Microbial Cryptography: How Bacteria Could Secure Our Digital World

Lee Chun Yin Jefferson (**Y3 Business Analytics**)

Personal Motivation:

Given my interests in cryptocurrencies and all things cryptography, I have always been fascinated by the creative ways of securing our digital world. As a computing student myself now taking a microbiology class, I started noticing cool intersections between these fields. What if living organisms could help protect our digital data the way complex algorithms do? That's exactly the spark behind microbial cryptography.

I chose this topic because it perfectly blends my passion for crypto with the intriguing world of microbes. The idea of microbial cryptography might sound futuristic, but real research is beginning to explore how engineered bacteria can do just that. In this essay, I will share a couple of exciting cases that highlight how bacteria might one day secure our information, and discuss how these methods might differ from traditional encryption techniques.

Main Body:

How Traditional Basic Encryption Works

Before we even delve into the novel microbial encryption methods, let us take a moment to understand how data is encrypted traditionally. To understand encryption, it is simply all about converting readable data into an unreadable format, so that only someone with the correct key can decode it back into its original form. In its simplest form, this process basically relies on mathematical algorithms to scramble data. Think of it as using a secret recipe to mix ingredients in such a way that one is unable to taste the flavours of the original ingredients, unless you know exactly how to "reverse-cook" them back. Many of the modern encryption methods, like the Advanced Encryption Standard (AES) or RSA (Rivest–Shamir–Adleman), use complex math operations and large numbers to create keys, which are essentially long strings of bits that help secure information. These keys are static for a given session or data set, and a breach in security usually means that someone has either guessed or somehow obtained the key, leaving the entire encrypted data vulnerable. This traditional approach lays the groundwork for understanding how a dynamic and ever-changing system like microbial cryptography might offer significant advantages since it involves its "keys" continuously evolving through natural biological processes like cell division.

Microbial Data Encoding

One of the coolest but oldest research made in this aspect dates back to a 2011 research paper featured in Nature, titled "Bacteria encode secret messages" [1], where scientists described how bacteria can be used to encode secret messages by genetically engineering Escherichia coli (E. coli) bacteria to each produce fluorescent proteins in vibrant colours like red, green, and yellow. They then arranged these bacteria in pairs to create a code, with each unique pairing corresponding to letters or symbols, allowing for 49 possible combinations [2]. To store messages, the bacteria were "printed" onto a surface like nitrocellulose paper, which

kept them invisible until activated. When a receiver has to decode the message, the paper would be placed onto an agar plate containing a chemical trigger that activates the fluorescent proteins, causing the bacteria to glow and reveal the encoded characters [3]. To secure the message further, some bacteria are made resistant to specific antibiotics, meaning that without the correct antibiotic, the message would remain jumbled.

The technique was dubbed as “SPAM” (Steganography by Printed Arrays of Microbes) [2] at that time, whereby while these messages can be created and sent through the post, they could only be unlocked with antibiotics and deciphered using simple laboratory equipment. Even though this breakthrough in bacterial message encoding combining microbiology, genetics, and cryptography was not the first example of biological encryption, as researchers have previously hidden messages in DNA, this method was way easier to use as it did not require access to a DNA synthesiser [2] and hence it subsequently served as a building block to many other future work done on microbial encryption.

The Biological Twist on Encryption

Another fascinating case is detailed in a more recent study titled "Encrypting messages with artificial bacterial receptors" [4]. In this work, researchers demonstrated that by similarly engineering genetically modified bacteria, they could create unique optical patterns that can serve as cryptographic keys. They engineered E. coli (again) to express His-tagged outer membrane proteins where these proteins then became docking stations for DNA-based artificial receptors that were tagged with fluorescent dyes like FAM, TAMRA, and Cy5 [4].

The magic really happens through a process known as Förster Resonance Energy Transfer (FRET) when these fluorescent receptors bind to the bacterial surface. Picture it as a molecular light show: when the fluorescent tags are close enough, energy transfers between them, generating a distinct light pattern – a unique optical “fingerprint” that can serve as an encryption key. As the bacteria divide, the receptors get distributed among the daughter cells, causing these fluorescent patterns to naturally change, giving the system a dynamic quality. Since the keys are not static but evolve with every division, it makes it extremely tough for an unauthorised party to crack the system. The continuous evolution of these patterns also meant that any intercepted key is only valid for a short period giving a natural advantage over traditional, static encryption methods.

Enhancing Computational Integrity

There are still challenges, of course, such as maintaining environmental conditions to ensure consistent bacterial behaviour and accurately reading the fluorescence in real time. Although my previous explanation touched on the fundamentals of how bacterial encryption works, it’s essential to understand that computational enhancements in this arena is still heavily needed. This is largely due to the fact that the molecular security devices rely on precise, reproducible computational and physical processes for encryption, decryption, and information protection. That is why breakthroughs in enhancing computational integrity is crucial: such as a computer vision system that captures images of glowing bacterial cultures and sends them through a convolutional neural network (CNN) [5] that has been finely tuned to recognise even the tiniest differences in FRET-generated fluorescence patterns. By blending synthetic biology with

computational tools like AI and machine learning, researchers can even automate the detection and analysis of these fluorescence patterns, by training deep learning models [6], to detect subtle shifts in these bacterial light patterns in real time, ensuring smooth encryption and decryption processes.

By employing advanced algorithms, I foresee how scientists will one day be able to predict how bacterial populations will grow and how the encryption keys will change over time as cell division occurs, giving them more control over the whole encryption process. For example, software can simulate how different experimental conditions like temperature or nutrient supply might alter bacterial growth and fluorescence distribution, to help refine the system so that the encryption keys remain secure even outside the controlled conditions of a lab. Such a system would need to integrate deep learning with real-time data analytics, ensuring that the dynamic encryption remains robust throughout its use.

Real-World Implications and Potential Game-Changing Use Cases

Now that we have a rough understanding of biological encryption, let's think about the broader impact of microbial cryptography. Imagine applying this technology in fields where any interference or hacking could lead to disastrous consequences [7]. For instance, when secure communications is needed like in defence communications, having encryption keys that continuously evolve would protect sensitive transmissions against even the most sophisticated digital attacks. Other possible use cases would involve medical data security where sensitive medical and genetic data might be secured with these biological keys, or even for product authentication; as beyond digital security, engineered bacteria could mark physical products, such as high-value pharmaceuticals, with unique invisible signatures. This biological watermarking can then prevent counterfeiting and ensure product authenticity. Lastly, a final use case could potentially involve using biological encryption in the field of cryptocurrencies since blockchain technology, specifically Ethereum, fundamentally uses the Elliptic Curve Digital Signature Algorithm (ECDSA) with the secp256k1 curve [8] for signing transactions hence I envision the day whereby a hash function generated by biological means could replace the traditional process of generating a public-private key pair that is required to "sign" transactions.

Conclusion & Reflections:

There is a certain poetry to the idea that the same living systems that drive natural processes could someday protect our digital world.

For me, delving into this topic has been a journey of discovery. My early interest in cryptocurrencies led me to think about more advanced cryptographic methods, and now I see that the future of encryption might very well lie intertwined with biology itself. The fact that microbial cryptography is now more than just a cool idea, but a real and innovative approach that challenges the traditional concepts of digital security keeps me excited to dig deeper. By using engineered bacteria to create dynamic and ever-changing encryption keys, we may be looking at the future of how data is secured. Furthermore, as we integrate computational tools such as AI and machine learning with these biological systems, it not only enhances reliability but also opens up numerous practical applications.

From encryption keys that evolve naturally with bacterial growth to the intricate computational models that predict and manage such changes, there is a great potential for microbial cryptography to be involved in interdisciplinary breakthroughs. Throughout this research, it has awed me how human creativity helped merge life sciences with computer science. I'm excited to see where this research leads and how it may someday transform the way we secure our digital world.

References:

1. Yong, E. (2011). *Bacteria encode secret messages.* Retrieved from Nature: https://www.nature.com/articles/news.2011.557
2. Aron, J. (26 September, 2011). *Spies could hide messages in gene-modified microbes*. Retrieved from NewScientist: https://www.newscientist.com/article/dn20965-spies-could-hide-messages-in-gene-modified-microbes/
3. Service, R. F. (26 Sept, 2011). *Science*. Retrieved from A Different Kind of Secret Code: A Different Kind of Secret Code A Different Kind of Secret Code A Different Kind of Secret Code A Different Kind of Secret Code
4. Prasad, P. K., Lahav, N., Motiei, L., & Margulies, D. (November, 202). *Encrypting messages with artificial bacterial receptors.* Retrieved from ResearchGate: https://www.researchgate.net/publication/346846160_Encrypting_messages_with_artificial_bacterial_receptors
5. Przymus, P., Rykaczewski , K., Martín-Segura , A., & Truu, J. (January, 2025). *Deep learning in microbiome analysis: a comprehensive review of neural network models.* Retrieved from ResearchGate: https://www.researchgate.net/publication/388303566_Deep_learning_in_microbiome_analysis_a_comprehensive_review_of_neural_network_models#pf19
6. Zhang, J., Md, M., Yao, Y., Ma, P., Zhang, J., Zhao, X., . . . Grzegorzek, M. (29 September, 2021). *A comprehensive review of image analysis methods for microorganism counting: from classical image processing to deep learning approaches.* Retrieved from Springer: https://link.springer.com/article/10.1007/s10462-021-10082-4
7. Daniel, C. (May, 2024). *Biocrypto: Cracking the Code of Digital Security .* Retrieved from ResearchGate: https://www.researchgate.net/publication/380600689_Biocrypto_Cracking_the_Code_of_Digital_Security
8. Raza, S. (22 August, 2023). *Ethereum's Elliptic Curve Digital Signature Algorithm (ECDSA).* Retrieved from Medium: https://fitsaleem.medium.com/ethereums-elliptic-curve-digital-signature-algorithm-ecdsa-88e1659f4879