Follow-up Discussion of Link security

Weiqiang Cheng, CMCC

Haojie Wang, CMCC

Lily Lyu, Huawei

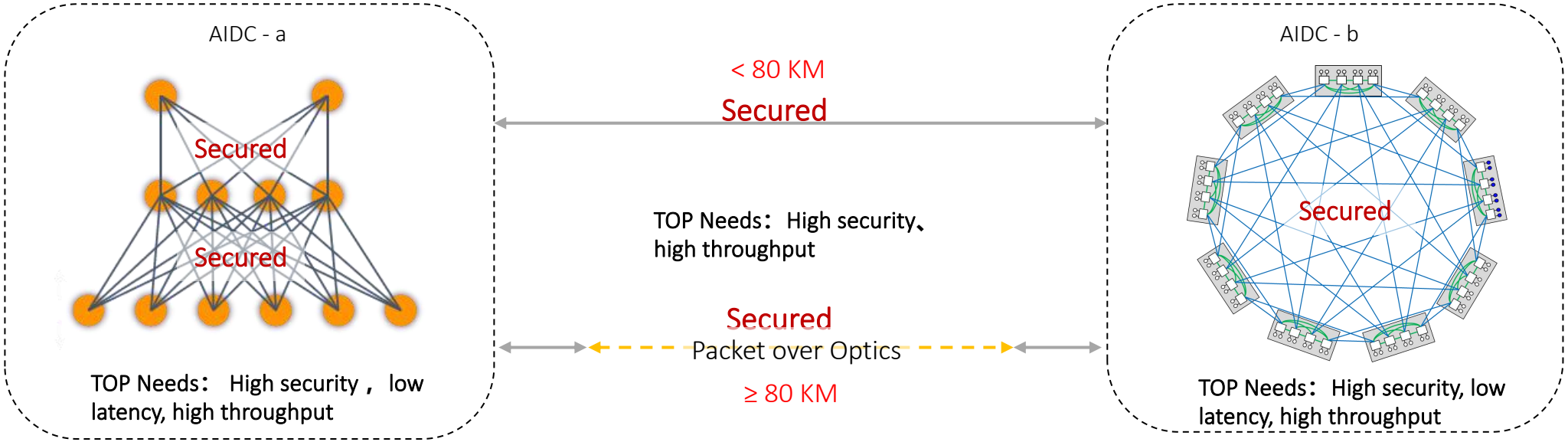
Recap

- Two contributions were presented in NENDICA
  - “New Requirements and Challenges of Network Link Security”
  - “Consideration on a new solution of network link security”
- The motivation is to encourage discussion on link level security for emerging scenarios, especially AI data centers.
- What we propose is to explore physical layer security to meet new requirements.
- This contribution intends to clarify and respond comments received previously, and make a conclusion in NENDICA.

Security expected by AI Data Centers

The expected security solution :

provide point-to-point link protection for both the interconnection within the AI data center (low latency & high throughput) and the interconnection between AI data centers (enhanced protection & high throughput)

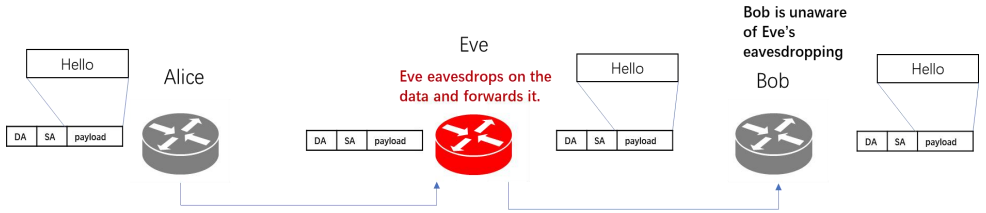


Security requirements	Inter-AIDC	Intra-AIDC
Enhanced protection (data protection + privacy protection)	Yes	Yes
Low latency		Yes
Low overhead	Yes	Yes

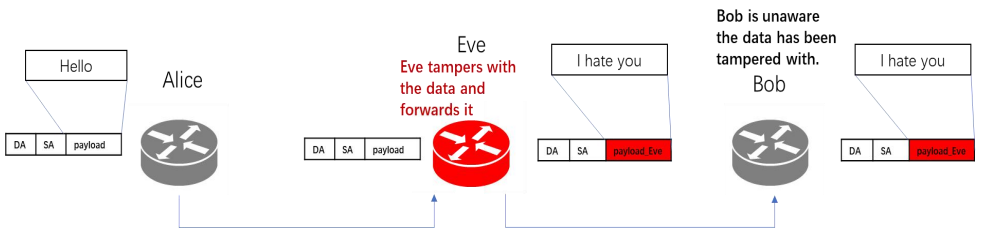
Challenges of existing Link Security

Link security aims at protecting data confidentiality and integrity

- L2 eavesdropping threatens data confidentiality

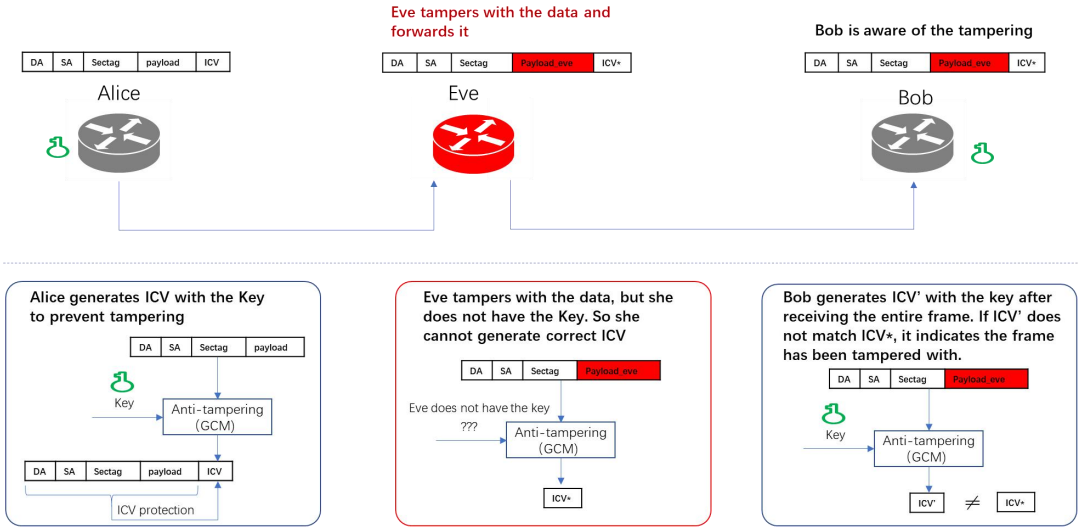


- L2 tampering threatens data integrity



MACsec protects data confidentiality and integrity using AES-GCM, but at the cost of increased latency and overhead

- Requires SecTAG and ICV, which introduces additional overhead.
- The receiver needs to collect the entire frame before performing ICV verification, increasing latency.

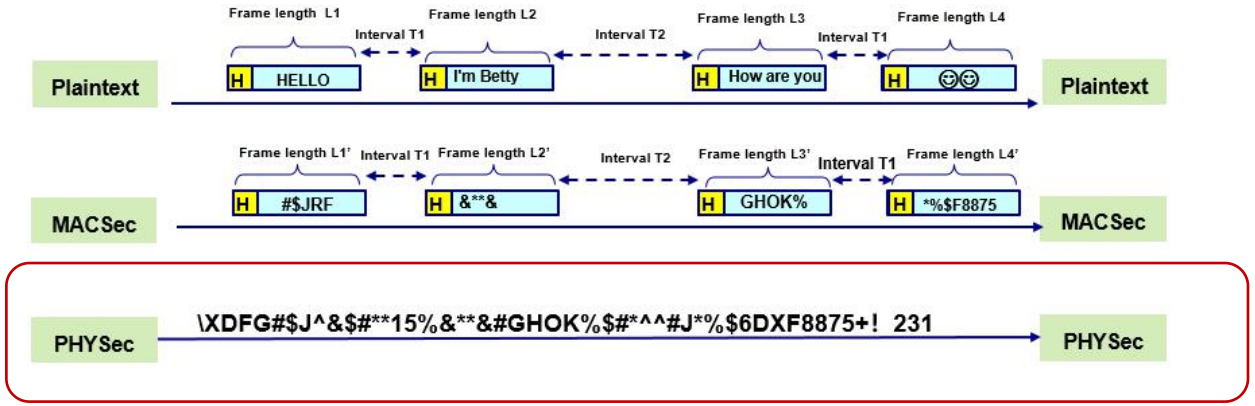


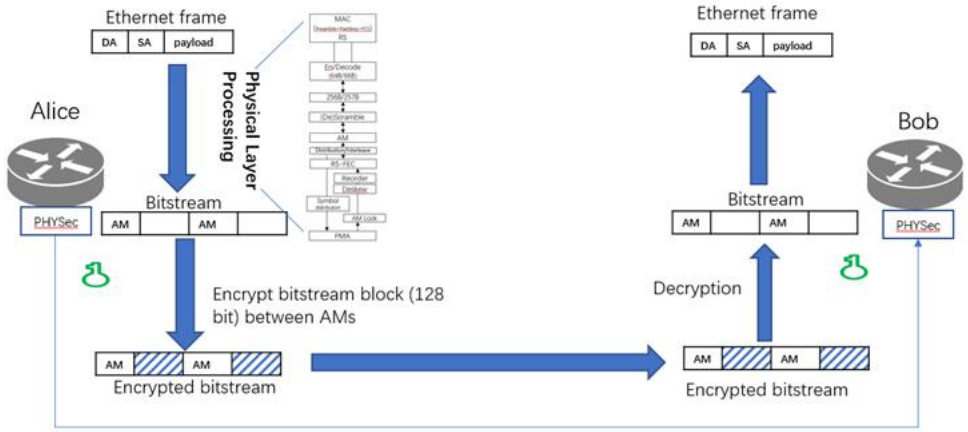
Have an impact on computing efficiency. latency >100ns@400G; bandwidth utilization 72.4%@64B

The addition of privacy protection introduces more latency and overhead.

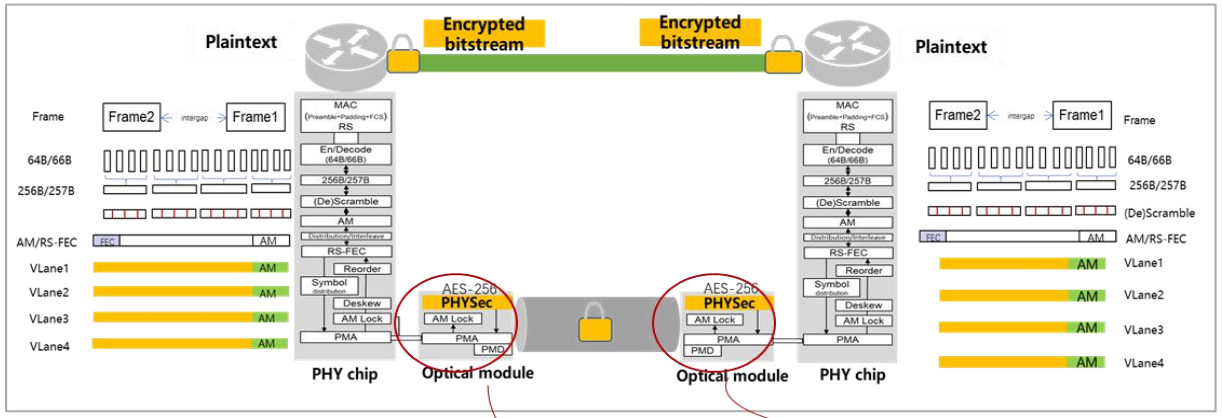
Proposed Solution-- PHYSec

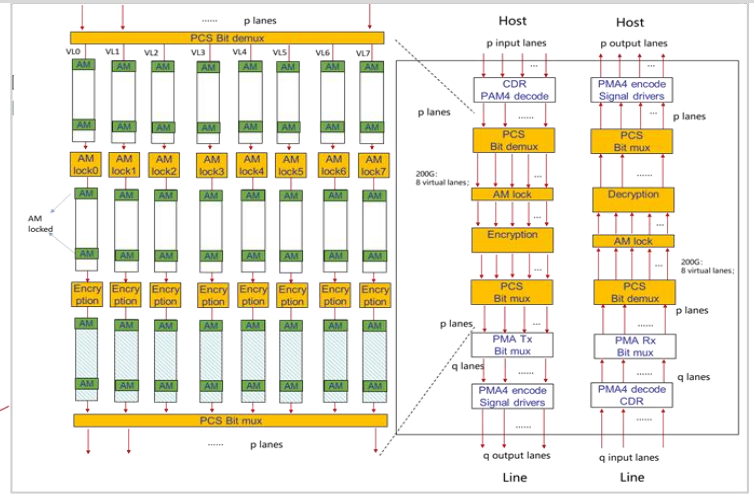
PHYsec is to protect link security on physical layer. It encrypts/decrypts bitstream blocks，hiding user data pattern, protecting user data confidentiality and integrity.





Physical layer processing and encryption/decryption

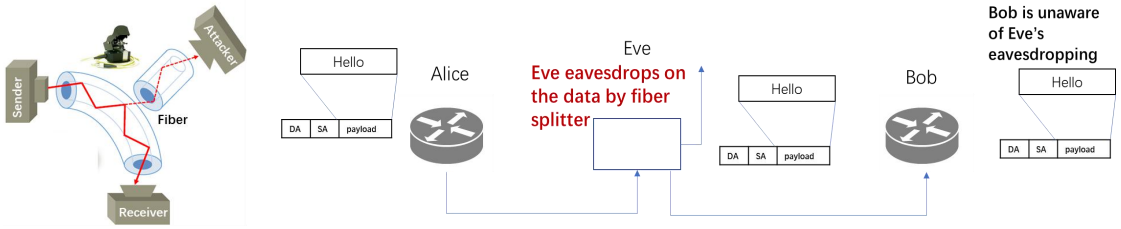




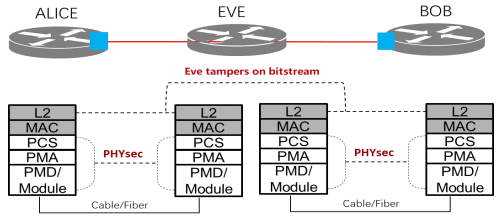
Link Security enabled by PHYSec

Link security aims at protecting data confidentiality and integrity

L1 eavesdropping threatens data confidentiality

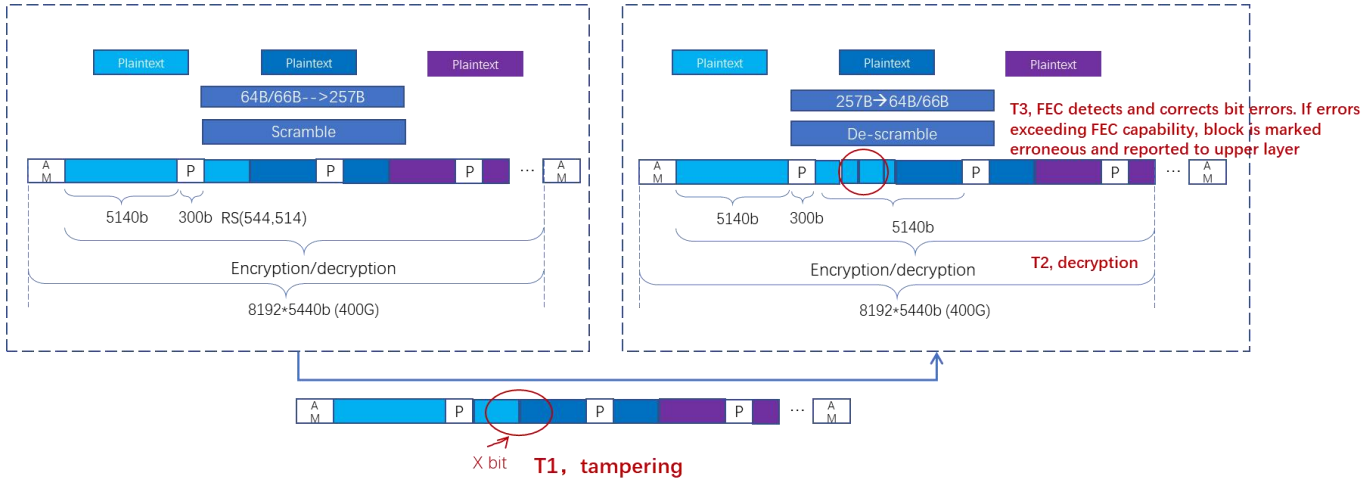


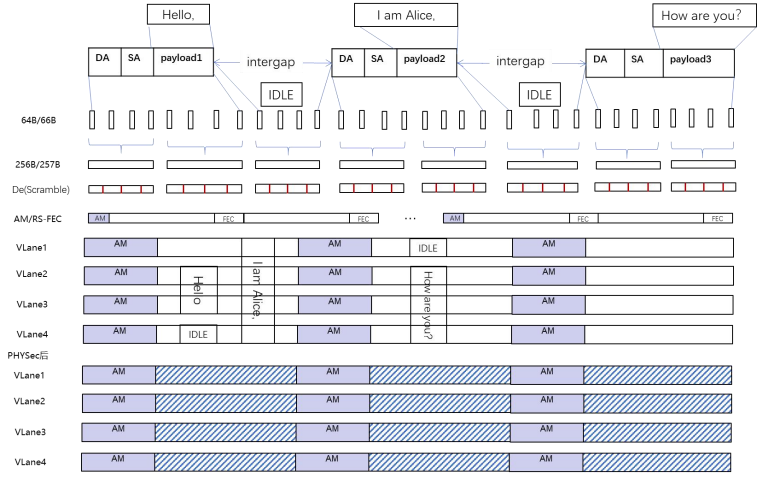
L1 tampering threatens data integrity



PHYsec protects data confidentiality and integrity using AES-256

- AES-256 ensures data confidentiality (the security of the AES algorithm is strong enough, with no reports of it being cracked so far) .
- Physical layer procedure is inherently sensitive to tampering, as it has the capability to detect and correct bit errors
- Furthermore, once the MAC layer frames and inter-gap are encoded at the physical layer, there is no clear correspondence, making it difficult to perform meaningful or precise tampering at the physical layer





PHYsec Meets AI Data Center Needs

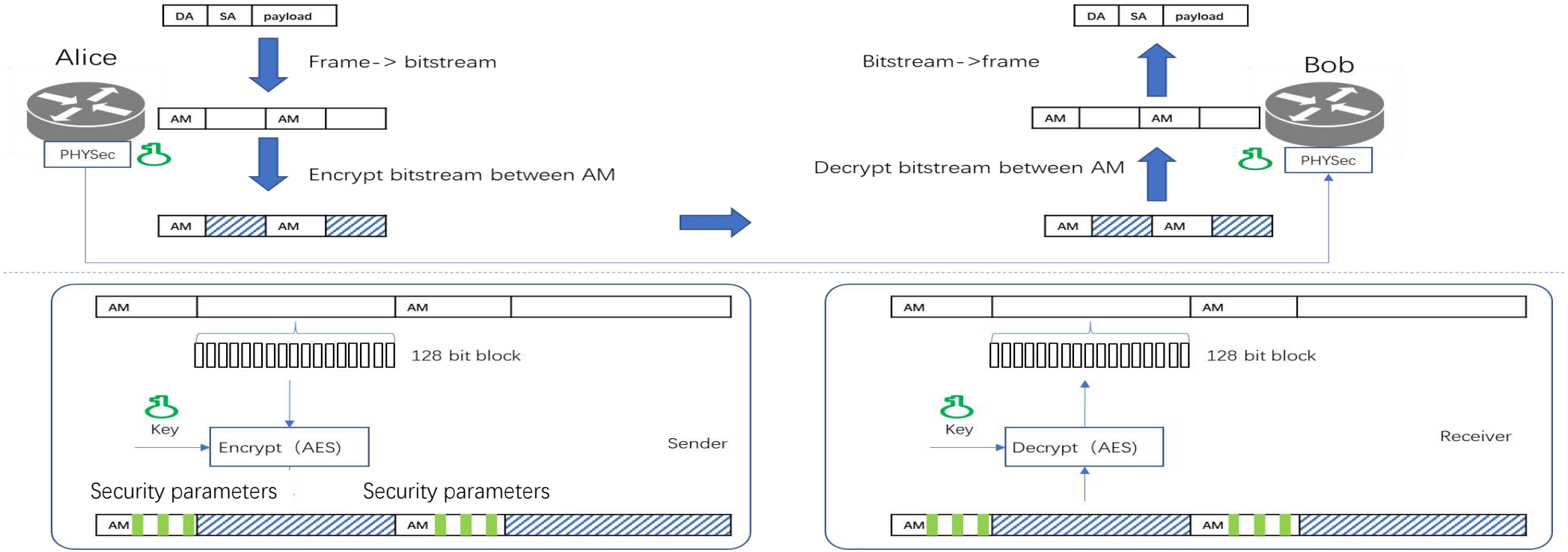
PHYsec: Enabling Low Latency, Low Overhead, and Enhanced Data Protection

✓ **Overhead advantage:**

En/Decryption parameters are carried within the physical layer's AM (Alignment Marker) fields, avoiding any consumption of user bandwidth.

✓ **Latency advantage:**

PHYsec does not perform ICV-based anti-tampering, allowing the receiver to decrypt then forward each 128 bits as it is received, without waiting for the entire frame.



7

Conclusion

- AI data centers need security solutions that balance high security, low latency, and low overhead.
- Existing security solutions do not fully meet these requirements, so PHYsec is proposed.
- PHYsec leverages physical layer technology, and, as suggested in a previous NENDICA meeting, further discussion will be considered in 802.3.