# Modelling the Secure Computational Marketplace by Deriving Abstractions From Technical Implementations in Modern Cryptography

Josh Fourie

State of the art cryptographic routines have historically exposed unforeseen economic opportunities for the market, and contemporary advancements in zero-knowledge, and secure multi-party computation primitives will continue to reveal similar and exciting prospects in the future. The schemes discussed here are all commonly capable of uniquely guaranteeing the integrity of computational processes without compromising, or otherwise reducing, the privacy of market participants. This paper introduces a novel conception of the *secure computational marketplace*, which refers to a collection of abstract observations and qualities inherent to these technologies, and then coalesced as an impression of a descriptive, pseudo-economic model. The marketplace operates as an extension of modern cloud-computing architecture to manifest as a solution for the development of an interim bridge apprehending the realisation of, and transition into,the homomorphic data-economy.

## 1 Introduction: Cryptography

Cryptographic routines encode and embed security into information systems so as to protect the substantive content of data-stores or lines of communication from unauthorised access. The underlying cryptographic primitives of an implementation 'hide' the sensitive authorisation codes governing access to the vulnerable information within computationally hard problems that cannot be efficiently solved on a classical or quantum computer. A party has proven authorisation wherever they are capable of providing, or demonstrating a knowledge of the solution. Importantly, cryptographic schemes adapt alongside the development of computing technology, but methodologies may be deprecated where efficient solutions to the underlying challenge are discovered.

**RSA.** The structural implications of novel cryptographic routines are evident in the implementation of the RSA digital-signature scheme underlying the modern internet-economy [SOURCE]. The protocol was developed in response to a paper from Diffie and Hellman [SOURCE], calling for the development of cryptographically encoded communication schemes that would provide security in the presence of an adversary, based on a public-private encryption-decryption routine reliant on the hardness of exponents problem [CONFIRM]. The technology empowered any party to verify the origins of a secretly exchanged message with strong guarantees. Subsequently, the routines embedded an element of verifiability in the open-communication protocols which exposed opportunities for early e-commerce and trusted messaging schemes.

**The Trident.** Contemporary advancements within the distinct design and implementations of zero-knowledge, multi-party, and homomorphic computation routines promise to disruptively embed privacy-as-a-default within cyber-infrastructure with similar economic benefits. The protocols are commonly motivated by an impetuous to verifiably compute on data, without transferring or otherwise exposing the information along vulnerable lines of communication, or revealing the substantive content when inadvertently engaging an adversary. Secure multi-party computation and zero-knowledge proofing routines pre-empt the realisation of homomorphic encryption, which will substantially narrow, but not necessarily obviate, the utility of the aforementioned systems. The development of variations to these routines, as well as particular technical augmentations, distinguish themselves with regards to the underlying mathematical problem or assumption, such as a choice of lattice or number-theoretic hardness. Consequentially, it is permissible to extrapolate the essential character of the schemes in resolving the tension between privacy and computational integrity as a workable technical abstraction.

**Homomorphism.** Homomorphic encryption is the 'Goldilocks' of modern-Cryptography enabling any party to compute on an encrypted data-set without decryption. [FILL OUT INTRO.] The realisation of homomorphic technology intuitively disrupts the economic infrastructure of the data-economy.

**Multi-Party.** Secure multi-party computation was introduced by Yao [SOURCE] to resolve the motivating dilemma where a collection of parties wish to compute the aggregate analysis of their data without sharing the information amongst themselves. [FILL OUT INTRO.] Similarly, secure multi-party computation would provide significant economic opportunities for cases such as decentralised aggregate analysis of a population.

**Zero-Knowledge.** The zero-knowledge construction is used loosely within this paper to describe the technologies deriving from GWR [SOURCE], enabling a single party to prove the integrity of a computation without revealing the underlying information. [1] Generically, a zero-knowledge routine requires that a party $\mathcal{P}$ initially computes a pre-agreed circuit over a set of private witness inputs, which are then blinded and abstracted to an alternate representation such as 3-Circuit-Satisfiability (3-SAT) [SOURCE]. [2] The counter-party verifies the computational integrity of the circuit by checking the logic of the blinded abstraction at randomly selected points. Contrary to traditional cryptographic routines, zero-knowledge schemes avoid enabling authorised access to the witness inputs, such that a party external to the circuit computation is incapable of decrypting or revealing the sensitive information. The

[1] The term also refers to the 'zero-knowledge' condition common to each routine.

[2] A witness is an efficiently checkable solution to an computationally hard problem.

zero-knowledge condition forms a tripartite description of the schemes, alongside a remaining guarantee that the verification of a proof of computational integrity will correctly discern between honest and dishonest actors within negligible error bounds.

The remainder of the paper is concerned with explicating the architectural consequences of these technologies, evaluating the state-of-the-art, and then extracting the yet-unexplained secure computational marketplace model.

## 2 Introduction: Cloud-Computing

The probable economic significance of modern cryptographic routines rely on limitations inherent to the architecture of the data-economy, with regards to privacy and security structures. It is important to elucidate the relevant constraints by detouring through a contextual analysis of existing and near-future cloud-computing systems. Note that although cryptography is not a panacea, the consequential structural augmentations may provide some relief for these limitations and reveal alternate implementation options.

**The Cloud.** Cloud-computing is a network architecture that off-loads localised computations on sensitive information to a central repository, which may itself be distributed or reliant on cloud services. The motivation for these systems is connected to the inherent character or computational requirements of the task, as well as the need for verifiability and integrity in the computational processes. There are benefits to layering and distributing the architecture amongst the 'edge' and 'fog' components that are connected to performance, security and privacy considerations. There is an important role for modern cryptography within cloud-computing design, not only in securing the transmission of information along lines of communication for decryption and analysis, but in reducing the need for authorised access to that information and promoting localisation.

**Risk and Monopoly.** The capacity to manage risk in the cloud-computing model is disproportionately distributed amongst the parties contributing to the transmission and analysis of sensitive information rather than the data-source. These entities are held accountable to the damages of a breach *ex ante* by legal or market remedies, rather than an intrinsic loss of property or value. Securing the lines of communication transmitting and processing the flow of information en route to the cloud is notoriously difficult, and requires implementing a range of cryptographic and cyber-security routines and mechanisms, which expose the network to implementation vulnerabilities. Cloud-computing requires that any data is securely transmitted along these encrypted channels, and an adversarial exploit will expose any shared information. Data sources manage and mitigate the risk of breaches through selective data transmission along at least semi-trusted communication pathways, where there exists a legal or social identity that may be held accountable. Consequentially, data-ownership monopolises amongst corporates capable of off-setting the risk through demonstrated technical skill, or compensatory regimes.

The cyber-architecture of contemporary systems are organised around the underpinning assumption that a computation over the data will only maintain integrity when processed on any of the layers of the cloud, which inherently requires possession and thereby secure data transmission. The guarantees provided by modern cryptographic primitives have been developed to explicitly challenge the premise that computational integrity is incoherent alongside the localisation of data analytics, and therefore represents a potential alternative for cloud-computing architecture.

**IoT.** The concept of an Internet of Things is engendered within cloud-computing technology and refers to the intelligent devices communicating both locally on the network and with the cloud

, but the architecture is particularly vulnerable to data-transmission breaches and privacy concerns.

**IoT.** The 'revolution' accompanying the Internet of Things engendered within cloud-technology exposes relevant yet distinct opportunities for the matter at hand. There is an evident motivation to extract the data processed by devices positioned in the household that are capable of measuring and extrapolating previously inaccessible information. There exists, however, a parallel concern that a cloud-computing model reliant on lines of communication for that information would embed a security risk in the architecture. Moreover, there may be a societal resistance to accurately sharing the collected information without strong privacy guarantees. The implications of these privacy and security concerns are influential amongst industry, but a concrete and substantial resolution appears unlikely.

**AI.** Though not necessarily a consequence of cloud-computing, Artificial Intelligence relies predominantly on layered cloud-architecture for computing machine-learning routines and other essential processes. The utility of AI technology is, furthermore, deeply and inherently connected to 'Big Data' analysis consuming sensitive information for the development of training models, typically executed on the cloud-layer. The relevant dilemma relates to the AI's dependence on the integrity of the computations responsible for analysing data-sets and deriving learning models, which resists the privacy-preserving mechanisms required to ensure the legitimacy and granularity of the collected data.