Qrypthaven Overview

(Software only)

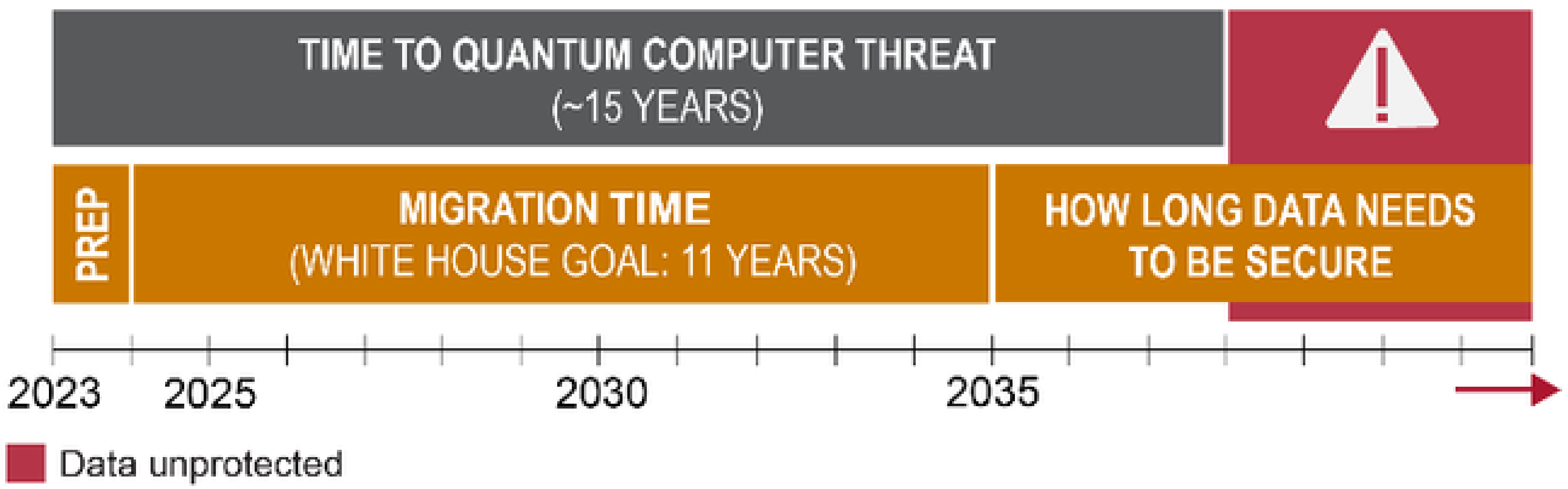
qrypthaven.com

INTRODUCTION

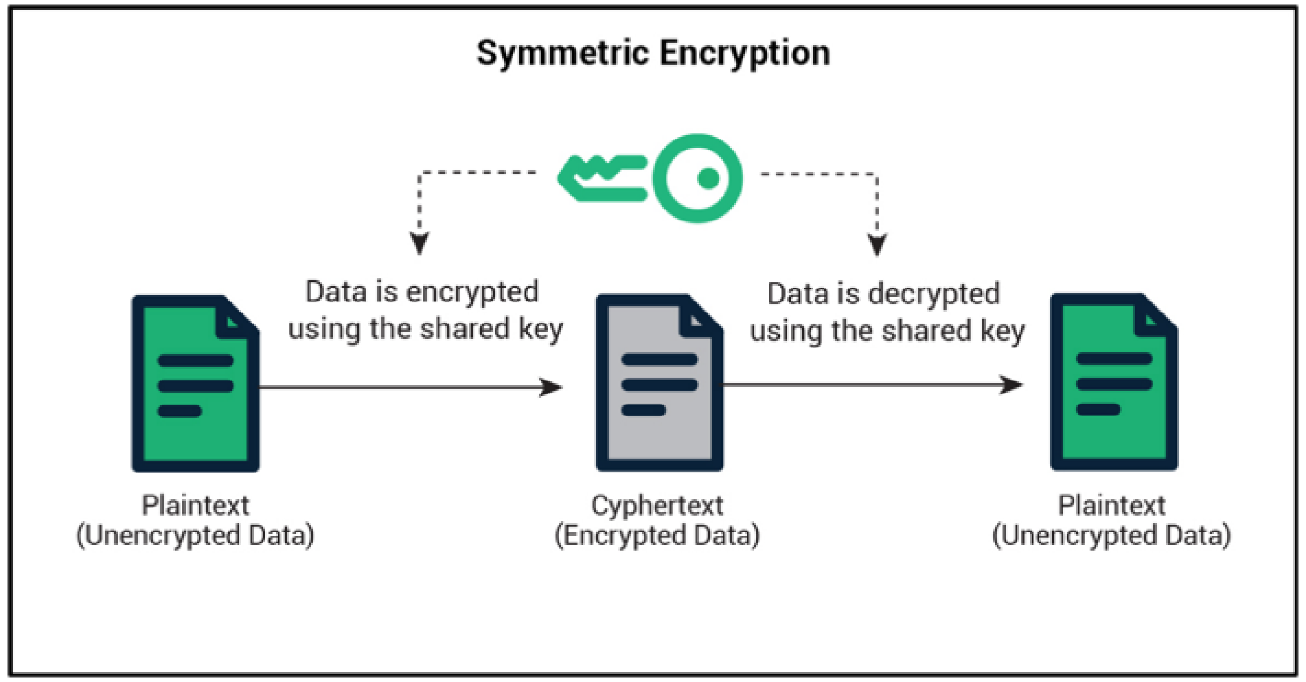
Addressing key challenges in the quantum computing industry and covering related cryptography topics at a high-level + qrypthaven's solution.

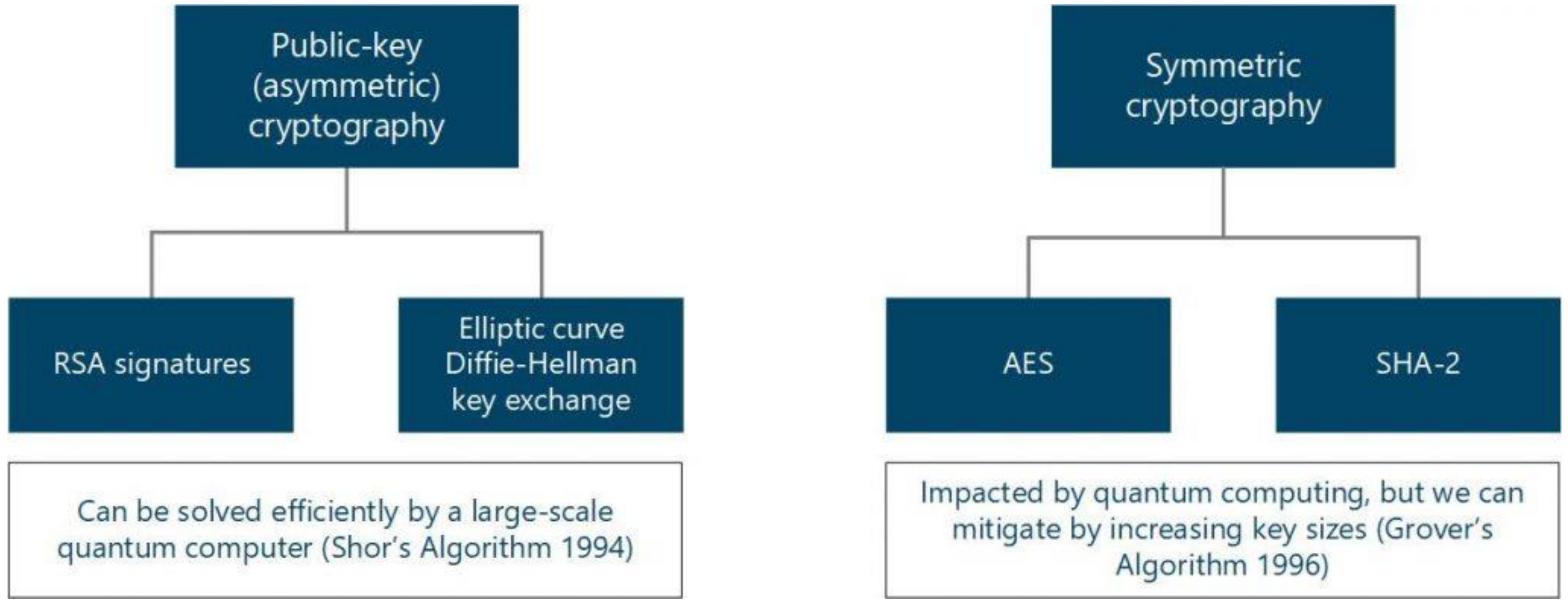
PROBLEM AT HAND

If quantum-resistant encryption isn't in place by the time quantum computers become a practical reality, any data encrypted with old standards could be retroactively decrypted, potentially leading to breaches of sensitive information.



Source: GAO adaptation of Mosca's theorem. | GAO-23-106559





BACKGROUND OF THE STUDY + PRODUCT

Our preliminary research was based on finding a solution that allowed the average citizen to utilize quantum-resistant solutions.

By understanding quantum computing functionality, PQC algorithms, and possible integrations, we aimed to understand and unlock the widespread potential of quantum-resistant devices, applications, and software applications.

qrypthaven.com

Bliss Algorithm

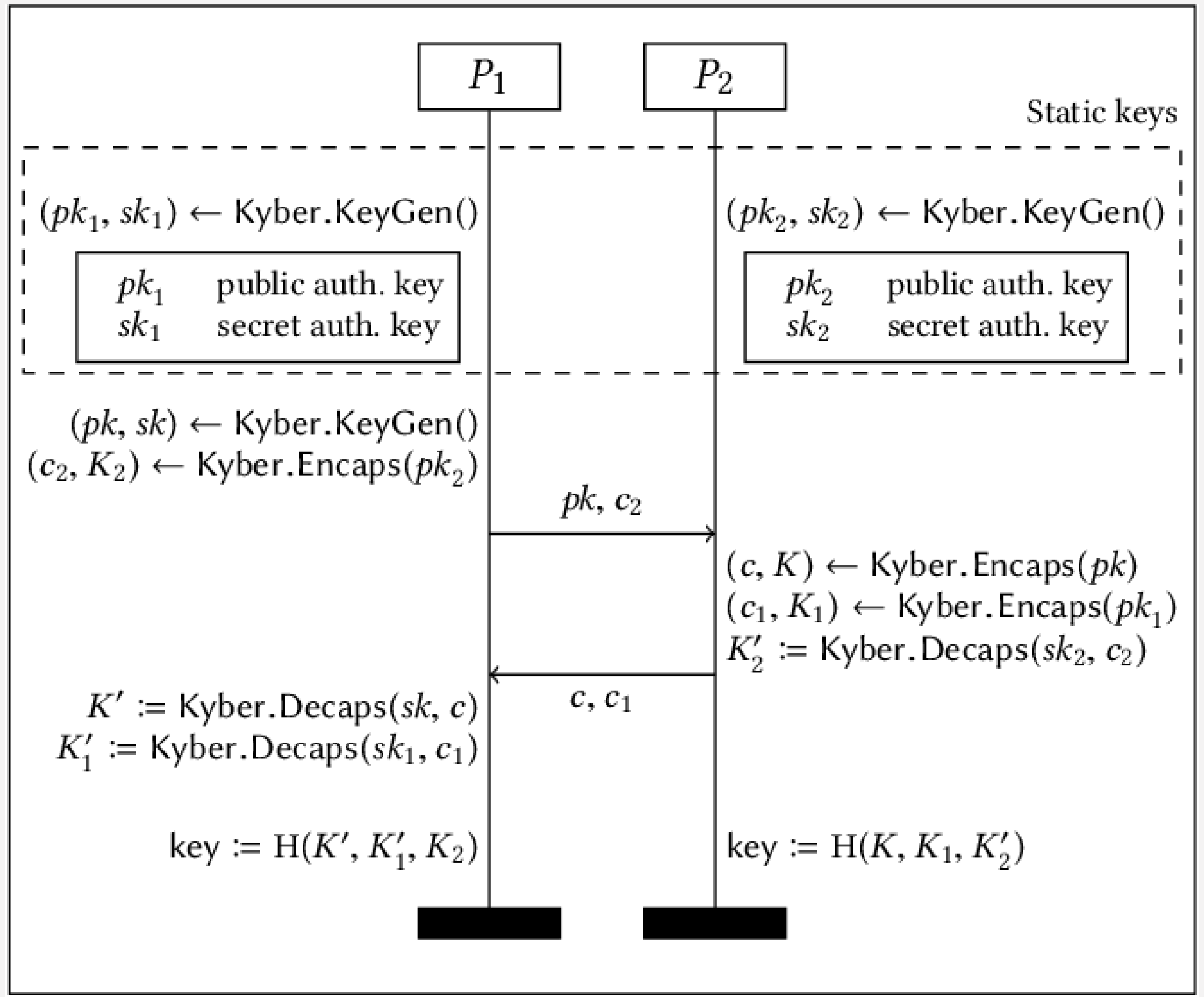
Algorithm 2.2. BLISS Signature Algorithm

Input: Message μ, public key $\mathbf{A} = (\mathbf{a}_1, q-2)$, secret key $\mathbf{S} = (\mathbf{s}_1, \mathbf{s}_2)$
Output: A signature $(\mathbf{z}_1, \mathbf{z}_2^\dagger, \mathbf{c}) \in \mathbb{Z}_{2q}^n \times \mathbb{Z}_p^n \times \{0,1\}^n$ of the message μ

$\mathbf{y}_1, \mathbf{y}_2 \leftarrow D_{\mathbb{Z}^n,\sigma}$
$\mathbf{u} = \zeta \cdot \mathbf{a}_1 \cdot \mathbf{y}_1 + \mathbf{y}_2 \bmod 2q$
$\mathbf{c} = H(\lfloor \mathbf{u} \rceil_d \bmod p, \mu)$
choose a random bit b
$\mathbf{z}_1 = \mathbf{y}_1 + (-1)^b \mathbf{s}_1 \cdot \mathbf{c} \bmod 2q$
$\mathbf{z}_2 = \mathbf{y}_2 + (-1)^b \mathbf{s}_2 \cdot \mathbf{c} \bmod 2q$
continue with a probability based on σ, $\|\mathbf{Sc}\|$, $\langle \mathbf{z}, \mathbf{Sc} \rangle$ (details in [9]), **else** restart
$\mathbf{z}_2^\dagger = (\lfloor \mathbf{u} \rceil_d - \lfloor \mathbf{u} - \mathbf{z}_2 \rceil_d) \bmod p$
return $(\mathbf{z}_1, \mathbf{z}_2^\dagger, \mathbf{c})$

https://www.semanticscholar.org/paper/CRYSTALS-Kyber%3A-A-CCA-Secure-Module-Lattice-Based-Bos-Ducas/a57342d25e255b75a469a8ebc990cb136c6bf2e1/figure/4

Crystals-Kyber Algorithm



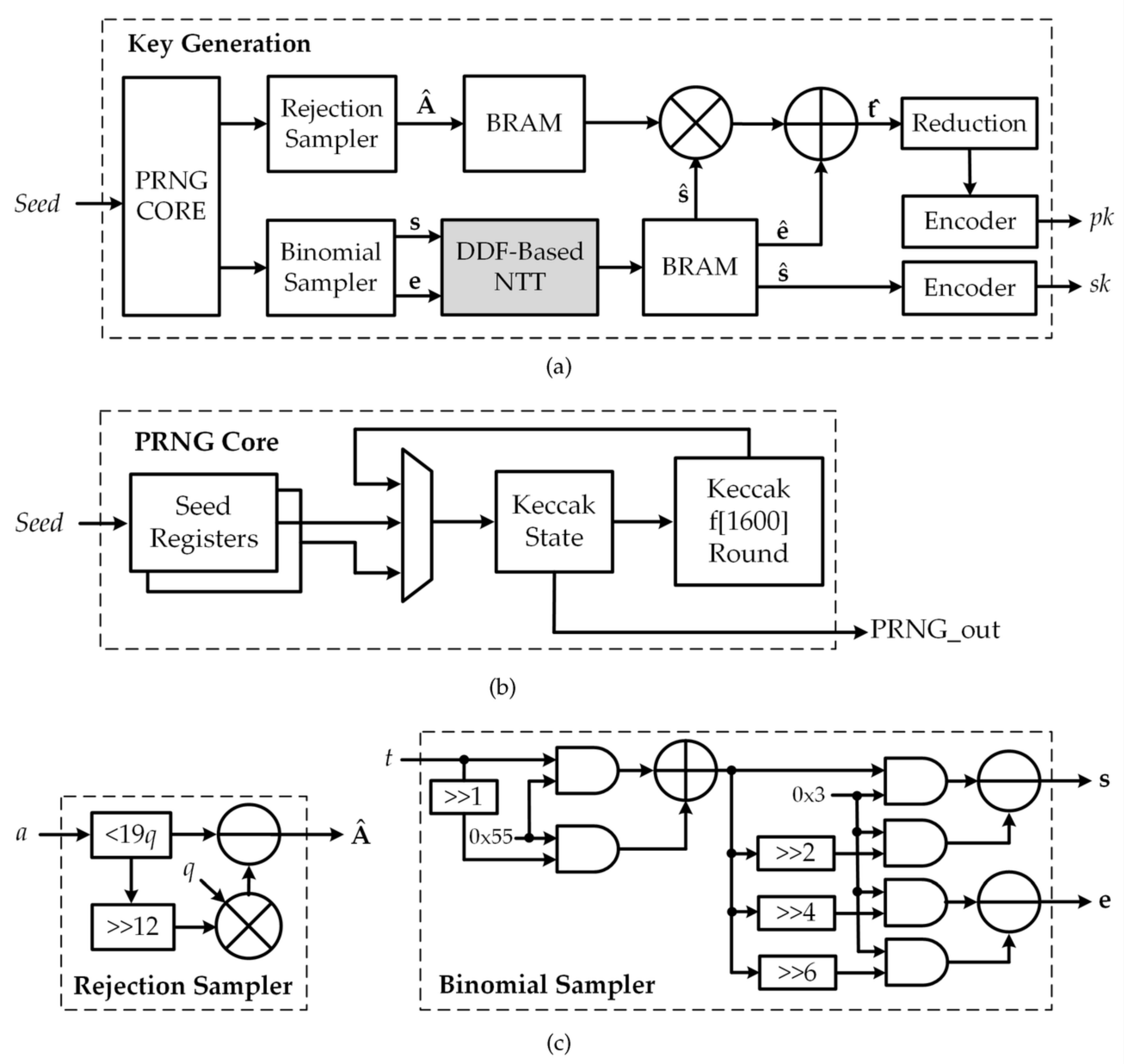
FRAMEWORK / METHODOLOGY

EARLY PLANS

Due to the limited variety of PQC algorithms, we designed prototypes and integrated viable options to test out the specific algorithms that were most suitable.

QUANTITATIVE METHODS

We conducted research methods that involved analyzing numerical data to quantify relationships, encryption times, and usability. After rigorous testing, we decided that the Bliss algorithm (not-NIST approved) and the Crystals-Kyber algorithm (NIST approved) were the most suitable options for our goal.

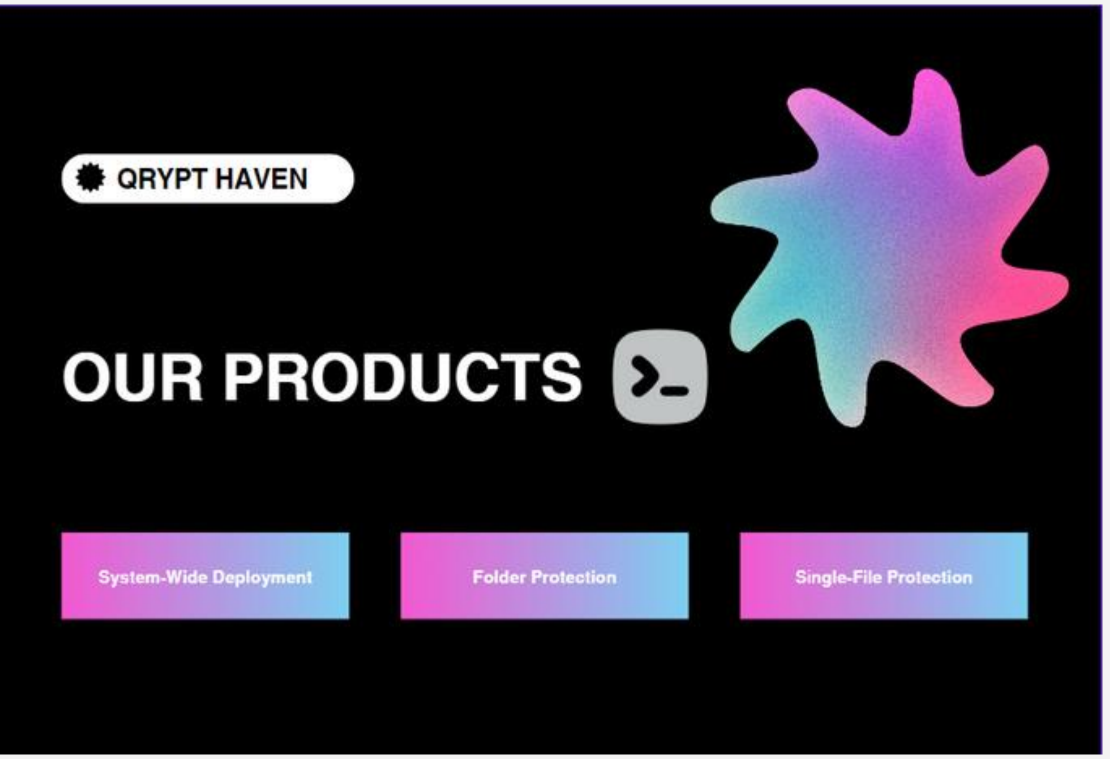


CRYSTALS-KYBER

KEY ENCAPSULATION METHODOLOY

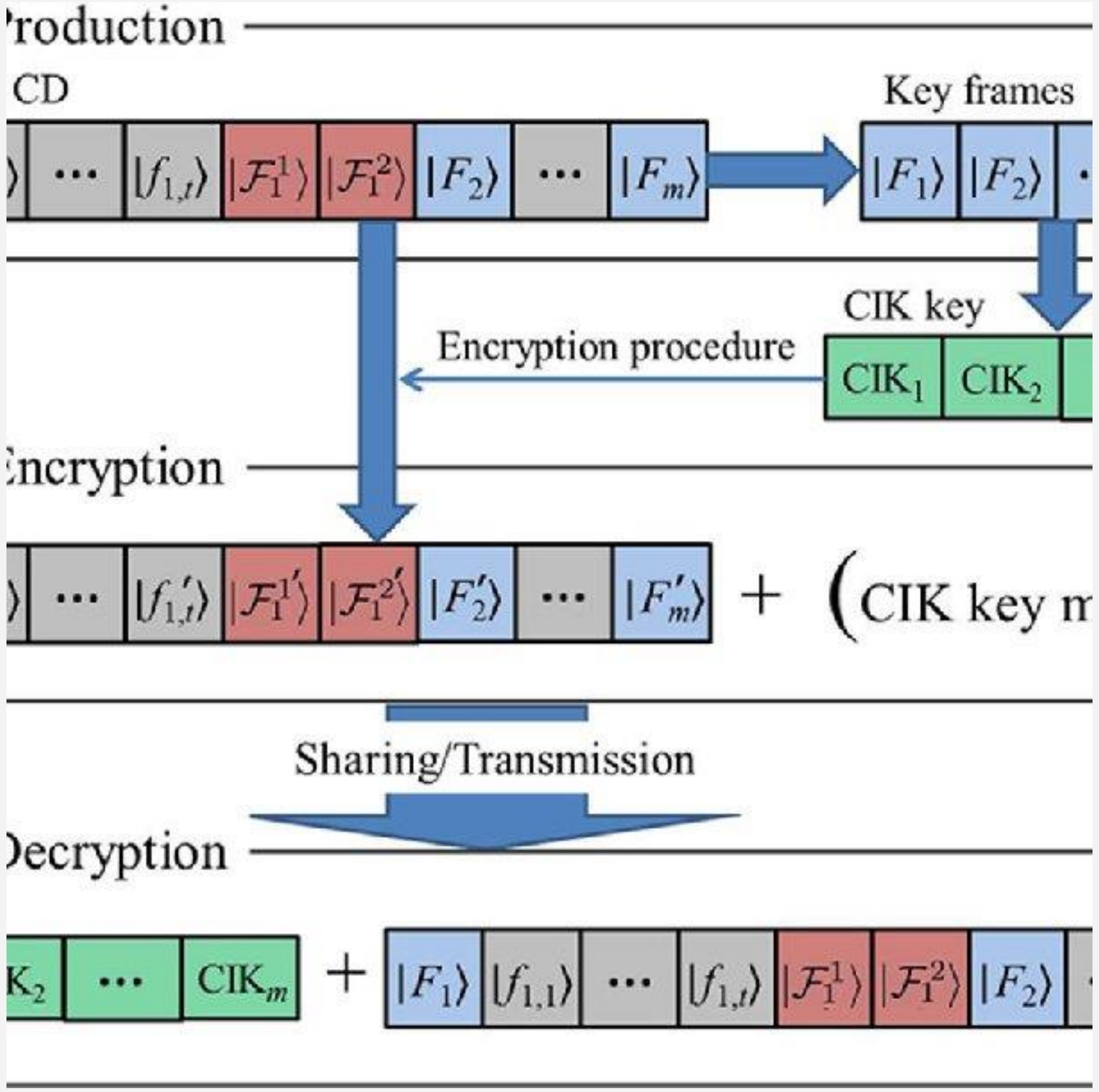
1. Pseudorandom Number Generator (PRNG) Core
2. Rejection Sampler
3. Binomial Sampler
4. DDF-Based NTT
5. BRAM
6. Reduction and Encoder

Whitepaper: https://ieeexplore.ieee.org/document/8406610



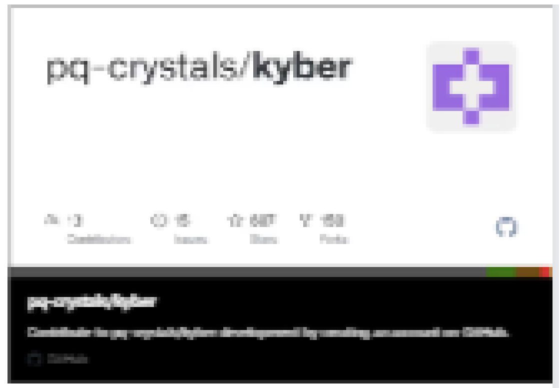
Prototype (Working)

FRAMEWORK / METHODOLOGY

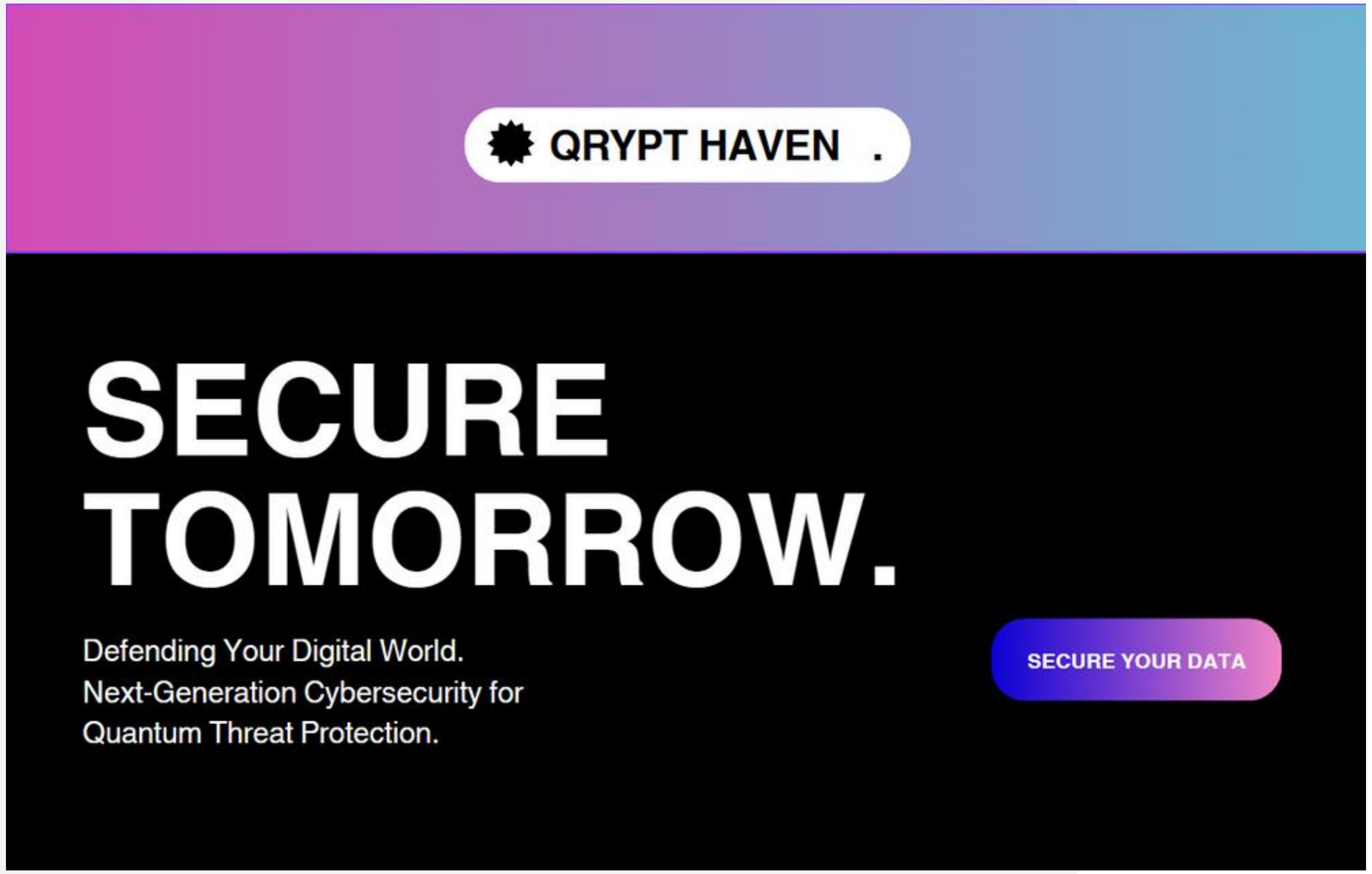


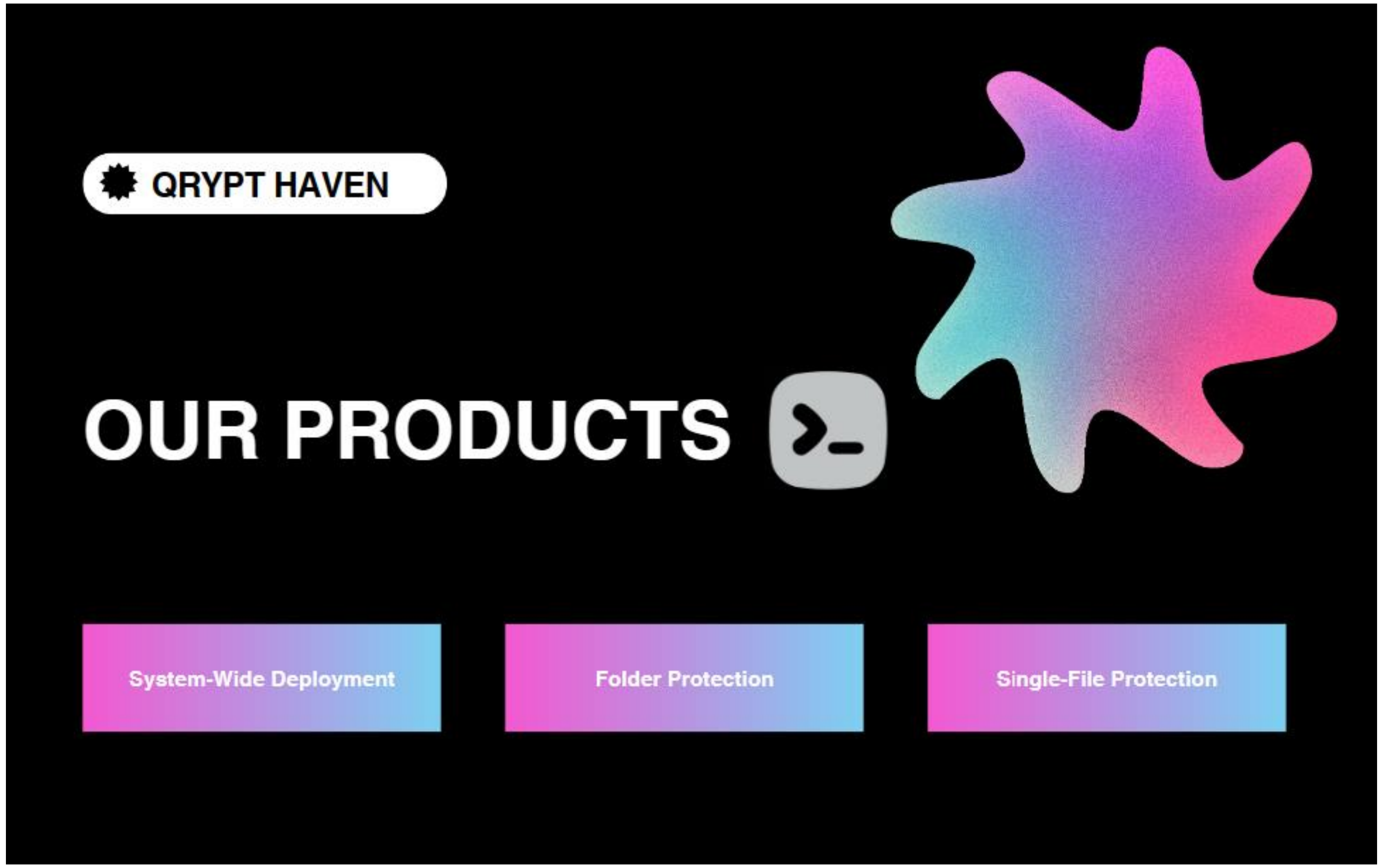
INTEGRATION INTO WEB PLATFORM

By utilizing public APIs developed by the Crystals team, we integrated the algorithm into a user-friendly interface. (Seen top left)



THE PRODUCT


QRYPT HAVEN .
SECURE TOMORROW.
Defending Your Digital World.
Next-Generation Cybersecurity for
Quantum Threat Protection.
SECURE YOUR DATA


QRYPT HAVEN
OUR PRODUCTS
System-Wide Deployment
Folder Protection
Single-File Protection

TIMELINE

END OF 2024

- Q 1, 2: Finalize Research Proposal Outline and Objectives
- Q 3, 4: Conduct user tests and refine web platform.
- Attend conferences, discover angel investors, and attract VC firms.

EARLY 2025

- Develop platform to the final stage and prepare for rollout
- Obtain Ethical Approval, Legal Approval, Permissions for Data Collection + Licensing Frameworks

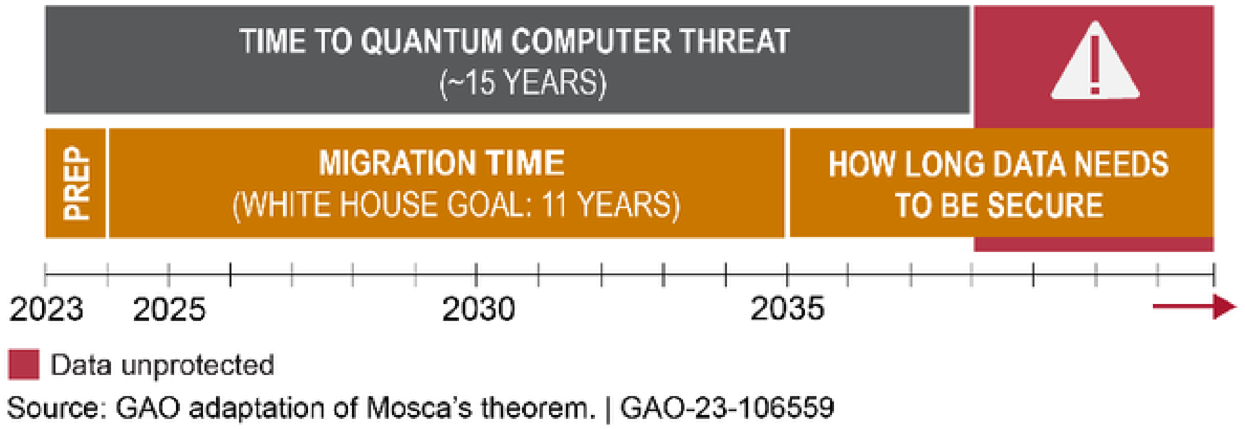
END OF 2025

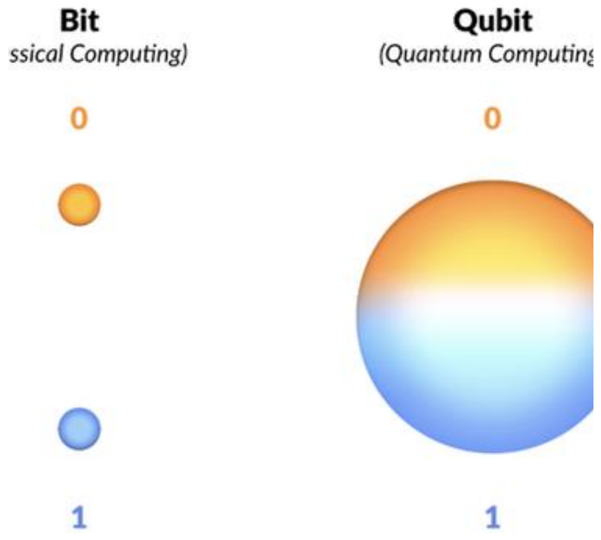
- Distribute and rollout product licenses
- Conduct Data Collection and Examine Various Marketing Avenues.

2026 <

- Transcribe and Analyze User Data, Identify Emerging Themes
- Design and Refine Product to Combat the Competitive Market

OVERVIEW/CONCLUSION





The prominent issue of the quantum threat to our digital society is imminent; our encryption methods are ill-prepared for the quantum leap in computing power. We have a finite timeline window to act and protect our data.

Integration API (Java):

The journey toward a quantum-safe future will be a collective effort. We invite each one of you to join us in this vital mission to protect our data, our privacy, and our digital infrastructure for generations to come.

qrypthaven.com