[B. Ghosh, I. K. Dutta, S. Khare, A. Carlson and M. Totaro. (Oct. 27-30, 2021). Isomorphic Cipher Reduction, 2021 IEEE 12th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Vancouver, BC, Canada, 2021, pp. 0947-0953, doi: https://doi.org/10.1109/IEMCON53756.2021.9623135]

Isomorphic Cipher Reduction

Bhaskar Ghosh
CACS
University of Louisiana at Lafayette
Louisiana, USA
bhaskar.ghosh1@louisiana.edu

Indira Kalyan Dutta
Comp and Info Sci
Arkansas Tech University
Arkansas, USA
idutta@atu.edu

Shivanjali Khare
ECECS
University of New Haven
Connecticut, USA
skhare@newhaven.edu

Albert Carlson
CIT
Austin Community College
Texas, USA
albert.carlson@austincc.edu

Michael Totaro
CMIX
University of Louisiana at Lafayette
Louisiana, USA
michael.totaro@louisiana.edu

***Abstract*—All ciphers are a form of the substitution cipher. Variations of ciphers, such as the P cipher, block ciphers, and product ciphers have been introduced in an effort to hide the patterns that filter through the obscuring process. Still, if the right parameters are used, it is possible to substitute an equivalent substitution cipher for most encryption algorithms and then use a property of substitution to greatly simplify the analysis and decryption of even block product ciphers. In this paper we also identify and explain exceptions to this reduction. The purpose of applying this cipher reduction is to strengthen security by eliminating the weaknesses that reduction identifies.**

***Index Terms*—Cryptography, Polymorphic Encryption, Key Space, Isomorphic Reduction, Round Ciphers**

I. Introduction

The proliferation of different encryption algorithms over the last half century have also resulted in the corresponding creation of breaks in order to both try and prove the efficacy and weakness of those algorithms. Some of these attacks are simple and others are extremely complicated. Recent advances in cryptography involve more information theoretic [1], [2] techniques in message attack and defense. One of those new techniques is isomorphic cipher reduction [2], which is the practice of treating one cipher as if it were another cipher for purposes of attack, evaluation, and the design of stronger ciphers. The use of cipher reduction requires the user to have some basic background in cryptography and an in-depth understanding of the mathematics behind the use of ciphers.

II. Background

In this section, we present the required background beyond what is normally found in classes on the subject.

A. Differences in Ciphers

Most ciphers are classified by the type of obscuring that is used in the encryption algorithm. Shannon indicated that the major types of obscuring were substitution, permutation, and transformation [3]. Additionally, some ciphers are said to be "linear." The linear cipher is

$$CT = (a(PT) + b)\%m \tag{1}$$

where CT is the cipher text, PT is the plain text, % indicates the modulo function, m is the modulus, and a and b are the secret key(s) shared by the parties to the encryption. Shannon indicates that this can be any linear operation, which is characterized by the following relationship

$$f(x \circ y) = f(x) \circ f(y) \tag{2}$$

Transformation (T) ciphers are ciphers that change the order of symbols, but do not necessarily obscure the symbols. This reordering of the symbols can be disorienting, but often it is easily solved. This type of obscuring is a form of a permutation (P) cipher that operates on symbols instead of bits.

P ciphers transpose the bits of a symbol and reorder them in such a way as to obscure the information. There are two main ways to reorder the information: inside the same symbol and inside a block of symbols taken together and remapped. The key for P ciphers is the mapping or location of the bit in the new symbol/block of symbols. Since most symbols are composed of a byte, relocation can be thought of as either inside the same byte or having the possibility of moving across byte boundaries. Moving bytes into different bytes prevents byte-wise evaluation of a P cipher since all of the information for a single byte may not be found in the same byte. Examples of P ciphers include a bit rotation cipher or rotating bytes in a block.

While there are many individual encryption functions, all encryptions treat keys in one of two ways: symmetric and asymmetric. Symmetric keys use the same key to encrypt and decrypt, while asymmetric keys employ one key to encrypt and another to decrypt. There are many ciphers that make use of symmetric keys. They include most of the S, P, and T ciphers. Public key encryptions (PKE/PKI) [4] are the foremost examples of ciphers that use asymmetric keys;

978-1-6654-0066-4/21/$31.00 ©2021 IEEE

however, the value of having two keys is limited by revealing the public key and leaving only the private key secret.

Ciphers are not always applied to a single symbol [5]. Many ciphers take a block of m symbols from a message at a time. For example, AES 256 encrypts 64 byte sized symbols simultaneously [6]. These ciphers are known as "block" ciphers, the Lucifer cipher (later revised and accepted as the first Data Encryption Standard (DES) cipher [7]) developed at IBM by Horst Feistel, is generally considered the first such cipher to be developed and released for use. Block ciphers come in many forms and complexities, ranging from block substitution to complex Feistel Round ciphers [6]. Block ciphers have a larger alphabet than single byte ciphers and are generally more secure than ciphers with a smaller alphabet size.

An advancement on block ciphers is the practice of re-encrypting the output of a cipher with a second cipher. These ciphers are generally classified as being either "cascade" or "product ciphers" [5]. The difference between the two types of ciphers is that a cascade cipher uses the same key for all of the ciphers applied and a product cipher uses different keys for each cipher. Cascade ciphers are generally weaker than product ciphers. With a cascade cipher the security of the cipher is only as strong as the weakest cipher used [8]. Product ciphers are generally stronger, but that strength comes at the cost of overhead and latency.

Of the ciphers mentioned, the most important cipher for this paper is the substitution cipher. Other cipher algorithms are important, but it can be shown that all ciphers can be represented as a substitution cipher. Therefore, a more in-depth understanding of the substitution cipher is warranted.

B. The Substitution Cipher

One of the most basic ciphers is one that has been used for thousands of years, the substitution (S) cipher. S ciphers have been known since at least the time of Julius Caesar [6]. The principle involved is that for every symbol in an alphabet of a language, that symbol is replaced in an alphabet (A) by some symbol from the replacement alphabet (A'). Mathematically $A \mapsto A'$. However, it is not required that $A \neq A'$, and in principle, it is quite possible that $A \mapsto A$. In practice it often occurs that the two alphabets are identical to each other. The function $\mapsto$ is known as a "mapping" and is a mathematical function that pairs a member of the domain of the function to a member of the range of the function. When used in cryptography, the mapping function is a 1:1 and onto (or "bijunctive" [9]) function. While the mapping from the domain to the range can follow some easily identified mathematical rule, there is no requirement for a rule to be specified. Therefore, the mapping can be arbitrarily assigned between the sets of $\{A\}$ and $\{A'\}$.

The S cipher is defined by an instantiation of a particular mapping $A \mapsto A'$. Shannon noted that this type of mapping constitutes the practice of "confusion" of encrypted information [3], one of the basic types of obscuring of information. In addition to identifying the type of encryption provided by the S cipher, Shannon also noted that the application of confusion does not disguise patterns in the encryption. Patterns are one of the keys that allow attackers to decrypt messages without the secret key [10] and recover hidden messages. The inability to hide patterns during encryption is a major flaw in the S cipher.

Despite the flaw of failing to hide patterns, the S cipher is still one of the major building blocks of ciphers. S blocks are routinely used in modern block ciphers [6] and are foundational for all ciphers. Horst Feistel, the father of modern round ciphers, said that, at a fundamental level, all ciphers are S ciphers [11]. While most cryptographers acknowledge this (in principle, at least), the equivalence is also literal. Every cipher can be shown to be an instance of an S cipher, under the proper conditions.

C. The Metacharacter Assumption

Shannon discusses groupings of letters in a language, called "*n*-grams" [3]. These groups of letters are formed from n consecutive letters, ignoring spaces and punctuation, concatenated together. Taken as a group, these collections of letters have a frequency characteristic to a language. Some of the combinations never appear in a language and are termed "forbidden" [2]. The use of *n*-grams in decryption methods is well documented [2], [3], [12] and has proven to be very powerful. However, the use of *n*-grams has traditionally been limited to the evaluation of S ciphers. Permutation (P) ciphers [6] make use of a property of encryption known as "diffusion," to spread information across different symbols in an effort to make decryption more difficult [3]. By moving bits of information between symbols during encryption the grouping of the original information is not known and therefore evaluating encryption symbol by symbol results in errors that confound decryption efforts. For this reason, P ciphers, or algorithms that mix P ciphers with other types of encryption, are thought to be very powerful [3]. Shannon indicates that compound, or "product" ciphers [5] of the form

$$F = LSLSLT \tag{3}$$

where L are linear ciphers and T are transposition ciphers are considered to be mathematically strong. Transposition is a form of the P cipher that changes the order of the symbol or bits representing the symbol. Transposing bits of a cipher among a block of symbols is considered even stronger.

Countering permutation is not difficult. Consider an m-gram where $m = |B|$, where B is a block of symbols in which diffusion takes place. If that block is considered to be a symbol (a "metacharacter") in a new, related language [2], then all of the information remains in the same metacharacter and analysis can be greatly simplified. Metacharacters are part of a "metalanguage" related to the original, single character block language from which they are abstracted. It can be shown that metacharacters have a characteristic frequency that arises from the speaker in the text [13], [14]. Therefore, an attacker can use metacharacters as if they were single characters in the new metalanguage for lexical, syntactical, and semantical analysis. The typical approach, when used, is to set the metacharacter size to be the size of a block that is being encrypted [2].

This approach was used with the collision attack to break applications of the Cipher Block Chaining (CBC) Mode [15]–[17].

D. Idempotence

Idempotence is a very important property of some mathematical and computer science operations. This property can be applied multiple times without changing the result of the application to the multiple individual operations. That is, if the same operation can be applied more than once and the result is the same when the operation is applied one, two, or n times, the operation is said to be 'idempotent" [18], [19]. For example, consider the logical AND operation. AND is said to be idempotent because the result of

$$A \wedge B = (A \wedge B) \wedge B = ((A \wedge B) \wedge B \wedge B) \tag{4}$$

The repeated application of logically ANDing B has the same effect as doing the operation exactly once. The same happens with logical OR. In mathematics the repeated application of identities is also idempotent. Boolean algebra is a lattice and all lattices are known to be idempotent.

In a closely related operation in computer science and cryptography, idempotence can be applied to some ciphers. For the S cipher, assume that the output of one S cipher is then encrypted by another S cipher. That is

$$CT(M) = E_{S,k_0}(E_{S,k_1}(M)) \tag{5}$$

For two applications of the S cipher, there exists a third key (k_2) such that [20]

$$E_{S,k_0}(E_{S,k_1}(M)) = E_{S,k_2}(M) \tag{6}$$

This says that repeatedly encrypting with the S cipher does not mean that, as is commonly practiced, that each S cipher must be solved separately, but rather that *all* of the S ciphers can be replaced with a single S cipher. Therefore, any chain of applied S ciphers can be solved as if it is a single S cipher with the appropriate key. Mathematically

$$E_{S,k_0}(E_{S,k_1}(...(E_{S,k_n}(M))...) = E_{S,k'}(M) \tag{7}$$

or symbolically

$$S_0 S_1 ... S_n = S' \tag{8}$$

III. Cipher Reduction

Cipher reduction is the action of replacing one encryption with another for analysis and work on a particular cipher, or group of ciphers. Reduction states that for two ciphers, c_0 and c_1, that $\exists c_0$ with k_0 and c_1 with k_1 such that

$$E_{c_0,k_0}(M) = E_{c_1,k_1}(M) \tag{9}$$

Furthermore, $\forall M$ having a k_i using the cipher $c_0 \rightarrow \exists$ some k_j such that the mapping $\{CT\} \mapsto \{PT\}$ is identical for both pairs of cipher/key. If this is the case, then the cipher that was originally used to encrypt the message (c_0) can be replaced, or "reduced," to the new cipher (c_1), because the ciphers and keys are equivalent [2].

In order for reduction to take place, there are certain requirements that must be true for the ciphers involved and the message that is being treated by the reduction. These requirements are

1) The domain for the reducing cipher must include the domain of the reduced cipher - The reducing cipher must contain the same alphabet from which mappings are made, if not actually be the same alphabet. If there is no mapping available for the plain text to be made into cipher text, then some information may not be encrypted. This means that for the original alphabet ($\{A\}$) the reducing cipher alphabet ($\{A'\}$) must have the property that $\{A\} \subseteq \{A'\}$
2) The range for the reducing cipher must include the range for the cipher being reduced - The reducing cipher must contain the same alphabet, or include the alphabet, of range. If this is not true the two encryptions cannot map the same way. That is to say, if the original cipher and key pair map $A \mapsto B$ then the second cipher and key pair must map $A \mapsto C$ where ($\{B\} \subseteq \{C\}$). Omission of a single character in the output alphabet will not allow for identical mappings in all cases.
3) There must exist a key such that the mappings for the two ciphers remains the same - For all cases there must be a key that corresponds to any possible mapping for the original key.

These conditions apply *only* to encryptions, and not to modes. Modes are a special case of randomization functions that are designed to be both reversible and to allow for mappings that violate the 1:1 assumption. Therefore, modes, such as Cipher Block Chaining Mode (CBC) [6], are not encryption functions.

A. XOR Equivalence to S

One of the more common ciphers used as a constituent in block product ciphers is the XOR cipher. Applied to a block of b bits, the key for the cipher is also b bits long. Fore each block B_i in a message composed of n concatenated blocks $M = ||_{i=1}^{n} B_i$, encryption follows the formula

$$CT_i = PT_i \oplus K_{XOR} \tag{10}$$

This performs a bitwise XOR for each bit in the block and the key. The plain text alphabet for the function is the set of all combinations of 0 and 1 bits contained in a block of size b bits. The cipher text is composed of the same combinations, as the bits may change value, but are still in the same set. Thus $\{PT\} = \{CT\} = \{00...0, 11...1\}$ for collections of bits of size b. Using the $\mapsto$ function, it is possible to map any PT to CT values, using the constraint that the mapping follows the applied XOR function with the key. Each bit maps to either a 0, or 1, which is in the range of the set for the bit. Therefore, all conditions are met for reduction of the XOR to the S function, assuming the function is applied on the block level for blocks of the same size.

B. P Equivalence to S

The P cipher also works on the bit level. In this case the bits are mapped from one location in a block to another bit location. For a block of b bits the location in the key set corresponds to the bit location in the plain text. So, for key location K_i plain text bit B_i

$$CT_{K_i} = PT_{B_i} \tag{11}$$

As with the XOR cipher, the plain text alphabet is the set of all combinations of 0 and 1 bits contained in a block of size b bits. The cipher text is composed of the same combinations, as the bits may change value, but are still in the same set. Thus $\{PT\} = \{CT\} = \{00...0, 11...1\}$ for collections of bits of size b. Using the $\mapsto$ function, it is possible to map any PT to CT values, using the constraint that the mapping follows the mapping key for the P cipher. This meets the conditions for reduction of the P cipher to the S cipher.

C. Feistel Reduction

Consider a round based cipher, such as a Feistel Round Cipher [6] whose typical structure is shown in Figure 1. A Feistel Round is actually a part of a product cipher composed of multiple simple ciphers. A simple Feistel Round is shown in Figure 2. There are many types of rounds that use various ciphers, but commonly used ciphers include the XOR, S, Rotation (P), and may also use S and P networks such as those used in AES. However, for ease of illustration, this paper will use one of the type shown in Figure 2.

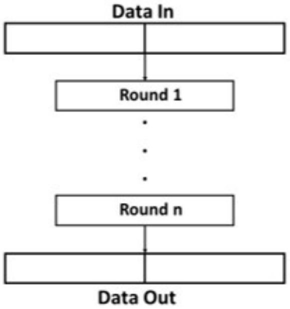

Fig. 1. Feistel Block Cipher Structure

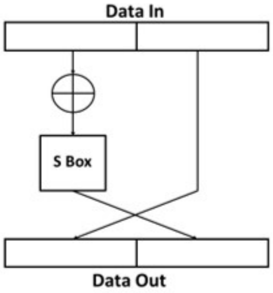

Fig. 2. A Typical Round

The number of rounds that are used in block ciphers of this type can vary from 2 to any desired number. Analysis of the number of rounds has indicated that at least 8 rounds are required in order to achieve a good mixing of the bits in the cipher. More rounds ensure a better mix, and 16 rounds are generally recommended. However, AES uses 14 rounds [6].

Reducing a round of the type selected in the example begins with ensuring that all data is being subjected to the same encryption methods. The round as shown in Figure 2 subjects half of the data to an XOR and S cipher before applying the P rotation. Such an "unbalanced" encryption can quickly be made balanced by applying an XOR with the key of all 0 bits and an S cipher whose key is the identity key, such that for any symbol (s_i) in the block $s_i \mapsto s_i$ (see Figure 3). Then the two blocks can be combined in to a combined, single encryption step.

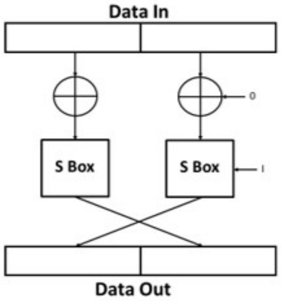

Fig. 3. A Balanced Round

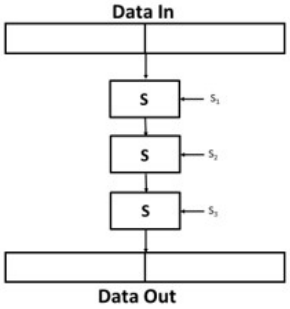

Fig. 4. The Reduced Round

The XOR cipher with block size of n bits is equivalent to an S cipher of identical size with an equivalent key S_1 such that

$$E_{XOR,k_1}(M) = E_{S,S_1}(M) \tag{12}$$

No reduction needs to be done to the S cipher boxes. This is already an S cipher with key S_2. Half of the key is the identity key and is already known.

Following the S boxes, the cipher then rotates the two half blocks, reversing the order of the half blocks. Rotation of this type is a form of the P cipher with a very simple key. Each bit is rotated to the right by an offset of

$$O = \frac{|B|}{2} \tag{13}$$

with mappings from the original bit location of

$$b_{new} = (b_{old} + O) \ \% \ |B| \tag{14}$$

It has previously been shown that P ciphers reduce to an S cipher. In this case the key is S_3. As a result of the reduction process, the Feistel Round can now be represented as shown in Figure 4.

Next, the property of idempotence is applied to the separate ciphers in the round. By idempotence the three S ciphers can be reduced from three S ciphers to a single S cipher with an equivalent key

$$S_e = S_1 S_2 S_3 \tag{15}$$

Each round can therefore be replaced by a single S cipher with key $S_{e,rn}$, where rn indicates the round number. With sixteen rounds, idempotence is again applied to the individual round ciphers.

$$S_{e,r} = S_{e,r1} ... S_{e,r16} \tag{16}$$

Substituting this into the round cipher results in a single PSP product block cipher as shown in Figure 5. At this point, the P ciphers that feed the equivalent S cipher and also is fed by the S cipher can be replaced with equivalent S ciphers. After reduction, the three S ciphers can be reduced into a single S

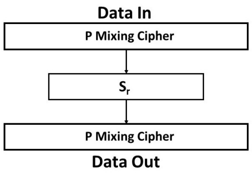

Fig. 5. Structure of a PSP Type Round Cipher

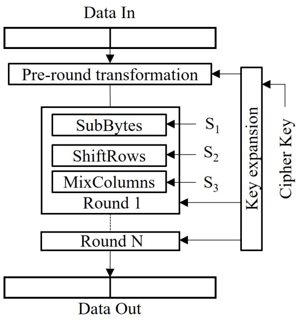

Fig. 6. Structure of AES Reduced

cipher by idempotence. As long as the ciphers being reduced are applied to the same block sizes, reduction is possible on Feistel round ciphers, including AES and other related ciphers. This reduction applies only to ciphers and does *not* apply to modes or ciphers with modes. AES is a Fiestel Round type cipher. The structure of AES is shown in Figure 6. Using the same approach and by applying idempotence, the rounds in AES also reduce to a single S cipher, so AES is also vulnerable to this attack.

IV. Using Cipher Reduction

Cipher reduction allows the analysis of complex ciphers, such as block product ciphers, and gives insight into how to handle those ciphers. Many popular block ciphers are in the form of PSP and SPS type ciphers. Combining P and S ciphers is thought to be much more secure, especially if the P cipher has bit mappings that cross symbol boundaries. However, are PSP and related types of ciphers really all that much more secure than S block ciphers with the same size key?

The answer can be shown in two parts. First, consider the relative security of a PSP cipher to an S cipher of equivalent sizes and using the same alphabet. The comparison is made using the measure of the unicity distance, which indicates how fast information is allowed to accumulate using both types of ciphers. Sec is the security ratio between the two types of ciphers. Both cipher types are assumed to be of the same block size, consisting of b bits and having an alphabet of $|A|$ symbols. The derivation of the relationship is

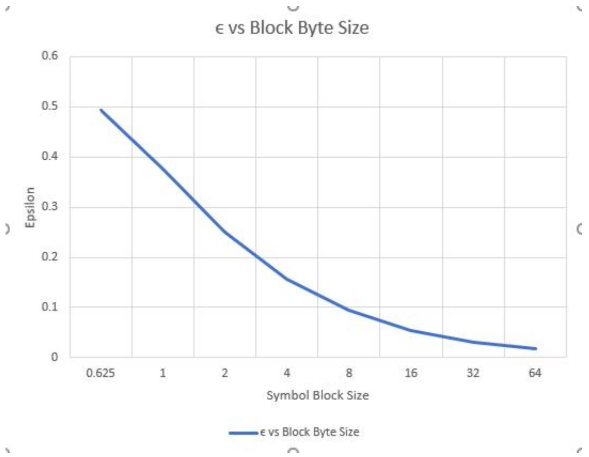

Fig. 7. Epsilon by Block Size

$$\begin{aligned} Sec_{PSP,S} &= \frac{n_{PSP}}{n_S} && (17) \\ &= \frac{\frac{log(|K_{PSP}|)}{R_\lambda log|A|}}{\frac{log(|K_S|)}{R_\lambda log|A|}} && (18) \\ &= \frac{log(|K_{PSP}|)}{|log(K_S|)} && (19) \\ &= \frac{log(2^b|A|!2^b)}{log(|A|!)} && (20) \\ &= \frac{log(2^b)+log(|A|!)+log(2^b)}{log(|A|!)} && (21) \\ &= 1+\frac{2log(2^b)}{log(|A|!)} && (22) \end{aligned}$$

Let

$$\epsilon = \frac{2log(2^b)}{log(|A|!)} \qquad (23)$$

Then

$$Sec_{PSP,S} = 1+\epsilon \qquad (24)$$

The relationship between $|A|$ and b is such that the number of bits required, at a minimum, to represent a unique encoding of the alphabet requires more bits than the number of symbols in the alphabet when

$$|A| > 4 \qquad (25)$$

At that point, $\epsilon < 1$. The larger the size of the block, and therefore the size of the alphabet, the smaller ϵ becomes. Eventually, $\epsilon = 0$. Figure 7 shows the drop in ϵ with increasing block size, in terms of bits. This chart starts with the minimum encoding for the lower case English alphabet at 26 characters. Additional block sizes, normalized for 8 bit character encoding, such as found in ASCII encoding, in powers of 2. By the time that encryption reaches block sizes of 256 bits, the present size of government required security, $\epsilon = 0.03125$, a small additional measure of security.

These figures for ϵ depend on the maximum size of the key space and possible alphabet size. If the effective key space is smaller than the maximum, the value for ϵ will be correspondingly smaller. Practically, the curve shown in Figure 7 is actually an *upper limit* on the value of ϵ. If the key space is smaller than is expected, then the value may be smaller. But, the use of cipher reduction can gives a more accurate view of the relative security. In the preceding discussion, it was shown that a PSP type cipher can be replaced with a single S cipher. Therefore, mathematically the ratio becomes

$$Sec_{PSP,S} = \frac{n_{K_e,S}}{n_S} = 1 \tag{26}$$

Therefore, there is *no* difference in security between a block PSP cipher and a block S cipher of the same block size and for the same message. Cipher reduction enables an easy way to compare what appear to be two fundamentally different ciphers. The strength that comes from block product ciphers comes primarily from the increased size of the key rather than the mixing of disparate ciphers.

A second outcome of cipher reduction is applicable in decryption. For many years security professionals have been creating decryption algorithms to attack specific encryption algorithms. Hackers and researchers have speculated that a single, universal decryption algorithm exists and can be used to attack all types of encryptions. Using cipher reduction to reduce the constituent ciphers involved into a single S cipher of a particular block size allows an attacker to use the proper language statistics and employ a single decryption algorithm for a large number of ciphers, including block ciphers. That algorithm is the attack approach used for a block substitution cipher. Any algorithm that is effective for block S ciphers will work for a wide variety of ciphers.

The universal approach will not work when some additions are made to ciphers. These include:

- Product block ciphers with block boundaries that do not coincide - Product ciphers do not have to have the same boundaries for changing keys. Those ciphers which have key changes at different, but regular, offsets from each other break up the blocks and make it impossible to match the block size and accomplish isomorphic reduction.
- Product block ciphers where each cipher has different block sizes - In a polymorphic environment the block size of a cipher does not always remain constant. It is quite possible to encrypt with block ciphers whose block size is chosen either at random or through a guided security function to maximize message security. Reducing a cipher requires that the block size be identical to the original cipher, making a changing block size difficult, if not impossible, to predict *a priori* accurately. Therefore, an elastic and changing block size frustrates reduction.
- Polymorphic ciphers - Polymorphic, or “mutating” ciphers [2] employ evolving and unpredictable changes in ciphers and block sizes. Changing the key for a submessage means that the attacker must know the boundaries of each of the shards in the message in order to correctly reduce the cipher(s). This makes polymorphic ciphers reduction resistant, if not reduction proof.
- Ciphers with randomization functions - The additions of randomization alters the composite key of a message and is designed to make each block in the cipher resistant to reduction. While this makes the cipher resistant there are other attacks, such as the collision attack [15], [16], which are side channel attacks that target the randomization algorithm to accomplish encryption breaks.
- Modes - Most modes add randomization algorithms to encryption. Of the eight modes, six employ various randomization routines to make the encryption look like it has no patterns and is more random. Electronic Codebook (ECB) mode uses no randomization and one mode changes block ciphers into serial ciphers. Cipher reduction is possible in ECB mode, but is not used in other modes. See the comments on ciphers with randomization functions and side channel attacks that are viable in those situations/modes.

V. Conclusion

Feistel said that at their hearts, all ciphers are S ciphers [11]. This comment, made in the 1970’s, should be interpreted literally. Using the metacharacter assumption and the property of idempotence it can easily be shown how to replace (or reduce) other ciphers to the S cipher. In this paper, we have shown the path to reduce XOR, P, and block ciphers to the S cipher and how to treat block product ciphers, such as Feistel round and AES type ciphers into a single S cipher. Cipher reduction allows for these ciphers to be attacked as an S cipher and shows that a universal decryptor is possible based on S cipher attack methods. We also presented the proof that, with cipher reduction, that the security that is added by using mixes of P and S ciphers is negligible.

While cipher reduction is a powerful tool, it is not a universally useful attack. Cipher reduction does not work well with certain encryption techniques. Any type of block cipher that is polymorphic, changes block sizes, and randomly mixes different keys throughout its application can be made resistant to cipher reduction. Further, most modes are also immune because they add a layer of randomization. However, modes appear to be susceptible to side channel attacks based on their randomizing layer.

Cipher reduction should be considered when designing encryption algorithms and mixing different encryption methods. Decryption strategies can also be adjusting by using the same approach. By understanding how the encryption algorithms relate to each other and weaken the total security a much stronger encryption is possible. Cipher reduction is another, powerful tool for all security providers.

References

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

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

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

[4] Johannes A. Buchmann, Evangelos Karatsiolis, and Alexander Wiesmaier. *Introduction to Public Key Infrastructures*. Springer-Verlag, Berlin, Germany, 2013.

[5] Uli Maurer and James Massey. Cascade ciphers: The importance of being first. *Journal of Cryptology*, 6(1):55 – 61, 1993.

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

[7] W. Diffie and M.e. Hellman. Special feature exhaustive cryptanalysis of the nbs data encryption standard. *Computer*, 10(6):74–84, 1977.

[8] Uli Maurer and James Massey. Cascade ciphers: The importance of being first. *Journal of Cryptology*, 6(1):55 – 61, 1993.

[9] John B. Fraleigh. *A First Course in Abstract Algebra*. Addison-Wesley, 7^{th} edition, 2003.

[10] Auguste Kerckhoffs. La cryptographie militaire. *Journal des sciences militaires*, IX:5 – 83, 161 – 191, 1883.

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

[12] Shmuel Peleg and Azriel Rosenfeld. Breaking a substitution cipher using a relaxation algorithm. *Communications of the ACM*, 22:598 – 605, 1979.

[13] Andrew Morton. *Literary Detection*. Scribners, New York, 1978.

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

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

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

[17] 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.

[18] Cesar Polcino Milies and Sudarshan K. Sehgal. *An Introduction to Group Rings, Algebras and Applications*. Kluwer Academic Publishers, 2002.

[19] Encyclopedia of mathematics, 2001.

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