MERLINCRYPTION®

Anti-Statistical Block Encryption

Forward-Looking Innovation Secures Today's Threats and Tomorrow's Risks

MERLINCRYPTION WHITE PAPER
www.merlincryption.com

Contact MerlinCryption
512-348-SAFE

The Critical Need for a Superior Encryption Algorithm

An element of stealth is required to effectively navigate today's uncertain cyber terrain. Anti-Statistical Block Encryption (ASBE) fulfills this prerequisite with breakthrough innovation. As news headlines frequently report, current methods of encryption key creation and algorithmic flaws have caused repeated security breaches, exposing sensitive data, trade secrets, and critical intelligence of American business and government.

MerlinCryption overcomes fundamental weaknesses, which exist in the industry's approach to securing data, Cloud, VoIP, and networks. 1) Encryption key methods have inherent risks and reveal why keys and passwords are the first-line target of today's attacks. 2) Static encryption algorithms with predictable patterns and output.

WEAKNESS #1: Encryption Key Approach

Commonly used encryptions produce simple short key strands with fixed lengths. Business and government entities have been compromised, even when using RSA keys, due to their mathematically based structure.

These solutions must transfer keys from the encrypting party to the decrypting party. Criminals intercept the key in transit, steal confidential data, or change the message for criminal intent. Frequently used Public Key Infrastructure (PKI) and certificate authorities create gaping attack vectors.

SOLUTION #1: *ASBE's key method derails key attack*:

- Variable-length keys scale between 2008 bits and 2GB. Because keys change in length, criminals cannot identify the key in the resulting cyphertext. After key creation, the ASBE encryption platform dynamically alters generated data, exponentially increasing protection.
- Keys are reinforced by variable-length file passwords up to 64KB, which are automatically deployed in each encryption instance.
- MerlinCryption's Embedded Encryption Platform circumvents MiTM, key theft, and other attacks against the key. The patented random data generator outputs keys and passwords, which are created-used-destroyed at the encrypting end point and then re-created-used-destroyed at the point of decryption. No transfer necessary. No PKI. No risky certificates.

AND…A BOTTOM-LINE BONUS: *Research shows that organizations spend between $47 and $598 for the creation, distribution, and maintenance of each PKI key in use.[1] ASBE significantly reduces the cost and labor of PKI by eliminating key certificates, registration authority, directory management, central key deposit, external validation, and complex protocols.*

WEAKNESS #2: Static Encryption Algorithms

The second drawback of today's encryption is static algorithms, which repeat processes over and over again. These predictable and anticipated behaviors make hacking easier.

SOLUTION #2: *Anti-Statistical Block Encryption (ASBE) algorithmic complexity leverages dynamic action*:

- ASBE has no static behavior and creates variable output. Patterns cannot be anticipated.
- Every encryption instance produces different cyphertext, even when repeating identical keys, passwords, and plaintext input. No two encryptions are alike.
- The algorithm incorporates a unique table-driven approach

Anti-Statistical Block Encryption (ASBE)

Radically Different…Irrefutably Secure

The ASBE algorithm differentiates from its encryption predecessors to overcome inherent risks, which are subject to today's increasing computer power and contemporary criminal technique.

Game Changers:

- Described as anti-statistical + key-dependent block encryption, ASBE uses blocks as part of the algorithm. These blocks are manipulated in ways different from all currently known and published existing encryption algorithms in a variable way, which depends on the key.
- Variable key length scales between 2008 bits and 2 gigabytes.
- Passwords scale to 524,280 bits in length.
- ASBE always produces different cyphertext, even when repeating the same data input, same key, and same password. No two encryptions are alike.
- ASBE is twice as fast as AES.
- ASBE's small footprint satisfies restricted memory requirements. The encryption engine is less than 22KB, the low overhead platform is 55KB, and the embedded encryption platform is 200KB

Security Strengths:

- The algorithm is not subject to attack models and methods of Cryptanalysis.
- Byte frequency cannot be used against it.
- A mathematical approach of factoring, ECDLP, or similar analysis cannot be used against the algorithm, which uses a sequence of non-linear steps and exhibits no periodic repetition.
- Keys and passwords are generated-used-destroyed-recreated, on demand at each end-point.
- Key transfer between end points is not necessary: no storage required. Eliminates PKI and need for Certificate Authorities.
- The encryption engine scrubs memory before exiting so the key, password, and other parameters are not available.

Operational Benefits:

- Embedded Encryption Platform (200K) easily integrates into code modules of other systems
- Low Overhead Embedded Encryption Platform (55K) secures where space is critical, such as UAV/UAS solutions
- Encryption is portable to any CPU
- Encrypted Payloads are transmitted by *any* communications protocol and on *any* network
- Written in C, the platform SDK compiles for Linux, Windows, DOS, and custom systems

ASBE's Exponential Function Drives Invulnerable Protection

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 $2^3 = 2 \times 2 \times 2 = 8$.

In cryptography, encryption keys are fixed in length, repeating over and over to produce the cyphertext. Brute force guesses and cryptanalysis deduces to determine the key and extract plain text from cyphertext.

The ASBE algorithm allows for keys of variable length from 2008 bits to 2 gigabyte. 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. Thus, each additional byte in the key increases by a multiplier of 2^8 = 256 times.

The ASBE algorithm further allows passwords, with the same exponential characteristics as the key. Using the largest password of 64KB this multiplies the number of possibilities by $2^{8 \text{ X } 65535}$, which is 2^{524280} which is approximately 10^{157284}.

The cryptosystem of the ASBE algorithm extracts keys and passwords from any existing file or from randomly generated data. Using a 2-GB data source, there are up to 4,000,000,000,000,000,000 possible keys or 1,200,000,000,000,000 possible passwords. And, using the platform, these large keys can be scripted to automatically change, as desired; for example, every minute, every second, every message, or other.

Dynamic Security…'Above and Beyond'

All solutions developed at MerlinCryption leverage a dynamic quality. This dynamic element is critical to achieving secure data, as well as guaranteeing client system integrity.

ASBE patent pending Embedded Encryption Platforms delivers a customized ecosystem, which is distinctive to each particular client's environment. Each platform contains special components that dynamically alter generated data, as well as independent control mechanisms.

Encryption vendors generally do not provide encrypted authentication and typically structure authentication on 'something you know', 'something you have' or 'something you are'. MerlinCryption innovated a new authentication category, incorporating dynamic factors, which leverage "something temporary and always unique." Customized authentication factors are changeable and variable, and cannot be identified or predicted by hackers. The current market's typical 2- and 3-factor authentication, pales to ASBE's extensive fourth-factor options.

Summary

In today's IT environment of constant cyber threats, it takes a forward-thinking approach to conquer attack. Compliance is necessary to uphold government regulations. Standards support good architecture. But, neither compliance nor standards guarantee security.

ASBE technology surpasses all competing solutions with pioneering innovation that delivers the security that business and military need, now. Organizations achieve compliance, standards, *and* security with 'above and beyond' comprehensive Embedded Encryption Platform solutions, featuring encryption, authentication, and no-cost key management.

MerlinCryption's forward-looking technology proactively secures against today's threats and tomorrow's risks.

About Paul "Prem" Sobel, Cryptographer and ASBE Developer

Paul H. (Prem) Sobel is an American cryptographer, mathematician, engineer, and designer of the Anti-Statistical Block Encryption (ASBE) algorithm. He holds three U.S. patents in CPU Architecture and one U.S. classified patent.

Sobel graduated with honors and a B.S.E.E. Electrical Engineering from Pratt Institute, and graduated second in his class with an M.S.E.E. Electrical Engineering from California Institute of Technology (Caltech).

Sobel's focus in cryptography began during his master's work at Caltech in the late 1960's. He later invented a new algorithm for testing probability distributions, by viewing the data in multiple dimensions. After discovering flaws in currently used random number generators and studying limitations of fixed key length encryption algorithms, Sobel began developing a new cryptographic approach that would overcome these weaknesses.

His advanced work in the foundations of mathematics along with Sobel's new random test, contributed to the development of the ASBE algorithm, which introduces variable key length and Cryptanalysis-defeating properties.

Sobel developed one of the first graphical hidden line removal algorithms used for data analysis. Jet Propulsion Lab (JPL) NASA used this algorithm, with Sobel's Gaussian surfaces technique, for Mars terrain modeling and robotic mission planning.

As a summer college intern, Sobel identified a recurrent problem in IBM's testing system that saved the company $1 million per year. Upon Caltech graduation, Sobel worked for (JPL) NASA where he was recognized with an individual commendation for his automation of Mariner 9 and Viking 75 spacecraft programming on planetary probes.

Sobel's earlier security work encompasses log management, NAC, super computer design, graphical and audio presentation of Big Data in eleven or more dimensions, and image processing. Sobel was a co-founder of Vitesse Semiconductor in 1984 and of MerlinCryption in 2011 where he is currently Chief Technical Officer and leads Cryptographic Architecture.

About MerlinCryption

MerlinCryption develops infrastructure security software, delivering advanced encryption, authentication, a patented random data generator and two breakthrough Embedded Encryption Platforms for Cloud, VoIP, eCommerce, M2M, and storage media hardware. The company focuses in critical-need areas, including financial services, healthcare, critical infrastructure sectors, and military.

Forward-looking encryption technology secures data against known and critical risk factors, which are inherent in today's encryption. The unprecedented Embedded Encryption Platform SDK protects the integrity of data-at-rest, data-in-motion, data-in-use, and data-in-change as it is created, viewed, edited, shared, stored, and moved across communications channels and through the Cloud.

ASBE has successfully undergone review and testing at Cyber Innovation Center/LA Tech, as well as withstood commercial pentesting attacks. Encryption products are BIS approved for export without a license, subject to OFAC. Solutions enable clients with FDA, HIPAA, and HITECH compliance.

1. http://www.nymity.com/Free_Privacy_Resources/Previews/ReferencePreview.aspx?guid=8539fba5-9d92-4293-b3ea-d10bf4b52cf0