Cache timing attacks on recent microarchitectures

Cache timing attacks have been known for a long time, however since the rise of cloud computing and shared hardware resources, such attacks found new potentially devastating applications. One prominent example is S$A$ (presented by Irazoqui et al at S&P 2015) which is a cache timing attack against AES or similar algorithms in virtualized environments. This paper applies variants of this cache timing attack to Intel's latest generation of microprocessors. It enables a spy-process to recover cryptographic keys, interacting with the victim processes only over TCP. The threat model is a logically separated but CPU co-located attacker with root privileges. We report successful and practically verified applications of this attack against a wide range of microarchitectures, from a two-core Nehalem processor (i5-650) to two-core Haswell (i7-4600M) and four-core Skylake processors (i7-6700). The attack results in full key recovery. Compared to earlier processor generations, the attacks are more involved, but still of practical complexity, requiring between $2^{19}$ and $2^{21}$ encryptions. For the last two processors, the cache slice selection algorithm (CSSA) was not known before and had to be reverse engineered as part of this work. This is the first time CSSAs for the Skylake architecture are reported. Our attacks demonstrate that cryptographic applications in cloud computing environments using key-dependent tables for acceleration are still vulnerable even on recent architectures, including Skylake. Our reverse engineering of the CSSAs of these processors will also be beneficial for developers in many other contexts, for instance for implementing page colouring in modern operating systems.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science , Cyber Security
Authors: Andreou, A. (Ekstern), Bogdanov, A. (Intern), Tischhauser, E. W. (Intern)
Pages: 155-155
Publication date: 2017

Host publication information
Title of host publication: Proceedings of 2017 IEEE International Symposium on Hardware Oriented Security and Trust
Publisher: IEEE
ISBN (Print): 9781538639290
Series: 2017 Ieee International Symposium on Hardware Oriented Security and Trust (host)
Main Research Area: Technical/natural sciences
Conference: 2017 IEEE International Symposium on Hardware Oriented Security and Trust, McLean, United States, 01/05/2017 - 01/05/2017
Timing, Cryptography, Microarchitecture, Cloud computing, Computer architecture, Hardware, Microprocessors
DOIs: 10.1109/HST.2017.7951819
Source: FindIt
Source-ID: 2371671235
Publication: Research - peer-review › Article in proceedings – Annual report year: 2017
Efficient configurations for block ciphers with unified ENC/DEC paths

Block Ciphers providing the combined functionalities of encryption and decryption are required to operate in modes of operation like CBC and ELmD. Hence such architectures form critical building blocks for secure cryptographic implementations. Depending on the algebraic structure of a given cipher, there may be multiple ways of constructing the combined encryption/decryption circuit, each targeted at optimizing lightweight design metrics like area or power etc. In this paper we look at how the choice of circuit configuration affects the energy required to perform one encryption/decryption. We begin by analyzing 12 circuit configurations for the Advanced Encryption Standard (AES-128) cipher and establish some design rules for energy efficiency. We then extend our analysis to several lightweight block ciphers. In the second part of the paper we also investigate area optimized circuits for combined implementations of these ciphers.

Adaptable AES implementation with power-gating support

In this paper, we propose a reconfigurable design of the Advanced Encryption Standard capable of adapting at run-time to the requirements of the target application. Reconfiguration is achieved by activating only a specific subset of all the instantiated processing elements. Further, we explore the effectiveness of power gating and clock gating methodologies to minimize the energy consumption of the processing elements not involved in computation.
Atomic-AES: A compact implementation of the AES encryption/decryption core

The implementation of the AES encryption core by Moradi et al. at Eurocrypt 2011 is one of the smallest in terms of gate area. The circuit takes around 2400 gates and operates on an 8 bit datapath. However this is an encryption only core and unable to cater to block cipher modes like CBC and ELMD that require access to both the AES encryption and decryption modules. In this paper we look to investigate whether the basic circuit of Moradi et al. can be tweaked to provide dual functionality of encryption and decryption (ENC/DEC) while keeping the hardware overhead as low as possible. As a result, we report an 8-bit serialized AES circuit that provides the functionality of both encryption and decryption and occupies around 2645 GE with a latency of 226 cycles. This is a substantial improvement over the next smallest AES ENC/DEC circuit (Grain of Sand) by Feldhofer et al. which takes around 3400 gates but has a latency of over 1000 cycles for both the encryption and decryption cycles.

Exploring Energy Efficiency of Lightweight Block Ciphers

In the last few years, the field of lightweight cryptography has seen an influx in the number of block ciphers and hash functions being proposed. One of the metrics that define a good lightweight design is the energy consumed per unit operation of the algorithm. For block ciphers, this operation is the encryption of one plaintext. By studying the energy consumption model of a CMOS gate, we arrive at the conclusion that the energy consumed per cycle during the encryption operation of an r-round unrolled architecture of any block cipher is a quadratic function in r. We then apply our model to 9 well known lightweight block ciphers, and thereby try to predict the optimal value of r at which an r-round unrolled architecture for a cipher is likely to be most energy efficient. We also try to relate our results to some physical design parameters like the signal delay across a round and algorithmic parameters like the number of rounds taken to achieve full diffusion of a difference in the plaintext/key.
Fast and Memory-Efficient Key Recovery in Side-Channel Attacks

Side-channel attacks are powerful techniques to attack implementations of cryptographic algorithms by observing its physical parameters such as power consumption and electromagnetic radiation that are modulated by the secret state. Most side-channel attacks are of divide-and-conquer nature, that is, they yield a ranked list of secret key chunks, e.g., the subkey bytes in AES. The problem of the key recovery is then to find the correct combined key.

An optimal key enumeration algorithm (OKEA) was proposed by Charvillon et al. at SAC’12. Given the ranked key chunks together with their probabilities, this algorithm outputs the full combined keys in the optimal order — from more likely to less likely ones. OKEA uses plenty of memory by its nature though, which limits its practical efficiency. Especially in the cases where the side-channel traces are noisy, the memory and running time requirements to find the right key can be prohibitively high.

To tackle this problem, we propose a score-based key enumeration algorithm (SKEA). Though it is suboptimal in terms of the output order of candidate combined keys, SKEA’s memory and running time requirements are more practical than those of OKEA. We verify the advantage at the example of a DPA attack on an 8-bit embedded software implementation of AES-128. We vary the number of traces available to the adversary and report a significant increase in the success rate of the key recovery due to SKEA when compared to OKEA, within practical limitations on time and memory. We also compare SKEA to the probabilistic key enumeration algorithm (PKEA) by Meier and Staffelbach and show its practical superiority in this case.

SKEA is efficiently parallelizable. We propose a high-performance solution for the entire conquer stage of side-channel attacks that includes SKEA and the subsequent full key testing, using AES-NI on Haswell Intel CPUs.
Low-area hardware implementations of CLOC, SILC and AES-OTR
The most compact implementation of the AES-128 algorithm was the 8-bit serial circuit proposed in the work of Moradi et al. (Eurocrypt 2011). The circuit has an 8-bit datapath and occupies area equivalent to around 2400 GE. Since many authenticated encryption modes use the AES-128 algorithm as the underlying block cipher, we investigate if they can be implemented in a compact fashion using the 8-bit serialized AES circuit. In this context we investigate three authenticated encryption modes CLOC, SILC and AES-OTR. Using the standard cell library of the STM 90nm process, we implemented CLOC and SILC with around 3110 GE whereas AES-OTR was implemented with around 4720 GE.

Round Gating for Low Energy Block Ciphers
Pushed by the pervasive diffusion of devices operated by battery or by the energy harvested, energy has become one of the most important parameter to be optimized for embedded systems. Particularly relevant would be to optimize the energy consumption of security primitives.
In this paper we explore design techniques for implementing block ciphers in a low energy fashion. We concentrate on round based implementation and we discuss how gating, applied at round level can affect and improve the energy consumption of the most common lightweight block cipher currently used in the internet of things. Additionally, we discuss how to needed gating wave can be generated. Experimental results show that our technique is able to reduce the energy consumption in most block ciphers by over 60% while incurring only a minimal overhead in hardware.
Towards Practical Whitebox Cryptography: Optimizing Efficiency and Space Hardness

Whitebox cryptography aims to provide security for cryptographic algorithms in an untrusted environment where the adversary has full access to their implementation. Typical security goals for whitebox cryptography include key extraction security and decomposition security: Indeed, it should be infeasible to recover the secret key from the implementation and it should be hard to decompose the implementation by finding a more compact representation without recovering the secret key, which mitigates code lifting. Whereas all published whitebox implementations for standard cryptographic algorithms such as DES or AES are prone to practical key extraction attacks, there have been two dedicated design approaches for whitebox block ciphers: ASASA by Birykov et al. at ASIACRYPT'14 and SPACE by Bogdanov and Isobe at CCS'15. While ASASA suffers from decomposition attacks, SPACE reduces the security against key extraction and decomposition attacks in the white box to the security of a standard block cipher such as AES in the standard blackbox setting. However, due to the security-prioritized design strategy, SPACE imposes a sometimes prohibitive performance overhead in the real world as it needs many AES calls to encrypt a single block. In this paper, we address the issue by designing a family of dedicated whitebox block ciphers SPNbox and a family of underlying small block ciphers with software efficiency and constant-time execution in mind. While still relying on the standard blackbox block cipher security for the resistance against key extraction and decomposition, SPNbox attains speed-ups of up to 6.5 times in the black box and up to 18 times in the white box on Intel Skylake and ARMv8 CPUs, compared to SPACE. The designs allow for constant-time implementations in the blackbox setting and meet the practical requirements to whitebox cryptography in real-world applications such as DRM or mobile payments. Moreover, we formalize resistance towards decomposition in form of weak and strong space hardness at various security levels. We obtain bounds on space hardness in all those adversarial models. Thus, for the first time, SPNbox provides a practical whitebox block cipher that features well-understood key extraction security, rigorous analysis towards decomposition security, demonstrated real-world efficiency on various platforms and constant-time implementations. This paves the way to enhancing susceptible real-world applications with whitebox cryptography.

General information

State: Published
Organisations: Department of Applied Mathematics and Computer Science, Cyber Security, Sony Global Manufacturing & Operations Corporation
Authors: Bogdanov, A. (Intern), Isobe, T. (Ekstern), Tischhauser, E. W. (Intern)
Number of pages: 33
Pages: 126-158
Publication date: 2016

Host publication information

Title of host publication: Advances in Cryptology – ASIACRYPT 2016
Volume: 10031
Publisher: Springer
ISBN (Print): 978-3-662-53886-9

Series: Lecture Notes in Computer Science
Volume: 10031
ISSN: 0302-9743
Main Research Area: Technical/natural sciences
DOIs: 10.1007/978-3-662-53887-6_5
Source: FindIt
Source-ID: 2349670714
Publication: Research - peer-review › Article in proceedings – Annual report year: 2017

APE: Authenticated Permutation-Based Encryption for Lightweight Cryptography

The domain of lightweight cryptography focuses on cryptographic algorithms for extremely constrained devices. It is very costly to avoid nonce reuse in such environments, because this requires either a hardware source of randomness, or non-volatile memory to store a counter. At the same time, a lot of cryptographic schemes actually require the nonce assumption for their security. In this paper, we propose APE as the first permutation-based authenticated encryption scheme that is resistant against nonce misuse. We formally prove that APE is secure, based on the security of the underlying permutation. To decrypt, APE processes the ciphertext blocks in reverse order, and uses inverse permutation calls. APE therefore requires a permutation that is both efficient for forward and inverse calls. We instantiate APE with the permutations of three recent lightweight hash function designs: Quark, Photon, and Spongent. For any of these permutations, an implementation that supports both encryption and decryption requires less than 1.9 kGE and 2.8 kGE for 80-bit and 128-bit security levels, respectively.

General information

State: Published
Organisations: Department of Applied Mathematics and Computer Science, Cryptology, KU Leuven
Comb to Pipeline: Fast Software Encryption Revisited

AES-NI, or Advanced Encryption Standard New Instructions, is an extension of the x86 architecture proposed by Intel in 2008. With a pipelined implementation utilizing AES-NI, parallelizable modes such as AES-CTR become extremely efficient. However, out of the four non-trivial NIST-recommended encryption modes, three are inherently sequential: CBC, CFB, and OFB. This inhibits the advantage of using AES-NI significantly. Similar observations apply to CMAC, CCM and a great deal of other modes. We address this issue by proposing the comb scheduler – a fast scheduling algorithm based on an efficient look-ahead strategy, featuring a low overhead – with which sequential modes profit from the AES-NI pipeline in real-world settings by filling it with multiple, independent messages.

We apply the comb scheduler to implementations on Haswell, Intel's latest microarchitecture, for a wide range of modes. We observe a drastic speed-up of factor 5 for NIST's CBC, CFB, OFB and CMAC performing around 0.88 cpb. Surprisingly, contrary to the entire body of previous performance analysis, the throughput of the authenticated encryption (AE) mode CCM gets very close to that of GCM and OCB3, with about 1.64 cpb (vs. 1.63 cpb and 1.51 cpb, resp.), despite Haswell's heavily improved binary field multiplication. This suggests CCM as an AE mode of choice as it is NIST-recommended, does not have any weak-key issues like GCM, and is royalty-free as opposed to OCB3. Among the CAESAR contestants, the comb scheduler significantly speeds up CLOC/SILC, JAMBU, and POET, with the mostly sequential nonce-misuse resistant design of POET, performing at 2.14 cpb, becoming faster than the well-parallelizable COPA.

Finally, this paper provides the first optimized AES-NI implementations for the novel AE modes OTR, CLOC/SILC, COBRA, POET, McOE-G, and Julius.

General information

State: Published
Organisations: Department of Applied Mathematics and Computer Science, Cryptology
Authors: Bogdanov, A. (Intern), Lauridsen, M. M. (Intern), Tischhauser, E. W. (Intern)
Pages: 150-171
Publication date: 2015
Cryptanalysis of Two Fault Countermeasure Schemes

In this paper, we look at two fault countermeasure schemes proposed very recently in literature. The first proposed in ACISP 2015 constructs a transformation function using a cellular automata based linear diffusion, and a non-linear layer using a series of bent functions. This countermeasure is meant for the protection of block ciphers like AES. The second countermeasure was proposed in IEEE-HOST 2015 and protects the Grain-128 stream cipher. The design divides the output function used in Grain-128 into two components. The first called the masking function, masks the input bits to the output function with some additional randomness and computes the value of the function. The second called the unmasking function, is computed securely using a different register and undoes the effect of the masking with random bits. We will show that there exists a weakness in the way in which both these schemes use the internally generated random bits which make these designs vulnerable. We will outline attacks that cryptanalyze the above schemes using 66 and 512 faults respectively.

Exploring the energy consumption of lightweight blockciphers in FPGA

Internet of things and cyber-physical systems requiring security functionality has pushed for the design of a number of block ciphers and hash functions specifically developed for being implemented in resource constrained devices. Initially the optimization was mainly on area and power consumption, but, nowadays the attention is more on the energy consumption. In this paper, for the first time, we look at energy consumption of lightweight block ciphers implemented in reconfigurable devices, and we analyze the effects that round unrolling might have on the energy consumed during the encryption. Concentrating on applications that require a number of parallel encryptions, we instantiate several designs on the target FPGA and we analyze how the energy consumption varies in each algorithm when changing the amount of unrolled rounds. Our results, obtained on the Xc6slx45t device of the Spartan6 family, demonstrate that Present is the most energy efficient algorithm and that the relation between the energy consumption and the number of unrolled rounds measured on FPGA is similar to the one measured on dedicated hardware.
Twisted Polynomials and Forgery Attacks on GCM

Polynomial hashing as an instantiation of universal hashing is a widely employed method for the construction of MACs and authenticated encryption (AE) schemes, the ubiquitous GCM being a prominent example. It is also used in recent AE proposals within the CAESAR competition which aim at providing nonce misuse resistance, such as POET. The algebraic structure of polynomial hashing has given rise to security concerns: At CRYPTO 2008, Handschuh and Preneel describe key recovery attacks, and at FSE 2013, Procter and Cid provide a comprehensive framework for forgery attacks. Both approaches rely heavily on the ability to construct forgery polynomials having disjoint sets of roots, with many roots (“weak keys”) each. Constructing such polynomials beyond naïve approaches is crucial for these attacks, but still an open problem.

In this paper, we comprehensively address this issue. We propose to use twisted polynomials from Ore rings as forgery polynomials. We show how to construct sparse forgery polynomials with full control over the sets of roots. We also achieve complete and explicit disjoint coverage of the key space by these polynomials. We furthermore leverage this new construction in an improved key recovery algorithm.

As cryptanalytic applications of our twisted polynomials, we develop the first universal forgery attacks on GCM in the weak-key model that do not require nonce reuse. Moreover, we present universal weak-key forgeries for the nonce-misuse resistant AE scheme POET, which is a CAESAR candidate.
ALE: AES-based lightweight authenticated encryption

In this paper, we propose a new Authenticated Lightweight Encryption algorithm coined ALE. The basic operation of ALE is the AES round transformation and the AES-128 key schedule. ALE is an online single-pass authenticated encryption algorithm that supports optional associated data. Its security relies on using nonces. We provide an optimized low-area implementation of ALE in ASIC hardware and demonstrate that its area is about 2.5 kGE which is almost two times smaller than that of the lightweight implementations for AES-OCB and ASC-1 using the same lightweight AES engine. At the same time, it is at least 2.5 times more performant than the alternatives in their smallest implementations by requiring only about 4 AES rounds to both encrypt and authenticate a 128-bit data block for longer messages. When using the AES-NI instructions, ALE outperforms AES-GCM, AES-CCM and ASC-1 by a considerable margin, providing a throughput of 1.19 cpb close that of AES-OCB, which is a patented scheme. Its area- and time-efficiency in hardware as well as high performance in high-speed parallel software make ALE a promising all-around AEAD primitive. © 2014 Springer-Verlag.

How to Securely Release Unverified Plaintext in Authenticated Encryption

Scenarios in which authenticated encryption schemes output decrypted plaintext before successful verification raise many security issues. These situations are sometimes unavoidable in practice, such as when devices have insufficient memory to store an entire plaintext, or when a decrypted plaintext needs early processing due to real-time requirements. We introduce the first formalization of the releasing unverified plaintext (RUP) setting. To achieve privacy, we propose using plaintext awareness (PA) along with IND-CPA. An authenticated encryption scheme is PA if it has a plaintext extractor, which tries to fool adversaries by mimicking the decryption oracle, without the secret key. Releasing unverified plaintext to the attacker then becomes harmless as it is infeasible to distinguish the decryption oracle from the plaintext extractor. We introduce two notions of plaintext awareness in the symmetric-key setting, PA1 and PA2, and show that they expose a new layer of security between IND-CPA and IND-CCA. To achieve integrity, INT-CTXT in the RUP setting is required, which we refer to as INT-RUP. These new security notions are compared with conventional definitions, and are used to make a classification of symmetric-key schemes in the RUP setting. Furthermore, we re-analyze existing authenticated encryption schemes, and provide solutions to fix insecure schemes.
Key Recovery Attacks on Recent Authenticated Ciphers

In this paper, we cryptanalyze three authenticated ciphers: AVALANCHE, Calico, and RBS. While the former two are contestants in the ongoing international CAESAR competition for authenticated encryption schemes, the latter has recently been proposed for lightweight applications such as RFID systems and wireless networks. All these schemes use well-established and secure components such as the AES, Grain-like NFSRs, ChaCha and SipHash as their building blocks. However, we discover key recovery attacks for all three designs, featuring square-root complexities. Using a key collision technique, we can recover the secret key of AVALANCHE in $2^{n/2}$, where $n \in \{28; 192; 256\}$ is the key length. This technique also applies to the authentication part of Calico whose 128-bit key can be recovered in $2^{64}$ time. For RBS, we can recover its full 132-bit key in $2^{65}$ time with a guess-and-determine attack. All attacks also allow the adversary to mount universal forgeries.
Large-scale high-resolution computational validation of novel complexity models in linear cryptanalysis

Linear cryptanalysis is one of the few major attack techniques in today’s cryptography. Every new cipher comes with strong arguments against it. Still, some recent relevant ciphers such as the ISO/IEC lightweight block cipher present proved to be particularly vulnerable to linear cryptanalysis. Since most attacks published today — including the linear cryptanalysis — have complexities beyond practical reach, the evaluation of their complexities has to rely on rather theoretical computational models. The latter are often based on unproven and not always precise assumptions that might result in inexact models.

Very recently, in FSE’13, it has been demonstrated that the standard models the cryptanalysts have been relying on for a long time in linear attacks, while being quite adequate for a wide range of parameters, tend to fail when the attack to be evaluated tries to recover a high number of bits in the secret key of the cipher. However, this is actually the top-priority goal of any adversary. To amend the standard models that proved somewhat inaccurate in this crucial parameter range, a new model has been proposed based on an enhanced wrong key randomization hypothesis. However, this model has been verified only for quite small ciphers of 20-bit block size. At the same time, in the real-world applications, the block size of a cipher is usually 32 bits and higher. Thus, the experimental verification of the model remains quite limited.

In this article, we aim to bridge this gap and study this novel model for much bigger ciphers. We are able to perform its computational validation for cipher with up to 36 bits with meaningful resolution. Our work confirms that the new model of FSE’13 is significantly more accurate for a wide range of cipher parameters.
Lightweight cryptography for constrained devices

Lightweight cryptography is a rapidly evolving research field that responds to the request for security in resource constrained devices. This need arises from crucial pervasive IT applications, such as those based on RFID tags where cost and energy constraints drastically limit the solution complexity, with the consequence that traditional cryptography solutions become too costly to be implemented. In this paper, we survey design strategies and techniques suitable for implementing security primitives in constrained devices.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Cryptology, University of Lugano, Politecnico di Milano
Authors: Alippi, C. (Ekstern), Bogdanov, A. (Intern), Regazzoni, F. (Ekstern)
Pages: 144-147
Publication date: 2014

Host publication information
Title of host publication: Proceedings of the 14th International Symposium on Integrated Circuits (ISIC 2014)
Publisher: IEEE
ISBN (Print): 978-1-4799-4833-8
Main Research Area: Technical/natural sciences
Conference: 14th International Symposium on Integrated Circuits, Singapore, Singapore, 10/12/2014 - 10/12/2014
Components, Circuits, Devices and Systems, Computing and Processing, Engineered Materials, Dielectrics and Plasmas, Photonics and Electrooptics, Signal Processing and Analysis, Algorithm design and analysis, Ciphers, Encryption, Hardware, Optimization, Standards

Multidimensional zero-correlation attacks on lightweight block cipher HIGHT: Improved cryptanalysis of an ISO standard

HIGHT is a block cipher designed in Korea with the involvement of Korea Information Security Agency. It was proposed at CHES 2006 for usage in lightweight applications such as sensor networks and RFID tags. Lately, it has been adopted as ISO standard. Though there is a great deal of cryptanalytic results on HIGHT, its security evaluation against the recent zero-correlation linear attacks is still lacking. At the same time, the Feistel-type structure of HIGHT suggests that it might be susceptible to this type of cryptanalysis. In this paper, we aim to bridge this gap.

We identify zero-correlation linear approximations over 16 rounds of HIGHT. Based upon those, we attack 27-round HIGHT (round 4 to round 30) with improved time complexity and practical memory requirements. This attack of ours is the
best result on HIGHT to date in the classical single-key setting. We also provide the first attack on 26-round HIGHT (round 4 to round 29) with the full whitening key.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Cryptology, Shandong University
Authors: Wen, L. (Ekstern), Wang, M. (Ekstern), Bogdanov, A. (Intern), Chen, H. (Ekstern)
Pages: 322–330
Publication date: 2014
Main Research Area: Technical/natural sciences
On the (In)Equivalence of Impossible Differential and Zero-Correlation Distinguishers for Feistel- and Skipjack-Type Ciphers

For many word-oriented block ciphers, impossible differential (ID) and zero-correlation linear (ZC) cryptanalyses are among the most powerful attacks. Whereas ID cryptanalysis makes use of differentials which never occur, the ZC cryptanalysis relies on linear approximations with correlations equal to zero. While the key recovery parts of ID and ZC attacks may differ and are often specific to the target cipher, the underlying distinguishing properties frequently cover the same number of rounds. However, in some cases, the discrepancy between the best known IDs and ZC approximations is rather significant. At EUROCRYPT'13, a link between these two distinguishers has been presented. However, though being independent of the underlying structure of the cipher, it is usually not useful for most known ID or ZC distinguishers. So despite the relevance of those attacks, the question of their equivalence or inequivalence has not been formally addressed so far in a constructive practical way. In this paper, we aim to bridge this gap in the understanding of the links between the ID and ZC properties. We tackle this problem at the example of two wide classes of ciphers, namely, Feistel- and Skipjack-type ciphers. As our major contribution, for those ciphers, we derive conditions for impossible differentials and zero-correlation approximations to cover the same number of rounds. Using the conditions, we prove an equivalence between ID and ZC distinguishers for type-I and type-II Feistel-type ciphers, for Rule-A and Rule-B Skipjack-type ciphers, as well as for TWINE and LBlock. Moreover, we show this equivalence for the Extended Generalised Feistel construction presented at SAC'13. We also use our theoretical results to argue for an inequivalence between ID and ZC distinguishers for a range of Skipjack-type ciphers.

On the Wrong Key Randomisation and Key Equivalence Hypotheses in Matsui's Algorithm 2

This paper aims to improve the understanding of the complexities for Matsui's Algorithm 2 — one of the most well-studied and powerful cryptanalytic techniques available for block ciphers today. We start with the observation that the standard
interpretation of the wrong key randomisation hypothesis needs adjustment. We show that it systematically neglects the varying bias for wrong keys. Based on that, we propose an adjusted statistical model and derive more accurate estimates for the success probability and data complexity of linear attacks which are demonstrated to deviate from all known estimates. Our study suggests that the efficiency of Matsui’s Algorithm 2 has been previously somewhat overestimated in the cases where the adversary attempts to use a linear approximation with a low bias, to attain a high computational advantage over brute force, or both. These cases are typical since cryptanalysts always try to break as many rounds of the cipher as possible by pushing the attack to its limit. Surprisingly, our approach also reveals the fact that the success probability is not a monotonously increasing function of the data complexity, and can decrease if more data is used. Using less data can therefore result in a more powerful attack. A second assumption usually made in linear cryptanalysis is the key equivalence hypothesis, even though due to the linear hull effect, the bias can heavily depend on the key. As a further contribution of this paper, we propose a practical technique that aims to take this into account. All theoretical observations and techniques are accompanied by experiments with small-scale ciphers.

**General information**

State: Published
Organisations: Department of Applied Mathematics and Computer Science, Cryptology, Katholieke Universiteit
Authors: Bogdanov, A. (Intern), Tischhauser, E. (Ekstern)
Pages: 19-38
Publication date: 2014

**Host publication information**

Title of host publication: Fast Software Encryption. Revised Selected Papers
Publisher: Springer
ISBN (Print): 978-3-662-43932-6
ISBN (Electronic): 978-3-662-43933-3

Series: Lecture Notes in Computer Science
Volume: 8424
ISSN: 0302-9743
BFI conference series: Fast Software Encryption (5000118)
Main Research Area: Technical/natural sciences
Workshop: 20th International Workshop on Fast Software Encryption (FSE 2013), Singapore, Singapore, 10/03/2013 - 10/03/2013
Block ciphers, Linear cryptanalysis, Data complexity, Wrong key randomisation hypothesis, Key equivalence, Linear hull effect
DOIs: 10.1007/978-3-662-43933-3_2
Publication: Research - peer-review › Article in proceedings – Annual report year: 2014

**Route 66: Passively Breaking All GSM Channels**
The A5/2 stream cipher used for encryption in the GSM mobile phone standard has previously been shown to have serious weaknesses. Due to a lack of key separation and flaws in the security protocols, these vulnerabilities can also compromise the stronger GSM ciphers A5/1 and A5/3. Despite GSM's huge impact in the field, only a small selection of its channels have been analyzed. In this paper, we perform a complete practical-complexity, ciphertext-only cryptanalysis of all 66 encoded GSM channels. Moreover, we present a new passive attack which recovers the encryption key by exploiting the location updating procedure of the GSM protocol. This update is performed automatically even when the phone is not actively used. Interestingly, the attack potentially enables eavesdropping of future calls.

**General information**

State: Published
Organisations: Department of Applied Mathematics and Computer Science, Cryptology, Technical University of Denmark
Authors: Vejre, P. S. (Ekstern), Bogdanov, A. (Intern)
Pages: 422-429
Publication date: 2014

**Host publication information**

Publisher: Springer
ISBN (Print): 978-3-319-08343-8
ISBN (Electronic): 978-3-319-08344-5

Series: Lecture Notes in Computer Science
Volume: 8544
ISSN: 0302-9743
Main Research Area: Technical/natural sciences
Towards understanding the known-key security of block ciphers

Known-key distinguishers for block ciphers were proposed by Knudsen and Rijmen at ASIACRYPT 2007 and have been a major research topic in cryptanalysis since then. A formalization of known-key attacks in general is known to be difficult. In this paper, we tackle this problem for the case of block ciphers based on ideal components such as random permutations and random functions as well as propose new generic known-key attacks on generalized Feistel ciphers. We introduce the notion of known-key indifferentiability to capture the security of such block ciphers under a known key. To show its meaningfulness, we prove that the known-key attacks on block ciphers with ideal primitives to date violate security under known-key indifferentiability. On the other hand, to demonstrate its constructiveness, we prove the balanced Feistel cipher with random functions and the multiple Even-Mansour cipher with random permutations known-key indifferentiable for a sufficient number of rounds. We note that known-key indifferentiability is more quickly and tightly attained by multiple Even-Mansour which puts it forward as a construction provably secure against known-key attacks.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Cryptology, Katholieke Universiteit
Authors: Andreeva, E. (Ekstern), Bogdanov, A. (Intern), Mennink, B. (Ekstern)
Pages: 348-366
Publication date: 2014

Host publication information
Publisher: Springer
Editor: Moria, S.
ISBN (Print): 978-3-662-43932-6
ISBN (Electronic): 78-3-662-43933-3
Series: Lecture Notes in Computer Science
Volume: 8424
ISSN: 0302-9743
BFI conference series: Fast Software Encryption (5000118)
Main Research Area: Technical/natural sciences
Workshop: 20th International Workshop on Fast Software Encryption (FSE 2013), Singapore, Singapore, 10/03/2013 - 10/03/2013

Zero-correlation linear cryptanalysis with FFT and improved attacks on ISO standards Camellia and CLEFIA

Zero-correlation linear cryptanalysis is based on the linear approximations with correlation exactly zero, which essentially generalizes the integral property, and has already been applied to several block ciphers - among others, yielding best known attacks to date on round-reduced TEA and CAST-256 as published in FSE'12 and ASIACRYPT'12, respectively. In this paper, we use the FFT (Fast Fourier Transform) technique to speed up the zero-correlation cryptanalysis. First, this allows us to improve upon the state-of-the-art cryptanalysis for the ISO/IEC standard and CRYPTREC-portfolio cipher Camellia. Namely, we present zero-correlation attacks on 11-round Camellia-128 and 12-round Camellia-192 with FL/FL-1 and whitening key starting from the first round, which is an improvement in the number of attacked rounds in both cases. Moreover, we provide multidimensional zero-correlation cryptanalysis of 14-round CLEFIA-192 and 15-round CLEFIA-256 that are attacks on the highest numbers of rounds in the classical single-key setting, respectively, with improvements in memory complexity. © 2014 Springer-Verlag.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Cryptology, Shandong University, Univeriste Catholique de Louvain
Authors: Bogdanov, A. (Intern), Geng, H. (Ekstern), Wang, M. (Ekstern), Wen, L. (Ekstern), Collard, B. (Ekstern)
Efficient and side-channel resistant authenticated encryption of FPGA bitstreams

State-of-the-art solutions for FPGA bitstream protection rely on encryption and authentication of the bitstream to both ensure its confidentiality, thwarting unauthorized copying and reverse engineering, and prevent its unauthorized modification, maintaining a root of trust in the field. Adequate protection of the FPGA bitstream is of paramount importance to sustain the central functionality of dynamic reconfiguration in a hostile environment. In this work, we propose a new solution for authenticated encryption (AE) tailored for FPGA bitstream protection. It is based on the recent proposal presented at DIAC'12: the AES-based authenticated encryption scheme ALE. Our comparison to existing AES-based schemes reveals that ALE is at least twice more resource-efficient than the best AE modes of operation instantiated with AES. In the view of the recent successful side-channel attacks on Xilinx Virtex bitstream encryption, we investigate the possibility for side-channel resistant implementations of all these AES-based AE algorithms using state-of-the-art threshold masking techniques. Also in this side-channel resistant setting, the protected ALE design is about twice more resource-efficient than the best AE modes of operation with the same countermeasure. We conclude that the deployment of dedicated AE schemes such as ALE significantly facilitates the real-world efficiency and security of FPGA bitstream protection in practice: Not only our solution enables authenticated encryption for bitstream on low-cost FPGAs but it also aims to mitigate physical attacks which have been lately shown to undermine the security of the bitstream protection mechanisms in the field.
as 793 GE and 1001 GE for 80-bit and 96-bit security, respectively. This is at least two times smaller than its closest competitors Hummingbird-2 and Grain-128a. While being extremely compact, Fides is both throughput and latency efficient, even in its most serial implementations. This is attained by our novel sponge-like design approach. Moreover, cryptographically optimal 5-bit and 6-bit S-boxes are used as basic nonlinear components while paying a special attention on the simplicity of providing first order side-channel resistance with threshold implementation.

**General information**
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Cryptology, Katholieke Universiteit, NXP Semiconductors, Graz University of Technology
Authors: Bilgin, B. (Ekstern), Bogdanov, A. (Intern), Knezevic, M. (Ekstern), Mendel, F. (Ekstern), Wang, Q. (Ekstern)
Pages: 142-158
Publication date: 2013

**Host publication information**
Title of host publication: Cryptographic Hardware and Embedded Systems - CHES 2013: 15th International Workshop, Santa Barbara, CA, USA, August 20-23, 2013. Proceedings
Publisher: Springer
ISBN (Print): 978-3-642-40348-4
ISBN (Electronic): 978-3-642-40349-1
Series: Lecture Notes in Computer Science
Volume: 8086
ISSN: 0302-9743
BFI conference series: Cryptographic Hardware and Embedded Systems (5000423)
Main Research Area: Technical/natural sciences
Workshop: 15th International Workshop on Cryptographic Hardware and Embedded Systems (CHES 2013), Santa Barbara, California, United States, 20/08/2013 - 20/08/2013
Lightweight cryptography, Authenticated encryption, Keyed sponge, Glitch-free masking, APN permutation, Almost bent permutation
DOIs: 10.1007/978-3-642-40349-1_9
Source: dtu
Source-ID: n:oai:DTIC-ART:inspec/391644794::31716
Publication: Research - peer-review > Article in proceedings – Annual report year: 2013

**Generalized Feistel networks revisited**
This work deals with the classification, security and efficiency of generalized Feistel networks (GFNs) with 4 lines. We propose a definition of a GFN, essentially limiting consideration to Feistel-type constructions with domain-preserving F-functions and rotation by one line between rounds. Under this definition, we demonstrate that there are only two non-contracting representatives in the class of 4-line GFNs up to equivalence, namely, the type-I and type-II GFNs that avoid obvious differential effects. We propose to instantiate the GFNs with SPS-functions (two substitution layers separated by a permutation layer) instead of single SP-functions (one substitution-permutation layer only). We prove tight lower bounds on the number of differentially and linearly active functions and S-boxes in such ciphers. We show that the instantiation with SPS-functions using MDS diffusion provides a proportion of differentially and linearly active S-boxes by up to 33 and 50 % higher than that with single SP-functions for type-I and type-II GFNs, respectively, if the same matrix is used in all rounds. Moreover, we present the upper bounds on the differential and the linear hull probability for the type-II GFNs with SPS-functions. This opens up the possibility of designing more efficient block ciphers based on GFN structure.

**General information**
State: Published
Organisations: Sony Corporation, Katholieke Universiteit Leuven
Authors: Bogdanov, A. (Intern), Shibutani, K. (Ekstern)
Pages: 75-97
Publication date: 2013
Main Research Area: Technical/natural sciences

**Publication information**
Journal: Designs, Codes and Cryptography
Volume: 66
Issue number: 3-3
ISSN (Print): 0925-1022
Ratings: BFI (2018): BFI-level 1
Web of Science (2018): Indexed yes
Improved Impossible Differential Attacks on Large-Block Rijndael

In this paper, we present more powerful 6-round impossible differentials for large-block Rijndael-224 and Rijndael-256 than the ones used by Zhang et al. in ISC 2008. Using those, we can improve the previous impossible differential cryptanalysis of both 9-round Rijndael-224 and Rijndael-256. The improvement can lead to 10-round attack on Rijndael-256 as well. With $2^{198.1}$ chosen plaintexts, an attack is demonstrated on 9-round Rijndael-224 with $2^{195.2}$ encryptions and $2^{140.4}$ bytes memory. Increasing the data complexity to $2^{216}$ plaintexts, the time complexity can be reduced to $2^{130}$ encryptions and the memory requirements to $2^{93.6}$ bytes. For 9-round Rijndael-256, we provide an attack requiring $2^{229.3}$ chosen plaintexts, $2^{194}$ encryptions, and $2^{139.6}$ bytes memory. Alternatively, with $2^{245.3}$ plaintexts, an attack with a reduced time of $2^{217.1}$ encryptions and a memory complexity of $2^{90.9}$ bytes can be mounted. With $2^{244.2}$ chosen plaintexts, we can attack 10-round Rijndael-256 with $2^{253.9}$ encryptions and $2^{186.8}$ bytes of memory.
Parallelizable and Authenticated Online Ciphers

Online ciphers encrypt an arbitrary number of plaintext blocks and output ciphertext blocks which only depend on the preceding plaintext blocks. All online ciphers proposed so far are essentially serial, which significantly limits their performance on parallel architectures such as modern general-purpose CPUs or dedicated hardware. We propose the first parallelizable online cipher, COPE. It performs two calls to the underlying block cipher per plaintext block and is fully parallelizable in both encryption and decryption. COPE is proven secure against chosenplaintext attacks assuming the underlying block cipher is a strong PRP. We then extend COPE to create COPA, the first parallelizable, online authenticated cipher with nonce-misuse resistance. COPA only requires two extra block cipher calls to provide integrity. The privacy and integrity of the scheme is proven secure assuming the underlying block cipher is a strong PRP. Our implementation with Intel AES-NI on a Sandy Bridge CPU architecture shows that both COPE and COPA are about 5 times faster than their closest competition: TC1, TC3, and McOE-G. This high factor of advantage emphasizes the paramount role of parallelizability on up-to-date computing platforms.
SPONGENT: The Design Space of Lightweight Cryptographic Hashing
The design of secure yet efficiently implementable cryptographic algorithms is a fundamental problem of cryptography. Lately, lightweight cryptography—optimizing the algorithms to fit the most constrained environments—has received a great deal of attention, the recent research being mainly focused on building block ciphers. As opposed to that, the design of lightweight hash functions is still far from being well investigated with only few proposals in the public domain. In this paper, we aim to address this gap by exploring the design space of lightweight hash functions based on the sponge construction instantiated with present-type permutations. The resulting family of hash functions is called spongent. We propose 13 spongent variants—or different levels of collision and (second) preimage resistance as well as for various implementation constraints. For each of them, we provide several ASIC hardware implementations—ranging from the lowest area to the highest throughput. We make efforts to address the fairness of comparison with other designs in the field by providing an exhaustive hardware evaluation on various technologies, including an open core library. We also prove essential differential properties of spongent permutations, give a security analysis in terms of collision and preimage resistance, as well as study in detail dedicated linear distinguishers.
Beyond the Limits of DPA: Combined Side-Channel Collision Attacks

The problem of extracting the highest possible amount of key-related information using the lowest possible number of measurements is one of the central questions in side-channel attacks against embedded implementations of cryptographic algorithms. To address it, this work proposes a novel framework enhancing side-channel collision attacks with divide-and-conquer attacks such as differential power analysis (DPA). An information-theoretical metric is introduced for the evaluation of collision detection efficiency. Improved methods of dimension reduction for side-channel traces are developed based on a statistical model of euclidean distance. Experimental results confirm that DPA-combined collision attacks are superior to both DPA-only and collision-only attacks. The new methods of dimension reduction lead to further complexity improvements. All attacks are treated for the case of AES-128 and are practically validated on a widespread 8-bit RISC microcontroller.
Efficient reconfigurable hardware architecture for accurately computing success probability and data complexity of linear attacks

An accurate estimation of the success probability and data complexity of linear cryptanalysis is a fundamental question in symmetric cryptography. In this paper, we propose an efficient reconfigurable hardware architecture to compute the success probability and data complexity of Matsui's Algorithm 2 which is the central technique in linear cryptanalysis for block ciphers. Using this dedicated architecture, we are able to investigate the complexity of the algorithm for up to 40-bit block ciphers for low-correlation linear approximations and high advantages. Performing experiments on larger block lengths ensures that any empirical observations are not due to differences in statistical behavior for artificially small block lengths. Rather surprisingly, we observed in previous experiments a significant deviation between the theory and practice for Matsui's Algorithm 2 for larger block sizes in a vast range of parameters. The new hardware architecture allows us to verify the existing theoretical models for the complexity estimation in linear cryptanalysis. The designed hardware architecture is realized on two Xilinx Virtex-6 XC6VLX240T FPGAs for smaller block lengths, and on RIVYERA platform with 128 Xilinx Spartan-3 XC3S5000 FPGAs for larger block lengths.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Cryptology, Ruhr-University Bochum, Katholische Universität
Authors: Bogdanov, A. (Intern), Kavun, E. B. (Ekstern), Tischhauser, E. (Ekstern), Yalcin, T. (Ekstern)
Publication date: 2012
Integral and Multidimensional Linear Distinguishers with Correlation Zero

Zero-correlation cryptanalysis uses linear approximations holding with probability exactly 1/2. In this paper, we reveal fundamental links of zero-correlation distinguishers to integral distinguishers and multidimensional linear distinguishers. We show that an integral implies zero-correlation linear approximations and that a zero-correlation linear distinguisher is actually a special case of multidimensional linear distinguishers. These observations provide new insight into zero-correlation cryptanalysis which is illustrated by attacking a Skipjack variant and round-reduced CAST-256 without weak key assumptions. © International Association for Cryptologic Research 2012.

Key-Altering Ciphers in a Provable Setting: Encryption Using a Small Number of Public Permutations (Extended Abstract)

This paper considers—for the first time—the concept of key-altering ciphers in a provable security setting. Key-altering ciphers can be seen as a generalization of a construction proposed by Even and Mansour in 1991. This construction builds a block cipher PX from an n-bit permutation P and two n-bit keys k0 and k1, setting PXk0,k1(x)=k1⊕P(x⊕k0) . Here we consider a (natural) extension of the Even-Mansour construction with t permutations P1,...,Pt and t+1 keys, k0,...,kt . We demonstrate in a formal model that such a cipher is secure in the sense that an attacker needs to make at least 22n/3 queries to the underlying permutations to be able to distinguish the construction from random. We argue further that the bound is tight for t=2 but there is a gap in the bounds for t>2, which is left as an open and interesting problem. Additionally, in terms of statistical attacks, we show that the distribution of Fourier coefficients for the cipher over all keys is close to ideal. Lastly, we define a practical instance of the construction with t=2 using AES referred to as AES2. Any attack on AES2 with complexity below 285 will have to make use of AES with a fixed known key in a non-black box manner. However, we conjecture its security is 2128.
On security arguments of the second round SHA-3 candidates

In 2007, the US National Institute for Standards and Technology (NIST) announced a call for the design of a new cryptographic hash algorithm in response to vulnerabilities like differential attacks identified in existing hash functions, such as MD5 and SHA-1. NIST received many submissions, 51 of which got accepted to the first round. 14 candidates were left in the second round, out of which five candidates have been recently chosen for the final round.

An important criterion in the selection process is the SHA-3 hash function security. We identify two important classes of security arguments for the new designs: (1) the possible reductions of the hash function security to the security of its underlying building blocks and (2) arguments against differential attack on building blocks. In this paper, we compare the state of the art provable security reductions for the second round candidates and review arguments and bounds against classes of differential attacks. We discuss all the SHA-3 candidates at a high functional level, analyze, and summarize the security reduction results and bounds against differential attacks. Additionally, we generalize the well-known proof of collision resistance preservation, such that all SHA-3 candidates with a suffix-free padding are covered.
SHA-3 competition, Hash functions, Classification, Security reductions, Differential attacks

DOI: 10.1007/s10207-012-0156-7
Source: dtu
Source-ID: n::oai:DTIC-ART:swets/361567489::19490
Publication: Research - peer-review > Journal article – Annual report year: 2012

The 11 papers presented were carefully reviewed and selected from 61 submissions. The papers are organized in topical sections on symmetric-key algorithms and cryptanalysis, cryptographic implementations, side channel analysis and countermeasures, fault tolerance of cryptosystems, physically unclonable functions, public-key schemes and cryptanalysis, analysis and design of security protocol, security of systems and applications, high-performance computing in cryptology and cryptography in ubiquitous devices.

General information
State: Published
Organisations: Department of Mathematics, Discrete mathematics, IIIT Delhi
Authors: Bogdanov, A. (ed.) (Intern), Sanadhya, S. (ed.) (Ekstern)
Number of pages: 185
Publication date: 2012

Publication information
Publisher: Springer
ISBN (Electronic): 978-3-642-34416-9
Original language: English

Series: Lecture Notes in Computer Science
Volume: 7644
ISSN: 0302-9743
Main Research Area: Technical/natural sciences
authentication, fault attack, key generation, power analysis attacks, side channel attacks

Links:
Source: dtu
Source-ID: n::oai:DTIC-ART:inspec/373690576::25394
The provable constructive effect of diffusion switching mechanism in CLEFIA-type block ciphers

CLEFIA is a block cipher designed by Sony Corporation, adopted as a lightweight encryption algorithm of the new ISO/IEC 29192-2 standard, and proposed as a Japanese e-Government recommendation cipher CRYPTREC candidate. Provable security properties of cryptographic design are crucial in any security evaluation. Providing lower bounds on the number of active S-boxes in differential and linear characteristics has been one of the few important provable properties that can be formally shown for block ciphers and hence received a lot of attention. In this work, we prove tighter lower bounds on the number of linearly active S-boxes in CLEFIA-type generalized Feistel networks (GFNs) with diffusion switching mechanism (DSM). We show that every 6 rounds of such GFNs provide 50% more linearly active S-boxes than proven previously. Moreover, we experimentally demonstrate that the new bound is tight for up to at least 12 rounds, whereas the previous one is not. Thus, this paper delivers first provable evidence that diffusion switching mechanism actually provides an advantage by guaranteeing more active S-boxes in GFNs.

General information
State: Published
Organisations: Shanghai Jiao Tong University, Katholieke Universiteit
Authors: Wang, Q. (Ekstern), Bogdanov, A. (Intern)
Pages: 427-432
Publication date: 2012
Main Research Area: Technical/natural sciences

Publication information
Journal: Information Processing Letters
Volume: 112
Issue number: 11
ISSN (Print): 0020-0190
Ratings:
BFI (2018): BFI-level 2
Web of Science (2018): Indexed yes
BFI (2017): BFI-level 2
Web of Science (2017): Indexed Yes
BFI (2016): BFI-level 2
Scopus rating (2016): SJR 0.57 SNIP 0.967 CiteScore 1.02
BFI (2015): BFI-level 2
Scopus rating (2015): SJR 0.602 SNIP 1.167 CiteScore 0.93
BFI (2014): BFI-level 2
Scopus rating (2014): SJR 0.593 SNIP 0.934 CiteScore 0.94
Web of Science (2014): Indexed yes
BFI (2013): BFI-level 2
Scopus rating (2013): SJR 0.609 SNIP 1.047 CiteScore 0.95
ISI indexed (2013): ISI indexed yes
Web of Science (2013): Indexed yes
BFI (2012): BFI-level 2
Scopus rating (2012): SJR 0.603 SNIP 1.037 CiteScore 0.92
ISI indexed (2012): ISI indexed yes
Web of Science (2012): Indexed yes
BFI (2011): BFI-level 2
Scopus rating (2011): SJR 0.612 SNIP 0.929 CiteScore 0.85
ISI indexed (2011): ISI indexed yes
Web of Science (2011): Indexed yes
BFI (2010): BFI-level 2
Scopus rating (2010): SJR 0.625 SNIP 1.016
Web of Science (2010): Indexed yes
BFI (2009): BFI-level 2
Scopus rating (2009): SJR 0.708 SNIP 1.062
BFI (2008): BFI-level 1
Scopus rating (2008): SJR 0.837 SNIP 1.161
Zero correlation linear cryptanalysis with reduced data complexity

Zero correlation linear cryptanalysis is a novel key recovery technique for block ciphers proposed in [5]. It is based on linear approximations with probability of exactly 1/2 (which corresponds to the zero correlation). Some block ciphers turn out to have multiple linear approximations with correlation zero for each key over a considerable number of rounds. Zero correlation linear cryptanalysis is the counterpart of impossible differential cryptanalysis in the domain of linear cryptanalysis, though having many technical distinctions and sometimes resulting in stronger attacks. In this paper, we propose a statistical technique to significantly reduce the data complexity using the high number of zero correlation linear approximations available. We also identify zero correlation linear approximations for 14 and 15 rounds of TEA and XTEA. Those result in key-recovery attacks for 21-round TEA and 25-round XTEA, while requiring less data than the full code book. In the single secret key setting, these are structural attacks breaking the highest number of rounds for both ciphers. The findings of this paper demonstrate that the prohibitive data complexity requirements are not inherent in the zero correlation linear cryptanalysis and can be overcome. Moreover, our results suggest that zero correlation linear cryptanalysis can actually break more rounds than the best known impossible differential cryptanalysis does for relevant block ciphers. This might make a security re-evaluation of some ciphers necessary in the view of the new attack. © 2012 Springer-Verlag.
A 3-Subset Meet-in-the-Middle Attack: Cryptanalysis of the Lightweight Block Cipher KTANTAN

In this paper we describe a variant of existing meet-in-the-middle attacks on block ciphers. As an application, we propose meet-in-the-middle attacks that are applicable to the KTANTAN family of block ciphers accepting a key of 80 bits. The attacks are due to sonic weaknesses in its bitwise key schedule. We report an attack of time complexity $2^{75.170}$ encryptions on the full KTANTAN32 cipher with only 3 plaintext/ciphertext pairs and well as $2^{75.044}$ encryptions on the full KTANTAN48 and $2^{75.584}$ encryptions on the full KTANTAN69 with 2 plaintext/ciphertext pairs. All these attacks work in the classical attack model without any related keys. In the differential related-key model, we demonstrate 218- and 174-round differentials holding with probability $1$. This shows that a strong related-key property can translate to a successful attack in the non-related-key setting. Having extremely low data requirements, these attacks are valid even in RFID-like environments where only a very limited amount of text material may be available to an attacker.

General information
State: Published
Organisations: Department of Mathematics, Discrete mathematics
Authors: Bogdanov, A. (Intern), Rechberger, C. (Intern)
Pages: 229-240
Publication date: 2011
Workshop: 17th International Workshop on Selected Areas in Cryptography, Waterloo, Canada, 12/08/2010 - 12/08/2010
Main Research Area: Technical/natural sciences

Publication information
Journal: Lecture Notes in Computer Science
Volume: 6544
ISSN (Print): 0302-9743
Ratings:
BFI (2018): BFI-level 1
Web of Science (2018): Indexed yes
BFI (2017): BFI-level 1
BFI (2016): BFI-level 1
Scopus rating (2016): CiteScore 0.67 SJR 0.315 SNIP 0.552
Web of Science (2016): Indexed yes
BFI (2015): BFI-level 1
Scopus rating (2015): SJR 0.328 SNIP 0.618 CiteScore 0.37
BFI (2014): BFI-level 1
Scopus rating (2014): SJR 0.325 SNIP 0.678 CiteScore 0.42
BFI (2013): BFI-level 1
Scopus rating (2013): SJR 0.329 SNIP 0.699 CiteScore 0.49
ISI indexed (2013): ISI indexed no
Web of Science (2013): Indexed yes
BFI (2012): BFI-level 1
Scopus rating (2012): SJR 0.323 SNIP 0.708 CiteScore 0.49
ISI indexed (2012): ISI indexed no
Web of Science (2012): Indexed yes
BFI (2011): BFI-level 1
Scopus rating (2011): SJR 0.325 SNIP 0.721 CiteScore 0.49
ISI indexed (2011): ISI indexed no
BFI (2010): BFI-level 1
Scopus rating (2010): SJR 0.314 SNIP 0.634
Web of Science (2010): Indexed yes
BFI (2009): BFI-level 1
Scopus rating (2009): SJR 0.305 SNIP 0.548
Web of Science (2009): Indexed yes
BFI (2008): BFI-level 1
Scopus rating (2008): SJR 0.281 SNIP 0.447
Scopus rating (2007): SJR 0.294 SNIP 0.494
Web of Science (2007): Indexed yes
Analysis of 3-line generalized Feistel networks with double SD-functions

Generalized Feistel networks (GFN) are broadly employed in the design of primitives for block ciphers, stream ciphers, and hash functions. Lately, endowing the functions of GFNs with the structure of nonlinear substitution followed by linear diffusion (substitution–diffusion, SD) has received a great deal of attention. In this contribution, we prove tight lower bounds on the number of differentially and linearly active S-boxes for 3-line GFNs with double SD-functions where two SD-structures are applied one after another. We also show 8-round impossible differentials for 3-line GFNs with bijective functions. Moreover, we demonstrate that the proportion of active S-boxes in all S-boxes for such GFNs is by up to 14% higher than that for 4-line GFNs with double SD-functions, when instantiated with MDS matrices. This indicates that, rather surprisingly, the 3-line GFNs can be more efficient in practice than those with 4 lines.
Since Rijndael was chosen as the Advanced Encryption Standard (AES), improving upon 7-round attacks on the 128-bit key variant (out of 10 rounds) or upon 8-round attacks on the 192/256-bit key variants (out of 12/14 rounds) has been one of the most difficult challenges in the cryptanalysis of block ciphers for more than a decade. In this paper, we present the novel technique of block cipher cryptanalysis with bicliques, which leads to the following results: The first key recovery method for the full AES-128 with computational complexity $2^{126.1}$. The first key recovery method for the full AES-192 with computational complexity $2^{189.7}$. The first key recovery method for the full AES-256 with computational complexity $2^{254.4}$. Key recovery methods with lower complexity for the reduced-round versions of AES not considered before, including cryptanalysis of 8-round AES-128 with complexity $2^{124.9}$. Preimage search for compression functions based on the full AES versions faster than brute force. In contrast to most shortcut attacks on AES variants, we do not need to assume related-keys. Most of our techniques only need a very small part of the codebook and have low memory requirements, and are practically verified to a large extent. As our cryptanalysis is of high computational complexity, it does not threaten the practical use of AES in any way. © 2011 International Association for Cryptologic Research.
Double SP-Functions: Enhanced Generalized Feistel Networks: Extended Abstract
This work deals with the security and efficiency of type-I and type-II generalized Feistel networks (GFNs) with 4 lines. We propose to instantiate the GFNs with double SP-functions (substitution-permutation layer followed by another substitution-permutation layer) instead of single SP-functions (one substitution-permutation layer). We provide tight lower bounds on the number of differentially and linearly active functions and S-boxes in such ciphers. Based on these bounds, we show that the instantiation with double SP-functions using MDS diffusion has a proportion of differentially and linearly active S-boxes by up to 33% and 50% higher than that with single SP-functions for type-I and type-II GFNs, respectively. This opens up the possibility of designing more efficient block ciphers based on GFN structure. Note that type-I and type-II GFNs are the only non-contracting OFNs with 4 lines under a reasonable definition of a GFN.

General information
State: Published
Organisations: Universite Catholique de Louvain, Sony Corporation
Authors: Bogdanov, A. (Intern), Shibutani, K. (Ekstern)
Pages: 106-119
Publication date: 2011

Host publication information
Title of host publication: Information Security and Privacy. Proceedings
Publisher: Springer
ISBN (Print): 978-3-642-22496-6
ISBN (Electronic): 978-3-642-22497-3
Series: Lecture Notes in Computer Science
Volume: 6812
ISSN: 0302-9743
Main Research Area: Technical/natural sciences
Conference: 16th Australasian Conference on Information Security and Privacy, ACISP 2011, Melbourne, Australia, 01/01/2011
Source: dtu
Source-ID: n::oai:DTIC-ART:isi/364857217::25838
Publication: Research - peer-review › Article in proceedings – Annual report year: 2011

Spongent: A lightweight hash function
This paper proposes spongent - a family of lightweight hash functions with hash sizes of 88 (for preimage resistance only), 128, 160, 224, and 256 bits based on a sponge construction instantiated with a present-type permutation, following the hermetic sponge strategy. Its smallest implementations in ASIC require 738, 1060, 1329, 1728, and 1950 GE, respectively. To our best knowledge, at all security levels attained, it is the hash function with the smallest footprint in hardware published so far, the parameter being highly technology dependent. spongent offers a lot of flexibility in terms of serialization degree and speed. We explore some of its numerous implementation trade-offs. We furthermore present a security analysis of spongent. Basing the design on a present-type primitive provides confidence in its security with respect to the most important attacks. Several dedicated attack approaches are also investigated. © 2011 International Association for Cryptologic Research.

General information
State: Published
Organisations: Discrete mathematics, Department of Mathematics, NXP Semiconductors, Katholieke Universiteit
Authors: Bogdanov, A. (Intern), Knežević, M. (Ekstern), Leander, G. (Intern), Toz, D. (Ekstern), Varici, K. (Ekstern), Verbauwhede, I. (Ekstern)
Pages: 312-325
Publication date: 2011

Host publication information
Title of host publication: Cryptographic hardware and embedded systems - CHES 2011. Proceedings
Volume: 6917
Publisher: Springer
ISBN (Print): 9783642239502
Series: Lecture Notes in Computer Science
Volume: 6917
ISSN: 0302-9743
Main Research Area: Technical/natural sciences
Differential Cache-Collision Timing Attacks on AES with Applications to Embedded CPUs

This paper proposes a new type of cache-collision timing attacks on software implementations of AES. Our major technique is of differential nature and is based on the internal cryptographic properties of AES, namely, on the MDS property of the linear code providing the diffusion matrix used in the MixColumns transform. It is a chosen-plaintext attack where pairs of AES executions are treated differentially. The method can be easily converted into a chosen-ciphertext attack. We also thoroughly study the physical behavior of cache memory enabling this attack. On the practical side, we demonstrate that our theoretical findings lead to efficient real-world attacks on embedded systems implementing AES at the example of ARM9. As this is one of the most wide-spread embedded platforms today [7], our experimental results might make a revision of the practical security of many embedded applications with security functionality necessary. To our best knowledge, this is the first paper to study cache timing attacks on embedded systems. © 2010 Springer-Verlag.

On the differential and linear efficiency of balanced Feistel networks

Balanced Feistel networks (BFN) have been widely used for constructing efficient block ciphers. They are known to provide high efficiency with respect to differential and linear cryptanalysis, when instantiated with SL-type round functions (BFN–SL). This work suggests that BFNs attain higher efficiency when the round function is defined as a composition of two substitution layers connected by a linear diffusion layer (SLS-type round function). The resulting structure is called BFN–SLS. Tight upper bounds on the differential and linear trail probabilities are proven for such constructions. When compared to BFN–SL with single-round diffusion, BFN–SLS exhibits an increase by almost 1/3 in the proportion of active S-boxes. When compared to BFN–SL with multiple-round diffusion, BFN–SLS provides the same proportion of active S-boxes, requiring, however, twice less linear operations and a single diffusion matrix for all rounds. It is argued that the cost of linear operations cannot be ignored when dealing with efficiency. Different BFNs are compared under consideration of the relative complexity of linear and nonlinear finite field operations. As a result, since BFN–SLS minimizes the number of necessary linear operations, its efficiency is higher than that of the known BFN–SL constructions.
Algebraic methods in side-channel collision attacks and practical collision detection

This paper presents algebraic collision attacks, a new powerful cryptanalytic method based on side-channel leakage which allows for low measurement counts needed for a successful key recovery in case of AES. As opposed to many other side-channel attacks, these techniques are essentially based on the internal structure of the attacked cryptographic algorithm, namely, on the algebraic properties of AES. Moreover, we derived the probability distributions of Euclidean distance for collisions and non-collisions. On this basis, a statistical framework for finding the instances of side-channel traces leaking most key information in collision attacks is proposed. Additionally to these theoretical findings, the paper also contains a practical evaluation of these side-channel collision attacks for a real-world microcontroller platform similar to many smart card ICs. To our best knowledge, this is the first real-world study of collision attacks based on generalized internal collisions. We also combined our methods with ternary voting [1] which is a recent multiple-differential collision detection technique using profiling, where neither plaintexts, ciphertexts nor keys have to be known in the profiling stage. © 2008 Springer Berlin Heidelberg.

Fast Multivariate Signature Generation in Hardware: The Case of Rainbow

This paper deals with the design of an area-time efficient hardware architecture for the multivariate signature scheme, Rainbow. As a part of this architecture, a high-performance hardware optimized variant of the well-known Gaussian elimination over GF(2^l) and its efficient implementation is presented. Besides solving LSEs, the architecture is also reused for the linear transformation operations of the scheme, thereby saving on area. The resulting signature generation core of Rainbow requires 63,593 gate equivalents and signs a message in just 804 clock cycles. A comparison of our architecture with implementations of the RSA, the ECDSA and the en-TTS scheme shows that Rainbow in hardware provides significant performance improvements.
Hash functions and RFID tags: Mind the gap

The security challenges posed by RFID-tag deployments are well-known. In response there is a rich literature on new cryptographic protocols and an on-tag hash function is often assumed by protocol designers. Yet cheap tags pose severe implementation challenges and it is far from clear that a suitable hash function even exists. In this paper we consider the options available, including constructions based around compact block ciphers. While we describe the most compact hash functions available today, our work serves to highlight the difficulties in designing lightweight hash functions and (echoing [17]) we urge caution when routinely appealing to a hash function in an RFID-tag protocol. © 2008 Springer-Verlag Berlin Heidelberg.

Linear slide attacks on the KeeLoq block cipher

KeeLoq is a block cipher used in numerous widespread passive entry and remote keyless entry systems as well as ill various component identification applications. The KeeLoq algorithm has a 64-bit key and operates on 32-bit blocks. It is based oil all NLFSR with a nonlinear feedback function of 5 variables. In this paper new key recovery attacks on KeeLoq are proposed. The first one has a complexity of about $2^{50.6}$ KeeLoq encryptions. The second attack finds the key in $2^{37}$ encryptions and works for the whole key space. In our attacks we use the techniques of guess-and-determine, slide, and linear attacks as well as cycle structure analysis. Both attacks need $2^{32}$ known plaintext-ciphertext pairs. We also analyze the KeeLoq key management and authentication protocols applied in rolling-code and IFF access systems widely used in real-world applications. We demonstrate several practical vulnerabilities.
Multiple-Differential Side-Channel Collision Attacks on AES

In this paper, two efficient multiple-differential methods to detect collisions in the presence of strong noise are proposed - binary and ternary voting. After collisions have been detected, the cryptographic key can be recovered from these collisions using such recent cryptanalytic techniques as linear [1] and algebraic [2] collision attacks. We refer to this combination of the collision detection methods and cryptanalytic techniques as multiple-differential collision attacks (MDCA). When applied to AES, MDCA using binary voting without profiling requires about 2.7 to 13.2 times less traces than the Hamming-weight based CPA for the same implementation. MDCA on AES using ternary voting with profiling and linear key recovery clearly outperforms CPA by requiring only about 6 online measurements for the range of noise amplitudes where CPA requires from 163 to 6912 measurements. These attacks do not need the S-box to be known. Moreover, neither key nor plaintexts have to be known to the attacker in the profiling stage.

Periodic Ciphers with Small Blocks and Cryptanalysis of KeeLoq

KeeLoq is a lightweight block cipher that is massively used in the automobile industry [12, 13, 31, 32]. KeeLoq has two remarkable properties: it is periodic and has a very short block size (32 bits). Many different attacks on KeeLoq have been published in recent years [8, 15, 9, 10, 5]. In this paper we study a unique way of attacking KeeLoq, in which the periodic property of KeeLoq is used to distinguish 512 rounds of KeeLoq from a random permutation. Our attacks require the knowledge of the entire code-book and are not among the fastest attacks known on this cipher. However one of them works for 100 % of all keys, including so called "strong keys", see [15]. In general, it is important to show how many different attacks are possible on a weak cipher such as KeeLoq.
Time-area optimized public-key engines: MQ-cryptosystems as replacement for elliptic curves?
In this paper ways to efficiently implement public-key schemes based on ultrivariate quadratic polynomials (MQ-schemes for short) are investigated. In particular, they are claimed to resist quantum computer attacks. It is shown that such schemes can have a much better time-area product than elliptic curve cryptosystems. For instance, an optimised FPGA implementation of amended TTS is estimated to be over 50 times more efficient with respect to this parameter. Moreover, a general framework for implementing small-field MQ-schemes in hardware is proposed which includes a systolic architecture performing Gaussian elimination over composite binary fields. © 2008 Springer-Verlag Berlin Heidelberg.