xBGPsec: Enhancing BGP Security with Transitive Signatures and External Validation

1st Nils Höger
University of Twente
Enschede, Netherlands
nils.hoeger@utwente.nl

2nd Cristian Hesselman
SIDN Labs
Arnhem, The Netherlands
University of Twente
Enschede, Netherlands
c.e.w.hesselman@utwente.nl

3rd Moritz Müller
SIDN Labs
Arnhem, The Netherlands
University of Twente
Enschede, Netherlands
m.c.muller@utwente.nl

4th Savvas Kastanakis
University of Twente
Enschede, Netherlands
s.kastanakis@utwente.nl

***Abstract*—The Border Gateway Protocol (BGP), a cornerstone of global Internet routing, remains vulnerable to various attacks due to its lack of integrated security features and mechanisms to verify the authenticity and integrity of routing information. Although BGPsec was introduced as a standardized solution to address these concerns, it has not seen real-world deployment even after eight years, primarily due to operational complexity and deployment challenges. We present the design and implementation of xBGPsec, a protocol that improves BGP security by attaching digital signatures to BGP updates using optional transitive attributes. These signatures cover both the AS path and dedicated BGP attributes, and are generated and verified by a dedicated external validator, allowing enhanced security without disrupting existing routing operations. To demonstrate the feasibility of this approach, we built a dedicated testbed integrating xBGPsec-enabled routers and a supporting cryptographic infrastructure. This proof-of-concept provides the foundation for future empirical evaluation and offers initial insights for network operators and researchers exploring scalable, interoperable BGP security solutions.**

***Index Terms*—xBGPsec, BGPsec, RPKI, transitive attributes**

I. Introduction

The Border Gateway Protocol (BGP) [1] forms the backbone of today's interdomain routing, interconnecting Autonomous Systems (ASes) and thereby constituting the foundation of the global Internet. Despite its critical role, BGP is plagued by severe and well-documented security vulnerabilities [2]. For example, the AS path contained within BGP update messages lacks integrity protection, making it susceptible to path manipulation attacks. Additionally, prefix hijacking is a prominent threat, in which an AS, maliciously or inadvertently, announces IP prefixes it does not legitimately own, causing traffic to be diverted from its intended destination [3]. These vulnerabilities are actively beeing exploited by adversaries to redirect traffic or to suppress originally legitimate updates, thereby undermining the reliability and security of inter-domain routing [4]. Additional risks include route leaks, in which BGP updates are propagated in violation of established routing policies [5]. These vulnerabilities are not merely theoretical: they are regularly exploited by malicious actors [6], but can also arise from operator error or misconfiguration [7], posing persistent threats to the stability and security of the Internet. With the increasing deployment of the Resource Public Key Infrastructure (RPKI) [8] and Route Origin Validation (ROV) [9], first security measures are beginning to see broader adoption. However, these solutions address only some vulnerabilities, and malicious attackers still have several available attack vectors like path manipulation or route leaks. Although resilient protection mechanisms like BGPsec have been proposed, adoption remains low due to deployment complexity and a lack of direct benefits for early adopters [10]. BGPsec requires the participation of all ASes along an update path, so its advantages are limited until widespread adoption is achieved. Nevertheless, peer-to-peer BGPsec sessions between neighboring ASes can still provide incremental security benefits, even if end-to-end protection is not possible. In addition to deployment challenges, these approaches often impose significant drawbacks, such as increased computational overhead for BGP routers [11] and lack of prefix packing support [12], further discouraging adoption by network operators.

Inspired by BGPsec, this work secures interdomain routing with cryptographic signatures, avoiding previous operational and deployment barriers. We introduce a lightweight mechanism using transitive signatures, generated on dedicated hardware external to routers, that protect the integrity of BGP update paths and dedicated attributes without disrupting existing routing infrastructure. Our approach supports partial deployment, prevents route leaks, and mitigates path manipulation. Our testbed consists of a real-world setup using GoBGP [13] and the NIST BGP-SRx framework [14], demonstrating the operational feasibility of our approach and providing a foundation for future experimentation. The modular, open-source implementation is publicly available to encourage researchers, network operators, and educators to explore and experiment with secure routing protocols. More details and examples can be found in the repository [15].

The remainder of this paper is structured as follows. Section II provides an overview of relevant background and related work. The requirements our approach has to fulfill are detailed in Section III. Section IV describes the architecture of xBGPsec and Section V details how this design meets our proposed requirements. Broader implications, discussion of findings, and potential directions for future research are explored in Section

978-3-903176-75-1 ©2025 IFIP

VI, before the paper concludes in Section VII.

II. Background and Related Work

This section provides an overview of key vulnerabilities affecting BGP, surveys existing security solutions, and highlights how our approach addresses their limitations.

A. Route Leaks

Route leaks represent a significant threat to Internet routing integrity. They occur when an AS improperly propagates BGP routing information violating routing policies. Route leaks typically result from misconfigurations rather than malicious intent, making them particularly common and difficult to prevent. The consequences can be severe: traffic may be redirected through unintended paths, creating inefficiencies, performance degradation, and potential security vulnerabilities where traffic traverses untrusted networks. However, BGP lacks integrated mechanisms to detect such leaks [5] [16].

B. Path Manipulation

The integrity of the path attribute in BGP messages is inherently unprotected, allowing any AS along the propagation path to modify it. While network operators legitimately use this capability to control traffic flow [17], it simultaneously presents a significant attack vector for malicious actors, a practice known as AS path forgery [18]. Attackers may employ various path manipulation techniques: shortening paths to make routes artificially attractive, inserting AS numbers (ASNs) of targeted systems to trigger BGP's loop detection mechanism (causing updates to be dropped), or injecting their own ASN to deceive targets into routing traffic through attacker-controlled networks. These path forgery techniques can also serve as building blocks for more sophisticated attack scenarios, such as forged-origin hijacks [4]. This ongoing threat emphasizes the need for a reliable technique to protect the integrity of the AS path and thus prevent such attacks.

C. Resource Public Key Infrastructure (RPKI)

The RPKI is a globally distributed database for Internet resources. It has a hierarchical structure that reflects the allocation hierarchy used for distributing ASNs and IP prefixes [8]. The Regional Internet Registries (RIRs) serve as the root of trust. RPKI allows resource holders to store cryptographically signed objects, making them publicly available for other ASes to access and validate. The most prominent of these objects are Route Origin Authorizations (ROAs), which are used for ROV.

D. Border Gateway Protocol Security (BGPsec)

BGPsec is an IETF proposed standard that extends BGP to provide cryptographic security for the AS path in BGP updates. Each participating AS publishes its public router key in the RPKI, signs the BGP update path with its private key, and appends the resulting signature as a new non-transitive path attribute. When a BGPsec update is received, ASes can validate the attached signatures by retrieving the corresponding public keys from the RPKI. Each AS on the path adds its own signature, which covers the preceding signatures, resulting in an interlocking chain of cryptographic assurances.

Despite its conceptual advantages BGPsec has seen no adoption in modern interdomain routing nearly a decade after its proposal. One major barrier is the significant computational overhead imposed by cryptographic operations, which existing BGP routers are not generally optimized to perform at scale. Additionally, BGPsec does not support partial or incremental deployment; all ASes along a given path must participate for the security guarantees to be effective. This requirement means that early adopters face significant deployment costs but do not receive immediate security benefits, since the advantages of the protocol can only be realized when it is widely implemented across many networks [10]. Furthermore, BGPsec focuses exclusively on ensuring the integrity of the AS path and does not address other well-known BGP vulnerabilities, such as route leaks. As a result, the combination of limited incentives for initial deployment and the protocol's restricted security scope has so far prevented its adoption in operational networks [12].

E. BGP-iSec

Morris et al. [19] proposed an extension of BGP, called BGP-iSec. Unlike BGPsec, BGP-iSec uses transitive BGP attributes to carry signatures, similar to the approach taken in our proposed extension. Furthermore, they introduced new attributes to provide route-leak prevention capabilities, which are also protected by the signatures. Although this is not the primary focus of our work, our extension similarly offers the possibility to cover additional attributes, which can, for example, be used to prevent route leaks [19]. There are, however, two key differences between their approach and ours. First, we implemented our extension on a real BGP router, whereas BGP-iSec was evaluated using emulations, which allows us to create a realistic testbed and evaluate our new approach in more detail. Second, and more importantly, our study demonstrates that signature computation can be offloaded from routers to a centralized external service, regardless of the protocol used (BGPsec, BGP-iSec, xBGPsec). This enables cryptographic operations to be performed on specialized hardware optimized for such tasks, reducing the computational burden on routers.

III. Requirements

The design of xBGPsec is guided by requirements across three domains: security, operational feasibility, and scalability. These requirements address the limitations of existing approaches while ensuring practical deployability.

A. Security Requirements

xBGPsec must ensure cryptographic integrity and authenticity of the AS path while integrating route leak prevention capabilities by default. It must also support scalable deployment across diverse network environments. In addition, it should incorporate mechanisms to prevent replay attacks. The solution should provide clear evidence of AS path tampering

or violations of valley-free routing, thereby strengthening the security of interdomain routing.

B. Operational Requirements

Deploying xBGPsec in real-world networks requires balancing enhanced security with minimal disruption to existing infrastructure. To ensure interoperability, the protocol must allow legacy BGP routers to process updates seamlessly despite lacking support for security metadata. A critical challenge lies in distinguishing between routes that legitimately lack signatures due to non-participation and those where signatures may have been maliciously stripped during transit. Addressing this requires a reliable mechanism to identify which ASes are expected to contribute signatures, enabling accurate validation without generating false positives. Performance optimization is equally crucial. xBGPsec must minimize the computational overhead on routers while supporting rapid signing and validation of frequent BGP updates. This necessitates an efficient design that scales with network growth without degrading routing responsiveness or convergence time. Underpinning these considerations is the requirement for robust, low-overhead key management. Secure distribution, storage, and rotation of cryptographic keys must function in a way that aligns with operational realities of network providers, avoiding unnecessary complexity for network operators while maintaining strong security guarantees.

C. Scalability Requirements

Given the scale and dynamic nature of today's Internet routing system, any security solution for BGP must function efficiently under conditions of high update volume and frequent route changes. The mechanism should support scalable deployment, allowing for the use of advanced hardware and parallel processing when necessary. To handle frequent routing churn and minimize latency, the protocol must enable rapid validation of routing updates without introducing significant computational overhead at each AS hop. Message sizes should remain within established BGP limits, and the approach should ensure compatibility and interoperability across diverse network environments. Overall, the solution is required to maintain low latency and high throughput, even in large-scale and dynamic scenarios.

IV. Architecture

xBGPsec introduces a modular architecture designed to retrofit cryptographic validation into the existing BGP ecosystem with minimal disruption. The architecture consists of three main components: (i) the xBGPsec Validator, a centralized cryptographic authority within each AS; (ii) the xBGPsec-using Router, which interacts with the validator for signing and validation tasks; and (iii) control-plane extensions for RPKI access that enable both the retrieval of router key objects from other ASes and the modification of an AS's own objects to signal operational state.

A. System Overview

Figure 1 illustrates the architecture of xBGPsec in a typical AS as well as the update flow which is described in more detail in the following section. Components highlighted with light-grey labels correspond to those implemented in our prototype. The validator acts as a central service responsible for verifying incoming updates and generating cryptographic signatures for outgoing announcements. Routers offload computationally intensive tasks, such as signature generation and validation, to the validator over a secure internal channel.

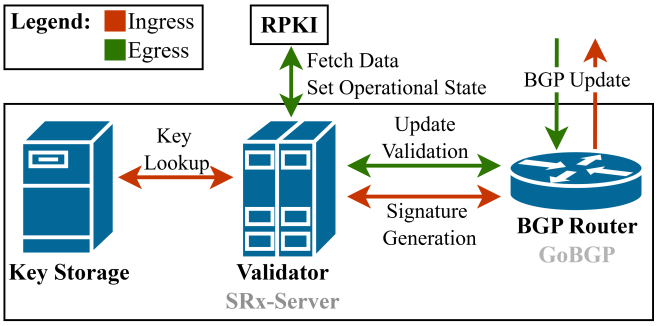

Fig. 1. High-level architecture and update flow of xBGPsec.

B. Update Processing Flow

When a BGP router sends an update to a peer, it initiates a signature generation request to the validator. Figure 1 displays this request with the green line between the router and the validator. The validator retrieves the private key from key storage, constructs a signature block for each peer, and returns these blocks to the router. To mitigate replay attacks, each signature incorporates a timestamp, binding it to a specific update context. The router then attaches the received signature block as an optional transitive path attribute to the BGP update, consistent with BGP's extensibility model [1]. This approach ensures that signatures are preserved across non-participating ASes and do not disrupt legacy BGP routers, which simply ignore unrecognized attributes.

Upon receiving a BGP update, the router sends mandatory information to the validator for signature verification. Figure 1 shows this data stream with red arrows between the validator and the router, and between the validator and the RPKI. The validator returns the result, and the router processes the update according to its routing policies.

C. Signature Chaining and Attribute Protection

xBGPsec enhances path integrity through interlocking signatures: each AS signs the current AS path and all previous signatures. This forms a verifiable cryptographic chain that allows recipients to detect any modification of the path or omission of intermediate ASes. The signature mechanism protects not only the current state of the update as processed by the current AS, but also preserves the integrity of previous signatures and their corresponding update states. xBGPsec also integrates the cryptographic protection of selected attributes.

To strengthen route leak prevention capabilities, our approach specifically includes the Only To Customer (OTC) attribute as defined in [20] within the signature coverage. This integration ensures that policy-based routing restrictions expressed through the OTC attribute are integrity protected.

D. RPKI Integration

To support partial deployment, xBGPsec extends the RPKI router key object to include a flag indicating the operational status of xBGPsec within an AS. Since this flag is not included in the current router key object specification, the existing design of this RPKI object needs to be updated to accommodate it. This allows neighboring ASes to distinguish between honest non-participation and malicious stripping of signatures. Validators check the RPKI status of each AS in the path to determine whether a missing signature is acceptable or indicative of an attack.

E. Key Management and Validator Architecture

All cryptographic material is managed by the validator, which stores private keys and performs signing on behalf of BGP routers. This centralization simplifies key rotation, reduces on-router complexity, and improves operational control.

Moreover, the validator can be deployed on highly optimized hardware with support for parallel processing, enabling extremely fast signature generation and verification. Centralizing logic also enables flexible integration of additional security mechanisms, such as Autonomous System Provider Authorization (ASPA), by updating a single component rather than all routers.

This design opens up further optimization opportunities, including presigning of frequent routes, batching of signature operations, or signature aggregation techniques, which can reduce cryptographic overhead in high-churn environments. These capabilities directly support xBGPsec's goals of scalable validation, low data-plane overhead, and future extensibility, as outlined in Section III.

F. Cryptographic Algorithms and Key Material

xBGPsec employs standardized cryptographic primitives to ensure compatibility, performance, and strong security guarantees. For digital signatures, we adopt the Elliptic Curve Digital Signature Algorithm (ECDSA) consistent with existing RPKI infrastructure and BGPsec [12].

V. Security Design Justification

This section justifies how xBGPsec's design satisfies its intended security goals through analysis of our protocol architecture and prototype implementation. We demonstrate how specific design choices directly address the threats in our threat model, particularly focusing on AS path integrity protection, route leak detection, replay attack prevention, and security in partial deployment scenarios. Our prototype implementation shown in Figure 1 demonstrates these security properties in practice. The implementation is publicly available [15].

A. Threat Model

We assume an adversary capable of observing, modifying, or injecting BGP messages between ASes. The attacker may:

- Modify the AS path (e.g., prepend or remove ASNs)
- Remove or alter cryptographic signature attributes
- Replay outdated announcements
- Announce unauthorized prefixes (if origin authentication is not enforced)

Based on this threat model, we now justify how xBGPsec's design elements specifically address each of the key security requirements outlined in Section III.

B. AS Path Integrity

Each BGP announcement in xBGPsec carries a chained signature block, where each AS signs the full path and the preceding signature chain. Removing or changing ASes from the path breaks this chain, resulting in a signature verification failure. This satisfies the AS path authenticity and integrity requirement defined in Section III.

C. Replay Protection

Each signature incorporates a timestamp that enables receivers to establish time-bound validity windows. By comparing the embedded timestamp against their local clock, receivers can reject messages that fall outside a designated freshness period. This timestamp validation mechanism effectively prevents replay attacks, as attackers cannot reuse otherwise valid signatures once they've expired.

D. Route Leak Detection

xBGPsec protects selected BGP attributes, particularly the OTC attribute, to enforce propagation constraints. If a misconfigured or malicious AS violates valley-free routing or strips the OTC attribute, the OTC attribute will either indicate it or its absence will result in a signature mismatch, and the update will be rejected by compliant validators.

E. Partial Deployment and Downgrade Resilience

In cases where an AS does not yet participate in xBGPsec, the absence of a signature is tolerated as long as the AS has not published a router key object in the RPKI. Once the AS publishes such an object, it must explicitly declare its operational status. Only if it indicates non-operational status will a missing signature be accepted. This design prevents downgrade attacks, where attackers attempt to bypass validation by omitting otherwise valid signatures.

The security mechanisms described above collectively demonstrate how xBGPsec's design achieves its security goals while maintaining practical deployment considerations. By addressing the core threats of path manipulation, replay attacks, route leaks, and downgrade attempts, the protocol provides a comprehensive security enhancement to BGP that can function in real-world, heterogeneous environments.

VI. Discussion

Our xBGPsec design addresses key limitations of BGPsec while maintaining strong security: centralizing cryptographic operations in a validator removes on-router overhead and enables parallelism, caching, and presigning, improving deployability without touching the data path.

Although our prototype demonstrates feasibility, operational deployments will require robust failover, which we envision through active-active validator clusters or active-standby configurations with fast health detection and bounded switchover. Using multiple validators also aligns with current RPKI best practices [21]. However, this design introduces trade-offs: The validator becomes a critical dependency, and operational complexity shifts toward it. As a result, xBGPsec is primarily suited for larger ASes with sufficient technical resources to deploy and maintain such systems.

Using an optional transitive attribute enables incremental deployment, but risks signature dropping. We consider storing minimal operational state in RPKI router-key objects; however, as RPKI publication lags BGP propagation, relying on it for operational state may introduce unacceptable delays [22]. Future work should evaluate faster, backward-compatible ways to expose an AS's operational state that is easy to look up and update, while preserving security guarantees. We plan to empirically measure signature retention and coverage under partial deployment.

Compared to BGPsec and BGP-iSec, xBGPsec offloads cryptographic operations from routers and centralizes policy and RPKI integration, while retaining incremental deployability. Furthermore, the validator has the potential to integrate with emerging security frameworks such as ASPA, allowing a layered defense against a wider spectrum of routing attacks.

Our testbed confirms the feasibility of our approach but does not yet provide a comprehensive performance evaluation. Key aspects such as signing and verification latency or validator throughput under high churn remain to be measured at larger scales. We consider these evaluations essential for future work, particularly to validate Internet-scale applicability.

VII. Conclusion

We introduced xBGPsec, a flexible approach to interdomain routing security that overcomes major deployment challenges of BGPsec. By centralizing cryptographic operations in an AS-wide validator, xBGPsec reduces operational complexity and attack surface, while enabling advanced security features like route leak prevention through attribute protection. The design builds on established cryptographic algorithms and can incorporate mechanisms such as ROV or ASPA. Our prototype demonstrates the feasibility of xBGPsec in a realistic environment. Results emphasize the advantages of external validation and signing, and the need for extensible, operationally robust security architectures in interdomain routing. To support future research and adoption, we provide our implementation as open source at [15], enabling reproduction, extension, and further exploration of BGP security with minimal overhead.

References

[1] Y. Rekhter, S. Hares, and T. Li, "A Border Gateway Protocol 4 (BGP-4)," RFC 4271, Jan. 2006. [Online]. Available: https://www.rfc-editor.org/info/rfc4271

[2] K. Butler, T. Farley, P. McDaniel, and J. Rexford, "A survey of bgp security issues and solutions," *Proceedings of the IEEE*, vol. 98, pp. 100 – 122, 02 2010.

[3] S. Cho, R. Fontugne, K. Cho, A. Dainotti, and P. Gill, "Bgp hijacking classification," 06 2019, pp. 25–32.

[4] B. A. Scott, M. N. Johnstone, and P. Szewczyk, "A survey of advanced border gateway protocol attack detection techniques," *Sensors (Basel, Switzerland)*, vol. 24, no. 19, p. 6414, 2024.

[5] K. Sriram, D. Montgomery, D. R. McPherson, E. Osterweil, and B. Dickson, "Problem Definition and Classification of BGP Route Leaks," RFC 7908, Jun. 2016. [Online]. Available: https://www.rfc-editor.org/info/rfc7908

[6] A. Siddiqui, "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/, accessed: 2025-06-26.

[7] D. Madory, "Large European routing leak sends traffic through China Telecom," https://blog.apnic.net/2019/06/07/large-european-routing-leak-sends-traffic-through-china-telecom/, accessed: 2025-06-26.

[8] M. Lepinski and S. Kent, "An Infrastructure to Support Secure Internet Routing," RFC 6480, Feb. 2012. [Online]. Available: https://www.rfc-editor.org/info/rfc6480

[9] G. Huston and G. Michaelson, "Validation of Route Origination Using the Resource Certificate Public Key Infrastructure (PKI) and Route Origin Authorizations (ROAs)," RFC 6483, Feb. 2012. [Online]. Available: https://www.rfc-editor.org/info/rfc6483

[10] D. Clark, C. Testart, M. Luckie, and K. Claffy, "A path forward: improving internet routing security by enabling zones of trust," *Journal of Cybersecurity*, vol. 10, no. 1, p. tyae023, 2024.

[11] M. Abdelhafez and Y. Fadlalla, "Bgpsec deployment challenges and optimization efforts," in *2024 IEEE 22nd Student Conference on Research and Development (SCOReD)*. IEEE, 2024, pp. 277–281.

[12] M. Lepinski and K. Sriram, "BGPsec Protocol Specification," RFC 8205, Sep. 2017. [Online]. Available: https://www.rfc-editor.org/info/rfc8205

[13] "Gobgp," https://github.com/osrg/gobgp, 2025.

[14] S. K. D. M. P. G. Oliver Borchert, Kyehwan Lee, "Bgp (s)ecure (r)outing e(x)tension software suite," https://github.com/usnistgov/NIST-BGP-SRx, 2024.

[15] N. Hoeger, "xBGPsec: Extended BGP Security Protocol," Aug. 2025. [Online]. Available: https://github.com/nhoeger/xBGPsec

[16] L. Gao and J. Rexford, "Stable internet routing without global coordination," *IEEE/ACM Transactions on networking*, vol. 9, no. 6, pp. 681–692, 2001.

[17] P. Marcos, L. Prehn, L. Leal, A. Dainotti, A. Feldmann, and M. Barcellos, "As-path prepending: there is no rose without a thorn," in *Proceedings of the ACM Internet Measurement Conference*, 2020, pp. 506–520.

[18] T. Holterbach, T. Alfroy, A. Phokeer, A. Dainotti, and C. Pelsser, "A system to detect forged-origin bgp hijacks," in *21st USENIX Symposium on Networked Systems Design and Implementation (NSDI 24)*, 2024, pp. 1751–1770.

[19] C. Morris, A. Herzberg, B. Wang, and S. Secondo, "Bgp-isec: Improved security of internet routing against post-rov attacks," in *Network and Distributed System Security (NDSS) Symposium 2024*. Internet Society, 2024.

[20] A. Azimov, E. Bogomazov, R. Bush, K. Patel, and K. Sriram, "Route Leak Prevention and Detection Using Roles in UPDATE and OPEN Messages," RFC 9234, May 2022. [Online]. Available: https://www.rfc-editor.org/info/rfc9234

[21] S. S. Berenguer, "Rpki best practices and lessons learned," https://www.arin.net/blog/2025/09/25/nro-rpki-best-practices/, 2025, accessed: 2025-09-26.

[22] R. Fontugne, A. Phokeer, C. Pelsser, K. Vermeulen, and R. Bush, "Rpki time-of-flight: Tracking delays in the management, control, and data planes," in *International Conference on Passive and Active Network Measurement*. Springer, 2023, pp. 429–457.