Gene-Editing Biosecurity: Cryptographic Lock-and-Key Systems for CRISPR

Rafat Tausique
Bachelors of Technology in Department of Computer Science, Kalinga Institute of Industrial Technology, Bhubaneswar, Odisha, India

Aryan Lall
Bachelors of Technology in Department of Computer Science, Kalinga Institute of Industrial Technology, Bhubaneswar, Odisha, India

Abstract

As CRISPR technology becomes increasingly decentralized, existing biosecurity measures—primarily biological and compartmentalized—struggle to keep up with the velocity, scale, and sophistication of emerging threats. Despite expanded experimentation with containment protocols, a coherent framework integrating molecular safeguards with programmable, policy-governed access control is still absent, revealing a significant research gap in the secure deployment of gene-editing platforms. To mitigate this evolving vulnerability, we propose an innovative bio-digital paradigm that reconceptualizes CRISPR containment through the lens of cryptographic security. By drawing analogies between synthetic biology and contemporary cybersecurity, we recast biological containment strategies such as kill switches, auxotrophy, and sequence-level gating as digital counterparts—including timeout protocols, tokenized access, and cryptographic signatures. This interdisciplinary synthesis culminates in a unique "lock-and-key" model, wherein molecular genetic locks are seamlessly integrated with blockchain-based access regulation and zero-trust security architectures. Far from metaphorical, this model enables programmable, tamper-evident enforcement of context-specific, policy-compliant gene-editing privileges—spanning institutional laboratories and decentralized biohacking communities. Contrary to legacy models reliant on retrospective regulation, our design-forward methodology introduces a proactive paradigm for CRISPR security. By embedding cryptographic mechanisms like multi-factor authentication and immutable ledgers, the framework transforms genomic oversight into a verifiable, adaptive system, establishing a globally harmonized, cryptographically anchored biosecurity model for the post-scarcity bioengineering era. Aryan Lall is a B.Tech student specializing in Computer Science and Engineering with research interests in biosecurity, cryptography, and AI-driven security frameworks.