

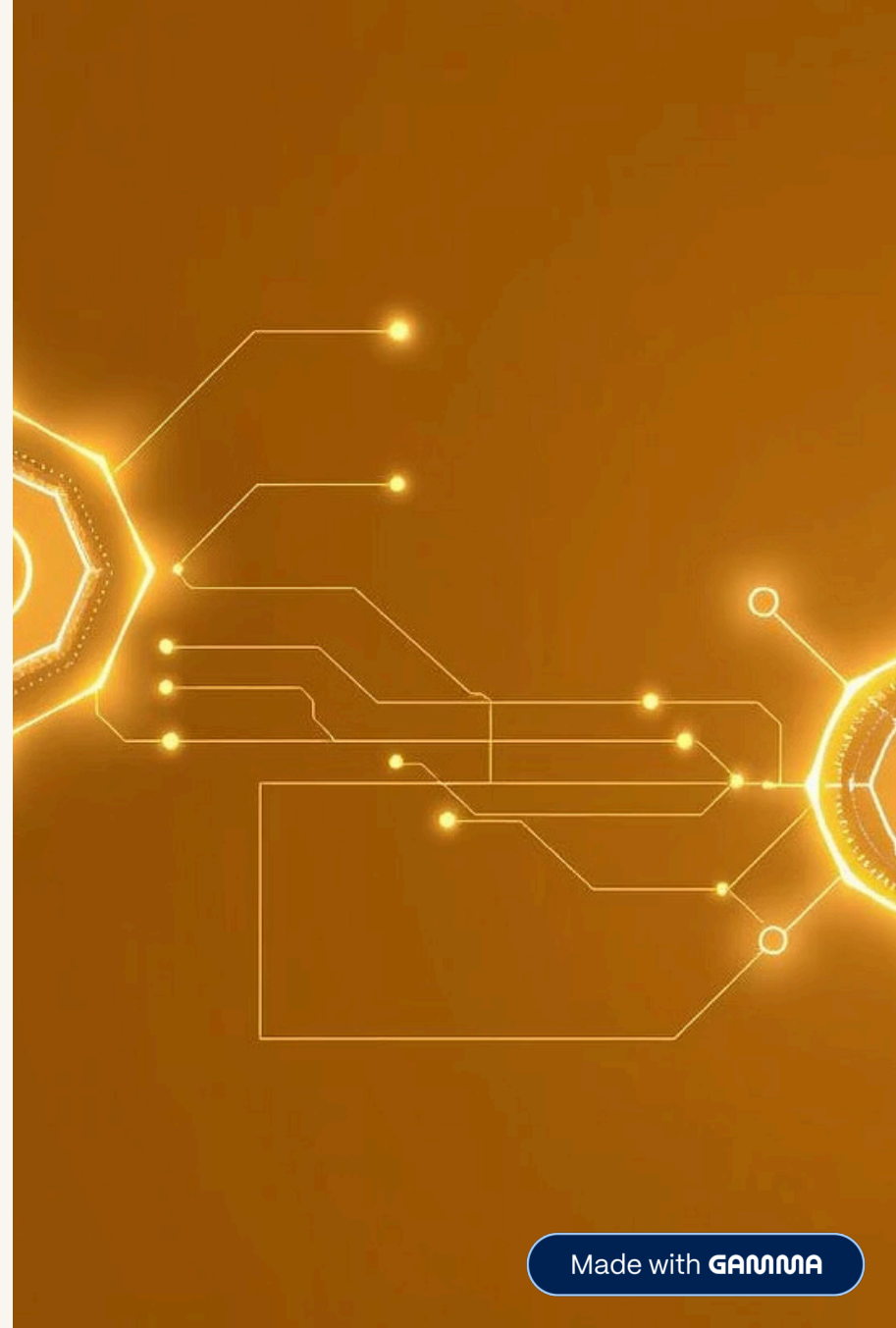
# A New Approach to Cryptographic Algorithms for the Quantum Era

Leveraging Natural Language Processing for Quantum-Resistant Encryption

Zahra Dorostkar

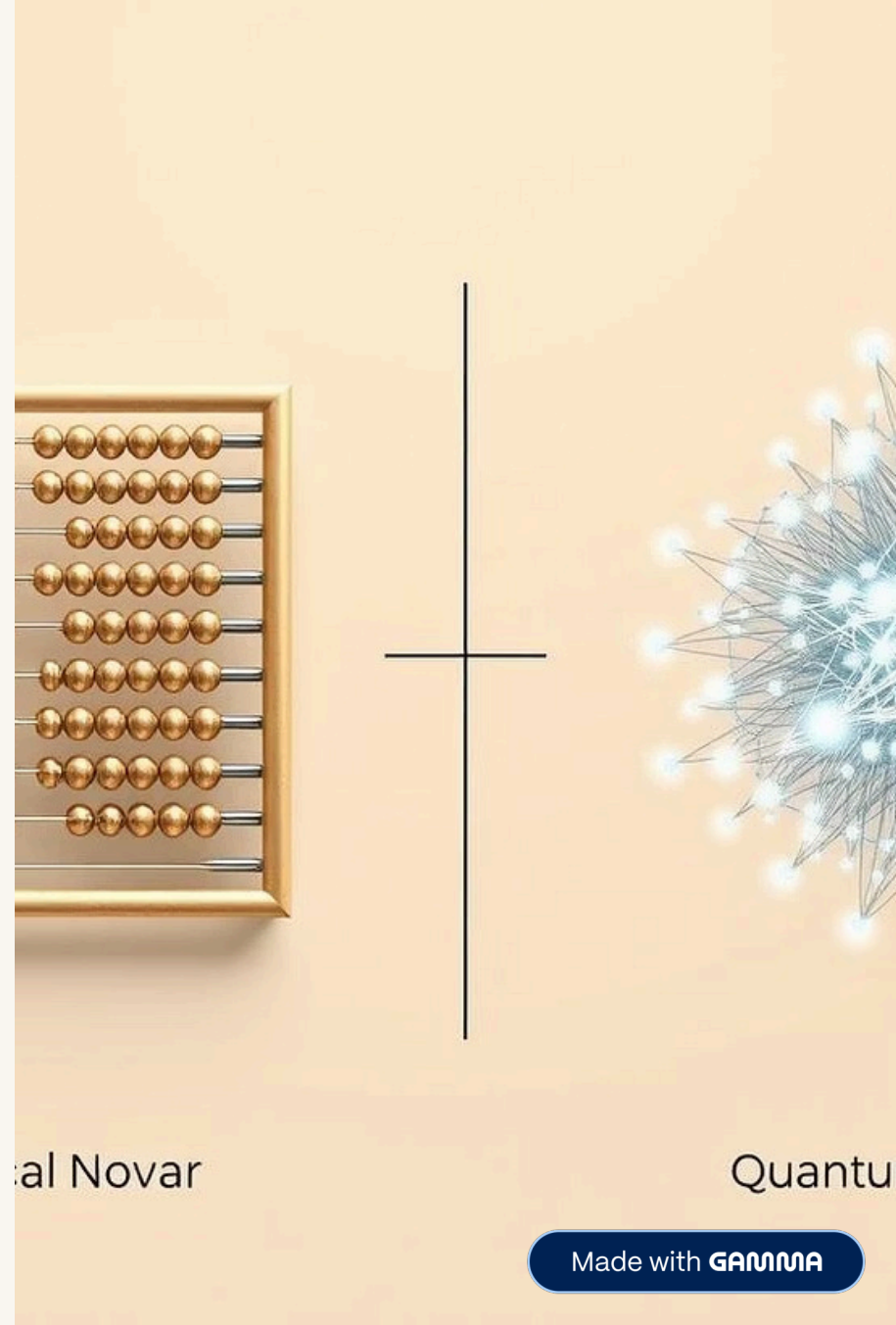
*Skolkovo Institute of Science and Technology*

*July 2025*



# The Quantum Threat to Classical Cryptography

Quantum computers pose a significant threat, capable of factoring large numbers exponentially faster than classical systems and also can break algorithms based on the difficulty of computing discrete logarithms in a finite field. This advancement directly compromises widely used encryption algorithms like RSA and elliptic curve cryptography, jeopardizing our digital infrastructure.



al Novar

Quantu

# Current Post-Quantum Cryptography Landscape



## Quantum Key Distribution (QKD)

Utilizes quantum mechanics for secure key exchange.



## Lattice-Based Cryptography

Relies on the hardness of problems on mathematical lattices.



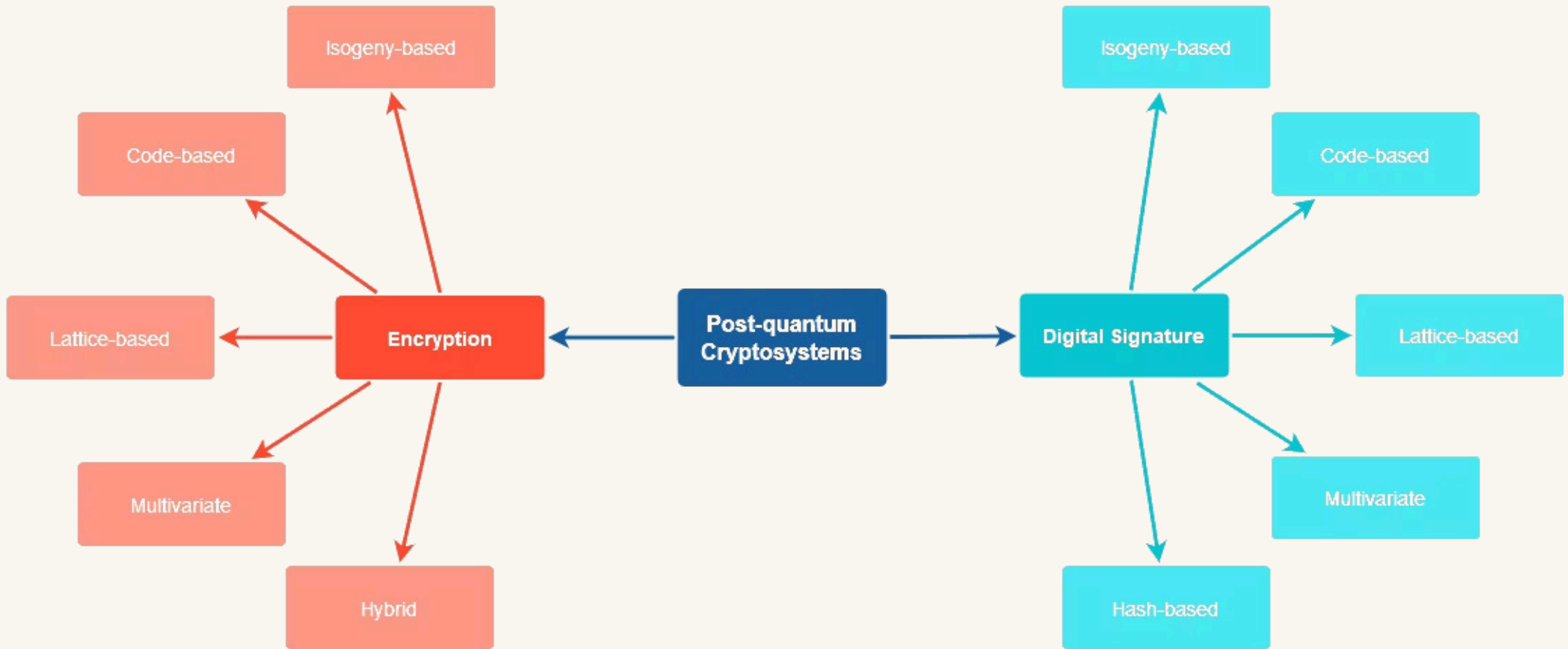
## Code-Based Cryptography

Leverages error-correcting codes for encryption.



## Multivariate Cryptography

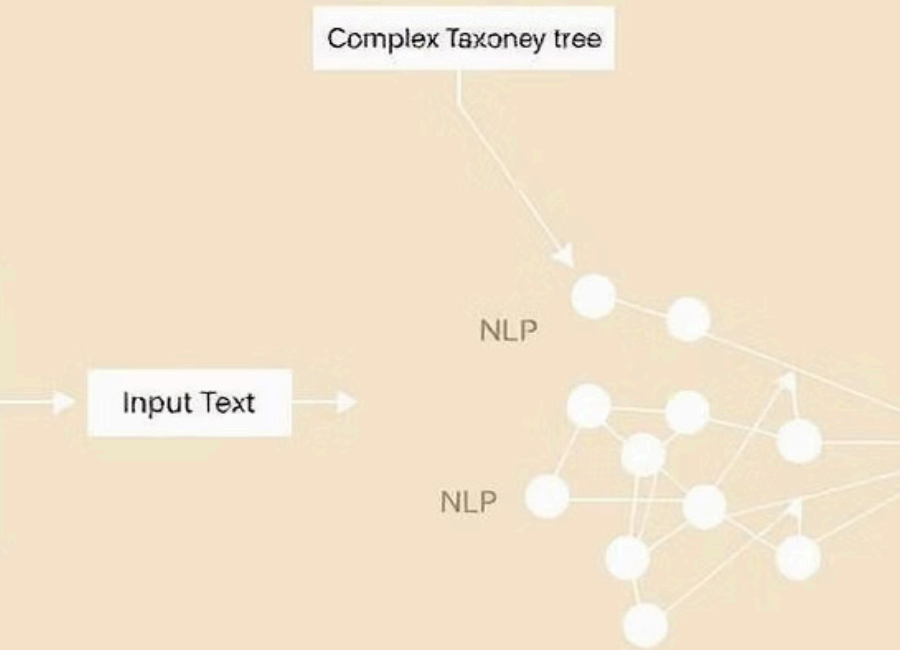
Based on solving systems of multivariate polynomial equations.



# Limitations of Existing Quantum-Resistant Solutions

- **Lattice-Based:**
  - Key Size
  - Performance Overhead
  - Complexity
- **Code-Based:**
  - Key Size
  - Key Management
  - Worst-case Scenario
- **Group-based:**
  - Computational Overhead
  - Limited Applicability
  - Key Management





# Introducing Secure Linguistic Encryption (SLE)

SLE represents a paradigm shift, employing natural language processing to construct robust, quantum-resistant encryption. By leveraging the inherent complexity and ambiguity of human language, SLE offers a novel defense against future quantum threats.

# Leveraging NLP to Create a Quantum-Resistant Encryption Key

Secure Linguistic Encryption utilizes several advanced Natural Language Processing techniques to construct robust, context-aware cryptographic keys. By understanding the intricate layers of human language, SLE generates dynamic keys that are inherently resilient to quantum computing threats.

## Taxonomy creation

We use NLP to create a taxonomy of words and phrases, which can be used to generate a highly structured and complex encryption key.

## Semantic analysis

We use NLP to perform semantic analysis on the input text, which can help us identify the underlying meaning and context of the text.

## Word embeddings

We use NLP to create word embeddings, which can help us represent words and phrases as vectors in a high-dimensional space.

## Dynamic key generation

We use NLP to generate encryption keys dynamically, based on the input text and the context in which it is being used.

# SLE's Intrinsic Quantum Resistance

The inherent complexity and ambiguity of natural language form SLE's core defense against quantum adversaries. Unlike numerical problems, linguistic intricacies resist brute-force quantum analysis, ensuring persistent security.

1

## Linguistic Complexity

Quantum computers struggle with the vast, non-linear structures of human language.

2

## Semantic Ambiguity

Determining precise meaning and context defies algorithmic exploitation, even with quantum aid.

3

## High Entropy

Natural language has high entropy, making it an ideal source of randomness for generating encryption keys.

# The advantage of utilizing NLP

In the context of post-quantum cryptography, the main advantage of introducing an NLP-based cryptosystem could be in the area of ***Key Management***. Natural language processing techniques have the potential to offer innovative solutions for key generation, distribution, and management, which are critical aspects of cryptographic systems. By leveraging NLP in this area, it may be possible to enhance the scalability, security, and efficiency of key management processes.

# Conclusion

Our project aims to revolutionize post-quantum cryptography by leveraging natural language processing techniques. By introducing this scheme, we enhance key management, optimize performance, and increase system security. Our algorithm design process, from problem definition to implementation, testing, and optimization, underscores our commitment to innovation and excellence. We are excited about the potential of our NLP-based cryptosystem to shape the future of cryptographic systems and invite further exploration and discussion in this groundbreaking field.

# Future Work

Our roadmap for Secure Linguistic Encryption (SLE) focuses on advancing its capabilities and ensuring widespread adoption:

- **Research and Validation:** Conduct further in-depth research to rigorously assess and enhance SLE's security and efficiency across diverse real-world scenarios and attack vectors.
- **Protocol Development:** Develop a comprehensive suite of SLE-based cryptographic protocols designed for various applications, including secure communication, data storage, and digital signatures.
- **System Integration:** Facilitate seamless integration of SLE with existing widely-used cryptographic systems and platforms to ensure broader adoption and interoperability within current digital infrastructures.



# Thank You

For your attention

Contact me: [zahradorostkar68@gmail.com](mailto:zahradorostkar68@gmail.com)

