Industry Security Brief

MERLINCRYPTION®

A Review of Attacks & Exploits Against Encryption

How ASBE Defeats Statistical Analysis, Cryptanalysis, & Attacks

OVERVIEW: ADVANCEMENTS AGAINST ENCRYPTION ATTACK

Anti-Statistical Block Encryption (ASBE) uses blocks [Ref-27, p.43-82] as part of the algorithm. These blocks are manipulated in ways different from all currently known and published existing encryption algorithms.

The ASBE algorithm is designed to be exponentially stronger than existing encryption algorithms and to defeat Statistical Analysis, all known Cryptanalysis and other attacks. The purpose of this Security Brief is to describe some of the attacks and provide a high-level view for ASBE's inherent ability to eliminate these threats.

STATISTICAL ANALYSIS

Since early encryption, techniques are typically variations of substitution ciphers. Statistical analysis attempts to defeat such substitution ciphers, based on statistical knowledge of the language. [Ref-1] [Ref-2] [Ref-3] [Ref-26, p.10-13]. These techniques include identifying substitution ciphers in letter frequency or byte frequency, repeating patterns, and other statistical data.

> *Some of the fundamental attributes of ASBE, which overcome a statistical analysis, include its ability to never repeat patterns, its nondeterministic outputs, including cyphertext, variable keys, and digital signatures.*

MATHEMATICAL ANALYSIS

RSA ENCRYPTION, which is not symmetric, depends on factoring large numbers into a small number of primes. The efficacy of this encryption algorithm depends on the non-symmetry of the ease of multiplication vs. the much harder steps needed to factor a number. Because of steady advances in mathematics in factoring of large numbers, RSA keys up to 1000 bits can relatively easily be broken [Ref-5] [Ref-6] [Ref-26, p.159-162, 255-261, 470-474] [Ref-27, p.185-206, 223-244].

ELLIPTICAL CURVE CRYPTOGRAPHY [Ref-25], is not symmetric. It is based on the algebraic structure of elliptical curves. This encryption algorithm depends on the (unproven) assumption that finding the

discrete logarithm of a random elliptic curve element with respect to a publicly known base point is infeasible. Because of continual advances in mathematics, this assumption is likely to be proven invalid, and will increasingly require larger and larger keys, as is evident for RSA [Ref-26, p.261-263, 480-481, 496-498].

SIMPLE XOR AND COUNTING COINCIDENCES [Ref-26, p.13-15]. Simple XOR is symmetric. This approach attempts to determine, first the length of the key, and then eliminate the key without knowing its value, to determine the plaintext. This approach does not apply to ASBE because: the key is not used in a predictably cyclical fashion.

> *ANTI-STATISTICAL BLOCK ENCRYPTION: Mathematical analysis is inconsequential to the ASBE algorithm, as it has no fixed steps where mathematics can be used to discover random values. This aspect is reinforced by the non-linear techniques of its random data generator (which never repeats a pattern) and its key approach, which are also not mathematically driven.*

KEY EXCHANGE

One of the two highly successful attacks against encryption is the fixed and well-defined key exchange mechanism. Keys must be exchanged by some manner or protocol, and then must be stored. Key lifecycle management schemes, including the transfer and storage of keys, are complex and the process, itself, creates multiple attack vectors.

> *ASBE has no fixed or defined key exchange mechanism or protocol [Ref-27, p.245-278]. Keys are created and only exist during the encryption or decryption instance and then promptly destroyed, with all memory scrubbed. Associated risk is eliminated, as there is no key to transfer or store. It is not necessary to exchange keys when setting up or using ASBE. The resulting benefit is a significant reduction in the overhead cost to manage keys [Ref-27, p.297-346], as well as a surge in operational efficiency and productivity.*

RANDOM NUMBER GENERATORS

Another successful technique in breaking encryption or inserting back doors in encryption is through exploiting the limitations of random number generators (RNG), which are at the heart of most encryption. Most attacks on encryption are actually attacks on RNGs and one notable back door/hack dealt with random number generators and involved elliptic curves, specifically DUAL_EC_DRBG. That standard has a relationship to a secret set of numbers. Anyone who knows those numbers can effectively predict the standard's output and break any encryption schemes using it.

The primary shortcoming of RNGs is 'periodic behavior' where patterns eventually must repeat. Historically, the flaw has been abused to profit from casino/slot machine payouts or to out-maneuver frequency hopping, but more recently has become a formidable threat of crimes, which exploit Artificial Intelligence and Quantum Computing capabilities.

Another defective issue with RNG is that the sequence of random numbers is correlated in multiple dimensions. This problematic behavior decreases entropy, which reinforces the hacker's ability to beat the RNG. When the hacker obtains enough samples, all the subsequent values of the RNG become completely predictable and its randomness is vanquished.

> *MerlinCryption's parameterized Random Data Generator (RDG) uses non-linear technique and never repeats a pattern, which together, solve decreasing entropy issues and periodic behavior issues. The exponentially large space of the MerlinCryption RDG changes patterns every time it is used, which overwhelms the reasoning, pattern matching, and predictability techniques of AI. Coupled with its non-linear aspects, the RDG thwarts any attempt toward mathematical parallelism, factoring, encoding/decoding, and order-finding capabilities of the quantum computer.*

CRYPTANALYSIS AND OTHER ATTACKS

Over the last decades, multiple forms of cryptanalysis [Ref-4] [Ref-26, p.5-7] have been developed to break or mathematically reverse engineer encryption.

ASBE is designed to defeat these techniques, including those shown in the table below. Definitions of various cryptanalysis and other attacks are shown and referenced later in this paper.

A.1 Boomerang attack	**A.10** Chosen-plaintext attack
A.2 Brute Force attack	**A.11** Adaptive-chosen-plaintext attack
A.3 Davies' attack	**A.12** Chosen-cyphertext attack
A.4 Meet-in-the-middle attack	**A.13** Chosen-key attack
A.5 Related-key attack	**C.1** Differential cryptanalysis
A.6 Slide attack	**C.2** Impossible differential cryptanalysis
A.7 XSL attack	**C.3** Integral cryptanalysis
A.8 Cyphertext-only attack	**C.4** Linear cryptanalysis
A.9 Known-plaintext attack	**C.5** Mod-n cryptanalysis

ASBE CRYPTOGRAPHIC CONTRIBUTIONS

- The algorithm is nondeterministic and exhibits different behaviors regardless of input. Each encryption process always results in a different cyphertext, even when repeating the same plaintext to encrypt, key, and digital signature. No two encryptions are alike.
- The algorithm is not subject to attack models and methods of Cryptanalysis, Statistical Analysis, or Mathematical Analysis.
- Mathematical approach of factoring or ECDLP or similar analysis cannot be used against the algorithm, as it uses a sequence of non-linear steps, which exhibit no periodic repetition.
- The use of the key is not cyclic in its length. Standard differential analysis and byte frequency cannot be used against it.
- The algorithm allows for keys and digital signatures of variable length.
- Key generation, communication, and storage cannot be detected, as random data generators create-use-destroy the parameter-controlled key during the encrypting instance and then recreate-use-destroy the key at time of decryption. The key only exists at its time of use. There is no key to store, and no key to transfer.

ASBE CHARACTERISTICS

- The algorithm is symmetric encryption.
- Described as anti-statistical, nondeterministic, and stochastic.
- Variable key length scales between 2008 bits and 2 gigabytes.
- Variable digital signatures scale up to 64KB in length and are also encrypted.
- The encryption engine scrubs memory before exiting so the key, digital signature, and other parameters are not available to be discovered by another program which allocates all available memory to examine its contents.
- ASBE's small footprint satisfies restricted memory requirements with its 17KB encryption engine, 25KB low-overhead solution, and 220KB encryption authentication system.
- The encryption software is portable to any CPU.
- Payloads can be transmitted by any communications protocol and on any network.

ASBE EXPONENTIAL QUALITIES

- Mathematical exponential notation is the quantity representing the power to which a number or expression is to be raised. An exponential quantity is a number with a superscripted number.

This indicates that one should multiply the number by itself, the number of times of the superscripted number. For example, $2^3 = 2 * 2 * 2 = 8$.

- In cryptography, encryption keys are fixed in length, repeating over and over to produce the cyphertext. Brute force guesses and cryptanalysis deduces in order to determine the key and extract plaintext from cyphertext.
- The ASBE algorithm allows for keys of variable length from 2008 Bits to 2 Gigabytes. A 2008-bit key is a billion times a billion times a billion (times a Billion 58 times) stronger than a 256-bit key length. Every additional bit in a key, doubles the number of possibilities and doubles the time to break it by brute force. Each additional byte in the key increases by a multiplier of $2^8 = 256$ times.
- The ASBE algorithm further allows digital signatures, with the same exponential characteristics as the key. Using the largest digital signature of 64KB this multiplies the number of possibilities by $2^{8*65535}$ which is 2^{524280} which is approximately 10^{157284}.

ATTACKS & EXPLOITS DEFINED WITH THE ASBE ATTRIBUTES WHICH DEFEAT EACH

A.1 Boomerang Attack

A variation of Differential Cryptanalysis which uses differences in multiply selected input data to be encrypted that takes advantage of the different stages or rounds used by the algorithm in order to determine the key. [Ref-20] Differential cryptanalysis, [Ref-19], and the Boomerang Attack, [Ref-20], do not apply to ASBE for multiple reasons:

- The length of the resulting cyphertext is a stochastic variable.
- Differences in the input plaintext or key have no linear correlation with the resulting cyphertext.

A.2 Brute Force Attack

This approach tries every possible key to decrypt an intercepted encrypted message. It is only useful for small keys. Brute force attacks use a combination of:

- A very fast and/or quantum computer,
- Many computers, and/or
- Special purpose hardware.

Examples of Brute Force Attacks include:

- DES encryption, with its 56-bit keys, is broken in a matter of hours by custom hardware. [Ref-7] [Ref-8] [Ref-26, p.265-285]. **NIST** has since declared DES (among others) as not secure, see [Ref-9].

- SSL encryption is broken by 112 computers in hours [Ref-10]. SSL is broken by 200 PSPs with added factor of weakness of MD5 hash [Ref-11].

Note that the age of the universe is about 13.5 billion years, which is about $4.34*10^{17}$ seconds [Ref-12]. The current fastest computer can execute just under 10^{15} instructions per second, and it can take many thousands to millions of instructions to try each key. This means this fastest computer could try about 10^{11} to 10^{14} keys per second. It would take this computer a few minutes to less than hour to brute force crack a 56 bit DES encrypted message.

- MerlinCryption's ASBE Algorithm, with its scalable keys (with lengths of 2008 bits up to 2GB (Giga Bytes), make this kind of attack astronomically impractical. Each additional key bit doubles the number of possible keys, or, every additional key byte multiplies the time for brute force attack by 256, an exponential growth [Ref-26, p.153].
    - There are 2^{256} or about $10^{9*8.5}$ (a billion times a billion less than 9 times) possible AES keys of length 256 bits.
    - ASBE's smallest key has 2008-256 = 1752 more bits, increasing the brute force time by $2^{1752} = 10^{9*58.3}$ (a billion times a billion 58 times).
- Using every available computer (over 10^{12} computers) it would still take over a billion times a billion 32 times the age of the universe to brute force guess the smallest ASBE key.

A.3 Davies' Attack

This attack is specific to DES encryption and does not apply to ASBE because the ASBE key length is not only larger than the DES key, but is also variable in length [Ref-13].

A.4 Meet-in-the-Middle Attack

The Meet-in-the-Middle Attack attempts to work forward from the plaintext and backwards from the cyphertext, for the purpose of "meeting in the middle" to reduce the amount of work needed to deduce the key. There is an assumption that this same key will be used again. This attack does not apply to ASBE because for any given input, (plaintext, key, and digital signature), there is no single output cyphertext: the cyphertext is *different every time*, and yet it always decrypts correctly [Ref-14] [Ref-26, p.48-49]. In addition, there is no need to use the same key repeatedly, and with the MerlinCryption system**,** the key can be automatically changed for every encryption.

A.5 Related-Key Attack

The Related-Key Attack attempts to use different keys with known mathematical relationships as a method to mathematically deduce a target key. This attack does not apply to ASBE because there is no predictable mathematical relationship between keys used in different encryptions that mathematically map to changes in the cyphertext [Ref-15].

- There is no predicable relationship between keys used in different encryptions.
- The length of the encrypted digital signature is likely to be different.
- The length of encrypted data is a stochastic variable.

A.6 Slide Attack

The Slide Attack attempts to defeat multi-round encryption by exploiting the sub key used in each round which may be used in a repetitive way, which then renders the number of rounds irrelevant. This attack does not apply to ASBE because fixed sliding is not used, and there is no inherent sub-key or algorithmic step related to a round. [Ref-16].

A.7 XSL Attack

An XSL Attack attempts to find and solve quadratic simultaneous equations which describe the algorithm, and then use eXtended Sparse Linearization to solve for the key. This attack, while effective against AES encryption, does not apply to ASBE. Because of the stochastic nature of the ASBE algorithm, there is no fixed inverse function [Ref-17].

A.8 Cyphertext-Only Attack

Given multiple encrypted messages (or ciphertexts), the goal is to deduce the plaintext, and/or the key [Ref-26, p.5-6]. This method is not effective against ASBE encrypted data or files for multiple reasons:

- Each encrypted message contains an encrypted digital signature of unknown length.
- The length of encrypted data is a stochastic variable.

A.9 Known Plaintext Attack

In this attack, [Ref-26, p.6, 7], the cryptographic analyst has both the encrypted message and the resulting cyphertext, with the goal to deduce the key. This method is not effective against ASBE encrypted data or files for multiple reasons:

- Each encrypted message contains an encrypted digital signature of unknown length.
- The length of encrypted data is a stochastic variable.

A.10 Chosen Plaintext Attack, and

A.11 Adaptive-Chosen Plaintext Attack

These attacks, [Ref-26, p.6], combine the known plaintext attack with the ability to choose the plaintext to encrypt and see the resulting cyphertext. This method is not effective against ASBE encrypted data or files for multiple reasons:

- Each encrypted message contains an encrypted digital signature of unknown length.
- The length of encrypted data is a stochastic variable.

A.12 Chosen-Cyphertext Attack

In this attack, [Ref-26, p.6], the cryptographic analyst can choose different cyphertext to be decrypted and has access to resulting cyphertext, with the goal to deduce the key. This method is not effective against ASBE encrypted data or files for multiple reasons:

- Each encrypted message contains an encrypted digital signature of unknown length.
- The length of the resulting cyphertext is a stochastic variable.

A.13 Chosen-Key Attack

In this attack, [Ref-26, p.7], the cryptographic analyst doesn't actually choose the key, but knows something about the relationship between the keys. This method is not effective against ASBE encrypted data or files for multiple reasons:

- Each encrypted message contains an encrypted digital signature of unknown length.
- The length of encrypted data is a stochastic variable.

C.1 Differential Cryptanalysis

Differential Cryptanalysis is based on the correlation between changes in the input and the resulting changes to the output after encryption. This is done by knowledge of the transforms performed by the encryption algorithm. The skipjack encryption algorithm, [Ref-18], as well as DES encryption (among others), have been broken by differential cryptanalysis. Differential cryptanalysis, [Ref-19], and the Boomerang Attack, [Ref-20], do not apply to ASBE for multiple reasons:

- The length of the resulting cyphertext is a stochastic variable.
- Differences in the input plaintext or key have no linear correlation with the resulting cyphertext.

C.2 Impossible Differential Cryptanalysis

Impossible differential cryptanalysis exploits the impossibility (that is, changes having probability 0) of differences in every stage of the encryption algorithm to improve what differential cryptanalysis predicts as possible [Ref-21]. Impossible differential cryptanalysis does not affect ASBE for multiple reasons, including that every possible block value *can* occur, independent of the input.

C.3 Integral Differential Cryptanalysis

Integral cryptanalysis uses sets of plaintexts where some of the content is held constant and some of the content is varied through all possibilities, with the intent to deduce how the algorithm works. Integral differential cryptanalysis, [Ref-22], does not affect ASBE for multiple reasons. Two reasons are because:

- Every possible block value *can* occur.
- The change of a single bit in the input plaintext, does not result in a change in the cyphertext having a fixed or predictable position.

C.4 Linear Cryptanalysis

Linear cryptanalysis [Ref-23] is based on finding affine [Ref-28] approximations to the algorithm. Linear cryptanalysis does not apply to ASBE for multiple reasons which include:

- The length of resulting cyphertext is a stochastic variable.
- For any given input (plaintext, key, or digital signature) there is no single output cyphertext (it is different every time – yet always decrypts correctly).
- There is nothing even remotely similar to an affine transformation in the algorithm between the inputs (plaintext, key, and digital signature) and the output (cyphertext).

C.5 Mod-n Cryptanalysis

Mod-n cryptanalysis [Ref-24] exploits unevenness in how an encryption algorithm operates over congruence classes modulo n. Mod-n cryptanalysis does not apply to ASBE for multiple reasons. The change of a single bit in the input plaintext or key, does not result in a:

- Change in the cyphertext having a fixed position.
- Change in a single or fixed number of positions in the cyphertext.t

REFERENCES:

[Ref-1] http://en.wikipedia.org/wiki/Letter_frequency

[Ref-2] http://en.wikipedia.org/wiki/Frequency_analysis

[Ref-3] http://www.letterfrequency.org/

[Ref-4] http://en.wikipedia.org/wiki/Cryptanalysis

[Ref-5] http://techie-buzz.com/tech-news/1024-bit-rsa-cracked.html

[Ref-6] http://arstechnica.com/uncategorized/2007/05/researchers-307-digit-key-crak-endangers-1024-bit-rsa

[Ref-7] http://en.wikipedia.org/wiki/Brute_force_attack

[Ref-8] http://en.wikipedia.org/wiki/EFF_DES_cracker

[Ref-9] http://www.nist.gov/manuscript-publication-search.cfm?pub_id=907517

[Ref-10] http://www.marktaw.com/technology/HowlongdoesittaketocrackS.html

[Ref-11] http://hackaday.com/2008/12/30/25c3-hackers-completely-break-ssl-using-200-ps3s/

[Ref-12] http://en.wikipedia.org/wiki/Age_of_the_universe

[Ref-13] http://en.wikipedia.org/wiki/Davies'_attack

[Ref-14] http://en.wikipedia.org/wiki/Meet-in-the-middle_attack

[Ref-15] http://en.wikipedia.org/wiki/Related-key_attack

[Ref-16] http://en.wikipedia.org/wiki/Slide_attack

[Ref-17] http://en.wikipedia.org/wiki/XSL_attack

[Ref-18] http://en.wikipedia.org/wiki/Skipjack_(cipher)

[Ref-19] http://en.wikipedia.org/wiki/Differential_cryptanalysis

[Ref-20] http://en.wikipedia.org/wiki/Boomerang_attack

[Ref-21] http://en.wikipedia.org/wiki/Impossible_differential_cryptanalysis

[Ref-22] http://en.wikipedia.org/wiki/Integral_cryptanalysis

[Ref-23] http://en.wikipedia.org/wiki/Linear_cryptanalysis

[Ref-24] http://en.wikipedia.org/wiki/Mod-n_cryptanalysis

[Ref-25] http://en.wikipedia.org/wiki/Elliptic_curve_cryptography

[Ref-26] "Applied Cryptography", by Bruce Schneier, 2nd Ed. 1996, John Wiley & Sons, ISBN 047117099

[Ref-27] Practical Cryptography", by Niels Ferguson and Bruce Schneier, 2003, John Wiley & Sons, ISBN 0471223573

[Ref-28] http://en.wikipedia.org/wiki/Affine_transformation