

Routing Security in the Post-Quantum Future

Marco Pioppini
ETH Zürich
Zürich, Switzerland

Jonghoon Kwon
ETH Zürich
Zürich, Switzerland

Yi-Min Lin
ETH Zürich
Zürich, Switzerland

Adrian Perrig
ETH Zürich
Zürich, Switzerland

Abstract

Post-quantum cryptography has gained urgency with recent advances in quantum computing. This transition is particularly consequential for inter-domain routing, whose compromise can undermine connectivity across the Internet. Current work on making routing security quantum-safe has focused primarily on migrating existing mechanisms, especially the RPKI, to post-quantum cryptography. We argue that this framing is too narrow. Rather than treating the transition as a one-time replacement of cryptographic algorithms, we examine how post-quantum constraints may reshape routing security itself. We discuss more flexible designs that accommodate multiple algorithms, the scalability challenges of post-quantum signatures, and alternatives based on more efficient cryptographic primitives. Based on these observations, we outline a broader research agenda for routing security in the post-quantum era.

CCS Concepts

• Security and privacy → Network security; • Networks → Routing protocols.

Keywords

Routing security, BGP, RPKI, post-quantum cryptography

ACM Reference Format:

Marco Pioppini, Yi-Min Lin, Jonghoon Kwon, and Adrian Perrig. 2026. Routing Security in the Post-Quantum Future. In *The 25th ACM Workshop on Hot Topics in Networks (HotNets '26)*, November 16-17, 2026, Salt Lake City, UT, USA. ACM, New York, NY, USA, 9 pages. <https://doi.org/10.1145/3847290.3859936>



This work is licensed under a Creative Commons Attribution 4.0 International License.

HotNets '26, Salt Lake City, UT, USA

© 2026 Copyright held by the owner/author(s).

ACM ISBN 979-8-4007-3029-0/2026/11

<https://doi.org/10.1145/3847290.3859936>

1 Introduction

With recent advances in quantum computing [10], the threat of a cryptographically relevant quantum computer (CRQC), i.e., a machine capable of breaking today's cryptography at scale, is becoming imminent. To address this threat, standardization bodies have published recommendations for the migration to quantum-safe cryptographic algorithms, commonly referred to as post-quantum cryptography (PQC). The NIST timeline aims for migration by 2035 [32], and similarly, a European Union roadmap targets a migration date of 2030 to 2035 for different use cases [2]. For some systems, changes are already underway; e.g., changes to the web PKI are already being implemented and evaluated by large players such as Google and Cloudflare [3, 6, 11, 45], and Let's Encrypt is planning to issue post-quantum certificates by 2027 [8].

The need to secure inter-domain routing, the mechanism that underpins the Internet, against the looming quantum threat has been recognized by the routing community, especially given that routing attacks can have widespread consequences and undermine the security of other (possibly already quantum-proofed) systems [14, 40].

Discussions on how to quantum-proof inter-domain routing revolve around securing the Resource Public Key Infrastructure (RPKI), the out-of-band system used to verify information exchanged via the Border Gateway Protocol (BGP). An approach to replace the cryptographic algorithms used in the RPKI is described in RFC6916 [20], and this approach could be used to switch the RPKI to new quantum-safe algorithms. However, the suggested migration approach requires operators to maintain two synchronized sets of information (one for the old algorithm, one for the new one) for an extended period of time until all participants have switched. An algorithm migration as described in RFC6916 has never been tried in practice; its feasibility has been called into question, and alternative approaches have been suggested [4, 17, 31].

Like RFC6916, the suggested alternatives and community discussion all revolve around how to best perform *the migration* to a new post-quantum algorithm, with a secondary focus on the performance impacts of PQC on the RPKI. The central argument of this paper is that *the current conversation*

focus is too narrow and places less emphasis on two important aspects.

First, the emphasis on *the migration* to PQC is too short-sighted and neglects the possibility of having to change algorithms more than once, for example due to the discovery of cryptographic weaknesses. This is of particular concern in the context of new PQC designs which are less battle-tested than classical cryptography. Famously, the Rainbow signature scheme advanced to the final NIST standardization round before a way to break it on a laptop was found [13]. Of course, in case of a broken algorithm, the migration procedure could be applied again, but, as emerges from the discussions on the topic, migration is a slow process and requires substantial operational effort.

Second, the community has focused on quantum-proofing the currently deployed routing security mechanisms, primarily route origin validation (ROV). While this is understandable from a practical point of view, a discussion on how quantum-proofing could enable or hinder the future evolution of routing security is also warranted. BGPsec provides a concrete example. Although it protects against more sophisticated routing attacks than ROV alone, it has yet to see widespread deployment, despite being standardized almost a decade ago [27], in part because of concerns about cryptographic processing on routers and increased convergence times. A naive replacement of its existing signatures with more expensive PQC schemes would only exacerbate these deployment barriers. The post-quantum transition therefore strengthens the case for exploring more resource-efficient ways to achieve routing security rather than simply replacing the cryptographic algorithms in existing designs.

Broadening the discussion on quantum-proof inter-domain routing to include new, more flexible designs and additional security mechanisms opens up a large design space, and we present several promising research directions in this paper.

Ethics statement. This work raises no ethical concerns.

2 The Quantum Threat

We start by contextualizing the cryptographic capabilities of quantum computers and providing an overview of PQC.

Symmetric vs asymmetric cryptography. Although a large-scale quantum computer has yet to be built, researchers have devised quantum algorithms that can break cryptographic algorithms in use today. It is important to note that asymmetric and symmetric cryptography are impacted differently. The security of asymmetric schemes, e.g., RSA or elliptic curve cryptography, hinges on the fact that their underlying mathematical problems, such as integer factorization or the discrete logarithm problem, are considered hard to solve. Quantum computers, however, are expected to be able to

Table 1: Key and signature sizes and signing/verification costs for representative classical and post-quantum signature schemes. Timings were measured using liboqs and OpenSSL on an M4 CPU.

Scheme	Public Key (B)	Sig (B)	Sign (μ s)	Verify (μ s)
ECDSA P-256	64	64	15.8	35.7
RSA-2048	256	256	681.5	19.4
ML-DSA-44	1,312	2,420	114.8	33.0
ML-DSA-65	1,952	3,309	181.8	53.1
Falcon-512	897	666	97.6	15.8
SLH-DSA-128s	32	7,856	182,561.6	189.3
SLH-DSA-128f	32	17,088	9,007.0	503.8

solve both these problems much more efficiently.¹ For example, by applying Shor’s algorithm [39] to retrieve the private key from a public key, thus breaking existing asymmetric cryptography.

The situation is different for symmetric cryptography: although Grover’s algorithm [21] could, in theory, be used to attack symmetric cryptography, such attacks are believed to remain impractical given the limited attack speedup and the inability to parallelize the algorithm [7, 44, 47]. Hence, existing symmetric cryptography is expected to remain safe, even when faced with a quantum-capable attacker.

Signatures vs encryption. The threat posed by quantum computers also impacts the two distinct purposes of asymmetric cryptography differently.

The first purpose of asymmetric cryptography is to ensure the confidentiality of information. Generally, this means that asymmetric cryptography is used to protect or exchange a symmetric key. A quantum attacker could retrieve these keys, breaking confidentiality. What makes this threat particularly insidious is that an attacker can collect currently undecryptable data and decrypt it once a quantum computer becomes available. This places even data exchanged before the availability of a CRQC at risk. In systems that handle confidential data, e.g., TLS or SSH, the possibility of these so-called “harvest now, decrypt later” attacks is the main driver for an early replacement of cryptographic algorithms.

The second purpose of asymmetric cryptography is to ensure the integrity and authenticity of data via signatures. Because a quantum attacker could forge signatures arbitrarily, all signatures, regardless of when they were issued, lose their trustworthiness once a CRQC appears.

Post-quantum cryptography. To address the quantum threat, new asymmetric cryptography schemes are being developed

¹However, this is neither free nor instant: a 2021 estimate requires 890 MWh to break RSA-2048 in 8 hours (about 85 U.S. households’ annual use) [36].

and standardized to replace the existing ones. NIST has already standardized three such post-quantum cryptography schemes: ML-KEM (key encapsulation) [34], ML-DSA (signatures) [33], and SLH-DSA (signatures) [35]. The standardization of Falcon, another signature scheme, is ongoing [1].² These signature and key encapsulation schemes are considered safe against quantum computers. Unfortunately, they are not usually a drop-in replacement for current algorithms, as their larger key sizes and signatures (see Table 1) must be considered. Some PQC algorithms are also more computationally expensive. As for classical algorithms, the key and signature sizes (and the computational cost) of PQC algorithms increase with higher security levels.

Crucially, the security of SLH-DSA hinges on very different properties than those of the other schemes. Most schemes rely on different mathematical puzzles than classical asymmetric cryptography, which has no known efficient quantum algorithm to solve them. Because these algorithms are young and less battle-tested than classical cryptography, they are often used in a hybrid construction. In a hybrid construction, as used, e.g., by TLS [26], a PQC algorithm is combined with a classical one, and messages are signed or encrypted once with each algorithm. Because an attacker would have to break both algorithms, this alleviates concerns regarding the maturity of PQC algorithms while still providing quantum-safety.

SLH-DSA, on the other hand, is based on symmetric cryptography and derives its security from well-understood hash functions. Although based on hash functions, SLH-DSA still functions as a regular signature algorithm with a private-public key pair. Its drawbacks are a significantly increased computational cost and larger signature size. SLH-DSA is more expensive but a more conservative option in terms of security assumptions compared to ML-DSA and was included by NIST as a safe “backup” algorithm.

3 The State of Quantum-safe Inter-Domain Routing

This section gives an overview of routing security mechanisms and summarizes the ongoing discussion on how to migrate the RPKI to PQC.

3.1 Routing Security Mechanisms

BGP is the inter-domain routing protocol used by autonomous systems (ASes) to exchange reachability information. BGP relies on the resource public key infrastructure (RPKI) to provide security. The RPKI is an out-of-band system that

²The comparatively small signature size and verification cost of Falcon make it an attractive candidate. However, it relies on floating point operations, which appear to be challenging to implement efficiently without creating side-channel vulnerabilities [22, 29, 48].

can be used to verify information exchanged via BGP. The hierarchical design of the RPKI mirrors the assignment of Internet resources, with the five regional Internet registries (RIRs) as trust roots. As the RIRs delegate resources (such as IP address ranges) to other entities, they attest to this delegation via certificates. In the RPKI, each participant is also a certificate authority, allowing it to further delegate its resources. RPKI participants can publish signed objects with information about their resources. Usually, this information is published to a repository hosted by a RIR, but a delegated repository may also be used. In the latter case, a reference to the sub-repository is included in the higher-level repository.

The simplest and most widely deployed security mechanism is route origin validation (ROV). In ROV, ASes publish route origin authorization (ROA) objects attesting their ownership of a specific prefix. ROV-validating ASes download the RPKI information from all repositories, starting with the trust roots, and verify the associated signatures following the chain of trust. Data is downloaded and verified by a separate service, not the BGP routers, and pushed to the routers after verification. Using this information, BGP speakers then check the originating AS of each received prefix announcement against the prefix owner stated in the RPKI information and reject announcements for which a different origin AS is registered in the RPKI. This mechanism is opt-in; if no ROA for a certain prefix exists, even ROV-validating ASes accept all routes towards that prefix.

ROV is only the simplest security mechanism and it only protects against misconfigurations and a narrow slice of routing attacks. Two complementary mechanisms provide further protections. The first step up from ROV is “autonomous system provider authorization” (ASPA). ASPA is currently being standardized [9, 43] and allows ASes to authorize their upstream providers; validating ASes then use this information to check the plausibility of received announcements. An even stronger mechanism is BGPsec [27], in which routers sign the AS-level path of all announcements they process. Unlike ROV and ASPA, BGPsec works in-band and requires routers to perform cryptographic operations themselves. BGPsec was standardized almost a decade ago but has yet to be deployed in practice, in part due to performance concerns.

3.2 Migration Pressure

Since the RPKI is used to certify publicly available information, routing security relies only on signatures, not on encryption, and “harvest now, decrypt later” attacks do not apply. Still, a large-scale quantum computer would have a devastating impact on routing security: Once a CRQC is available, classical signatures lose their trustworthiness, and validating ROVs will no longer prevent prefix hijacks, as an attacker could forge the corresponding ROAs, too. Worse

yet, if signatures can be forged, ROVs must be disregarded to preserve the opt-in nature of the RPKI. Otherwise, attacks on non-ROV-enabled prefixes become possible. The simplest such case is an attacker creating a cryptographically correct (but illegitimate) ROA for a currently unsigned victim prefix, tricking validating ASes into rejecting the legitimate announcements for the victim prefix. More elaborate attacks are also possible [17]. Thus, to avoid chaos, vulnerable signatures must be replaced before the quantum threat materializes. Implementing such a change will take considerable time and require coordination among RPKI participants. As the estimated arrival date of a CRQC keeps inching closer, starting this process as early as possible seems prudent.

3.3 Discussions on PQC for the RPKI

The RPKI currently uses RSA signatures [25] that need to be replaced to address the quantum threat. RFC6916 [20] specifies a migration procedure towards a new signature algorithm for the RPKI. As support for the new algorithm is expected to pick up gradually, this migration procedure includes a transition period during which two RPKI trees exist, one for each algorithm. Once all ASes have migrated to the new algorithm, the old tree is abandoned. The feasibility of the RFC6916-approach has been called into question, and a test migration from RSA to ECDSA has been suggested as a dry-run for a later migration to PQC [4, 41].

Alternative proposals for an easier transition to a new algorithm exist. These include a “mixed tree” approach [17] and a hybrid [31]. pqRPKI [28] proposes a design change based on Merkle tree ladders, greatly reducing the number of required signatures to cope with the size of PQC signatures. Additionally, there is orthogonal work on shrinking RPKI size by removing redundant information and signatures, which is beneficial given the increased size of PQC keys and signatures [38].

Although these proposals have launched a discussion on the post-quantum future of routing security, their focus lies on two distinct problems. The first problem that existing proposals tackle is how to approach a globally coordinated migration of the RPKI to a new algorithm in order to provide cryptographic agility. The second problem, addressed by designs such as pqRPKI, is how to shrink repository size or otherwise handle the increased storage requirements of PQC. The next section aims to complement this discussion by raising two questions that these existing works do not focus on. First, is there an alternative to coordinated migration to enable cryptographic agility? And second, what impact will PQC have on the future of routing security, e.g., on BGPsec?

4 A Broader Perspective

Stepping back from the question of how to migrate the RPKI to post-quantum cryptography, we consider how routing security can remain adaptable if cryptographic algorithms need to change again in the future and how the higher cost of post-quantum cryptography will affect the design and deployment of stronger routing security mechanisms.

4.1 Migration: One and Done?

The need for cryptographic agility and the possibility of future algorithm changes are addressed through migration rounds. We instead suggest exploring how to reduce the dependence on repeated ecosystem-wide migrations. The proposed solutions for migration all consider an algorithm change to PQC a one-time event. In reality, however, we should consider the need or desire to change algorithms more than once, and repeated algorithm migration rounds are likely not an adequate solution. The most evident situation in which changing algorithms becomes necessary again is the discovery of new weaknesses in cryptography. Such attacks may render a signature algorithm useless in a short time, which would require an emergency migration to a new signature algorithm. The currently discussed migration strategies do not address this risk. In fact, RFC6916 considers an emergency migration infeasible, describes algorithm migration as an orderly multi-year process, and acknowledges the possibility of downgrade attacks during the transition period [20].

Even if an algorithm remains secure, switching to a newer, more resource-efficient algorithm may be desirable; however, it may be impractical if the costs of migration outweigh the benefits. This is already the case: the RPKI uses RSA signatures, despite a cheaper option being available in the form of elliptic curves [41]. A similar situation may arise again with PQC algorithms, e.g., the not-yet-standardized Falcon is cheaper than ML-DSA, and more PQC algorithms are bound to be developed in the future. Still, the selection of a new algorithm cannot be postponed indefinitely; waiting too long to introduce a PQC algorithm conflicts with the need to start the migration early.

What emerges from the discussion around RPKI migration is that a migration will require substantial operational effort. If cryptographic agility is achieved only by system-wide algorithm migration, the same effort would have to be put in again when the need for migration arises in the future. We instead suggest shifting the focus away from migration towards design changes that make routing security less dependent on any one signature algorithm and that make new algorithms easier to roll out. Implementing any such changes will require significant, coordinated effort, but as such an effort will be required to quantum-proof the RPKI in the first

place, this occasion appears to be a good opportunity. We explore possible research directions in Section 5.

4.2 Routing Security Beyond ROV

The community is currently focused on ROV [4, 17, 31, 41], the only widely deployed routing security mechanism currently. However, the switch to PQC has implications for the future of routing security beyond ROV, particularly for BGPsec. An important characteristic of ROV is that information is fetched and verified in bulk and out-of-band by dedicated validators, which are then pushed to routers; BGP messages are not modified. The same applies to ASPA. Although the use of dedicated validators is primarily intended to avoid potentially heavyweight operations on routers, it has a secondary benefit: implementing changes (such as a new algorithm) is, at least in theory, simplified, because only a few validator machines per AS need to be updated. BGPsec, however, follows a very different model than ASPA and ROV. In BGPsec, router certificates are distributed through the RPKI, but information is verified in-band, with every router verifying and signing the AS-level path of prefix announcements it processes. These signatures are included in BGP messages. Although a draft document [46] acknowledges the need for PQC signatures in BGPsec and suggests new signatures for BGPsec router certificates (but not yet for UPDATE messages), we are unaware of any discussion of the impact PQC would have. Quantum-proofing BGPsec faces issues related to message size and ease of updating.

Message Size. Naively replacing the ECDSA signatures currently specified for BGPsec with PQC signatures would significantly increase the size of BGPsec messages (see Fig. 1). Falcon-512 signatures already push messages with more than five hops (5.3 % of paths) past the default 4 KiB message size limit of BGP. ML-DSA-44 pushes essentially every message past 4 KiB, though all remain within the 64 KiB ceiling of the extended message format (RFC 8654 [15]). The most conservative scheme, SLH-DSA-128f, inflates 60 % of messages past even the extended limit. Although the extended message format accommodates larger messages, this capability must be negotiated bilaterally, so extended messages require all on-path sessions to support it. We show the message sizes for pure PQC signatures, if a hybrid signature scheme were used (as is common), messages would be even larger.

Future Migrations. Since BGPsec is not currently deployed, a PQC migration could be circumvented by deploying BGPsec with a PQC signature algorithm right away. However, as argued in Section 4.1, we need to consider the need for future algorithm changes in BGPsec, too. Although BGPsec’s design includes a migration strategy that involves every message carrying double the signatures (one old, one new),

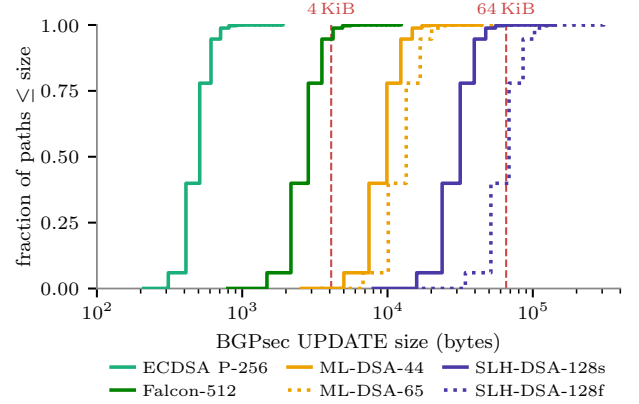


Figure 1: CDF of BGPsec UPDATE message sizes with different signature algorithms over 18.16 million AS paths from a Route Views 2 snapshot on July 13, 2026.

such an algorithm migration is even less feasible than for the RPKI for two reasons. First, during the migration period, messages would carry twice the signatures, further increasing message sizes and potentially increasing processing and convergence times. Second, and more importantly, because BGPsec operates directly on routers, an update to BGPsec implies an update to all participating BGP routers. Given that updating a few RPKI validators per AS already presents an operational challenge, an algorithm migration for BGPsec seems prohibitively expensive and infeasible.

Both these problems show that quantum-proofing BGPsec is not as straightforward as replacing a signature algorithm, and this makes it even less likely that BGPsec will see widespread adoption anytime soon. The fact that PQC is not easily applicable to BGPsec strengthens the case for exploring design changes and alternatives, and we explore a few promising directions in the next section.

5 Two Alternative Approaches

Two paths towards quantum-safe routing seem particularly promising. First, supporting multiple signature algorithms may enable better security-cost tradeoffs and allow for more flexibility. Second, moving from classical to PQC signatures is not the only way to quantum-proof a system, and alternatives to PQC are worth considering.

5.1 Supporting Multiple Algorithms

Rather than considering algorithm migration as the solution to cryptographic agility for routing security, we instead suggest making the RPKI (and associated mechanisms) more flexible, i.e., exploring the possibility of using multiple signature algorithms. Supporting multiple algorithms encompasses two independent directions: using different algorithms to

sign objects with different purposes, and using multiple different algorithms to sign a single object.

5.1.1 Different algorithms for different objects. We observe that not all keys in the RPKI have the same trust requirements and lifetime; hence, different signature algorithms should be used depending on the use case. In particular, trust in the RPKI is rooted in a handful of trust anchors, a set of keys owned by the RIRs. These are long-lived keys; they are rotated rarely and are distributed out of band, e.g., by updating validator software.³ Since trust anchors are hard to replace and compromise allows forgery of arbitrary RPKI information, they are a particularly attractive target for a quantum attacker. Due to the importance and long lifetime of these keys, SLH-DSA is an ideal choice for trust roots, as it is the most conservative PQC option in terms of security assumptions. Although significantly more expensive, the fact that SLH-DSA derives its security from well-understood hash functions makes it less likely that weaknesses in the signature scheme will require a replacement of trust anchors. In the current RPKI database, switching the trust roots to SLH-DSA only increases the overall size by 43 KiB and adds 1 ms of verification overhead (Table 2). We view this as a practical first step towards quantum-proofing the RPKI.

Lower-level certificates and signatures on ROA objects may then use other, cheaper PQC schemes, given the large number and validation frequency of such objects: ROAs and CA certificates live for days to months, number in the hundreds of thousands [42], and are periodically re-validated by every validator. For these objects, directly replacing the signature algorithm with the conservative SLH-DSA inflates repository size roughly eightfold and verification time roughly tenfold (Table 2), so using a cheaper, less conservative signature is likely more appropriate. Provided the trust roots are safe, lower-level signatures can always be re-issued. This has two advantages. First, even if the algorithm used for these signatures is vulnerable (either to a quantum attacker or to cryptanalysis), re-issuing these signatures frequently can, at least temporarily, provide protection, if attacks take sufficiently long.⁴ Second, it facilitates changing the algorithm used for lower-level signatures.

Another option for lower-level objects is signing and verifying them in bulk. As proposed for the RPKI [28] and the Web PKI [3], Merkle-tree-based batching can substantially reduce the cost of post-quantum signatures. Instead of signing every object individually, a certification authority signs

Table 2: Estimated RPKI repository size and per-validator cryptographic verification time with and without Merkle Tree Batching.

Algorithm(s)		Repository (GiB)		Verify (s)	
Root	Non-root	Plain	Batch	Plain	Batch
RSA-2048	RSA-2048	0.97	0.73	17.5	2.6
SLH-DSA-128s	RSA-2048	0.97	0.73	17.5	2.6
SLH-DSA-128s	Falcon-512	1.62	0.81	15.6	2.4
SLH-DSA-128s	ML-DSA-44	3.43	1.02	32.6	4.4
SLH-DSA-128s	SLH-DSA-128s	7.84	1.53	186.7	22.3
SLH-DSA-128s	RSA-2048 + ML-DSA-44	3.79	1.06	50.0	6.4
SLH-DSA-128s	Falcon-512 + ML-DSA-44	4.45	1.14	48.2	6.2

a Merkle-tree root covering multiple objects, amortizing the asymmetric signature cost across the batch. We estimate the resulting RPKI costs with SLH-DSA-based roots and report the results in Table 2.⁵ The estimates are consistent with those reported for pqRPKI [28] and additionally show the effect of using different algorithms for root and lower-level CAs. With batching, even expensive signatures incur modest overhead: using SLH-DSA only for the five root CAs is nearly negligible, while batching greatly reduces the number of lower-level signatures. Compared with the current RSA-2048 deployment without batching, a full SLH-DSA hierarchy increases repository size by roughly 560 MiB and verification time by about 5 s, whereas a mixed SLH-DSA/Falcon configuration is even smaller and faster to verify.

Batching shows promising results at first glance. However, the results are based on the current relatively flat RPKI hierarchy. How effectively batching can absorb the cost of post-quantum cryptography, if delegated RPKI repositories become more common, remains future work.

5.1.2 Different algorithms for the same object. Inter-domain routing’s global scope makes algorithm migration a coordination problem. Routing information propagates across independently operated networks, and signatures must be verifiable by participants beyond the signer’s immediate peers. Maintaining interoperability therefore requires agreement on supported cryptographic algorithms, motivating coordinated algorithm migration. By contrast, connection-oriented protocols such as TLS and SSH can negotiate algorithms between endpoints, allowing new algorithms to be introduced with less global coordination.

Signing the same object with multiple algorithms could loosen this coordination requirement. Relying parties could independently select which algorithms to trust and which

³In-band key rotation (RFC9691 [30]) can be used for trust anchor succession, but only as long as the existing signature algorithm is considered safe; otherwise, an attacker could forge a signature for a new trust root.

⁴This is known as *quantum-annoying*: using classical signatures with a lifetime shorter than the time a quantum computer would need to break them. [18, 23]. The obvious risk is underestimating the speed of such attacks.

⁵Based on an rpki-client 9.8 snapshot from July 13, 2026 (547,129 objects), using batches of 64 objects for ROAs, manifests, and ASPAs.

signatures to require, allowing new algorithms to be introduced without universal agreement on a single algorithm or combination. Within a selected combination, a relying party could require all component signatures to verify.

This approach raises two main challenges. First, different verification policies may cause the same object to be accepted by some ASes and rejected by others, raising questions about operational behavior and routing consistency. Second, carrying and verifying multiple signatures increases resource costs, particularly for PQC. To estimate these costs, we extend the model in Table 2 to two algorithms per non-root object, adding their signature sizes, public-key sizes, and verification costs while counting shared content and Merkle proofs only once. Batching substantially reduces the additional cost for signed objects, but certificates and CRLs remain unbatched. These estimates inform the resource costs of multi-signature RPKI; they do not establish its end-to-end scalability or the feasibility of applying the same approach to BGPsec.

Nevertheless, this form of agility may become increasingly relevant as national standards diverge in their choice of post-quantum algorithms [5, 19]. Further research should examine how to accommodate such diversity while preserving interoperability and predictable routing behavior. One direction is to investigate whether groups of networks with shared trust could coordinate algorithm migration within a smaller scope. Architectures such as SCION [16, 49] already provide scoping for trust roots and update policies, offering a basis for exploring this approach. However, preserving interoperability across domains with different algorithm choices remains a research challenge for such architectures as well.

5.2 Alternatives to Asymmetric Crypto

Replacing classical asymmetric cryptography with a PQC equivalent wherever signatures are needed is the most obvious solution to quantum-proofing existing systems. However, PQC is not the only solution. Symmetric cryptography is also not threatened by a quantum attacker. We believe that exploring where and how signatures could be replaced with symmetric primitives, such as MACs or hash functions, is another promising research direction.

The idea was explored before active discussion on post-quantum cryptography: SPV [24] authenticates the BGP UPDATE messages using symmetric primitives only, but its security degrades if the same few-time keys are reused across multiple path announcements. With the increased cost of PQC, the efficiency advantage of symmetric cryptography is more relevant than ever. SLH-DSA already shows that a many-time signature can be built from symmetric primitives alone, and its large signatures are the price of turning few-time keys into a many-time scheme [12]. While SLH-DSA is

designed as a general-purpose many-time signature scheme, more tailored solutions may offer sufficient security at a lower cost for specific use cases. We believe this direction is worth exploring further, especially for BGPsec's hop-by-hop authentication, though symmetric primitives may also be more widely applicable.

Delayed-disclosure message authentication codes in the style of TESLA [37] occupy the same symmetric-only space at an even lower cost, at the price of serving only live, loosely synchronized verifiers. If and how this restriction can be reconciled with routing security is another avenue worth exploring.

6 Conclusion

The current conversation around quantum-safety for BGP and the RPKI is focused primarily on migration strategies and the implications of PQC for existing mechanisms, but the design space around quantum-proof inter-domain routing is much larger. We suggest exploring more flexible routing security designs that can accommodate multiple cryptographic algorithms and better adapt to future changes. More fundamentally, the high cost and large signatures of post-quantum cryptography may make some existing designs, such as BGPsec, increasingly difficult to deploy, motivating alternative constructions based on more efficient primitives such as symmetric cryptography and potentially new routing architectures designed with post-quantum constraints in mind. The post-quantum transition should therefore be viewed not only as an algorithm-replacement problem but also as an opportunity to rethink routing security for greater efficiency, flexibility, and scalability.

Acknowledgements

We gratefully acknowledge support for this project from the Werner Siemens Stiftung (WSS) Center for Cyber Trust at ETH Zurich, ETH Zurich, and the Zurich Information Security and Privacy Center (ZISC). We also thank our shepherd, Yossi Gilad, and the anonymous reviewers for their constructive feedback and suggestions.

References

- [1] 2024. NIST Releases First 3 Finalized Post-Quantum Encryption Standards. <https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards>.
- [2] 2025. A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography. <https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography>
- [3] 2025. Keeping the Internet fast and secure: introducing Merkle Tree Certificates. <https://blog.cloudflare.com/bootstrap-mtc/>
- [4] 2025. [Sidrops] Master's thesis paper: PQC for the RPKI (and the "null scheme"). Sidrops mailing list. https://mailarchive.ietf.org/arch/msg/sidrops/T5PvNu_fYa8ZIV_dfhsx3K9_Cd8/.

- [5] 2026. Beijing wants its own quantum-resistant encryption standards rather than adopt NIST's. <https://www.csoonline.com/article/4147736/beijing-wants-its-own-quantum-resistant-encryption-standards-rather-than-adopt-nists.html>.
- [6] 2026. Cultivating a robust and efficient quantum-safe HTTPS. <https://blog.google/security/cultivating-a-robust-and-efficient-quantum-safe-https/>
- [7] 2026. NIST: Post Quantum Cryptography FAQs. <https://csrc.nist.gov/Projects/post-quantum-cryptography/faqs>
- [8] 2026. A Post-Quantum Future for Let's Encrypt. <https://letsencrypt.org/2026/06/03/pq-certs>
- [9] Alexander Azimov, Eugene Bogomazov, Randy Bush, Keyur Patel, Job Snijders, and Kotikalapudi Sriram. 2026. *BGP AS_PATH Verification Based on Autonomous System Provider Authorization (ASPA) Objects*. Internet-Draft. Internet Engineering Task Force. <https://datatracker.ietf.org/doc/draft-ietf-sidrops-aspa-verification/26/>
- [10] Ryan Babbush, Adam Zalcman, Craig Gidney, Michael Broughton, Tanuj Khattar, Hartmut Neven, Thiago Bergamaschi, Justin Drake, and Dan Boneh. 2026. Securing Elliptic Curve Cryptocurrencies against Quantum Vulnerabilities: Resource Estimates and Mitigations. <https://arxiv.org/abs/2603.28846>
- [11] David Benjamin, Devon O'Brien, Bas Westerbaan, Luke Valenta, and Filippo Valsorda. 2026. *Merkle Tree Certificates*. Internet-Draft. Internet Engineering Task Force. <https://datatracker.ietf.org/doc/draft-ietf-plants-merkle-tree-certs/04/>
- [12] Daniel J Bernstein, Andreas Hülsing, Stefan Kölbl, Ruben Niederhagen, Joost Rijneveld, and Peter Schwabe. 2019. The SPHINCS+ signature framework. In *Proceedings of the ACM SIGSAC conference on computer and communications security*.
- [13] Ward Beullens. 2022. Breaking Rainbow Takes a Weekend on a Laptop. Cryptology ePrint Archive, Paper 2022/214. <https://eprint.iacr.org/2022/214>
- [14] Henry Birge-Lee, Yixin Sun, Anne Edmundson, Jennifer Rexford, and Prateek Mittal. 2018. Bamboozling Certificate Authorities with BGP. In *Proceedings of the USENIX Security Symposium*.
- [15] Randy Bush, Keyur Patel, and David Ward. 2019. Extended Message Support for BGP. RFC 8654. <https://doi.org/10.17487/RFC8654>
- [16] Laurent Chuat, Markus Legner, David Basin, David Hausheer, Samuel Hitz, Peter Müller, and Adrian Perrig. 2022. *The complete guide to SCION: from design principles to formal verification*. Springer.
- [17] Dirk Doesburg. 2025. *Post-Quantum Cryptography for the RPKI*. Master's thesis. Radboud University.
- [18] Edward Eaton and Douglas Stebila. 2021. The "quantum annoying" property of password-authenticated key exchange protocols. Cryptology ePrint Archive, Paper 2021/696. <https://eprint.iacr.org/2021/696>
- [19] Cath Firmin. 2025. South Korea announces winners of KpqC competition. <https://pqshield.com/south-korea-announces-winners-of-kpqc-competition/>.
- [20] Roque Gagliano, Stephen Kent, and Sean Turner. 2013. Algorithm Agility Procedure for the Resource Public Key Infrastructure (RPKI). RFC 6916. <https://doi.org/10.17487/RFC6916>
- [21] Lov K Grover. 1996. A fast quantum mechanical algorithm for database search. In *Proceedings of the annual ACM symposium on Theory of Computing*.
- [22] Morgane Guerreau, Ange Martinelli, Thomas Ricosset, and Mélissa Rossi. 2022. The Hidden Parallelepiped Is Back Again: Power Analysis Attacks on Falcon. *IACR Transactions on Cryptographic Hardware and Embedded Systems* 2022, 3 (Jun. 2022), 141–164.
- [23] Daniel Herzinger, Linus Heise, Daniel Loebenberger, and Matthias Söllner. 2025. Time-Based State-Management of Hash-Based Signature CAs for VPN-Authentication. arXiv:2509.11695 <https://arxiv.org/abs/2509.11695>
- [24] Yih-Chun Hu, Adrian Perrig, and Marvin A. Sirbu. 2004. SPV: secure path vector routing for securing BGP. In *Proceedings of the ACM SIGCOMM Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication*.
- [25] Geoff Huston and George Michaelson. 2016. The Profile for Algorithms and Key Sizes for Use in the Resource Public Key Infrastructure. RFC 7935. <https://doi.org/10.17487/RFC7935>
- [26] Kris Kwiatkowski, Panos Kampanakis, Bas Westerbaan, and Douglas Stebila. [n. d.]. *Post-quantum hybrid ECDHE-MLKEM Key Agreement for TLSv1.3*. Internet-Draft. Internet Engineering Task Force. <https://datatracker.ietf.org/doc/draft-ietf-tls-ecdhe-mlkem/05/>
- [27] Matt Lepinski and Kotikalapudi Sriram. 2017. BGPsec Protocol Specification. RFC 8205. <https://doi.org/10.17487/RFC8205>
- [28] Weitong Li, Yuze Li, and Taejoong Chung. 2026. pqRPKI: A Practical RPKI Architecture for the Post-Quantum Era. arXiv:2603.06968 <https://arxiv.org/abs/2603.06968>
- [29] Xiuhua Lin, Mehdi Tibouchi, Yang Yu, and Shiduo Zhang. 2025. Do not disturb a sleeping falcon: floating-point error sensitivity of the falcon sampler and its consequences. In *Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT)*.
- [30] Carlos Martinez-Cagnazzo, George Michaelson, Tom Harrison, Tim Bruijnzeels, and Rob Austein. 2024. A Profile for Resource Public Key Infrastructure (RPKI) Trust Anchor Keys (TAKs). RFC 9691. <https://doi.org/10.17487/RFC9691>
- [31] Katharina Miesch, Haya Schulmann, and Niklas Vogel. 2025. Poster: The Rocky Road Towards RPKI Algorithm Agility. In *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security*.
- [32] Dustin Moody, Ray Perlner, Andrew Regenscheid, Angela Robinson, and David Cooper. 2024. *Transition to Post-Quantum Cryptography Standards*. Technical Report. National Institute of Standards and Technology. <https://doi.org/10.6028/nist.ir.8547.ipd>
- [33] National Institute of Standards and Technology. 2024. Module-Lattice-Based Digital Signature Standard. <https://doi.org/10.6028/NIST.FIPS.204>
- [34] National Institute of Standards and Technology. 2024. Module-Lattice-Based Key-Encapsulation Mechanism Standard. <https://doi.org/10.6028/NIST.FIPS.203>
- [35] National Institute of Standards and Technology. 2024. Stateless Hash-Based Digital Signature Standard. <https://doi.org/10.6028/NIST.FIPS.205>
- [36] Edward Parker and Michael J. D. Vermeer. 2023. Estimating the Energy Requirements to Operate a Cryptanalytically Relevant Quantum Computer. arXiv:2304.14344 <https://arxiv.org/abs/2304.14344>
- [37] Adrian Perrig, Ran Canetti, J. D. Tygar, and Dawn Xiaodong Song. 2000. Efficient Authentication and Signing of Multicast Streams over Lossy Channels. In *Proceedings of the IEEE Symposium on Security and Privacy*.
- [38] Haya Schulmann and Niklas Vogel. 2026. Pruning the tree: Rethinking RPKI architecture from the ground up. In *Proceedings of the Symposium on Network and Distributed System Security (NDSS)*.
- [39] Peter W. Shor. 1997. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM J. Comput.* 26, 5 (1997), 1484–1509.
- [40] Aftab Siddiqui. 2018. What Happened? The Amazon Route 53 BGP Hijack to Take Over Ethereum Cryptocurrency Wallets. <https://www.internetsociety.org/blog/2018/04/amazons-route-53-bgp-hijack/>
- [41] Job Snijders. 2023. [Sidrops] Signed Object signed with Ed25519 (RFC 8419 proof-of-concept). IETF SIDROPS mailing list. <https://mailarchive.ietf.org/arch/msg/sidrops/CG2BWxOa6Ly8F0huOULIBd4hGEC/>.

- [42] Job Snijders. 2026. RPKI's 2025 year in review. <https://blog.apnic.net/2026/02/20/rpkis-2025-year-in-review/>.
- [43] Job Snijders, Alexander Azimov, Eugene Uskov, Randy Bush, Russ Housley, and Ben Maddison. 2026. *A Profile for Autonomous System Provider Authorization*. Internet-Draft. Internet Engineering Task Force. <https://datatracker.ietf.org/doc/draft-ietf-sidrops-aspa-profile/27/>
- [44] Filippo Valsorda. 2026. Quantum Computers Are Not a Threat to 128-bit Symmetric Keys. <https://words.filippo.io/128-bits/>
- [45] Bas Westerbaan. 2025. Cloudflare Blog: State of the post-quantum Internet in 2025. <https://blog.cloudflare.com/pq-2025/>
- [46] Tomoki Yoshikawa and Loganaden Velvindron. 2026. *Post-Quantum Signature Experiments and Migration Considerations for the Resource Public Key Infrastructure (RPKI)*. Internet-Draft draft-yoshikawa-sidrops-pqc-rpki-02. Internet Engineering Task Force. <https://datatracker.ietf.org/doc/draft-yoshikawa-sidrops-pqc-rpki/02/> Work in Progress.
- [47] Christof Zalka. 1999. Grover's quantum searching algorithm is optimal. *Physical Review A* 60, 4 (Oct. 1999), 2746–2751. <https://doi.org/10.1103/physreva.60.2746>
- [48] Shiduo Zhang, Xiuhan Lin, Yang Yu, and Weijia Wang. 2023. Improved power analysis attacks on falcon. In *Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT)*.
- [49] Xin Zhang, Hsu-Chun Hsiao, Geoffrey Hasker, Haowen Chan, Adrian Perrig, and David G. Andersen. 2011. SCION: Scalability, Control, and Isolation on Next-Generation Networks. In *2011 IEEE Symposium on Security and Privacy*. 212–227. <https://doi.org/10.1109/SP.2011.45> ISSN: 2375-1207.