Ciphers in Use in the Internet
draft-irtf-cfrg-cipher-catalog-01

Abstract

This note catalogs the ciphers in use on the Internet, to guide users and standards processes. It presents the security goals, security analysis and results, specification, intellectual property considerations, and publication date of each cipher. Background information and security guidance is provided as well.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on April 25, 2013.

Copyright Notice

Copyright (c) 2012 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as
described in the Simplified BSD License.

Table of Contents

1. Introduction .................................................. 3
   1.1. Document History ........................................ 3
   1.2. Requirements Language .................................. 3
2. Background .................................................... 3
   2.1. Attack Models ............................................ 4
   2.2. Security Goals ........................................... 5
      2.2.1. Exhaustive Search ................................... 6
      2.2.2. Attacks on reduced-round versions ................... 6
      2.2.3. Indistinguishability and the birthday bound .......... 6
3. Guidance ....................................................... 7
   3.1. AES Compatibility ......................................... 8
4. 128-bit Block Ciphers ........................................ 8
   4.1. ARIA ..................................................... 8
   4.2. CLEFIA .................................................. 9
   4.3. SMS4 .................................................... 9
   4.4. SEED ................................................... 10
   4.5. Camellia ................................................ 11
   4.6. CAST-256 ................................................ 11
   4.7. Advanced Encryption Standard (AES) ...................... 12
   4.8. Twofish ................................................ 14
   4.9. Serpent ................................................ 14
5. 64-bit Block Ciphers .......................................... 15
   5.1. MISTY1 .................................................. 15
   5.2. SKIPJACK ............................................... 16
   5.3. RC2 ...................................................... 16
   5.4. CAST-128 ............................................... 17
   5.5. BLOWFISH ............................................... 17
   5.6. International Data Encryption Algorithm (IDEA) .......... 17
   5.7. GOST 28147-89 ......................................... 18
   5.8. Triple Data Encryption Standard (TDES) .................. 19
   5.9. Data Encryption Standard (DES) .......................... 19
6. Stream Ciphers ............................................... 20
   6.1. Kcipher-2 ............................................... 20
   6.2. Rabbit .................................................. 20
   6.3. RC4 ..................................................... 20
7. Acknowledgements .............................................. 21
8. IANA Considerations .......................................... 22
9. Security Considerations ........................................ 22
10. References .................................................... 22
    10.1. Normative References ................................... 22
    10.2. Informative References ................................ 22
Authors’ Addresses ............................................. 58
1. Introduction

This note is a catalog of the ciphers in use on the Internet, and/or defined or referenced in IETF RFCs.

This note is not a standards document; instead it aims to capture the consensus of the Cryto Forum Research Group at the time of publication, and to provide technical guidance to standards groups that are selecting ciphers.

This note groups together ciphers with similar block structure, and lists ciphers in decreasing order of the year of their publication.

1.1. Document History

This is the second version of this note; it is a work in progress, and it should not yet be considered as representative of a consensus. Comments are solicited and should be sent to the authors and to cfrg@irtf.org.

This section is to be removed by the RFC Editor upon publication as an RFC.

1.2. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

2. Background

A cipher is an encryption method. Encryption is a transformation of data that uses a secret key to change a plaintext value, which needs to be kept secret, into a ciphertext value, which can be safely revealed without the loss of the confidentiality of the plaintext. Ciphertext can be converted back into plaintext, through the use of the secret key, via a decryption algorithm that is the reverse of the encryption algorithm. Importantly, encryption does not protect the integrity or authenticity of the plaintext; it does not provide a data integrity service, or a data origin authentication service [RFC4949].

Authenticated Encryption is an encryption method that does protect the integrity and authenticity of the plaintext, as well as the confidentiality of the plaintext. Authenticated Encryption with Associated Data (AEAD) protects the confidentiality, integrity, and authenticity of the plaintext, and also protects the integrity and
A Block Cipher is an encryption algorithm that encrypts a fixed-size plaintext block with a secret key, resulting in a fixed-size ciphertext block. The encryption is reversible, so that the plaintext block can be computed from the key and the ciphertext block. Block ciphers are not directly used to encrypt data, but instead are used in a mode of operation, as described below. A block cipher has two parameters: block size (the number of bits in the fixed-size blocks), and key size (the number of bits in the key). Some block ciphers accept more than one key size.

A Block Cipher Mode of Operation is a method for encrypting and/or authenticating data. Most modes of operation can operate on arbitrary-length data, unlike the block cipher itself, which can only operate on fixed length data. The mode of operation logically breaks plaintext into fixed-size blocks, and processes these blocks using the block cipher (and other operations such as bitwise exclusive-or).

A Stream Cipher is an encryption method that does not use a block cipher, and is not used in a mode of operation; instead, the stream cipher defines its own encryption method. Most stream ciphers encrypt plaintext by generating pseudorandom data with a secret key, then bitwise exclusive-oring the pseudorandom data with the plaintext to produce the ciphertext. Some stream ciphers take an Initialization Vector (IV) as input; a different IV is provided to the cipher for each different message that is encrypted. A stream cipher has two parameters: IV size (the number of bits in the IV), and key size (the number of bits in the key). Some stream ciphers accept more than one key size.

2.1. Attack Models

There are many different attack models that are used to analyze the security of ciphers. An attack model is a formal statement of the attacker’s capabilities. A particular cipher may be strong in one attack model, but weak in another; the suitability of that cipher for use in a particular application will depend entirely on the attacker’s actual capabilities in the real world.

In a Known-Plaintext Attack (KPA), the attacker knows some (but not all) of the plaintexts that are encrypted with an unknown secret key, and can learn the resulting ciphertexts. The attacker’s goal is to determine the value of some of unknown plaintexts.

In a Chosen-Plaintext Attack (CPA), the attacker can choose some (but not all) of the plaintexts that are encrypted with an unknown secret key, and can learn the resulting ciphertexts. A CPA is adaptive if
the attacker can adapt the plaintexts that it chooses based on the
ciphertexts that it observes. The attacker’s goal is to determine
the value of some of the plaintexts that it does not choose and that
it does not know.

In a Chosen-Ciphertext Attack (CCA), the attacker can cause the
decryption of some ciphertexts of its choice, and can learn the
results of those decryptions. The attacker can also observe the
ciphertext resulting from the encryption of some unknown plaintexts.
A CCA is adaptive if the attacker can adapt the ciphertexts that it
chooses based on other data that it observes. The attacker’s goal is
to determine the value of some of the unknown plaintexts.
(Authenticated Encryption protects against these attacks.)

In a Related-Key Attack (RKA), the attacker can cause the encryption
of unknown plaintext values under two or more keys, where the
relationship between the keys is known to the attacker, but the
actual value of the keys is not known. For example, if keys K1 and
K2 are in use, the attacker might know the value of the bitwise
exclusive-or of K1 and K2, while not knowing the value of either key.
Related-Key Attacks do not have any effect on security when keys are
chosen independently, as is the case in most communication security
protocols. It is a theoretical impossibility for a cipher to be
resistant to all types of RKAs, which underscores the need for sound
key generation and key management.

In a Side-Channel Attack (SCA), the attacker has access to physical
side information beyond the digital representation of the plaintexts
and ciphertexts, such as the voltage levels used during the
encryption process, or fine-grained timing information about the
duration of the encryption operations. SCAs act against an
implementation of a cipher, rather than against the cipher design,
since the side information is a property of the former and not the
latter. Nonetheless, it is important to study methods of defending a
particular cipher design from SCAs.

In a Key Recovery Attack (KRA), the attacker learns the secret key
that is used to encrypt some ciphertext. In a Plaintext Recovery
Attack (PRA), the attacker learns some unknown plaintext, but does
not learn the secret key. A successful KRA is devastating, but a
successful PRA can also be just as damaging.

2.2. Security Goals

There are several security goals for block ciphers; understanding
these goals is important to understanding the actual security
provided by ciphers in the real world. This section reviews the most
important security goals.
2.2.1. Exhaustive Search

For each cipher, the best attack is described. Any cipher can be defeated, in theory, by exhaustively searching over every possible key, but in practice this attack is computationally feasible only for smaller key sizes. The 1998 Deep Crack machine cost $250,000 and could break a 56-bit key by exhaustive search in about one day [K98]. Due to the exponentially fast decrease in the cost of computing power (Moore’s Law), the length of a key that can be broken for a fixed amount of money goes up by one bit every 1.5 years. Combining these facts, we estimate that a $250,000 machine can break 66-bit keys via exhaustive search in 2013, and that a $32M machine can break 73-bit keys.

2.2.2. Attacks on reduced-round versions

In most block ciphers, the encryption operation essentially consists of a round function that is repeated multiple times, each time with a different subkey. The plaintext block is input to the first round, and the ciphertext block is the output of the final round. Cryptanalysts investigating the security of a block cipher often consider the strength of the cipher against reduced-round versions, that is, a variant of the cipher that includes fewer rounds than the actual cipher. Most attacks against block ciphers can be easily generalized to attacks on reduced-round variants of block ciphers. The effectiveness of an attack against a block cipher is measured, in part, by the number of rounds that the attack can defeat.

The number of chosen plaintext blocks, chosen ciphertext blocks, or known plaintext blocks that are used in an attack is an important measure of the strength of that attack. For instance, an attack against a 128-bit block cipher that requires more than $2^{64}$ known plaintext blocks has little effect on practical security, because those ciphers are not used to encrypt that much data with a single key (see Section 2.2.3).

2.2.3. Indistinguishability and the birthday bound

An encryption method is indistinguishable from random whenever its ciphertext cannot be distinguished from a random value by a computationally limited adversary. This idea has been mathematically formalized, and is fundamental to the analysis of ciphers. A cipher cannot be secure unless it is indistinguishable, and thus, this is the main security goal.

Typical block cipher modes of operation are insecure when the amount of data processed by a single key is larger than $w \times 2^{w/2}$ bits, where $w$ is the block size of the block cipher.
denotes 2 to the power w.) This limit is called the birthday bound, by analogy to the fact that, in a group of people, a birthday common to two people is more likely than one might expect. The birthday bound is a primary consideration for the security of block ciphers. Above the birthday bound, all of the block cipher modes of operation that are in common use are distinguishable from random, and are vulnerable to plaintext recovery attacks.

The bound for a 64-bit block cipher is $2^{34}$ bytes, or 4 Gigabytes, and

The bound for a 128-bit block cipher is $2^{67}$ bytes, or 128 Trillion Gigabytes.

In practice, it is highly desirable that the amount of data is significantly below the birthday bound, in order to make the likelihood of a successful plaintext recovery attack negligible.

It is highly desirable that a block cipher be indistinguishable from random even if the attacker knows most of the $2^w$ possible w-bit plaintext/ciphertext pairs for a given key. However, because of the birthday bound, a block cipher should not be used to encrypt more than $2^{(w/2)}$ plaintexts, and attacks against a block cipher that require more than $2^{(w/2)}$ plaintexts or ciphertexts likely have no effect on the practical security of that cipher.

3. Guidance

It is STRONGLY RECOMMENDED that any cipher used be secure in the KPA, adaptive CPA, and adaptive CCA models. The security against this type of attack is determined by the cipher design.

It is RECOMMENDED that any implementation of a cipher be secure in the SCA model, and it is STRONGLY RECOMMENDED that any implementation that must operate while in the physical possession of an attacker be secure in the SCA model. The security against this type of attack is determined by the particulars of the implementation, and not the design of the cipher. However, a specific cipher design may be easier to implement such that it is secure in the SCA model, compared to other ciphers.

When encryption is in use, it is STRONGLY RECOMMENDED that either 1) Authenticated Encryption or AEAD be used, or 2) an encryption method be used in conjunction with an algorithm that protects the authenticity of the data, such as a Message Authentication Code [RFC4949].
64-bit block ciphers SHOULD NOT be used in general-purpose systems, because of the plaintext recovery attacks that are possible against them. When a 64-bit block cipher is used for legacy reasons, it is RECOMMENDED that the amount of data encrypted by a single key is 1 Megabyte. For special purpose applications in which the amount of encrypted data is below this threshold, 64-bit block ciphers MAY be used.

3.1. AES Compatibility

At present, the most widely used cipher is the Advanced Encryption Standard (see Section Section 4.7), which is believed to provide adequate security for the foreseeable future. It has a block size of 128 bits, and key sizes of 128, 192, or 256 bits. We say that a cipher is AES-compatible if it supports the same block and key sizes, and that a cipher is partially AES-compatible if it supports the same block size and at least one of the key sizes.

AES-compatible ciphers include ARIA, CAST-256, Camellia, Serpent, and Twofish. Partly-AES-compatible ciphers include SEED and SMS4, both of which only support 128 bit keys. All of these ciphers, except for SMS4, are either free from intellectual property claims, or are available worldwide royalty free.

The existence of strong ciphers that are free of intellectual property restrictions shows that it is not necessary to use encumbered ciphers in order to obtain good security.

4. 128-bit Block Ciphers

4.1. ARIA

ARIA was first published in 2003 [NBC:KKP03] by a large group of researchers from the Republic of South Korea. It is specified in [RFC5794], and supports a block length of 128 bits and keys length of 128 bits, 192 bits, and 256 bits. Thus ARIA is AES-compatible.

Intellectual Property Rights have not been claimed on ARIA.

The best known attack against this cipher is meet-in-the-middle attack on 8 rounds (out of 12) with data complexity $2^{56}$, which was shown in [MMA:TSLL10]. There have been other analyses as well. Classical linear and differential cryptanalysis were shown in [SPAA:BC03]. Truncated differentials, boomerang and slide attacks were shown in [INDOCRYPT:FFGL10] and [SPAA:BC03]. Impossible differential
cryptanalysis appeared in [CANS:DuChe10]. SCA security was considered in [WISA:YHMOM06].

In 2004, the Korean Agency for Technology and Standards selected ARIA as a standard cryptographic technique. The algorithm uses a substitution-permutation network (SPN) structure like that of AES. The number of rounds is 12, 14, or 16, depending on the key sizes. ARIA uses two 8 x 8-bit substitution tables and their inverses in alternate rounds; one of these is the AES substitution table. The key schedule processes the key using a 3-round 256-bit Feistel cipher.

4.2. CLEFIA

CLEFIA was designed by the SONY corporation, and was first published in 2007 [BC:SSAMI07],[FSE:SSAMI07]. It is specified in [RFC6114], and supports keys lengths of 128, 192, and 256.

IETF uses include 1 RFC, which specifies the cipher, and 2 Internet Drafts, defining its use in IPsec and TLS.

Intellectual Property Rights have been claimed on CLEFIA. The owner of those rights is SONY.

The best known attack against this cipher is the improbable differential cryptanalysis of reduced round CLEFIA presented in [INDOCRYPT:Tezcan10]. It requires $2^{126.8}$ chosen plaintexts and breaks 13 (out of 18) rounds with a complexity of $2^{126.8}$ encryptions for the key size of 128 bits. Similar attacks apply for 14 and 15 rounds of CLEFIA for the key sizes 192 and 256 bits, respectively.

This cipher has also been analyzed by differential and linear cryptanalysis. Impossible Differential Cryptanalysis was shown in [IDCC:TTSSSK08]. SCA has been considered; cryptanalysis using differential methods with cache trace patterns was described in [RSA:RebMuk11] and differential fault analysis was described in [ICICS:CheWuFen07].

CLEFIA has 18, 22, or 16 rounds, for key sizes of 128 bits, 192 bits, and 256 bits, respectively. It is intended to be used in Digital Rights Management (DRM) systems.

4.3. SMS4

SMS4 was first published in 2006. It is specified in [SMS4], and supports a keys length of 128 bits.

There are not yet any IETF uses.
Intellectual Property Rights have been claimed on SMS4. The owner of those rights is BDST.

The best known attack against SMS4 are the linear and differential attacks against 22 rounds (out of 32) shown in [LDC:KKHS08]. These attacks require $2^{117}$ known plaintexts and $2^{118}$ chosen plaintexts, respectively. Rectangle and impossible differential attacks were shown in [AARRS:DT08]. Other attacks against reduced-round versions of SMS4 have appeared [ACISP:ZhaZhaWu08] [SAC:EtrRob08] [ICICS:TozDun08] [ICICS:Lu07].

Algebraic and XLS attacks against reduced-round SMS4 have been pursued [CANS:ChoYapKho09] [ICISC:EriDinChr09] [INDOCRYPT:JiHu07].

SMS4 is used in the Chinese National Standard for Wireless LAN WAPI. SMS4 was a proposed cipher to be used in IEEE 802.11i standard, but so far has been rejected by ISO. One of the reasons for the rejection has been opposition to the WAPI fast-track proposal by the IEEE. SMS4 uses an 8-bit substitution table, and performs 32 rounds to process one block. A non-linear key schedule is used to produce the round keys.

4.4. SEED

SEED was first published in 1998. It is specified in [RFC4269], and supports a key length of 128 bits.

IETF use includes 7 RFCs and 1 Internet Draft, which specify the cipher and define its use in CMS, TLS, IPsec, SRTP, and MIKEY.

Intellectual Property Rights have not been claimed on SEED.

The best attack against SEED is a differential attack against eight (out of 16) rounds [S11] that requires $2^{125}$ chosen plaintexts. Differential and linear attacks were also shown [DC:YS03] [SKES:WMF03] [SCN:YanShi02]. SCA was considered in [WISA:YKHMP04].

SEED is a 16-round Feistel network that uses two 8 x 8 S-boxes that are derived from discrete exponentiation, as in the design of the SAFER block cipher. It was developed by the Korean Information Security Agency (KISA). It is used broadly in South Korea, but not often used elsewhere. It was adopted in Korea because the 40-bit "export strength" cryptography, as was common at the time in the Secure Sockets Layer (SSL) in web browsers, was rightly regarded as insufficient; KISA developed its own the SEED standard to address this fact. However, SEED is a national rather than international standard, and this fact limits the interoperability of SEED implementations in communications across national borders.
4.5. Camellia

Camellia was first published in 2000 in [SC:AIKMMNT00]. It is specified in [RFC3713], and supports keys lengths 128, 192, and 256. IETF uses include 15 RFCs and 6 Internet Drafts, which specify the cipher and define its use in XMLsec, TLS, IPsec, OpenPGP, CMS, PSKC, and Kerberos.

Intellectual Property Rights have been claimed on CAMELLIA. The owner of those rights is NTT, who has stated that it "intends to grant royalty-free licenses for the essential patents" needed to implement Camellia [NTT].

The best known attack against Camellia is an impossible differential attack against 10 (out of 18) rounds that uses 2^112.4 chosen plaintext blocks [ISPEC:BaiLi11]. Higher order differential attacks were shown in [HRDA:HSK02] and [SAC:HatSekKan02]. Truncated and impossible differential cryptanalysis have been presented [AC: SugKobIma01] [ICISC:LHLLY01] [FSE:KanMat01] [DLBRC:S02] [RSA:LKKD08] [SAC:WuZhaZha08] [SAC:MSDB09] [FSE:ShiKanAbe02]. Other analyses include the square attack (integral cryptanalysis) [ICICS:LeiLiFen07] [FSE:YeoParKim02] [ICICS:HeQin01] and collision attacks [CANS: JieZho06][SAC:WuFenChe04].

Camellia is a 128-bit block cipher jointly developed by Mitsubishi and NTT. The cipher has been approved for use by the ISO/IEC, the European Union’s NESSIE project and the Japanese CRYPTREC project. The cipher has security levels and processing abilities comparable to the Advanced Encryption Standard. Camellia’s block size is 16 bytes (128 bits). The block cipher was designed to be suitable for both software and hardware implementations, from low-cost smart cards to high-speed network systems. Camellia is a Feistel cipher with either 18 rounds (for 128-bit keys) or 24 rounds (for 192 or 256 bit keys). Every six rounds, a logical transformation layer is applied: the so-called "FL-function" or its inverse. Camellia uses four 8 x 8-bit S-boxes with input and output affine transformations and logical operations. The cipher also uses input and output key whitening. The diffusion layer uses a linear transformation based on an MDS matrix with a branch number of 5.

4.6. CAST-256

CAST-256 was first published in 1998 in [EA:C98]. It is specified in [RFC2612], and supports keys lengths 128, 160, 192, 224 and 256.

Its IETF use is RFC 2612, which defines the cipher.
Intellectual Property Rights have been claimed on CAST-256 by Entrust. According to RFC 2612, it "is available worldwide on a royalty-free and license-free basis for commercial and non-commercial uses."

The best known attack against 12 (out of 48) rounds of CAST-256 is linear attack that requires $2^{101}$ known plaintext blocks [SAC:WamWanHu08]. Other analysis includes differential and linear attacks [CA:AHTW99] higher order differential attacks [FSE:MorShiKan98].

The CAST-256 (or CAST6) block cipher was submitted as a candidate for the Advanced Encryption Standard (AES); however, it was not among the five AES finalists. It is an extension of an earlier cipher, CAST-128; both were designed according to the "CAST" design methodology invented by Carlisle Adams and Stafford Tavares. Howard Heys and Michael Wiener also contributed to the design. CAST-256 uses the same elements as CAST-128, including S-boxes, but is adapted for a block size of 128 bits, twice the size of its 64-bit predecessor. (A similar construction occurred in the evolution of RC5 into RC6). CAST-256 is composed of 48 rounds, sometimes described as 12 "quad-rounds", arranged in a generalised Feistel network.

4.7. Advanced Encryption Standard (AES)

 AES was first published in 1998 in [AP:DR99], and was originally called RIJNDAEL. It is specified in [FIPS-197], and supports keys lengths of 128, 192, and 256 bits.

IETF uses include 29 RFCs and 3 Internet Drafts.

Intellectual Property Rights have not been claimed on AES.

The best known attack against this cipher is biclique cryptanalysis, which works against the full 10 rounds of AES-129 and requires $2^{88}$ chosen plaintexts and $2^{126}$ operations [AC:BogKhoRec11]. Besides this work, there has been considerable attention paid to the AES cipher by cryptanalysts, making it the most-studied cipher ever. Much of this work is in the KPA, CPA, and CCA models [C:BouDerFou11] [FSE:DemSe108] [FSE:BucPysWei06] [INDOCRYPT:DTCB09] [INDOCRYPT:LDKK08] [SAC:MPRS09] [AC:PSCL02] [SAC:ZWZF06] [CAOR:GM00] [KRBR:BDK05] [RKIDA:BDK06] [MITMA:DS08] [ACISP:FleGotLec09] [SAC:KleiMeiTav01] [FSE:GilPey10] [AC:DenKeilSha10] [AFRICACRYPT:GalMin08] [FSE:Sasak111] [EC:BirNik10] [ISC:ZWPKY08] [ISC:NakPav07].

The RKA model for AES has also been well studied [C:BirKhoNik09] [SAC:JakDes03] [AC:BirKho09] [INDOCRYPT:ZWF07] [INDOCRYPT:GorLuc08] [FSE:HKLP05] [RSA:BihDunKeil06] [FSE:KimHonPre07] [IWSEC:Sasaki10].
Considerable work has been done on SCA, including power analysis attacks and defenses [CHES:GouMar11] [AFRICACRYPT: GenProQui11] [AFRICACRYPT:AliMuk11] [ACNS:LuPanHar10] [ACNS:CanBat08] [ACNS:TilHerMan07] [ASIACCS:NevSeiWan06] [ACISP:FouTun06] [ACNS: DusLetViv03] [INDOCRYPT:KumMukCho07] [ISC:BatGieLem08] [SAC: Bogdanov07] [CANS:ZhaYuLiu10] [CHES:KimHonLim11] [CHES:RKSF11] [SAC: CEJV02] [CHES:DerFouLer11] [ICISC:ZhaWuFen07] [INDOCRYPT:M DRM10] [INDOCRYPT:MulWysPre10] [FSE:OMPR05] [CHES:RivPro10] [CHES: Bogdanov08] [CHES:RenStaVey09] [CHES:SSHA08] [CHES:KerRey08] [CHES: TilHer08] [CHES:Jaffe07] [CHES:SLFP04] [CHES:PirQui03] [CHES: ManPraOsw05] [CHES:AkkGir01] [CHES:TriDeSGer02] [CHES:GolTym02] [RSA: BEPW10] [RSA:SakYagOht09] [FC:BloSei03] [ICICS:ZSMS07] [RSA: SchPaa06] [ICISC:Mangard02] [INDOCRYPT:ProRoc10] [WISA:SchKim08] [WISA:OswSch05] [ICISC:CouGou05] [ICISC:Karroumi10] [SAC:BloGuaKru04] [SAC:BilGi1Ech04] [CHES:GebHoTiu05] [CHES:StaBerPre04].

Cache-timing attacks and defenses have also been analyzed [RSA: Konighofer08] [CHES:KasSch09] [CHES:BonMir06] [RSA:AciSchKoc07] [RSA: OsvShaTro06] [SP:GulBanKre11] [ICICS:AciKoc06] [SAC:BloKru07] [SAC: NevSei06] [WISA:GalKizTun10].

The mathematical structure of AES has also been studied [SCN: DaeRij06] [SAC:BaiVau05] [ICICS:MonVau04] [FSE:SonSeb03] [FSE: Wernsdorf02] [ICISC:SonSeb02] [C:MurRob02] [AC:BarBih02] [SAC: FegSchWhi01].

(AES) is a specification for the encryption of electronic data. It has been adopted by the U.S. government and is now used worldwide. AES was announced by National Institute of Standards and Technology (NIST) as U.S. FIPS PUB 197 (FIPS 197) on November 26, 2001 after a five-year standardization process in which fifteen competing designs were presented and evaluated before it was selected as the most suitable. It became effective as a Federal government standard on May 26, 2002 after approval by the Secretary of Commerce. It is available in many different encryption packages. AES is the first publicly accessible and open cipher approved by the National Security Agency (NSA) for top secret information. Originally called Rijndael, the cipher was developed by two Belgian cryptographers, Joan Daemen and Vincent Rijmen, and submitted by them to the AES selection process. AES is based on a design principle known as a substitution-permutation network. It is fast in both software and hardware. AES operates on a 4 x 4 column-major order matrix of bytes, termed the state (versions of Rijndael with a larger block size have additional columns in the state). Most AES calculations are done in a special finite field. The AES cipher is specified as a number of repetitions of transformation rounds that convert the input plaintext into the final output of ciphertext. Each round consists of several processing steps, including one that depends on the encryption key.
A set of reverse rounds are applied to transform ciphertext back into the original plaintext using the same encryption key.

4.8. Twofish

Twofish was first published in 1998. It is specified in [Twofish], and supports keys lengths of 128, 192, and 256 bits.

IETF use include 9 RFCs, that specify its use in OpenPGP, SSH, and ZRTP.

Intellectual Property Rights have not been claimed on Twofish.

Attack: The best known attack against this cipher is truncated differential attack, which was shown in [TC:MY00]. Truncated differential, impossible differential attack that breaks was shown in [TC:MY00]. The Saturation Attack - A Bait for Twofish was shown in [FSE:Lucks01]. Analysis: Improved Impossible Differentials on Twofish was shown in [INDOCRYPT:BihFur00]. On the Twofish Key Schedul was shown in [SAC:SKWWH98].

Twofish is a symmetric key block cipher with a block size of 128 bits. It was one of the five finalists of the Advanced Encryption Standard contest, but was not selected for standardisation. Twofish is related to the earlier block cipher Blowfish. Twofish’s distinctive features are the use of pre-computed key-dependent S-boxes, and a relatively complex key schedule. Twofish borrows some elements from other designs; for example, the pseudo-Hadamard transform (PHT) from the SAFER family of ciphers. Twofish uses the same Feistel structure as DES. On most software platforms Twofish was slightly slower than Rijndael for 128-bit keys, but somewhat faster for 256-bit keys. Twofish was designed by Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, and Niels Ferguson; Twofish algorithm is free for anyone to use without any restrictions whatsoever. It is one of a few ciphers included in the OpenPGP standard (RFC 4880). However, Twofish has seen less widespread usage than Blowfish, which has been available longer.

4.9. Serpent

Serpent was first published in 1998. It is specified in [Serpent], and supports keys lengths of 128, 192, and 256 bits.

IETF uses include 6 RFCs, which specify its use in SSH.

Intellectual Property Rights have not been claimed on Serpent.

Attack: The best known attack against this cipher is linear attack.
The Rectangle Attack - Rectangling the Serpent was shown in [EC: BihDunKel01]. Amplified Boomerang Attacks Against Reduced-Round MARS and Serpent was shown in [FSE:KelKohSch00]. A Differential-Linear Attack on 12-Round Serpent was shown in [INDOCRYPT:DunIndKel08]. Analysis: Amplified boomerang, rectangle, differential cryptanalysis, linear cryptanalysis and differential-linear cryptanalysis were shown in [ABA:KKS00], [RA:BDK01], [DC:WH00], [LC: BDK02], [DLC:BDK03]. Multidimensional Linear Cryptanalysis of Reduced Round Serpent was shown in [ACISP:HerChoNyb08]. Experiments on the Multiple Linear Cryptanalysis of Reduced Round Serpent was shown in [FSE:ColStaQui08]. Differential-Linear Cryptanalysis of Serpent was shown in [FSE:BihDunKel03a]. Linear Cryptanalysis of Reduced Round Serpent was shown in [FSE:BihDunKel01]. A New Technique for Multidimensional Linear Cryptanalysis with Applications on Reduced Round Serpent was shown in [ICISC:ChoHerNyb08]. A Dynamic FPGA Implementation of the Serpent Block Cipher was shown in [CHES: Patterson00]. On the Pseudorandomness of the AES Finalists - RC6 and Serpent was shown in [FSE:IwaKur00]. Serpent: A New Block Cipher Proposal was shown in [FSE:BihAndKnu98].

Serpent was a finalist in the AES contest, where it came second to Rijndael. Serpent was designed by Ross Anderson, Eli Biham, and Lars Knudsen. Serpent was widely viewed as taking a more conservative approach to security than the other AES finalists, opting for a larger security margin: the designers deemed 16 rounds to be sufficient against known types of attack, but specified 32 rounds as insurance against future discoveries in cryptanalysis. The Serpent cipher is in the public domain and has not been patented. There are no restrictions or encumbrances whatsoever regarding its use. As a result, anyone is free to incorporate Serpent in their software (or hardware implementations) without paying license fees.

5. 64-bit Block Ciphers

5.1. MISTY1

MISTY1 was first published in 1995. It is specified in [RFC2994], and supports key lengths 128.

IETF use includes RFC 2994, which specifies the cipher.

Intellectual Property Rights have been claimed on MISTY1. The owner of those rights is Mitsubishi. According to [RFC2994], "the algorithm is freely available for academic (non-profit) use. Additionally, the algorithm can be used for commercial use without paying the patent fee if you contract with Mitsubishi Electric Corporation. For more information, please contact at
Attack: An Improved Impossible Differential Attack on MISTY1 was shown in [AC:DunKel08a]. Higher Order Differential Attacks on Reduced-Round MISTY1 was shown in [ICISC:TSSK08]. Improved Integral Attacks on MISTY1 was shown in [SAC:SunLai09]. Analysis: Cryptanalysis of Reduced-Round MISTY was shown in [EC:Kuhn01]. Improved Cryptanalysis of MISTY1 was shown in [FSE:Kuhn02]. Security Analysis of MISTY1 was shown in [WISA:THSK07]. Improving the Efficiency of Impossible Differential Cryptanalysis of Reduced Camellia and MISTY1 was shown in [RSA:LKKD08]. On MISTY1 Higher Order Differential Cryptanalysis was shown in [ICISC:BabFri00]. Security of the MISTY Structure in the Luby-Rackoff Model was shown in [SAC:PirQui04]. Round Security and Super-Pseudorandomness of MISTY Type Structure was shown in [FSE:IYYK01]. A Very Compact Hardware Implementation of the MISTY1 Block Cipher was shown in [CHES:YamYajIto08]. New Block Encryption Algorithm MISTY was shown in [FSE:Matsui97].

5.2. SKIPJACK

SKIPJACK was first published in 1998, and is specified in [SKIPJACK]. It supports a key length of 80 bits.

IETF use includes 15 RFCs, which describe its use in CMS and TELNET.

Intellectual Property Rights have not been claimed on SKIPJACK.

Attack: Saturation Attacks on Reduced Round Skipjack was shown in [FSE:KLLLL02]. Analysis: Provable Security for the Skipjack-like Structure against Differential Cryptanalysis and Linear Cryptanalysis was shown in [AC:SLLHP00]. Truncated Differentials and Skipjack was shown in [C:KnuRobWag99]. Cryptanalysis of Skipjack Reduced to 31 Rounds Using Impossible Differentials was shown in [EC:BihBirSha99]. Flaws in Differential Cryptanalysis of Skipjack was shown in [FSE:Granboulan01]. Markov Truncated Differential Cryptanalysis of Skipjack was shown in [SAC:ReiWag02]. Initial Observations on Skipjack:Cryptanalysis of Skipjack-3XOR (Invited Talk) was shown in [SAC:BBBBRS98].

5.3. RC2

RC2 was first published in 1998. It is specified in [RFC2268], and supports key lengths of 8, 16, 24, ..., 1024 bits.

IETF use includes 36 RFCs, which specify the cipher and describe its use in CMS, SMIME, TLS, and PKIX.
Intellectual Property Rights have not been claimed on RC2, though [RFC2268] says that "RC2 is a registered trademark of RSA Data Security, Inc. RSA’s copyrighted RC2 software is available under license from RSA Data Security, Inc."

On the Design and Security of RC2 was shown in [FSE:KRRR98]. Related-key cryptanalysis of 3-WAY Biham-DES, CAST DES-X, NewDES, RC2, and TEA was shown in [ICICS:KelSchWag97].

5.4. CAST-128

CAST-128 was first published in 1997. It is specified in [RFC2144], and supports a key length of 128 bits.

IETF use includes 20 RFCs that specify the cipher and define its use in OpenPGP, IPsec, CMS, and PKIX.

Intellectual Property Rights have been claimed on CAST-128 by Entrust. According to [RFC2144], "The CAST-128 cipher described in this document is available worldwide on a royalty-free basis for commercial and non-commercial uses."

5.5. BLOWFISH

BLOWFISH was first published in 1994. It is specified in [Blowfish], and supports keys lengths 32, 64, 96, ..., 448.

IETF use includes None.

Intellectual Property Rights have not been claimed on BLOWFISH.

A New Class of Weak Keys for Blowfish was shown in [FSE:KarMan07]. On the Weak Keys of Blowfish was shown in [FSE:Vaudenay96]. Description of a New Variable-Length Key 64-bit Block Cipher (Blowfish) was shown in [FSE:Schneier93].

5.6. International Data Encryption Algorithm (IDEA)

IDEA was first published in 1992. It is specified in [IDEA], and supports key length of 128 bits.

IETF use includes 9 RFCs, which describe its use in TLS and IPsec (but not in OpenPGP, though IDEA was used in earlier PGP versions).

Intellectual Property Rights have been claimed on IDEA. The owner of those rights is MediaCrypt AG.

Attack: Two Attacks on Reduced IDEA was shown in [EC:BorKnuRij97]. A
New Attack on 6-Round IDEA was shown in [FSE:BihDunKel07b]. New Attacks Against Reduced-Round Versions of IDEA was shown in [FSE:Junod05]. Miss in the Middle Attacks on IDEA and Khufu was shown in [FSE:BihBirSha99]. A New Meet-in-the-Middle Attack on the IDEA Block Cipher was shown in [SAC:DemSelTur03]. Square-like Attacks on Reduced Rounds of IDEA was shown in [SAC:Demirci02]. Analysis: On the Security of the IDEA Block Cipher was shown in [EC:Meier93]. Cryptanalysis of IDEA-X/2 was shown in [FSE:Raddum03]. New Cryptanalytic Results on IDEA was shown in [AC:BihDunKel06]. On Applying Linear Cryptanalysis to IDEA was shown in [AC:HawOCo96]. Key-Schedule Cryptoanalysis of IDEA G-DES, GOST SAFER, and Triple-DES was shown in [C:KelSchWag96]. Fault Analysis Study of IDEA was shown in [RSA:ClaGieVer08]. Differential-Linear Weak Key Classes of IDEA was shown in [EC:Hawkes98]. Improved DST Cryptanalysis of IDEA was shown in [SAC:AyaSel06]. Weak Keys for IDEA was shown in [C:DaeGovVan93]. New Weak-Key Classes of IDEA was shown in [ICICS:BNPV02].

DPA on n-Bit Sized Boolean and Arithmetic Operations and Its Application to IDEA RC6, and the HMAC-Construction was shown in [CHES:LemSchPaa04]. Switching Blindings with a View Towards IDEA was shown in [CHES:NeiPu04]. Tradeoffs in Parallel and Serial Implementations of the International Data Encryption Algorithm IDEA was shown in [CHES:CTLL01]. Revisiting the IDEA Philosophy was shown in [FSE:JunMac09]. Nonlinearity Properties of the Mixing Operations of the Block Cipher IDEA was shown in [INDOCRYPT:Yildirim03]. A Note on Weak Keys of DES IDEA, and Some Extended Variants was shown in [ISC:NakPreVan03]. IDEA: A Cipher For Multimedia Architectures? was shown in [SAC:Lipmaa98].

5.7. GOST 28147-89

The GOST 28147-89 was first published in 1989. It is specified in [RFC5830], and supports a key length of 256 bits. 256 Bit Standardized Crypto for 650 GE - GOST Revisited was shown in [CHES:PosLinWan10].

IETF use includes 7 RFCs.

Intellectual Property Rights have not been claimed on GOST 28147-89.

Attack: A Single-Key Attack on the Full GOST Block Cipher was shown in [FSE:Isobe11]. Analysis: Cryptanalysis of the GOST Hash Function was shown in [C:MPRKS08]. Key-Schedule Cryptoanalysis of IDEA G-DES, GOST SAFER, and Triple-DES was shown in [C:KelSchWag96]. Differential Cryptanalysis of Reduced Rounds of GOST was shown in [SAC:SekKan00].
5.8. Triple Data Encryption Standard (TDES)

The Triple Data Encryption Standard (TDES, or sometimes 3DES) was first published in 1979. It is specified in [FIPS-46-3], and supports key lengths of 112.

IETF uses include citations in 143 RFCs, which describe the use of the cipher in IPsec, TLS, SMIME, CMS, PKIX, PPP, SSH, GSAXMP.

Intellectual Property Rights have been claimed on TDES. The owner of those rights is IBM. According to [FIPS-46-3], TDES may be "covered by U.S. and foreign patents, including patents issued to the International Business Machines Corporation. However, IBM has granted nonexclusive, royalty-free licenses under the patents to make, use and sell apparatus which complies with the standard."

Attack: Attacking Triple Encryption was shown in [FSE:Lucks98]. A Known Plaintext Attack on Two-Key Triple Encryption was shown in [EC: VanWie90]. Analysis: The Security of Triple Encryption and a Framework for Code-Based Game-Playing Proofs was shown in [EC: BelRog06].

5.9. Data Encryption Standard (DES)

DES was first published in 1977. It is specified in [FIPS-46], and its key length is 56 bits.

IETF use includes 66 drafts and 158 RFCs.

Intellectual Property Rights have been claimed on DES. The owner of those rights is IBM. According to [FIPS-46-3], TDES may be "covered by U.S. and foreign patents, including patents issued to the International Business Machines Corporation. However, IBM has granted nonexclusive, royalty-free licenses under the patents to make, use and sell apparatus which complies with the standard."

DES is currently obsolete; its key size is inadequate to protect against attackers with access to modern computing resources. The security implications of using DES are discussed at length in [RFC4772]. Historically, DES was instrumental in the development of modern cryptography; Differential [C:BihSha90] and Linear [EC: Matsui93] Cryptanalysis were developed through the analysis of the DES algorithm.

DES was designed by an IBM research team led by Horst Feistel, a German-born cryptographer. DES was a refinement of the earlier LUCIFER cipher, which is the first modern block cipher that has been publicly described.
6. Stream Ciphers

6.1. Kcipher-2

Kcipher-2 was first published in 2011. It is specified in [I-D.kiyomoto-kcipher2] and supports a key length of 128 bits, and a 128-bit initialization vector.

IETF use includes 2 drafts, which specify the cipher and describe its use in TLS.

Intellectual Property Rights have been claimed on Kcipher-2. The owners of those rights are KDDI and Qualcomm.

KCipher-2 has been used for industrial applications, especially for mobile health monitoring and diagnostic services in Japan.

6.2. Rabbit

Rabbit was first published in 2003 [FSE:BVPCS03] in a peer-reviewed workshop. It is specified in [RFC4503], and supports a keys length of 128 bits, and a 64-bit IV.

The only citation in IETF documents is the cipher specification itself.

Intellectual Property Rights have been claimed on this cipher. The owner of those rights is Cryptico A/S.

The best known attacks against this cipher have a complexity greater than $2^{128}$, and thus do not violate its security goals. Distinguishing attacks were shown in [ISC:LuDes10] [ISC:LuWanLin08]. Side channels and fault injection attacks were considered in [INDOCRYPT:BerCanGou09] and [SAC:KirYou09], which described state-recovery attacks with $2^{38}$ complexity.

Rabbit is the only finalist from eSTREAM, the ECRYPT Stream Cipher Project, that appears in this note. Rabbit has a relatively small internal state of about 64 bytes, and it updates all words of state at each iteration, in contrast to RC4 (Section 6.3).

6.3. RC4

RC4 was first described in 1994. No normative specification exists; it is sometimes called ARCFOUR, which is short for alleged RC4. The cipher supports key lengths of 8, 16, 24, ..., 1024 bits. RC4 does not accept an initialization vector.
IETF use includes 54 RFCs and 23 drafts, which describe the use of RC4 in TLS, Kerberos, and SSH.

Intellectual Property Rights have not been claimed on RC4.

Attack: A Practical Attack on the Fixed RC4 in the WEP Mode was shown in [AC:Mantin05]. New State Recovery Attack on RC4 was shown in [C:MaxKho08]. Statistical Attack on RC4 - Distinguishing WPA was shown in [EC:SepVauVua11]. Predicting and Distinguishing Attacks on RC4 Keystream Generator was shown in [EC:Mantin05]. Attack on Broadcast RC4 Revisited was shown in [FSE:MaiPauSen11]. Key Collisions of the RC4 Stream Cipher was shown in [FSE:Matsui09]. Two Linear Distinguishing Attacks on VMPC and RC4A and Weakness of RC4 Family of Stream Ciphers was shown in [FSE:Maximov05]. A Practical Attack on Broadcast RC4 was shown in [FSE:ManSha01]. Collisions for RC4-Hash was shown in [ISC:IndPre08]. Passive-Only Key Recovery Attacks on RC4 was shown in [SAC:VauVua07]. Generalized RC4 Key Collisions and Hash Collisions was shown in [SCN:CheMiy10]. Analysis: New Correlations of RC4 PRGA Using Nonzero-Bit Differences was shown in [ACISP:MiySuk09]. Cache Timing Analysis of RC4 was shown in [ACNS:ChaFouLer11]. Impossible Fault Analysis of RC4 and Differential Fault Analysis of RC4 was shown in [FSE:BihGraNgu05]. Statistical Analysis of the Alleged RC4 Keystream Generator was shown in [FSE:FluMcG00]. Analysis of RC4 and Proposal of Additional Layers for Better Security Margin was shown in [INDOCRYPT:MaiPau08]. Analysis of Non-fortuitous Predictive States of the RC4 Keystream Generator was shown in [INDOCRYPT:PauPre03]. Cryptanalysis of RC4-like Ciphers was shown in [SAC:VauVua07]. Recovering RC4 Permutation from 2048 Keystream Bytes if j Is Stuck was shown in [ACISP:MaiPau08]. (Not So) Random Shuffles of RC4 was shown in [C:Mironov02]. Linear Statistical Weakness of Alleged RC4 Keystream Generator was shown in [EC:Golic97a]. New Form of Permutation Bias and Secret Key Leakage in Keystream Bytes of RC4 was shown in [FSE:MaiPau08]. Efficient Reconstruction of RC4 Keys from Internal States was shown in [FSE:BihCar08]. A New Weakness in the RC4 Keystream Generator and an Approach to Improve the Security of the Cipher was shown in [FSE:PauPre04]. One Byte per Clock: A Novel RC4 Hardware was shown in [INDOCRYPT:SSMS10]. New Results on the Key Scheduling Algorithm of RC4 was shown in [INDOCRYPT:AkgKavDem08]. Discovery and Exploitation of New Biases in RC4 was shown in [SAC:SepVauVua10]. Permutation After RC4 Key Scheduling Reveals the Secret Key was shown in [SAC:PauMai07]. Weaknesses in the Key Scheduling Algorithm of RC4 was shown in [FSE:FluManSha01].

7. Acknowledgements

Thanks are due to Jon Callas and Kevin Igoe.
8. IANA Considerations

This memo includes no request to IANA.

9. Security Considerations

Security is the main topic of this note.

10. References

10.1. Normative References


10.2. Informative References


Notes in Computer Science asiacrypt09vol, 2009.


[AC:SugKobIma01]

[ACISP:FleGorLuc09]

[ACISP:FouTun06]

[ACISP:HYYKT10]

[ACISP:HerChoNyb08]

[ACISP:MaiPau08]

[ACISP:MiySuk09]

[ACISP:ZhaZhaWu08]

[ACNS:CanBat08]
[ACNS:ChaFouLer11]

[ACNS:DusLetViv03]

[ACNS:HerOswMan06]

[ACNS:LuPanHar10]

[ACNS:TilHerMan07]

[AFRICACRYPT:AliMuk11]

[AFRICACRYPT:BSQPR08]

[AFRICACRYPT:GalMin08]

[AFRICACRYPT:GenProQuill11]
[AFRICACRYPT:MinPhaPou09]  

[AFRICACRYPT:YapKhoPos10]  

[AP:DR99]  

[ASIACCS:NevSeiWan06]  

[BC:SSAMI07]  

[Blowfish]  
Schneier, "Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish)", Lecture Notes in Computer Science fse94vol, 1994.

[C:BihSha90]  

[C:BirKhoNik09]  

[C:BouDerFou11]  

[C:DaeGovVan93]  
[C:KelSchWag96]

[C:KnuRobWag99]

[C:MPRKS08]

[C:MaxKho08]

[C:Mironov02]

[C:MurRob02]
J., M. and S. Murphy, "Essential Algebraic Structure within the AES", Lecture Notes in Computer Science crypto02vol, 2002.

[CA:AHTW99]

[CANS:ChoYapKho09]

[CANS:DuChe10]

[CANS:JieZho06]
Zhongya, Z. and G. Jie, "Improved Collision Attack on Reduced Round Camellia", Lecture Notes in Computer
Science cans06vol, 2006.

[CANS:RebSelDev06]

[CANS:ZhaYuLiu10]

[CAOR:GM00]

[CHES:AkkGir01]

[CHES:BBKK07]

[CHES:Bogdanov08]

[CHES:BonMir06]

[CHES:BosOzeSta11]

[CHES:CFGRV11]


Benaissa, M. and T. Good, "AES on FPGA from the Fastest to
[CHES:GouMar11]

[CHES:Hamburg09]

[CHES:HarWal07]

[CHES:Jaffe07]

[CHES:KasSch09]

[CHES:KerRey08]

[CHES:KimHonLim11]

[CHES:KuoVer01]

[CHES:LWFB07]
Wolkerstorfer, J., Felber, N., Braendli, M., and S.


[CHES:NeiPul04]

[CHES:Patterson00]

[CHES:PirQui03]

[CHES:PosLinWan10]

[CHES:ProRoc11]

[CHES:RKSF11]

[CHES:RenStaVey09]

[CHES:RivPro10]

[CHES:SLFP04]
[CHES:SRQL03]

[CHES:SSHA08]
Sugawara, T., Homma, N., Aoki, T., and A. Satoh, "High-Performance Concurrent Error Detection Scheme for AES Hardware", Lecture Notes in Computer Science ches08vol, 2008.

[CHES:SatMor03]

[CHES:StaBerPre04]

[CHES:TilGro06]

[CHES:TilGro07]

[CHES:TilHer08]

[CHES:TriDeSGer02]

[CHES:YamYajIto08]
Hardware Implementation of the MISTY1 Block Cipher”, Lecture Notes in Computer Science ches08vol, 2008.


[EC:BirNik10]

[EC:BorKnuRij97]  

[EC:DaeRij02]  

[EC:Golic97a]  

[EC:Hawkes98]  

[EC:Kuhn01]  

[EC:MPLPW11]  

[EC:Mantin05]  

[EC:Matsui93]  

[EC:Meier93]  
[EC:SepVauVua11]  

[EC:VanWie90]  

[FC:BloSei03]  

[FC:DamKell10]  

[FIPS-197]  

[FIPS-46]  

[FIPS-46-3]  

[FSE:AES97]  

[FSE:BVPCS03]  

[FSE:Bernstein05]  

[FSE:BihAndKnu98]  
J., R., R., L., and E. Biham, "Serpent: A New Block Cipher

[FSE:BihBirSha99]  

[FSE:BihCar08]  

[FSE:BihDunKel01]  

[FSE:BihDunKel03a]  

[FSE:BihDunKel07b]  

[FSE:BihGraNgu05]  

[FSE:BucPysWei06]  

[FSE:CidMurRob05]  

[FSE:ColStaQui08]  
[FSE:DemSel08]

[FSE:FluMcG00]

[FSE:GilPey10]

[FSE:Granboulan01]

[FSE:Gueron09]

[FSE:HKLP05]
Kim, J., Lee, S., Preneel, B., and S. Hong, "Related-Key Rectangle Attacks on Reduced Versions of SHACAL-1 and AES-192", Lecture Notes in Computer Science fse05vol, 2005.

[FSE:IYYK01]

[FSE:Isobe11]

[FSE:IwaKur00]

[FSE:JunMac09]
Macchetti, M. and P. Junod, "Revisiting the IDEA Philosophy", Lecture Notes in Computer Science fse09vol,
[FSE:Junod05]

[FSE:KLLLL02]

[FSE:KRRR98]

[FSE:KanMat01]

[FSE:KarMan07]

[FSE:KelKohSch00]

[FSE:KimHonPre07]
Hong, S., Preneel, B., and J. Kim, "Related-Key Rectangle Attacks on Reduced AES-192 and AES-256", Lecture Notes in Computer Science fse07vol, 2007.

[FSE:Kuhn02]
Kuhn, U., "Improved Cryptanalysis of MISTY1", Lecture Notes in Computer Science fse02vol, 2002.

[FSE:Lucks01]

[FSE:Lucks98]
[FSE:MaiPau08]

[FSE:MaiPauSen11]

[FSE:ManSha01]

[FSE:Matsui09]

[FSE:Matsui97]

[FSE:Maximov05]

[FSE:MenPraRec08]

[FSE:Messerges00]

[FSE:MinTsu06]

[FSE:MorShiKan98]
[FSE:OBSC10]

[FSE:OMPR05]

[FSE:PauPre04]

[FSE:Raddum03]

[FSE:SSAMI07]

[FSE:Sasaki11]

[FSE:Schneier93]
Schneier, B., "Description of a New Variable-Length Key 64-bit Block Cipher (Blowfish)", Lecture Notes in Computer Science fse93vol, 1993.

[FSE:ShiKanAbe02]

[FSE:SonSeb03]

[FSE:Vaudenay96]

[FSE:Wernsdorf02]  

[FSE:YeoParKim02]  

[HRDA:HSK02]  

[I-D.kiyomoto-kcipher2]  

[ICICS:AciKoc06]  
Kaya, . and O. Acii\ccmez, "Trace-Driven Cache Attacks on AES (Short Paper)", Lecture Notes in Computer Science icics06vol, 2006.

[ICICS:BNPV02]  

[ICICS:CheWuFen07]  

[ICICS:HeQin01]  

[ICICS:KelSchWag97]  


Dunkelman, O. and D. Toz, "Analysis of Two Attacks on Reduced-Round Versions of the SMS4", Lecture Notes in Computer Science icics08vol, 2008.


Ding, J., Christensen, C., and J. Erickson, "Algebraic

[ICISC:Karroumi10]

[ICISC:LHLLY01]

[ICISC:LopRodDia05]

[ICISC:Mangard02]

[ICISC:SonSeb02]

[ICISC:TSSK08]

[ICISC:YanParYou06]

[ICISC:ZhaWuFen07]

[IDCC:TTSSSK08]
Tsunoo, Y., Tsujihara2, E., Shigeri, M., Saito, T.,


[INDOCRYPT:FFGL10] Förlre, C., Gorski, M., Lucks, S., and E. Fleischmann,

[INDOCRYPT:GorLuc08]

[INDOCRYPT:JiHu07]
Hu, L. and W. Ji, "New Description of SMS4 by an Embedding over GF(2^8)", Lecture Notes in Computer Science indocrypt07vol, 2007.

[INDOCRYPT:KumMukCho07]

[INDOCRYPT:LDKK08]

[INDOCRYPT:MDRM10]

[INDOCRYPT:MaiPau08]

[INDOCRYPT:ManGre10]

[INDOCRYPT:MulWysPre10]

[INDOCRYPT:PauPre03]
Notes in Computer Science indocrypt03vol, 2003.

[INDOCRYPT:ProRoc10]

[INDOCRYPT:SSMS10]

[INDOCRYPT:Tezcan10]

[INDOCRYPT:Yildirim03]

[INDOCRYPT:ZZWF07]

[ISC:BatGieLem08]

[ISC:CGBS01]

[ISC:GueKou08]

[ISC:IndPre08]
Preneel, B. and S. Indesteege, "Collisions for RC4-Hash",
Lecture Notes in Computer Science isc08vol, 2008.

[ISC:LuDes10]  

[ISC:LuWanLin08]  

[ISC:NakPav07]  

[ISC:NakPreVan03]  

[ISC:SatMor03]  

[ISC:ZWPKY08]  

[ISPEC:BaiLi11]  

[IWSEC:HSST08]  

[IWSEC:KRCJ06]  
Sasaki, Y., "Known-Key Attacks on Rijndael with Large Blocks and Strengthening ShiftRow Parameter", Lecture Notes in Computer Science iwsec10vol, 2010.

Cryptography Research, "Record Breaking DES Key Search Completed", 1998.


Kim, T., Kim, J., Hong, S., and J. Sun, "SMS4: Linear and Differential Cryptanalysis of Reduced SMS4 Block Cipher", Cryptology ePrint Archive LDC08vol, 2008.


Epstein, L., Shachnai, H., Tamir, T., and H. Attiya,

[Bilham, Dunkelman, Keller, 2001]


[Adams, 1997]


[Rivest, 1998]


[Adams and Gilchrist, 1999]


[Ohta and Matsui, 2000]


[Matsui, Nakajima, Moriai, 2004]


[Lee, Lee, Yoon, Cheon, Lee, 2005]


[Boesgaard, Vesterager, Zenner, 2006]


[Kelly, 2006]


[Shirey, 2007]


[McGrew, 2008]


[Lee, Lee, Kim, Kwon, Kim, 2010]


[Dolmatov, 2010]


[Katagi and Moriai, 2009]

Katagi, M. and S. Moriai, "The 128-Bit Blockciper
CLEFIA", RFC 6114, March 2011.

[RKIDA:BDK06]

[RSA:AciSchKoc07]

[RSA:BEPW10]

[RSA:BihDunKel06]

[RSA:ClaGieVer08]

[RSA:Konighofer08]

[RSA:LKKD08]
Kim, J., Keller, N., Dunkelman, O., and J. Lu, "Improving the Efficiency of Impossible Differential Cryptanalysis of Reduced Camellia and MISTY1", Lecture Notes in Computer Science rsa08vol, 2008.

[RSA:MBPV05]

[RSA:OsvShaTro06]
Shamir, A., Tromer, E., and D. Arne, "Cache Attacks and Countermeasures: The Case of AES", Lecture Notes in


[SAC:BilGilEch04]

[SAC:BloGuaKru04]

[SAC:BloKru07]

[SAC:Bogdanov07]

[SAC:CEJV02]

[SAC:CanOsV09]

[SAC:DemSelTur03]

[SAC:Demirci02]

[SAC:EtrRob08]

[SAC:FegSchWhi01]

[SAC:FluManSha01]
Mantin, I., Shamir, A., and S. R., "Weaknesses in the Key

[SAC:HatSekKan02]

[SAC:JakDes03]

[SAC:KelMeiTav01]

[SAC:KirYou09]

[SAC:LeiChaFen05]
Chao, L., Feng, K., and D. Lei, "New Observation on Camellia", Lecture Notes in Computer Science sac05vol, 2005.

[SAC:Lipmaa98]

[SAC:MPRS09]
Peyrin, T., Rechberger, C., Schl\alphaffer, M., and F. Mendel, "Improved Cryptanalysis of the Reduced Gr\ostl Compression Function ECHO Permutation and AES Block Cipher," , Lecture Notes in Computer Science sac09vol, 2009.

[SAC:MSDB09]

[SAC:MisTav98]
E., S. and S. Mister, "Cryptanalysis of RC4-like Ciphers",
Lecture Notes in Computer Science sac98vol, 1999.

[SAC:NevSei06]

[SAC:Nikolic10]

[SAC:PauMai07]

[SAC:PirQuis04]

[SAC:ReiWag02]

[SAC:SKWHWH98]

[SAC:SekKan00]

[SAC:SepVauVua10]

[SAC:SunLai09]
Lai, X. and X. Sun, "Improved Integral Attacks on MISTY1", Lecture Notes in Computer Science sac09vol, 2009.

[SAC:Tsow09]
Tsow, A., "An Improved Recovery Algorithm for Decayed AES Key Schedule Images", Lecture Notes in Computer


OSCCA, "The SMS4 Block Cipher", 2006.


Authors’ Addresses

David McGrew
Cisco Systems
13600 Dulles Technology Drive
Herndon, VA  20171
USA

Email: mcgrew@cisco.com

Sean Shen
Chinese Academy of Science
No.4 South 4th Zhongguancun Street
Beijing,  100190
China

Phone: +86 10-58813038
Email: shenshuo@cnnic.cn