**Table 1. Common elements in block ciphers.**

| Algorithm | No. of rounds | Block size (bits) | Feistel | Substitution-permutation (SP) network | Arithmetic S-box | Pseudo-random S-box | Fixed permutations | Addition (mod 2w) | Fixed shift/ rotation | Variable shift/ rotation | Modular multiplication | Multiplication with a constant |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| DES/ Triple DES | 6/48 | 64 | Yes | | | Yes | Yes | | Yes | | | |
| IDEA | 8 | 64 | Yes | | | | | Yes | | | Yes | |
| RC5 | 12/16 | 32/128 | Yes | | | | | Yes | | Yes | | |
| AES (Rijndael) | 10/12/14 | 128 | | Yes | Yes | | Yes | | Yes | | | Yes |
| RC6 | 20 | 128 | Yes | | | | | Yes | | Yes | Yes | |
| MARS | 2 × 16 | 128 | Yes | | | Yes | | Yes | Yes | Yes | Yes | |
| Serpent | 32 | 128 | | Yes | | Yes | Yes | | Yes | | | |
| Twofish | 16 | 128 | Yes | | | Yes | | Yes | Yes | | Yes | Yes |
| XTEA | More than 31 | 32 | Yes | | | | | Yes | Yes | | | |

but for the entire ubiquitous computing field.

As the "Ultralow-Power Application Domain" sidebar describes, to provide cryptographic functions for this class of devices, designers must make power consumption their first priority. Thus far, research has concentrated on WSNs' network-specific aspects and on software implementations of cryptographic algorithms. Only recently have researchers published studies of special hardware implementations.[4-8]

A wireless sensor node's main power consumer is its RF transceiver, or radio. Hardware developed specifically for radios combines a low data rate, low power consumption, and the ability to interface directly with low-power microcontrollers. Providing adequate security for ultralow-power applications such as WSNs and RFID devices requires an approach similar to that used for radios—that is, specialized hardware combined with application-specific algorithms.

Other factors also play a role. For example, despite advances in radio design, transmission power is still costly compared to computations. Hence, we must keep the transmission overhead that applying security incurs to an absolute minimum.

Furthermore, most current cryptographic algorithms are designed for high performance, mostly in software on 32-bit microprocessors. On sensor nodes and RFID devices, computation time isn't as critical as power and space conservation. To this end, we introduce useful techniques for cryptographic algorithm implementers as well as guidelines for designing cryptographic algorithms for ultralow-power applications.

## SURVEY OF CRYPTOGRAPHIC ALGORITHMS

As a first step, we examine current popular cryptographic algorithms as well as some we have found particularly interesting for use in this domain.[8]

### Block ciphers

A wide variety of established block cipher designs share similar functions and structures. Our list of algorithms consists of classic block ciphers (Data Encryption Standard/Triple DES, International Data Encryption Algorithm [IDEA], and RC5), the Advanced Encryption Standard (AES) finalists, and the Extended Tiny Encryption Algorithm (XTEA). Table 1 summarizes their features.

**Round structures.** Virtually all modern block ciphers are *iterated product ciphers*—that is, the encryption process consists of repeated applications of a round function. The round function consists of multiple layers of transformations (also called confusion and diffusion layers) that perform substitution and permutation. The round function itself isn't considered secure, but each additional round increases the security level.

Popular round structures—used by DES, RC5, MARS, and so on—are variations of the Feistel network, in which the round function typically modifies only part of the round data. Some publications therefore refer to rounds in Feistel ciphers as half-rounds. Substitution and permutation networks used by IDEA, Rijndael (AES), and so on typically modify the entire data set in each round.

**Substitution functions.** All product ciphers use some form of substitution function, or *S-box*, to introduce nonlinearity into the encryption process. Techniques range from lookup-table-based pseudorandom substitutions to high-degree nonlinear arithmetic functions.

**Permutation.** Product ciphers combine various transformations for confusion and diffusion. They achieve diffusion through fixed permutations (for example, initial permutation [IP], inverse IP [$IP^{-1}$], and permutation [P] in DES) or data-dependent (variable) shifts and rotations (used by RC5/6 and MARS, for example).

**Key mixing.** Most block ciphers add subkeys to the round data using XOR operations, which are fast and