

Syncrosoft Crypto Toolbox

The discovery of encryption keys is one of the most prevalent threats to security systems.

Syncrosoft's white-box algorithms are designed to defeat this threat.

Introduction

The security of DRM, Conditional Access and other security systems that run on untrusted hosts heavily depends on the protection of crypto-algorithms like ECC and AES. The algorithm's keys and internally processed data are traditionally protected using obfuscation techniques, but are usually revealed during the process and thus vulnerable to attacks.

Consequently, there is a need for the protection of an algorithm's program code, the encryption keys and internally processed data in a secure way.

Product Overview

The Syncrosoft Crypto Toolbox includes white-box implementations of the encryption algorithms ECC, AES, DES and Triple-DES, and the hash functions SHA-1 and SHA-256. Using these algorithms, keys and data of DRM and security systems that run on untrusted hosts can be protected.

White-box cryptography is an effective technique used to prevent that encryption keys or internal processing data of algorithms are exposed. Syncrosoft's white-box implementations compute on permanently encrypted keys and data, and they are robust against debugging, reverse-engineering, analysis and tampering.

Proven Security

MCFACT™, a core part of Syncrosoft's white-box technology, is deployed on hundred thousands of PCs and has never been cracked since the launch of the technology in the year 2000.

Targeted Customers

The Syncrosoft Crypto Toolbox is designed for companies, who are actively developing security solutions or are in need for robust security technology for the protection of software and digital content.



Syncrosoft Crypto Toolbox

Featuring: ECC and AES Algorithms

ECC and AES are standard algorithms widely deployed in DRM systems. By using Syncrosoft's white-box implementations of ECC and AES, DRM systems running on untrusted hosts or in hostile environments can be protected against attacks and tampering, thus securing digital content from illicit decryption and distribution.

Syncrosoft's white-box AES is offered in three variants, which allows for scaling of performance and level of security.

White-Box Algorithms combined with MCFACT

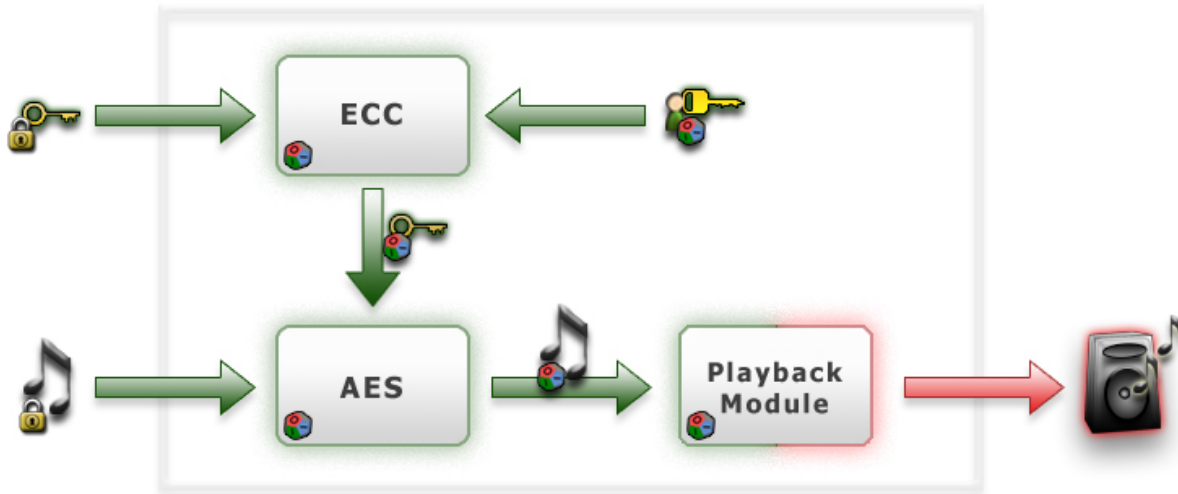
The white-box algorithms may be integrated in unprotected program modules, but this alone does not prevent the algorithm's surrounding program code from being attacked. If the white-box algorithms are used within program modules which are protected by Syncrosoft's MCFACT technology, the security level is increased dramatically. In such a scenario, even the algorithm's input/output data would not be exposed, because MCFACT protects the surrounding program code and data against debugging, analysis and tampering.

Application Areas

- Protection of encryption keys and data used by applications that run in hostile environments, for instance DRM and Conditional Access systems, banking applications, security applications, games, etc.
- Protection of encryption keys and data that are processed in a digital media pipeline of software media players, etc.
- Protection of client-side encryption keys, data and program code in client-server environments, etc.
- Ensuring the security of DRM systems and digital media pipelines that have to comply with robustness rules required by the content industry.
- Applications and libraries can be individualized by embedding a constant encryption key securely in the algorithm's program code.

Syncrosoft Crypto Toolbox

Application Example: Protected Media Pipeline



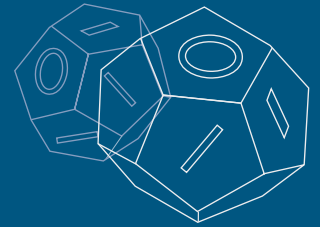
This diagram shows how a digital media pipeline can be protected securely by applying Syncrosoft's white-box and MCFACT technologies. All secure elements of the pipeline are represented by the color green, whereas the color red is used to represent the insecure elements.

Syncrosoft's white-box implementations of ECC and AES in combination with MCFACT allows the keys and digital contents to remain protected while being processed in the modules and while forwarded from one module to another. The user key remains protected when used to decrypt the ECC protected content key, as well as the AES key remains protected, both while being decrypted in the ECC component, and while used for the actual content decryption in the AES module. The contents remain secure even when forwarded from the AES module to the playback module.

Security Features

- Debugging and reverse-engineering does not reveal any useable information about an encryption key, because the algorithm's internal program code and data are always kept encrypted.
- Syncrosoft's white-box technology and MCFACT protect the algorithm's program code and make it resistant against debugging, reverse-engineering, analysis, illegal re-use and tampering.
- Syncrosoft's white-box technology and MCFACT protects the actual program code and data of the algorithms. These technologies do not rely on superfluous protection code or libraries, which could be circumvented or removed.
- A constant encryption key can be integrated in the algorithm's program code, making it impossible to replace the key.

Syncrosoft Crypto Toolbox



Other Key Features

- Fundamental attributes of the algorithms, like security level, execution speed and memory allocation, can be tuned to meet specific requirements.
- All major PC platforms, including operating systems like Microsoft Windows 2000, XP, Vista and Mac OS X, are supported.
- The Crypto Toolbox supports the ANSI C and C++ programming languages for all major PC platforms.
- Deploying the Crypto Toolbox is transparent to the end-user and does not require the installation of additional software modules.

Crypto Toolbox Suite

The Syncrosoft Crypto Toolbox Suite provides the tools, documentation and developer support required to integrate the white-box encryption and hashing algorithms into applications.

For more information about Syncrosoft's Crypto Toolbox, technical details and other Syncrosoft products, please visit our website or send an e-mail to contact@syncrosoft.com

Syncrosoft - The Company

Syncrosoft, founded in Hamburg/Germany in 1991, develops and markets superior crypto and security solutions used for IP- and software copy-protection.

Syncrosoft targets international markets, and successfully supplies its patented technologies to customers in the software, digital content and security solutions industry in Europe, USA and Japan.