Quantum-Resistant Crypto-Agile Inline Authentication and Encryption Framework for IEC 61850 Digital Substations

Moritz Gstür
Karlsruhe Institute of Technology (KIT)
Karlsruhe, Germany
moritz.gstuer@kit.edu

Mohammed Ramadan
Karlsruhe Institute of Technology (KIT)
Karlsruhe, Germany
mohammed.ramadan@kit.edu

Veit Hagenmeyer
Karlsruhe Institute of Technology (KIT)
Karlsruhe, Germany
veit.hagenmeyer@kit.edu

Abstract

Smart electricity grids increasingly rely on communication between distributed subsystems, leading to an increased attack surface. Standards for smart grid communication security, such as IEC 62351, do not sufficiently cover the developments of quantum computing. To bridge this gap, we propose a novel quantum-resistant crypto-agile authentication and encryption framework. The framework safeguards the confidentiality, authenticity, integrity, and non-repudiation of industrial network communication using a bump-in-the-wire approach. The framework is tailored to the strict time constraints of low-latency protocols deployed in IEC 61850 digital substations. To evaluate the framework and demonstrate its applicability in digital substations, we conduct a performance analysis and a laboratory-based experiment using intelligent electronic devices, merging units, and I/O boxes communicating via the GOOSE and SV protocol. The results show that the framework is able to secure low-latency digital substation communication, as authenticated and encrypted frames achieve a transfer time below 3 ms. Moreover, the laboratory-based experiment indicates that the novel bypass-capable architecture of the framework enables deployment via retrofitting of existing substations, as it allows adaption to partially incompatible environments via configurable fine-grained bypassing of network streams.

CCS Concepts

• **Security and privacy** → **Public key encryption**; **Hash functions and message authentication codes**; **Authentication**; **Security protocols**; *Distributed systems security*; *Domain-specific security and privacy architectures*; Firewalls; • **Computer systems organization** → Embedded and cyber-physical systems; Real-time systems; • **Networks** → **Security protocols**; *Middle boxes / network appliances*; *Cyber-physical networks*; Firewalls; Network performance analysis.

Keywords

Authentication, Smart Grid, Digital Substation, Substation Automation System, Cyber-Physical System, Low-Latency Communication, Bump-in-the-Wire, Generic Object Oriented Substation Events, Sampled Values, IEC 61850, IEC 62351

ACM Sustainability Week Companion '26, Banff, AB, Canada

ACM ISBN 979-8-4007-2199-1/26/06
https://doi.org/10.1145/3765611.3815134

ACM Reference Format:
Moritz Gstür, Mohammed Ramadan, and Veit Hagenmeyer. 2026. Quantum-Resistant Crypto-Agile Inline Authentication and Encryption Framework for IEC 61850 Digital Substations. In *ACM Sustainability Week 2026 (ACM Sustainability Week Companion '26), June 22–25, 2026, Banff, AB, Canada.* ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/3765611.3815134

1 Introduction

The infrastructure in the energy-related sector currently transforms from traditional top-down energy transmission and distribution systems to smart grids with bidirectional data and energy flows [10]. This transformation leads to an increased reliance of deployed operational technology (OT) on information and communication technology (ICT), as smart grids heavily rely on communication between distributed OT subsystems. The development of OT enables new possibilities, including the integration of distributed subsystems into supervisory control and data acquisition (SCADA) systems, but also leads to new challenges with regard to cybersecurity [28]. Mitigation strategies and cybersecurity approaches of the IT domain may not be viable solutions for OT, due to the differing characteristics of OT systems [7, 28].

Historical evidence indicates that economically or politically motivated adversaries pose a risk to OT systems, including energy-related systems [6]. Furthermore, current developments of quantum computers towards cryptographically or cryptanalytically relevant quantum computers (CRQC) [29] increase the risk for OT system security [7]. Despite the fact that OT systems rely less on cryptographic mechanism in comparison to IT systems, OT systems are vulnerable to the adversarial misuse of a CRQC due to their criticality, increasing connectivity, legacy devices, and low-computational capabilities [7, 25]. In particular, public-key cryptography relying on the hardness of the integer factorization problem, discrete logarithm problem (DLP), and elliptic curve discrete logarithm problem (ECDLP) are endangered by CRQCs, as quantum algorithms exist to solve these problems efficiently [2, 5, 7].

The present paper focuses on strategies to enhance the information security of communication protocols in digital substations and their substation automation systems (SAS). An SAS represents the entirety of communication and control equipment of a substation [27]. Satisfying security requirements including integrity, authenticity, non-repudiation, and confidentiality without compromising the strict time constraints of communication protocols are key factors for the cybersecurity in an SAS [19]. These protocols include among others the generic object oriented substation event (GOOSE) and sampled values (SV) protocol, as defined in

IEC 61850 [15, 17]. These protocols rely on symmetric cryptography for mandatory authentication and optional encryption of transferred data [16]. The symmetric cryptography algorithms used for SAS communication, including AES-GCM, AES-CBC, AES-GMAC, and HMAC-SHA are believed to be secure against post-quantum attacks [2]. However, the traditional key agreement protocols Diffie-Hellman-Merkle (DH) and elliptic-curve Diffie-Hellman-Merkle (ECDH), which are utilized to establish shared keys, are not secure against post-quantum attacks as they rely on the hardness of the DLP and ECDLP. While today's versions of widely accepted standards for cybersecurity in substations underline the importance of crypto-agility and quantum-resistant cryptography [18], quantum adversaries may pose a risk for already deployed substations, especially due to a substation's long lifecycle.

To bridge this gap, we propose a quantum-resistant crypto-agile inline authentication and encryption framework for SAS communication. Our framework provides mandatory authentication and optional authenticated encryption via a bump-in-the-wire (BITW) approach. Due to its BITW or inline deployment, our framework is a viable solution to provide confidentiality, integrity, authenticity, and non-repudiation not only in a newly constructed SAS but also via retrofitting of existing substations. To address the aforementioned objectives and considerations, the present paper comprises the following main contributions:

- **C1 Framework:** A novel quantum-resistant crypto-agile inline authentication and encryption framework enhancing the security of low-latency SAS communication.
  - **C1.1 Architecture:** A security-oriented SAS architecture integrating industrial components as well as components responsible for inline cryptographic procedures.
  - **C1.2 Protocol:** A lightweight encapsulation-based communication protocol based on a hybrid cryptosystem enabling transparent in-flight authentication and encryption of data frames.
  - **C1.3 Operation:** An adaptation approach based on operating modes and selective frame bypassing, which simplifies deployment and debugging for SAS operators, and increases retrofitting capabilities.
- **C2 Implementation:** An open source implementation of our framework using object-oriented high-level programming languages.
- **C3 Evaluation:** An experimental evaluation analyzing the performance and applicability of our framework.

The remainder of the present paper is organized as follows: In Section 2, we present the related literature of the present paper. In Section 3, the architecture, communication protocol, and adaptation strategies of the framework are introduced and discussed. In Section 4, we present a performance analysis and an experimental demonstration of applicability. In Section 5, we present a summary and provide insights into prospective future research.

2 Related Work

A FALCON-based quantum-resistant digital signature scheme for time-critical substation communication is presented by Hussain et al. [13]. The scheme aims to safeguard the authenticity and integrity of the routable GOOSE (R-GOOSE) and routable SV (R-SV) protocol defined in IEC 61850-90-5 [14]. Based on a delay analysis using experiments and network simulations, the authors demonstrate that the approach is able to meet the end-to-end delay requirements of R-GOOSE and R-SV. Similar to the work of Hussain et al. [13], the present paper emphasizes the viability of employing public-key cryptography for enhancing SAS security. By employing a hybrid quantum-resistant cryptosystem, our framework not only benefits from the security characteristics of asymmetric cryptography but also from the smaller message overhead and faster computation of traditional quantum-resistant symmetric cryptography. Moreover, the crypto-agility of our framework allows adaptation to future developments.

An inline authentication approach for network packets between intelligent electronic devices (IED) and merging units (MU) is presented by Ishchenko and Nuqui [19]. A BITW device called security filter is deployed as an add-on device at Ethernet-based communication busses using the GOOSE or SV protocol. The security filter appends MAC tags to outgoing messages of an IEDs and verifies incoming MAC tags. Thus, the security filter safeguards integrity and authenticity of SAS communication. The authors show that the security filter is able to meet the performance requirements of GOOSE and SV using a hash message authentication code (HMAC) and Galois message authentication code (GMAC) algorithm on off-the-shelf ARM hardware. Our framework is inspired by the BITW architecture of the security filter [19]. We extend the concept by not only providing authentication but also authenticated encryption to SAS devices. Moreover, aspects of quantum-resistant cryptography, especially with regard to key agreement, are not considered by the security filter approach [19].

A quantum-resistant communication protocol for smart grids based on the ring learning with errors problem is presented by Bera et al. [3]. The approach aims to secure network communication between edge servers, service providers, and smart meters. The feasibility of the approach is demonstrated by performing an experimental evaluation and comparative analysis on computation and communication costs. Moreover, the authors prove the claimed security characteristics formally. In contrast to the approach by Bera et al. [3], the goal of our framework is to support low-latency protocols employed in smart grids. The hybrid characteristic and crypto-agility of our framework ensure that communication is as secure as possible while considering strict communication constraints.

Instant messaging services, another domain which is at risk of quantum attacks including '*Harvest Now, Decrypt Later*' attacks, are in need of quantum-resistant authentication and encryption. PQXDH is a post-quantum key agreement protocol by Kret and Schmidt for Signal [4, 20]. Apple's iMessage uses the PQ3 messaging protocol to secure both, the initial key establishment and the ongoing message exchanges using post-quantum cryptography [1, 22]. However, both industrial approaches partially rely on non-quantum-resistant elliptic curve cryptography. Our framework emphasizes the viability of a fully quantum-resistant approach by combining post-quantum and traditional quantum-resistant cryptography. Moreover, our framework is lightweight with regard to the number of different keys used for key agreement, and used for domain-specific message authentication and encryption.

3 Quantum-Resistant Crypto-Agile Inline Authentication & Encryption Framework

As digital substations are part of smart grids and, thus part of the critical electricity infrastructure, securing intra- and inter-substation communication becomes increasingly more relevant. In the present paper, we focus on securing the low-latency communication of digital substations, including GOOSE and SV communication. To safeguard the confidentiality, authenticity, integrity, and non-repudiation of low-latency message exchanges against today's adversaries as well as quantum adversaries in the future, we propose a quantum-resistant crypto-agile inline authentication and encryption framework. The framework comprises the following key characteristics:

Transparent Inline Cryptography: The framework provides authentication and authenticated encryption to substation devices. These services are provided inline, i.e., these services are provided to the corresponding service consumers automatically and invisibly. This BITW approach enables deployment of the framework in newly constructed substations and existing substations via retrofitting.

Hybrid Cryptosystem: The framework is based on a multi-phase approach featuring three cryptographic mechanisms. A digital signature algorithm (DSA) and a key encapsulation mechanism (KEM) are responsible for establishing a mutually-authenticated secure connection between two system entities. An authenticated data encapsulation mechanism (DEM) provides secure and lightweight authentication and authenticated encryption services for arbitrary domain-specific data.

Quantum-Resistance: The framework emphasizes the importance of a fully quantum-resistant approach to secure communication against non-quantum adversaries, passive quantum adversaries, and active quantum adversaries. Consequently, the framework does not rely on non-quantum-resistant cryptography.

Crypto-Agility: As no CRQC exists yet, uncertainties regarding the performance and abilities of quantum computers remain to exist. To deal with these uncertainties and make the framework future-proof, the framework does not rely on the characteristics of specific algorithms but rather supports the replacement of algorithms depending on communication requirements and cybersecurity developments at the time of deployment. Moreover, this algorithm-agnostic approach enables operators or devices to choose cryptographic algorithms, that fit their security requirements and performance constraints best.

No Key Escrow: While the framework employs a trusted third party for identity binding, the private cryptographic material used for DSA, KEM, and DEM is only known to the communicating entities.

3.1 Architecture

The architecture of the framework is shown in Figure 1. The architecture consists of three types of entities:

SAS Device: OT devices that aim to exchange domain-specific data at the data link layer. Depending on the protocol used, communication between these devices might be time-critical.

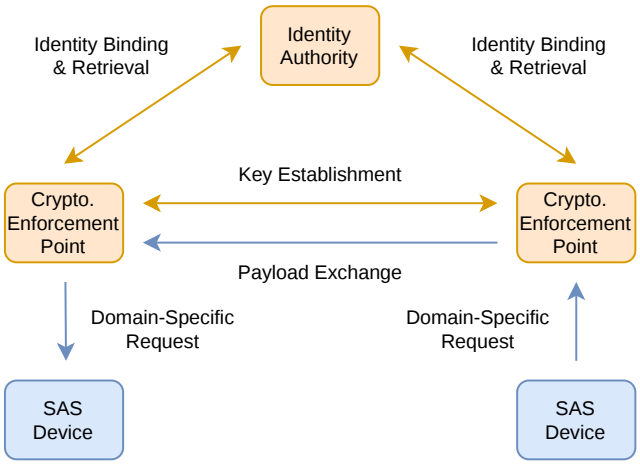

Figure 1: Framework architecture and message exchanges.

CEP: The cryptography enforcement point (CEP) handles data link layer frames by either applying an authenticated data encapsulation to them or verifying and decapsulating them.

IA: The identity authority (IA) binds the identity of SAS devices to the identity of a CEP. Moreover, it acts as a key store for authentication-related public keys.

3.2 Authentication & Encryption Protocol

Our framework relies on a three-phase protocol for initialization, key establishment, and payload exchange. The overarching goal of the protocol is to securely exchange domain-specific data frames between SAS devices via their CEPs. The protocol is executed by a CEP on behalf of its SAS device. The protocol is unidirectional, i.e., the initiator of a so-called session determines the session-specific parameters. Thus, the opposite direction of an already established session not necessarily uses the same session parameters. The phases of the protocol rely on the following parameters:

3.2.1 *Parameters.*

Device-Specific Parameters.

ID_{CEP_i}: Unique identifier of CEP_i.
ID_{SAS_i}: Unique identifier of SAS device SAS_i.
ID_{IA}: Unique identifier of the trusted IA.
DSA_χ: Digital signature algorithm (DSA) used by device χ.
PK_{DSA_χ}: Public key of DSA_χ.
SK_{DSA_χ}: Private key of DSA_χ.

Session-Specific Parameters.

KEM_{ij}: KEM used by CEP_i for communication to CEP_j.
$PK_{KEM_{ij}}$: Public key of KEM_{ij}.
$SK_{KEM_{ij}}$: Private key of KEM_{ij}.
DEM_{ij}: DEM used by CEP_i for communication to CEP_j.
$PK_{DEM_{ij}}$: Public key of DEM_{ij}.
$SK_{DEM_{ij}}$: Private key of DEM_{ij}.
Note: $PK_{DEM_{ij}} = SK_{DEM_{ij}}$ if DEM is symmetric cryptography. For more general applicability, the notation in the following sections assumes asymmetric cryptography.

Encapsulations.

$[M]_{DSA_\chi}$: Arbitrary message M authenticated with DSA_χ.
$[K]_{KEM_{ij}}$: Key K encapsulated with KEM_{ij}.
$[M]_{DEM_{ij}}$: Arbitrary message M authenticated, or authenticated and encrypted with DEM_{ij}.

3.2.2 Initialization Phase. The initialization phase aims to uniquely bind the identity of a CEP to the identity of an SAS device. Moreover, this phase is responsible for computing and publishing device-global cryptographic parameters. The identity binding $\widetilde{ID}_i$ is created by a CEP_i and permanently stored and distributed by the IA. In addition to the unique identifiers ID_{CEP_i} and ID_{SAS_i} of the CEP and its SAS device, the binding contains the identifier of the used DSA algorithm DSA_{CEP_i} and the associated public key $PK_{DSA_{CEP_i}}$. The initialization algorithm is shown in Algorithm 1.

Algorithm 1 Initialization procedure performed by CEP_i.

Require: $\lambda_i := (ID_{CEP_i}, ID_{SAS_i}, DSA_{CEP_i}, ID_{IA}, PK_{DSA_{IA}})$
function Initialize(λ_i)
  $(PK_{DSA_{CEP_i}}, SK_{DSA_{CEP_i}}) \leftarrow$ KeyGeneration(DSA_{CEP_i})
  Store($SK_{DSA_{CEP_i}}, ID_{IA}, PK_{DSA_{IA}}$)

  // Send identity binding request to IA
  $\widetilde{ID}_i \leftarrow (ID_{CEP_i}, ID_{SAS_i}, PK_{DSA_{CEP_i}}, DSA_{CEP_i})$
  Send($ID_{IA}, [\widetilde{ID}_i]_{DSA_{CEP_i}}$)
end function

3.2.3 Key Establishment Phase. The key establishment phase is started by CEP_i who wants to send data to CEP_j but has not established a secure session yet. Accordingly, CEP_i requests a KEM public key $PK_{KEM_{ij}}$ from CEP_j. This public key is used to encapsulate a generated DEM private key $SK_{DEM_{ij}}$ and exchange it with CEP_j securely. Both key pairs $(PK_{KEM_{ij}}, SK_{KEM_{ij}})$ and $(PK_{DEM_{ij}}, SK_{DEM_{ij}})$ are ephemeral keys, i.e., both pairs are regenerated and not re-used for further key establishments. However, while the KEM keys are only used once for key exchange, the DEM keys can be used for multiple message exchanges. The determination of appropriate usage limits or lifetimes of the DEM keys is beyond the scope of the present paper. The key establishment initiation algorithm executed at CEP_i is shown in Algorithm 2. The algorithm responding to a key establishment request at CEP_j is shown in Algorithm 3.

3.2.4 Payload Exchange Phase. The payload exchange algorithm is started by a CEP at delivery of a domain-specific data frame. Since the involved CEPs are already mutually authenticated and established DEM keys, no communication to the IA is necessary. Consequently, each message exchange represents exactly one domain-specific data frame. The algorithms for sending and receiving payload exchange requests at CEP_i and CEP_j are shown in Algorithm 4 and Algorithm 5.

The payload exchange phase is only initiated if a successful key establishment has already been performed. However, the initiator can re-perform the key establishment, if the ephemeral keys $PK_{DEM_{ij}}$ and $SK_{DEM_{ij}}$ are too old or utilized too often.

Algorithm 2 Key establishment initiation by CEP_i.

Require: $KEM_{ij}, DEM_{ij}, Frame := (ID_{SAS_i}, ID_{SAS_j}, Payload)$
function InitiateEstablishment($KEM_{ij}, DEM_{ij}, Frame$)
  Load($SK_{DSA_{CEP_i}}, PK_{DSA_{IA}}, ID_{IA}$)
  $ID_{SAS_j} \leftarrow$ GetReceiver($Frame$)

  // Send identity resolution request to IA
  $[\widetilde{ID}_j]_{DSA_{IA}} \leftarrow$ Send($ID_{IA}, [ID_{SAS_j}]_{DSA_{CEP_i}}$)
  if not Verify($[\widetilde{ID}_j]_{DSA_{IA}}, PK_{DSA_{IA}}$) **then**
    Abort()
  end if
  Store($\widetilde{ID}_j$)

  // Send KEM public key request to CEP_j
  $[PK_{KEM_{ij}}]_{DSA_{CEP_j}} \leftarrow$ Send($ID_{CEP_j}, [KEM_{ij}]_{DSA_{CEP_i}}$)
  if Verify($[PK_{KEM_{ij}}]_{DSA_{CEP_j}}, PK_{DSA_{CEP_j}}$) **then**
    // Send payload exchange with piggybacked DEM key
    $(PK_{DEM_{ij}}, SK_{DEM_{ij}}) \leftarrow$ KeyGeneration(DEM_{ij})
    Store($PK_{DEM_{ij}}$)
    Send($ID_{CEP_j}, \left[[SK_{DEM_{ij}}]_{KEM_{ij}} \,||\, [Frame]_{DEM_{ij}}\right]_{DSA_{CEP_i}}$)
  end if
end function

Algorithm 3 Key establishment response by CEP_j.

Require: $Request := (ID_{CEP_i}, ID_{CEP_j}, [KEM_{ij}]_{DSA_{CEP_i}})$
function RespondEstablishment($Request$)
  Load($SK_{DSA_{CEP_j}}, PK_{DSA_{IA}}, ID_{IA}$)
  $ID_{CEP_i} \leftarrow$ GetSender($Request$)

  // Send identity resolution request to IA
  $[\widetilde{ID}_i]_{DSA_{IA}} \leftarrow$ Send($ID_{IA}, [ID_{CEP_i}]_{DSA_{CEP_j}}$)
  if not Verify($[\widetilde{ID}_i]_{DSA_{IA}}, PK_{DSA_{IA}}$) **then**
    Abort()
  end if
  Store($\widetilde{ID}_i$)

  // Get and verify payload from key establishment request
  $[KEM_{ij}]_{DSA_{CEP_i}} \leftarrow$ GetPayload($Request$)
  if Verify($[KEM_{ij}]_{DSA_{CEP_i}}, PK_{DSA_{CEP_i}}$) **then**
    // Send KEM public key to CEP_i
    $(PK_{KEM_{ij}}, SK_{KEM_{ij}}) \leftarrow$ KeyGeneration(KEM_{ij})
    Store($SK_{KEM_{ij}}$)
    Send($ID_{CEP_i}, [PK_{KEM_{ij}}]_{DSA_{CEP_j}}$)
  end if
end function

Algorithm 4 Sending of domain-specific data frame at CEP_i.

Require: $Frame := (ID_{SAS_i}, ID_{SAS_j}, Payload)$
function SendPayloadExchange($Frame$)
  Load($\widetilde{ID}_j, PK_{DEM_{ij}}$)
  Send($ID_{CEP_j}, [Frame]_{DEM_{ij}}$)
end function

Algorithm 5 Receiving of a payload exchange at CEP_j.

Require: $Request := (ID_{CEP_i}, ID_{CEP_j}, [Frame := (ID_{SAS_i}, ID_{SAS_j}, Payload)]_{DEM_{ij}})$

1: **function** ReceivePayloadExchange($Request$)
2: Load($SK_{DEM_{ij}}$)
3: **if** Verify($[Frame]_{DEM_{ij}}, SK_{DEM_{ij}}$) **then**
4: Send($ID_{SAS_j}, Frame$)
5: **end if**
6: **end function**

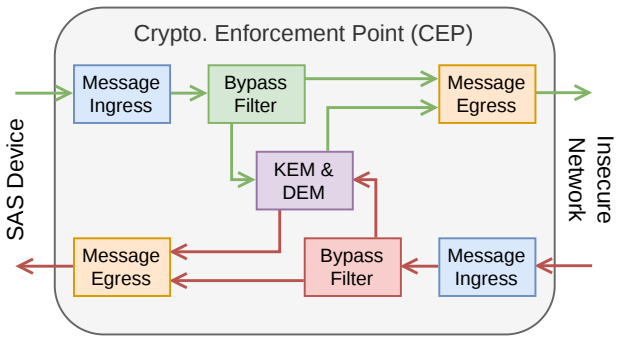

Figure 2: Internal cryptography enforcement point (CEP) architecture with bypass filtering.

3.3 Selective Frame Bypassing

A central novelty of our framework is the selective frame bypassing. The bypass-enabled internal architecture of a CEP is shown in Figure 2. By providing a bypass option for specific data frames at data link layer, the framework simplifies deployment and debugging for substation operators, and increases retrofitting capabilities. Upon arrival of a data frame, either from the SAS device or insecure network, a CEP checks whether this specific frame has to be encapsulated or forwarded to an egress interface without alteration. These checks are based on bypass filters, which are arbitrarily deep network frame inspections. The selective frame bypassing safeguards the compatibility of the framework with protocols that are either susceptible to temporal inconsistencies resulting from authentication and encryption, or provide services not only to SAS devices but also to auxiliary intermediate devices, such as network switches and routers. Among others, these protocols include network time protocols, such as the (simple) network time protocol (NTP / SNTP) and the precision time protocol (PTP), and lower-layer network management protocols, such as the address resolution protocol (ARP), parallel redundancy protocol (PRP), and media redundancy protocol (MRP).

3.4 Operation Modes

In contrast to the frame-dependent selective bypassing discussed in Section 3.3, a CEP operates in exactly one of the following modes for any non-bypassed type of network frame. The operating modes determine how a data frame is handled at a CEP during the payload exchange phase. Consequently, these modes neither influence the KEM nor the DSA algorithms used.

Authenticated Encryption Mode: Quantum-resistant authenticated encryption is applied to each data frame encapsulated by a CEP during the payload exchange phase. This mode safeguards confidentiality, authenticity, integrity, and non-repudiation of domain-specific data frames.

Authentication-Only Mode: Quantum-resistant authentication is applied to each data frame encapsulated by a CEP during the payload exchange phase. This mode safeguards authenticity, integrity, and non-repudiation of domain-specific data frames. With regard to GOOSE and SV communication, this mode complies to the non-recommended encryption but mandatory authentication policy of the IEC 62351 standards [16]. Furthermore, this mode enables mirroring of network traffic required for debugging purposes and network-based intrusion detection systems.

4 Evaluation

We conduct an experimental evaluation to analyze the performance and applicability of our framework. The experiments are based on a multithreaded object-oriented software implementation of the framework using Java 25. The implementation relies on cryptographic algorithms, which are recommended by NIST and the IEC 62351 standards: For DSA and KEM, we use the NIST standardized quantum-resistant module-lattice-based DSA (ML-DSA) [23], formerly known as Dilithium, and module-lattice-based KEM [24], formerly known as Kyber. For DEM, the framework supports ML-DSA as well as a set of traditional quantum-resistant symmetric algorithms. The algorithm implementations are provided by OpenJDK 25.0.2 [26] and Bouncy Castle [21]. The supported DEM algorithms and their performance metrics are shown in Table 1 and Table 2, and discussed in Section 4.1. The implementation of our framework is published open source on GitHub [11] under the European Union Public License (EUPL) [9].

4.1 Performance Analysis

The goal of the performance analysis is to evaluate the behavior of the framework with regard to delay caused by authentication and authenticated encryption during the operation of the framework. Thereby, we aim to demonstrate that the framework is able to handle time-critical message exchanges. To highlight the lightweight design of the framework, the performance-related experiment is conducted using a testbed based on non-specialized off-the-shelf hardware. A detailed visualization of the network topology and devices can be found in the appendix, in Figure 3.

We analyze the performance of the framework based on a round-trip time (RTT) estimation. Thus, no synchronization is required between the deployed computers and, under the assumption of symmetric transmission times, the accuracy of the RTT measurements only depends on the accuracy of the system clock of the measuring entity. To estimate the RTT, we implement a benchmark program in Python, which is published open source alongside the implementation and analysis results of the framework [11]. The benchmark program features two roles, a sending and a mirroring entity. The sending entity sends a user datagram protocol (UDP) packet with a timestamp, which is mirrored by the second entity without alteration. After receiving a mirrored packet, the sending

Table 1: Round-trip times of encapsulated data frames in ms.

Data Encapsulation Algorithm	Mean $\bar{x}$	Median $\tilde{x}$	Deviation σ	Extrema Min	Extrema Max
Control Group	0.64	0.63	0.02	0.61	0.70
Authentication-Only					
HMAC-SHA256	1.99	2.01	0.18	1.69	3.57
AES-256-GMAC	2.14	2.05	0.26	1.91	3.51
ML-DSA-44	6.03	5.69	0.82	5.07	9.23
ML-DSA-65	8.25	7.93	1.22	6.61	14.08
ML-DSA-87	12.37	12.16	0.92	10.91	16.98
Auth. Encryption					
AES-256-GCM	2.48	2.46	0.12	2.33	3.69
AES-256-CCM	2.61	2.61	0.29	1.98	3.98
ChaCha20-Poly1305	2.27	2.27	0.11	2.10	3.21

Table 2: Throughput and message type share of algorithms.

Data Encapsulation Algorithm	Throughput Packets / s	Cumulative Share in Types 1A / 4 ≤ 6 *ms*	Cumulative Share in Types 1B / 2 / 3 / 5 / 6 ≤ 40 *ms*
Control Group	1412	100 %	100 %
Authentication-Only			
HMAC-SHA256	486	100 %	100 %
AES-256-GMAC	453	100 %	100 %
ML-DSA-44	163	63 %	100 %
ML-DSA-65	120	0 %	100 %
ML-DSA-87	80	0 %	100 %
Auth. Encryption			
AES-256-GCM	397	100 %	100 %
AES-256-CCM	377	100 %	100 %
ChaCha20-Poly1305	426	100 %	100 %

entity calculates the RTT by subtracting the received timestamp from the current timestamp. A visualization of the steps of the RTT estimation is shown in Figure 4 in the appendix. The RTT estimation is conducted for each of the selected DEM algorithms. To compensate for fluctuations in the measurements, the RTT-related metrics of each algorithm shown in Table 1 and Table 2 are derived from 1000 sequential measurements. The results indicate that all tested symmetric authentication and authenticated encryption algorithms are viable solutions for securing low-latency substation communication, as 100 % of the packets have an RTT of less than 6 ms. Thus, these algorithms are able to satisfy the 3 ms transfer time constraint of the GOOSE and SV protocol. The data show that ML-DSA cannot be used to authenticate GOOSE and SV frames. However, ML-DSA can be employed to authenticate the IEC 61850 message types 1B, 2, 3, 5, and 6 as the RTT is below 40 ms for all measurements. The sequential packet throughput of the framework is between 486 packets per second (PPS) with HMAC-SHA256 and 80 PPS with ML-DSA-87. In comparison to the control group, i.e., measurements without authentication or authenticated encryption, symmetric cryptography achieves a throughput of 26.6 % to 34.4 %. Asymmetric cryptography achieves a throughput of 5.6 % to 11.5 % of the control group throughput. Therefore, while satisfying the transfer time requirements of low-latency SAS communication, applying authentication and authenticated encryption reduces the maximum achievable throughput of packets to at least 34.4 %.

4.2 Demonstration of Applicability

We conduct a demonstration of applicability in our smart grid cybersecurity laboratory [8] to show that the framework is compatible with industrial SAS hardware. The demonstration procedure discussed in the following has originally been developed to demonstrate the applicability of our inline access control for SAS. Thus, a more detailed description of the conducted experiment, its steps, limitations, and OT devices can be found in the paper of our real-time attribute-based access control for SAS [12]. The utilized hardware and steps of the experiment can be found in the appendix, in Table 3 and Figure 5.

Our laboratory features three so-called bays, which consist of a MU, IED, and IO-box. These devices are compliant to IEC 61850 and mimic the behavior of a digital substation. For each of the bays, we set the experiment up by disconnecting the bay's MU, IED, and IO-box from the process and station bus of the SAS. We then reconnect the devices to the busses via separate CEPs and connect the IA to both busses. By simulating an overcurrent situation via an Omicron relay tester, we are able to trigger a trip situation and check if the SV and GOOSE communication behave as expected. With our framework in place, all three MUs successfully exchange SV frames with their corresponding IEDs, and all three IEDs successfully exchange GOOSE frames with their corresponding IO-boxes. Accordingly, the experiment shows that our framework is compatible with SAS equipment compliant to IEC 61850 and does not negatively influence its functionality.

5 Conclusions & Outlook

As quantum computers may pose a great threat to critical electricity infrastructure in the future, we propose a novel quantum-resistant crypto-agile inline authentication and encryption framework for IEC 61850 digital substations. It provides a lightweight bump-in-the-wire authentication and authenticated encryption protocol, which enhances the communication security of low-latency protocols used in substations by providing confidentiality, authenticity, integrity, and non-repudiation. We present the applicability of the proposed framework by conducting an experimental performance analysis and a laboratory-based demonstration of applicability using industrial devices deployed in digital substations. In the future, we plan to integrate the framework into our real-time attribute-based access control for digital substations [12] to protect it against quantum adversaries, as it heavily relies on authenticated communication. Moreover, we plan to formally prove its security characteristics and further harden the framework against different cyberattacks. Additionally, further research is required to evaluate the applicability of the framework for other time-critical systems with similar requirements as a digital substation, including industry 4.0, robotics, avionics, and medical systems.

Acknowledgments

This work was supported by funding from the topic Engineering Secure Systems of the Helmholtz Association (HGF) and by KASTEL Security Research Labs (structure 46.23.02).

References

[1] Apple Security Engineering and Architecture (SEAR). 2024. *iMessage with PQ3: The new state of the art in quantum-secure messaging at scale.* Technical Report. Apple Inc. https://security.apple.com/blog/imessage-pq3

[2] Abdullah Aydeger, Engin Zeydan, Awaneesh Kumar Yadav, Kasun T. Hemachandra, and Madhusanka Liyanage. 2024. Towards a Quantum-Resilient Future: Strategies for Transitioning to Post-Quantum Cryptography. In *2024 15th International Conference on Network of the Future (NoF).* IEEE, 195–203. doi:10.1109/nof62948.2024.10741441

[3] Basudeb Bera, Rohini Poolat Parameswarath, and Biplab Sikdar. 2025. Fortifying the Security of Smart Grid Networks With Post-Quantum Communication. *IEEE Transactions on Smart Grid* 16, 6 (Nov. 2025), 5430–5445. doi:10.1109/tsg.2025.3592991

[4] Karthikeyan Bhargavan, Charlie Jacomme, Franziskus Kiefer, and Rolfe Schmidt. 2023. *An Analysis of Signal's PQXDH.* Technical Report. Cryspen Sarl. https://cryspen.com/post/pqxdh

[5] Lily Chen, Stephen Jordan, Yi-Kai Liu, Dustin Moody, Rene Peralta, Ray Perlner, and Daniel Smith-Tone. 2016. *Report on Post-Quantum Cryptography.* Technical Report. National Institute of Standards and Technology. doi:10.6028/NIST.IR.8105

[6] Communications Security Establishment Canada. 2021. *Cyber threat bulletin: Cyber threat to operational technology.* Retrieved March 15, 2026 from https://open.canada.ca/data/dataset/98bad300-28f1-49b9-9b34-2d46de4c9a58

[7] Cybersecurity and Infrastructure Security Agency. 2024. *Post-Quantum Considerations for Operational Technology.* Technical Report. https://www.cisa.gov/resources-tools/resources/post-quantum-considerations-operational-technology

[8] Ghada Elbez, Gustavo Sánchez, Sine Canbolat, Sophie Corallo, Clemens Fruböse, Florian Lanzinger, Nicolai Kellerer, Gustav Keppler, Felix Neumeister, Bernhard Beckert, Anne Koziolek, Martina Zitterbart, and Veit Hagenmeyer. 2025. Insights and Lessons Learned from a Realistic Smart Grid Testbed for Cybersecurity Research. In *Proceedings of the 16th ACM International Conference on Future and Sustainable Energy Systems (E-Energy '25).* ACM, 805–812. doi:10.1145/3679240.3734649

[9] European Union. 2017. *European Union Public Licence (EUPL) Version 1.2.* Retrieved March 15, 2026 from https://joinup.ec.europa.eu/collection/eupl

[10] Xi Fang, Satyajayant Misra, Guoliang Xue, and Dejun Yang. 2012. Smart Grid — The New and Improved Power Grid: A Survey. *IEEE Communications Surveys & Tutorials* 14, 4 (2012), 944–980. doi:10.1109/surv.2011.101911.00087

[11] Moritz Gstür. 2026. *Quantum-Resistant Inline Retrofittable Authentication (QIRA).* Retrieved March 15, 2026 from https://github.com/gstuer/QIRA

[12] Moritz Gstür, Gustav Keppler, Mohammed Ramadan, Ghada Elbez, and Veit Hagenmeyer. 2026. RTS-ABAC: Real-Time Server-Aided Attribute-Based Authorization & Access Control for Substation Automation Systems. arXiv:2603.23012 [cs.CR] doi:10.48550/arXiv.2603.23012

[13] S.M. Suhail Hussain, Mohd. Asim Aftab, Shaik Mullapathi Farooq, Abdul Latif, Charalambos Konstantinou, and Mohammad A. Abido. 2025. A Public key Based Quantum Secure Digital Signature Scheme for Securing IEC 61850 R-GOOSE and R-SV Messages. *IEEE Transactions on Industry Applications* 61, 3 (May 2025), 5135–5147. doi:10.1109/tia.2025.3542726

[14] International Electrotechnical Commission. 2012. Part 90-5: Use of IEC 61850 to transmit synchrophasor information according to IEEE C37.118. *Communication networks and systems for power utility automation (IEC 61850)* (2012).

[15] International Electrotechnical Commission. 2014. Part 5: Communication requirements for functions and device models. *Communication networks and systems for power utility automation (IEC 61850)* (2014).

[16] International Electrotechnical Commission. 2020. Part 6: Security for IEC 61850. *Power systems management and associated information exchange - Data and communications security (IEC 62351)* (2020).

[17] International Electrotechnical Commission. 2022. Part 8-1: Specific communication service mapping (SCSM) - Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3. *Communication networks and systems for power utility automation (IEC 61850)* (2022).

[18] International Electrotechnical Commission. 2023. Part 9: Cyber security key management for power system equipment. *Power systems management and associated information exchange - Data and communications security (IEC 62351)* (2023).

[19] Dmitry Ishchenko and Reynaldo Nuqui. 2018. Secure Communication of Intelligent Electronic Devices in Digital Substations. In *2018 IEEE/PES Transmission and Distribution Conference and Exposition (T&D).* IEEE. doi:10.1109/tdc.2018.8440438

[20] Ehren Kret and Rolfe Schmidt. 2024. *The PQXDH Key Agreement Protocol.* Technical Report. Signal Technology Foundation. https://signal.org/docs/specifications/pqxdh

[21] Legion of the Bouncy Castle Inc. 2026. *Bouncy Castle – Open-source cryptographic APIs.* Retrieved March 15, 2026 from https://www.bouncycastle.org/

[22] Felix Linker, Ralf Sasse, and David Basin. 2025. A Formal Analysis of Apple's iMessage PQ3 Protocol. In *34th USENIX Security Symposium.* 5015–5034.

[23] National Institute of Standards and Technology. 2024. Module-Lattice-Based Digital Signature Standard. *Federal Information Processing Standards Publication (FIPS PUB)* 204 (2024). doi:10.6028/NIST.FIPS.204

[24] National Institute of Standards and Technology. 2024. Module-Lattice-Based Key-Encapsulation Mechanism Standard. *Federal Information Processing Standards Publication (FIPS PUB)* 203 (2024). doi:10.6028/NIST.FIPS.203

[25] Javier Oliva del Moral, Antonio deMarti iOlius, Gerard Vidal, Pedro M. Crespo, and Josu Etxezarreta Martinez. 2024. Cybersecurity in Critical Infrastructures: A Post-Quantum Cryptography Perspective. *IEEE Internet of Things Journal* 11, 18 (Sept. 2024), 30217–30244. doi:10.1109/jiot.2024.3410702

[26] Oracle Corporation. 2026. *OpenJDK JDK 25.0.2 General-Availability Release.* Retrieved March 15, 2026 from https://jdk.java.net/25

[27] Evelio Padilla. 2015. *Substation Automation Systems: Design and Implementation.* Wiley. doi:10.1002/9781118987216

[28] Keith Stouffer, Michael Pease, CheeYee Tang, Timothy Zimmerman, Victoria Pillitteri, Suzanne Lightman, Adam Hahn, Stephanie Saravia, Aslam Sherule, and Michael Thompson. 2023. *Guide to Operational Technology (OT) Security.* Technical Report NIST Special Publication 800-82,Rev.3. National Institute of Standards and Technology. doi:10.6028/nist.sp.800-82r3

[29] Frank K. Wilhelm, Rainer Steinwandt, Paul Lageyre, and Susanna Kirchhoff. 2025. *Status of quantum computer development V2.2.* Technical Report. Federal Office for Information Security (BSI). https://www.bsi.bund.de/dok/study_status_quantum_computer

A Appendix

The appendix comprises tables and figures adapted from [12], which further explain the performance analysis and laboratory-based demonstration of applicability of our approach.

A.1 Performance Analysis

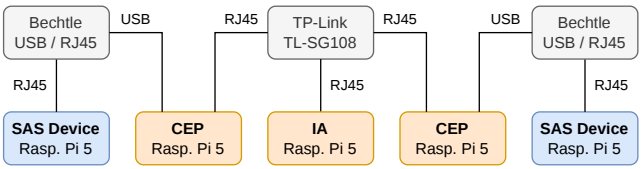

Figure 3: Devices and network topology of the performance analysis testbed.

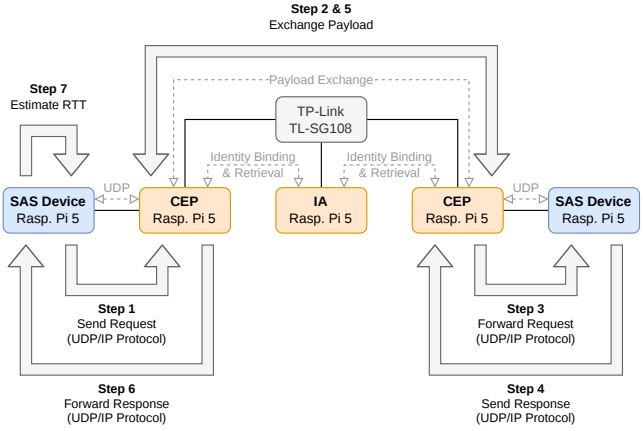

Figure 4: Sequence of events of the experimental message exchange latency estimation.

A.2 Demonstration of Applicability

Table 3: Hardware used for the laboratory-based demonstration of applicability.

	Manufacturer	Device	Task
Bay I	General Electric General Electric Siemens	Reason MU320 Multilin F60 SIPROTEC 6MD84	Process Bus MU Protection IED Input/Output Box
Bay II	SEL Hitachi ABB Siemens	SEL-401 REL670 SIPROTEC 6MD84	Process Bus MU Protection IED Input/Output Box
Bay III	Siemens Siemens Siemens	SIPROTEC 6MU85 SIPROTEC 7SX85 SIPROTEC 6MD84	Process Bus MU Protection IED Input/Output Box
Grid Simulation	OMICRON OMICRON	CMC 356 Process Simulator	Universal Relay Test Set Circuit Breaker
Networking	Weidmüller FS.COM Bechtle	IE-SW-SL28M-SV UMC-1F1T ARTICONA Adapter	Industrial Ethernet Switch Ethernet Media Converter USB-A to RJ45 Adapter
Auxiliary	Raspberry Pi Ltd	Raspberry Pi 5 8GB	CEP & IA

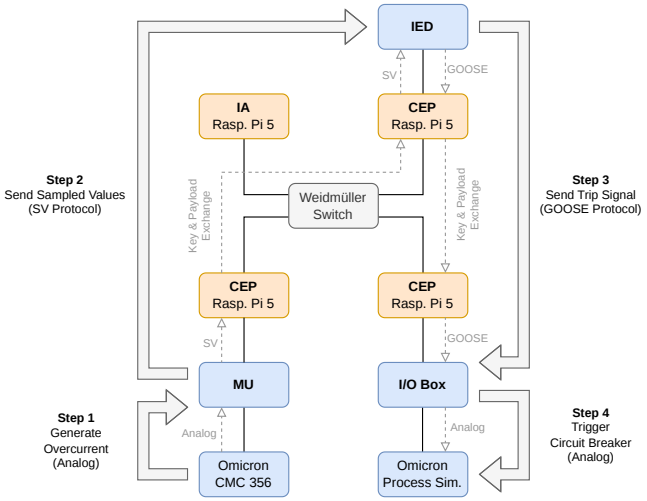

Figure 5: Sequence of events of the laboratory-based demonstration of applicability.