Dynamic Encryption HW/SW integration

Søren Sennels, COO

April 2019

Dynamic Encryption is a patented novel encryption principle, which allows building new cryptosystems with improved security and flexibility. This white paper describes how Dynamic Encryption can be used to construct new secure cryptosystems and how it applies to a wide range of applications.

Advanced Encryption Standard (AES)

Today, the AES symmetric block cipher has become the de-facto encryption standard worldwide and is used in a wide range of applications such as HTTPs, FTPs, TLS communication protocols and most VPN applications. It was adopted as a US federal standard in 2002 and is included in the ISO/IEC 18033-3 standard.

The original algorithm (Rijndael) was invented in 1997 by Vincent Rijmen and was the winner of a competition called by the American National Institute of Standards and Technology (NIST) to find a successor for the insecure Data Encryption Standard (DES).

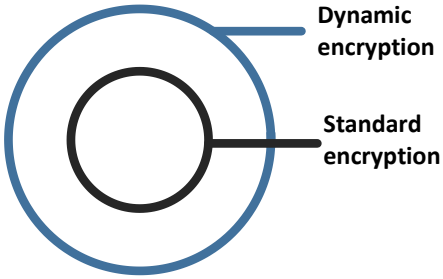
AES has proven its worth and is, 20 years later, still robust against any known practical attacks despite the many attempts by researchers worldwide.

However, the success of AES is also its drawback. As AES is adopted worldwide and is by far the most used encryption standard, attackers can focus on a single cryptosystem and dedicate all processing power towards breaking the AES. It is well-known how far cryptanalysis of AES has developed in the academics, but how far state-sponsored actors has reached in breaking AES is not known.

This threat leads to concerns for the lifetime of the AES-standard mostly among military, governments and financial institutions.

Dynamic Encryption principle

The Dynamic Encryption principle is the invention of Professor Lars Ramkilde Knudsen at the Technical University of Denmark.



The principle provides enhanced protection by changing not only the encryption keys but also the cryptosystem for every new data transmission.

The principle can be realised in many ways, but usually, a two-layer encryption approach is used, where a standard encryption (i.e. AES) is wrapped by a dynamic layer which adds encryption components configured by a key (i.e. randomly generated S-boxes).

"We conclude that the method of Dynamic Encryption is sound and secure according to the state of the art in cryptology."

-Vincent Rijmen

The advantages of the two-layer approach are:

- Seen from the outside the crypto-system changes each time the dynamic layer is configured. It may happen at the beginning of data transmissions or anytime during the transmissions.
- The cryptosystem is guaranteed to have a minimum level of security. Even if a particular realization of the dynamic layer does not provide any added protection, the cryptosystem is still as strong as the standard encryption forming the inner layer. In practice, it will be more secure as encryption components have been added.

Advantages of Dynamic Encryption

Applying the Dynamic Encryption principle has several benefits over traditional standard encryption systems:

- **Prevents cryptanalysis.** The art of cryptanalysis requires vast amounts of data encrypted by the same algorithm. Using the dynamic encryption principle, each data transmission is encrypted using a unique cryptosystem. Hence the cryptanalyst is not able to collect the required data material.
- "**Moving target defence.**" With an ever-changing cryptosystem, an adversary cannot automate his attack but is forced to change the methodology for each data transmission.
- **Outside the "AES-spotlight"**. It is expected that state-sponsored actors focus most of their effort on the AES-encryption due to its wide adaptation. Using the Dynamic Encryption principle brings the application outside the target area for these attacks.
- **Lifetime extension.** As the Dynamic Encryption layer shields the inner algorithm from attacks, the Dynamic Encryption principle extends the lifetime of the cryptosystem

Applications

In general, the Dynamic Encryption principle can be used in all applications requiring advanced end-to-end encryption, such as:

- Satellite and cellular communications
- Tactical data links (wired and wireless)
- Radio links
- IoT devices
- High-speed backbone networks
- Sensor networks
- Vehicles

The cryptosystems may be optimized for the specific application to ensure optimal performance wrt security, latency, speed, overhead.

Proprietary crypto systems

A special application of the Dynamic Encryption principle is the possibility of designing new secure cryptosystems or enhance existing proprietary cryptosystems.

This is useful for nations with a need to obtain a national encryption scheme or with a need to strengthen an existing national crypto.

A novel crypto system can be constructed by wrapping a standard encryption with a customized and proprietary implementation of the Dynamic Encryption layer.

Likewise, an existing crypto be strengthened by wrapping an existing proprietary cryptosystem with a Dynamic Encryption layer.

In both cases, a minimum level of security is guaranteed by choice of the inner, standard encryption.

About Dencrypt

Dencrypt A/S specialises in developing and providing solutions based on the principle of Dynamic Encryption.

Dencrypt was established to enable everyone to communicate in confidence. Dencrypt combines advanced encryption technology with user-friendly operation.

Dencrypt delivers Common Criteria certified products, which has been accredited for classified information by NATO and the Danish Defence. All Dencrypt personnel and board members have security clearance for Danish SECRET by the Danish Defence Intelligence Service.

Dynamic Encryption was invented by Lars Ramkilde Knudsen, professor at the Technical University of Denmark.

Dencrypt has offices in Copenhagen and Aalborg, Denmark.

www.dencrypt.dk