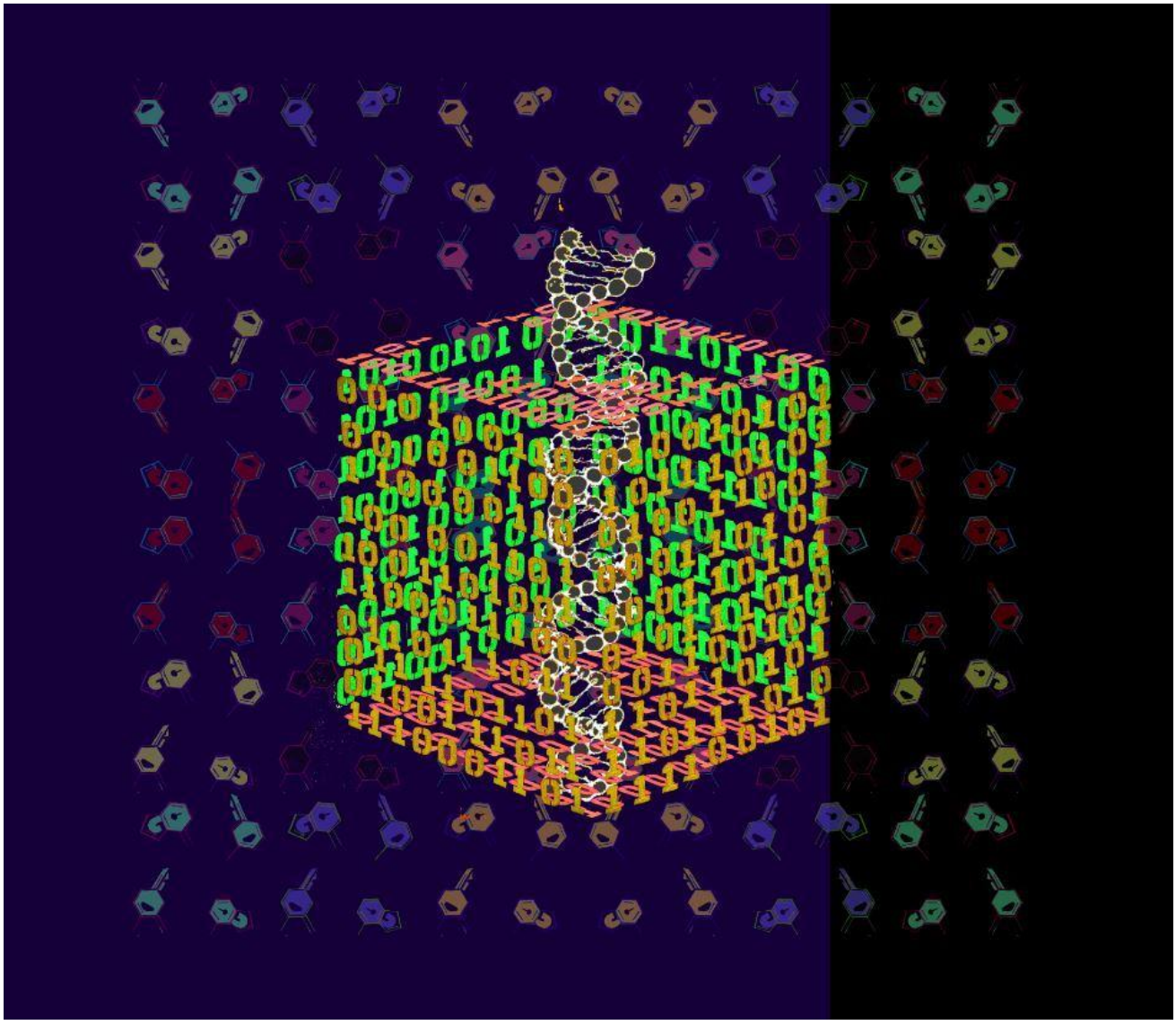
Genomic Encryption Systems: The Standard of Personalized Transaction Security

August 13, 2017

By Joseph Guadarrama, Aharon Herbert and Jaime Weber M.S.

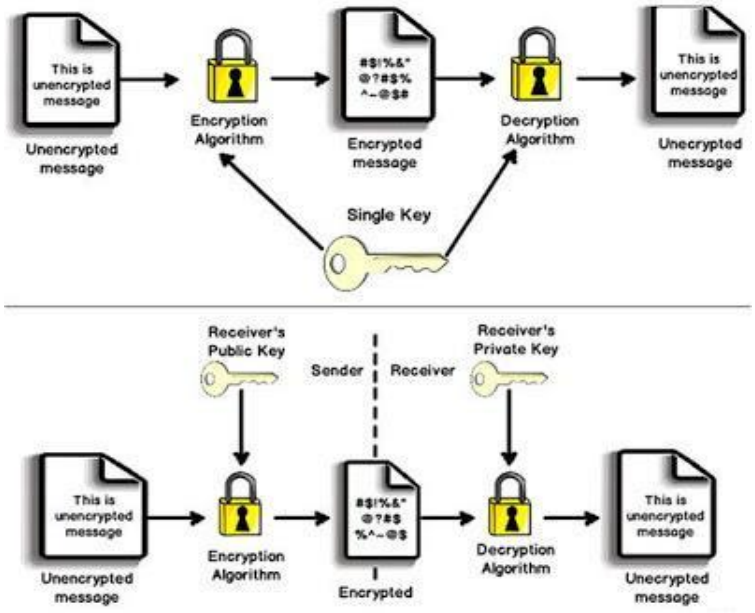


("DNA Cube" by Mengyu Zhou [a])

Today's standard method of binary encoding for data storage is vulnerable and easily susceptible to hacking. With the growing capabilities of hackers to tap into sensitive data sources, we believe VISA should take our solution into consideration for increasing data security. One recent technological advance is the development of quantum computing systems. Quantum computing systems have the ability to store data on multiple inputs beyond our current binary system of encoding on 0's and 1's. Hackers in the near future will be able to exploit the increased processing power of quantum computers to potentially compromise current security systems, such as those currently found in Visa. Bio-encryption provides a wealth of opportunities for increasing current security systems at VISA by utilizing DNA's data storage capabilities. As demonstrated in all living organisms, DNA reveals extraordinary density and reliability in storing large volumes of information. The four bases of DNA, Adenine (A), Cytosine (C), Guanine (G) and Thymine (T) provide four input values for data storage. Our proposal is that Visa can develop encryption software based off of four values instead of today's standard of two. With bio-encryption, personal transaction security will be transformed into an individualized system that is based on each customer's unique DNA. With this growing field and collaboration with Visa's access to Artificial Intelligence, *Watson*, Visa would be more equipped to resist the growing threats of advanced hacking capabilities that infringe our current data security systems.

Current encryption methods include Private Key (symmetric) encryption, and Public Key (asymmetric) encryption [Figure 1-1] [1]. In symmetric encryption, both the encryption and decryption use the same keys [2]. However, in asymmetric encryption the encryption key is different for both encryption and decryption [2]. The major limitation of both symmetric and asymmetric encryption is their reliance on a binary system. We anticipate that the current methods of binary encryption will not be able to maintain security against the emerging technologies such as quantum computing. Quantum computing utilizes the quantum-mechanical phenomena of superposition and entanglement and can represent a bit as either a zero, one, or any quantum superposition between zero and one turning a bit into a qubit [3]. Theoretically, a quantum computer will have the potential to employ qubits as a method to exponentially increase its processing power to 2^n [4]. For example, a quantum computer with 20 qubits will increase processing performance by 2^{20} times. To demonstrate today's vulnerabilities, with current technology, it would take approximately 50 years to defend against a brute force attack on a case sensitive 12 character length password [5]. In comparison, a 20 qubit quantum computer can complete this same defense task in 27 minutes. With companies like Google on the cusp of a quantum computing breakthrough, it should be Visa's priority to establish a team to revitalize the current encryption and decryption methodologies.

Figure 1-1:

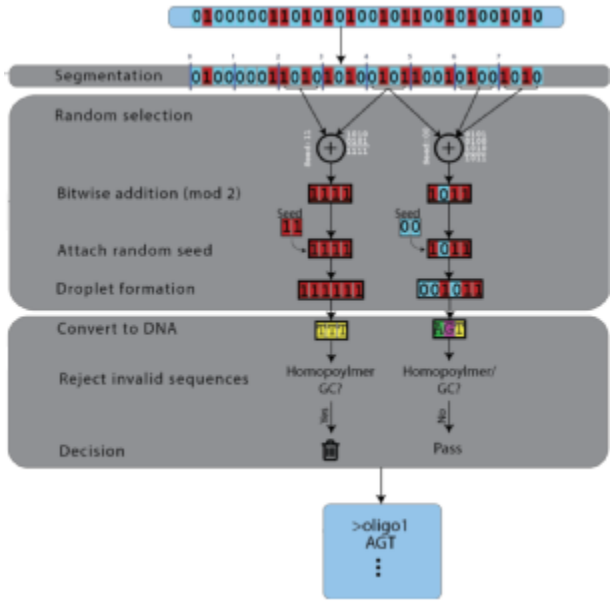


(Symmetric-key cryptography, where a single key is used for encryption and decryption vs. Asymmetric-key cryptography (or Public Key) where different keys are used for encryption and decryption.)

Our proposal aims to advance DNA beyond its standard role within biological organisms. We aspire to use DNA as a way to encrypt security keys for personal transactions. Approximately 98% of all human DNA is identical. The remaining ~2% includes the subtle differences such as single nucleotide polymorphisms and satellite repeat sequences that distinguish each person as unique. Our team envisions a future where humans will no longer require the use of physical cards and may use their own DNA as a marker for self-identification and transactional operations.

In order to achieve this goal, we would employ the principles of bio-encryption and DNA digital data storage to prevent the inevitable future attacks on current vulnerable encryption methods. We will call this the Genomic Encryption Systems and our utilization of this innovative method will be the groundbreaking technology that would define the future of security systems. By examining the role of DNA in biological organisms, there is an observable parallel between DNA and binary code. The differentiating factor is that current computing only operates in zeroes and ones, whereas DNA uses four nucleotides that constitute its sequence: A, T, C, G. The four bases of DNA have revealed a highly desirable and robust target to reliably encode sensitive information. However, using DNA as a means of storing digital information isn't novel. Currently, there are many companies and educational institutions that are researching methods to appropriate this medium due to its attractive features. Earlier this year, researchers at Columbia University and the New York Genome Center developed a process for storing 214 petabytes of data per gram of DNA (for comparison most current hard drives are available in Terabyte format, 1000 Terabytes = 1 Petabyte) [6]. Another example of a promising rising technology is the Capacity-Approaching DNA Storage (codename: DNA Fountain) which allows data to be stored at a maximum theoretical limit per nucleotide [Figure 1-2] [7]. These are examples of the established genomic technologies that we can incorporate into our own security transaction pursuits.

Figure 1-2:

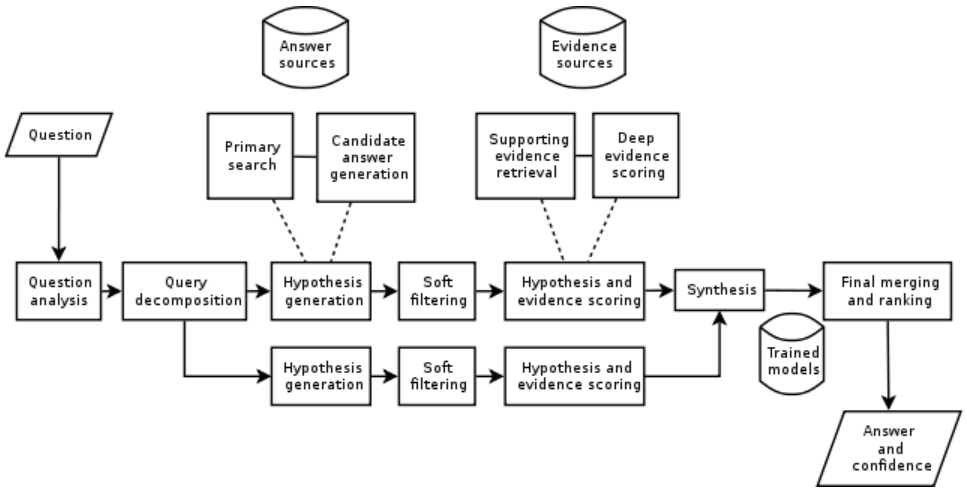


(Capacity-approaching DNA storage, also known as DNA Fountain, is a method of encoding DNA into nucleotides by using commercially available oligonucleotide synthesis machines for storage as well as DNA sequencing machines for information retrieval.)

Our team is thrilled about the future of the bio-encryption. Specifically, we believe that by utilizing the maximum theoretical limit of information storage per nucleotide, Visa will be able to surpass its restraints on cloud computing storage of user's security keys and other viable information. A data center of approximately 100 servers can be scaled down by a factor of 1000, reducing costly maintenance fees and assist in an environmentally friendly transition for the company. One of the major anticipated drawbacks that we have identified is the fact that DNA digital data storage sequencing and information retrieval is expensive. However, considering Visa's vast network and resources, the initial costs will subside based on a new chain of supply and demand for this innovative security system.

The first steps toward achieving our proposal includes developing an integration between IBM's cognitive computer *Watson* and customer's security keys that are coded into their DNA. For clarification, "*Watson* is a question answering computing system built by IBM as a software to apply natural language processing, knowledge representation, machine learning, automated reasoning and information retrieval to a field of open domain question answering" [8][Figure 1-3] [9]. Due to *Watson*'s fluidity, the program can generate a nearly infinite number of encryption keys based on the consumers' unique DNA sequence. By utilizing Watson, the system can detect the unique DNA associated with the consumer, generate a key and conclude the transaction with a two or three step verification process. By utilizing this system, the consumer is relieved from the obligations of maintaining possession of physical cards or payment methods. In addition to the added convenience of our proposed system, there is an increase in confidence in security with each transaction. Finally, we believe pursuing this method of bio-encryption could provide a way for Visa to build its personal brand beyond the credit card.

Figure 1-3:



(High level architecture of IBM's DeepQA used in Watson)

Regarding the location for physically securing clients' DNA data, we would use the *Cyber Fusion Center*, Visa's top secret data fortress in Ashburn, VA. The *Cyber Fusion Center* is an appealing location due to its reputation as "a secure facility that enables rapid cyber threat detection, centralized command and control for cyber operations" [10]. We believe that the *Cyber Fusion Center* is the leading location to resist quantum computing hacking; in turn, this would provide reassurance to Visa's clients regarding privacy concerns.

The outline of our proposed method of transactions is as follows: When the customer decides to purchase a product or service they will swath their hand on a self-cleaning glass material tempered with titanium dioxide which will read their DNA, encrypt it, and communicate with Visa's Cyber Fusion Center using VisaNet's Base II messaging system, where the approval message will be a random set of donor DNA extracted from Cyber Fusion Center by Watson.

One primary security concern revolves around the sensitivity behind revealing a client's DNA to Visa. We propose that clients will donate their personal DNA sequence to the overall Watson DNA server. From the Watson server, our algorithm will associate each transaction with a random sequence of DNA and form a new set of encryption keys accordingly. The client will not be associated with their personal DNA sequence, rather, as a form of information/security separation between the client and their sensitive genetic information, the client will have a transaction code that will automatically and randomly select a piece of donor DNA from the server to provide the encryption keys for the transaction.

Our team believes these proposed theories could revolutionize current security systems and reaffirm Visa as the leading business in transaction security. With technology continuously advancing, we believe that our Genomic Encryption Systems can protect Visa and its customers from the inevitable hacking attacks. We believe that with Visa’s resources, our team can make these proposals into a reality and potentially change the course of Visa and the future of transactions that will not only benefit Visa, but can have a world altering affect if executed properly.

Acknowledgements: Mengyu Zhou and Francis Ray.

[a] Zhou, Mengyu. *DNA Cube*. 2017. Digital Media. Toadstool Artworks 2017, San Francisco.

[1] Koirala, Shivprasad. "C# and .NET Interview Questions Shivprasad Koirala." *C# and .NET Interview Question: - What Are Symmetric and Asymmetric Algorithms?* N.p., 01 Jan. 1970. Web. 21 July 2017.

[2] Young, Bill, Dr. "Lecture 44: Symmetric vs Asymmetric Encryption." *Foundations of Computer Security* (n.d.): 1-7. Web. 19 July 2017.

[3] Freiberger, Marianne. "How Does Quantum Computing Work?" *Plus Magazine*. Plus Magazine, 1 Oct. 2015. Web. 20 July 2017.

[4] Dunningham, Jacob, and Vlatko Vedral. "Chapter 11 Quantum Entanglement." *Introductory Quantum Physics and Relativity*. London: Imperial College, 2011. 188-89. Print.

[5] Richardson, Joel. "How Secure Is My Password." *How Long Would It Take to Crack Your Password? Find Out! - Randomize*. N.p., n.d. Web. 23 July 2017.

[6] Whitwam, Ryan. "Researchers Increase the Storage Capacity of DNA to 214 Petabytes per Gram." *Extreme Tech*. Extreme Tech, 3 Mar. 2017. Web. 21 July 2017.

[7] Erlich, Yaniv. "Capacity-approaching DNA Storage." *DNA Fountain - Capacity-approaching DNA Storage*. N.p., 2016. Web. 23 July 2017.

[8] "FAQs." *IBM - DeepQA Project: FAQs*. IBM, n.d. Web. 21 July 2017.

[9] *Ferrucci, D.; et al. (2010). "Building Watson: An Overview of the DeepQA Project". AI Magazine. 31 (3). Retrieved February 19, 2011.*

[10] “Governor McAuliffe Helps Open Visa Cyber Fusion Center in Northern Virginia.” *Governor - Newsroom*, Office of the Governor, 14 Jan. 2016, governor.virginia.gov/newsroom/newsarticle?articleId=13932.