

7th INTERNATIONAL CONFERENCE ON PUBLIC KEY INFRASTRUCTURE AND ITS APPLICATIONS (PKIA 2026) SEPTEMBER 10-11th, 2026

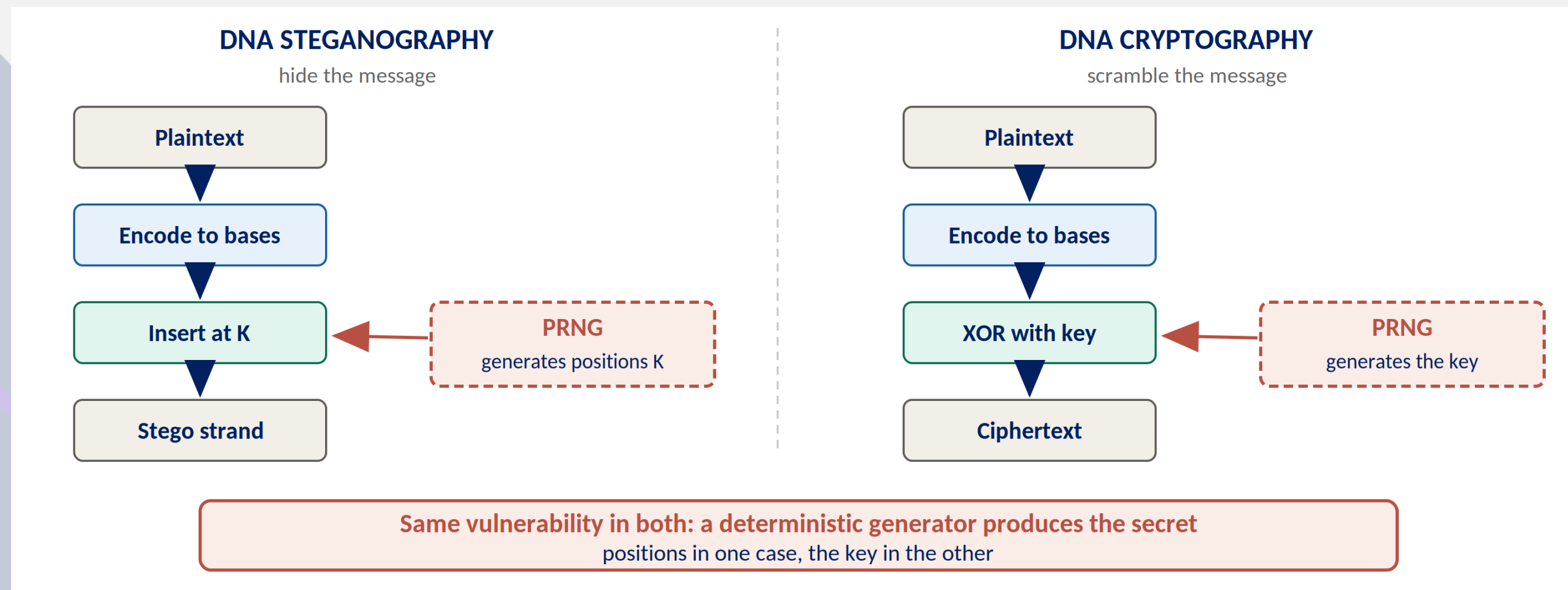
A Quantum Attack Pipeline on DNA-based Encryption

Anjali Tiwari, TRUST-STU, C-DAC Bengaluru | Mohammed Misbahuddin, TRUST-STU, C-DAC

Bengaluru

DNA-BASED SECURITY: THE FUNDAMENTALS

- Both schemes encode the message into DNA bases: 00=A 01=C 10=G 11=T
- Steganography** hides it at chosen positions. **Cryptography** scrambles it with a key



THE TERMS WE WILL USE

- **R_DNA** the cover strand, a message-free sequence. **K** the insertion positions, which are the key.
PRNG the generator that produces K

A worked example

message

HI

becomes bits

01001000 01001001

two bits at a time

C A G A C A G C

cover strand

R_DNA

T G A C T T G C A A T C G G A T C C A G T T A C G A T C G

positions

K = the key

3 9 16 22

chosen by the PRNG

stego strand

T G **C** A C T T G **A** C A A T C G **G** G A T C C **A** A G T T A C G

looks like ordinary DNA

THE IDEA: PREDICT POSITIONS FROM PERIODICITY

- If the generator repeats, the positions repeat, and the key becomes predictable

A PRNG is deterministic

seed $\rightarrow$ $x_1, x_2, x_3, x_4, \dots$

Same seed, same sequence, every time.

Given enough output, the seed is recoverable.

So the attack is

observe positions $\rightarrow$ find the period

$\rightarrow$ recover the seed $\rightarrow$ predict all positions

The hidden message follows.

Finding a hidden period is exactly what quantum period finding does

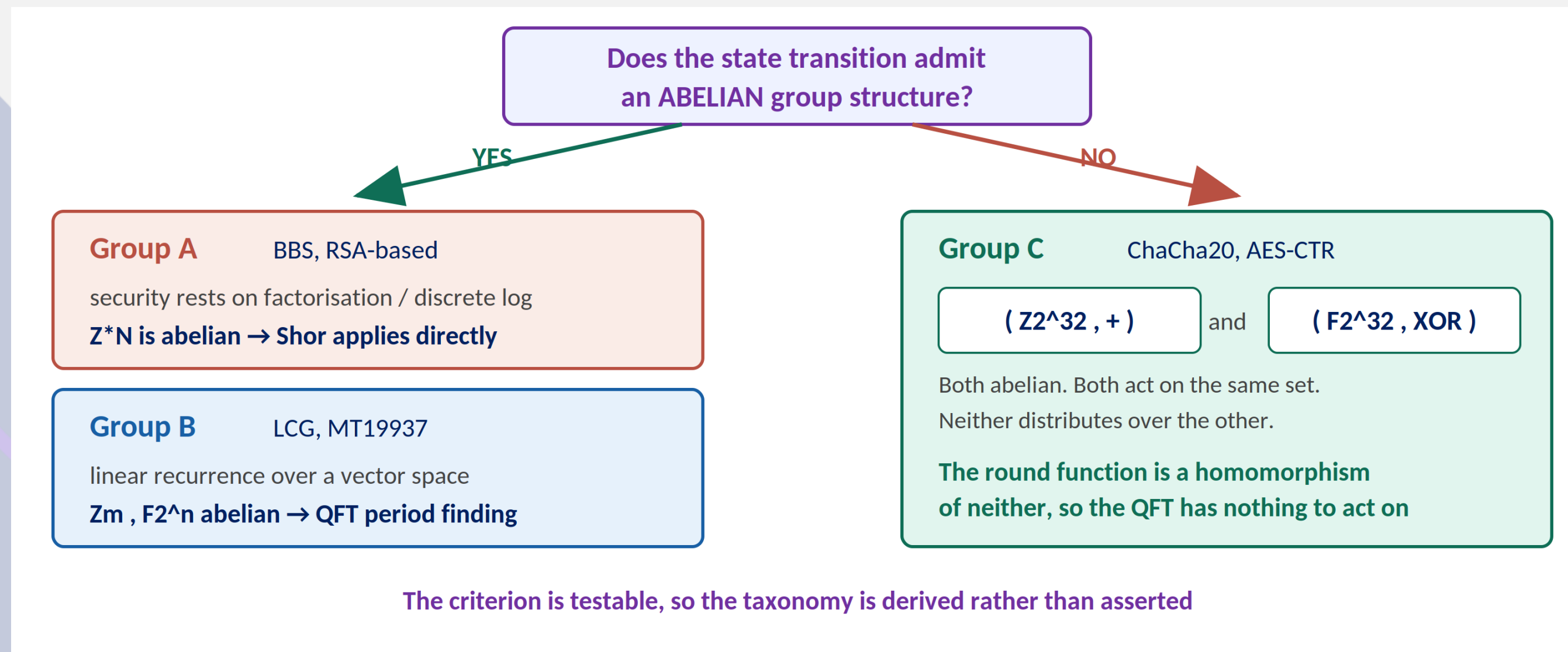
Shor and Simon are both special cases of the hidden subgroup problem

So the question becomes: which generators actually expose a period

that a quantum algorithm could find?

WHICH GENERATORS EXPOSE A PERIOD?

- Quantum advantage needs an **abelian** structure [Simon 1997, Kitaev 1995]



HOW WE TESTED IT

- **Cipher** ChaCha20, the most widely deployed ARX construction (TLS 1.3, WireGuard, Signal)
- **Variable** round count, swept from 2 up to the full 20, everything else held fixed
- **Question** at each round count, is there any detectable repetition in the output?
- **Controls** true randomness as a negative control, 2-round output as a positive control, and RFC 8439 vectors to verify the implementation

WHAT WE FOUND

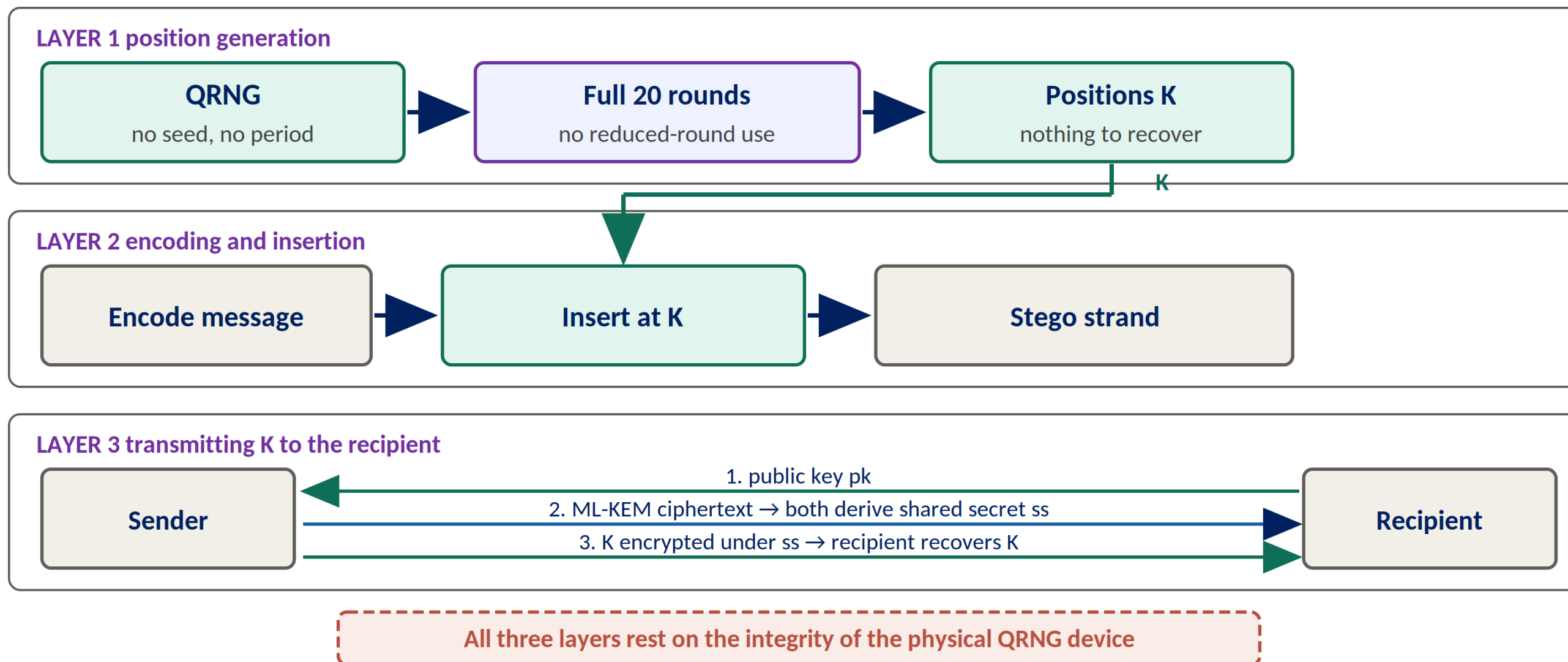
- **At 2 rounds** structure is obvious. Every autocorrelation lag fires. The method works
- **By 4 rounds** nothing. Diffusion has removed any detectable repetition
- **At 20 rounds** full-round ChaCha20 is statistically indistinguishable from true randomness, confirmed by NIST SP 800-22 and a distributional comparison
- **The threshold was calibrated against known-random data rather than assumed**

WHAT THIS MEANS

- **Established** classical statistical screening cannot resolve whether structure exists in full-round ChaCha20 at this scale
- **Not established** absence of detectable structure is not absence of structure, and nothing here bears on quantum security
- **This is a statement about the instrument, not about the cipher**
- It is also why a threshold-free method such as the QFT remains worth asking about

THE PROPOSED DEFENSE

- If the seed is the vulnerability, remove the seed



OPEN PROBLEMS AND CONCLUSION

- **Oracle access** quantum period finding needs a function evaluable in superposition; an adversary sees only output
- **Approximate periodicity** weak statistical repetition is not an exact period, and no speedup is known to transfer
- **Observation for ARX** at full rounds there is no recurrence to observe in the first place
- **Establishing the absence of exploitable structure requires calibrated instruments**

KEY REFERENCES

Quantum algorithms

- Shor, SIAM J. Comput. 26(5), 1997. Grover, STOC 1996. Simon, SIAM J. Comput. 26(5), 1997.
- Kitaev, arXiv quant-ph/9511026, 1995. Childs and van Dam, Rev. Mod. Phys. 82(1), 2010.
- Kaplan et al., CRYPTO 2016. Grassl et al., PQCrypto 2016.

DNA cryptography and steganography

- Clelland, Risca and Bancroft, Nature 399, 1999. Sukumaran and Misbahuddin, IJNS 20(3), 2018.
- Aljahdali and Al-Harbi, PeerJ Comput. Sci. 9, e1379, 2023.

Ciphers, randomness and standards

- Bernstein, SASC 2008. RFC 8439, IETF 2018. Ljung and Box, Biometrika 65(2), 1978.
- NIST SP 800-22 Rev 1a. NIST FIPS 203, 2024. Wasserstein and Lazar, Am. Stat. 70(2), 2016.

THANK YOU