WhiteboxCRYPTO

Cryptographic Key Hiding with Tunable Security and Performance

Cryptographic Key Protection

Access to data, information systems, and digital content is commonly protected using cryptographic methods. Unfortunately, cryptography was designed to operate in private. In most systems, this privacy assumption can be violated, hence the moment a cipher uses its keys, it risks exposing them—and thereby eliminating all cryptographic security guarantees. The usage of cryptographic keys is easily identifiable in software routines using signature, pattern, and memory analysis. Typically, key extraction attacks against keys coded as literal data arrays in unprotected applications can be successfully completed in a matter of hours.

Microsemi's WhiteboxCRYPTO™ product combines mathematical algorithms, data, and code obfuscation techniques to transform the key and related crypto operations in complex ways requiring deep knowledge in multiple disciplines to attack. Importantly, the key is never present in static or runtime memory. Rather, the key becomes an inert collection of data that is useless without the uniquely generated white box algorithm. WhiteboxCRYPTO comes in many variants:

WhiteboxAES™	128, 192, and 256-bit key protection
WhiteboxRSA™	Encrypt/decrypt/sign/verify all key sizes
WhiteboxECC™	p160/192/224/256/384/521 prime curve
WhiteboxSHA™	SHA1, SHA2 224/256/384/512 + HMAC
Whitebox3DES™	DES and 3DES for all key sizes
WhiteboxOXD™	Obfuscation for sensitive data transfer
WhiteboxSSL™	provides protection from known and future OpenSSL vulnerabilities and attack vectors
WhiteboxFFC™	Finite Field Crypto/Diffie-Hellman-Merkle
WhiteboxJCE™	Facilitates the use of third party implementations through Java Cryptography Extension (JCE)
WhiteboxTLS™	Transport Layer Security (TLS) protocol
WhiteboxNK108™	NIST SP800-108 KDF

Whitebox Key Transformation

To protect encrypted information, it is imperative that the key never be revealed in memory or on disk. Standard crypto implementations leave both the algorithm and key vulnerable to tampering and reverse engineering. WhiteboxCRYPTO mathematically transforms the cipher arithmetic (and correspondingly, the key) using a variety of mathematical transforms tailored to the specific features of the cipher. In this form, the cipher can operate without exposing the key, even under the intense scrutiny of white-box attack.

Hardware ID binding allows integration of a hardware identifier into the WhiteboxCRYPTO library offering the potential for node-locking or introduction of hardware-based checks as a prerequisite for initializing the crypto implementation.

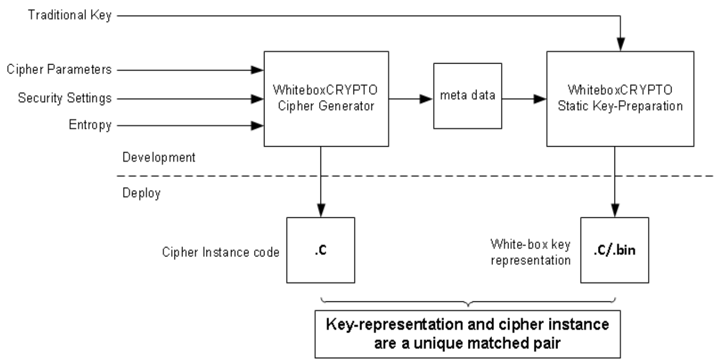
Traditional Key
Cipher Parameters
Security Settings
Entropy
WhiteboxCRYPTO Cipher Generator
meta data
WhiteboxCRYPTO Static Key-Preparation
Development
Deploy
Cipher Instance code
.c
White-box key representation
.c/.bin
Key-representation and cipher instance are a unique matched pair

Figure 1: WhiteboxCRYPTO generates diverse uniquely randomized white-box instances using complex transformations tailored to the target cipher's mathematics

The WhiteboxCRYPTO product allows you to: Generate a unique crypto library for each application shipped, and encode the same classical key for each; produce a single library and encode many keys to work with it; or encode multiple keys for multiple libraries. Each deployment of WhiteboxCRYPTO is supported by key-preparation tools for the deployed white-box instances, and debugging support libraries. Instances are typically deployed as a static library with associated C header files that can be integrated into an application using a fully documented software API.

Supported Platforms

WhiteboxCRYPTO libraries support configurable key sizes, are little and big endian compatible, run on both 32-bit and 64-bit systems, and are fully compatible with any environment that can link C libraries. WhiteboxCRYPTO was developed in a US only facility by cleared US citizens, is EAR export controlled, and is immediately ready for deployment in C and C++ software applications running on nearly any hardware and operating system configuration.

WhiteboxCRYPTO

Cryptographic Key Hiding with Tunable Security and Performance

Use Cases

WhiteboxCRYPTO is useful wherever cryptography must be performed in a potentially vulnerable environment or where the crypto keys and/or plaintext data must be protected even if an untrusted user has taken complete control of the host system. Such use cases include compromise of networked systems, software delivered to business competitors, or commercially deployed software with private keys.

Additionally, WhiteboxCRYPTO can receive input and produce output in an obfuscated data format, suitable for use with other algorithms in the WhiteboxCRYPTO suite. In this way, WhiteboxCRYPTO can keep data secured in addition to key material.

Security Features

- Key Hiding
- Hardware Binding
- Runtime Randomization
- Performance Customization
- CodeSEAL™ Interoperability

Table 1: Features and Benefits

Features	WhiteboxCRYPTO Benefits
Hides Keys Completely	Actual key bits never form in memory, thwarting various memory attacks. The obfuscated white box form is resistant to break-once-run-everywhere exploits.
Simple, Documented API	A simple, fully documented API enables quick implementation of secure encryption, decryption, signing, and verifying functionality.
Binds Keys to Hardware	Hardware identifiers can be mathematically integrated into a key, binding an application and sensitive data to a particular hardware platform.
Customizable Performance	Tunable encrypt/decrypt throughput allows full performance vs. security tradeoffs.
Highly Portable	Source code based implementation is portable to all platforms and compatible with any software protection technique. WhiteboxCRYPTO functions as little or big endian, 32-bit or 64-bit, compatible with any environment that can link C libraries.
Managed Keys Solution	The white box version of the key can be stored externally to a WhiteboxCRYPTO library enabling key updates, key escrow, etc.
Protects data in-transit	WhiteboxCRYPTO produces data in obfuscated form usable by other algorithms within the WhiteboxCRYPTO suite. Thus, data is protected during intermediate stages of a sequence of cryptographic operations.

Microsemi makes no warranty, representation, or guarantee regarding the information contained herein or the suitability of its products and services for any particular purpose, nor does Microsemi assume any liability whatsoever arising out of the application or use of any product or circuit. The products sold hereunder and any other products sold by Microsemi have been subject to limited testing and should not be used in conjunction with mission-critical equipment or applications. Any performance specifications are believed to be reliable but are not verified, and Buyer must conduct and complete all performance and other testing of the products, alone and together with, or installed in, any end-products. Buyer shall not rely on any data and performance specifications or parameters provided by Microsemi. It is the Buyer's responsibility to independently determine suitability of any products and to test and verify the same. The information provided by Microsemi hereunder is provided "as is, where is" and with all faults, and the entire risk associated with such information is entirely with the Buyer. Microsemi does not grant, explicitly or implicitly, to any party any patent rights, licenses, or any other IP rights, whether with regard to such information itself or anything described by such information. Information provided in this document is proprietary to Microsemi, and Microsemi reserves the right to make any changes to the information in this document or to any products and services at any time without notice.

Microsemi Corporation (Nasdaq: MSCC) offers a comprehensive portfolio of semiconductor and system solutions for communications, defense & security, aerospace and industrial markets. Products include high-performance and radiation-hardened analog mixed-signal integrated circuits, FPGAs, SoCs and ASICs; power management products; timing and synchronization devices and precise time solutions, setting the world's standard for time; voice processing devices; RF solutions; discrete components; security technologies and scalable anti-tamper products; Ethernet solutions; Power-over-Ethernet ICs and midspans; as well as custom design capabilities and services. Microsemi is headquartered in Aliso Viejo, Calif., and has approximately 3,600 employees globally. Learn more at www.microsemi.com.

Microsemi Corporate Headquarters
One Enterprise, Aliso Viejo, CA 92656 USA
Within the USA: +1 (800) 713-4113
Outside the USA: +1 (949) 380-6100
Sales: +1 (949) 380-6136
Fax: +1 (949) 215-4996
email: sales.support@microsemi.com
www.microsemi.com