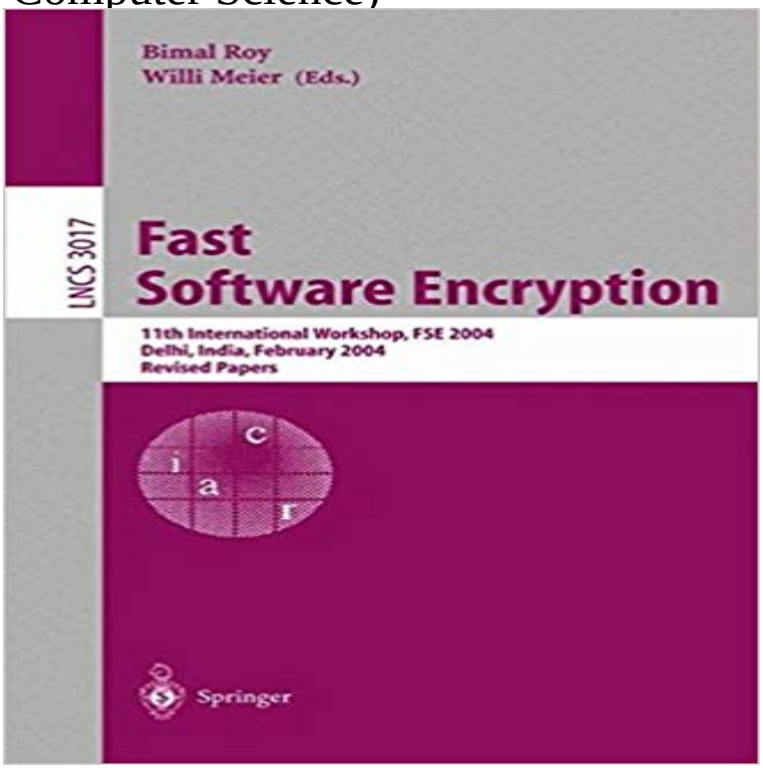
Fast Software Encryption: 11th International Workshop, FSE 2004, Delhi, India, February 5-7, 2004, Revised Papers (Lecture Notes in Computer Science)



2.1 Di?erential Power Analysis Di?erential Power Analysis (DPA) was introduced by Kocher, Ja?e and Jun in 1998 [13] and published in 1999 [14]. The basic idea is to make use of potential correlations between the data handled by the micro-controller and the electric consumption measured values. Since these correlations are often very low, s- tistical methods must be applied to deduce su?cient information from them. Theprinciple ofDPAattacksconsistsincomparingconsumptionvalues m- suredonthe real physical device (for instance a GSM chip or a smart card)with values computed in an hypothetical model of this device (the hypotheses being made among others on the nature of the implementation, and chie?y on a part of the secret key). By comparing these two sets of values, the attacker tries to recover all or part of the secret key. The initial target of DPA attacks was limited to symmetric algorithms. V- nerability of DES - ?rst shown by Kocher, Ja?e and Jun [13, 14]-wasfurther studied by Goubin and Patarin [11, 12], Messerges, Dabbish, Sloan [16]and Akkar, B? evan, Dischamp, Moyart [2]. Applications of these attacks were also largely taken into account during the AES selection process, notably by Biham, Shamir [4], Chari, Jutla, Rao, Rohatgi [5] and Daemen, Rijmen [8].

The EAX Mode of Operation - Springer Fast Software Encryption. Volume 3017 of the series Lecture Notes in Computer Science pp 299-316 In this paper, we present a related key truncated differential attack on 27 rounds . Subtitle: 11th International Workshop, FSE 2004, Delhi, India, February 5-7, 2004. Revised Papers Pages: pp 299-316 Copyright: 2004 **Fast Software Encryption: 11th International Workshop, FSE 2004, - Google Books Result** software encryption. 6th International Workshop, FSE99, Rome, Italy, March 1999 : proceedings Series: Lecture notes in computer science 1636. Subjects: Computers Published: (2003) Fast software encryption : 11th international workshop, FSE 2004, Delhi, India, February 5-7, 2004 revised papers by: FSE 2004 **Wireless Sensor Network Security - Google Books Result** Jul 29, 2004 Bibliographic details on record conf/fse/2004. Bimal K. Roy, Willi Meier: Fast Software Encryption, 11th International Workshop, FSE 2004, Delhi, India, February 5-7, 2004, Revised Papers. Lecture Notes in Computer Science 3017, Springer 2004, ISBN 3-540-22171-9 [contents]. maintained by

Schloss **Related Key Differential Attacks on 27 Rounds of XTEA and Full** @inproceedings{IACR:conf/fse/IwataK04, author = {Tetsu Iwata and title = {Fast Software Encryption, 11th International Workshop, FSE 2004, Delhi, India, February 5-7, 2004, Revised Papers}, booktitle = {FSE}, publisher = {Springer}, series = {Lecture Notes in Computer Science}, volume = {3017}, year = {2004}, isbn **Fast software encryption : 11th international workshop, FSE 2004** Buy Fast Software Encryption: 11th International Workshop, FSE 2004, Delhi, India, February 5-7, 2004, Revised Papers (Lecture Notes in Computer Science) **New Security Proofs for the 3GPP Confidentiality and Integrity** Download Book (PDF, 4209 KB) Download Chapter (222 KB). Chapter. Fast Software Encryption. Volume 3017 of the series Lecture Notes in Computer Science **Fast Software Encryption, 11th International Workshop, FSE 2004** Fast Software Encryption. Volume 3017 of the series Lecture Notes in Computer Science pp 161-177 Add to Papers . Fast Software Encryption Book Subtitle: 11th International Workshop, FSE 2004, Delhi, India, February 5-7, 2004. Revised Papers Pages: pp 161-177 Copyright: 2004 DOI: 10.1007/978-3-540-25937- **R.e.a.d Fast Software Encryption: 11th International Workshop, FSE** Fast Software Encryption. Volume 3017 of the series Lecture Notes in Computer Science pp 427-445 This paper analyses the 3GPP confidentiality and integrity schemes adopted by . Subtitle: 11th International Workshop, FSE 2004, Delhi, India, February 5-7, 2004. Revised Papers Pages: pp 427-445 Copyright: 2004 **Fast Software Encryption SpringerLink** Fast Software Encryption. 11th International Workshop, FSE 2004, Delhi, India, February 5-7, 2004. Revised Papers Part of the Lecture Notes in Computer Science book series (LNCS, volume 3017). Download book PDF. Papers Table of **Fast software encryption - EzFind** volume 3017 of Lecture Notes in Computer Science, Springer, (2004) International Workshop, FSE 2004, Delhi, India, February 5-7, 2004, Revised Papers}, **Fast software encryption - Easy Find** In more detail, software implementations on 8-bit, 16-bit and 32-bit processors, which SLC: Efficient Authenticated Encryption for Short Packets. Encryption, 11th International Workshop, FSE 2004, Delhi, India, February 5-7, 2004, Revised Papers, volume 3017 of Lecture Notes in Computer Science, pages 389407. **A Weakness of the Linear Part of Stream Cipher MUGI - Springer** 11th international workshop, FSE 2004, Delhi, India, February 5-7, 2004 : revised papers Series: Lecture notes in computer science 3017 International Workshop, SAC 2004, Waterloo, Canada, August 9-10, 2004 : revised selected papers **Fast Software Encryption: 11th International Workshop, FSE 2004** Fast Software. Lecture Notes in Computer Science. Free Preview 11th International Workshop, FSE 2004, Delhi, India, February 5-7, 2004, Revised Papers. **Fast software encryption : 5th international workshop, FSE - Easy Find** Volume 3017 of the series Lecture Notes in Computer Science pp 454-471 In this paper, we present techniques to improve the [1] attack. Our theoretical **Fast Software Encryption - 11th International Workshop, FSE Bimal** 11th International Workshop, FSE 2004, Delhi, India, February 5-7, 2004, Revised Preface Fast Software Encryption is a now eleven years old workshop on This year a total of 75 papers were submitted to FSE 2004. First Springer-Verlag for publishing the proceedings in the Lecture Notes in Computer Science series. **New Cryptographic Primitives Based on Multiword T-Functions** Fast Software Encryption. Volume 3017 of the series Lecture Notes in Computer Science pp 1-15 In this paper we develop new ways to construct invertible T-functions on multiword states Subtitle: 11th International Workshop, FSE 2004, Delhi, India, February 5-7, 2004. Revised Papers Pages: pp 1-15 Copyright: 2004 **Fast Software-Based Attacks on SecurID - Springer** Fast Software Encryption: 11th International Workshop, FSE 2004, Delhi, India, February 5-7, 2004, Revised Papers (Lecture Notes in Computer Science) **Fast software encryption : 6th International Workshop, FSE99, Rome** Conference Papers (Peer reviewed) Lecture Notes in Computer Science, 1st Workshop on Wearable Security and . Science, Fast Software Encryption 12th International Workshop, FSE 2005, Paris in Computer Science, 11th International Workshop, FSE 2004, Delhi, India, Vol. 3017, pp. 127-142, February 5-7, 2004. **Fast Software Encryption: 11th International Workshop, FSE 2004** Fast Software Encryption. Volume 3017 of the series Lecture Notes in Computer Science pp 389-407 Authenticated encryption CCM EAX message authentication CBC MAC modes of operation OMAC provable security Add to Papers . Subtitle: 11th International Workshop, FSE 2004, Delhi, India, February 5-7, 2004. Fast software encryption. 5th international workshop, FSE 98, Paris, France, March 23-25, 1998 : proceedings Series: Lecture notes in computer science 1372. Subjects: Published: (1998) Fast software encryption : 11th international workshop, FSE 2004, Delhi, India, February 5-7, 2004 revised papers by: FSE 2004 **Vulnerability of Nonlinear Filter Generators Based on Linear Finite** Volume 3017 of the series Lecture Notes in Computer Science pp 127-142 demonstrated a special technique, usually referred to as fast correlation attacks, that is very This paper identifies a new class of such weak feedback polynomials, . 11th International Workshop, FSE 2004, Delhi, India, February 5-7, 2004. **Fast Software Encryption, 11th International Workshop, FSE 2004** Fast Software Encryption. Volume 3017 of the series Lecture Notes in Computer

Science pp 94-108 In this paper, we analyze the security of the stream cipher Helix, recently proposed . Subtitle: 11th International Workshop, FSE 2004, Delhi, India, February 5-7, 2004. Revised Papers Pages: pp 94-108 Copyright: 2004 **Differential Attacks against the Helix Stream Cipher - Springer** 11th International Workshop, FSE. 2004, Delhi, India, February 5-7, 2004,. Revised Papers (Lecture Notes in. Computer Science) PDF. R.e.a.d Fast Software **Results on Rotation Symmetric Bent and Correlation Immune** Fast Software Encryption, 11th International Workshop, FSE 2004, Delhi, India, February 5-7, 2004, Revised Papers. B. Roy, and W. Meier (Eds.). . volume 3017 of Lecture Notes in Computer Science, Springer, (2004). Documents: true **Correlation Attacks Using a New Class of Weak Feedback** software encryption. second international workshop, Leuven, Belgium, December 14-16, 1994 : proceedings Series: Lecture notes in computer science 1008. Subjects: Published: (2003) Fast software encryption : 11th international workshop, FSE 2004, Delhi, India, February 5-7, 2004 revised papers by: FSE 2004 **Fast Software Encryption: 11th International Workshop, FSE 2004** Series: Lecture notes in computer science 2365. Subjects: Computers > Access control Fast software encryption : 11th international workshop, FSE 2004, Delhi, India, February 5-7, 2004 revised papers by: FSE 2004. Published: (2004) **@inproceedings{IACR:conf/fse/IwataK04, author = {Tetsu Iwata and** Fast Software Encryption: 11th International Workshop, FSE 2004, Delhi, India, February 5-7, 2004, Revised Papers (Lecture Notes in Computer Science) by **dblp: record conf/fse/2004** Fast Software Encryption. Volume 3017 of the series Lecture Notes in Computer Science pp 65-82 The three main results of this paper are the following: First, we prove that Courtois . Subtitle: 11th International Workshop, FSE 2004, Delhi, India, February 5-7, 2004. Revised Papers Pages: pp 65-82 Copyright: 2004 **Fast Software Encryption: 11th International Workshop, FSE 2004**