

PHY-Layer Security: Configurable non-binary polar codes

The invention presents a non-binary polar-coding framework to strengthen PHY-layer security. Unlike classic I/R/F-based wiretap schemes, which ensure information-theoretic secrecy only when Eve experiences a degraded channel relative to Bob, the proposed method adds computational hardening, keeping security even for similar channels and is especially well suited for real IoT deployments characterized by short-packet and tight resource constraints.



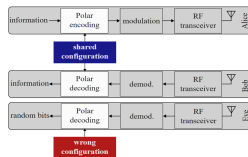
Channel Independent Physical Layer Security Enhancement

The model is a low-overhead PHY-layer confidentiality and hardening layer that shrinks the attack surface of real IoT deployments, especially short-packet and constrained links. When a Bob-Eve SNR gap exists, it recovers wiretap secrecy; when not, keyed configurability preserves robustness as a channel-independent alternative to I/R/F-only designs.

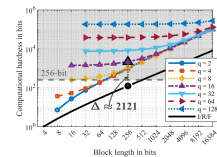
- 01 Beyond information-theoretic secrecy by computational hardening
- 02 Achieves beyond 256-bit security even at very small block lengths
- 03 Joint channel coding and security scheme eliminates the need for computational-intensive higher-layer security mechanisms
- 04 Maintains full bandwidth efficiency while enhancing security

REFERENCES:

- IEEE Xplore (2026): Generalized Non-Binary Polar Codes for Physical-Layer Security



Block diagram of the non-binary polar secured system.



Computational hardness of proposed Polar codes compared against the I/R/F approach. As can be seen, the hardness of the proposed scheme grows rapidly with both field size and block length and can exceed the 256-bit high-security threshold even at relatively short block lengths when the field size is sufficiently large.

CHALLENGE

Conventional cryptography relies on computational hardness and key management at higher layers, but its complexity clashes with strict cost and energy limits in IoT devices. Physical Layer Security (PLS) instead exploits channel noise and coding, using the same physical-layer resources for both error correction and secrecy. Conventional polar-code PLS wiretap schemes offer information-theoretic security only if Eve's channel is degraded versus Bob's—a highly restrictive requirement that limits their practical applicability.

INNOVATION

The scheme realizes PLS via a user-specific symbol-level configuration known to the transmitter Alice and intended receiver Bob but unknown to the adversary Eve. While binary polar codes offer only a small, performance-constrained configuration space, non-binary polar codes with non-Kronecker constructions and finite bi-right-quasigroup (FBRQ)-based arithmetic vastly enlarges this space. With a matched configuration and SCL decoding, Bob recovers the message, while Eve sees near-random outputs. The vast configuration space thwarts brute-force attacks, exceeding 256-bit high-security threshold even for short block lengths.

01 Basic principles observed · 02 Technology concept formulated · 03 Experimental proof of concept · 04 Technology validated in lab · 05 Technology validated in relevant environment · 06 Technology demonstrated in relevant environment · 07 System prototype demonstrated in operational environment · 08 System complete and qualified

TRL 08
TRL 07
TRL 06
TRL 05
TRL 04
TRL 03
TRL 02
TRL 01

Technology Readiness Level (TRL)

