ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Volume 12, Issue 08, August 2025

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

[1] Rafat Tausique, [2] Aryan Lall

[1] [2] Bachelors of Technology in Department of Computer Science, Kalinga Institute of Industrial Technology, Bhubaneshwar
Corresponding Author Email: [1] tausiquerafat@gmail.com, [2] aryanlall0712@gmail.com

Abstract*— As CRISPR (Clustered Regularly Interspaced Short Palindromic Repeats) technology becomes increasingly decentralised, current biosecurity measures, largely bi- ological and isolated, fail to match the pace and com- plexity of emerging threats. This study introduces a pi- oneering bio-digital framework that reimagines CRISPR containment through the lens of cryptographic security. Bridging synthetic biology and cybersecurity, we map genetic safeguards such as kill-switches, auxotrophy, and sequence-based controls to digital security counterparts such as timeout protocols, access tokens, and digital sig- natures. This conceptual convergence informs a novel "lock-and-key" architecture that integrates molecular- level genetic locks with blockchain-enabled access poli- cies and zero-trust governance models. Unlike exist- ing frameworks, our approach enables programmable, tamper-resistant access control over gene editing func- tionalities, potentially transforming CRISPR biosecu- rity from reactive regulation to proactive, design-driven containment. This work not only addresses a critical gap in hybridised containment strategies but also lays the foundation for globally standardised, cryptographi- cally enforced biosecurity in an age of DIY gene editing.

Index Terms*— Bio-digital security, CRISPR, crypto- graphic access control, decentralised governance, genetic containment, synthetic biology.

I. BACKGROUND

The science of genetic engineering has been completely transformed by CRISPR-Cas (Clustered Regularly In-terspaced Short Palindromic Repeats and CRISPR-associated protein-9) systems [1], which were initially identified as a component of prokaryotes' adaptive im- mune systems. CRISPR technologies provide previ- ously unheard-of levels of precision, efficiency, and pro- grammability, allowing targeted genome editing in a va- riety of organisms. These developments have sparked revolutionary applications in industries like environmen- tal engineering, synthetic biology, medicine, and agri- culture. But when CRISPR techniques become more widely available, even to nonscientists through Do-It-Yourself(DIY) biology platforms, they raise serious questions about regulatory control, biosecurity, and eth- ical supervision [2].

Numerous studies have emphasised the versatility of CRISPR technology. DiEuliis and Giordano [3] high- light the pressing need for comprehensive biosecurity standards by warning that CRISPR may be used to de- velop new bioweapons or improve neurological processes. Arani and Zeinoddini (2023) [4] highlighted the poten- tial destabilizing impact of CRISPR-based bioweapons on geopolitical stability. Although their suggested pro- cedures are yet disjointed and lack systematic consis- tency, Hoffmann et al. [5]. (2023) recommends creating biological "firewall" systems to identify and stop unlaw- ful genome changes. Stasi and Thongpravati [6] suggest that blockchain-based governance structures and cryp- tographic permissions should be implemented to handle risks in decentralised scientific communities.

II. MOTIVATION AND OBJECTIVE

Existing biocontainment techniques, such as nutritional requirements and genetic kill switches and auxotro- phy [7], remain mainly isolated and biologically driven, despite increased knowledge of the biosecurity dangers associated with CRISPR. Unlike cryptographic access control, they do not use layered digital security con- cepts. Currently, there is no comprehensive framework that combines digital cryptography mechanisms with bi- ological containment to systematically limit unautho- rized genome editing activities.

Inspired by cybersecurity multi-factor authentication approaches and encryption technologies, this research suggests a novel hybrid architecture for CRISPR biose- curity. We seek to develop a strong bio-digital archi- tecture that can enforce safe, multi-level access control over gene-editing technologies by reinterpreting biologi- cal safeguards as programmed lock-and-key mechanisms and combining them with digital verification layers [8].

III. METHODS

A. List of Materials Used

This study was conceptual and relied on academic mate- rials such as articles and journals rather than using phys- ical tools from a laboratory. The resources included:

- Approximately 10–12 peer-reviewed research arti- cles on CRISPR-Cas biosecurity, synthetic biology, and cybersecurity from journals such as *iScience*, *OBM Genetics*, and *The CRISPR Journal* [5, 6, 9].
- Regulatory guidelines and reports from worldwide institutions such as the FAO (Food and Agriculture Organisation) and the European Union.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Volume 12, Issue 08, August 2025

- Conceptual models of biological containment strategies such as genetic kill-switches, auxotrophy, and sequence-based systems [10, 11].
- Digital security frameworks including access con- trol models, encryption techniques, blockchain- based governance proposals, and zero-trust archi- tectures [8] [12, 13].

Genetic containment strategies, such as kill-switches, serve to limit unintended or malicious consequences of genetically modified organisms (GMOs) [14]. Models

like auxotrophy, in which organisms are designed to be dependent on an external nutrient to survive, en- sure that genetically modified organisms cannot grow or multiply unchecked in uncontrolled environments. Sim- ilarly, sequence-based systems, where genes are engi- neered to require specific sequences or triggers for ex- pression, help to limit the spread of engineered traits.

The research draws parallels between biological con- tainment and digital security measures. Frame- works such as access control models (e.g Role- Based Access Control), encryption techniques (e.g Rivest–Shamir–Adleman (RSA), Advanced Encryption Standard (AES)) and blockchain-based governance pro- posals (e.g., using smart contracts for transparent and immutable record keeping) are relevant for safeguard- ing genetic data and preventing unauthorized access to gene editing platforms. Zero-trust architectures, which assume that threats are always present, are also inte- grated to ensure robust protection across all layers of the bio-digital framework.

B. Step-by-Step Procedure

The methodology took place in three stages:

a. Literature-Driven Conceptual Mapping

A systematic review of peer-reviewed literature and reg- ulatory documents was conducted to map:

- Biosecurity challenges posed by CRISPR and syn- thetic biology technologies [15].
- Current biological containment strategies, includ- ing kill-switch designs and host-environment depen- dency systems [7].
- Digital security analogues such as authentication mechanisms, encryption key management, and sig- nature validation frameworks [8, 9].

Analysis of several scientific journals and institutional publications were thematically analysed to extract key models, risk areas, and regulatory limitations.

This section investigates potential security and eth- ical risks posed by CRISPR and synthetic biology technologies. For example, CRISPR's precision might also enable malicious modifications in DNA sequences, potentially leading to unintended consequences such as bioweapon creation or environmental contamina- tion. Kill-switch designs (which can disable a geneti- cally modified organism if it escapes the intended en- vironment) and host-environment dependency systems (where organisms are reliant on specific environmental factors, such as nutrient availability, for survival) are explored as tools for controlling engineered organisms.

Drawing parallels between biological containment and cybersecurity practices, the study highlights how en- cryption key management, signature validation, and au- thentication mechanisms in digital systems can be anal- ogous to genetic safeguards. Just as encryption ensures the integrity of digital data, genetic containment strate- gies ensure the safe handling of genetically modified or- ganisms.

b. Biocontainment as Cryptographic System Analysis

Existing biocontainment strategies were conceptualised as "lock-and-key" analogues:

- Kill-switch activation was mapped to encryption key dependencies.
- Host-environment dependencies were compared to authentication token systems.
- Sequence-based detection was framed as equivalent to digital hashing and signature verification.

Each mechanism was critically assessed on three cri- teria:

- **Containment fidelity:** Ability to reliably prevent unauthorised genome access.
- **Key specificity:** Precision of the chemical or en- vironmental trigger required.
- **Tamper resistance:** Difficulty for an attacker or rogue agent to override the system.

Host-environment dependencies are mechanisms by which organisms are engineered to only function in spe- cific environments, like a lab. This parallels digital au- thentication, where systems require a valid token (such as a password or biometric) before granting access. This analogy helps to conceptualise the access control mech- anisms necessary for biosecurity.

c. Proposed Framework Development

Building on the conceptual mapping, a hybrid bio- digital framework was proposed. This integrates:

- Genetic access controls at the DNA/protein expres- sion level.
- Digital oversight systems such as blockchain-based credential issuance using hashing techniques and smart contracts for authorization [9].
- Institutional or decentralised governance struc- tures, including DAO (Decentralised Autonomous Organisation) models for regulating access to gene synthesis platforms.

This hybrid model is designed as a bio-digital zero- trust architecture, ensuring that genome editing actions can only occur following verified multi-layer authentica- tion and that every incoming or outgoing set of infor- mation needs to be validated.

This suggests developing molecular controls that func- tion similarly to digital access controls. For example, specific

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Volume 12, Issue 08, August 2025

genetic sequences could act as "passwords" that grant access to certain biological functions, preventing unauthorised manipulation of genetic material.

A DAO could function as a decentralised governing body for managing the approval of genetic modifica- tions. Using blockchain, DAOs can provide a transpar- ent and decentralized system in which stakeholders can vote on the legitimacy and ethicality of genetic modi- fications before approval. This approach ensures that there is no single point of control, and all modifications are carefully vetted by a diverse community.

C. Tools and Instruments Used for Data Analysis

For organising and synthesising the collected informa- tion:

- Zotero was used for reference management.
- Conceptual mapping was manually performed based on thematic coding.
- Diagrams and system architecture models were cre- ated using draw.io and Lucidchart.

Zotero is a powerful tool for managing citations and references. It allows for easy collection and organisation of research articles, books, and reports, helping to main- tain the integrity of the research process and ensuring that all sources are properly attributed.

This method involves categorising and organising key themes and concepts from the literature to identify trends, connections, and gaps in knowledge. Thematic coding allows for a structured analysis of complex data, facilitating the identification of underlying patterns and insights.

Using tools like draw.io and Lucidchart, the study vi- sualises complex concepts, such as the hybrid bio-digital framework, making it easier to communicate complex ideas.

D. Ensuring Reliability of Conceptual Findings

To ensure the reliability and validity of this conceptual research:

- Only peer-reviewed scientific publications and in- stitutional reports were included.
- Cross-validation between the synthetic biology and cybersecurity fields was conducted to ensure logical coherence.
- Proposed frameworks were checked for internal con- sistency and alignment with accepted biosecurity and cybersecurity standards.

By relying exclusively on peer-reviewed sources, the research ensures that the findings are based on estab- lished and scientifically valid information. This min- imises the potential for bias or errors that could arise from non-peer-reviewed or speculative sources.

This step ensures that the frameworks and models proposed in the research are coherent and consistent across both domains. By comparing practices in syn- thetic biology with those in cybersecurity, the study can identify the best practices for cross-domain integration. The proposed bio-digital frameworks were thoroughly vetted to ensure that they comply with existing biose- curity and cybersecurity standards. This helps ensure that the proposed solutions are feasible and applicable to real-world scenarios.

E. Mapping Biological Safeguards to Cryptographic Analogues

We define a mapping between biological containment strategies (denoted by B) and digital security principles (denoted by D) as follows:

- $B \in$ {Auxotrophy, Kill Switch, Sequence Motif Detection}

Access Token Authentication,

- $D \in$ Timeout Protocol, □□ Digital Signature Validation

We introduce a mapping function:

$\Phi: B \rightarrow D$

Specific mappings are defined as:

Φ(Auxotrophy) = Access Token Authentication Φ(Kill Switch) = Timeout Protocol

Φ(Sequence Motif Detection) = Digital Signature Validation

IV. RESULTS

The study evaluated current CRISPR containment strategies through a cryptographic framework lens and identified conceptual analogues between biological safe- guards and digital security primitives. These results are presented across three key areas: containment classifi- cation, digital analogues, and the proposed hybrid ar- chitecture.

A. Containment Strategy Classification

Analysis of the literature revealed three dominant con- tainment strategies used in CRISPR-Cas enabled sys- tems [5, 7] [16, 17]:

- **Metabolic Containment (Auxotrophy):** Or- ganisms are genetically engineered to depend on synthetic nutrients, which are compounds not naturally occurring in the environment, for their survival and growth. Without access to these molecules, organisms cannot sustain essential metabolic processes, leading to death or dormancy. This strategy ensures that escaped organisms can- not survive or proliferate in uncontrolled environ- ments.
- **Kill-Switch Mechanisms:** Kill-switches are en- gineered safety circuits embedded within organisms that monitor their environment for specific condi- tions or molecules. If environmental triggers (such as chemical inducers or temperature ranges) are ab- sent, altered, or tampered with, the kill-switch ac- tivates a programmed cell death pathway, ensuring organisms cannot survive outside authorised set- tings.
- **Sequence-Based Control Systems:** Organisms are engineered to recognise and respond to partic- ular DNA or RNA sequences (motifs). Essential biological processes like replication or transcription are activated

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Volume 12, Issue 08, August 2025

only when the correct motifs are de- tected, effectively acting as molecular gatekeepers that halt function in the absence of verified inputs.

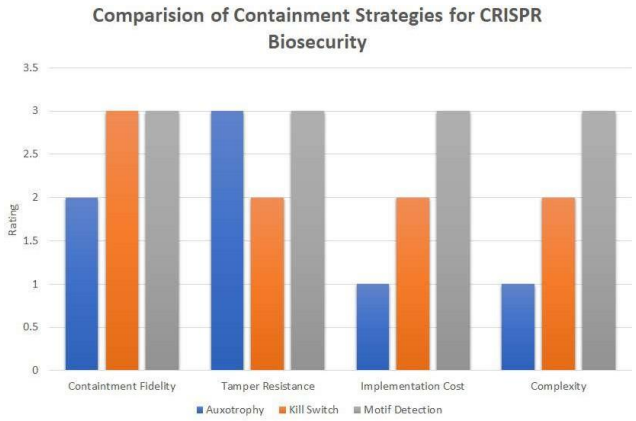

Fig. 1. Comparison of Containment Strategies for CRISPR Biosecurity across four dimensions: contain- ment fidelity, tamper resistance, implementation cost, and complexity.

B. Biological-Cryptographic Mapping

A comparative model was developed to map biological strategies onto digital security principles. Drawing par- allels between biological containment and digital secu- rity, several CRISPR-based strategies closely resemble cryptographic mechanisms. For example, auxotrophy, where an organism is engineered to require a synthetic amino acid to survive, functions analogously to an access token or cryptographic key—the organism only operates in the presence of a specific external input. Kill-switch circuits, which induce cell death in the absence of an

environmental cue, mirror timeout or auto-logout pro- tocols that terminate access after a period of inactivity or if certain conditions aren't met. Similarly, inducible gene control systems, which require multiple inputs to activate gene expression, reflect two-factor authentica- tion in cybersecurity. Lastly, the practice of screening for DNA motif, which allows genome editing only if the sequence input matches a predefined whitelist, is com- parable to digital signature validation used to authen- ticate legitimate communication or code. This map- ping supports the hypothesis that synthetic gene control systems can implement cryptographic-like functionality, acting as "locks" that require environmental, chemical, or sequence-specific "keys."

C. Proposed Bio-Digital Lock-and-Key Framework

The final output of this study is a hybrid biosecurity framework comprising the following:

Genetic Locks: Molecularly engineered, multi- layered biological security mechanisms that combine kill-switch circuits, motif identification systems, and auxotrophy dependencies [5, 7]. This composite struc- ture ensures strict regulation of an organism's survival, gene expression, and replication, preventing unautho- rised use or environmental escape.

Cryptographic Keys: These function as essential authorisation tokens needed to "unlock" genetic func- tions, comparable to digital keys in cybersecurity sys- tems [8] [18]. Keys could be tied to blockchain-based gene synthesis registries for secure authorisation, requir- ing both digital validation and physical verification, such as molecular barcodes or synthetic metabolites.

Access Policy Layer: A governance system respon- sible for managing access to gene editing capabilities. This layer could be institutional (for example, regula- tory agencies or research consortiums) or decentralized (for example, DAOS) [9]. Credentials would be issued based on strict criteria, including identity verification, purpose validation, and adherence to biosecurity and ethical standards. Continuous monitoring and revoca- tion mechanisms would ensure dynamic oversight and prevent policy breaches.

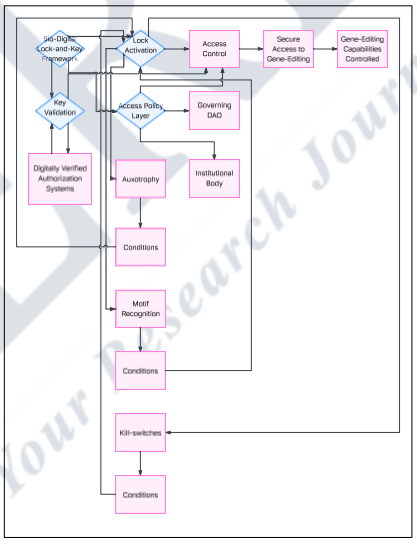

Fig. 2. Proposed bio-digital lock-and-key frame- work integrating biological mechanisms (auxotrophy, kill switches, motif recognition) with cryptographic authori- sation systems and policy governance layers.

V. DISCUSSION

The results of this study highlight a compelling conver- gence between the containment mechanisms of synthetic biology and the core concepts of cryptographic access control. By reframing genetic safeguards as analogues to digital security systems, we introduced a new per- spective for addressing CRISPR-related biosecurity con- cerns—particularly those arising from the liberalisation and decentralisation of gene editing technologies [2, 3].

A. Biosecurity Through Bio-Digital Synthesis

Auxotrophy, gene circuit kill-switches, and motif- dependent activation are examples of traditional bio- containment mechanisms that are usually assessed sep- arately for biosafety. However, these approaches show great promise as biodigital security layers when organ- ised as a

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Volume 12, Issue 08, August 2025

component of a larger access control scheme [7]. For example, using a synthetic nutrient as an "access to- ken" is comparable to digital two-factor authentication, while employing engineered DNA motif recognition is similar to a public-key signature verification.

These findings lend credence to the notion that CRISPR access should be technically managed at the molecular level, employing physical or digital "keys" to unlock genome editing functionality, rather than de- pending exclusively on institutional oversight or labo- ratory protocol compliance. This approach advances the field toward a zero-trust biosecurity architecture [8], where authorisation is continuously verified rather than assumed.

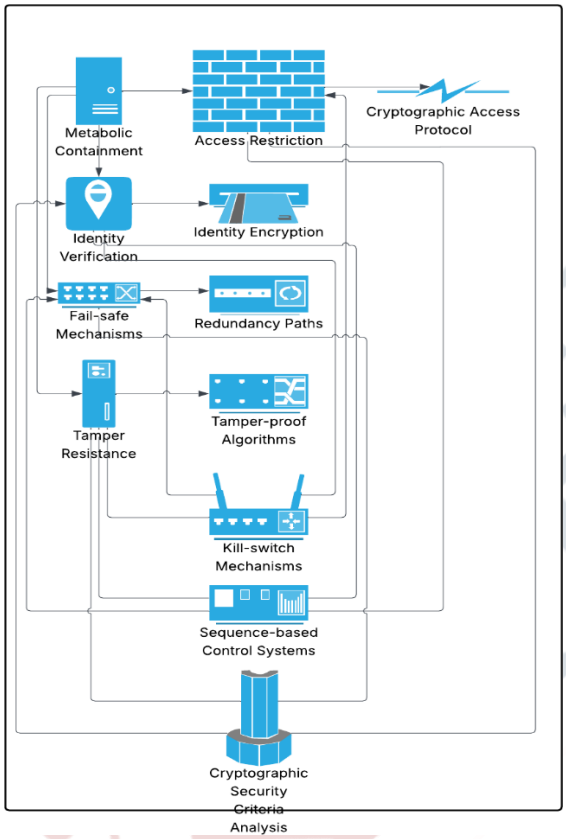

Fig. 3. Overlay of biological containment mechanisms and cryptographic access protocols showing alignment across security criteria such as identity verification, re- dundancy, and tamper resistance.

B. Advantages of Cryptographic Fram- ing

There are various advantages to the cryptographic fram- ing of biological containment:

- **Granular Control:** Using programmable biomolecular keys, researchers or organisations could grant access to CRISPR per project or user.
- **Robustness Against Tampering:** Integrated safeguards, such as kill switches, ensure that unau- thorised modifications are automatically reversed.
- **Scalability:** Modular designs would allow a wide deployment of secure gene editing applications in DIY, clinical, agricultural, and industrial settings.

In addition, linking physical gene synthesis machines (such as DNA printers) to institutional cryptographic servers or blockchain-based registries could enable chain of custody tracking, usage monitoring, and auditability of gene editing activities.

C. Limitations and Challenges

Several limitations must be addressed before the hybrid framework can be practically implemented:

- **Biological Complexity:** Biological systems are in- herently noisy, context-dependent, and mutation- prone, which may compromise containment fidelity.
- **Design Standardisation:** There is currently no unified framework or library to construct modular, programmable genetic locks [6].
- **Ethical Governance:** Embedding access control into biological systems raises questions about key issuance, access criteria, and mechanisms for the detection of response and abuse.

Furthermore, physical synthesis methods could still be misused or reverse-engineered in fully offline or rogue environments, bypassing proposed safeguards.

D. Future Work

Future research should prioritise the development of re- liable, low-leakage genetic lock mechanisms that func- tion consistently in various hosts and environmental set- tings [7].

Additionally, formal standards for cryptographic key generation, issuance, and revocation within synthetic bi- ology must be established

Efforts should also focus on designing regulatory mod- els that integrate cryptographic access control with ethi- cal, legal, and human rights frameworks [19]. Achieving these goals will require interdisciplinary collaboration among synthetic biologists, cybersecurity experts, legal scholars, and ethicists to operationalise secure, scalable, and ethical bio-digital systems [20].

VI. CONCLUSION

This study's goal was to provide an extensive structure that improves CRISPR biosecurity by comparing cryp- tographic access control methods with biological con- tainment techniques. A proactive, enforceable approach to prevent malicious or unauthorised genome editing was the goal of the study, which recognised the in- creasing concerns associated with the democratisation of gene-editing technologies, particularly through decen- tralised and do-it-yourself platforms.

The primary findings of the research show that digital security features like access tokens, timeout protocols, and digital signatures may be conceptually mapped to biological protections like auxotrophy, kill-switch mech- anisms, and sequence-based recognition systems [21]. A hybrid

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Volume 12, Issue 08, August 2025

bio-digital framework was developed as a result of this mapping, in which institutional governance layers and digital cryptographic verification mechanisms sup- port molecular-level genetic locks. The model reflects the zero-trust architecture principles applied within syn- thetic biology.

This work has significant implications for the future of biosecurity. Researchers, organisations, and regulatory agencies can transition from reactive regulatory frame- works to design-based, proactive containment tactics by directly integrating cryptographic verification into bio- logical systems. The suggested paradigm could be used to impose secure, conditional access to gene-editing tools across DNA synthesis facilities, CRISPR kit distribu- tions, and academic research environments.

Future research should focus on developing and test- ing programmable genetic locks with integrated crypto- graphic key management. In addition, significant im- provements to global biosecurity frameworks could be achieved by developing decentralised governance mod- els, such as blockchain-driven systems, and establishing international standards for biodigital containment in the synthetic biology domain.

REFERENCES

[1] D. G. Gibson *et al.*, "Creation of a bacterial cell controlled by a chemically synthesized genome," *Science*, vol. 329, no. 5987, pp. 52–56, 2010.

[2] J. B. Tucker, "Innovation, dual use, and security: Managing the risks of emerging biological and chemical technologies," *Har- vard Kennedy School*, 2012. [Online]. Available: https://www.belfercenter.org

[3] D. DiEuliis and J. Giordano, "Why gene editors like crispr need to be on biosecurity radar," *The Conversation*, 2017. [Online]. Available: https://tinyurl.com/4ae76avh

[4] M. G. Arani and M. Zeinoddini, "The use of crispr gene-editing technology in bioweapons and secu- rity issues," *SHS Web of Conferences*, vol. 134, p. 00048, 2023.

[5] S. Hoffmann, J. Diggans, D. Densmore *et al.*, "Safety by design: Biosafety and biosecurity in the age of synthetic genomics," *iScience*, vol. 26, no. 4, p. 106165, 2023.

[6] A. Stasi and O. Thongpravati, "Biotechnology in- novation in do-it-yourself (diy) gene editing and biosecurity governance," *OBM Genetics*, vol. 8, no. 2, 2024.

[7] J. Kou, Z. Yang *et al.*, "A genetic firewall: Bio- containment and release of genetically modified mi- croorganisms," *Nature Communications*, 2023.

[8] R. Van Est and F. Brom, "Digital security and re- sponsible innovation: Redesigning trust," *Journal of Responsible Innovation*, 2020.

[9] J. Bobe *et al.*, "Open science, decentralized ethics, and participatory oversight in synthetic biology," *Frontiers in Bioengineering and Biotechnology*, vol. 10, 2022.

[10] E. P. on Genetically Modified Organisms, "Scien- tific opinion on the adequacy and sufficiency evalu- ation of existing guidelines for the molecular char- acterisation of genetically modified plants," *EFSA Journal*, vol. 19, no. 5, p. e06554, 2021.

[11] E. P. on Biotechnology, "Synthetic biology devel- opments for application in genetically modified mi- croorganisms and their implications for risk assess- ment," *EFSA Journal*, vol. 20, no. 4, p. e07262, 2022.

[12] Y. Zhang and et al., "A blockchain-based access control scheme for zero trust cross-organizational data sharing," *ACM Transactions on Internet Technology*, vol. 22, no. 3, pp. 1–21, 2022.

[13] X. Li and et al., "Zero-trust access control mech- anism based on blockchain and inner-product en- cryption," *Sensors*, vol. 23, no. 5, p. 11769087, 2023.

[14] C.-H. Chan and et al., "Genetically stable crispr- based kill switches for engineered microbes," *Na- ture Communications*, vol. 13, no. 1, pp. 1–11, 2022.

[15] B. Matthews, "Surveillance and biosecurity in syn- thetic biology," *Science and Engineering Ethics*, vol. 26, no. 6, pp. 3195–3217, 2020.

[16] E. Asin-Garcia, M. Martin-Pascual, C. de Buck, M. Allewijn, A. Mu¨ller, and V. A. P. M. dos Santos, "Genomine: a crispr-cas9-based kill switch for biocontainment of pseudomonas putida," *Frontiers in Bioengineering and Biotech- nology*, vol. 12, p. 1426107, 2024. [Online]. Available: https://www.frontiersin.org/ articles/ 10.3389/fbioe.2024.1426107/full

[17] S. Benatmane, N. Aydin, B. Djilali, and P. Barman, "A new hybrid cryptosystem involving dna, rabin, one time pad and fiestel," *arXiv preprint arXiv:2307.09322*, 2023. [Online]. Available: https://arxiv.org/abs/2307.09322

[18] Y. Wan, P. Wang, F. Huang, J. Yuan, D. Li, K. Chen, J. Kang, Q. Li, T. Zhang, S. Sun, Z. Qiu, and Y. Yao, "Bionic optical physical unclonable functions for authentication and encryption," *arXiv preprint arXiv:2109.03505*, 2021. [Online]. Available: https://arxiv.org/abs/2109.03505

[19] R. Araujo, D. Lindner, and H. Smith, "Governance of cryptographic access in synthetic biology: Eth- ical and legal considerations," *Journal of Biosecu- rity and Policy*, vol. 5, no. 1, pp. 22–39, 2024.

[20] Y. Teng, Y. Zhang, and X. Li, "Cyberbiosecurity: Advancements in dna-based information security," *Biosafety and Health*, vol. 6, no. 2, pp. 123–130, 2024.

[21] J. E. Gallegos, X. Li, G. Wang, Y. Zhang, and C. Zhong, "Synthetic biology for biosecu- rity: Integrated gene circuit containment using cryptographic methods," *Nature Communications*, vol. 11, no. 1, p. 4562, 2020.