Distributed Cyber-infrastructures and Artificial Intelligence in Hybrid Post-Quantum Era

Attila A. Yavuz
University of South Florida
attilaayavuz@usf.edu

Saif E. Nouma
University of South Florida
saifeddinenouma@usf.edu

Thang Hoang
Virginia Tech
thanghoang@vt.edu

Duncan Earl
Qubitekk, Inc.
dearl@qubitekk.com

Scott Packard
Qubitekk, Inc.
spackard@qubitekk.com

***Abstract*—Distributed cyber-infrastructures and Artificial Intelligence (AI) are transformative technologies that will play a pivotal role in the future of society and the scientific community. Internet of Things (IoT) applications harbor vast quantities of connected devices that collect a massive amount of sensitive information (e.g., medical, financial), which is usually analyzed either at the edge or federated cloud systems via AI/Machine Learning (ML) algorithms to make critical decisions (e.g., diagnosis). It is of paramount importance to ensure the security, privacy, and trustworthiness of data collection, analysis, and decision-making processes. However, system complexity and increased attack surfaces make these applications vulnerable to system breaches, single-point of failures, and various cyber-attacks. Moreover, the advances in quantum computing exacerbate the security and privacy challenges. That is, emerging quantum computers can break conventional cryptographic systems that offer cyber-security services, public key infrastructures, and privacy-enhancing technologies. Therefore, there is a vital need for new cyber-security paradigms that can address the resiliency, long-term security, and efficiency requirements of distributed cyber infrastructures.**

In this work, we propose a vision of distributed architecture and cyber-security framework that uniquely synergizes secure computation, Physical Quantum Key Distribution (PQKD), NIST Post-Quantum Cryptography (PQC) efforts, and AI/ML algorithms to achieve breach-resilient, functional and efficient cyber-security services. At the heart of our proposal lies a new *Multi-Party Computation Quantum Network Core* (MPC-QNC) that enables fast and yet quantum-safe execution of distributed computation protocols via integration of PQKD infrastructure and hardware-acceleration elements. We showcase the capabilities of MPC-QNC by instantiating it for Public Key Infrastructures (PKI) and federated ML in our HDQPKI and TPQ-ML, frameworks, respectively. HDQPKI (to the best of our knowledge) is the first hybrid and distributed post-quantum PKI that harnesses PQKD and NIST PQC standards to offer the highest level of quantum safety with a breach-resiliency against active adversaries. TPQ-ML presents a post-quantum secure and privacy-preserving federated ML infrastructure.

***Index Terms*—cyber-infrastructures; post-quantum security; artificial intelligence; machine learning; multi-party computation.**

I. Introduction

Internet of Things (IoT) has seen enormous growth over the last decades. It is expected that the number of IoT devices will continue to increase at significant rates [1]. Its applications can be extended to a wide range of fields, including but not limited to healthcare, smart cities, manufacturing, and military. The IoT ecosystems gather, process, and exchange a sheer amount of privacy and security-critical information. For example, IoT nodes (e.g., air drones, mobile devices, sensors) communicate massive amounts of telemetry to the cloud servers for processing and long-term maintenance. Designing autonomous IoT systems might substantially reduce human interventions via enabling cooperation, machine-to-machine (M2M) communications, and harnessing distributed designs [2].

The high volume of sensitive and valuable information is considered one of the main fuels of the emerging Artificial Intelligence (AI) and Machine Learning (ML) [3] approaches. The collected data can be processed at the edge before offloading it to a cloud system, or it can be directly transferred to a federated cloud cluster for analysis. IoT components can benefit from AI/ML systems by enabling autonomous decision-making and orchestrating their distributed nature [4]. Such applications [3] can be seen in numerous potential domains such as autonomous driving, smart homes, health care systems, and smart agriculture, to name a few.

With all the advantages brought by IoT networks and distributed cyber-infrastructures in general, there also exist numerous challenges related to their security and privacy [5]. The scalability hurdles and resource limitations of the edge devices increased attack vectors and system breaches. This makes it a highly challenging task to ensure the trustworthiness of IoT systems and distributed cyber-infrastructures. For instance, Public Key Infrastructures (PKI) form the foundation of fundamental security services in cyber-infrastructures. Yet, they usually rely on centralized architectures that lead to several single points of failures and system breaches. Similarly, the various AI/ML applications only recently started to receive benefits from the emerging federated cloud infrastructures.

One of the major cyber-security technologies, Multi-Party Computation (MPC) [6], enables multiple data owners to cooperatively compute a given function by separately integrating their resources, in a way that prevents leakage of confidential data. The aforementioned function can be any cryptographic (e.g., digital signature) or AI/ML algorithm and therefore MPC can interplay with both emerging areas to enable trustworthy data processing methods. For instance, NIST [7] recently provided a roadmap toward the standardization of threshold (distributed) schemes for cryptographic primitives. However, there is a significant gap in the existing cyber-infrastructures and their applications for harnessing secure distributed technologies to mitigate hurdles stemming from centralization. Moreover,

despite the recent progress of MPC techniques, they may still incur high overhead for IoT and ML applications [8].

On top of the security challenges due to centrality, the advent of quantum computers threatens the conventional cryptographic primitives that lay the foundation of essential security services. That is, Shor [9] showed that quantum computing can break the conventional intractability assumptions such as factorization of large integers (RSA) and discrete logarithms problems (Elliptic Curves). This threat requires urgent action to protect sensitive data (e.g., finance, health, military). Such data is currently circulated over pre-quantum cyber-infrastructures, encrypted with classic cryptosystems (e.g., RSA [10]). Even though the current progress of quantum computers is still underway, a potential threat, known as Store-and-Decrypt [11], is considered the major menace that pushes regulation firms (e.g., NIST) to accelerate the standardization of post-quantum cryptography (PQC). NIST's standartization [12] efforts play a pivotal role in migration from conventional to post-quantum settings. However, the adaptation of these new technologies is challenging due to their complexity and heavy overhead [11].

In this paper, we propose an architectural design and framework that synergizes the emerging cyber-security building blocks and cyber-infrastructure elements to cohesively offer efficient, trustworthy, and scalable real-life applications. This architecture and framework integrate post-quantum cryptography, physical quantum key distribution, hardware-acceleration components, and distributed computation paradigm that interplay with the de-centralized nature of emerging IoTs and information technology systems. We outline some of the desirable features of our architecture below:

• Optimized MPC framework via PQKD Infrastructures: MPC offers an ideal algorithmic framework to address the resiliency and trust distribution needs of decentralized systems. However, MPC may introduce significant delays due to multi-round communications, and high computation overhead for complex cryptographic schemes and ML algorithms. These performance challenges grow when post-quantum security is required. We identify that an ideal infrastructure to execute MPC requires a dedicated high-speed network among servers, which are connected via pairwise secure channels (ideally quantum-safe). Moreover, notable MPC paradigms receive benefits from online-offline techniques, wherein expensive cryptographic operations are pre-computed, while communication-intensive steps are done online.

Our key observation is that emerging PQKD infrastructures and hardware-acceleration platforms offer an ideal infrastructure to execute MPC with post-quantum security. In our MPC-QNC framework (Section III-A), we harness the dedicated optical network with quantum-safe pairwise connection of PQKD systems to raise a MPC core (e.g., 2-3 server setup) platform. MPC-QNC also couples PQKD with GPU/FPGA commonly presence in modern federated cloud architectures. Therefore, MPC-QNC can enhance both the online and offline phases of MPC with post-quantum security.

• Distributed and Quantum-Safe Root of Trust: The centralized nature of the current CA entities poses several vulnerabilities against cyber-attacks [13]. We utilize MPC-QNC to design a Hybrid Post-Quantum Distributed PKI (HDQPKI, Section III-B) that thresholds NIST PQC standards to generate breach-resilient and quantum-safe certificates. Moreover, HDQPKI uses quantum-random number generators to minimize side-channel attacks for lattice-based schemes, while increasing the scalability of PQKD via NIST PQC standards.

• Privacy-Preserving and Quantum-Safe ML: We present a Trustworthy Post-Quantum Machine Learning (TPQ-ML) platform, which enables a breach-resilient execution of classical ML algorithms (e.g., linear regression) on MPC-QNC. This design showcases applications of distributed computation to ML with an omitted aspect of quantum safety.

The organization of this paper is as follows. In Section II, we first give the algorithmic and architectural building blocks forming our proposed framework and architecture. We then describe our proposed vision in Section III, with a focus on our distributed post-quantum secure computation framework that is instantiated to enable trustworthy PKI and AI/ML applications. Section IV concludes this paper. The notations, used in the paper, are described in Table I.

TABLE I: List of Acronyms

Notations	Description
IoT	Internet of Things
NIST	National Institute of Standards and Technology
CA	Certificate Authority
PQC	Post-Quantum Cryptography
PKI	Public-key Infrastructure
MPC	Multi-Party Computation
ML	Machine Learning
KEM	Key Encapsulation Mechanism
KEX	Key Exchange
MPC-QNC	Multi-Party Computation Quantum Network Core
TPQ-ML	Trustworthy Post-Quantum Machine Learning
HDQPKI	Hybrid Distributed Quantum Public-Key Infrastructure
HQKD	Hybrid Quantum Key Distribution
PQKD	Physical Quantum Key Distribution
HA-MPC	Hardware-Accelerated Multi-Party Computation

II. Building Blocks of the Proposed Framework

Our architecture harnesses various cryptographic primitives, protocols, machine learning techniques, and cyber infrastructures with special hardware components to achieve its intended goals. We first outline computationally secure post-quantum cryptographic primitives with an emphasis on the recent NIST PQC standards. We then summarize PQKD approaches that form the physical foundation for some aspects of our architecture. We then discuss secure multi-party computation and ML algorithms that enable trustworthy distributed computation and analytics capabilities for our framework.

A. Post-Quantum Cryptographic Primitives

We first outline NIST PQC Standards, and then summarize alternative schemes considered in the NIST PQC competition.

1) NIST PQC Standards: NIST announced the cryptosystems to be standardized [12], namely Dilithium [14], Falcon [15], and SPHINCS+ [16] as digital signatures while only Kyber [17] have been selected as Key Encapsulation Mechanism (KEM). While Dilithium [14], Falcon [15], and Kyber [17] are lattice-based algorithms, SPHINCS+ [16] is a hash-based digital signature. NIST also holds other cryptosystems as alternatives and proceed to the 4^{th} round [18].

Kyber [17] is a Key Encapsulation Mechanism (KEM) secure under chosen-ciphertext attack (IND-CCA). It relies on Module Learning with Errors (M-LWE) [19]. The KEM is obtained via Fujisaki-Okamoto transform [20] over Kyber public-key encryption. Additionally, Kyber offers an (authenticated) key exchange protocol (KEX) that can support quantum-safe TLS protocol for ephemeral key exchange over the Internet. It works on a pre-defined single ring (i.e., $R_q = \mathbb{Z}_{7681}[x]/(x^{256}+1)$) that offers different security and performance trade-offs by merely modifying a system parameter.

Dilithium [14] is built from an identification (ID) scheme, whose security relies on both learning with errors over rings problem (R-LWE) and finding the shortest integer solution in lattices (R-SIS) [21]. Afterward, the signature is constructed from the ID scheme via Fiat-Shamir with Aborts transformation [22]. It avoids the use of costly operation, Gaussian rejection sampling, that prior lattice-based signatures are employing, which led to devastating side-channel attacks [23], [24]. Rather, Dilithium uses a sampler from uniform distribution to add noises from a secret seed during the signature generation. As a lattice-based scheme, Dilithium enjoys different hardware/software optimizations. For instance, the vectorization technique can enable a significant speedup on multi-core machines (e.g., the use of AVX2 instructions can achieve $4.5\times$ speedup over the basic implementation). Dilithium has a well-balanced computational overhead and private/public key sizes.

Falcon [15] is a lattice-based digital signature that offers smaller key and signature sizes, compared with Dilithium and SPHINICS+ [16]. Falcon is a combination GPV framework [25], NTRU lattices [26], and Fast Fourier sampling [27]. NTRU lattices enable a compact public key and signature size (e.g., $3.4\times$ smaller than Dilithium) while Fast Fourier sampling offers a significant speed-up for signing (e.g., $4.25\times$ faster than SPHINCS+ [16]). However, its signature generation harness double-precision floating-point arithmetic that hinders its deployment in resource-constrained devices (e.g., IoT devices). Also, Falcon employs discrete Gaussian sampling over integers and therefore is more prone to side-channel attacks [28].

SPHINCS+ [16] is a hash-based signature based on a One-Time Signature (OTS) called WOTS+ [29]. It employs a hypertree data structure to build a multiple-time signature scheme. SPHINCS+ is a stateless scheme following Goldreich's scheme [30]. Hence, it does not require state management during the signature generation. SPHINCS+ offers a stronger security guarantee since it is solely relying on the cryptographic hash functions. Its agile design enables a smooth update in case the used hash function is broken. However, it has very large key sizes and slow signature generation/verification that makes it unsuitable for low-end devices and time-critical applications.

2) Alternative PQC Cryptosystems: Apart from lattice and hash-based primitives, there are various other PQC techniques relying on different intractability assumptions.

Code-based Cryptosystems originated from McEliece's public-key encryption system, which relies on the Syndrome Decoding Problem and binary Goppa codes [31]. They offer strong security reductions and fast signature generation/verification. However, they were not selected for the standardization due to the large public keys ($\approx$ 1MB) compared to hash-based and lattice-based approaches.

Multivariate-Quadratic (MQ) Signatures rely on the hardness of solving multivariate quadratic equations over a finite field. Despite having a slow signing algorithm, MQ-based schemes heavily rely on algebraic operations, making them a suitable candidate for thresholding [32]. Numerous schemes were considered in NIST PQC successive rounds, but none is among the finalists. Several such signature schemes (e.g., Rainbow [33], UOV [34]) have been attacked.

Isogeny-based Cryptosystems is based on the properties of supersingular elliptic curves and isogeny graphs [35]. They use the mathematics of supersingular elliptic curves to create KEX protocols, which mainly fall into two categories: supersingular isogeny Diffie-Hellman (SIDH) [35] and commutative supersingular isogeny Diffie-Hellman (CSIDH) [36]. Isogeny-based schemes offer remarkably smaller private/public key and signature sizes compared to their post-quantum counterparts. However, Castryck et al. [37] recently broke a SIDH-based KEX algorithm, named SIKE [38]. We note that the broken scheme successfully passed *three successive rounds* in the NIST competition. NIST announced that SIDH-based algorithms should not be used, but this does not affect other isogeny-based cryptosystems such as CSIDH [36] or SQISign [39].

B. Physical Quantum Key Distribution

Quantum Key Distribution (QKD) is an emerging technology that uses quantum phenomena to ensure the security of critical communications. QKD technology uses key aspects of quantum physics, as opposed to mathematical techniques, to generate and securely distribute a secret encryption key. Seminal works (e.g., [40]) use QKD to exchange secret cryptographic keys. This allows for the real-time detection of an adversary's attempt to intercept the key exchange, because an attempt to steal the key as it is communicated between trusted/authenticated parties changes the key in an immediate and measurable way, reducing the possibility that information has been compromised.

The method of QKD used in this protocol, BBM92, is based on the BB84 [41]. Similar to BB84, BBM92 uses entangled photon pairs for encryption, as depicted in Fig.1. Where BBM92 differs is in the employment of decoy states [42] of multiple photons to a single photon for BB84, and the use of only two polarization states instead of the four states used in BB84, as shown in the Equation 1.

$$|\phi >= \frac{1}{\sqrt{2}}|H_1 \cdot V_2 > + |V_1 \cdot H_2 > \tag{1}$$

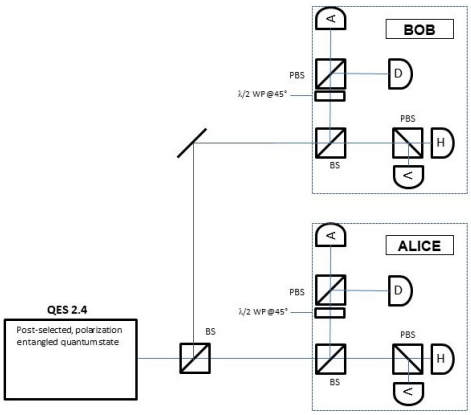

Fig. 1: BBM92 Model.

The resulting randomly generated qubits are used to produce symmetric cryptographic keys rather than relying on complex mathematical assumptions that may or may not be immune to quantum computing resources.

The advantages of QKD include the ability to offer long-term communication security, immediate detection of channel eavesdropping, and maintenance-free key management. However, QKD is limited by signal loss in fiber transmission, as well as polarization mode preservation problem caused by stress-induced birefringence and the mechanical rotation of the fiber carrying the quantum signal.

Optical fiber can support two orthogonal polarization modes. When light in a definite polarization state is launched into a fiber, it will remain in a definite polarization state as it propagates [1]. However, stress-induced birefringence in the fiber and simple mechanical rotation changes the polarization so that the state at the end of the fiber is not the same as the launch state. Moreover, the state is constantly changing unless the fiber is in a very stable environment (e.g., taped down to an optical table in a temperature-stabilized laboratory). This effect is particularly problematic for pole-mounted fiber. The solutions that have been developed for this problem involve a probe beam and active stabilization. Measurements on the probe beam(s) after propagating the length of the fiber make it possible to determine the relationship between the initial and final polarization states. This information is then used to drive active stabilization components that provide the adjustments necessary to align the final state with the initial state. When used to stabilize a QKD channel, these systems are typically treated as an external "add-on" technology, rather than an integral part of QKD systems. Moreover, they are designed for classical communication systems. This presents two problems for QKD applications: the classical solutions use very strong (compared to quantum) optical fields for the probes, and the fiber-based phase modulators used to correct the polarization state are often quite lossy [2]. The strong probe fields overwhelm the quantum signals so that time or spectral multiplexing techniques are needed. Time multiplexing means that system alternates between QKD and classical stabilization, bringing the risk that the channel will degrade during the QKD sequence. Spectral multiplexing is perhaps even more problematic, since the probe wavelengths are required to be quite different than the QKD wavelength in order to adequately isolate the QKD detectors from the probe light. Because the polarization effects are not independent of wavelength, this approach introduces the risk that the polarization is corrected for the probe wavelength, but not the QKD wavelength.

A potential approach, developed by Qubitekk Inc., is based on the special properties of entangled photons, namely that quantum correlations are present in all measurement bases. This is usually interpreted to mean that the two receivers, Alice and Bob, can choose any basis (e.g., horizontal/vertical or diagonal/anti-diagonal), as long as those basis choices match. The more correct interpretation is that, as long as the two receivers each use a pair of mutually unbiased bases, there exists a polarization-entangled state that will yield the correlations needed for QKD using those bases. In simpler terms: the proposed approach tailors the entangled state to the channel rather than correcting the channel for a standard quantum state. That is, the source produces exactly the state that is needed for QKD across whatever channel is presented. This solution still needs probe beams to determine the fiber properties, but instead of employing lossy modulators at the receivers to make the corrections, the information from the probe beams will be used to reconfigure the source, itself. This approach makes use of an entangled photon source that can be reconfigured to access any state in the two-photon polarization Hilbert space. The adjustments to the source can be made quickly enough to adapt to polarization changes typically seen in deployed fiber. Moreover, the reconfiguration can be done in a way that imparts lower loss if done in the source instead of in the optical fiber.

C. Multi-Party Computation

Muti-Party Computation (MPC) permits n parties to jointly evaluate a function $f(x_1, \ldots, x_n) \rightarrow (y_1, \ldots, y_n)$, in which each party $\mathcal{P}_i$ learns its output y_i without leaking its private input x_i to the other parties $\mathcal{P}_j$. There are two main techniques in MPC: garbled circuit (GC) and linear secret sharing (LSS).

GC permits efficient secure evaluation of boolean operations such as AND, OR, XOR, inequality/equality check, while LSS is efficient for arithmetic operations such as addition, multiplication. Depending on the underlying MPC schemes, the parties can share their secret input x with each other via either XOR ($x = \oplus_i x_i$), addition ($x = \sum_i x_i$), or in special forms (e.g., Yao sharings). We denote $[\![x]\!]_i$ as the share of the secret x to party $\mathcal{P}_i$ and we omit the subscript to denote the share of the secret being computed in MPC in general.

Authentication. To achieve integrity against malicious adversaries, a Message Authentication Code (MAC) can be used. There are two types of MAC: the BDOZ-style [43], which is mostly used in GC protocols with constant-round (e.g., [44]), and SPDZ-style, which is mostly used in LSS protocols [45].

[1]Here, we neglect polarization dependent loss and other nonlinear effects that are more problematic for classical fields.

[2]Low-loss fiber-based modulators are also available, but they are typically too slow for classical applications.

BDOZ-style MAC: In this style, an authenticated share of a secret x to party $\mathcal{P}_i$ is a tuple $\langle x\rangle_i = (x_i, \{m_{i,j}\}_{i\neq j}, \{k_{j,i}\}_{i\neq j})$, where $x = \oplus_i x_i$, $k_{j,i}$ is the MAC key that $\mathcal{P}_i$ uses to authenticate the share b_j of party $\mathcal{P}_j$, and $m_{i,j} = k_{i,j} \oplus b_i \cdot \Delta_j$ is the MAC of the share b_i authenticated by party $\mathcal{P}_j$ under $\mathcal{P}_j$'s global MAC key $\Delta_j \in \{0,1\}^\lambda$.

SPDZ-style MAC: In this style, an authenticated share of a secret x to party $\mathcal{P}_i$ is a tuple $\langle x\rangle_i = (x_i, y_i, \alpha_i)$ such that $x = \sum_i x_i$, $y = \sum_i y_i$, $y = \alpha \cdot x$ and $\alpha = \sum_i \alpha_i$, where $\alpha \in \mathbb{F}$ is the *global* MAC key.

Secure Operations. In MPC, all the linear computations (e.g., addition, scalar multiplication) on the authenticated shares can be performed locally. Specifically, $\langle x + y\rangle = \langle x\rangle + \langle y\rangle$ and $\langle c \cdot x\rangle = c \cdot \langle x\rangle$, where $c \in \mathbb{F}$ is a public scalar and $+, \cdot$ denote the addition and multiplication over the field $\mathbb{F}$ (note that $+, \cdot$ is equivalent to XOR and AND over $\mathbb{F}_2$).

For multiplication between shares, it can be achieved with the aid of pre-processing that generates correlated randomness such as Beaver multiplication triples $(\langle a\rangle, \langle b\rangle, \langle c\rangle)$, where $c = a \cdot b$ generated in the offline phase. Specifically, to obtain $\langle x \cdot y\rangle$ from $\langle x\rangle$ and $\langle y\rangle$, each party locally computes $\langle \epsilon\rangle = \langle x\rangle - \langle a\rangle$ and $\langle \rho\rangle = \langle y\rangle - \langle b\rangle$. All parties come together to open ϵ and ρ (only the secret, not its MAC). Finally, each party locally computes and obtains $\langle x \cdot y\rangle = \langle c\rangle + \rho \cdot \langle x\rangle + \epsilon \cdot \langle u\rangle - \epsilon \cdot \rho$.

There are several MPC protocols that offer efficiency for special situations. For example, some MPC protocols require a fixed number of parties (e.g., $n \in \{2, 3, 4\}$), some are hybrid protocols that can perform both boolean and arithmetic operations efficiently. Generally, these protocols require pre-computation to compute correlated randomness for efficient conversion between boolean and arithmetic MPC.

MPC plays an important role to transform many centralized techniques into the distributed setting, thereby avoiding single point of failure and achieving a distributed trust. For example, MPC can threshold conventional PKIs to achieve distributed PKIs. Another application of MPC is Privacy-Preserving Machine Learning, in which multiple servers can jointly train a common ML model together without leaking the data samples of individual servers. MPC is also an important building block for privacy-preserving federated learning, where secure aggregation can be performed in the distributed manner by multiple servers, thereby avoiding single-point of failure and increasing the privacy resiliency against malicious adversary.

D. Machine Learning

Machine Learning (ML) provides invaluable functionalities to realize various sophisticated expert systems ranging from healthcare [46], [47] to network security (e.g., intrusion detection, malware classification) [48]. These functionalities play a vital role in critical security systems and networking infrastructure supported by artificial intelligence. In ML-assisted applications, there are two phases: the training phase and the inference phase. The training phase focuses on building an ML model from a set of observations, while the inference phase computes an inference result for a new observation based on the model obtained in the training phase. Figure 2 presents

$\mathbf{w} \leftarrow \mathsf{LR.Train}(\{\vec{x}_i, y_i\}_{i=1}^N)$:
1: Initialize $\mathbf{w}_0 \xleftarrow{\$} \mathbb{R}^{d\times C}$, $\vec{\delta}_c \leftarrow \{0\}^d$ for each $c \in \{1, \ldots, C\}$
2: **for** $i = 1$ to T **do** ▷ T: predefined number of iterations
3: **for** $j = 1$ to N **do**
4: $\gamma_j \leftarrow \sum_{c=1}^{C} e^{\mathbf{w}_{i-1}[*,c]^\top \cdot \vec{x}_j}$
5: **for** $c = 1$ to C **do**
6: $p_{j,c} \leftarrow \frac{e^{\mathbf{w}_{i-1}[*,c]^\top \cdot \vec{x}_j}}{\gamma_j}$
7: $\vec{\delta}_c = \vec{\delta}_c + (I[y_j = c] - p_{j,c}) \cdot \vec{x}_j$ for each $c \in [C], j \in [N]$
8: $\mathbf{w}_i[*,c]^\top = \mathbf{w}_{(i-1)}[*,c]^\top + \eta \cdot \vec{\delta}_c$ for each $c \in [C]$ ▷ η : pre-defined
9: **return** $\mathbf{w}_T$

$c \leftarrow \mathsf{LR.Predict}(\vec{x}_p, \mathbf{w})$:
1: **for** $c = 1$ to C **do**
2: $p_c \leftarrow e^{\mathbf{w}[*,c]^\top \cdot \vec{x}_p}$
3: **return** c where $p_c = \max\{p_1, \ldots, p_C\}$

Fig. 2: Linear Regression Algorithm.

as an example of the training and inference protocols of the logistic regression ML algorithm. The reliability of ML systems depends on the trustworthiness of input data and reliable execution of ML algorithms under untrusted environments.

III. Proposed Vision

We propose a Multi-Party Computation Quantum Network Core (MPC-QNC) aiming to achieve two interoperable frameworks: *(i) Hybrid Distributed Quantum Public-Key Infrastructure (*HDQPKI*):* is a key distribution management system that takes advantage of the power of post-quantum cryptography, along with the recent advances in quantum technology, such as quantum key servers [3]. This can achieve flexible modes of public-key distribution with a high breach resiliency against single points of failure [13]. *(ii) Trustworthy Post-Quantum Machine Learning (*TPQ-ML*):* enhances the privacy layer of ML applications with quantum optic channels.

As shown in Figure 3, an MPC-QNC instance consists of $(n = 3)$ servers, connected via PQKD optic networks which itself offer quantum safety. During the set-up, a master secret key msk is secretly shared among different parties. Note that this setting offers a breach resiliency of t-out-of-n servers. Unlike commonly deployed PKI servers, our framework offers more immunity against rogue-PKI attacks. Indeed, one has to break at least t servers to compromise the system. Moreover, our framework distributes trust among multiple entities, offering improved service and robustness to its users.

In the following, we first describe the infrastructure aspects of our envisioned MPC-QNC framework, in which we synergize various architectural and hardware components to permit an accelerated and secure distributed computation. We then present our HDQPKI framework that utilizes MPC-QNC to develop practical, low-cost, and resilient quantum-safe CA services. Finally, we give our TPQ-ML framework that harness MPC-QNC to offer privacy-preserving ML services with post-quantum security and breach-resiliency.

[3]https://qubitekk.com/products/qkd-for-industrial-control-systems-ics/

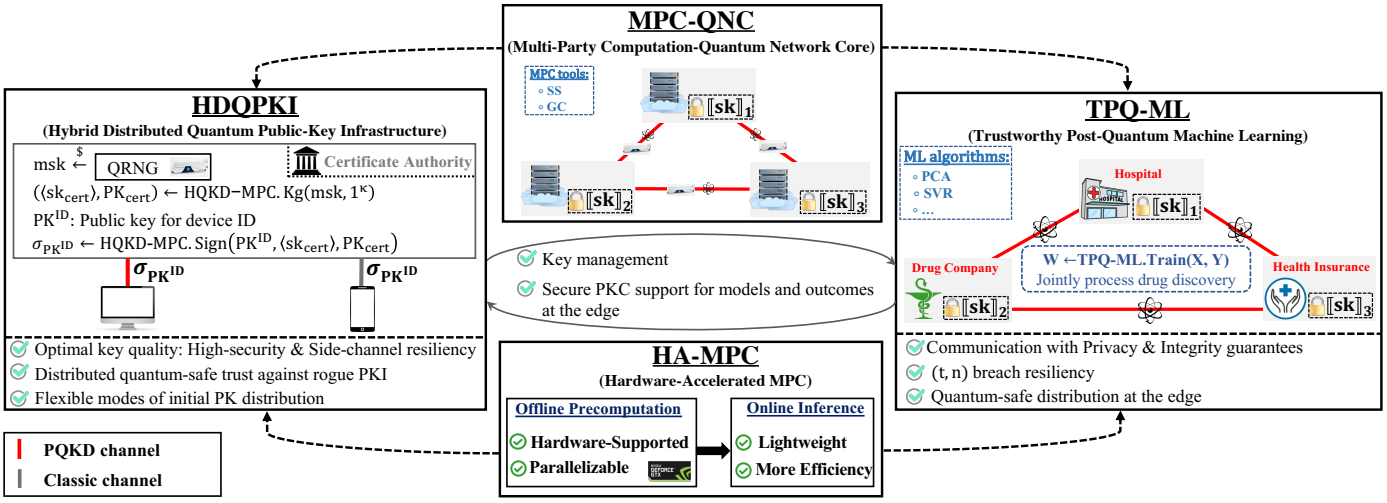

Fig. 3: High-level Description of Our Proposed MPC-QNC Infrastructure and Framework.

A. MPC-QNC- *Infrastructure for Lightning* MPC

Given that MPC will serve as an important building block for threshold cryptography and distributed computation with provable security in the long-term, we envision building dedicated infrastructure and facilities to optimize certain phases of MPC regarding the importance of making it more practical. As briefly outlined in II-C, efficient state-of-the-art MPC techniques generally follow the online/offline model, where the offline phase generates data-independent materials (e.g., correlated randomnesses) to be used in the online evaluation that incurs input-dependent computations (e.g., signature generation on the input message, ML computation over training/testing data). We envision two approaches that can be useful to improve the overall performance of MPC as follows.

•*Pre-computation of independent/correlated randomness via hardware acceleration:* Offline computation is generally costly as it harnesses computationally expensive cryptographic protocols such as homomorphic encryption, and oblivious transfer. Given that the goal of the offline phase is to generate a set of independently correlated randomnesses, such computation can be accelerated by deploying special hardware that offers high parallelism such as GPU [49], FPGA [50] or even TEE [51]. Several academic works have shown that these hardware techniques are useful to generate sufficient randomnesses being supplied for the online evaluation [52].

• *Improve communication efficiency in the online phase via pairwise secure optical network*: For MPC online phase, the most expensive cost stems from the network cost, while the computation is generally inexpensive. For example, in boolean MPC techniques, they require to transfer garbled table from the garbler party to the evaluator party at the beginning of online phase for secure evaluation. Since the size of the garbled table is equal to the size of the entire circuit for the program to be evaluated, it incurs a high bandwidth overhead especially when the garbled table is authenticated, where each bit is attached with a λ-bit MAC. On the other hand, in arithmetic MPC techniques (e.g.,), the parties need to interact with each other in a communication round to evaluate a multiplication. Given that the evaluated program has high multiplication depth, it incurs high network latency as the number of communication rounds depends on the depth of the multiplication in the evaluated program. Therefore, to improve the online phase, we believe that having a dedicated optical network that offers low latency, high bandwidth, and integrity guarantees against threats will be of great benefit. PQKD infrastructures not only offer fast communication via optical networks, but also an inherently secure pairwise connection among the servers. In classical settings, this has been achieved via key pre-distributions or with conventional cryptography. Here, the native offers a fast and secure pairwise connection which is an ideal setup to offer our envisioned MPC operations.

In the following, we propose two frameworks that can be built on top of MPC-QNC infrastructure including Hybrid Distributed Post-Quantum PKI (HDQPKI) and Trustworthy Post-Quantum ML (TPQ-ML). Note that these platforms are not the only ones that receive great benefits from MPC-QNC, but also other frameworks that harness MPC as the main building block such as privacy-preserving data storage and sharing [53]–[56] schemes as well as encrypted query platforms [57], [58] with meta-data privacy.

B. Hybrid Distributed Post-Quantum Public-Key Infrastructure

PKIs form the backbone of foundational cryptographic services in modern networked systems. Specifically, PKIs ensure the authenticity of public keys, thereby providing scalable authentication for large-scale networks via public key certificates [59]. Through Certificate Authorities (CAs) in PKIs, the cryptographic key distribution, exchange, public key encryption, and digital signatures services can be offered reliably.

The long-term trustworthiness of next-generation networked systems requires post-quantum security. Therefore, it is of paramount importance to ensure that *PKI systems are Quantum-*

safe . In addition to post-quantum security, as discussed before, PKIs have been a prime target due to their key role as CA. A vulnerable CA may lead root certificates to be compromised, thereby creating a severe disruption of the underlying applications [60]. Hence, it is necessary to ensure CAs are not only post-quantum secure but also offer breach resiliency via distributed cyber-infrastructure that is an integral part of modern networked architectures. Moreover, a relevant limitation of centralized PKIs is that the users must inherently trust a few CAs for their security. The distribution of trust among CAs ensure more trustworthy and reliable services for the user, thereby enhancing the overall functionality of PKIs.

In this section, towards addressing these limitations, we instantiate our MPC-QNC to raise a Hybrid Distributed Quantum Public-Key Infrastructures (HDQPKI) that enable a scalable, low-cost, and resilient cyber-infrastructure for public key distribution, and digital certificates alike.

Our HDQPKI has two major elements: (i) A Hybrid Quantum Key Distribution (HQKD) framework that harnesses the best of both NIST and PQKD schemes to offer trustworthy CA services. HQKD harnesses both Quantum Random Number Generators (QRNGs) and various public key distribution options to enable quantum safety. (ii) A threshold computation of key and signature generation algorithms of the selected post-quantum secure cryptographic schemes. That is, we use our MPC-QNC framework to generate private/public key pairs derived from QRNGs and certificates via threshold NIST PQC schemes. In tandem, these approaches ensure the high quality of randomness, safe initial public key distribution, and breach-resilient computation of cryptographic keys. Below, we first outline HQKD followed by its thresholding via MPC.

1) HQKD *Components:* In Figure 4, we showcase an example of our HQKD components and workflow, which is based on the framework in [61].

HQKD combines the strengths of PQKD and NIST PQC schemes, which can enable low-cost yet quantum-secure key distribution with high scalability. During the offline CA phase, HQKD bootstrap PKIs via Quantum Random Number Generators (QRNG)s. For example, this can be achieved via Qubitekk's 810nm Quantum Key DataLocTM Server, which utilizes a variation of the BBM92 protocol [62] to generate the entangled photons. They are then used to produce random numbers and symmetric keys (e.g., AES-256). This strategy ensures a high-quality randomness for the master private/public keys $(\mathsf{sk}_{\text{cert}}, \mathsf{pk}_{\text{cert}})$, thereby increases their side-channel attack resiliency. The periodic re-generation of high-quality randomness also offers key freshness and forward-secrecy.

As depicted in 4, we choose Dilithium [63] as a digital signature for the certification of users' public keys. Indeed, our analysis indicates that the lattice-based signatures are the most suitable alternatives, as discussed in Section II-A. In our framework, we opted for a threshold-variant of Dilithium via MPC as it will be detailed in Section III-B2. The first phase is the key generation. As recently discussed, our differentiating factor is the use of PQKD devices to generate a high-quality of true

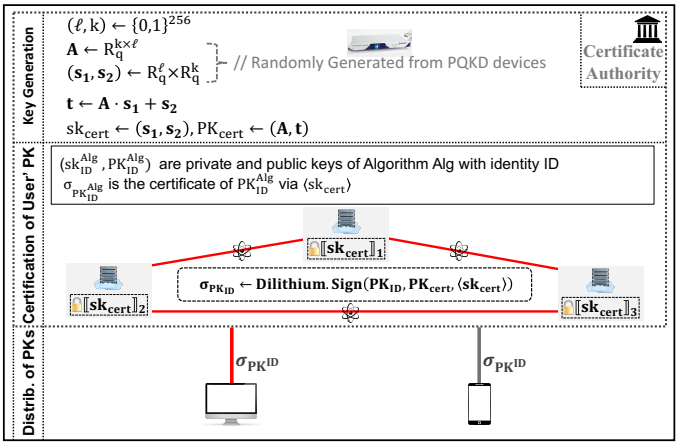

Fig. 4: An Example Flow of HQKD Framework with Dilithium.

randomness for the CA private/public keys. After the selection of system-wide parameters (i.e., (l, k)), the QRNG generate a $l \times k$ public matrix $\mathbf{A}$ and a couple of two private error vectors $(\mathbf{s_1}, \mathbf{s_2})$. For the full key generation algorithm, we refer to [14]. We formally describe the Dilithium signature generation algorithm in Figure 5 for a better depiction of its threshold-variant. In the following, we will demonstrate how we achieve a distributed (threshold) version of our HQKD framework.

$(\sigma) \leftarrow \mathsf{Dilithium.Sign}(m, \mathsf{pk}, \mathsf{sk})$

1: Parse sk as $\mathsf{sk} = (\mathbf{s_1}, \mathbf{s_2})$, where $\mathbf{s_1} \in R_q^l$, $\mathbf{s_2} \in R_q^r$
2: Parse pk as $\mathsf{pk} = (\mathbf{A}, \mathbf{t})$, where $\mathbf{A} \in R_q^{k \times l}$, $t \in R_q^k$
3: $\mathbf{z} \leftarrow \perp$
4: **while** $\mathbf{z} = \perp$ **do**
5: Sample a short vector $\mathbf{y} \in R_q^l$ with $||\mathbf{y}||_\infty \leq \gamma_1$
6: $\mathbf{v} \leftarrow \mathbf{A} \times \mathbf{y} \in R_q^l$
7: $\mathbf{w} = (w_1, \ldots, w_k) \leftarrow \mathsf{ExtractMSB}(\mathbf{v}, k)$
8: $c \leftarrow \mathsf{Hash}(m||\mathbf{w}) \in R_q$
9: $\mathbf{z} \leftarrow \mathbf{y} + c \cdot \mathbf{s}_1 \in R_q^l$
10: $\hat{b} \leftarrow \mathsf{IsLessThan}(\mathbf{z}, \tau)$
11: $\mathbf{x}' \leftarrow \mathbf{v} - c \cdot \mathbf{s}_2$
12: $(x'_1, \ldots, x'_k) \leftarrow \mathsf{ExtractLSB}(\mathbf{x}', k)$
13: **for** $i = 1$ to k **do**
14: $b'_i \leftarrow \mathsf{IsLessThan}(x'_i, \tau)$
15: $b \leftarrow \hat{b} \oplus b'_1 \oplus \cdots \oplus b'_k$
16: **if** $b = 0$ **then**
17: $\mathbf{z} \leftarrow \perp$
18: **return** $\sigma \leftarrow (\mathbf{z}, c)$

Fig. 5: Dilithium Signature Algorithm.

2) Hybrid Distributed Post-quantum PKI via MPC-QNC: Figure 6 presents our idea of thresholding the post-quantum Dilithium signature algorithm using MPC. We can see that to sign a message with Dilithium under distributed setting, it requires MPC arithmetic operation including addition $\boxplus$ and share multiplication $\boxtimes$ (steps 6, 9, 11) as well as boolean operations including bit extraction ExtractMSB, ExtractLSB, comparison IsLessThan, and XOR computation $\oplus$ (e.g., steps 7, 10, 12, 14). While boolean operations can be realized efficiently using GC techniques (e.g., [44], [64]), arithmetic operations can be performed with additive secret sharing techniques (e.g., [45], [65]). These two techniques can receive a great benefit in the online evaluation phase by having an optic network

$(\sigma) \leftarrow \mathsf{Dilithium.Sign}(m, \mathsf{pk}, \langle \mathsf{sk} \rangle)$

1: Parse $\langle \mathsf{sk} \rangle$ as $\langle \mathsf{sk} \rangle = (\langle \mathbf{s}_1 \rangle, \langle \mathbf{s}_2 \rangle)$, where $\langle \mathbf{s}_1 \rangle \in R_q^l$, $\langle \mathbf{s_2} \rangle \in R_q^r$
2: Parse pk as $\mathsf{pk} = (\mathbf{A}, \mathbf{t})$, where $\mathbf{A} \in R_q^{k \times l}$, $\mathbf{t} \in R_q^k$
3: $\langle \mathbf{z} \rangle \leftarrow \perp$
4: **while** $\langle \mathbf{z} \rangle = \perp$ **do**
5: Sample a short vector $\langle \mathbf{y} \rangle \in R_q^l$ with $||\mathbf{y}||_\infty \leq \gamma_1$
6: $\langle \mathbf{v} \rangle \leftarrow \mathbf{A} \times \langle \mathbf{y} \rangle \in R_q^l$
7: $\langle \mathbf{w} \rangle = (\langle w_1 \rangle, \ldots, \langle w_k \rangle) \leftarrow \mathsf{MPC.ExtractMSB}(\langle \mathbf{x}' \rangle, k)$
8: $\langle c \rangle \leftarrow \langle \mathsf{Hash} \rangle (m || \langle \mathbf{w} \rangle) \in R_q$
9: $\langle \mathbf{z} \rangle \leftarrow \langle \mathbf{y} \rangle + \langle c \rangle \boxtimes \langle \mathbf{s}_1 \rangle \in R_q^l$
10: $\langle \hat{b} \rangle \leftarrow \mathsf{MPC.IsLessThan}(\langle \mathbf{z} \rangle, \tau)$
11: $\langle \mathbf{x}' \rangle \leftarrow \langle \mathbf{v} \rangle - \langle c \rangle \boxtimes \langle \mathbf{s}_2 \rangle$
12: $(\langle x'_1 \rangle, \ldots, \langle x'_k \rangle) \leftarrow \mathsf{MPC.ExtractLSB}(\langle \mathbf{x}' \rangle, k)$
13: **for** $i = 1$ to k **do**
14: $\langle b'_i \rangle \leftarrow \mathsf{MPC.IsLessThan}(\langle x'_i \rangle, \tau)$
15: $\langle b \rangle \leftarrow \langle \hat{b} \rangle \oplus \langle b'_1 \rangle \oplus \cdots \oplus \langle b'_k \rangle$
16: $b \leftarrow \mathsf{MPC.Open}(\langle b \rangle)$
17: **if** $b = 0$ **then**
18: $\langle \mathbf{z} \rangle \leftarrow \perp$
19: **return** $\sigma \leftarrow (\langle \mathbf{z} \rangle, \langle c \rangle)$

Fig. 6: Threshold Dilithium Signature with MPC.

infrastructure to reduce network overhead burden (bandwidth, round-trip latency) as discussed in III-B.

We can see that the algorithm requires converting boolean MPC and arithmetic MPC (e.g., from step 11 to step 12). This conversion can be done effectively by using authenticated shares of the same random bits (e.g., daBit [66]) on both $\mathbb{F}_2$ and $\mathbb{F}_p$ in the precomputation phase. Given that the offline phase can be optimized with hardware acceleration techniques (e.g., GPU, FGPA), it will supply sufficient correlated random bits for efficient conversion during the online signature generation.

Other Instantiations with Alternative Signature Schemes: We focused on NIST PQC standards in our analysis, and opted for Dilithium over Falcon due to its computational efficiency. However, Falcon is also a potentially suitable alternative for thresholding. However, thresholding SPHINCS+ incurs significant overhead. For example, the threshold-based SPHINCS+ requires thousands of hash calls to execute a single signature generation. The signing time becomes in the order of 100 minutes with state-of-the-art GC implementations [32].

One can employ post-quantum signatures with advanced security properties (e.g., forward security, tag aggregation). For instance, ANT [67] is a lattice-based signature scheme offering forward-security and optimal signature generation, at the cost of a slow signature verification due to the reliance on a set of non-colluding distributed servers. We also expect generic post-quantum forward-secure signatures [68] to receive benefit from our framework. Dilithium variants with faster verification [69] are another suitable alternatives for instantiations. Moreover, signature aggregation is also important for an efficient authentication of massive streams from multiple entities (e.g., IoT). FAAS [70] is a generic algorithm that enables fast signing of any aggregate signature (e.g., NTRU [26]). Finally, one can fuse the aforementioned cryptographic mechanisms with physical-layer security to construct robust key agreement protocols [71].

C. Safe Distribution of Certificates

Initial Distribution via PQKD*:* In the case PQKD is available, this is an ideal way to distribute the quantum-safe certificates. This mode can be useful when high-end devices such as servers and edge-cloud components are directly connected to the PKI core via PQKD. For instance, the certificate (chains) can be carried through PQKD networks connecting high-end devices as further in the network as possible. When the certificates reach a component without PQKD infrastructure, then one can follow the below approach.

Distribution via NIST PQC Schemes: This approach is akin to the current conventional secure PKIs, wherein the certificates are distributed to the users via a certificate chain. For example, consider a smart-grid application, smart-meters are provisioned along with their certificates via wireless connection (e.g., with a handheld device on the field). This can be achieved by establishing a secure channel via NIST PQC signature and KEM standards as in [61]. Any NIST PQC signature, that is suitable for the system attributes, can be used for this purpose.

D. Trustworthy Post-Quantum Machine Learning (TPQ-ML)

In Figure 7, we present a concrete example of an ML algorithm (i.e., linear regression) that can be performed in a distributed manner using MPC techniques to improve breach resiliency (non-single point of failure), privacy (collusion) and post-quantum security. We can see that most the operation in the training phase can be realized solely of arithmetic MPC as it only incurs addition $\boxplus$, multiplication $\boxtimes$ and exponentiation exp operations (step 10). Thus, having good pre-computation phase to generate Beaver arithmetic multiplication triples will be of great benefit to the online evaluation of ML training. On the other hand, the inference phase incurs mostly boolean operations (comparison) (i.e., isEqual, isGreaterThan, Select) to obtain the final inference class that the data sample has the highest probability of belonging to among all possible classes. This can be done efficiently by generating Beaver boolean multiplication triples via hardware acceleration techniques and optical network to reduce the transmission latency of transmitting the garbled table at the beginning of the online evaluation.

IV. Conclusion

In this paper, we proposed a cryptographic architecture and framework to usher trustworthy distributed cyber-infrastructures in the post-quantum era. We aim to mitigate the resiliency and long-term security challenges in cyber-infrastructures and AI/ML applications that stem from the centrality and threat of emerging quantum computers. The key element of our design is *Multi-Party Computation Quantum Network Core* (MPC-QNC) that harnesses the quantum-safe pairwise optical infrastructures, QRNGs, and hardware-acceleration (e.g., GPUs) to enhance the online and offline phase of MPC protocols, respectively. We outline a hybrid distributed quantum-safe PKI (HDQPKI) that thresholds a NIST PQC standard signature via MPC-QNC. HDQPKI offers the best of PQKD and NIST PQC standards for post-quantum security, while also providing breach-resiliency against active adversaries. Finally, we discuss TPQ-ML that exemplifies a privacy-preserving execution of ML algorithms

$(\perp; \langle \mathbf{w} \rangle_1, \ldots, \langle \mathbf{w} \rangle_n) \leftarrow \mathsf{DLR.Train}(\{\vec{x}_i, y_i\}_{i=1}^N; \perp)$:

$\vec{x}'_i \leftarrow \mathsf{MPC.Encode}(\vec{x}_i)$

Set $\vec{I} \leftarrow \{0\}^C$, set $\vec{I}[y_i] \leftarrow 1$ for each $i \in \{1, \ldots, N\}$

for $i = 1 \ldots N$ **do**

  $\langle \vec{x'_i} \rangle_1, \ldots, \langle \vec{x'_i} \rangle_n \leftarrow \mathsf{MPC.Share}(\vec{x'_i})$

  $\langle \vec{I_i} \rangle_1, \ldots, \langle \vec{I_i} \rangle_n \leftarrow \mathsf{MPC.Share}(\vec{I_i})$

Init $\langle \mathbf{w}_0 \rangle \xleftarrow{\$} \mathbb{F}^{d \times C}$ and $\langle \vec{\delta_c} \rangle \leftarrow \{0\}^d$ for each $c \in [C]$

for $i = 1$ to T **do** ▷ T: Predifined number of iterations

  for $j = 1$ to N **do**

    for $c = 1$ to C **do** ▷ T: Number of classes

      $\langle \lambda_{j,c} \rangle \leftarrow \langle \mathsf{exp} \rangle (e, \langle \mathbf{w}_{i-1}[*, c]^\top \rangle \boxtimes \langle \vec{x}_j \rangle_l)$

      $\langle \gamma_j \rangle \leftarrow \langle \gamma_j \rangle \boxplus \langle \lambda_{j,c} \rangle$

    $\langle p_{j,c} \rangle \leftarrow \langle \lambda_{j,c} \rangle \boxtimes \langle \gamma_j \rangle^{-1}$ for each $c \in [C]$

  for $c = 1$ to C, $j = 1$ to N **do**

    $\langle I_{j,c} \rangle \leftarrow \mathsf{MPC.isEqual}(\langle y \rangle_j, c)$

    $\langle \vec{\delta_c} \rangle = \langle \vec{\delta_c} \rangle \boxplus ((\langle I_{j,c} \rangle - \langle p_{j,c} \rangle) \boxtimes \langle \vec{x}_j \rangle)$

  $\langle \mathbf{w}_i[*, c]^\top \rangle = \langle \mathbf{w}_{(i-1)}[*, c]^\top \rangle \boxplus (\eta \boxdot \langle \vec{\delta_c} \rangle)$ for each $c \in [C]$

$(y; \perp) \leftarrow \mathsf{DLR.Inference}(\vec{x}_p; \langle \mathbf{w} \rangle_1, \ldots, \langle \mathbf{w}_n \rangle)$:

$\vec{x}'_p \leftarrow \mathsf{Encode}(\vec{x}_p)$

$(\langle \vec{x}_p \rangle_1, \ldots, \langle \vec{x}_p \rangle_n) \leftarrow \mathsf{MPC.Share}(\vec{x}_p)$

$\langle p \rangle \leftarrow -\infty$, $\langle y \rangle \leftarrow -\infty$

for $c = 1$ to C **do**

  $\langle p_c \rangle \leftarrow \langle \mathsf{exp} \rangle (e, \langle \mathbf{w}[*, c]^\top \rangle \boxtimes \langle \vec{x}_p \rangle)$

  $\langle b \rangle \leftarrow \mathsf{MPC.isGreaterThan}(\langle p_c \rangle, \langle p \rangle)$

  $\langle y \rangle \leftarrow \mathsf{MPC.Select}(\langle b \rangle, \langle y \rangle, \langle c \rangle)$

$y \leftarrow \mathsf{MPC.Open}(\langle y \rangle)$

return (y)

Fig. 7: Distributed multinomial logistic regression with MPC.

over MPC-QNC, thereby enabling distributed trust and post-quantum security simultaneously. Our proposed framework is expected to offer new architectural elements and cryptographic tool sets for domain experts to design their cyber-security solutions while inspiring practitioners to develop trustworthy applications for cyber-infrastructures in the post-quantum era.

ACKNOWLEDGMENTS

Dr. Attila A. Yavuz is supported by the unrestricted gift from the Cisco Research Award (220159), and the NSF CAREER Award CNS-1917627. Dr. Thang Hoang is supported by an unrestricted gift from Robert Bosch, and the Commonwealth Cyber Initiative (CCI), an investment in the advancement of cyber R&D, innovation, and workforce development. For more information about CCI, visit www.cyberinitiative.org. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation and the Commonwealth Cyber Initiative.

REFERENCES

[1] Statista, "Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025," https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide, accessed: Oct 10, 2022.

[2] P. K. Verma, R. Verma, A. Prakash, A. Agrawal, K. Naik, R. Tripathi, M. Alsabaan, T. Khalifa, T. Abdelkader, and A. Abogharaf, "Machine-to-Machine (M2M) communications: A survey," *Journal of Network and Computer Applications*, vol. 66, pp. 83–105, 2016.

[3] M. S. Mahdavinejad, M. Rezvan, M. Barekatain, P. Adibi, P. Barnaghi, and A. P. Sheth, "Machine learning for Internet of Things data analysis: A survey," *Digital Communications and Networks*, vol. 4, no. 3, pp. 161–175, 2018.

[4] A. Uprety and D. B. Rawat, "Reinforcement learning for IoT security: A comprehensive survey," *IEEE Internet of Things Journal*, vol. 8, no. 11, pp. 8693–8706, 2020.

[5] S. Khanam, I. B. Ahmedy, M. Y. I. Idris, M. H. Jaward, and A. Q. B. M. Sabri, "A survey of security challenges, attacks taxonomy and advanced countermeasures in the internet of things," *IEEE access*, vol. 8, pp. 219 709–219 743, 2020.

[6] C. Zhao, S. Zhao, M. Zhao, Z. Chen, C.-Z. Gao, H. Li, and Y.-a. Tan, "Secure multi-party computation: theory, practice and applications," *Information Sciences*, vol. 476, pp. 357–372, 2019.

[7] L. Brandao, M. Davidson, A. Vassilev *et al.*, "NIST roadmap toward criteria for threshold schemes for cryptographic primitives," *National Institute of Standards and Technology, Tech. Rep*, 2020.

[8] C. Dong, J. Weng, J.-N. Liu, A. Yang, L. Zhiquan, Y. Yang, and J. Ma, "Maliciously secure and efficient large-scale genome-wide association study with multi-party computation," *IEEE Transactions on Dependable and Secure Computing*, 2022.

[9] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM review*, vol. 41, no. 2, pp. 303–332, 1999.

[10] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[11] R. De Wolf, "The potential impact of quantum computers on society," *Ethics and Information Technology*, vol. 19, no. 4, pp. 271–276, 2017.

[12] G. Alagic, D. Apon, D. Cooper, Q. Dang, T. Dang, J. Kelsey, J. Lichtinger, C. Miller, D. Moody, R. Peralta *et al.*, "Status report on the third round of the NIST post-quantum cryptography standardization process," *National Institute of Standards and Technology, Gaithersburg*, 2022.

[13] N. Serrano, H. Hadan, and L. J. Camp, "A complete study of PKI (PKI's Known Incidents)," in *TPRC47: The 47th Research Conference on Communication, Information and Internet Policy*, 2019.

[14] L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, P. Schwabe, G. Seiler, and D. Stehlé, "Crystals-dilithium: A lattice-based digital signature scheme," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pp. 238–268, 2018.

[15] P.-A. Fouque, J. Hoffstein, P. Kirchner, V. Lyubashevsky, T. Pornin, T. Prest, T. Ricosset, G. Seiler, W. Whyte, and Z. Zhang, "Falcon: Fast-fourier lattice-based compact signatures over NTRU," *Submission to the NIST's post-quantum cryptography standardization*, vol. 36, no. 5, 2018.

[16] D. J. Bernstein, A. Hülsing, S. Kölbl, R. Niederhagen, J. Rijneveld, and P. Schwabe, "The SPHINCS+ signature framework," in *Proceedings of the 2019 ACM SIGSAC conference on computer and communications security*, 2019, pp. 2129–2146.

[17] J. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J. M. Schanck, P. Schwabe, G. Seiler, and D. Stehlé, "CRYSTALS-Kyber: a CCA-secure module-lattice-based KEM," in *2018 IEEE European Symposium on Security and Privacy (EuroS&P)*. IEEE, 2018, pp. 353–367.

[18] NIST, "Round 4 Submissions in Post-Quantum Cryptography (PQC)," https://csrc.nist.gov/Projects/post-quantum-cryptography/round-4-submissions, accessed: Oct 29, 2022.

[19] A. Langlois and D. Stehlé, "Worst-case to average-case reductions for module lattices," *Designs, Codes and Cryptography*, vol. 75, no. 3, pp. 565–599, 2015.

[20] E. Fujisaki and T. Okamoto, "Secure integration of asymmetric and symmetric encryption schemes," in *Annual international cryptology conference*. Springer, 1999, pp. 537–554.

[21] D. Micciancio and C. Peikert, "Hardness of SIS and LWE with small parameters," in *Annual Cryptology Conference*, 2013, pp. 21–39.

[22] V. Lyubashevsky, "Fiat-shamir with aborts: Applications to lattice and factoring-based signatures," in *International Conf on the Theory and Application of Cryptology and Information Security*, 2009, pp. 598–616.

[23] T. Espitau, P.-A. Fouque, B. Gérard, and M. Tibouchi, "Side-channel attacks on bliss lattice-based signatures: Exploiting branch tracing against strongswan and electromagnetic emanations in microcontrollers," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, 2017, pp. 1857–1874.

[24] M. Tibouchi and A. Wallet, "One bit is all it takes: a devastating timing attack on BLISS's non-constant time sign flips," *Journal of Mathematical Cryptology*, vol. 15, no. 1, pp. 131–142, 2021.

[25] C. Gentry, C. Peikert, and V. Vaikuntanathan, "Trapdoors for hard lattices and new cryptographic constructions," in *Proceedings of the fortieth annual ACM symposium on Theory of computing*, 2008, pp. 197–206.

[26] J. Hoffstein, J. Pipher, and J. H. Silverman, "NTRU: A ring-based public key cryptosystem," in *International algorithmic number theory symposium*. Springer, 1998, pp. 267–288.

[27] L. Ducas and T. Prest, "Fast fourier orthogonalization," in *Proceedings of the ACM on International Symposium on Symbolic and Algebraic Computation*, 2016, pp. 191–198.

[28] H. Nejatollahi, N. Dutt, S. Ray, F. Regazzoni, I. Banerjee, and R. Cammarota, "Post-quantum lattice-based cryptography implementations: A survey," *ACM Computing Surveys (CSUR)*, vol. 51, no. 6, pp. 1–41, 2019.

[29] A. Hülsing, "W-OTS+–shorter signatures for hash-based signature schemes," in *Intern. Conf on Cryptology in Africa*, 2013, pp. 173–188.

[30] O. Goldreich, "Two remarks concerning the Goldwasser-Micali-Rivest signature scheme," in *Conference on the Theory and Application of Cryptographic Techniques*. Springer, 1986, pp. 104–110.

[31] R. J. McEliece, "A public-key cryptosystem based on algebraic," *Coding Thv*, vol. 4244, pp. 114–116, 1978.

[32] D. Cozzo and N. P. Smart, "Sharing the LUOV: Threshold Post-Quantum Signatures," in *IMA International Conference on Cryptography and Coding*, 2019, pp. 128–153.

[33] J. Ding and D. Schmidt, "Rainbow, a new multivariable polynomial signature scheme," in *International conference on applied cryptography and network security*, 2005, pp. 164–175.

[34] A. Kipnis, J. Patarin, and L. Goubin, "Unbalanced oil and vinegar signature schemes," in *International Conference on the Theory and Applications of Cryptographic Techniques*, 1999, pp. 206–222.

[35] D. Jao and L. D. Feo, "Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies," in *International Workshop on Post-Quantum Cryptography*. Springer, 2011, pp. 19–34.

[36] W. Castryck, T. Lange, C. Martindale, L. Panny, and J. Renes, "CSIDH: an efficient post-quantum commutative group action," in *International Conference on the Theory and Application of Cryptology and Information Security*. Springer, 2018, pp. 395–427.

[37] W. Castryck and T. Decru, "An efficient key recovery attack on SIDH (preliminary version)," *Cryptology ePrint Archive*, 2022.

[38] D. Jao, R. Azarderakhsh, M. Campagna, C. Costello, L. De Feo, B. Hess, A. Jalili, B. Koziel, B. LaMacchia, P. Longa *et al.*, "SIKE: Supersingular isogeny key encapsulation," *HAL*, vol. 2017, 2017.

[39] L. De Feo, D. Kohel, A. Leroux, C. Petit, and B. Wesolowski, "SQISign: compact post-quantum signatures from quaternions and isogenies," in *International Conference on the Theory and Application of Cryptology and Information Security*. Springer, 2020, pp. 64–93.

[40] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *arXiv preprint arXiv:2003.06557*, 2020.

[41] C. H. Bennett, G. Brassard, and N. D. Mermin, "Quantum cryptography without Bell's theorem," *Physical review letters*, vol. 68, no. 5, p. 557, 1992.

[42] H.-K. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution," *Physical review letters*, vol. 94, no. 23, p. 230504, 2005.

[43] R. Bendlin, I. Damgård, C. Orlandi, and S. Zakarias, "Semi-homomorphic encryption and multiparty computation," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 2011, pp. 169–188.

[44] X. Wang, S. Ranellucci, and J. Katz, "Authenticated garbling and efficient maliciously secure two-party computation," in *Proceedings of the 2017 ACM SIGSAC conference on computer and communications security*, 2017, pp. 21–37.

[45] I. Damgård, V. Pastro, N. Smart, and S. Zakarias, "Multiparty computation from somewhat homomorphic encryption," in *Annual Cryptology Conference*. Springer, 2012, pp. 643–662.

[46] "Doctor, meet your next consult: The AI diagnosis," Available at https://www.cisco.com/c/en/us/solutions/industries/healthcare/gartner-on-ai-diagnosis.html.

[47] "The future of healthcare," Available at https://blogs.cisco.com/healthcare/the-future-of-healthcare.

[48] "What is machine learning in security?" Available at https://www.cisco.com/c/en/us/products/security/machine-learning-security.html#~how-ml-helps-security.

[49] B. Knott, S. Venkataraman, A. Hannun, S. Sengupta, M. Ibrahim, and L. van der Maaten, "Crypten: Secure multi-party computation meets machine learning," *Advances in Neural Information Processing Systems*, vol. 34, pp. 4961–4973, 2021.

[50] X. Zhou, Z. Xu, C. Wang, and M. Gao, "PPMLAC: high performance chipset architecture for secure multi-party computation," in *Proc of the 49th Annual Inter. Symp on Computer Architecture*, 2022, pp. 87–101.

[51] R. Bahmani, M. Barbosa, F. Brasser, B. Portela, A.-R. Sadeghi, G. Scerri, and B. Warinschi, "Secure multiparty computation from SGX," in *Inter. Conf. on Financial Cryptography and Data Security*, 2017, pp. 477–497.

[52] I. Oleynikov, E. Pagnin, and A. Sabelfeld, "Outsourcing MPC Precomputation for Location Privacy," in *2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 2022, pp. 504–513.

[53] W. Chen, T. Hoang, J. Guajardo, and A. A. Yavuz, "Titanium: A metadata-hiding file-sharing system with malicious security," in *28th Annual Network and Distributed System Security Symposium)*, 2022.

[54] T. Hoang, C. D. Ozkaptan, A. A. Yavuz, J. Guajardo, and T. Nguyen, "S3oram: A computation-efficient and constant client bandwidth blowup oram with shamir secret sharing," in *Proc of the 2017 ACM SIGSAC Conf on Computer and Communications Security*, 2017, pp. 491–505.

[55] T. Hoang, J. Guajardo, and A. A. Yavuz, "Macao: A maliciously-secure and client-efficient active oram framework," in *27th Annual Network and Distributed System Security Symposium (NDSS)*, 2020.

[56] T. Hoang, A. A. Yavuz, and J. Guajardo, "A multi-server oram framework with constant client bandwidth blowup," *ACM Transactions on Privacy and Security (TOPS)*, vol. 23, no. 1, pp. 1–35, 2020.

[57] T. Hoang, A. A. Yavuz, F. B. Durak, and J. Guajardo, "Oblivious dynamic searchable encryption on distributed cloud systems," in *IFIP Annual Conf on Data and Applications Security and Privacy*, 2018, pp. 113–130.

[58] ——, "A multi-server oblivious dynamic searchable encryption framework," *Journal of Computer Security*, vol. 27, no. 6, pp. 649–676, 2019.

[59] R. Housley, W. Ford, W. Polk, and D. Solo, "Internet x. 509 public key infrastructure certificate and crl profile," Tech. Rep., 1999.

[60] Z. Dong, K. Kane, and L. J. Camp, "Detection of rogue certificates from trusted certificate authorities using deep neural networks," *ACM Trans on Privacy and Security (TOPS)*, vol. 19, no. 2, pp. 1–31, 2016.

[61] A. A. Yavuz, D. Earl, S. Packard, and S. E. Nouma, "Hybrid low-cost quantum-safe key distribution," in *Quantum 2.0*. Optica Publishing Group, 2022, pp. QTu4C–5.

[62] A. K. Ekert, "Quantum Cryptography and Bell's Theorem," in *Quantum Measurements in Optics*. Springer, 1992, pp. 413–418.

[63] L. Ducas, A. Durmus, T. Lepoint, and V. Lyubashevsky, "Lattice signatures and bimodal gaussians," in *Annual Cryptology Conference*. Springer, 2013, pp. 40–56.

[64] M. Bellare, V. T. Hoang, and P. Rogaway, "Foundations of garbled circuits," in *Proceedings of the 2012 ACM conference on Computer and communications security*, 2012, pp. 784–796.

[65] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[66] A. Aly, E. Orsini, D. Rotaru, N. P. Smart, and T. Wood, "Zaphod: efficiently combining lsss and garbled circuits in scale," in *Proceedings of the 7th ACM Workshop on Encrypted Computing & Applied Homomorphic Cryptography*, 2019, pp. 33–44.

[67] R. Behnia and A. A. Yavuz, *Towards Practical Post-Quantum Signatures for Resource-Limited Internet of Things*. New York, NY, USA: Association for Computing Machinery, 2021, p. 119–130.

[68] A. A. Yavuz and R. Behnia, "FROG: Forward-Secure Post-Quantum Signature," *arXiv preprint arXiv:2205.07112*, 2022.

[69] R. Behnia, M. O. Ozmen, A. A. Yavuz, and M. Rosulek, "Tachyon: Fast signatures from compact knapsack," in *ACM SIGSAC Conference on Computer and Communications Security*, 2018, pp. 1855–1867.

[70] M. O. Ozmen, R. Behnia, and A. A. Yavuz, "Fast authentication from aggregate signatures with improved security," in *International Conference on Financial Cryptography and Data Security*, 2019, pp. 686–705.

[71] Y. Qassim, M. E. Magaña, and A. A. Yavuz, "Post-quantum hybrid security mechanism for MIMO systems," in *International Conf on Computing, Networking and Communications (ICNC)*, 2017, pp. 684–689.