Homomorphic Routing: Private Data Forwarding in the Internet

Francesco Tusa*, David Griffin and Miguel Rio

2nd ACM SIGCOMM Workshop on Future of Internet Routing & Addressing (FIRA '23)
September 10th, 2023, New York, NY, USA

* email: f.tusa@westminster.ac.uk
Outline

- Motivation
- Solution Overview
- Homomorphic encryption
- System operation
- Preliminary evaluation
- Security and Deployment considerations
- Conclusions
Motivation

End-to-end encryption currently used to ensure data confidentiality of the payload

Issues

- IP headers transmitted as plaintext
- Network providers know source and destination IPs by design – no privacy
- Destination host always knows the identity of the source

Current solutions based on VPNs and Tor

- Performance impact
- Limited privacy
- Inability to enforce traffic engineering policies
Solution Overview: Homomorphic Routing

Private Source Routing (Previous Work)
- Inter-domain **source routing** to establish *private connections*
- **Source hosts select** *paths to the destination* that meet the *required characteristics* of the session

Homomorphic Routing
- *Hop-by-hop* announcements of **encrypted address ranges** a la BGP
- **ASes forward** to the *next hop* AS towards the destination *without knowing* the *destination address*
Solution Overview: Homomorphic Routing

In both Private Source Routing and Homomorphic Routing paths are encrypted:

- Destination host and full path cannot be reverse engineered

- Hard for network providers to identify the communicating entities
- ASes can only identify next hop for forwarding packets towards destination
- Source address/identity is not revealed to the destination host
Solution Overview: Homomorphic Routing

- **Homomorphic cryptosystem** for *address ranges in forwarding tables*
- *Sessions* begin with **INIT packet** containing *encrypted destination address*
- *Encrypted destinations match* with content of *encrypted forwarding tables* using **homomorphic operations**
- Subsequent *data packets forwarded* using encrypted **pre-computed paths** conveyed in *packet headers*
Solution Overview: Homomorphic Routing

RCs populate local forwarding tables in the EPFs with encrypted ranges.
Solution Overview: Homomorphic Routing

**EPFs perform INIT packet destination matching** with encrypted ranges via homomorphic operations – then *forward* the INIT packet between domains.
Solution Overview: Homomorphic Routing

The HEPS performs operations based on homomorphic encryption and distributes the required security parameters to relevant entities.
Solution Overview: Homomorphic Routing

After the session initialisation, data packets are transmitted from Src to Dest without further homomorphic encryption operations performed by the EPFs – encrypted path within packet headers.
Homomorphic Encryption

*Route Calculators* should **not have access** to *range* information

- *low* and *high* of each range are encrypted – **blinded** – by the *HEPS* using the *private key*
- RCs cannot obtain original plaintext for **blinded values** *low₁, high₁, low₂* and *high₂*
- **Randomised difference** when, e.g., *low₁* multiplied by *low₂* allows to check whether:
  
  \[
  \text{low}_1 \geq \text{low}_2 \text{ or } \text{low}_1 < \text{low}_2
  \]
Homomorphic Encryption

range_1 covers range_2

range_1 contiguous with range_2

range_1 intersects range_2

range_1 disjointed from range_2
Homomorphic Encryption

**Encrypted Packet Forwarders should not have access** to range information and destination addresses

- *low* and *high* of each range, as well as the *destination* address, are encrypted – **blinded**
- *Clients* retrieve *HE parameters* from the *HEPS* they can use to **self-blind** *destinations*
- *EPFs cannot obtain* original plaintext for *dst*, *low* and *high* **blinded values** in each table entry
- **Randomised difference** when *dst* is multiplied by *low* and *high* allows to check whether the address is **within** a range: *low* $\leq$ *dst* $\leq$ *high*
System Operation – **Step 1: Routing**

RC(A) verifies range signature – checks cover, intersection, contiguity or disconnection – updates the EPF’s forwarding table with aggregated range
Client retrieves **self-blinding HE parameters** from the HEPS and uses them to blind the destination within the *INIT packet* sent to domain A.
System Operation – Step 2: INIT

As the match is performed, the ESDP and EDSP are updated
Dest uses the fully constructed EDSP to send an **INIT-ACK** to Src that contains the ESDP to be used during the subsequent data transfer.
System Operation – Step 4: Data transfer

Same Session ID for all data packets – hop counter utilised as index to access elements of the ESDP to forward packet to the next hop domain.
Preliminary Evaluation

- *Paillier Partial HE* has better performance than *fully HE schemes*
- Additional **shift of computation** from HE *matching* to *encryption* – well suited to routing scenarios

- 142K IPv6 rules of a core domain **compressed** to 8K rules via our aggregation scheme
- Using a **2048 bits key** it takes **0.5ms** to **match** destination to **rule** via HE operations
- **10 checks** on average with **logarithmic search** – 5ms per **domain** per **flow** (initialisation)

- Further **optimisation** may be achieved using **dedicated hardware** and
- Considering **popularity** of destinations
Security Considerations

- **No party** can fully **decrypt** destinations or network paths – ASes only know the next hop AS.

- **ESDPs** and **EDSPs** based on **symmetric cryptography**
  - Private symmetric key **not shared** by an AS
  - Minimal size of ciphertext and improved **performance**
  - Symmetric algorithm is kept **secret** and depends upon a **salt** (session ID) – prevents brute-force attacks

- **Anonymised services**: network layer **does not enforce** that the destination has visibility of the source address

- **Signing of ranges** by **HEPS prevents** prefix hijacking
Deployment Considerations

- **Hop-by-hop** – not source routing
  - Clients **do not need to maintain** an up-to-date *network map*
  - **Implement** *BGP policies* – almost all *attributes*
  - *Intra- and inter-domain Traffic Engineering* still possible

- **Retrofittable** to *IPv6 packet headers*
  - *ESDP/EDSP* in the *source* and *destination address field* (or extension header)
  - *Session ID* and *hop counter* in the *flow label field*

- **HEPS** functionalities can be provided by *CAs* and *Internet registry*
  - **Multiple** organisations (~PKI) vs distributed deployment by **single** organisation
  - Acceptable **load**
    - *Clients* performs self-blinding
    - *RAs* to generate *100 new ranges per day globally on average*
Conclusions

- **Homomorphic routing** allows native **network level private connections** between *two end-points* with acceptable overhead.
- Intermediate ASes or eavesdroppers cannot identify communicating entities or the AS path.
- *Per-flow state* is **not needed** at intermediate routers/ASes.
- Possibility of **anonymised senders**: destinations **do not** need to **know** the address/identity of senders.
- *Intra* and *inter-domain* **Traffic Engineering** policies **can be maintained**.