KU LEUVEN

Challenges in Symmetric-Key Cryptography

Vincent Rijmen

KU Leuven and University of Bergen

Indocrypt 2024

Overview

- Some highlights of 25 years of blockcipher design
  - (a subjective view)
- The impact of Moore's law in the coming decades
- Challenges & research problems

1997: AES kick-off

All meetings are accessible to persons with disabilities. Sign language interpreters and an assistive listening system are available at all meetings.

David Capozzi,

Director, Office of Technical and Information Services.

[FR Doc. 96–33125 Filed 12–31–96; 8:45 am]

BILLING CODE 8150–01–P

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket No. 960924272–6272–01]

RIN 0693–ZA13

Announcing Development of a Federal Information Processing Standard for Advanced Encryption Standard

AGENCY: National Institute of Standards and Technology (NIST), Commerce.

ACTION: Notice; Request for comments.

SUMMARY: A process to develop a Federal Information Processing Standard (FIPS) for Advanced Encryption Standard (AES) incorporating an Advanced Encryption Algorithm (AEA) is being initiated by the National Institute of Standards and Technology (NIST). As the first step in this process, draft minimum acceptability requirements and draft

and Technology, Gaithersburg, MD 20899.

Electronic comments may be sent to AES@nist.gov.

Comments received in response to this notice will be made part of the public record and will be made available for inspection and copying in the Central Records and Reference Inspection Facility, Room 6020, Herbert C. Hoover Building, 14th Street between Pennsylvania and Constitution Avenues, NW, Washington, DC, 20230.

The AES Criteria Workshop will be held at the Green Auditorium, Administration Building, National Institute of Standards and Technology, Gaithersburg, Maryland. Copies of the comments submitted will be available at the Workshop. For planning purposes, advance registration is encouraged. To register, please fax your name, address, telephone, fax and e-mail address to 301–948–1233 (Attn: AES Criteria Workshop) by April 10, 1997. Registration will also be available at the door. The workshop will be open to the public.

FOR FURTHER INFORMATION CONTACT: Edward Roback, National Institute of Standards and Technology, Building 820, Room 426, Gaithersburg, MD 20899; telephone 301–975–3696 or via fax at 301–948–1233. Technical inquiries regarding the proposed draft evaluation criteria and draft submission requirements should be addressed to

alternatives may be proposed as a replacement standard at the 1998 review."

It is NIST's review that a multi-year transition period will be necessary to move toward any new encryption standard and that DES will continue to be of sufficient strength for many applications. NIST will consult with all interested parties so that a smooth transition can be accomplished.

In order to provide a basis for the evaluation of encryption algorithms submitted to be considered as the AEA for incorporation into the FIPS for AES, evaluation criteria will be used to review submitted algorithms. Comments on the draft criteria (and, at the appropriate time, or candidate algorithms) from voluntary consensus standards organizations are particularly encouraged.

Proposed Draft Minimum Acceptability Requirements and Evaluation Criteria

The draft minimum acceptability requirements and evaluation criteria are:

A.1 AES shall be publicly defined.

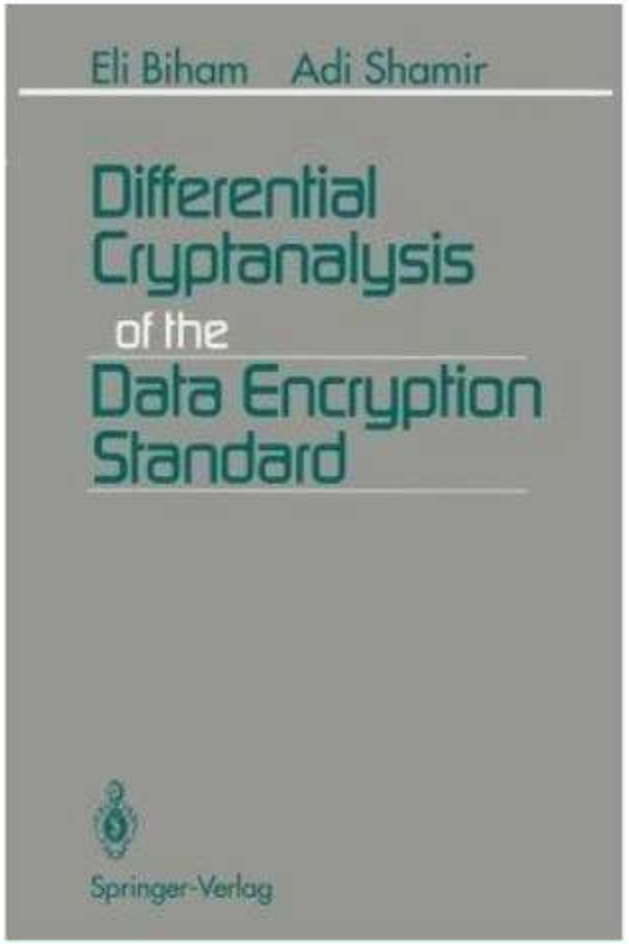
A.2 AES shall be a symmetric block cipher.

A.3 AES shall be designed so that the key length may be increased as needed.

A.4 AES shall be implementable in both hardware and software.

A.5 AES shall either be (a) freely available or (b) available under terms

AES prelude: cliffs ahead for DES



Linear Cryptanalysis Method for DES Cipher

Mitsuru Matsui

Computer & Information Systems Laboratory
Mitsubishi Electric Corporation
5-1-1, Ofuna, Kamakura, Kanagawa 247, Japan
E-mail matsui@mmt.isl.melco.co.jp

Abstract

We introduce a new method for cryptanalysis of DES cipher, which is essentially a known-plaintext attack. As a result, it is possible to break 8-round DES cipher with 2^{21} known-plaintexts and 16-round DES cipher with 2^{47} known-plaintexts, respectively. Moreover, this method is applicable to an only-ciphertext attack in certain situations. For example, if plaintexts consist of natural English sentences represented by ASCII codes, 8-round DES cipher is breakable with 2^{29} ciphertexts only.

1 Introduction

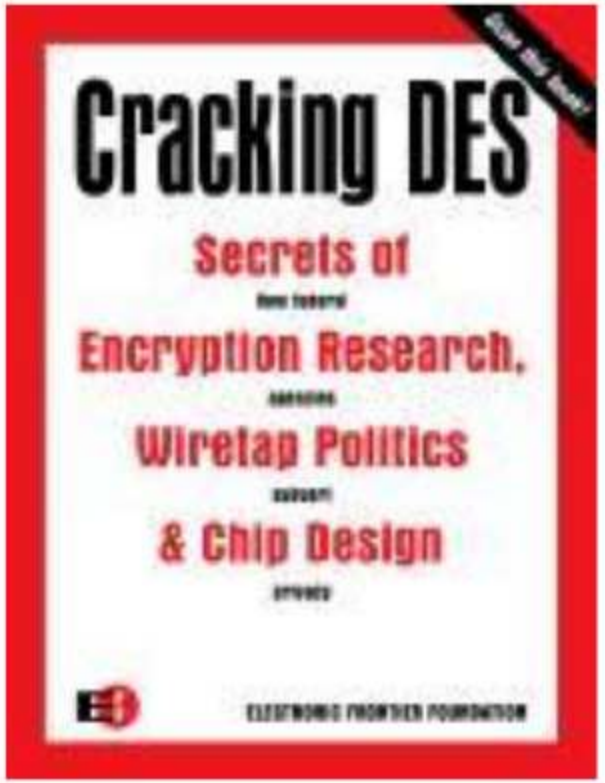
Differential Cryptanalysis has been one of main topics in cryptology since the first paper by Biham and Shamir in 1990 [1]. They have broken FEAL cipher in the subsequent paper [2], and recently succeeded in breaking the full 16-round DES cipher by a chosen-plaintext attack [3].

Although Differential Cryptanalysis is a technique for a chosen-plaintext attack, it is more noteworthy that it can be applied to a known-plaintext attack on condition that sufficiently many plaintexts are available.

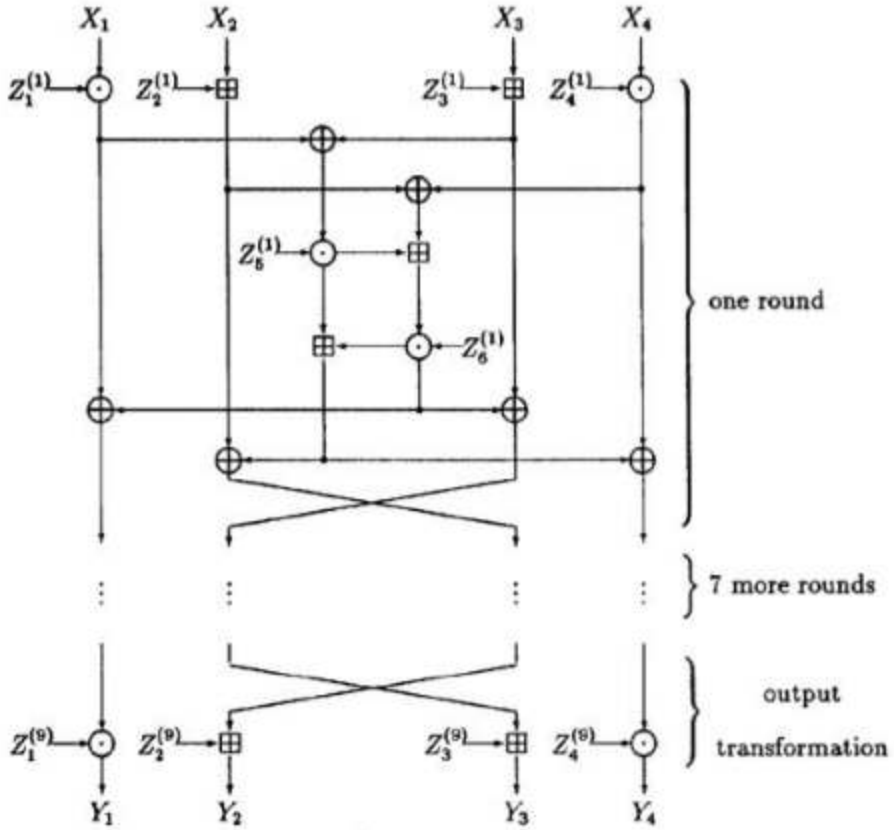
On the other hand, several new approaches to known-plaintext attacks have been also studied in special cases. As regards FEAL cipher, for example, Tardy-Corfdir and Gilbert have presented a statistical method to break FEAL-4 and FEAL-6 [4], and Matsui and Yamagishi have described a deterministic method to break FEAL-8 by a known-plaintext attack [5], respectively.

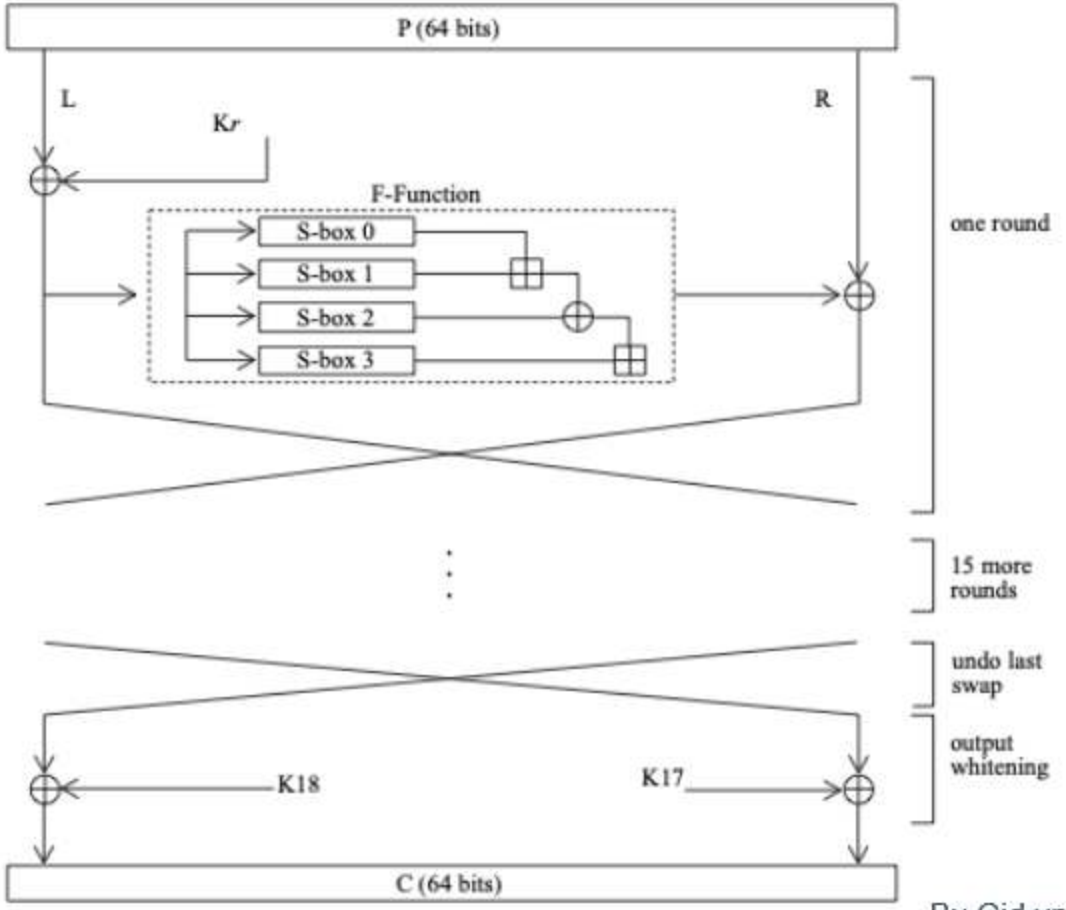
In this paper we introduce an essentially known-plaintext attack of DES cipher. The purpose of this method is to obtain a linear approximate expression of a given cipher algorithm. For this purpose, we begin by constructing a statistical linear path between input and output bits of each S-box. Then we extend this path to the entire algorithm, and finally reach a linear approximate expression without any intermediate value.

T. Helleseth (Ed.): Advances in Cryptology - EUROCRYPT '93, LNCS 765, pp. 386-397, 1994.



AES prelude: pirates sighted





By Gid.vn

1998-2001: the AES process

- Open
  - Clear view on the evaluation and selection procedure
  - Extensive documentation of decisions

- High profile
  - Cooperation with FSE conferences and community
    - 200-250 attendants at FSE and at dedicated AES conferences
  - Winner “guaranteed” to become an important standard

AES aftermath

Recommended Reading

1. Denning DE, Sacco GM (1981) Timestamps in key distribution protocols. Commun ACM 24(8):533–536
2. Lowe G (1995) An attack on the Needham-Schroeder public key authentication protocol. Inform Process Lett 56(3):131–133
3. Menezes A, van Oorschot PC, Vanstone SA (1996) Handbook of applied cryptography. CRC Press, Boca Raton, Florida
4. Needham RM, Schroeder MD (1978) Using encryption for authentication in large networks of computers. Commun ACM 21(12):993–999

NESSIE Project

Bart Preneel
Department of Electrical Engineering-ESAT/COSIC,
Katholieke Universiteit Leuven and IBBT,
Leuven-Heverlee, Belgium

Related Concepts

►Block Ciphers; ►Digital Signature Schemes; ►Hash Functions; ►Identification Schemes; ►MAC Algorithms; ►Public-Key Encryption Schemes; ►Stream Cipher

Definition

NESSIE (New European Schemes for Signature, Integrity and Encryption) [23] was a research project within the Information Societies Technology (IST) Programme of the European Commission (IST-1999-12324). The seven NESSIE participants were: Katholieke Universiteit Leuven (Belgium), coordinator; Ecole Normale Supérieure (France); Royal Holloway, University of London (U.K.); Siemens Aktiengesellschaft (Germany); Technion – Israel Institute of Technology (Israel); Université Catholique de Louvain (Belgium); and Universitetet i Bergen (Norway).

Background

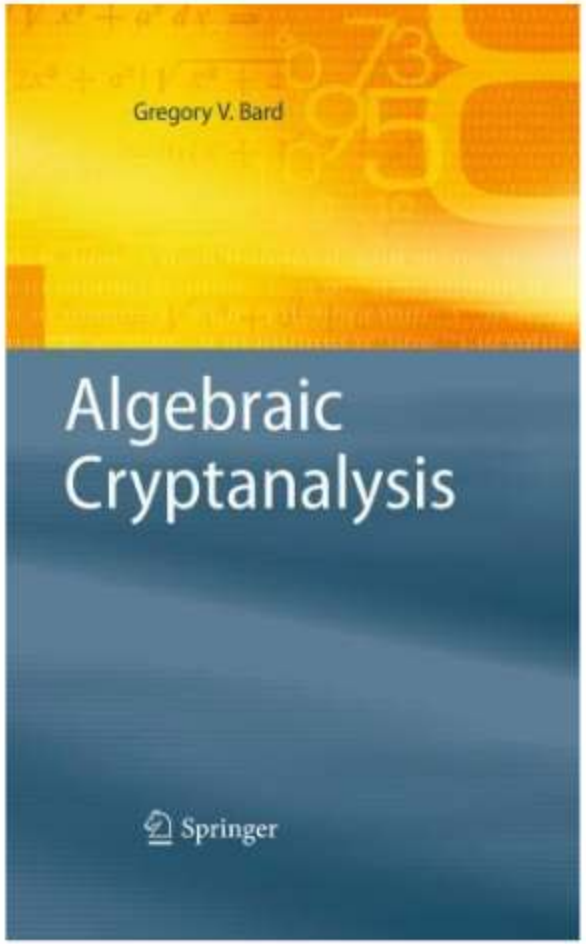
NESSIE was a 40 month project, which started in January 2000. The goal of the NESSIE project was to put forward

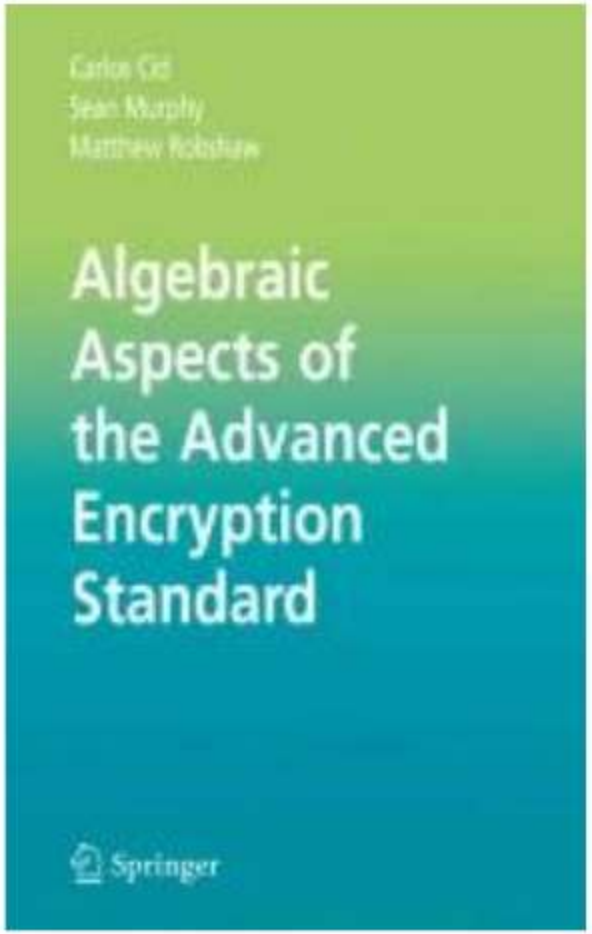
confidentiality, data integrity, and authentication. These algorithms include ►Block Ciphers, ►Synchronous and ►Self-Synchronizing Stream Ciphers, ►Hash Functions, ►MAC Algorithms, ►Digital Signature Schemes, public-key encryption schemes, and identification schemes. The call also invited the submission of evaluation methodologies for these algorithms. While key management protocols are also very important, it was felt that they should be excluded from the call, as the scope of the call was already rather wide. The scope has been defined together with the project industry board (consisting of more than 25 companies). The deadline for submissions was September 29, 2000. In response to this call NESSIE received 40 submissions from major players. Two-thirds of the submissions came from industry, and there was some industry involvement in every 5 out of 6 algorithms.

The scope of the NESSIE call was much wider than that of the *AES* call launched by NIST [24], which was restricted to 128-bit block ciphers, and that of the more recent *AHS* (SHA-3) call [25], which focuses on hash functions. It was comparable to that of the RACE Project RIPE (Race Integrity Primitives Evaluation, 1988–1992) [28] (confidentiality algorithms were excluded from RIPE for political reasons) and that of the Japanese *CRYPTREC* project [6] (which also includes key establishment protocols and pseudo-random number generation). Another difference was that the *AES* and *AHS* competitions and *CRYPTREC* intend to produce algorithms for government standards. The results of NESSIE were not intended for adoption by any government or by the European commission and have not become NESSIE Standards. However, the intention was that relevant standardization bodies would adopt these results.

The call also specified the main selection criteria which will be used to evaluate the proposals. These criteria are long-term security, market requirements, efficiency, and flexibility. Submissions could be targeted toward a specific environment (such as 8-bit smart cards or high-end 64-bit processors), but it is clearly an advantage to offer a wide

AES aftermath (ctd.)





2003: start of AES acceptance

FACT SHEET

CNSS Policy No. 15, Fact Sheet No. 1
National Policy on the Use of the Advanced Encryption Standard (AES) to Protect National Security Systems and National Security Information

June 2003

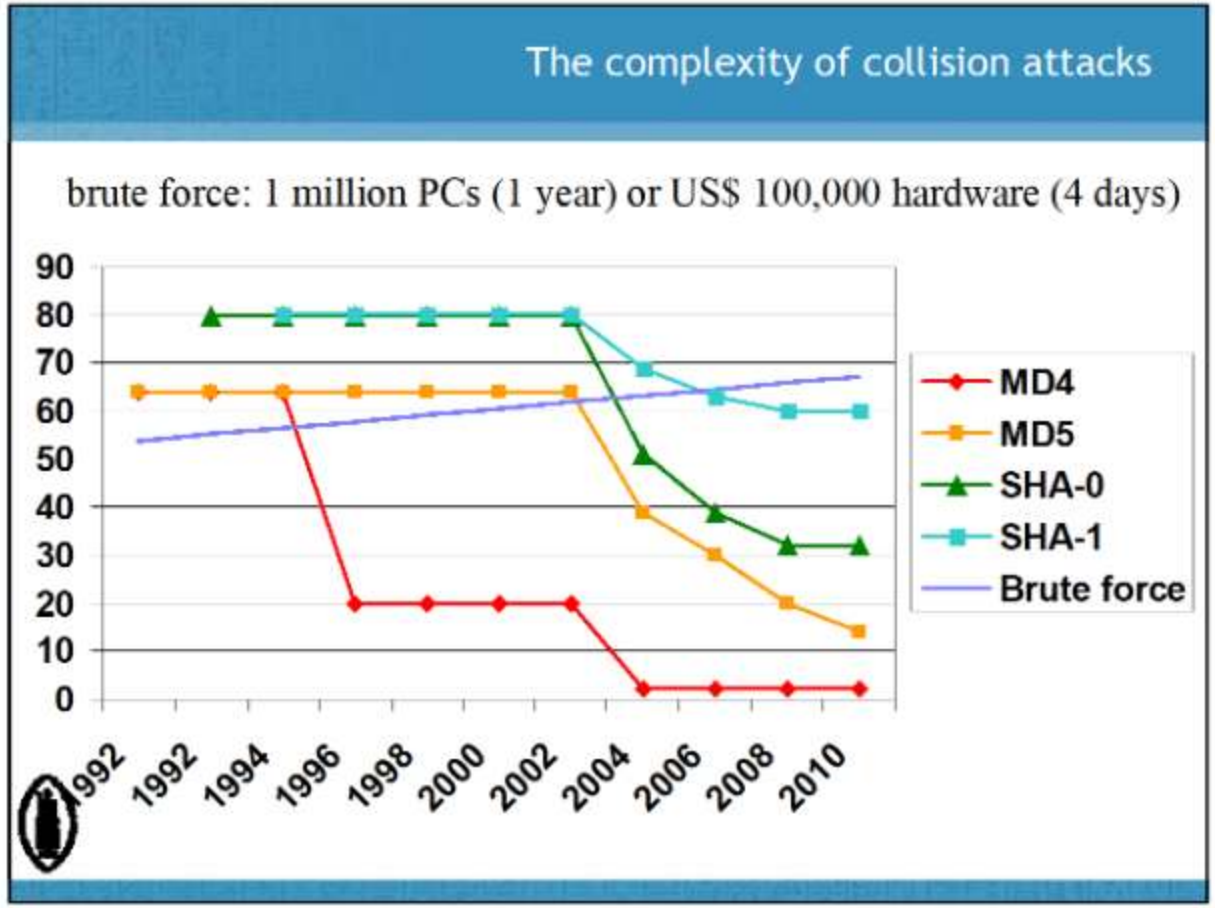
Background

(1) Federal Information Federal Information Processing Standard (FIPS) No. 197, dated 26 November 2001, promulgated and endorsed the Advanced Encryption Standard (AES) as the approved algorithm for protecting sensitive (unclassified) electronic data. Since that time, questions have arisen whether AES (or products in which AES is implemented) can or should be used to protect classified information and at what levels. Responsive to those questions, the National Security Agency (NSA) has conducted a review and analysis of AES and its applicability to the protection of national security systems and/or information. The policy guidance documented herein reflects the results of those efforts.

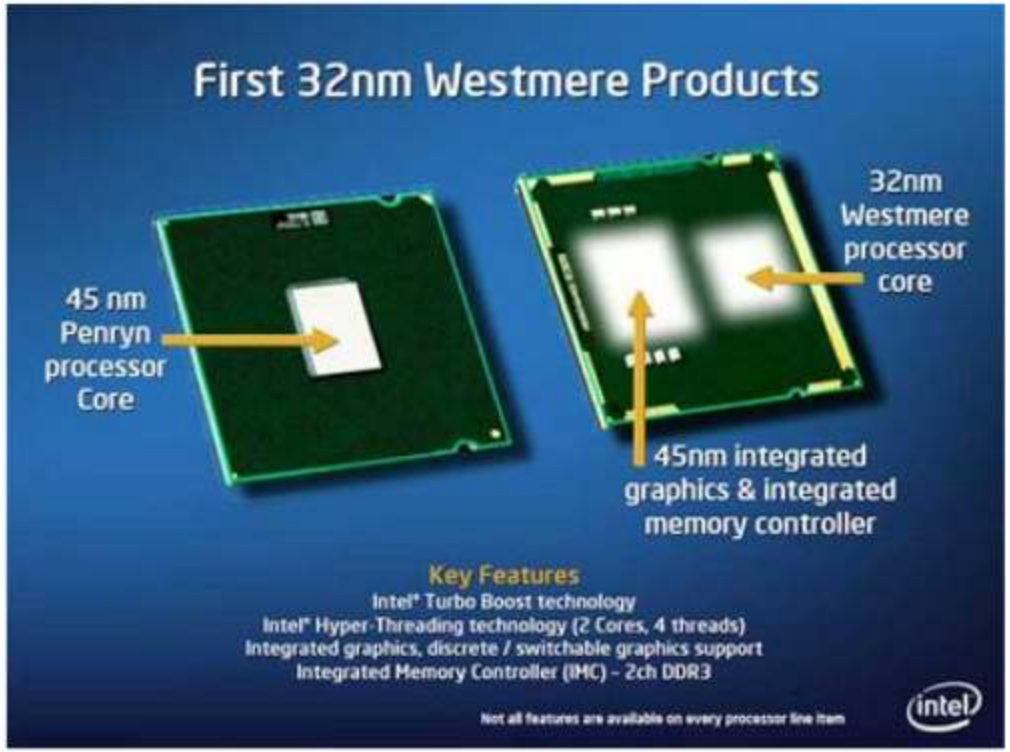
Introduction

(2) In the context of today's complex world and even more complex communicating environments, the need for protecting information takes on added importance and

2004: Hash function crisis



2010: wide AES deployment



Breakthrough cryptanalysis methods since 2000

- 2004: message modification techniques
  - Hash functions ≠ block ciphers
- 2009: cube attack (based on AIDA, 2005)
- 2015: division cryptanalysis
  - Nonlinear degree is important
- 2010: rotational cryptanalysis

Cryptographic competitions & initiatives

- SHA-3 2007-2012
- CAESAR 2012-2019
- Lightweight encryption 2013-2023
- Modes of Operation 2002-…
  - Authenticated encryption
  - Authentication
  - Format preserving encryption

New requirements for blockciphers

- Zero-Knowledge proving mechanisms
- Homomorphic Encryption schemes
- Secure MultiParty Computation protocols
- Quantum-Secure signature schemes
- Side-Channel Attack resistant designs

Current landscape

- Multitude of application-specific designs
- Slow progress in cryptanalysis
- Slow uptake of new ideas
- Difficult to keep focus and momentum

Evolution of computational power

- Moore's law:
  - Miniaturization of circuits and memory leads to faster computers
    - Market pressure keeps prices low
- When will Moore's law end?
- Cannot continue into sub-atomic level
  - Current technology: 3nm ≈ 30 atoms
  - Is the end in sight?

Diluted meaning of technology names

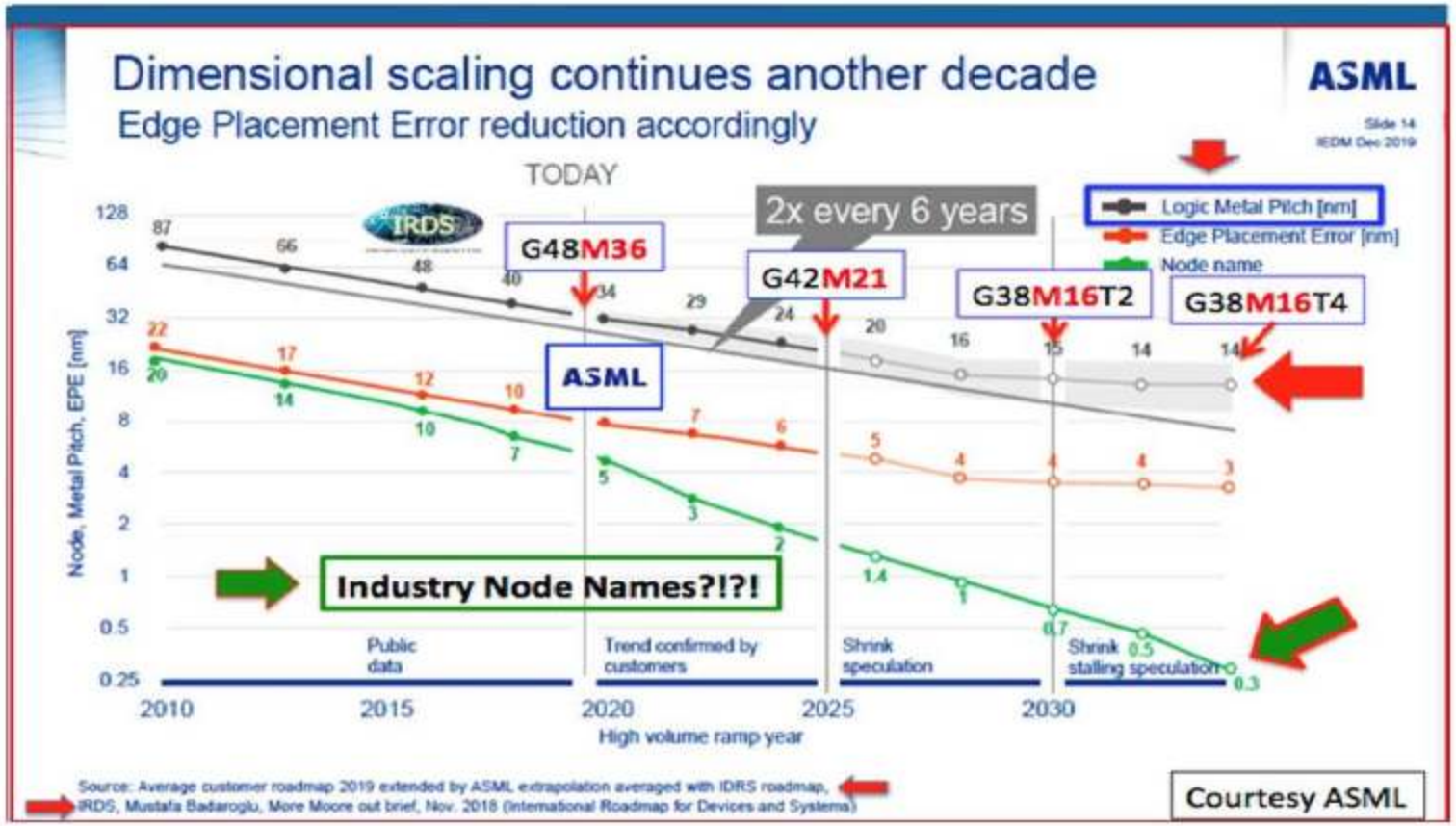


Figure ES29 *Consistent definition and trend of metal half-pitch reported by ASML and IRDS*

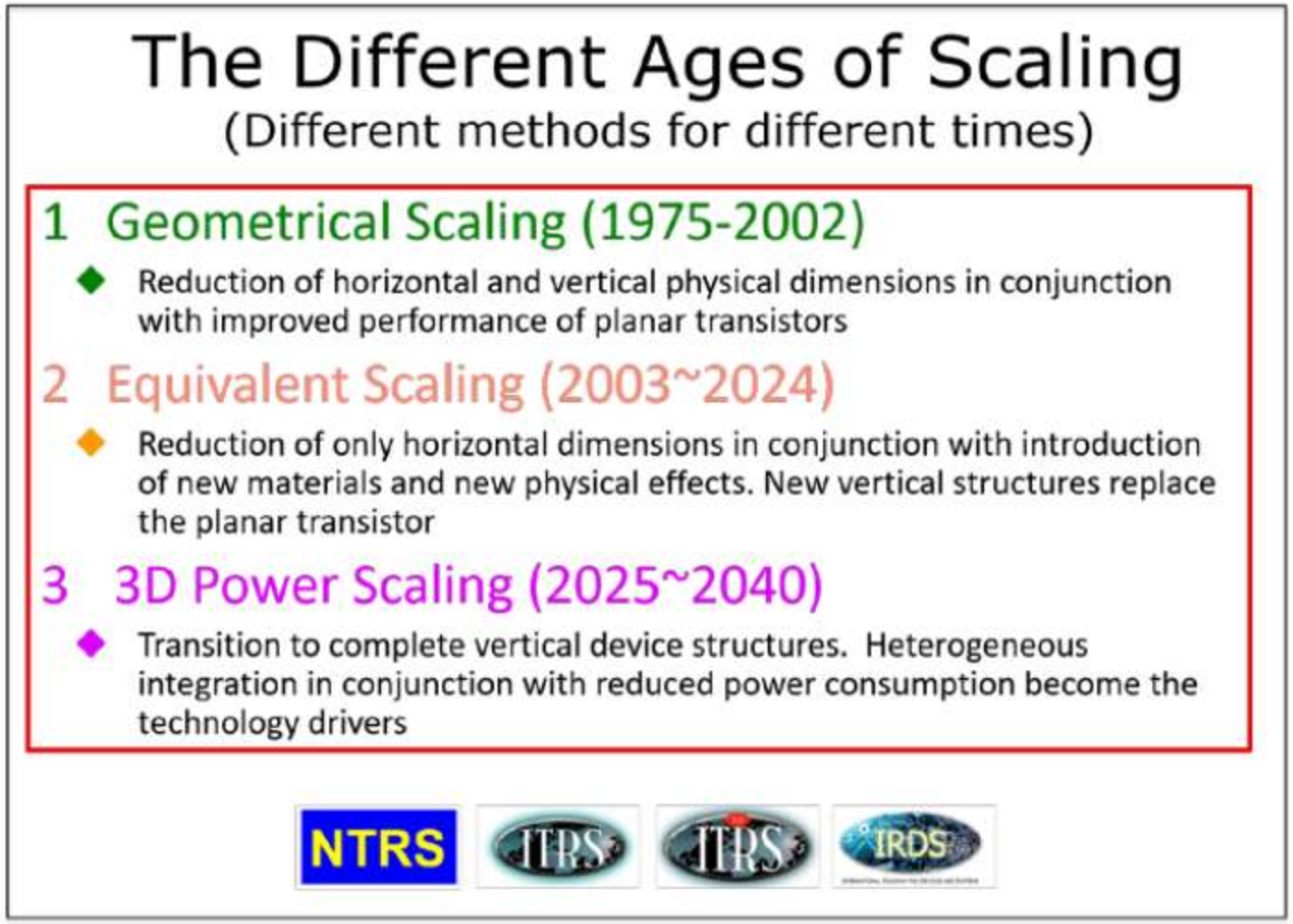


Figure ES55 *The 3 eras of scaling heralded by NTRS, ITRS, ITRS 2.0, and IRDS*

Computing beyond 2040

- Limits caused by
  - Energy consumption
  - Material required

- Quantum computers may break these limits

- Current quantum computing hardware is not scalable
- … but engineers will develop new technologies

Impact of QC on Symmetric-Key Cryptology

- Symmetric-key techniques may become (even) more important
- Necessity to perform more detailed quantum-security evaluations
  - Current results are generic attacks
    - Double key length (but not double double)
  - Impact of design decisions: ???
- Challenge: apply quantum algorithms to symmetric-key cryptanalysis

Improving symmetric-key theory

- Get away from the bits
- Higher level of abstraction
  - Tackle many of the new applications at once
  - Easier communication with quantum information researchers
  - Some problems present in current theory disappear

- Early examples:
  - AES description in GF(256)
  - Generalisations of linear cryptanalysis

Example 1: non-uniform diffusion layers

- AES: uniform diffusion layer
  - Branch number
  - MDS-based transformations

- Non-uniform layers:
  - Feistel
  - Lai-Massey
  - Misty
  - Unbalanced Feistel
  - Incomplete S-box layers

Example 1 (ctd.)

- Lai-Massey and Feistel are affine equivalent
  - Cf. next session

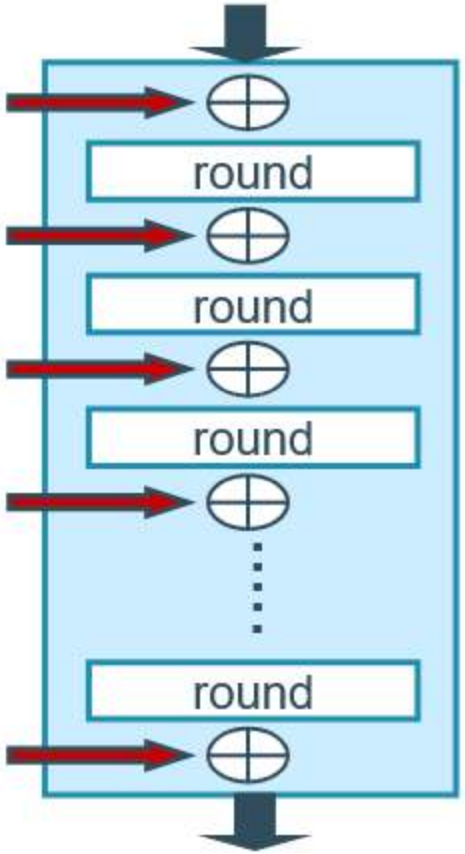
- Unbalanced Feistel Network vs. Incomplete Diffusion

- Challenge:
  - Develop criterion to measure the quality of unbalanced diffusion structures
  - Define optimality
  - Design optimal structures

Example 2: Markov cipher theory

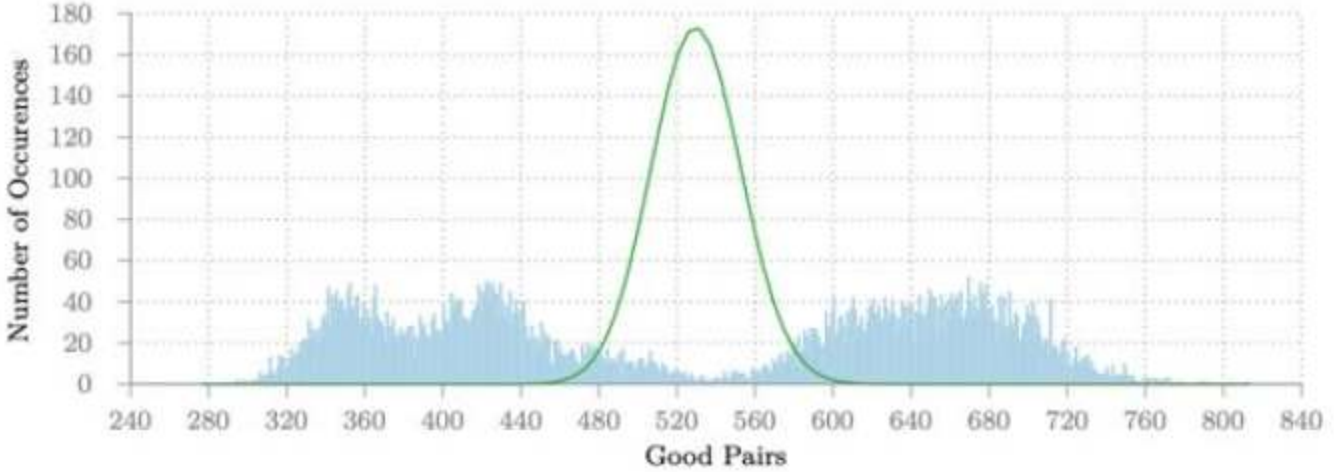
- Problematic assumptions:
  - Independent & uniformly random round keys
  - Hypothesis of stochastic equivalence

- Lead to
  - Invalid characteristics
  - Invalid results



Speck

- ARX cipher [Beaulieu+ 2013]
- Analysed in [Ankele,Kölbl 2018]
  - 7 rounds of Speck-64
  - Multimodal distribution



Geometric Approach

x	y=F(x)
000	111
001	010
010	100
011	101
100	001
101	110
110	011
111	000

"one-hot encoding"

$$Y = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} X$$

$$T^F[y, x] = 1 \Leftrightarrow y = F(x)$$

Geometric Approach: pairs

- Pairs: $\begin{bmatrix} Y \\ Y^* \end{bmatrix} = (T^F \otimes T^F) \begin{bmatrix} X \\ X^* \end{bmatrix}$

- $\begin{bmatrix} Y \\ Y^* \end{bmatrix}, \begin{bmatrix} X \\ X^* \end{bmatrix}$ range over all values with weight one: “standard basis” for $\mathbb{R}^{2n}$

Geometric Approach: change the basis

$$\begin{bmatrix} Y \\ Y^* \end{bmatrix} = (T^F \otimes T^F) \begin{bmatrix} X \\ X^* \end{bmatrix}$$

- For any invertible $R \in \mathbb{R}^{2n \times 2n}$, we can write:

$$\left.\begin{aligned} \begin{bmatrix} X \\ X^* \end{bmatrix} &= R \begin{bmatrix} U \\ A \end{bmatrix} \\ \begin{bmatrix} Y \\ Y^* \end{bmatrix} &= R \begin{bmatrix} V \\ B \end{bmatrix} \end{aligned}\right\} \Rightarrow \begin{bmatrix} V \\ B \end{bmatrix} = R^{-1}(T^F \otimes T^F) R \begin{bmatrix} U \\ A \end{bmatrix}$$

- Choose R to obtain a simple $R^{-1}(T^F \otimes T^F)R$

Quasi-Differential Trails

- For the right choice of R, we obtain a set $\left\{ \begin{bmatrix} U \\ A \end{bmatrix}_{u,a} \right\}_{u,a \in \mathbb{F}^n}$:

$$\begin{bmatrix} U \\ A \end{bmatrix}_{u,a} [x_1, x_2] = \begin{cases} 0, \text{if } x_1 + x_2 \neq a \\ 1, \text{if } x_1 + x_2 = a \text{ and } u^t x_1 = 0 \\ -1, \text{if } x_1 + x_2 = a \text{ and } u^t x_1 = 1 \end{cases}$$

We denote $R^{-1}(T^F \otimes T^F)R$ by D^F, the *quasi-differential transition matrix*

Quasi-Differential Transition Matrix

$$D^F_{(v,b),(u,a)} = \frac{1}{2^n} \sum_{x \in \mathbb{F}_2^n, F(x+a)=F(x)+b} (-1)^{u^t x + v^t F(x)}$$

- Contains the correlations measured over the set of right pairs of the differential
- $D^F_{(0,b),(0,a)}$: the DDT
- $D^F_{(v,0),(u,0)}$: the correlation matrix (= scaled version of the LAT table)

Accurate probability of a characteristic

- If $F = F_2 \circ F_1$ then $D^F = D^{F_2} \times D^{F_1}$
- $\Pr\big(\text{characteristic } (a_0, a_1, \dots, a_r)\big) = \sum_{\substack{u_i \in \mathbb{F}_2^n \\ i=1,\dots,r-1}} \prod_{i=1}^{r} \mathrm{D}^{F_i}_{(u_i,a_i),(u_{i-1},a_{i-1})}$

  With $F_{i-1}(x_{i-1}) = x_i, u_0 = u_r = 0$

Accurate probability of a characteristic (ctd.)

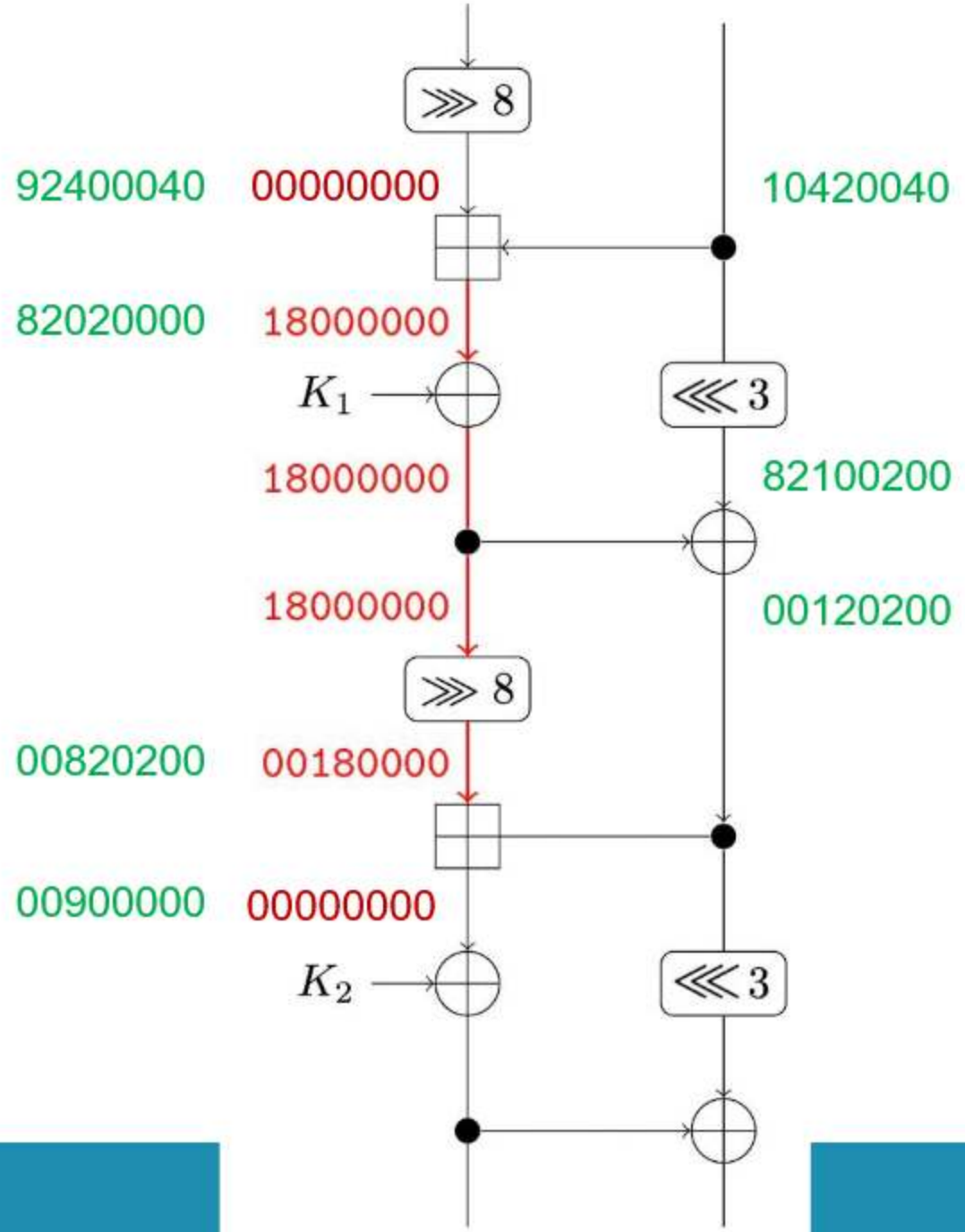
- For a key-alternating cipher:

$$\Pr\big(\text{characteristic } (a_0, a_1, \dots, a_r)\big) = \sum_{\substack{u_i \in \mathbb{F}_2^n \\ i=1,\dots,r-1}} \prod_{i=1}^{r} (-1)^{u_i^t k_i} D^F_{(u_i,a_i),(u_{i-1},a_{i-1})}$$

- No assumptions!! (Markov, independent roundkeys, …)
- Commonly made approximation corresponds to picking only one term ($u_i = 0$)

Speck: 1 extra quasidifferential trail

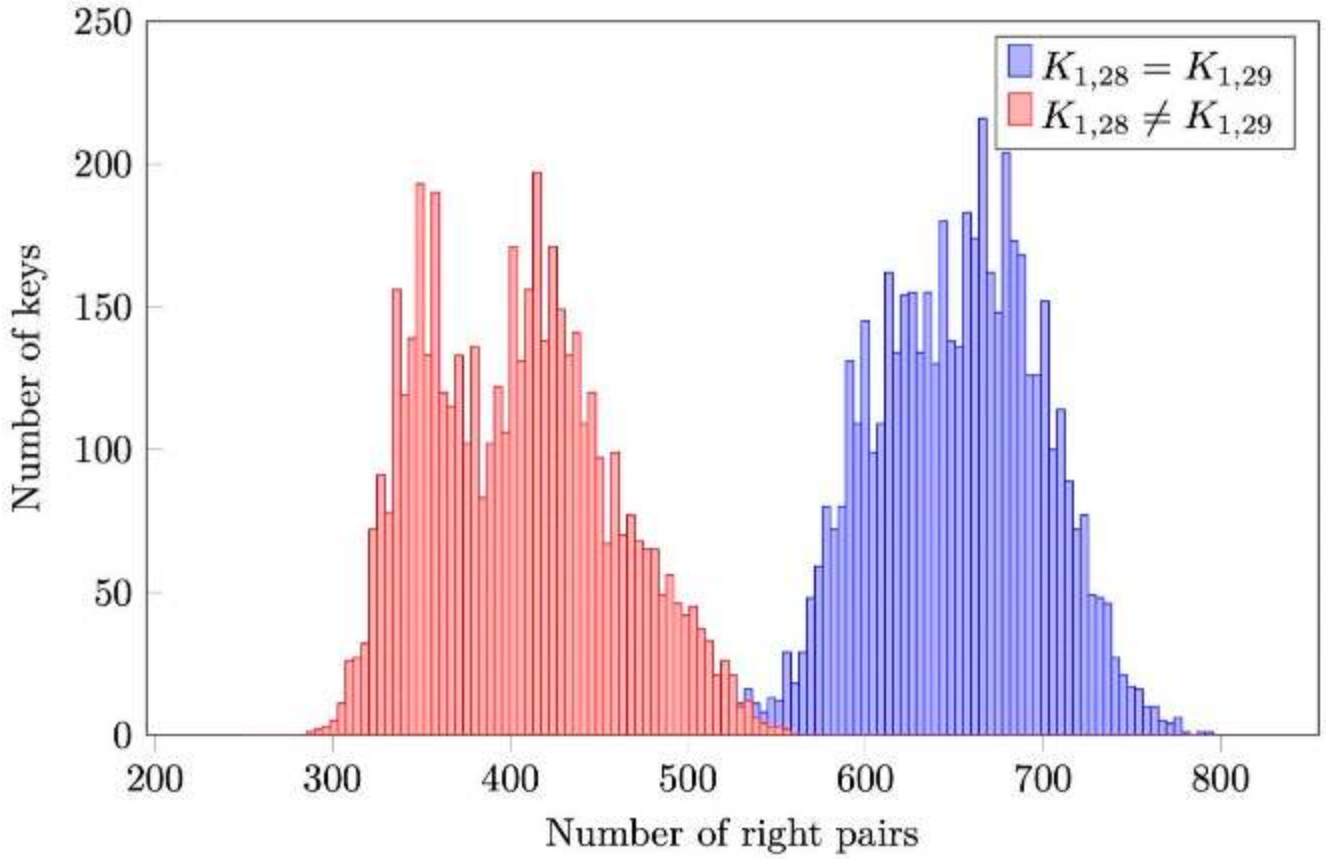
Very local effect: nonzero only in first two rounds



differences

masks

Coloring the key-dependence in the experimental results



Example 2: challenges

- Use differential transition matrices to compute accurate probabilities
  - In particular, for permutation-based designs
- Determine keys with higher-than-average probabilities
  - In particular, for hash functions

- Describe more cryptanalysis methods in this framework

Take-aways

- Competitions foster progress in cryptology
  - But organizers must ensure quality and impact

- Symmetric-key cryptology benefits from mathematics
  - To address novel requirements
  - To improve its theory of security