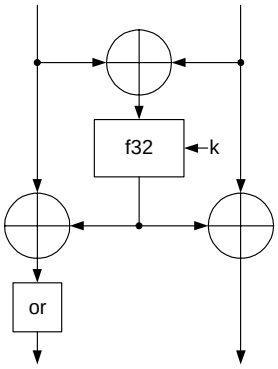
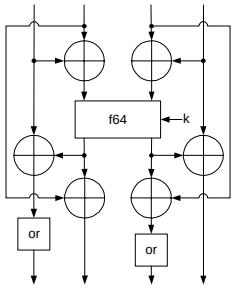
MediaCrypt®

IDEA NXT® Technical Description

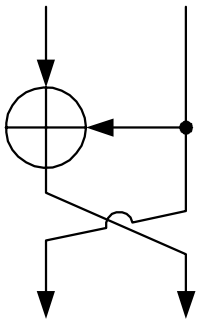
2005 FROST & SULLIVAN Excellence in Technology Award



Graph 1: *lmor64*



Graph 2: *elmor128*



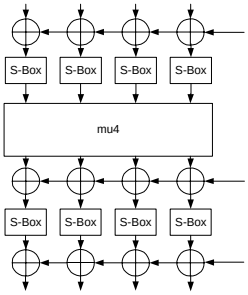
Graph 3: Ortomorphism *or*

IDEA NXT is the name for a patented and universally applicable family of block encryption algorithms that helps to secure digital media, communications and storage. It was inspired by comprehensive customer feedback and developed in partnership with university research at EPFL-LASEC (The Security and Cryptography Laboratory at the Swiss Federal Institute of Technology, in Lausanne).
The primary attributes of IDEA NXT are high security, high performance, and a unprecedented level of implementation flexibility.

It's high-level mathematical structure is based on a Lai-Massey scheme. The round functions are Substitution-Permutation Networks (SPNs). In addition, a new design of strong and efficient key schedule algorithms have been developed.
Peer reviews by Prof. David Wagner, University of California, Berkeley (USA), and Prof. Jacques Stern, Ecole Normale Supérieure, Paris (France), demonstrate evidence of security proof.

The Crypto algorithm

Both, the 64 bit (NXT64) and the 128 bit (NXT128) versions of IDEA NXT, are iteration of a round functions with an isomorphism, in the range of 1 up to 254 rounds, followed by an output-function without isomorphism.
The encryption process uses the sub keys created by the key management algorithm in their normal order, while the decryption process uses them in reverse order and inverted isomorphism.
The primary round function of the 64 bit-version *lmor64* (graph 1) is a Lai-Massey-scheme combined with an orthomorphism, while the 128 bit-version *elmor128* (graph 2) is an Extended-Lay-Massey-scheme combined with two orthomorphisms.
The orthomorphism *or* (graph 3) is a one-round Feistel scheme with the identity function as round function.



Graph 4: f32

The function f32 (graph 4) builds the core of NXT64, while the function f64 (2x f32) builds the core of NXT128. Both functions have three main parts:

– substitution part, denoted sigma4/sigma8
– diffusion part, denoted mu4/mu8
– round key addition part

The diffusive part of f32 is a linear (4;4)-multipermutation defined over GF(2^8), while the diffusive part of f64 is a linear (8; 8)-multipermutation defined over GF(2^8).

block size	key size	key schedule version
64	0 ≤ key ≤ 128	64-light
64	136 ≤ key ≤ 256	64-heavy
128	0 ≤ key ≤ 256	128

Table 1

The Key Management algorithm

'Key Management algorithm' denotes a sub-key schedule algorithm. This is the term used in the original specification and within our literature.

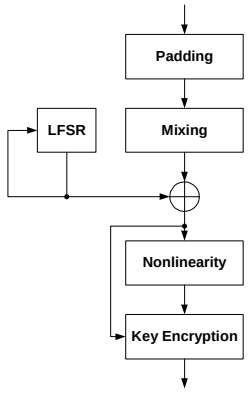
A key used in IDEA NXT must have a bit-length from 0 up to 256 bit, with a multiple of 8 bit. Depending on the key length and the block size, a member of the IDEA NXT block cipher family uses one out of three different key schedule algorithm versions.

Table 1 shows the relation between key size, block size and the key schedule algorithm.

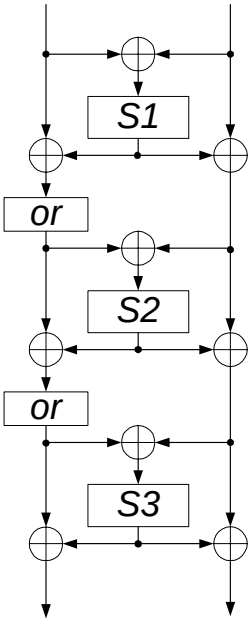
All three versions are constructed out of four main parts followed by a key encryption (graph 5):

– padding part P, expanding the input key into the full length in its category,
– mixing part M, mixing the randomness provided by the input key with the help of a Fibonacci recursion,
– diversification part D, whose core consists mainly in a linear feedback shift register LFSR and
– non-linear part NL, which passes the interim key through a substitution layer, a diffusion layer and a mixing layer, before passing it to the algorithm as round key.

To reflect on the three versions we also have three different NL parts, NL64, NL64h and NL128.



Graph 5: Key Management



Graph 6: S-box

Some rationales

S-box

The primary benefit of IDEA NXT is avoiding a purely algebraic construction for the S-box; a secondary benefit is the possibility to implement it on hardware technologies in a very efficient way.
The S-box function is a non-linear bijective mapping on 8-bit values. It consists of a Lai-Massey scheme with 3 rounds taking three different substitution boxes as round function where the orthomorphism of the third round is omitted (graph 6).

Linear Multipermutations

Both mu4 and mu8 are linear multipermutations. This kind of construction is optimal for its diffusion properties. A circulating-like construction is used, since not all constructions are very efficient to implement, especially on low-end smartcards with limited memory and computational power.

Key schedule Algorithms

The IDEA NXT key schedule algorithms offer many benefits, such as:

- The function, which takes a key and the round number and returns the sub keys, is a cryptographic pseudorandom, collision resistant and one-way function.
- The sequence of sub keys is generated in any direction without any complexity penalty.
- All bytes of the key from the mixing part are randomized even when the key size is very small with respect to the full length.
- The key schedule algorithm resists related-cipher attacks since IDEA NXT can use different number of rounds.

The key schedule algorithms have significant advantages in terms of security. The time needed to compute the sub keys is about the time needed to encrypt 6 blocks of data, which is sufficient for all kinds of applications.

Another central property of IDEA NXT key schedule algorithms is ensured by the LFSR construction. As it is possible to back-clock it easily, the sub key generation process can be computed in the encryption as well as in the decryption direction without any loss of speed.

Resistance to Cryptanalysis

Linear and Differential Cryptanalysis

Both f32 and f64 functions can be viewed as classical Substitution-Permutation Network constructions. Due to its kSPkSk-structure (key-Substitution-Permutation-key-Substitution-key) one can prove that it is impossible to find any useful differential or linear characteristics after 8 rounds for NXT64 as well as for NXT128. Hence, a minimal number of 12 rounds provides sufficient security for standard applications.

Statistical Attacks

Due to the very high diffusion properties of IDEA NXT's round functions, the high algebraic degree of the S-box mapping and the number of rounds, one is strongly convinced that IDEA NXT will resist to known variants of linear and differential cryptanalysis (like Differential-Linear cryptanalysis, Boomerang and Rectangle attacks), as well as generalizations thereof, like Knudsen's Truncated and Higher-Order differentials, Impossible differentials, and Harpes' Partitioning cryptanalysis.

Slide and Related-Key Attacks

Slide attacks exploit periodic key schedule algorithms, which is not a property of IDEA NXT's key schedule algorithms. Furthermore, due to very good diffusion and the high non-linearity of the key schedule, related-key attacks are very unlikely to be effective against IDEA NXT.

Interpolation and Algebraic Attacks

IDEA NXT's design avoids pure algebraic constructions for the S-box mapping, as it is the case for many modern designs of block cipher. Since IDEA NXT's non-linear mapping S-box does not possess any simple relation over GF(2) or GF(2^8), such attacks are certainly not effective.

Integral Attacks

Integral attacks apply to ciphers operating on well-aligned data, like SPN structures. As the round functions of IDEA NXT are SPN's, one can find an integral distinguisher on the whole structure of IDEA NXT with a complexity of about 2^{136} operations and negligible memory for 6 rounds of NXT64 and 4 rounds of NXT128.

References

The research and development specifications are public and available through our website at www.mediacrypt.com:
"FOX Specification V1.1" (November 2004). [1)]

Summary

IDEA NXT raises the bar for encryption algorithm design, providing an increased level of customization options that are based on the simplicity of standard solutions.
The highest level of security has been achieved by taking into account all currently known cryptanalysis methods. The mathematical structure reflects currently available hardware. It achieves excellent performance on 32 bit chip architectures and even superior performance on 64 bit chip architectures.
Two patents are registered in Europe and in the US: the crypto algorithm and the key management. They are evidence of the innovative construction.

[1)] 'FOX' has been the code-name of the R&D project