A Survey of Papers by Dr. Albert H. Carlson for AQED

Albert Carlson*.
*Computer Science Department, Austin Community College, Austin, TX, USA.
*Email: *albert.carlson@austincc.edu*

I. Introduction

Albert Carlson studied at various universities across the US, though primarily in Illinois and Idaho. Those universities include, along with majors and degrees:

- Chicago State University: 1975 - 1977, General Studies/History during High School
- University of Illinois, Urbana: 1977 - 1981, BS Computer Engineering
- Mankato State University (now Minnesota State University at Mankato): 1984, Physics
- Illinois Institute of Technology: 1985 - 1987, Computer Engineering
- University of Illinois, Chicago: 1987 - 1992, Electrical and Computer Engineering
- University of Idaho: 1993 - 2012, MS Computer Science 2003, Ph.D. Computer Science 2012

Finding all of the material written by Dr. Carlson requires knowing his Orchid number and location for papers. His Orchid number is 0000-0002-0087-6066. Copies of most papers, including patents and widely distributed white papers can be found on the Researchgate.org website located at https://www.researchgate.net/profile/Albert-Carlson/research.

II. Papers and Content

During his Ph.D. research, the foundations for polymorphic encryption, polymorphic Random Number Generators (polyRNGs), and analysis of the use of Set Theoretic Estimation (STE) with respect to cryptography were described in the dissertation entitled, "Set Theoretic Estimation Applied to the Information Content of Ciphers and Decryption" [1]. The contents of this work are math-intensive and include proofs of the approach. Until this time, STE was exclusively done in Hilbert and vector spaces, but the algorithms developed for use move STE into topological space. It proves that polymorphic encryption is possible and bases future work on Shannon theory and Information Theory (IT) [2], [3]. It led to many theoretical and practical advances in the field.

A. Post Dissertation Research

A simple explanation of polymorphic ciphers is found in the paper "Modeling Polymorphic Ciphers" [4]. The main thrust of the paper is to show that all ciphers can be classified as polymorphic. The main consideration is how often the keys change. Specifically, the content explores the relationship of the frequency of key changes to the entropy and "unicity distance" [2] of the sub-messages. It also defines the size of the sub-messages in terms of "shards." The paper defines a framework to classify ciphers by their polymorphic number.

In an extension of the work done in his dissertation, Carlson, et al, showed that the large numbers that are normally associated with modern ciphers can be reduced precipitously. This comes from two main approaches. They are:

1) Reduce the number and interaction of ciphers - Sometimes security practitioners confuse the complexity of a system with its security. Many ciphers have been created that seem safe due to the difficulty of seeing how the cipher can be "reduced" to an easier cipher system to solve. Feistel made the remark that at their heart, all ciphers are substitution (S) ciphers [5]. Carlson, et al, in the paper, "Isomorphic Cipher Reduction" [6], demonstrate how any non-polymorphic cipher can be replaced by an S cipher. Using this approach, even very large and complicated ciphers can be replaced by simpler ciphers that are more easily broken. Further, it intimates that a single decryption attack will solve an cipher that is non-polymorphic and does not employ a mode. Breaking modes is addressed in other research papers.
2) Reduce the possible number of mappings - The large number of keys that are theoretically possible in encryption gives a false sense of safety and security. Complexity does not mean safety. This is the theme of the research presented in the paper entitled, "Keyspace Reduction Using Isomorphs" [7]. Isomorphs are the name for "equivalent keys." Equivalent keys and language statistics are the results of syntax rules applied to the habits of language [8]. These rules are useful in reducing the number of possible decryptions for a message, allowing for attackers to make use of the techniques to read messages that should be safe. This paper shows how one such technique, called "isomorphic keyspace reduction" can be used to enable brute force attacks on an encrypted message [9]. Specifically, the research shows how to group similar keys together and use one as a representative for a much larger set of keys. Choosing a single representative key in the set can allow the acceptance or rejection of all of the keys in that set. The demonstration of the research in the isomorphic key paper is found in the paper entitled, "Evaluating True Cryptographic Key Space Size" [10]. In this paper,

concrete examples are used to show the extent of how much the keyspace can be reduced using this simple technique. The goal is to show that reliance on the maximum keyspace for a cipher is dangerous. Each message must be evaluated to see what cipher best fits it for security.

Carlson and an undergraduate research team from Fontbonne University, showed that the Cipher Block Chaining (CBC) cryptographic mode was vulnerable to attack. This attack was verified by parallel research work done by McGrew [11]. The demonstration of the methodology was presented at DefCon 23 by Carlson, et al [12] ("Breaking CBC, or Randomness Never Was Happiness") and updates were presented at ShowMeCon [13] ("Using Collisions to Break CBC") in 2016. A more formal report of the results was given in a conference paper entitled, " Using the Collision Attack for Breaking Cryptographic Modes." These papers and talks present the algorithm for breaking CBC and demonstrate that it is successful in returning the plain text in real-time. Additionally, it shows that modes can use attacks on the randomization routines in the modes to return the message. This algorithm does not require breaking the encryption routine in order to be successful in returning the message. It also suggests that modes are ineffective for use and should be abandoned. An extension of these papers/talks is that AES with CBC is not secure.

A discussion of how local unicity distance and entropy [1] was presented in the paper "An Introduction to Local Entropy and Local Unicity" [14]. It was demonstrated that unicity distance and entropy do not have to be calculated only for an entire message. By tracking both the entropy and unicity distance for a small part of the message, it is possible to use that information to focus on the area of a message to attack. Similarly, the same data can be used to size shards for use in a polymorphic cipher. In this manner, it is possible to prove that the concept of polymorphic encryption is both possible and practical. The use of local versions of entropy and unicity distance also gives clues to future research for increasing the security for a message.

One of the problems with product block ciphers is that many cipher designers use multiple keys that may be of different sizes. This often creates confusion and makes it difficult for cryptographers to apply an effective attack to break the cipher. Carlson, et al, demonstrated that a solution to this technique is both simple and effective. The papers "Breaking Block and Product Ciphers" [15] and "Breaking block and product ciphers applied across byte boundaries" [16] show that by treating the blocks as a metacharacter in the language [1] the new effective block size for the key is the lowest (least) common multiple (LCM) of the keys used in the cipher. The papers also show that even if the keys are not the same size as an integer multiple of a byte, the information still remains in a new block the size of the LCM of the keys. Therefore, spreading information across different blocks of the cipher text is not effective in securely encrypting the data. A deeper treatment of the problem is found in "The Problem with Regular Multiple Byte Block Boundaries in Encryption" [17].

While the advantages of polymorphism in encryption are easy to see for most types of ciphers, a question of the applicability of STE to serial ciphers was briefly debated. In "A Venona Style Attack to Determine Block Size, Language, and Attacking Ciphers" [18], Carlson, et al. explored the practice of reusing keys in a cyclical manner. The paper clearly shows that if keys are applied cyclically, even for a Vernam type cipher [19], [20], the cipher reduces itself to a serial cipher. During the late 1930s and up until the mid-1980s the United States systematically read encrypted messages [21] because of the reuse of Russian keypads. While the exact nature of the attack is not known, Carlson, et al, present an algorithm that can be used effectively to break any serial cipher or one-time pad (OTP) [2].

In the present cryptographic environment, there are many algorithms for breaking encrypted messages. Most of these algorithms are specific to a particular cipher. Carlson followed the example of Feistel [5] who declared in 1973 that all ciphers are, at their base, substitution (S) ciphers. This includes product ciphers and round type ciphers, such as AES [9]. This was the subject of the paper "Equivalence of Product Ciphers to Substitution Ciphers and their Security Implication" [22]. Part of the paper includes the analysis of decryption that states that all non-randomized cipher algorithms can be attacked using a single, universal attack: that of the S cipher. It also discusses the use of metacharacters in reducing ciphers.

As part of the decryption process and attacks on ciphers, Carlson, et al focused on how to reduce the resource requirements, including both memory and time. Studying the efficiency of the process, the authors focused on alternatives that speed work. The papers "Space Selection and Abstraction in Set Theoretic Estimation" [23] and "Using Set Theoretic Estimation to Implement Shannon Secrecy" [24] link efficiency to the space in which the effort takes place. Typical work in STE limits the approach to vector, metric, or Hilbert space [25]. However, by moving the work into a topological space there is no need for distance metrics or error bounding, such as bounding planes or optimal bounding ellipsoids (OBEs) [1], [26], [27], [28]. Further, Carlson, et al, demonstrate that the excursion into topological space retains the spirit of STE, as well as reduce required calculations.

B. Random Number Generators (RNGs)

Realizing that polymorphic encryption is dependent on the quality of the RNGs used in the selection of the keys, Carlson and his team began working on improving practical pseudorandom number generators (PRNGs). Most PRNGs are weak. Evaluating those PRNGs and then using the results of the research to improve generators convinced the team that polymorphic principles needed to be added to RNG and PRNG design. After finding Geffe Generators [29], Carlson, et al, combined the Geffe Generator with other RNGs to create and extensible architecture that also combined polymorphic techniques, rotating the component PRNGs in the generator, allowing for the possible cycles in the resultant PRNG to be as long as the encryption to which it is applied.

Following the "A Design for a Cryptographically Secure Pseudo Random Number Generator," research into improving

PRNGs with Geffe Generators showed that using even weak PRNGs can be made acceptable via polymorphic techniques. The techniques investigated that worked to improve overall randomness are discussed in the paper "Novel Innovations for Improving the Quality of Weak PRNGs" [30]. Techniques that were attempted and did not improve PRNGs were reported in the paper entitled, "Novel Innovations that Failed to Improve Weak PRNGs" [31].

C. Physically Unclonable Functions (PUFs)

One of the directions of research regarding polymorphic techniques has to do with decoupling the selecting RNG from the data it produces. Such an approach was introduced by Dr. Bertrand Cambou, an expert in the field of PUFs [32]. Dr. Cambou was looking for a strong encryption and chose to use the polymorphic approach. This first work was discussed in the paper, "Dynamic Key Generation for Polymorphic encryption" [33] the team showed it was possible to mix polymorphic RNGs, PUFs, and polymorphic functions to produce secure and random uncoupled keys from the RNG that selects them.

This approach was extended in the paper "Shadow PUFs: Generating Temporal PUFs with Properties Isomorphic to Delay-Based APUFs" [34]. In this paper, the team showed it was possible to generate new PUF tables, called "shadow" tables to create new PUF tables that had the same statistical properties as the original PUF table, but with different contents. By producing many PUF tables and using them for a short period of time before discarding the old table and replacing it with one of the new shadow PUF tables. Regular replacement of the tables after a short "time to live," or TTL, is analogous to the regular change in the key used in the polymorphic encryption process. The paper also indicates that polymorphism can be extended to RNGs and PRNGs, as well as encryption.

D. QSA Whitepapers

Dr. Carlson has published a number of white papers for the Quantum Security Alliance (QSA), where he holds the title of Chairman of the Entropy and Encryption Committee. The paper entitled, "Standard Password Practices for Organizations: Relative Theory and Recommendations" [35] explains the relationship between entropy and standard password practices that are suggested for protecting those passwords. Basics mathematics related to passwords are also presented, giving proof and support for the recommendations. This is a basic position paper with practical recommendations for the methods used to protect data using passwords. Most papers on the subject do not give the mathematical foundations and principles that allow security practitioners to understand why measures work and which measures can result in cyberfragility.

The first paper that Dr. Carlson co-authored for the QSA was a paper that suggested that information could be stored and transported using liquid chemicals, and chemicals in general, as a media for the data. Dr. Keeper Sharkey has presented research and developments that allow writing that data on the quantum level [36]. However, using this methodology does not secure the information so written. The choice of encryption for this proposal was Dr. Carlson's polymorphic encryption technology. The paper, entitled "Quantum Chemistry for Detecting Cybersecurity Threats to Information Systems," the paper introduces security at the quantum level and pulls the practice of encryption at the quantum level into the present, along with its advantages and problems.

A third paper was requested by the QSA to address recently released recommendations by NIST for quantum proof security algorithms (QPAs). Dr. Carlson summarized the foundations of the algorithms and the security of those approved algorithms. Entitled, "NIST Quantum Proof Algorithm Analysis" [37], the focus was on the named approved finalists for QPAs. Of note was that the algorithms were derived from the same basic technologies of vector mappings in hyperspaces. The base mathematics are "thought" to be hard, but that has not yet been proven. Further, one of the algorithms has been broken by a classical computer in a relatively short (one month) period of time. Such a quick break indicates that the testing is either incomplete or not sufficiently rigorous. Another point of concern is that all of the final candidates are the work of two, or more, of the NIST selection engineers that also authored the analysis. The conclusion is that if math providing the basis for the algorithms can be proven hard then the QPAs should be safe. However, the fact that one of the finalists was broken immediately after the paper selection was released and given the apparent conflict of interest of the selectors/authors, this data requires much more vetting before being accepted.

E. Patents

While working at CipherLoc Corporation, Dr. Carlson led a research team working on polymorphic encryption. The seminal patents giving the algorithms for polymorphic encryption were entitled "Virtual polymorphic hardware engine" [38], [39] and required an extension via a second divisional patent. This set of patents show how the OTP can be extended to larger block sizes without losing security. It also sets out the rules for TTL changes needed to keep the encryption process absolutely safe. Based on Shannon Theory [2] and Information Theory [3] the patent shows a mathematically secure encryption environment and algorithm.

The original polymorphic patent was followed by an update that allows the polymorphic encryption system to emulate a limited OTP in the patents entitled "Polymorphic One Time Pad Matrix" [40] and "Polymorphic Encryption Engine" [41]. There are two divisional patents that show different implementations of the method. One uses a microprocessor-based circuit architecture, the other allows for the OTP to be implemented at least partially in software. The patent also gives an analysis of the chance of repeated key selection.

A method for protecting a wired network and discovering a passive intruder in a network was presented in "Local Area Network Electronic Perimeter Security" [42]. In this patent, a method is presented that is based on the electrical characteristics of the network hardware. An active pulse is passed down the network and the electrical signature of the network is monitored. The pulse used allows the user to verify if the signature has been altered by the insertion of a passive listening device.

Finally, Carlson, et al received a patent for "Dynamic Pin Configurator" [43] for another polymorphic technique: changing the definition of a wired media as the media is being used. This method allows for the media to change wire definition and use it to prevent an attacker from effectively monitoring the media being used. Varying wire mappings increase the effective key space for security and create uncertainty when decrypting. Because the inputs and outputs change rapidly, this method also causes an attacker to lose data transmitted on the wires when the wire definitions change. Once data is lost, it can never be reliably recovered [20]. Since the changes happen irregularly and frequently, data loss is almost guaranteed and the amount of data lost quickly rises until the message can become unreadable.

III. Conclusion

Dr. Albert Carlson has actively researched security applications of polymorphism and set theory since 2002. Papers have been written through universities, colleges, CipherLoc Corporation, and the QSA. Not all of the papers published by Dr. Carlson are listed, as they do not apply to the work done by Dr. Carlson with AQED. A summary of relevant papers and what they give as advances is given here. More research is presently being conducted, primarily in unifying STE, neural networks, and Information Theory. Work is also underway to show that cryptographic modes [9] are ineffective.

References

[1] Albert Carlson. *Set Theoretic Estimation Applied to the Information Content of Ciphers and Decryption*. PhD thesis, University of Idaho, 2012.

[2] Claude Shannon. Communication theory of secrecy systems. *Bell System Technical Journal*, 28:656 – 715, 1949.

[3] Thomas Cover and Joy Thomas. *Elements of Information Theory*. John Wiley & Sons, Inc, New York, 2nd edition, 2005.

[4] Albert Carlson, Indira K. Dutta, Bhaskar Ghosh, and Michael Totaro. Modeling polymorphic ciphers.

[5] Horst Feistel. Cryptography and computer privacy. *Scientific American*, 228(5):15 – 20, 1973.

[6] Bhaskar Ghosh, Indira Dutta, Shivanjali Khare, Albert Carlson, and Michael Totaro. Isomorphic cipher reduction.

[7] Albert Carlson, Bhaskar Ghosh, Indira Dutta, Shivanjali Khare, and Michael Totaro. Keyspace reduction using isomorphs.

[8] D. Terence Langendoen and Paul Postal. *The Vastness of Natural Languages*. The Camelot Press, Ltd., Southampton, 1984.

[9] Bruce Schneier. *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. John Wiley and Sons Inc., New York, 2nd edition, 1996.

[10] Albert Carlson, Torsten Gang, Garrett Gang, Bhaskar Ghosh, and Indira Dutta. Evaluating true cryptographic key spacesize.

[11] David McGrew. Impossible plaintext cryptanalysis and probable-plaintext collision attacks of 64-bit block cipher modes. In *Proceedings of the Fast Software Encryption Workshop*, 2013.

[12] Albert Carlson, Patrick Doherty, Isaiah Eichen, and James Gall. Breaking cbc, or randomness never was happiness. Internet Video, August 2015.

[13] Albert Carlson, Patrick Doherty, Isaiah Eichen, and James Gall. Using collisions to break cbc, 2016.

[14] Albert H. Carlson, Sai Ranganath Mikkilineni, Michael Totaro, Robert Hiromoto, and Richard B. Wells. An introduction to local entropy and local unicity.

[15] Albert H. Carlson, Robert Hiromoto, and Richard B. Wells. Breaking block and product ciphers. 12:259 – 266, 2014.

[16] Albert H. Carlson, Robert E. Hiromoto, and Richard B. Wells. Breaking block and product ciphers applied across byte boundaries. In *The 6th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications*, pages 733–736, 2011.

[17] Albert H. Carlson, Indira Kalyan Dutta, Bhaskar Ghosh, and Robert Hiromoto. The problem with regular multiple byte block boundaries in encryption. 2022.

[18] Albert H. Carlson, Sai Ranganath Mikkilineni, Michael Totaro, and Christopher Briscoe. A venona style attack to determine block size, language, and attacking ciphers. 2022.

[19] Gilbert Vernam. Secret signal system.

[20] Uli Maurer. A universal test for random bit generators. *Journal of Cryptography*, 5(2):89–105, 1992.

[21] John Earl Haynes and Harvey Klehr. *Venona: Decoding Soviet Espionage in the United States (Yale Nota Bene)*. Yale University Press, 1999.

[22] Albert H. Carlson, Sai Ranganath Mikkilinen, Michael Totaro, and Robert Hiromoto. 2022), journaltitle = International Symposium on Networks, Computers, and Communictions, ISNCC 2022, title = Equivalence of Product Ciphers to Substitution Ciphers and their Security Implications,.

[23] Shivanjali Khare, Albert Carlson, Michael Totaro, Robert Hiromoto, and Ricahard B. Wells. Space selection and abstraction in set theoretic estimation,.

[24] Albert Carlson and Robert Hiromoto. Using set theoretic estimation to implement shannon secrecy theory. In *The Proceedings of the Third IEEE Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications*, pages 435 – 438, 2005.

[25] John Kelley. *General Topology*. D. Van Nostrand Company, Princeton, 1955.

[26] Patrick Combettes. The foundations of set theoretic estimation. *Proceedings of the IEEE*, 81(2):182 – 208, 1993.

[27] Richard Wells. *Applied Coding and Information Theory*. Prentice Hall, Upper Saddle River, 1999.

[28] M. Milanese and Antonio Vicino. Optimal estimation theory for dynamic systems with set membership uncertainty: An overview. *Automatica*, 27(6):997 – 1009, 1991.

[29] Benjamin Williams, Robert E. Hiromoto, and Albert Carlson. A design for a cryptographically secure pseudo random number generator. 2019.

[30] Benjamin Williams, Albert Carlson, and Robert Hiromoto. Novel innovations for improving the quality of weak prngs. 2022.

[31] Benjamin Williams, Albert Carlson, and Robert Hiromoto. Novel innovations for improving the quality of strong prngs. 2022.

[32] Bertrand Cambou. A xor data compiler: Combined with physical unclonable function for true random number generation. *2017 Computing Conference*, pages 819 – 827, 2017.

[33] Duane Booher, Bertrand Cambou, Albert Carlson, and Christopher Philabaum. Dynamic key generation for polymorphic encryption. page 482 – 487, 2019.

[34] Haytham Idriss, Pablo Rojas, Sara Alahmadi andTarek Idriss, Albert Carlson, and Magdy Bayoumi. Shadow pufs: Generating temporal pufs withproperties isomorphic to delay-based apufs.

[35] Albert Carlson. Standard password practices for organizations: Relative theory and recommendations. Technical report, Quantum Security Alliance, 2022.

[36] Albert H. Carlson, Hans C. Mumm, Keeper L. Sharkey, and Merrick Watchorn. Quantum chemistry for detecting cybersecurity threats to information systems. Technical report, Quantum Security Alliance, 2022.

[37] Albert H. Carlson and Keeper L. Sharkey. Technical report, 2022), institution = Quantum Security Alliance, title = NIST Quantum Proof Algorithm Analysis,.

[38] Albert Carlson and Robert Le Blanc. Virtual polymorphic hardware engine, 2018.

[39] Albert Carlson and Robert Le Blanc. Virtual polymorphic hardware engine, divisional 1.

[40] Albert Carlson, Bob Le Blanc, and Carlos Gonsalez. One time pad matrix, 2016.

[41] Albert Carlson, Robert Le Blanc, Robert Carlson, Patrick Doherty, and Carlos Gonzalez. One time pad matrix divisional 1, 2019.

[42] Albert Carlson and Rober Le Blanc. Local area network electronic perimeter security, 2018.

[43] Albert Carlson, Robert Le Blanc, Robert Carlson, and Carlos Gonzalez. Dynamic pin configurator, 2021.