Improved meet-in-the-middle attacks on reduced-round Piccolo

Piccolo is a lightweight block cipher that adopts a generalized Feistel network structure with 4 branches, each of which is 16 bit long. The key length is 80 or 128 bit, denoted by Piccolo-80 and Piccolo-128, respectively. In this paper, we mounted meet-in-the-middle attacks on 14-round Piccolo-80 without preand post-whitening keys and 18-round Piccolo-128 with post-whitening keys by exploiting the properties of the key schedule and Maximum Distance Separable (MDS) matrix. For Piccolo-80, we first constructed a 5-round distinguisher. Then 4 rounds and 5 rounds were appended at the beginning and at the end, respectively. Based on this structure, we mounted an attack on 14-round Piccolo-80 from the 5th round to the 18th round. The data, time, and memory complexities were $2^{52}$ chosen plaintexts, $2^{67.44}$ encryptions, and $2^{64.91}$ blocks, respectively. For Piccolo-128, we built a 7-round distinguisher to attack 18-round Piccolo-128 from the 4th round to the 21st round. The data, time, and memory complexities were $2^{52}$ chosen plaintexts, $2^{126.63}$ encryptions, and $2^{125.29}$ blocks, respectively. If not considering results on biclique cryptanalysis, these are currently the best public results on this reduced version of the Piccolo block cipher.
A Bayesian inference-based detection mechanism to defend medical smartphone networks against insider attacks

With the increasing digitization of the healthcare industry, a wide range of devices (including traditionally non-networked medical devices) are Internet- and inter-connected. Mobile devices (e.g. smartphones) are one common device used in the healthcare industry to improve the quality of service and experience for both patients and healthcare workers, and the underlying network architecture to support such devices is also referred to as medical smartphone networks (MSNs). MSNs, similar to other networks, are subject to a wide range of attacks (e.g. leakage of sensitive patient information by a malicious insider). In this work, we focus on MSNs and present a compact but efficient trust-based approach using Bayesian inference to identify malicious nodes in such an environment. We then demonstrate the effectiveness of our approach in detecting malicious nodes by evaluating the deployment of our proposed approach in a real-world environment with two healthcare organizations.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Cyber Security, City University of Hong Kong, Deakin University, University of Texas at San Antonio
Authors: Meng, W. (Intern), Li, W. (Ekstern), Xiang, Y. (Ekstern), Choo, K. K. R. (Ekstern)
Pages: 162-169
Publication date: 2017
Main Research Area: Technical/natural sciences

Publication information
Journal: Journal of Network and Computer Applications
Volume: 78
ISSN (Print): 1084-8045
Ratings:
BFI (2018): BFI-level 1
Web of Science (2018): Indexed yes
BFI (2017): BFI-level 1
Web of Science (2017): Indexed yes
BFI (2016): BFI-level 1
Scopus rating (2016): SJR 0.807 SNIP 2.509 CiteScore 4.42
BFI (2015): BFI-level 1
Scopus rating (2015): SJR 0.831 SNIP 2.817 CiteScore 3.98
BFI (2014): BFI-level 1
Scopus rating (2014): SJR 0.936 SNIP 3.08 CiteScore 3.82
BFI (2013): BFI-level 1
Scopus rating (2013): SJR 0.757 SNIP 2.859 CiteScore 3.21
BFI (2012): BFI-level 1
Scopus rating (2012): SJR 0.59 SNIP 2.14 CiteScore 2.48
BFI (2011): BFI-level 1
Scopus rating (2011): SJR 0.463 SNIP 1.896 CiteScore 1.97
BFI (2010): BFI-level 1
Scopus rating (2010): SJR 0.41 SNIP 1.083
BFI (2009): BFI-level 1
Scopus rating (2009): SJR 0.441 SNIP 1.595
A brief comparison of Simon and Simeck

SIMON is a new lightweight block cipher design based on combining the design principles of the SIMON and Speck block cipher. While the design allows a smaller and more efficient hardware implementation, its security margins are not well understood. The lack of design rationals of its predecessors further leaves some uncertainty on the security of SIMON. In this work we give a short analysis of the impact of the design changes by comparing the upper bounds on the probability of differential and linear trails with SIMON. We also give a comparison of the effort of finding those bounds, which surprisingly is significantly lower for SIMECK while covering a larger number of rounds at the same time. Furthermore, we provide new differentials for SIMECK which can cover more rounds compared to previous results on SIMON and study how to choose good differentials for attacks and show that one can find better differentials by building them from a larger set of trail with initially lower probability. We also provide experimental results for the differentials for SIMON32 and SIMECK32 which show that there exist keys for which the probability of the differential is significantly higher than expected. Based on this we mount key recovery attacks on 19/26/33 rounds of SIMECK32/48/64, which also give insights on the reduced key guessing effort due to the different set of rotation constants.
A Pilot Study of Multiple Password Interference Between Text and Map-Based Passwords

Today's computer users have to remember several passwords for each of their accounts. It is easily noticed that people may have difficulty in remembering multiple passwords, which result in a weak password selection. Previous studies have shown that recall success rates are not statistically dissimilar between textual passwords and graphical passwords. With the advent of map-based graphical passwords, this paper focuses on multiple password interference and presents a pilot study consisting of 60 participants to study the recall of multiple passwords between text passwords and map-based passwords under various account scenarios. Each participant has to create six distinct passwords for different account scenarios. It is found that participants in the map-based graphical password scheme could perform better than the textual password scheme in both short-term (one-hour session) and long term (after two weeks) password memorability tests (i.e., they made higher success rates). Our effort attempts to complement existing studies and stimulate more research on this issue.

General information

State: Published
Organisations: Department of Applied Mathematics and Computer Science, Cyber Security, Singapore University of Technology and Design, City University of Hong Kong, Institute for Infocomm Research
Pages: 145-162
Publication date: 2017
A Privacy-Preserving Framework for Collaborative Intrusion Detection Networks Through Fog Computing

Nowadays, cyber threats (e.g., intrusions) are distributed across various networks with the dispersed networking resources. Intrusion detection systems (IDSs) have already become an essential solution to defend against a large amount of attacks. With the development of cloud computing, a modern IDS is able to implement more complicated detection algorithms by offloading the expensive operations such as the process of signature matching to the cloud (i.e., utilizing computing resources from the cloud). However, during the detection process, no party wants to disclose their own data especially sensitive information to others for privacy concerns, even to the cloud side. For this sake, privacy-preserving technology has been applied to IDSs, while it still lacks of proper solutions for a collaborative intrusion detection network (CIDN) due to geographical distribution. A CIDN enables a set of dispersed IDS nodes to exchange required information. With the advent of fog computing, in this paper, we propose a privacy-preserving framework for collaborative networks based on fog devices. Our study shows that the proposed framework can help reduce the workload on cloud’s side.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science , Cyber Security, Guangzhou University, City University of Hong Kong, Technical University of Denmark
Authors: Wang, Y. (Ekstern), Xie, L. (Ekstern), Li, W. (Ekstern), Meng, W. (Intern), Li, J. (Ekstern)
Pages: 267-279
Publication date: 2017
Involvement of numerous stakeholders in cloud-based systems’ design and usage with varying degrees of nonfunctional requirements makes Architecturally Significant Requirements (ASRs) identification and management a challenge undertaking. The aim of the research presented in this chapter is to identify different types of design-time and run-time ASRs of the cloud-based systems, provide an ASRs classification scheme and present a framework to manage the requirements’ variability during life cycle of the cloud-based systems. We have used a multifaceted research approach to address the ASRs identification, classification, and change management challenges. We have explored findings from systematic as well as structured reviews of the literature on quality requirements of the cloud-based systems including but not limited to security, availability, scalability, privacy, and multi-tenancy. We have presented a framework for requirements classification and change management focusing on distributed Platform as a Service (PaaS) and Software as a Service (SaaS) systems as well as complex software ecosystems that are built using PaaS and SaaS, such as Tools as a Service (TaaS). We have demonstrated applicability of the framework on a selected set of the requirements for the cloud-based systems. The results of the research presented in this chapter show that key quality requirements of the cloud-based systems, for example, multi-tenancy and security, have a significant impact on how other quality requirements (such as scalability, reliability, and interoperability) are handled in the overall architecture design of a cloud-based system. It is important to distinguish tenant-specific run-time architecturally significant quality requirements and corresponding cloud-based systems’ components so that run-time status of the tenant-specific architecture quality requirements can be monitored and system configurations can be adjusted accordingly. For the systems that can be used by multiple tenants, the requirements change management framework should consider if the addition or modification (triggered by a specific tenant) of a quality requirement can impact quality requirements of other tenants, and whether or not a trade-off point should be introduced in the architecture (corresponding to the requirements). The trade-off point can also be referred as a variability point, that is, a compromise has to be made among the number of quality requirements and only some of the requirements can be satisfied. System analysts and software architects can use the proposed taxonomy and the management framework for identifying relevant quality requirements for multi-tenant cloud-based systems, for analyzing impact of changes in the requirements on the overall system architecture, and for managing variability of the architecturally significant requirements.

**General information**

**State:** Published  
**Organisations:** Department of Applied Mathematics and Computer Science, Cyber Security  
**Authors:** Chauhan, M. A. (Intern), Probst, C. W. (Intern)  
**Pages:** 181-205  
**Publication date:** 2017

**Host publication information**

**Title of host publication:** Requirements Engineering for Service and Cloud Computing  
**Publisher:** Springer  
**ISBN (Print):** 9783319513096  
**Chapter:** 8  
**Series:** Requirements Engineering for Service and Cloud Computing  
**Main Research Area:** Technical/natural sciences  
**Computer Science, Computer Communication Networks, Software Engineering, Business Process Management, Cloud computing, Platform as a service (PaaS), Software as a service (SaaS), Architecturally significant requirements (ARSS), Requirements classification, Requirements change management, Architecture quality

**DOIs:**

10.1007/978-3-319-51310-2_8  
**Source:** FindIt  
**Source-ID:** 2372098636  
**Publication: Research - peer-review › Book chapter – Annual report year:** 2017

**Authentication for E-Government in Developing Countries - With special focus on the North Africa Countries**

Recently, many countries include both developed countries as well as developing countries have transformed paper based systems into electronic systems using ICT technologies in order to improve service delivery and reduce cost. Several researches and International Organizations in the field of e-Government reports that many countries over the world have not achieved transaction stages of government e-services and most of those countries are from developing countries. One of the main issues challenge government e-service inclusion is digital divide which barriers achieving principle of equal access and benefit of government e-service. Therefore, This thesis aims to investigate digital divide and IDM issues challenge government e-service inclusion in developing countries such as North Africa Countries (NAC) from achieving the principle of equal access in a secure manner. To achieve this aim we, developed a framework that consists of two components include digital divide variables and a simple IDM model in order to assess the current state of government e-service in NAC. Moreover, we analyzed the existing IDM protocol’s concept to understand whether those concepts consider disadvantaged user’s needs. Based on the identified challenges in NAC using the developed framework and the analysis of IDM protocol’s concept we identify the requirements to be satisfied in order to allow large portion of citizens access and benefit of government e-service in equal and secure manner. One possible solution to improve e-Government inclusion is to consider vulnerable group needs such as the case in which users (citizens) do not have the ability either to read or write and as a result are excluded from e-services. Thus, a solution should enable such users to benefit from e-
services. Introducing vulnerable group such as illiterate individuals might introduce new risks which have not existed in citizens-government face to face interaction. Thus, considering security property include confidentiality, integrity, non-repudiation and accountability for a proposed solution is needed. User authentication based on social relationship protocol is proposed in order to bridge digital divide. We formalized the proposed protocol as well as IDM protocol's concept using Open Source Fixed Point Model Checker tool (OFMC) To verify security properties include secrecy of exchanged information and authenticity of communication parties of the target protocols. OFMC is an automatic protocol security verification tool to identify the strengths of the verified protocol. Based on the verification result of OFMC tool, an attack is found against the existing IDM protocol's concept when considering vulnerable users while the proposed protocol has achieved the specified goals without an attack at least in one session. We also, performed a simple usability comparison between the proposed protocol and public kiosk service delivery channel and the proposed protocol shows its effectiveness as well as efficient.

General information
State: Submitted
Organisations: Cyber Security, Department of Applied Mathematics and Computer Science
Authors: Elaswad, O. (Intern), Jensen, C. D. (Intern)
Number of pages: 130
Publication date: 2017

Publication information
Publisher: DTU Compute
Original language: English
Series: DTU Compute PHD-2017
Volume: 455
ISSN: 0909-3192
Main Research Area: Technical/natural sciences

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 219 and 221 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
Design and analysis of cryptographic algorithms

In today's world computers are ubiquitous. They can be found in virtually any industry and most households own at least one personal computer or have a mobile phone. Apart from these fairly large and complex devices, we also see computers on a much smaller scale appear in everyday objects in the form of micro-controllers and RFID chips.

What truly transformed our society are large scale networks, like the Internet or mobile telephone networks, which can link billions of devices. Our ways of communicating and conducting business have severely changed over the last decades due to this development. However, most of this communication happens over inherently insecure channels requiring methods to protect our communication. A further issue is the vast amount of data generated, which raises serious privacy concerns.

Cryptography provides the key components for protecting our communication. From securing our passwords and personal data to protecting mobile communication from eavesdroppers and our electronic bank transactions from manipulation. These applications would be impossible without cryptography.

The main topic of this thesis is the design and security analysis of the most fundamental algorithms used in cryptography, namely block ciphers and cryptographic hash functions. These algorithms are the building blocks for a vast amount of applications and play a vital role in providing both confidentiality and integrity for our communication.

This work is organized in two parts. First, an introduction to block ciphers and cryptographic hash functions is given to provide an overview over the state-of-the-art, the terminology, and how we can evaluate the security of an algorithm. The second part is a collection of scientific publications that have been written during the PhD studies and published.

In the first publication we analyze the security of cryptographic hash functions based on the AES and demonstrate practical attacks on reduced-round versions of these algorithms. The second publication provides cryptanalysis of the lightweight block cipher SIMON in particular how resistant the type of block ciphers are against differential and linear cryptanalysis. In the fourth publication we present a short-input hash function utilizing AES-specific instructions on modern CPUs in order to improve the performance of hashbased signature schemes. The last publication deals with the design of the tweakable lightweight block cipher Skinny which provides strong security bounds against differential and linear attacks while also competing with the performance of SIMON.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Cyber Security
Authors: Kölbl, S. (Intern), Rechberger, C. (Intern), Knudsen, L. R. (Intern)
Number of pages: 272
Publication date: 2017

Publication information
Place of publication: Kgs. Lyngby
Publisher: Technical University of Denmark (DTU)
Original language: English
Series: DTU Compute PHD-2016
Number: 434
ISSN: 0909-3192
Main Research Area: Technical/natural sciences
Electronic versions: 
phd434_Koelbl_S.pdf

Relations
Projects:
Design and analysis of cryptographic algorithms
Publication: Research › Ph.D. thesis – Annual report year: 2017

Detecting Malicious Nodes in Medical Smartphone Networks Through Euclidean Distance-Based Behavioral Profiling
With the increasing digitization of the healthcare industry, a wide range of medical devices are Internet- and inter-connected. Mobile devices (e.g., smartphones) are one common facility used in the healthcare industry to improve the
quality of service and experience for both patients and healthcare personnel. The underlying network architecture to support such devices is also referred to as medical smartphone networks (MSNs). Similar to other networks, MSNs also suffer from various attacks like insider attacks (e.g., leakage of sensitive patient information by a malicious insider). In this work, we focus on MSNs and design a trust-based intrusion detection approach through Euclidean distance-based behavioral profiling to detect malicious devices (or called nodes). In the evaluation, we collaborate with healthcare organizations and implement our approach in a real simulated MSN environment. Experimental results demonstrate that our approach is promising in effectively identifying malicious MSN nodes.

Developing advanced fingerprint attacks on challenge-based collaborative intrusion detection networks

Traditionally, an isolated intrusion detection system (IDS) is vulnerable to various types of attacks. In order to enhance IDS performance, collaborative intrusion detection networks (CIDNs) are developed through enabling a set of IDS nodes to communicate with each other. Due to the distributed network architecture, insider attacks are one of the major threats. In the literature, challenge-based trust mechanisms have been built to identify malicious nodes by evaluating the satisfaction levels between challenges and responses. However, such mechanisms rely on two major assumptions, which may result in a weak threat model. In this case, CIDNs may be still vulnerable to advanced insider attacks in real-world deployment. In this paper, we propose a novel collusion attack, called passive message fingerprint attack (PMFA), which can collect messages and identify normal requests in a passive way. In the evaluation, we explore the attack performance under both simulated and real network environments. Experimental results demonstrate that our attack can help malicious nodes send malicious responses to normal requests, while maintaining their trust values.
Do we educate engineers that can engineer?

Since 2008, the Bachelor of Engineering education at the Technical University of Denmark has been CDIO-based, including the software technology and IT and economics study lines. Consequently, the study plans of these study lines were revised to include cross-disciplinary CDIO projects in each of the first four semesters. These projects replaced 11 smaller, course-specific projects in the old study plans. The first three semesters contain design-build projects spanning several courses, and the fourth semester centers around a stand-alone CDIO project. These team-based projects aim at training the students’ engineering skills (CDIO competence category 4) and at improving the students’ skills in CDIO competence categories 2 and 3. In the tenth year of operation, we now decided to investigate, how content students and employers are with our students’ engineering skills. To this end we have designed a survey to provide us with insights for improving our study lines and to address the question: “Are we educating engineers who can engineer?” The questionnaire is aligned with the CDIO syllabus and can also serve for surveying other study lines, since it is not study line specific. To obtain meaningful results, we decided to target students who have at least passed the first four terms, and companies that have hosted a significant number of students in the last 3 years in internships or for the final thesis. These companies interact with the students for almost one year at the end of their studies, providing a good foundation for the company supervisors to answer questions about the students’ abilities as an engineer. In this paper, we discuss the design and result of the questionnaire, and the obtained results. As mentioned above, the survey will give us and the CDIO community detailed insights as to how our students and their employers experience the result of our education.

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.
Enhancing collaborative intrusion detection networks against insider attacks using supervised intrusion sensitivity-based trust management model

To defend against complex attacks, collaborative intrusion detection networks (CIDNs) have been developed to enhance the detection accuracy, which enable an IDS to collect information and learn experience from others. However, this kind of networks is vulnerable to malicious nodes which are utilized by insider attacks (e.g., betrayal attacks). In our previous research, we developed a notion of intrusion sensitivity and identified that it can help improve the detection of insider attacks, whereas it is still a challenge for these nodes to automatically assign the values. In this article, we therefore aim to design an intrusion sensitivity-based trust management model that allows each IDS to evaluate the trustworthiness of others by considering their detection sensitivities, and further develop a supervised approach, which employs machine learning techniques to automatically assign the values of intrusion sensitivity based on expert knowledge. In the evaluation, we compare the performance of three different supervised classifiers in assigning sensitivity values and investigate our trust model under different attack scenarios and in a real wireless sensor network. Experimental results indicate that our trust model can enhance the detection accuracy of malicious nodes and achieve better performance as compared with similar models.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Cyber Security, City University of Hong Kong
Authors: Li, W. (Ekstern), Meng, W. (Intern), Kwok, L. (Ekstern), IP, H. H. (Ekstern)
Number of pages: 11
Pages: 135-145
Publication date: 2017
Main Research Area: Technical/natural sciences

Publication information
Journal: Journal of Network and Computer Applications
Volume: 77
ISSN (Print): 1084-8045
Ratings:
BFI (2018): BFI-level 1
Web of Science (2018): Indexed yes
BFI (2017): BFI-level 1
Web of Science (2017): Indexed yes
BFI (2016): BFI-level 1
Scopus rating (2016): SJR 0.807 SNIP 2.509 CiteScore 4.42
BFI (2015): BFI-level 1
Scopus rating (2015): SJR 0.831 SNIP 2.817 CiteScore 3.98
BFI (2014): BFI-level 1
Scopus rating (2014): SJR 0.936 SNIP 3.08 CiteScore 3.82
BFI (2013): BFI-level 1
Enhancing Trust Management for Wireless Intrusion Detection via Traffic Sampling in the Era of Big Data

Internet of Things (IoT) has been widely used in our daily life, which enables various objects to be interconnected for data exchange, including physical devices, vehicles, and other items embedded with network connectivity. Wireless sensor network (WSN) is a vital application of IoT, providing many kinds of information among sensors, whereas such network is vulnerable to a wide range of attacks, especially insider attacks, due to its natural environment and inherent unreliable transmission. To safeguard its security, intrusion detection systems (IDSs) are widely adopted in a WSN to defend against insider attacks through implementing proper trust-based mechanisms. However, in the era of big data, sensors may generate excessive information and data, which could degrade the effectiveness of trust computation. In this paper, we focus on this challenge and propose a way of combining Bayesian-based trust management with traffic sampling for wireless intrusion detection under a hierarchical structure. In the evaluation, we investigate the performance of our approach in both a simulated and a real network environment. Experimental results demonstrate that packet-based trust management would become ineffective in a heavy traffic environment, and that our approach can help lighten the burden of IDSs in handling traffic while maintaining the detection of insider attacks.

General information
State: Accepted/In press
Organisations: Department of Applied Mathematics and Computer Science, Cyber Security, Technical University of Denmark, University of Aizu, Singapore University of Technology and Design, University of New Brunswick
Authors: Meng, W. (Intern), Li, W. (Ekstern), Su, C. (Ekstern), Zhou, J. (Ekstern), Lu, R. (Ekstern)
Number of pages: 10
Publication date: 2017
Main Research Area: Technical/natural sciences

Publication information
Journal: IEEE Access
ISSN (Print): 2169-3536
Ratings:
Web of Science (2018): Indexed yes
Scopus rating (2016): CiteScore 5.13
Scopus rating (2015): CiteScore 4.32
Exploring Effect of Location Number on Map-Based Graphical Password Authentication

Graphical passwords (GPs) that authenticate users using images are considered as one potential alternative to overcome the issues of traditional textual passwords. Based on the idea of utilizing an extremely large image, map-based GPs like PassMap and GeoPass have been developed, where users can select their secrets (geographical points) on a world map. In particular, PassMap allows users to select two locations on a map, while GeoPass reduces the number of locations to only one. At first glance, selecting one location is more vulnerable to attacks, while increasing the location number may add burden on users. In the literature, there is no research exploring this issue. Motivated by this, our purpose in this work is to explore the effect of location number (the number of geographical points) and compare two schemes of PassMap and GeoPass in terms of users' performance and feedback. In this work, we develop a generic and open platform for realizing map-based schemes, and conduct a user study with 60 participants. The study reveals that selecting two locations would not degrade the scheme performance. Our effort aims to complement exiting research studies in this area.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Cyber Security, Institute for Infocomm Research, Hong Kong Polytechnic University, University of Luxembourg
Authors: Meng, W. (Intern), Lee, W. (Ekstern), Au, M. H. (Ekstern), Liu, Z. (Ekstern)
Pages: 301-313
Publication date: 2017
From Higher-Order Differentials to Polytopic Cryptanalysis

Polytopic cryptanalysis was introduced at EUROCRYPT 2016 as a cryptanalytic technique for low-data-complexity attacks on block ciphers. In this paper, we give an account of how the technique was developed, quickly go over the basic ideas and techniques of polytopic cryptanalysis, look into how the technique differs from previously existing cryptographic techniques, and discuss whether the attack angle can be useful for developing improved cryptanalytic techniques.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Cyber Security
Authors: Tiessen, T. (Intern)
Pages: 544-552
Publication date: 2017

Harvesting Smartphone Privacy Through Enhanced Juice Filming Charging Attacks

The increasingly high demand for smartphone charging in people’s daily lives has apparently encouraged much more public charging stations to be deployed in various places (e.g., shopping malls, airports). However, these public charging facilities may open a hole for cyber-criminals to infer private information and data from smartphone users. Juice filming charging (JFC) attack is a particular type of charging attacks, which is capable of stealing users’ sensitive information from both Android OS and iOS devices, through automatically monitoring and recording phone screen during the whole
charging period. The rationale is that phone screen can be leaked through a standard micro USB connector, which adopts the Mobile High-Definition Link (MHL) standard. In practice, we identify that how to efficiently extract information from the captured videos remains a challenge for current JFC attack. To further investigate its practical influence, in this work, we focus on enhancing its performance in the aspects of extracting texts from images and correlating information, and then conducting a user study in a practical scenario. The obtained results demonstrate that our enhanced JFC attack can outperform the original one in collecting users’ information at large and extracting sensitive data with a higher accuracy. Our work aims to complement existing results and stimulate more efforts in defending smartphones against charging threats.

**JFCGuard: Detecting juice filming charging attack via processor usage analysis on smartphones**

Smartphones have become necessities in people’s lives, so that many more public charging stations are under deployment worldwide to meet the increasing demand of phone charging (i.e., in airports, subways, shops, etc). However, this situation may expose a hole for cyber-criminals to launch various attacks especially charging attacks and threaten user’s privacy. As an example, juice filming charging (JFC) attack is able to steal users’ sensitive and private information from both Android OS and iOS devices, through automatically recording phone-screen and monitoring users’ inputs during the whole charging period. More importantly, this attack does not need any permission or installing any pieces of apps on user’s side. The rationale is that users’ information can be leaked through a standard micro USB connector that employs the Mobile High-Definition Link (MHL) standard. Motivated by the potential damage of JFC attack, in this work, we investigate the impact of JFC attack on processor usage including both CPU- and GPU-usage. It is found that JFC attack would cause a noticeable usage increase when connecting the phone to the JFC charger. Then, we design a security mechanism, called JFCGuard, to detect JFC attack based on processor usage analysis for smartphone users. In the evaluation, we perform a user study with over 250 participants and the results demonstrate that JFCGuard can identify JFC attack in an effective way. Our work aims to complement existing research results and stimulate more research in this area.
Charging Threat, Mobile Security, Smartphone Privacy, Android and iOS Device, Juice Filming Charging, Attack, Detection Mechanism

Modeling and Verification of Insider Threats Using Logical Analysis

In this paper, we combine formal modeling and analysis of infrastructures of organizations with sociological explanation to provide a framework for insider threat analysis. We use the higher order logic (HOL) proof assistant Isabelle/HOL to support this framework. In the formal model, we exhibit and use a common trick from the formal verification of security protocols, showing that it is applicable to insider threats. We introduce briefly a three-step process of social explanation, illustrating that it can be applied fruitfully to the characterization of insider threats. We introduce the insider theory constructed in Isabelle that implements this process of social explanation. To validate that the social explanation is generally useful for the analysis of insider threats and to demonstrate our framework, we model and verify the insider threat patterns of entitled independent and Ambitious Leader in our Isabelle/HOL framework.
Reflection ciphers
This paper investigates ciphers where the set of encryption functions is identical to the set of decryption functions, which we call reflection ciphers. Equivalently, there exists a permutation $P$, named the coupling permutation, such that decryption under $k$ corresponds to encryption under $P(k)$. We study the necessary properties for this coupling permutation. Special care has to be taken of some related-key distinguishers since, in the context of reflection ciphers, they may provide attacks in the single-key setting. We then derive some criteria for constructing secure reflection ciphers and analyze the security properties of different families of coupling permutations. Finally, we concentrate on the case of reflection block ciphers and, as an illustration, we provide concrete examples of key schedules corresponding to several coupling permutations, which lead to new variants of the block cipher PRINCE.
SOOA: Exploring Special On-Off Attacks on Challenge-Based Collaborative Intrusion Detection Networks

The development of collaborative intrusion detection networks (CIDNs) aims to enhance the performance of a single intrusion detection system (IDS), through communicating and collecting information from other IDS nodes. To defend CIDNs against insider attacks, trust-based mechanisms are crucial for evaluating the trustworthiness of a node. In the literature, challenge-based trust mechanisms are well established to identify malicious nodes by identifying the deviation between challenges and responses. However, such mechanisms rely on two major assumptions, which may result in a weak threat model and render CIDNs still vulnerable to advanced insider attacks in a practical deployment. In this paper, our motivation is to investigate the effect of On-Off attacks on challenge-based CIDNs. In particular, as a study, we explore a special On-Off attack (called SOOA), which can keep responding normally to one node while acting abnormally to another node. In the evaluation, we explore the attack performance under simulated CIDN environments. Experimental results indicate that our attack can interfere the effectiveness of trust computation for CIDN nodes.

Towards effective and robust list-based packet filter for signature-based network intrusion detection: an engineering approach

Network intrusion detection systems (NIDSs) which aim to identify various attacks, have become an essential part of current security infrastructure. In particular, signature-based NIDSs are being widely implemented in industry due to their low rate of false alarms. However, the signature matching process is a big challenge for these systems, in which the cost is at least linear to the size of an input string. As a result, overhead packets will be a major issue for practical usage, where the incoming packets exceed the maximum capability of an intrusion detection system (IDS). To mitigate this problem, packet filtration is a promising solution to reduce unwanted traffic. Motivated by this, in this work, a list-based packet filter was designed and an engineering method of combining both blacklist and whitelist techniques was introduced. To further secure such filters against IP spoofing attacks, a lightweight but efficient IP verification mechanism was developed. In the evaluation, a list-based packet filter was deployed in both simulated and real network environments under honest and dishonest scenarios. Experimental results demonstrate that the developed list-based packet filter is effective in traffic filtration as well as workload reduction, and is robust against IP spoofing attacks.
Towards Effective Trust-Based Packet Filtering in Collaborative Network Environments

Overhead network packets are a big challenge for intrusion detection systems (IDSs), which may increase system burden, degrade system performance, and even cause the whole system collapse, when the number of incoming packets exceeds the maximum handling capability. To address this issue, packet filtration is considered as a promising solution, and our previous research efforts have proven that designing a trust-based packet filter was able to refine unwanted network packets and reduce the workload of a local IDS. With the development of Internet cooperation, collaborative intrusion detection environments (e.g., CIDNs) have been developed, which allow IDS nodes to collect information and learn experience from others. However, it would not be effective for the previously built trust-based packet filter to work in such a collaborative environment, since the process of trust computation can be easily compromised by insider attacks. In this paper, we adopt the existing CIDN framework and aim to apply a collaborative trust-based approach to reduce unwanted packets. More specifically, we develop a collaborative trust-based packet filter, which can be deployed in collaborative networks and be robust against typical insider attacks (e.g., betrayal attacks). Experimental results in various simulated and practical environments demonstrate that our filter can perform effectively in reducing unwanted traffic and can defend against insider attacks through identifying malicious nodes in a quick manner, as compared to similar approaches.
Towards enhancing click-draw based graphical passwords using multi-touch behaviours on smartphones

Graphical passwords (GPs) are recognised as one of the potential alternatives in addressing the limitations in conventional text-based password authentication. With the rapid development of mobile devices (i.e., the increase of computing power), GP-based systems have already been implemented not only on PCs, but also on smartphones to authenticate legitimate users and detect impostors. However, as compared to common computers, we identify that users are able to perform some distinct actions like multi-touch on smartphones. The multi-touch is a distinguished feature on current smartphones and its impact on graphical password creation is an important topic in the literature. In this paper, our interest is to investigate the influence of multi-touch behaviours on users' habit in creating graphical passwords, especially on click-draw based GPs (shortly CD-GPS) on mobile devices. In the evaluation, we develop a multi-touch enabled CD-GPS on smartphones and conduct two major experiments with a total of 90 participants. The study results indicate that participants are more likely to use multi-touch features to create their secrets, and multi-touch can make a positive impact on creating graphical passwords (i.e., offering higher success rates and less time consumption).

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Cyber Security, City University of Hong Kong, University of Texas at San Antonio
Authors: Meng, W. (Intern), Li, W. (Ekstern), Kwok, L. F. (Ekstern), Choo, K. K. R. (Ekstern)
Pages: 213-229
Publication date: 2017
Main Research Area: Technical/natural sciences

Publication information
Journal: Computers & Security
Volume: 65
ISSN (Print): 0167-4048
Ratings:
BFI (2018): BFI-level 1
Web of Science (2018): Indexed yes
BFI (2017): BFI-level 1
Web of Science (2017): Indexed yes
BFI (2016): BFI-level 1
Scopus rating (2016): CiteScore 3.59 SJR 0.866 SNIP 2.217
BFI (2015): BFI-level 1
Scopus rating (2015): SJR 0.828 SNIP 2.437 CiteScore 3.03
BFI (2014): BFI-level 1
Scopus rating (2014): SJR 0.66 SNIP 2.283 CiteScore 2.39
BFI (2013): BFI-level 1
Scopus rating (2013): SJR 0.741 SNIP 2.744 CiteScore 2.48
ISI indexed (2013): ISI indexed yes
BFI (2012): BFI-level 1
Scopus rating (2012): SJR 0.75 SNIP 2.581 CiteScore 2.56
ISI indexed (2012): ISI indexed yes
Towards Statistical Trust Computation for Medical Smartphone Networks Based on Behavioral Profiling

Due to the popularity of mobile devices, medical smartphone networks (MSNs) have been evolved, which become an emerging network architecture in healthcare domain to improve the quality of service. There is no debate among security experts that the security of Internet-enabled medical devices is woefully inadequate. Although MSNs are mostly internally used, they still can leak sensitive information under insider attacks. In this case, there is a need to evaluate a node’s trustworthiness in MSNs based on the network characteristics. In this paper, we focus on MSNs and propose a statistical trust-based intrusion detection mechanism to detect malicious nodes in terms of behavioral profiling (e.g., camera usage, visited websites, etc.). Experimental results indicate that our proposed mechanism is feasible and promising in detecting malicious nodes under medical environments.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Cyber Security, Hong Kong Polytechnic University
Authors: Meng, W. (Intern), Au, M. H. (Ekstern)
Pages: 152–159
Publication date: 2017

Host publication information
Title of host publication: IFIPTM 2017: Trust Management XI
Publisher: Springer

Series: IFIP Advances in Information and Communication Technology
Volume: 505
ISSN: 1868-4238
Main Research Area: Technical/natural sciences
Conference: 11th IFIP WG 11.11 International Conference on Trust Management, Gothenburg, Sweden, 12/06/2017 - 12/06/2017
Emerging network, Medical smartphone network, Intrusion detection, Insider attack, Statistical trust computation
DOIs:
10.1007/978-3-319-59171-1_12
Source: PublicationPreSubmission
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.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Cyber Security, University of Cagliari, ALaRI - USI, University of Sassari
Authors: Banik, S. (Intern), Bogdanov, A. (Intern), Fanni, T. (Ekstern), Sau, C. (Ekstern), Raffo, L. (Ekstern), Palumbo, F. (Ekstern), Regazzoni, F. (Ekstern)
Pages: 331-334
Publication date: 2016

Host publication information
Title of host publication: Proceedings of the ACM International Conference on Computing Frontiers (CF '16)
Publisher: Association for Computing Machinery
ISBN (Print): 978-1-4503-4128-8
BFI conference series: Computing Frontiers (5010518)
Main Research Area: Technical/natural sciences
Conference: ACM International Conference on Computing Frontiers (CF 2016), Como, Italy, 16/05/2016 - 16/05/2016
DOIs: 10.1145/2903150.2903488
Source: FindIt
Source-ID: 2306998280
Publication: Research - peer-review › Article in proceedings – Annual report year: 2016

A MAC Mode for Lightweight Block Ciphers

Lightweight cryptography strives to protect communication in constrained environments without sacrificing security. However, security often conflicts with efficiency, shown by the fact that many new lightweight block cipher designs have block sizes as low as 64 or 32 bits. Such low block sizes lead to impractical limits on how much data a mode of operation can process per key. MAC (message authentication code) modes of operation frequently have bounds which degrade with both the number of messages queried and the message length. We present a MAC mode of operation, LightMAC, where the message length has no effect on the security bound, allowing an order of magnitude more data to be processed per key. Furthermore, LightMAC is incredibly simple, has almost no overhead over the block cipher, and is parallelizable. As a result, LightMAC not only offers compact authentication for resource-constrained platforms, but also allows high-performance parallel implementations. We highlight this in a comprehensive implementation study, instantiating LightMAC with PRESENT and the AES. Moreover, LightMAC allows flexible trade-offs between rate and maximum message length. Unlike PMAC and its many derivatives, LightMAC is not covered by patents. Altogether, this makes it a promising authentication primitive for a wide range of platforms and use cases.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Cyber Security, KU Leuven, NTT Corporation
Authors: Luykx, A. (Ekstern), Preneel, B. (Ekstern), Tischhauser, E. W. (Intern), Yasuda, K. (Ekstern)
Pages: 43-59
Publication date: 2016

Host publication information
Title of host publication: Revised Selected Papers of the 23rd International Conference on Fast Software Encryption (FSE 2016)
Publisher: Springer
ISBN (Print): 978-3-662-52992-8
Series: Lecture Notes in Computer Science
Volume: 9783
ISSN: 0302-9743
BFI conference series: Fast Software Encryption (5000118)
Main Research Area: Technical/natural sciences
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 ELMID 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.

General information
State: Published
Organisations: Cryptology, Department of Applied Mathematics and Computer Science, Nanyang Technological University, University of Lugano
Authors: Banik, S. (Ekstern), Bogdanov, A. (Intern), Regazzoni, F. (Ekstern)
Pages: 173-190
Publication date: 2016

Building indifferentiable compression functions from the PGV compression functions
Preneel, Govaerts and Vandewalle (PGV) analysed the security of single-block-length block cipher based compression functions assuming that the underlying block cipher has no weaknesses. They showed that 12 out of 64 possible compression functions are collision and (second) preimage resistant. Black, Rogaway and Shrimpton formally proved this result in the ideal cipher model. However, in the indifferentiability security framework introduced by Maurer, Renner and Holenstein, all these 12 schemes are easily differentiable from a fixed input-length random oracle (FIL-RO) even when their underlying block cipher is ideal. We address the problem of building indifferentiable compression functions from the PGV compression functions. We consider a general form of 64 PGV compression functions and replace the linear feed-forward operation in this generic PGV compression function with an ideal block cipher independent of the one used in the generic PGV construction. This modified construction is called a generic modified PGV (MPGV). We analyse indifferentiability of the generic MPGV construction in the ideal cipher model and show that 12 out of 64 MPGV compression functions in this framework are indifferentiable from a FIL-RO. To our knowledge, this is the first result showing that two independent block ciphers are sufficient to design indifferentiable single-block-length compression functions.

General information
Compression function, Generic MPGV, Generic PGV, Hash function, Indifferentiability
Conditional differential cryptanalysis of 105 round Grain v1
In this paper we propose conditional differential cryptanalysis of 105 round Grain v1. This improves the attack proposed on 97 round Grain v1 by Knellwolf et al at Asiacrypt 2010. We take the help of the tool $\Delta$Grain $K_{SA}$ to track the differential trails introduced in the internal state of Grain v1 by any difference in the IV bits. We prove that a suitably introduced difference in the IV leads to a distinguisher for the output bit produced in the 105th round. This helps determine the values of 6 expressions in the Secret Key bits. Using the above attack as a subroutine, we propose a method that determines 9 Secret Key bits explicitly. Thus, the complexity for the Key recovery is proportional to $2^{71}$ operations, which is faster than exhaustive search by $2^{9}$.

Cryptanalysis of Selected Block Ciphers
The focus of this dissertation is to present cryptanalytic results on selected block ciphers. Block ciphers are the mathematical structure that will take a plaintext message and convert it into a ciphertext one block at a time using a secret
key. They play an essential role in many cryptographic architectures and frameworks. For a long time they were known as the main building block that will provide confidentiality in an information system. They would also be able to represent a full spectrum of cryptographic services as many block ciphers can be used to construct stream ciphers, hash functions, pseudorandom number generators, and authenticated encryption designs.

For this reason a multitude of initiatives over the years has been established to provide a secure and sound designs for block ciphers as in the calls for Data Encryption Standard (DES) and Advanced Encryption Standard (AES), lightweight ciphers initiatives, and the Competition for Authenticated Encryption: Security, Applicability, and Robustness (CAESAR).

In this thesis, we first present cryptanalytic results on different ciphers. We propose attack named the Invariant Subspace Attack. It is utilized to break the full block cipher PRINTcipher for a significant fraction of its keys. This new attack also gives us new insights into other, more well-established attacks. In addition, we also show that for weak keys, strongly biased linear approximations exists for any number of rounds.

Furthermore, we provide variety of attacks on the family of lightweight block cipher SIMON that was published by the U.S National Security Agency (NSA). The ciphers are developed with optimization towards both hardware and software in mind. While the specification paper discusses design requirements and performance of the presented lightweight ciphers thoroughly, no security assessment is given. We present a series of observations on the presented construction that, in some cases, yield attacks, while in other cases may provide basis of further analysis by the cryptographic community. Specifically, The attacks obtained are using classical- as well as truncated differentials. In addition to that, we also investigate the security of SIMON against different linear cryptanalysis methods, i.e., classic linear, and linear hull attacks. we present a connection between linear characteristic and differential characteristic, multiple linear and differential and linear hull and differential, and employ it to adapt the current known results on differential cryptanalysis of SIMON to linear cryptanalysis results.

Finally, we investigate links between different methods of cryptanalysis and how they can be utilized for block cipher cryptanalysis. We consider the known results on the links among integral, impossible differential and zero-correlation linear hulls in order to prove that constructing a zero-correlation linear hull always implies the existence of an integral distinguisher. Moreover, we show that constructing zero-correlation linear hull on a Feistel structure with SP-type round functions, where P is a binary matrix, is equivalent to constructing impossible differential on the same structure except that P is substituted by the transposed matrix PT . We present an integral distinguishers of 5-round Feistel structure with bijective round functions and 3-round Feistel structure with round functions not necessarily being bijective. In addition to an integral distinguishers of Camellia so far, i.e., 7-round integral distinguishers of Camellia with FL/FL−1 layer and 8-round integral distinguishers of Camellia without FL/FL−1 layer.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Cryptology
Authors: Alkhzaimi, H. A. (Intern), Knudsen, L. R. (Intern)
Number of pages: 140
Publication date: 2016

Publication information
Place of publication: Kgs. Lyngby
Publisher: Technical University of Denmark (DTU)
Original language: English

Series: DTU Compute PHD-2015
Number: 360
ISSN: 0909-3192
Main Research Area: Technical/natural sciences
Electronic versions:
phd360_Alkhzaimi_HA.pdf
Publication: Research › Ph.D. thesis – Annual report year: 2016

Design and Analysis of Symmetric Primitives
The subject of this thesis is the study of symmetric cryptographic primitives. We investigate these objects from three different perspectives: cryptanalysis, design and implementation aspects.

The first part deals with cryptanalysis of symmetric primitives, where one tries to leverage a property of the design to achieve some adversarial goal. Two of the most successful types of cryptanalysis are differential- and linear attacks. We apply variants of differential cryptanalysis to the lightweight block cipher SIMON which was proposed by researchers from the National Security Agency (NSA) in 2013. In particular, we present a search heuristic to find differentials of high probability, and we investigate the clustering of characteristics known as the differential effect. Finally, we apply impossible differential attacks using truncated differentials to a number of SIMON variants. Next, we define a theoretical model for key-less linear distinguishers, which captures the meaning of distinguishing a block cipher from an ideal permutation using...
linear cryptanalysis, when the key is either known or chosen by the adversary. Such models exist using differential properties but were never before defined using linear cryptanalysis. We apply this model to the standardized block cipher PRESENT. Finally, we present very generic attacks on two authenticated encryption schemes, AVALANCHE and RBS, by pointing out severe design flaws that can be leveraged to fully recover the secret key with very low complexity.

In the second part, we delve into the matter of the various aspects of designing a symmetric cryptographic primitive. We start by considering generalizations of the widely acclaimed Advanced Encryption Standard (AES) block cipher. In particular, our focus is on a component operation in the cipher which permutes parts of the input to obtain dependency between the state bits. With this operation in focus, we give a range of theoretical results, reducing the possible choices for the operation in generalized ciphers to a particular set of classes. We then employ a computer-aided optimization technique to determine the best choices for the operation in terms of resistance towards differential- and linear cryptanalysis. Also in the vein of symmetric primitive design we present PRØST, a new and highly secure permutation. Employing existing third-party modes of operation, we present six proposals based on PRØST for the ongoing CAESAR competition for authenticated encryption with associated data. We describe the design criteria, the usage modes and give proofs of security.

Finally, in the third part, we consider implementation aspects of symmetric cryptography, with focus on high-performance software. In more detail, we analyze and implement modes recommended by the National Institute of Standards and Technology (NIST), as well as authenticated encryption modes from the CAESAR competition, when instantiated with the AES. The data processed in our benchmarking has sizes representative to that of typical Internet traffic. Motivated by a significant improvement to special AES instructions in the most recent microarchitecture from Intel, codenamed Haswell, our implementations are tailored for this platform. Finally, we introduce the comb scheduler which is a low-overhead look-ahead strategy for processing multiple messages in parallel. We show that it significantly increases the throughput for sequential modes of operation especially, but also for parallel modes to a lesser extent.

Feasibility study of context-awareness device Comfort calculation methods and their application to comfort-based access control

Mobile devices have become more powerful and are increasingly integrated in the everyday life of people: from playing games, taking pictures and interacting with social media to replacing credit cards in payment solutions. Some actions may only be appropriate in some situations, so the security of a mobile device is therefore increasingly linked to its context, such as its location, surroundings (e.g. objects in the immediate environment) and so on. However, situational awareness and context are not captured by traditional security models. In this paper, we examine the notion of Device Comfort, which captures a device's ability to secure and reason about its environment. Specifically, we study the feasibility of two device comfort calculation methods we proposed in previous work. We do trace driven simulations based on a large body of sensed data from mobile devices in the real world. This allows us to analyze the influence of the context on the comfort level of the device in different perceived contexts in the real world. Moreover, to demonstrate the utility of our device comfort calculation methods, we apply it to comfort-based access control for mobile devices. We present the policy enforcement framework and show how to enforce our two methods using an existing security policy specification language.
Identity management for e-government Libya as a case study

Governments are strengthening their identity (ID) management strategies to deliver new and improved online services to their citizens. Such online services typically include applications for different types of permissions, requests for different types of official documents and management of different types of entitlements. The ID management scheme must therefore be able to correctly authenticate citizens and link online presence to real world identities.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Cyber Security
Authors: Elaswad, O. (Intern), Jensen, C. D. (Intern)
Pages: 106-113
Publication date: 2016

Introducing E-Government in Developing Countries Analysis of Egyptian e-Government Services

Online Identification and Authentication is an essential requirement for providing e-services. Few studies have investigated the challenges facing e-Government and IDM in developing countries and, to the best of our knowledge, none of the existing research has studied the challenges facing online identification and remote authentication in developing countries, such as the North Africa Countries (NAC), where a relatively large proportion of citizens are illiterate. Therefore, the design of a national IDM system in a NAC must explicitly consider illiteracy to allow this group of citizens to benefit from online services. Egypt is one of the NAC, which has implemented online identification and authentication services that are widely recognized as the most advanced among the NAC. This paper analyses the Egyptian digital IDM in order to identify IDM requirements for online identification and authentication services that guarantee equal access to online services and an inclusive society. The study identifies strengths and weaknesses of the Egyptian e-Government and IDM services, which we believe are common to most NAC, since the NAC are quite similar in terms of social culture, citizen's education level and skills, citizen's behaviours, digital infrastructure and legislation, but also common to many other developing countries. Our analysis of the Egyptian e-Government services indicates that the security requirements and principle of equal access are not fully met, which illustrates the difficulty of introducing e-Government in developing countries.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Cyber Security
Authors: Elaswad, O. (Intern), Jensen, C. D. (Intern)
Pages: 1-13
Publication date: 2016
MiMC: Efficient encryption and cryptographic hashing with minimal multiplicative complexity

We explore cryptographic primitives with low multiplicative complexity. This is motivated by recent progress in practical applications of secure multi-party computation (MPC), fully homomorphic encryption (FHE), and zero-knowledge proofs (ZK) where primitives from symmetric cryptography are needed and where linear computations are, compared to non-linear operations, essentially “free”. Starting with the cipher design strategy “LowMC” from Eurocrypt 2015, a number of bitoriented proposals have been put forward, focusing on applications where the multiplicative depth of the circuit describing the cipher is the most important optimization goal.

Surprisingly, albeit many MPC/FHE/ZK-protocols natively support operations in GF(p) for large p, very few primitives, even considering all of symmetric cryptography, natively work in such fields. To that end, our proposal for both block ciphers and cryptographic hash functions is to reconsider and simplify the round function of the Knudsen-Nyberg cipher from 1995. The mapping $F(x) := x^3$ is used as the main component there and is also the main component of our family of proposals called "MiMC". We study various attack vectors for this construction and give a new attack vector that outperforms others in relevant settings.

Due to its very low number of multiplications, the design lends itself well to a large class of applications, especially when the depth does not matter but the total number of multiplications in the circuit dominates all aspects of the implementation. With a number of rounds which we deem secure based on our security analysis, we report on significant performance improvements in a representative use-case involving SNARKs.
PMFA: Toward Passive Message Fingerprint Attacks on Challenge-Based Collaborative Intrusion Detection Networks

To enhance the performance of single intrusion detection systems (IDSs), collaborative intrusion detection networks (CIDNs) have been developed, which enable a set of IDS nodes to communicate with each other. In such a distributed network, insider attacks like collusion attacks are the main threat. In the literature, challenge-based trust mechanisms have been established to identify malicious nodes by evaluating the satisfaction between challenges and responses. However, we find that such mechanisms rely on two major assumptions, which may result in a weak threat model and make CIDNs still vulnerable to advanced insider attacks in practical deployment. In this paper, we design a novel type of collusion attack, called passive message fingerprint attack (PMFA), which can collect messages and identify normal requests in a passive way. In the evaluation, we explore the attack performance under both simulated and real network environments. Experimental results indicate that under our attack, malicious nodes can send malicious responses to normal requests while maintaining their trust values.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Cyber Security, City University of Hong Kong
Authors: Li, W. (Ekstern), Meng, W. (Intern), Kwok, L. (Ekstern), Ip, H. S. (Ekstern)
Pages: 433-449
Publication date: 2016

Host publication information
Title of host publication: Proceedings of the 10th International Conference on Network and System Security (NSS 2016)
Publisher: Springer
ISBN (Print): 978-3-319-46297-4
ISBN (Electronic): 978-3-319-46298-1
Series: Lecture Notes in Computer Science
Volume: 9955
ISSN: 0302-9743
BFI conference series: International Conference on Network and System Security (5010170)
Main Research Area: Technical/natural sciences
Intrusion Detection System, Collaborative network, Insider threats, Collusion attacks, Challenge-based trust mechanism
DOIs: 10.1007/978-3-319-46298-1_28
Source: PublicationPreSubmission
Source-ID: 127067931
Publication: Research - peer-review › Article in proceedings – Annual report year: 2016

Polytopic Cryptanalysis

Standard differential cryptanalysis uses statistical dependencies between the difference of two plaintexts and the difference of the respective two ciphertexts to attack a cipher. Here we introduce polytopic cryptanalysis which considers interdependencies between larger sets of texts as they traverse through the cipher. We prove that the methodology of standard differential cryptanalysis can unambiguously be extended and transferred to the polytopic case including impossible differentials. We show that impossible polytopic transitions have generic advantages over impossible differentials. To demonstrate the practical relevance of the generalization, we present new low-data attacks on round-reduced DES and AES using impossible polytopic transitions that are able to compete with existing attacks, partially outperforming these.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Cyber Security
Authors: Tiessen, T. (Intern)
Pages: 214-239
Publication date: 2016

Host publication information
Editors: Fischlin, M., Coron, J.
ISBN (Print): 978-3-662-49889-7
ISBN (Electronic): 978-3-662-49890-3
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.

Secure Refactoring with Java Information Flow

Refactoring means that a program is changed without changing its behaviour from an observer's point of view. Does the change of behaviour also imply that the security of the program is not affected by the changes? Using Myers and Liskov's distributed information flow control model DLM and its Java implementation Jif, we explore this question practically on common patterns of Refactoring as known from Fowler. We first illustrate on an example the "Extract method" refactoring and how it can endanger confidentiality. We then show how to construct a secure version of this major refactoring pattern by employing Jif to control information flows. Finally, we can show that security leaks as encountered at the outset are not possible anymore.
Smartphone User Authentication Using Touch Dynamics in the Big Data Era: Challenges and Opportunities

With the wide adoption of smartphones, touchscreens have become the leading input method on the mobile platform, with more than 78% of all phones using a touchscreen. Thus, more research studies started focusing on touch dynamics and its applications on user authentication. Generally, touch dynamics can be described as the characteristics of the inputs received from a touchscreen when a user is interacting with a device (e.g., a touchscreen mobile phone). Intuitively, touch dynamics is different from keystroke dynamics in that touch dynamics has more input types such as multi-touch and touch movement. On the other hand, the inputs of press button up and press button down in keystroke dynamics are similar to the actions of touch press up and touch press down (e.g., single-touch) in touch dynamics. Due to its characteristics, touch dynamics received more attention from the literature. In this chapter, we aim to present a review, introducing recent advancement relating to touch dynamics in the literature, and providing insights about its future trends in the big data era.

Towards Formal Analysis of Insider Threats for Auctions

This paper brings together the world of insider threats and auctions. For online-auction systems, like eBay, but also for high-value one-off auction algorithms as they are used for selling radio wave frequencies, the use of rigorous machine supported modelling and verification techniques is meaningful to prove correctness and scrutinize vulnerability to security and privacy attacks. Surveying the threats in auctions and insider collusions, we present an approach to model and analyze auction protocols for insider threats using the interactive theorem prover Isabelle. As a case study, we use the
cocaine auction protocol that represents a nice combination of cryptographic techniques, protocols, and privacy goals suitable for highlighting insider threats for auctions.

**General information**

**State:** Published  
**Organisations:** Department of Applied Mathematics and Computer Science, Cyber Security, University of Birmingham, Middlesex University  
**Authors:** Kammueller, F. (Ekstern), Kerber, M. (Ekstern), Probst, C. W. (Intern)  
**Pages:** 23-34  
**Publication date:** 2016

**Host publication information**

**Title of host publication:** Proceedings of the 8th ACM CCS International Workshop on Managing Insider Security Threats, MIST ’16  
**Publisher:** Association for Computing Machinery  
**ISBN (Print):** 978-1-4503-4571-2  
**Main Research Area:** Technical/natural sciences  
**Workshop:** 8th ACM CCS International Workshop on Managing Insider Security Threats, Vienna, Austria, 28/10/2016  
**Insider Threat, Auctions, Formal Methods**

**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
Analyzing Permutations for AES-like Ciphers: Understanding ShiftRows

Designing block ciphers and hash functions in a manner that resemble the AES in many aspects has been very popular since Rijndael was adopted as the Advanced Encryption Standard. However, in sharp contrast to the MixColumns operation, the security implications of the way the state is permuted by the operation resembling ShiftRows has never been studied in depth.

Here, we provide the first structured study of the influence of ShiftRows-like operations, or more generally, word-wise permutations, in AES-like ciphers with respect to diffusion properties and resistance towards differential- and linear attacks. After formalizing the concept of guaranteed trail weights, we show a range of equivalence results for permutation layers in this context. We prove that the trail weight analysis when using arbitrary word-wise permutations, with rotations as a special case, reduces to a consideration of a specific normal form. Using a mixed-integer linear programming approach, we obtain optimal parameters for a wide range of AES-like ciphers, and show improvements on parameters for Rijndael-192, Rijndael-256, PRIMATEs-80 and Prøst-128. As a separate result, we show for specific cases of the state geometry that a seemingly optimal bound on the trail weight can be obtained using cyclic rotations only for the permutation layer, i.e. in a very implementation friendly way.

General Information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Cryptology, Ruhr-Universität Bochum, Universität Passau, Ruhr-University Bochum
Authors: Beierle, C. (Ekstern), Jovanovic, P. (Ekstern), Lauridsen, M. M. (Intern), Leander, G. (Ekstern), Rechberger, C. (Intern)
Pages: 37-58
Publication date: 2015

Host publication information
Title of host publication: Topics in Cryptology – CT-RSA 2015 : Proceedings of the Cryptographers’ Track at the RSA Conference 2015
Publisher: Springer
Editor: Nyberg, K.
ISBN (Print): 978-3-319-16714-5
ISBN (Electronic): 978-3-319-16715-2

Series: Lecture Notes in Computer Science
Volume: 9048
ISSN: 0302-9743
Main Research Area: Technical/natural sciences
Conference: The RSA Conference Cryptographers’ Track (CT-RSA 2015), San Francisco, United States, 20/04/2015 - 20/04/2015
AES, AES-like, Differential cryptanalysis, Linear cryptanalysis, Diffusion, Optimization, Mixed-integer linear programming

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.
Ciphers for MPC and FHE

Designing an efficient cipher was always a delicate balance between linear and non-linear operations. This goes back to the design of DES, and in fact all the way back to the seminal work of Shannon.

Here we focus, for the first time, on an extreme corner of the design space and initiate a study of symmetric-key primitives that minimize the multiplicative size and depth of their descriptions. This is motivated by recent progress in practical instantiations of secure multi-party computation (MPC), fully homomorphic encryption (FHE), and zero-knowledge proofs (ZK) where linear computations are, compared to non-linear operations, essentially “free”.

We focus on the case of a block cipher, and propose the family of block ciphers “LowMC”, beating all existing proposals with respect to these metrics by far. We sketch several applications for such ciphers and give implementation comparisons suggesting that when encrypting larger amounts of data the new design strategy translates into improvements in computation and communication complexity by up to a factor of 5 compared to AES-128, which incidentally is one of the most competitive classical designs. Furthermore, we identify cases where “free XORs” can no longer be regarded as such but represent a bottleneck, hence refuting this commonly held belief with a practical example.
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.

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.

General information
State: Published
Organisations: Cryptology, Department of Applied Mathematics and Computer Science
Authors: Banik, S. (Intern), Bogdanov, A. (Intern)
Pages: 241-252
Publication date: 2015

Host publication information
Title of host publication: Progress in Cryptology – INDOCRYPT 2015 : Proceedings of the 16th International Conference on Cryptology in India
Editors: Biryukov, A., Goyal, V.
ISBN (Print): 978-3-319-26616-9
ISBN (Electronic): 978-3-319-26617-6
Series: Lecture Notes in Computer Science
Volume: 9462
ISSN: 0302-9743
BFI conference series: INDOCRYPT (5010749)
Main Research Area: Technical/natural sciences
Conference: 16th International Conference on Cryptology in India, Bangalore, India, 06/12/2015 - 06/12/2015
AES, Fault analysis, Grain-128, Infective countermeasures

Fast evaluation of polynomials over binary finite fields and application to side-channel countermeasures
We describe a new technique for evaluating polynomials over binary finite fields. This is useful in the context of anti-DPA countermeasures when an S-box is expressed as a polynomial over a binary finite field. For n-bit S-boxes, our new technique has heuristic complexity $O(2^{n/2}/n)$ instead of $O(2^{n/2})$ proven complexity for the Parity-Split method. We also prove a lower bound of $\Omega(2^{n/2}/n)$ on the complexity of any method to evaluate n-bit S-boxes; this shows that our method is asymptotically optimal. Here, complexity refers to the number of non-linear multiplications required to evaluate the polynomial corresponding to an S-box. In practice, we can evaluate any 8-bit S-box in 10 non-linear multiplications instead of 16 in the Roy–Vivek paper from CHES 2013, and the DES S-boxes in 4 non-linear multiplications instead of 7. We also evaluate any 4-bit S-box in 2 non-linear multiplications instead of 3. Hence our method achieves optimal complexity for the PRESENT S-box

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Cryptology, University of Luxembourg
Authors: Coron, J. (Ekstern), Roy, A. (Intern), Vivek, S. (Ekstern)
Pages: 73-83
Publication date: 2015
Main Research Area: Technical/natural sciences

Publication information
Journal: Journal of Cryptographic Engineering
Volume: 5
Issue number: 2
ISSN (Print): 2190-8508
Ratings:
Web of Science (2018): Indexed yes
Scopus rating (2016): SJR 0.528 SNIP 1.504 CiteScore 1.88
Scopus rating (2015): SJR 0.855 SNIP 1.925 CiteScore 2.04
Scopus rating (2014): SJR 0.844 SNIP 1.93 CiteScore 2.21
How Not to Combine RC4 States
Over the past few years, an attractive design paradigm has emerged, that aims to produce new stream cipher designs, by combining one or more independently produced RC4 states. The ciphers so produced turn out to be faster than RC4 on any software platform, mainly because the average number of internal operations used in the cipher per byte of keystream produced is usually lesser than RC4. One of the main efforts of the designers is to ensure that the existing weaknesses of RC4 are not carried over to the new ciphers so designed. In this work we will look at two such ciphers RC4B (proposed by Zhang et. al.) and Quad-RC4/m-RC4 (proposed by Maitra et. al.). We will propose distinguishing attacks against all these ciphers, and look at certain design flaws that made these ciphers vulnerable.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Cryptology, National Informatics Center
Authors: Banik, S. (Intern), Jha, S. (Ekstern)
Pages: 96-112
Publication date: 2015

Host publication information
Title of host publication: Proceedings of the 5th International Conference on Security, Privacy, and Applied Cryptography Engineering (SPACE 2015)
Publisher: Springer
Editors: Chakraborty, R. S., Schwabe, P., Solworth, J.
ISBN (Print): 978-3-319-24125-8
ISBN (Electronic): 978-3-319-24126-5
Series: Lecture Notes in Computer Science
Volume: 9354
ISSN: 0302-9743
Main Research Area: Technical/natural sciences
Conference: 5th International Conference on Security, Privacy, and Applied Cryptography Engineering (SPACE 2015), Jaipur, Rajasthan, India, 03/10/2015 - 03/10/2015
RC4, RC4B, Quad-RC4, m-RC4, Distinguishing Attacks, Stream Cipher
DOI's: 10.1007/978-3-319-24126-5_6
Source: FindIt
Source-ID: 2290010566
Publication: Research - peer-review › Article in proceedings – Annual report year: 2015

Improved Linear Cryptanalysis of Reduced-Round SIMON-32 and SIMON-48
In this paper we analyse two variants of SIMON family of light-weight block ciphers against variants of linear cryptanalysis and present the best linear cryptanalytic results on these variants of reducedround SIMON to date. We propose a time-memory trade-off method that finds differential/linear trails for any permutation allowing low Hamming weight differential/linear trails. Our method combines low Hamming weight trails found by the correlation matrix representing the target permutation with heavy Hamming weight trails found using a Mixed Integer Programming model representing the target differential/linear trail. Our method enables us to find a 17-round linear approximation for SIMON-48 which is the best current linear approximation for SIMON-48. Using only the correlation matrix method, we are able to find a 14-round linear approximation for SIMON-32 which is also the current best linear approximation for SIMON-32. The presented linear approximations allow us to mount a 23-round key recovery attack on SIMON-32 and a 24-round Key recovery attack on SIMON-48/96 which are the current best results on SIMON-32 and SIMON-48. In addition we have an attack on 24 rounds of SIMON-32 with marginal complexity.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Cryptology, SICS - Swedish ICT, Sharif University of Technology, Shahid Rajae Teachers Training University, Queensland University of Technology
Authors: Abdelraheem, M. A. (Ekstern), Alizadeh, J. (Ekstern), Alkhzaimi, H. A. (Intern), Aref, M. R. (Ekstern), Bagheri, N. (Ekstern), Gauravaram, P. (Ekstern)
Pages: 153-179
Linear Distinguishers in the Key-less Setting: Application to PRESENT

The application of the concept of linear cryptanalysis to the domain of key-less primitives is largely an open problem. In this paper we, for the first time, propose a model in which its application is meaningful for distinguishing block ciphers. Combining our model with ideas from message modification and rebound-like approaches, we initiate a study of cryptographic primitives with respect to this new attack vector and choose the lightweight block cipher PRESENT as an example target. This leads to known-key distinguishers over up to 27 rounds, whereas the best previous result is up to 18 rounds in the chosen-key model.

Host publication information
Title of host publication: Revised Selected Papers of the 22nd International Workshop on Fast Software Encryption (FSE 2015)
Publisher: Springer
Editor: Leander, G.
ISBN (Print): 978-3-662-48115-8
Series: Lecture Notes in Computer Science
Volume: 9054
ISSN: 0302-9743
BFI conference series: Fast Software Encryption (5000118)
Main Research Area: Technical/natural sciences
Workshop: 22nd International Workshop on Fast Software Encryption (FSE 2015), Istanbul, Turkey, 08/03/2015 - 08/03/2015
Hash function, Block cipher, Linear cryptanalysis, Distinguisher, PRESENT
DOIs:
10.1007/978-3-662-48116-5_11
Source: PublicationPreSubmission
Source-ID: 117990616
Publication: Research - peer-review > Article in proceedings – Annual report year: 2015
prove that \( a \rightarrow b \) is an impossible differential of a structure \( E \) if and only if it is a zero correlation linear hull of the dual structure \( E^\perp \). Meanwhile, our proof shows that the automatic search tool presented by Wu and Wang could find all impossible differentials of both Feistel structures with SP-type round functions and SPN structures. Secondly, by establishing some boolean equations, we show that a zero correlation linear hull always indicates the existence of an integral distinguisher. With this observation we improve the number of rounds of integral distinguishers of Feistel structures, CAST-256, SMS4 and Camellia. Finally, we conclude that an \( r \)-round impossible differential of \( E \) always leads to an \( r \)-round integral distinguisher of the dual structure \( E^\perp \). In the case that \( E \) and \( E^\perp \) are linearly equivalent, we derive a direct link between impossible differentials and integral distinguishers of \( E \). Our results could help to classify different cryptanalytic tools and facilitate the task of evaluating security of block ciphers against various cryptanalytic approaches.

**General information**

State: Published
Organisations: Department of Applied Mathematics and Computer Science, Cryptology, National University of Defense Technology, Shanghai Jiao Tong University, KU Leuven
Authors: Sun, B. (Ekstern), Liu, Z. (Ekstern), Rijmen, V. (Ekstern), Li, R. (Ekstern), Cheng, L. (Ekstern), Wang, Q. (Ekstern), Alkhzaimi, H. A. (Intern), Li, C. (Ekstern)
Pages: 95-115
Publication date: 2015

**Host publication information**

Title of host publication: CRYPTO 2015 : Proceedings of the 35th Annual Cryptology Conference
Volume: 9215
Publisher: Springer
ISBN (Print): 9783662479889

Series: Lecture Notes in Computer Science
Volume: 9215
ISSN: 0302-9743
Main Research Area: Technical/natural sciences
Computer Science (all), Theoretical Computer Science, ARIA, Camellia, CAST-256, Feistel, Impossible differential, Integral, PRESENT, PRINCE, SMS4, SPN, Zero correlation linear, Boolean algebra, Gears, Lyapunov methods, Zero correlation, Cryptography

DoIs: 10.1007/978-3-662-47989-6_5
Source: FindIt
Source-ID: 2287559936
Publication: Research - peer-review › Article in proceedings – Annual report year: 2015

**Observations on the SIMON Block Cipher Family**

In this paper we analyse the general class of functions underlying the Simon block cipher. In particular, we derive efficiently computable and easily implementable expressions for the exact differential and linear behaviour of Simon-like round functions.

Following up on this, we use those expressions for a computer aided approach based on SAT/SMT solvers to find both optimal differential and linear characteristics for Simon. Furthermore, we are able to find all characteristics contributing to the probability of a differential for Simon32 and give better estimates for the probability for other variants.

Finally, we investigate a large set of Simon variants using different rotation constants with respect to their resistance against differential and linear cryptanalysis. Interestingly, the default parameters seem to be not always optimal.
Practical Attacks on AES-like Cryptographic Hash Functions
Despite the great interest in rebound attacks on AES-like hash functions since 2009, we report on a rather generic, albeit keyschedule-dependent, algorithmic improvement: A new message modification technique to extend the inbound phase, which even for large internal states makes it possible to drastically reduce the complexity of attacks to very practical values for reduced-round versions. Furthermore, we describe new and practical attacks on Whirlpool and the recently proposed GOST R hash function with one or more of the following properties: more rounds, less time/memory complexity, and more relevant model. To allow for easy verification, we also provide a source-code for them.

Security of the AES with a Secret S-Box
How does the security of the AES change when the S-box is replaced by a secret S-box, about which the adversary has no knowledge? Would it be safe to reduce the number of encryption rounds?

In this paper, we demonstrate attacks based on integral cryptanalysis which allow to recover both the secret key and the secret S-box for respectively four, five, and six rounds of the AES. Despite the significantly larger amount of secret information which an adversary needs to recover, the attacks are very efficient with time/data complexities of $2^{17/2}$, $2^{38/2}$, and $2^{90/2}$, respectively.

Another interesting aspect of our attack is that it works both as chosen plaintext and as chosen ciphertext attack. Surprisingly, the chosen ciphertext variant has a significantly lower time complexity in the attacks on four and five round, compared to the respective chosen plaintext attacks.
Some Results on Sprout

Sprout is a lightweight stream cipher proposed by Armknecht and Mikhalev at FSE 2015. It has a Grain-like structure with two state Registers of size 40 bits each, which is exactly half the state size of Grain v1. In spite of this, the cipher does not appear to lose in security against generic Time-Memory-Data Tradeoff attacks due to the novelty of its design. In this paper, we first present improved results on Key Recovery with partial knowledge of the internal state. We show that if 50 of the 80 bits of the internal state are guessed then the remaining bits along with the secret key can be found in a reasonable time using a SAT solver. Thereafter, we show that it is possible to perform a distinguishing attack on the full Sprout stream cipher in the multiple IV setting using around 240 randomly chosen IVs on an average. The attack requires around 248 bits of memory. Thereafter, we will show that for every secret key, there exist around 230 IVs for which the LFSR used in Sprout enters the all zero state during the keystream generating phase. Using this observation, we will first show that it is possible to enumerate Key-IV pairs that produce keystream bits with period as small as 80. We will then outline a simple key recovery attack that takes time equivalent to 2^{66.7} encryptions with negligible memory requirement. This although is not the best attack reported against this cipher in terms of the time complexity, it is the best in terms of the memory required to perform the attack.
Some security results of the RC4+ stream cipher

The RC4+ stream cipher was proposed as an alternative to the well-known RC4 stream cipher. It was claimed by the authors that this new stream cipher was designed to overcome all the weaknesses reported against the alleged RC4 stream cipher. In the design specifications of RC4+, the authors make use of an 8-bit design parameter called pad that is fixed to the value 0xAA. The first distinguishing attack on RC4+ based on the bias of its first output byte was shown in a previous paper. In this paper, it was also mentioned that the distinguishing attack would still hold if the pad used in RC4+ is fixed to any even 8-bit constant other than 0xAA. Therefore, the question that naturally arises is whether the design of RC4+ can be protected by fixing the pad parameter to some constant odd value. In this paper, we try to answer this very question. We show that the design is still vulnerable by mounting a distinguishing attack even if the pad is fixed to some constant 8-bit odd value. Surprisingly, we find that if the value of the pad is made equal to 0x03, the design provides maximum resistance to distinguishing attacks. Lastly, we return to the original cipher, that is, in which pad is set to 0xAA and unearth another bias in the second output byte of the cipher. Thereafter, we will present a generalized way of finding biases in every M-th output byte (M ≡ 3) of RC4+, that is, ZM, based on the Hamming weight of m ≡ MmodN. Finally, we improve the differential fault attack on RC4+ proposed in a previous paper, both in terms of number of faults required and the computational complexity. In fact, we reduce the number of faults by around 11264 on average, and our algorithm is around 26 times faster.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Cryptology, National Informatics Center
Authors: Banik, S. (Intern), Jha, S. (Ekstern)
Pages: 4061-4072
Publication date: 2015
Main Research Area: Technical/natural sciences

Publication information
Journal: Security and Communication Networks
Volume: 8
Issue number: 18
ISSN (Print): 1939-0114
Ratings:
Web of Science (2018): Indexed yes
Web of Science (2017): Indexed Yes
Scopus rating (2016): SJR 0.319 SNIP 0.842 CiteScore 1.43
Scopus rating (2015): SJR 0.281 SNIP 0.814 CiteScore 1.09
Web of Science (2015): Indexed yes
Scopus rating (2014): SJR 0.297 SNIP 0.908 CiteScore 0.93
Scopus rating (2013): SJR 0.243 SNIP 0.623 CiteScore 0.71
Scopus rating (2012): SJR 0.187 SNIP 0.656 CiteScore 0.67
Scopus rating (2011): SJR 0.236 SNIP 1.087 CiteScore 0.86
Scopus rating (2010): SJR 0.175 SNIP 0.372
Original language: English
Distinguishing Attacks, RC4, RC4+, Stream Ciphers
DOIs:
10.1002/sec.1323
Publication: Research - peer-review › Journal article – Annual report year: 2015

State-Recovery Analysis of Spritz
RC4 suffered from a range of plaintext-recovery attacks using statistical biases, which use substantial, albeit close-to-practical, amounts of known keystream in applications such as TLS or WEP/WPA. Spritz was recently proposed at the rump session of CRYPTO 2014 as a slower redesign of RC4 by Rivest and Schuldt, aiming at reducing the statistical biases that lead to these attacks on RC4.

Even more devastating than those plaintext-recovery attacks from large amounts of keystream would be state- or key-recovery attacks from small amounts of known keystream. For RC4, there is unsubstained evidence that they may exist, the situation for Spritz is however not clear, as resistance against such attacks was not a design goal.

In this paper, we provide the first cryptanalytic results on Spritz and introduce three different state recovery algorithms. Our first algorithm recovers an internal state, requiring only a short segment of keystream, with an approximated complexity of 21400, which is much faster than exhaustive search through all possible states, but is still far away from a practical attack. Furthermore, we introduce a second algorithm that uses a pattern in the keystream to reduce the number of guessed values in our state recovery algorithm. Our third algorithm uses a probabilistic approach by considering the permutation table as probability distribution.
All in all, rather than showing a weakness, our analysis supports the conjecture that compared to RC4, Spritz may also provide higher resistance against potentially devastating state-recovery attacks.

**General information**

State: Published  
Organisations: Department of Applied Mathematics and Computer Science, Cryptology, Graz University of Technology  
Authors: Ankele, R. (Ekstern), Kölbl, S. (Intern), Rechberger, C. (Intern)  
Pages: 204-221  
Publication date: 2015

**Host publication information**

Title of host publication: Progress in Cryptology – LATINCRYPT 2015: Proceedings of the 4th International Conference on Cryptology and Information Security in Latin America  
Publisher: Springer  
Editors: Lauter, K., Rodríguez-Henríquez, F.  
ISBN (Print): 978-3-319-22173-1  
ISBN (Electronic): 978-3-319-22174-8

**The Rebound Attack and Subspace Distinguishers: Application to Whirlpool**

We introduce the rebound attack as a variant of differential cryptanalysis on hash functions and apply it to the hash function Whirlpool, standardized by ISO/IEC. We give attacks on reduced variants of the 10-round Whirlpool hash function and compression function. Our results are collisions for 5.5 and near-collisions for 7.5 rounds on the hash function, as well as semi-free-start collisions for 7.5 and semi-free-start near-collisions for 9.5 rounds on the compression function. Additionally, we introduce the subspace problem as a generalization of near-collision resistance. Finally, we present the first distinguishers that apply to the full compression function and the full underlying block cipher W of Whirlpool.

**General information**

State: Published  
Organisations: Department of Applied Mathematics and Computer Science, Cryptology, NXP Semiconductors Austria, Graz University of Technology, Katholieke Universiteit  
Authors: Lamberger, M. (Ekstern), Mendel, F. (Ekstern), Schläffer, M. (Ekstern), Rechberger, C. (Intern), Rijmen, V. (Ekstern)  
Number of pages: 40  
Pages: 257-296  
Publication date: 2015

**Publication information**

Journal: Journal of Cryptology  
Volume: 28  
Issue number: 2  
ISSN (Print): 0933-2790

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 0.861 SNIP 2.607 CiteScore 2.68  
BFI (2015): BFI-level 2
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.
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.
Cryptanalysis of SIMON Variants with Connections

SIMON is a family of 10 lightweight block ciphers published by Beaulieu et al. from the United States National Security Agency (NSA). A cipher in this family with K-bit key and N-bit block is called SIMONN/K. We present several linear characteristics for reduced-round SIMON32/64 that can be used for a key-recovery attack and extend them further to attack other variants of SIMON. Moreover, we provide results of key recovery analysis using several impossible differential characteristics starting from 14 out of 32 rounds for SIMON32/64 to 22 out of 72 rounds for SIMON128/256. In some cases the presented observations do not directly yield an attack, but provide a basis for further analysis for the specific SIMON variant. Finally, we exploit a connection between linear and differential characteristics for SIMON to construct linear characteristics for different variants of reduced-round SIMON. Our attacks extend to all variants of SIMON covering more rounds compared to any known results using linear cryptanalysis. We present a key recovery attack against SIMON128/256 which covers 35 out of 72 rounds with data complexity 2123. We have implemented our attacks for small scale variants of SIMON and our experiments confirm the theoretical bias presented in this work.

Cryptanalysis of the Double-Feedback XOR-Chain Scheme Proposed in Indocrypt 2013

For any modern chip design with a considerably large portion of logic, design for test (DFT) is a mandatory part of the design process which helps to reduce the complexity of testing sequential circuits. Scan-chains are one of the most commonly-used DFT techniques. However, the presence of scan-chains makes the device vulnerable to scan-based attacks from a cryptographic point of view. Techniques to cryptanalyze stream ciphers like Trivium, with additional hardware for scan-chains, are already available in literature (Agrawal et al. Indocrypt 2008). Such ideas were extended to more complicated stream ciphers like MICKEY 2.0 in the paper by Banik et al. at Indocrypt 2013. In this paper, we will look at the Double-Feedback XOR-Chain based countermeasure that was proposed by Banik et al. in Indocrypt 2013, to protect scan-chains from such scan-based attacks. We will show that such an XOR-Chain based countermeasure is vulnerable to attack. As an alternative, we propose a novel countermeasure based on randomization of XOR gates, that can protect scan-chains against such attacks.
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.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science , Cryptology, Katholieke Universiteit, iMinds, NTT Secure Platform Laboratories
Internal differential collision attacks on the reduced-round Grøstl-0 hash function

We analyze the Grøstl-0 hash function, that is the version of Grøstl submitted to the SHA-3 competition. This paper extends Peyrin's internal differential strategy, that uses differential paths between the permutations P and Q of Grøstl-0 to construct distinguishers of the compression function. This results in collision attacks and semi-free-start collision attacks on the Grøstl-0 hash function and compression function with reduced rounds. Specifically, we show collision attacks on the Grøstl-0-256 hash function reduced to 5 and 6 out of 10 rounds with time complexities $2^{48}$ and $2^{112}$ and on the Grøstl-0-512 hash function reduced to 6 out of 14 rounds with time complexity $2^{183}$. Furthermore, we demonstrate semi-free-start collision attacks on the Grøstl-0-256 compression function reduced to 8 rounds and the Grøstl-0-512 compression function reduced to 9 rounds. Finally, we show improved distinguishers for the Grøstl-0-256 permutations with reduced rounds.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Cryptology, Hitachi Ltd., Katholieke Universiteit
Authors: Ideguchi, K. (Ekstern), Tischhauser, E. W. (Intern), Preneel, B. (Ekstern)
Pages: 251-271
Publication date: 2014

Publication information
Journal: Designs, Codes and Cryptography
Volume: 70
Issue number: 3
ISSN (Print): 0925-1022
Ratings:
BFI (2018): BFI-level 1
Web of Science (2018): Indexed yes
BFI (2017): BFI-level 1
Web of Science (2017): Indexed yes
BFI (2016): BFI-level 1
Scopus rating (2016): CiteScore 1.09 SJR 0.64 SNIP 1.393
Web of Science (2016): Indexed yes
BFI (2015): BFI-level 1
Scopus rating (2015): SJR 0.604 SNIP 1.095 CiteScore 0.82
BFI (2014): BFI-level 1
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.
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

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 29-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
On the Efficacy of Solving LWE by Reduction to Unique-SVP

We present a study of the concrete complexity of solving instances of the unique shortest vector problem (uSVP). In particular, we study the complexity of solving the Learning with Errors (LWE) problem by reducing the Bounded-Distance Decoding (BDD) problem to uSVP and attempting to solve such instances using the ‘embedding’ approach. We experimentally derive a model for the success of the approach, compare to alternative methods and demonstrate that for the LWE instances considered in this work, reducing to uSVP and solving via embedding compares favorably to other approaches.

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.
Rotational Rebound Attacks on Reduced Skein

In this paper we combine two powerful methods of symmetric cryptanalysis: rotational cryptanalysis and the rebound attack. Rotational cryptanalysis was designed for the analysis of bit-oriented designs like ARX (Addition-Rotation-XOR) schemes. It has been applied to several hash functions and block ciphers, including the new standard SHA-3 (Keccak). The rebound attack is a start-from-the-middle approach for finding differential paths and conforming pairs in byte-oriented designs like Substitution-Permutation networks and AES.

We apply our new compositional attack to the reduced version of the hash function Skein, a finalist of the SHA-3 competition. Our attack penetrates more than two thirds of the Skein core—the cipher Threefish, and made the designers to change the submission in order to prevent it.

The rebound part of our attack has been significantly enhanced to deliver results on the largest number of rounds. We also use neutral bits and message modification methods from the practice of collision search in MD5 and SHA-1 hash functions. These methods push the rotational property through more rounds than previous analysis suggested, and eventually establish a distinguishing property for the reduced Threefish cipher. We formally prove that such a property cannot be found for an ideal cipher within the complexity limits of our attack. The complexity estimates are supported by extensive experiments.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Cryptology, Nanyang Technological University, University of Luxembourg
Authors: Khovratovich, D. (Ekstern), Nikolić, I. (Ekstern), Rechberger, C. (Intern)
Pages: 452-479
Publication date: 2014
Main Research Area: Technical/natural sciences

Publication information
Journal: Journal of Cryptology
Volume: 27
Issue number: 3
ISSN (Print): 0933-2790
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 0.861 SNIP 2.607 CiteScore 2.68
BFI (2015): BFI-level 2
Scopus rating (2015): SJR 1.171 SNIP 2.775 CiteScore 2.75
Web of Science (2015): Indexed yes
BFI (2014): BFI-level 2
Scopus rating (2014): SJR 1.114 SNIP 2.798 CiteScore 2.76
Web of Science (2014): Indexed yes
BFI (2013): BFI-level 2
Scopus rating (2013): SJR 1.371 SNIP 3.019 CiteScore 3.16
ISI indexed (2013): ISI indexed yes
Web of Science (2013): Indexed yes
BFI (2012): BFI-level 2
Scopus rating (2012): SJR 1.184 SNIP 3.049 CiteScore 3.06
ISI indexed (2012): ISI indexed yes
Web of Science (2012): Indexed yes
BFI (2011): BFI-level 2
Scopus rating (2011): SJR 1.504 SNIP 3.179 CiteScore 3.6
ISI indexed (2011): ISI indexed yes
BFI (2010): BFI-level 2
Scopus rating (2010): SJR 1.468 SNIP 2.975
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.

The LOCAL attack: Cryptanalysis of the authenticated encryption scheme ALE

We show how to produce a forged (ciphertext, tag) pair for the scheme ALE with data and time complexity of $2^{102}$ ALE encryptions of short messages and the same number of authentication attempts. We use a differential attack based on a local collision, which exploits the availability of extracted state bytes to the adversary. Our approach allows for a time-data complexity tradeoff, with an extreme case of a forgery produced after $2^{119}$ attempts and based on a single authenticated message. Our attack is further turned into a state recovery and a universal forgery attack with a time complexity of $2^{120}$
verification attempts using only a single authenticated 48-byte message.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Cryptology, University of Luxembourg
Authors: Khovratovich, D. (Ekstern), Rechberger, C. (Intern)
Pages: 174-184
Publication date: 2014

Host publication information
Title of host publication: Selected Areas in Cryptography - SAC 2013. Revised Selected Papers
Publisher: Springer
ISBN (Print): 978-3-662-43413-0
ISBN (Electronic): 978-3-662-43414-7

Series: Lecture Notes in Computer Science
Volume: 8282
ISSN: 0302-9743
BFI conference series: Selected Areas in Cryptography (5000230)
Main Research Area: Technical/natural sciences
Conference: 20th International Workshop on Selected Areas of Cryptography, Burnaby, Canada, 14/08/2013 - 14/08/2013
Data Encryption, Systems and Data Security, Algorithm Analysis and Problem Complexity, Coding and Information Theory
DOIs: 10.1007/978-3-662-43414-7_9
Source: FindIt
Source-ID: 2199676910
Publication: Research - peer-review › Article in proceedings – Annual report year: 2014

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
Conference: 20th International Workshop on Fast Software Encryption (FSE 2013), Singapore, Singapore, 10/03/2013 - 10/03/2013
Block ciphers, Known-key security, Known-key distinguishers, Indifferentiability
DOIs: 10.1007/978-3-662-43933-3_18
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.

Dynamic encryption method

Disclosed is a method of transmitting a data set using encryption, wherein the method comprises the steps of: selecting a first encryption technique, wherein said first encryption technique comprises a first encryption algorithm for encrypting plain data into cipher data, and a first decryption algorithm for on provision of a specific key, decrypting cipher data and reproduce plain data; encrypting the first data package comprising plain data, using a first encryption program implementing the first encryption algorithm of said first encryption technique, creating a first encrypted data package comprising cipher data; obtaining a first decryption program; and transmitting said first decryption program and said first encrypted data package to a receiver, wherein the first decryption, upon provision of the specific key and the first encrypted data package, will decrypt the cipher data in the first encrypted data package and reproduce the plain data of the first data package.
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.

Fides: Lightweight Authenticated Cipher with Side-Channel Resistance for Constrained Hardware

In this paper, we present a novel lightweight authenticated cipher optimized for hardware implementations called Fides. It is an online nonce-based authenticated encryption scheme with authenticated data whose area requirements are as low 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.
Improved cryptanalysis of the block cipher KASUMI

KASUMI is a block cipher which consists of eight Feistel rounds with a 128-bit key. Proposed more than 10 years ago, the confidentiality and integrity of 3G mobile communications systems depend on the security of KASUMI. In the practically interesting single key setting, only up to 6 rounds have been attacked so far. In this paper we use some observations on the FL and FO functions. Combining these observations with a key schedule weakness, we select some special input and output values to refine the general 5-round impossible differentials and propose the first 7-round attack on KASUMI with time and data complexities similar to the previously best 6-round attacks. This leaves now only a single round of security margin. The new impossible differential attack on the last 7 rounds needs $2^{114.3}$ encryptions with $2^{52.5}$ chosen plaintexts. For the attack on the first 7 rounds, the data complexity is $2^{62}$ known plaintexts and the time complexity is $2^{115.8}$ encryptions. © 2013 Springer-Verlag Berlin Heidelberg.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Cryptology, Tsinghua University, Shandong University
Authors: Jia, K. (Ekstern), Li, L. (Ekstern), Rechberger, C. (Intern), Chen, J. (Ekstern), Wang, X. (Ekstern)
Pages: 222-233
Publication date: 2013
Conference: 19th International Conference on Selected Areas in Cryptography, Windsor, Canada, 15/08/2012 - 15/08/2012
BFI conference series: Selected Areas in Cryptography (5000230)
Main Research Area: Technical/natural sciences

Publication information
Journal: Lecture Notes in Computer Science
Volume: 7707
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
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 a 10-round attack on Rijndael-256 as well. With 2198.1 chosen plaintexts, an attack is demonstrated on 9-round Rijndael-224 with 2 195.2 encryptions and 2140.4 bytes memory. Increasing the data complexity to 2216 plaintexts, the time complexity can be reduced to 2130 encryptions and the memory requirements to 2 93.6 bytes. For 9-round Rijndael-256, we provide an attack requiring 2229.3 chosen plaintexts, 2194 encryptions, and 2 139.6 bytes memory. Alternatively, with 2245.3 plaintexts, an attack with a reduced time of 2127.1 encryptions and a memory complexity of 290.9 bytes can be mounted. With 2244.2 chosen plaintexts, we can attack 10-round Rijndael-256 with 2253.9 encryptions and 2186.8 bytes of memory.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Cryptology, Shanghai Jiao Tong University, Katholieke Universiteit, Shandong University
Authors: Wang, Q. (Ekstern), Gu, D. (Ekstern), Rijmen, V. (Ekstern), Liu, Y. (Ekstern), Chen, J. (Ekstern), Bogdanov, A. (Intern)
Pages: 126-140
Publication date: 2013
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 chosen-plaintext 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.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Cryptology, Katholieke Universiteit
Authors: Andreeva, E. (Ekstern), Bogdanov, A. (Intern), Luykx, A. (Ekstern), Mennink, B. (Ekstern), Tischhauser, E. W. (Intern), Yasuda, K. (Ekstern)
Pages: 424-443
Publication date: 2013
Slender-Set Differential Cryptanalysis

This paper considers PRESENT-like ciphers with key-dependent S-boxes. We focus on the setting where the same selection of S-boxes is used in every round. One particular variant with 16 rounds, proposed in 2009, is broken in practice in a chosen plaintext/chosen ciphertext scenario. Extrapolating these results suggests that up to 28 rounds of such ciphers can be broken. Furthermore, we outline how our attack strategy can be applied to an extreme case where the S-boxes are chosen uniformly at random for each round, and where the bit permutation is key-dependent as well.
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.

SPONENT: 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.

General information
State: Published
Organisations: Department of Applied Mathematics and Computer Science, Cryptology, NXP Semiconductors, Katholieke Universiteit
Authors: Bogdanov, A. (Intern), Knezevic, M. (Ekstern), Leander, G. (Intern), Toz, D. (Ekstern), Varici, K. (Ekstern), Verbauwhede, I. (Ekstern)
Pages: 2041-2053
Publication date: 2013
Main Research Area: Technical/natural sciences

Publication information
Journal: IEEE Transactions on Computers
Volume: 62
Issue number: 10
ISSN (Print): 0018-9340
Ratings:
BFI (2018): BFI-level 2
Web of Science (2018): Indexed yes
The range of attraction for light traps catching Culicoides biting midges

General information

State: Published
Organisations: Department of Applied Mathematics and Computer Science, Cryptology, Dynamical Systems, National Veterinary Institute, Section for Epidemiology, Statistics and Data Analysis
Authors: Græsbøll, K. (Intern), Kirkeby, C. (Intern), Bødker, R. (Intern), Stockmarr, A. (Intern), Christiansen, L. E. (Intern), Lind, P. (Intern)
Number of pages: 1
Publication date: 2013
Event: Poster session presented at EDENext Annual Meeting, Barcelona, Spain.
The range of attraction for light traps catching Culicoides biting midges (Diptera: Ceratopogonidae)

Background
Culicoides are vectors of e.g. bluetongue virus and Schmallenberg virus in northern Europe. Light trapping is an important tool for detecting the presence and quantifying the abundance of vectors in the field. Until now, few studies have investigated the range of attraction of light traps.

Methods
Here we test a previously described mathematical model (Model I) and two novel models for the attraction of vectors to light traps (Model II and III). In Model I, Culicoides fly to the nearest trap from within a fixed range of attraction. In Model II Culicoides fly towards areas with greater light intensity, and in Model III Culicoides evaluate light sources in the field of view and fly towards the strongest. Model II and III incorporated the directionally dependent light field created around light traps with fluorescent light tubes. All three models were fitted to light trap collections obtained from two novel experimental setups in the field where traps were placed in different configurations.

Results
Results showed that overlapping ranges of attraction of neighboring traps extended the shared range of attraction. Model I did not fit data from any of the experimental setups. Model II could only fit data from one of the setups, while Model III fitted data from both experimental setups.

Conclusions
The model with the best fit, Model III, indicates that Culicoides continuously evaluate the light source direction and intensity. The maximum range of attraction of a single 4W CDC light trap was estimated to be approximately 15.25 meters. The attraction towards light traps is different from the attraction to host animals and thus light trap catches may not represent the vector species and numbers attracted to hosts.

General information
State: Published
Organisations: National Veterinary Institute, Section for Epidemiology, Department of Applied Mathematics and Computer Science, Cryptology, Dynamical Systems, Statistics and Data Analysis
Authors: Kirkeby, C. (Intern), Græsbøll, K. (Intern), Stockmarr, A. (Intern), Christiansen, L. E. (Intern), Bødker, R. (Intern)
Number of pages: 19
Publication date: 2013
Main Research Area: Technical/natural sciences

Publication information
Journal: Parasites & Vectors
Volume: 6
Issue number: 67
ISSN (Print): 1756-3305
Ratings:
BFI (2018): BFI-level 1
Web of Science (2018): Indexed yes
BFI (2017): BFI-level 1
Web of Science (2017): Indexed Yes
BFI (2016): BFI-level 1
Scopus rating (2016): CiteScore 3.23 SJR 1.458 SNIP 1.286
Web of Science (2016): Indexed yes
BFI (2015): BFI-level 1
Scopus rating (2015): SJR 1.676 SNIP 1.381 CiteScore 3.61
Web of Science (2015): Indexed yes
BFI (2014): BFI-level 1
Scopus rating (2014): SJR 1.51 SNIP 1.576 CiteScore 3.31
Web of Science (2014): Indexed yes
BFI (2013): BFI-level 1
Cryptanalysis of Some Lightweight Symmetric Ciphers

In recent years, the need for lightweight encryption systems has been increasing as many applications use RFID and sensor networks which have a very low computational power and thus incapable of performing standard cryptographic operations. In response to this problem, the cryptographic community designed a number of lightweight cryptographic primitives that varies from stream ciphers, block ciphers and recently to hash functions. Out of these many lightweight primitives, the block cipher PRESENT gets a lot of attention from the cryptographic community and it has been recently adopted by ISO as one of the international standards in lightweight cryptography. This thesis aims at analyzing and evaluating the security of some the recently proposed lightweight symmetric ciphers with a focus on PRESENT-like ciphers, namely, the block cipher PRESENT and the block cipher PRINTcipher.

We provide an approach to estimate the probability of differential and linear approximations with low-weight differential and linear characteristics on PRESENT-like ciphers as well as ciphers allowing low hamming weight differential and linear characteristics. We study the effect of key scheduling in the distribution of linear approximations on a variant of PRESENT with identical round keys. We propose a new attack named the Invariant Subspace Attack that was specifically mounted against the lightweight block cipher PRINTcipher. Furthermore, we mount several attacks on a recently proposed stream cipher called A2U2.

General information

State: Published
Organisations: Department of Applied Mathematics and Computer Science, Cryptology
Authors: Abdelraheem, M. A. A. M. A. (Intern), Knudsen, L. R. (Intern), Zenner, E. (Intern), Leander, G. (Intern)
Number of pages: 123
Publication date: 2012

Publication information

Place of publication: Kgs. Lyngby
Publisher: Technical University of Denmark (DTU)
Original language: English
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.