values (Munjal and Bhatia, 2022). This property enables secure data processing in scenarios where privacy is of the utmost importance, such as cloud computing, privacy-preserving data analysis, and confidential machine learning (Fontaine and Galand, 2007).

Homomorphic encryption comes in various forms, including partially homomorphic, somewhat homomorphic, and fully homomorphic encryption, each offering different levels of computational capability while maintaining the confidentiality of the underlying data (Munjal and Bhatia, 2022). However, it has limitations in fully safeguarding the identities of policyholders (Sun, et al. 2021). In particular, preserving full anonymity, while performing complex computations involving policyholder data, remains challenging. The potential for unintended data leakage through side-channel attacks, frequency analysis, and the intricacies of securely processing encrypted data pose obstacles to ensuring complete identity safeguarding in practical applications.

5.3 DIFFERENTIAL PRIVACY

Differential privacy is a fundamental concept in data privacy and protection that aims to strike a balance between sharing useful information and preserving individual privacy (Dwork, et al. 2006). It involves adding carefully calibrated noise to the results of data queries or analyses to prevent the identification of specific individuals within the dataset. By doing so, differential privacy ensures that even with access to the aggregated data, an adversary cannot infer sensitive details about any single data point (Zhao and Chen, 2022). In essence, differential privacy addresses the challenge of sharing sensitive information, while protecting individual identities within datasets. This approach enables organizations to release aggregated statistics or conduct analyses on sensitive datasets, while safeguarding individual privacy rights, making it a crucial tool in the age of big data and increasing concerns about personal data exposure. However, the drawback of differential privacy is that it can introduce significant noise or uncertainty into data, potentially limiting its utility for certain applications or analyses.

5.4 SECURE MULTI-PARTY COMPUTATION

Secure Multi-Party Computation (SMPC) is a cryptographic technique that distributes a computation task across multiple participants, where no individual participant can know the other participants' data (Yao, 1982; Sun, et al. 2021). In other words, the goal of SMPC is to enable collaborative computation in a data-sharing environment, while maintaining the privacy and confidentiality of the underlying data, such as a policyholder's social security number, birthday, medical history, etc. For example, SMPC enables insurance companies to jointly compute risk assessments, analyze data, and detect fraud without disclosing policyholders' private information (Veeningen, 2018; Agahari, Ofe, and de Reuver, 2022). While it safeguards data with encryption and anonymity during computations to protect privacy and yield valuable insights, the drawback of SMPC is its requirement for significant computational resources, complexity, and expertise for successful implementation.

5.5 PROXY RE-ENCRYPTION

Proxy re-encryption (PRE) represents an advanced cryptographic breakthrough that relies on a trusted intermediary known as a "proxy" to systematically modify data encryption from one cryptographic key to another (Blaze, Bleumer, and Strauss, 1998; Qin, et al. 2016). This intricate process not only enables secure data sharing and controlled access among diverse users, but also preserves the confidentiality of the original decryption key. Its significance is particularly pronounced for enterprises, notably insurers, engaged in cloud computing, where collaborative claims processing

involves insurance firms, clients, and service providers (Do, Song, and Park, 2011; Qin, et al. 2016). This is especially valuable for safeguarding sensitive healthcare record exchanges (Bhatia, Verma, and Sharma, 2018; Guo, et al. 2022).

However, while PRE offers a sophisticated cryptographic solution for secure data transformation, its adoption is accompanied by notable limitations. The complexity of its operations introduces potential computational overhead, which could impact performance (Qin, et al. 2016). Effective key management becomes pivotal, and concerns about trust in the proxy entity raise security considerations since a compromise could cause data confidentiality risks. This is particularly concerning since PRE cannot guarantee security from quantum attacks (Kim and Jeong, 2016). While PRE is suitable for specific scenarios, its integration may require significant system adjustments, potentially impeding compatibility (Qin, et al. 2016). Regular updates are crucial to address cryptographic vulnerabilities and scalability challenges could emerge when accommodating numerous users. The absence of standardized practices may hinder widespread implementation. In essence, while PRE offers distinct advantages, its intricate aspects and potential drawbacks demand careful consideration before implementation.

5.6 INTERACTING WITH ZKP

The assortment of privacy-enhancing technologies provides individual layers of protection, yet each comes with its drawbacks. Nonetheless, the synergistic combination of these technologies, particularly when integrated with ZKPs, presents an opportunity to mitigate individual drawbacks and maximize their collective effectiveness. For example, homomorphic encryption alone may carry the risk of unintended data leakage. However, when integrated with ZKP technology, it fortifies security and confidentiality by ensuring the data remains confidential, while adding an extra layer of privacy. This synergy proves particularly useful in applications such as medical insurance purchasing and medical insurance claiming by ensuring the legitimacy and privacy of patients' identities (Zheng, You, and Hu, 2022). Similarly, ZKPs can expand the utility of PRE to various other applications, enhancing security, privacy, and trust in data-sharing scenarios by enabling verification of PRE operations without relying on proxy trust. Among these opportunities, the healthcare sector stands as a crucial arena, offering a pivotal chance to employ ZKPs for authenticating patient identities and facilitating controlled access to healthcare service providers using PRE (Sharma, Halder, and Singh, 2020). This may further help verify billing services from medical providers, reducing the potential for fraudulent claims.

And so, as research continues to advance, ZKPs continue to provide great potential to efficiently address numerous data verification issues (Chen, et al. 2023; Gabay, Akkaya, and Cebe, 2020; Bai, et al. 2022). The integration of ZKPs with a diverse range of privacy-enhancing technologies offers a compelling avenue to enhance data security and uphold confidentiality within the insurance and non-insurance domains.

Section 6: Conclusion

Zero-Knowledge Proofs (ZKPs) have emerged as a revolutionary privacy assurance technology in the insurance sector, reshaping data handling, fraud prevention, regulatory compliance, and customer interactions. In insurance fraud, ZKPs serve as a robust defense, enabling insurers to verify claims while safeguarding sensitive information. For example, claimants can verify whether a claim is legitimate or not, a powerful tool in curbing fraudulent activities. Moreover, ZKPs play a pivotal role in ensuring regulatory adherence. They empower insurers to authenticate customer identities, assess risks, and conduct audits while preserving data confidentiality, a cornerstone for meeting stringent regulations such as HIPAA.

Additionally, ZKPs go beyond operational excellence, offering the potential to revolutionize insurance by fostering equity and inclusivity. In the realm of mental health benefits, the stigma associated with seeking help can be a significant impediment to care. ZKPs provide a discreet avenue for policyholders to confirm eligibility for mental health support without divulging specific conditions, creating an environment where individuals are more encouraged to seek assistance. Additionally, in the onboarding of new employees, ZKPs streamline access to group benefits like pension or healthcare plans, eliminating the need for divulging personal information and ensuring a seamless transition into the workforce. In an industry driven by data, ZKPs stand as a pivotal force, providing privacy, security, and inclusiveness while reimagining the possibilities in an increasingly intricate landscape.

In the near future, the enduring role of ZKPs in fortifying identity verification processes, facilitating claims adjudication, and ensuring unwavering regulatory compliance remains unequivocal. The versatility of ZKPs extends across a varied array of applications, illuminating a trajectory toward an insurance landscape fortified by diverse technological innovation for privacy enhancement, regulatory compliance, and fraud mitigation. This will provide new value propositions through innovative underwriting approaches, agile risk management, and expand customer partnerships.

Section 4: Acknowledgments

The researchers' deepest gratitude goes to those without whose efforts this project could not have come to fruition: the Project Oversight Group for their diligent work overseeing, reviewing, and editing this report for accuracy and relevance.

Project Oversight Group members:

Min Ji, FSA, FIA

Zack Moore, FSA, MAAA

Sudeep Palepu, FSA, ACIA, MAAA

Matthew Smith, FSA, MAAA

Peik Hong Tan, FSA

Tina Yang, FSA, MAAA, CERA

Jingcheng Yu, FSA, CERA

At the Society of Actuaries Research Institute:

Korrel Crawford, Senior Research Administrator

David Schraub, FSA, CERA, MAAA, AQ

References

Agahari, W., Ofe, H., & de Reuver, M. (2022). It is not (only) about privacy: How multi-party computation redefines control, trust, and risk in data sharing. *Electronic markets*, *32*(3), 1577-1602.

Al-Aswad, H., El-Medany, W. M., Balakrishna, C., Ababneh, N., & Curran, K. (2021). BZKP: Blockchain-based zero-knowledge proof model for enhancing healthcare security in Bahrain IoT smart cities and COVID-19 risk mitigation. *Arab Journal of Basic and Applied Sciences*, *28*(1), 154-171.

Al-Aswad, H., Hasan, H., Elmedany, W., Ali, M., & Balakrishna, C. (2019, August). Towards a blockchain-based zero-knowledge model for secure data sharing and access. In *2019 7th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)* (pp. 76-81). IEEE.

Allison, I. (2021, September), JP Morgan is quietly testing cutting-edge Ethereum privacy tech, online; accessed January 18, 2023. https://www.coindesk.com/tech/2019/02/28/jp-morgan-is-quietly-testing- cutting-edge-Ethereum-privacy-tech/

Aslam, F., Hunjra, A. I., Ftiti, Z., Louhichi, W., & Shams, T. (2022). Insurance fraud detection: Evidence from artificial intelligence and machine learning. *Research in International Business and Finance*, *62*, 101744.

Babel, M., & Sedlmeir, J. (2023). Bringing data minimization to digital wallets at scale with general-purpose zero-knowledge proofs. *arXiv preprint arXiv:2301.00823*.

Bai, T., Hu, Y., He, J., Fan, H., & An, Z. (2022). Health-zkIDM: A healthcare identity system based on fabric blockchain and zero-knowledge proof. *Sensors*, *22*(20), 7716.

Baum, C., Damgård, I., Lyubashevsky, V., Oechsner, S., & Peikert, C. (2018, August). More efficient commitments from structured lattice assumptions. In *International Conference on Security and Cryptography for Networks* (pp. 368-385). Cham: Springer International Publishing.

Beneish, M. D. (2001). Earnings management: A perspective. *Managerial finance*, *27*(12), 3-17.

Ben-Sasson, E., Bentov, I., Horesh, Y., & Riabzev, M. (2018). Scalable, transparent, and post-quantum secure computational integrity. *Cryptology ePrint Archive*.

Ben-Sasson, E., Chiesa, A., Tromer, E., & Virza, M. Succinct (2014, August) Non-Interactive Zero Knowledge for a von Neumann Architecture. In Proceedings of the 23rd USENIX Security Symposium (USENIX Security 14), San Diego, CA, USA; pp. 781–796

Berentsen, A., Lenzi, J., & Nyffenegger, R. (2023). An Introduction to Zero-Knowledge Proofs in Blockchains and Economics. *Federal Reserve Bank of St. Louis Review*.

Bhatia, T., Verma, A. K., & Sharma, G. (2018). Secure sharing of mobile personal healthcare records using certificateless proxy re-encryption in cloud. *Transactions on Emerging Telecommunications Technologies*, *29*(6), e3309.

Blaze, M., Bleumer, G., & Strauss, M. (1998, May). Divertible protocols and atomic proxy cryptography. In *International conference on the theory and applications of cryptographic techniques* (pp. 127-144). Berlin, Heidelberg: Springer Berlin Heidelberg.

Burger, E., Chiang, B., Chokshi, S., Lazzarin, E., Thaler, J. , and Ali, Y. (2022, September) Zero knowledge canon, part 1 & 2, https : / / a16zcrypto . com / zero - knowledge-canon/

Cao, S., Zhang, Q., Wang, D., Xiangli, P., & Zhang, X. (2022, April). Hybrid Smart Contracts for Privacy-Preserving-Aware Insurance Compensation. In *2022 IEEE Wireless Communications and Networking Conference (WCNC)* (pp. 1533-1538). IEEE.

Chang, Wayne and Cooban, Anna. (2023, July). China fines Jack Ma's Ant Group nearly $1 billion. *CNN Business*. https://www.cnn.com/2023/07/07/tech/jack-ma-ant-group-fine/index.html

Chen, Y. R., Sha, J. R., & Zhou, Z. H. (2019). IOV privacy protection system based on double-layered chains. *Wireless Communications and Mobile Computing*, *2019*.

Chen, Z., Jiang, Y., Song, X., & Chen, L. (2023). A Survey on Zero-Knowledge Authentication for Internet of Things. *Electronics*, *12*(5), 1145.

Chi, P. W., Lu, Y. H., & Guan, A. (2023). A Privacy-Preserving Zero-Knowledge Proof for Blockchain. *IEEE Access*.

Chiesa, A., Ojha, D., & Spooner, N. (2020). Fractal: Post-quantum and transparent recursive proofs from holography. In *Advances in Cryptology–EUROCRYPT 2020: 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, May 10–14, 2020, Proceedings, Part I 39* (pp. 769-793). Springer International Publishing.

Chin, E. T. W., Kamsin, I. F. B., Amin, S. B., & Zainal, N. K. B. (2023, January). Hybrid Zero-knowledge Access Control System in e-Health. In *2023 15th International Conference on Developments in eSystems Engineering (DeSE)* (pp. 106-111). IEEE.

Chondrogiannis, E., Andronikou, V., Karanastasis, E., Litke, A., & Varvarigou, T. (2022). Using blockchain and semantic web technologies for the implementation of smart contracts between individuals and health insurance organizations. *Blockchain: Research and Applications*, *3*(2), 100049.

Corporate Research and Investigations Group (2021). Insurance fraud case studies uncovered.https://crigroup.com/wp-content/uploads/2021/Insurance-Fraud-Case-Studies-Uncovered.pdf

Derrig, R. A. (2002). Insurance fraud. *Journal of Risk and Insurance*, *69*(3), 271-287.

Diro, A., Lu Zhou, L., Saini, A., Kaisar, S., & Pham, H. (2023, June). Leveraging Blockchain for Zero Knowledge Identify Sharing: A Survey of Advancements, Challenges and Opportunities. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4469520

Do, J. M., Song, Y. J., & Park, N. (2011, May). Attribute based proxy re-encryption for data confidentiality in cloud computing environments. In *2011 First ACIS/JNU International Conference on Computers, Networks, Systems and Industrial Engineering* (pp. 248-251). IEEE.

Dwork, C., McSherry, F., Nissim, K., & Smith, A. (2006). Calibrating noise to sensitivity in private data analysis. In *Theory of Cryptography: Third Theory of Cryptography Conference, TCC 2006, New York, NY, USA, March 4-7, 2006. Proceedings 3* (pp. 265-284). Springer Berlin Heidelberg.

ElSheikh, M., & Youssef, A. M. (2022). Dispute-free scalable open vote network using zk-SNARKs. *arXiv preprint arXiv:2203.03363*.

European Parliamentary Research Service (2019, July). Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law? https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf

Ferenczi, A. (2022, December). Zero-knowledge proof-based virtual cards, *American Express Travel Related Services Company*, US Patent 11,538,019.

Fiat, A., & Shamir, A. (1986, August). How to prove yourself: Practical solutions to identification and signature problems. In *Conference on the theory and application of cryptographic techniques* (pp. 186-194). Berlin, Heidelberg: Springer Berlin Heidelberg.

Fong, D., Han, F., Liu, L., Qu, J., & Shek, A. (2021, November). Seven technologies shaping the future of fintech. *McKinsey & Company*. https://www.mckinsey.com/cn/our-insights/our-i nsights/seven-technologies-shaping-the-future-of-fintech

Fontaine, C., & Galand, F. (2007). A survey of homomorphic encryption for nonspecialists. *EURASIP Journal on Information Security*, *2007*, 1-10.

Gaba, G. S., Hedabou, M., Kumar, P., Braeken, A., Liyanage, M., & Alazab, M. (2022). Zero knowledge proofs based authenticated key agreement protocol for sustainable healthcare. *Sustainable Cities and Society*, *80*, 103766.

Gabay, D., Akkaya, K., & Cebe, M. (2020). Privacy-preserving authentication scheme for connected electric vehicles using blockchain and zero knowledge proofs. *IEEE Transactions on Vehicular Technology*, *69*(6), 5760-5772.

Goldwasser, S., Micali, S., & Rackoff, C. (1989). The knowledge complexity of interactive proof-systems. In *SIAM J. Comput*. 18, 186-208.

Guo, H., Li, W., Nejad, M., & Shen, C. C. (2022). A Hybrid Blockchain-Edge Architecture for Electronic Health Record Management with Attribute-based Cryptographic Mechanisms. *IEEE Transactions on Network and Service Management*.

Haig, S. (2022, May), EY and Polygon unveil ZK and optimistic rollup hybrid, online; accessed January 18, 2023. https://www.yahoo.com/video/ey-polygon-unveil-zk-optimistic-101527165.html.

Han, X., Call, K. T., Pintor, J. K., Alarcon-Espinoza, G., & Simon, A. B. (2015). Reports of insurance-based discrimination in health care and its association with access to care. *American journal of public health*, *105*(S3), S517-S525.

Hao, M., Qian, K., & Chau, S. C. K. (2023). Privacy-preserving Blockchain-enabled Parametric Insurance via Remote Sensing and IoT. *arXiv preprint arXiv:2305.08384*.

Harikrishnan, M., & Lakshmy, K. V. (2019, March). Secure digital service payments using zero knowledge proof in a distributed network. In *2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS)* (pp. 307-312). IEEE

Huang, C., Wang, W., Liu, D., Lu, R., & Shen, X. (2022). Blockchain-assisted personalized car insurance with privacy preservation and fraud resistance. *IEEE Transactions on Vehicular Technology*, *72*(3), 3777-3792.

Huang, C., Lu, R., Ni, J., & Shen, X. (2020). DAPA: A decentralized, accountable, and privacy-preserving architecture for car sharing services. *IEEE Transactions on Vehicular Technology*, *69*(5), 4869-4882.

ING Group (2017, November), ING launches zero-knowledge range proof solution,a major addition to blockchain technology, online; accessed January 18, 2023. https://www.ingwb.com/en/insights/distributed-ledger-technology/ing-launches-major-addition-to-blockchain-technology,

Khanna, A. (2023, August). Fraud in insurance - Health insurance fraud on the rise. *Asia Insurance Review*. https://www.asiainsurancereview.com/Magazine/ReadMagazineArticle/ aid/47132/Fraud-in-insurance-Health-insurance-fraud-on-the-rise

Kassaras, S., & Maglaras, L. (2020, September). ZKPs: Does This Make The Cut?. CEUR-WS.https://dora.dmu.ac.uk/bitstream/handle/2086/20122/Kassaeas%20paper.pdf

Kim, K. S., & Jeong, I. R. (2016). Collusion-resistant unidirectional proxy re-encryption scheme from lattices. *Journal of Communications and Networks*, *18*(1), 1-7.

Lee, J., Choi, J., Oh, H., & Kim, J. (2021). Privacy-preserving identity management system. *Cryptology ePrint Archive*. https://eprint.iacr.org/2021/1459.pdf

Lin, C., Luo, M., Huang, X., Choo, K. K. R., & He, D. (2021). An efficient privacy-preserving credit score system based on noninteractive zero-knowledge proof. *IEEE systems journal*, *16*(1), 1592-1601.

Liu, W., Yu, Q., Li, Z., Li, Z., Su, Y., & Zhou, J. (2019, December). A blockchain-based system for anti-fraud of healthcare insurance. In *2019 IEEE 5th International Conference on Computer and Communications (ICCC)* (pp. 1264-1268). IEEE.

Lu, J., Lin, K., Chen, R., Lin, M., Chen, X., & Lu, P. (2023). Health insurance fraud detection by using an attributed heterogeneous information network with a hierarchical attention mechanism. *BMC Medical Informatics and Decision Making*, *23*(1), 1-17.

Marleau, P., Brubaker, E., Hilton, N. R., McDaniel, M., Schroeppel, R. C., Seager, K. D., & Deland, S. M. (2015). Zero Knowledge Protocol: Challenges and Opportunities. Sandia National Lab. https://www.osti.gov/biblio/1261022

Midha, M., Gupta, A. K., & Mathur, P. (2021). Review on Zero-Knowledge Proof Method. In *Proceedings of the Second International Conference on Information Management and Machine Intelligence: ICIMMI 2020* (pp. 299-306). Springer Singapore.

Mina Foundation (2022, June), State of zero knowledge report 2022, online; accessed January 18, 2023.https://minaprotocol.com/wp- content/uploads/zkReport 2022 EN.pdf,

Munjal, K., & Bhatia, R. (2022). A systematic review of homomorphic encryption and its contributions in healthcare industry. *Complex & Intelligent Systems*, 1-28.

National Association of Insurance Commissioners (2022, December), Insurance fraud https://content.naic.org/cipr-topics/insurance-fraud

Niraula, T., Pokharel, A., Phuyal, A., Palikhel, P., & Pokharel, M. (2022). Quantum computers' threat on current cryptographic measures and possible solutions. *Int. J. Wirel. Microw. Technol*, *12*, 10-20.

Pauwels, P. (2021). zkKYC: A solution concept for KYC without knowing your customer, leveraging self-sovereign identity and zero-knowledge proofs. *Cryptology ePrint Archive*.

Qi, H., Wan, Z., Guan, Z., & Cheng, X. (2020). Scalable decentralized privacy-preserving usage-based insurance for vehicles. *IEEE Internet of Things Journal*, *8*(6), 4472-4484.

Qin, Z., Xiong, H., Wu, S., & Batamuliza, J. (2016). A survey of proxy re-encryption for secure data sharing in cloud computing. *IEEE Transactions on Services Computing*.

Retail Banker International (2022, December), Cybersecurity innovation: Leading companies in zero-knowledge proof for the banking industry, online; accessed January 18, 2023. https://www.retailbankerinternational.com/data-insights/innovators-zero-knowledge-proof-banking/

Rivest, R. L., Adleman, L., & Dertouzos, M. L. (1978). On data banks and privacy homomorphisms. *Foundations of secure computation*, *4*(11), 169-180.

Sasson, E. B., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., & Virza, M. (2014, May). Zerocash: Decentralized anonymous payments from bitcoin. In *2014 IEEE symposium on security and privacy* (pp. 459-474). IEEE.

Sharma, B., Halder, R., & Singh, J. (2020, January). Blockchain-based interoperable healthcare using zero-knowledge proofs and proxy re-encryption. In *2020 International Conference on Communication Systems & Networks (COMSNETS)* (pp. 1-6). IEEE.

Sun, X., Yu, F. R., Zhang, P., Sun, Z., Xie, W., & Peng, X. (2021). A survey on zero-knowledge proof in blockchain. *IEEE network*, *35*(4), 198-205.

Thurman, A. (2022, March). Mina foundation raises $92M to accelerate the adoption of zero-knowledge proofs, *CoinDesk*, online; accessed February 12, 2023. https://www.coindesk.com/business/2022/03/17/ mina- foundation-raises- 92m- to- accelerate- adoption- of-zero-knowledge-proofs/

Vasconcelos Barros, M., Schardong, F., & Felipe Custódio, R. (2022). Leveraging self-sovereign identity, blockchain, and zero-knowledge proof to build a privacy-preserving vaccination pass. *Blockchain, and Zero-Knowledge Proof to Build a Privacy-Preserving Vaccination Pass*.

Veeningen, M., Chatterjea, S., Horváth, A. Z., Spindler, G., Boersma, E., van der Spek, P., ... & Veugen, T. (2018, January). Enabling Analytics on Sensitive Medical Data with Secure Multi-Party Computation. In *MIE* (pp. 76-80).

Wan, Z., Guan, Z., Zhou, Y., & Ren, K. (2019, July). Zk-AuthFeed: How to feed authenticated data into smart contract with zero knowledge. In *2019 IEEE International Conference on Blockchain (Blockchain)* (pp. 83-90). IEEE.

Wan, Z., Zhou, Y., & Ren, K. (2022). Zk-AuthFeed: Protecting data feed to smart contracts with authenticated zero knowledge proof. *IEEE Transactions on Dependable and Secure Computing*, *20*(2), 1335-1347.

Wang, D., Zhao, J., & Wang, Y. (2020). A survey on privacy protection of blockchain: The technology and application. *IEEE Access*, *8*, 108766-108781.

Wen, X. J., Chen, Y. Z., Fan, X. C., Zhang, W., Yi, Z. Z., & Fang, J. B. (2022). Blockchain consensus mechanism based on quantum zero-knowledge proof. *Optics & Laser Technology*, *147*, 107693.

Xiao, L., Deng, H., Tan, M., & Xiao, W. (2020). Insurance block: a blockchain credit transaction authentication scheme based on homomorphic encryption. In *Blockchain and Trustworthy Systems: First International Conference, BlockSys 2019, Guangzhou, China, December 7–8, 2019, Proceedings 1* (pp. 747-751). Springer Singapore.

Yao, A. C. (1982, November). Protocols for secure computations. In *23rd annual symposium on foundations of computer science (sfcs 1982)* (pp. 160-164). IEEE.

Zhang, W., Wei, C. P., Jiang, Q., Peng, C. H., & Zhao, J. L. (2021). Beyond the block: A novel blockchain-based technical model for long-term care insurance. *Journal of Management Information Systems*, *38*(2), 374-400.

Zhao, Y., & Chen, J. (2022). A survey on differential privacy for unstructured data content. *ACM Computing Surveys (CSUR)*, *54*(10s), 1-28.

Zheng, H., You, L., & Hu, G. (2022). A novel insurance claim blockchain scheme based on zero-knowledge proof technology. *Computer Communications*, *195*, 207-216.

Research Section are responsible for the reliability, accuracy or content of the third-party site(s). If you have questions about the content on such sites, please contact the site directly.

About The Society of Actuaries Research Institute

Serving as the research arm of the Society of Actuaries (SOA), the SOA Research Institute provides objective, data-driven research bringing together tried and true practices and future-focused approaches to address societal challenges and your business needs. The Institute provides trusted knowledge, extensive experience and new technologies to help effectively identify, predict and manage risks.

Representing the thousands of actuaries who help conduct critical research, the SOA Research Institute provides clarity and solutions on risks and societal challenges. The Institute connects actuaries, academics, employers, the insurance industry, regulators, research partners, foundations and research institutions, sponsors and non-governmental organizations, building an effective network which provides support, knowledge and expertise regarding the management of risk to benefit the industry and the public.

Managed by experienced actuaries and research experts from a broad range of industries, the SOA Research Institute creates, funds, develops and distributes research to elevate actuaries as leaders in measuring and managing risk. These efforts include studies, essay collections, webcasts, research papers, survey reports, and original research on topics impacting society.

Harnessing its peer-reviewed research, leading-edge technologies, new data tools and innovative practices, the Institute seeks to understand the underlying causes of risk and the possible outcomes. The Institute develops objective research spanning a variety of topics with its strategic research programs: aging and retirement; actuarial innovation and technology; mortality and longevity; diversity, equity and inclusion; health care cost trends; and catastrophe and climate risk. The Institute has a large volume of topical research available, including an expanding collection of international and market-specific research, experience studies, models and timely research.

Society of Actuaries Research Institute
475 N. Martingale Road, Suite 600
Schaumburg, Illinois 60173
www.SOA.org