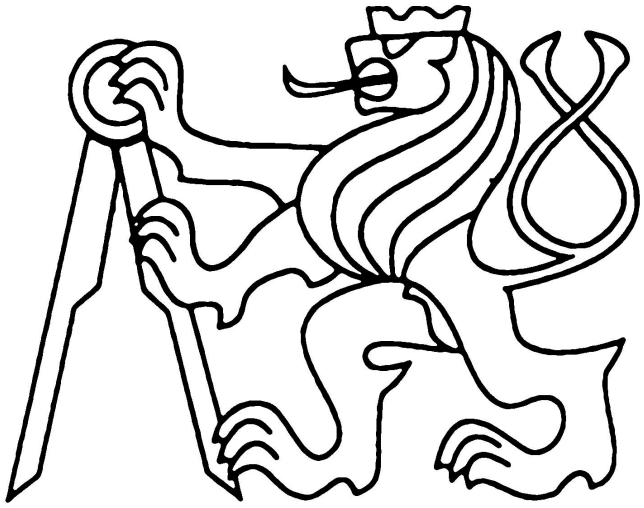
ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE



TEZE K DISERTAČNÍ PRÁCI

České vysoké učení technické v Praze
Fakulta elektrotechnická
katedra počítačů

Ing. Tomáš Rosa

MODERN CRYPTOLOGY: STANDARDS ARE NOT ENOUGH

Doktorský studijní program: Elektrotechnika a informatika
Studijní obor: 2612V025 - Informatika a výpočetní technika

Teze disertace k získání akademického titulu „doktor“, ve zkratce „Ph.D.“

Praha červenec 2004

Disertační práce byla vypracována v rámci prezenční formy doktorského studia na pracovišti katedry počítačů Fakulty elektrotechnické ČVUT v Praze.

Disertant: Ing. Tomáš Rosa
katedra počítačů
Fakulta elektrotechnická ČVUT v Praze
Karlovo náměstí 13, 121 35 Praha 2
email: t_rosa@volny.cz

Školitel: Doc. RNDr. Ing. Petr Zemánek, CSc.
katedra počítačů
Fakulta elektrotechnická ČVUT v Praze
Karlovo náměstí 13, 121 35 Praha 2
email: zemanekp@sun.felk.cvut.cz

Oponenti: .....

.....

.....

Teze byly rozeslány dne: .....

Obhajoba disertace se koná dne ..... v ..... hod. v zasedací místnosti č. ..... elektrotechnické fakulty ČVUT v Praze .... před komisí pro obhajobu disertační práce ve studijním oboru 2612V025 - Informatika a výpočetní technika.

S disertací je možno se seznámit na děkanátě elektrotechnické fakulty ČVUT v Praze, na oddělení pro vědeckou a výzkumnou činnost, Technická 2, Praha 6 – Dejvice.

Prof. Ing. Pavel Tvrdík, CSc.
předseda komise pro obhajobu disertační práce
ve studijním oboru Informatika a výpočetní technika
katedra počítačů
Fakulta elektrotechnická ČVUT v Praze
Karlovo náměstí 13, 121 35 Praha 2

Content

1. State of the Art

1.1 Modern Cryptology

Since the thesis is mainly focused on the area of *theory of applied cryptography* (as an integral part of *modern cryptology*), we will briefly show what this subject represents together with what its current state of the art is. The mainstream of applied cryptography can be seen in development and implementation of various cryptographic and security standards. Standards such as AES [34], SHA-1 [32], DSA [33], ECDSA ([33], [45]), RSA [89] or standards such as PKCS ([76], [77], [78], [79]), etc. are good examples of that. These standards are kept up-to-date and made public. However, does this mean that anyone with a basic knowledge of computer architecture and discrete mathematics can simply build up a secure cryptographic module following these standards? Also, does this tell us that all cryptographic modules using the same cryptographic standard have the same level of security? Unfortunately, it does not. The main focus of the thesis is to draw an attention on several topics of the area of applied cryptography, which are very often neglected by many security architects. These topics will be demonstrated mainly on practically feasible attacks which were or would be possible because of architects of security modules or even standards did not pay appropriate attention to certain key aspects of applied cryptography. It turns out that, despite of surviving belief of various experts, following even highly trusted security standards is simply not enough to build up a really secure security module. These standards can be used as useful hints of what we shall (not) do, but the definite responsibility of checking potential vulnerabilities of a particular security module designed is still left on their architects.

1.2 Main Issues of Modern Cryptology

There are two basic questions which seem to be so important for identifying and resolving potential vulnerabilities that even a high-skilled security architect should not regret of paying an appropriate attention to them. The first question is:

What environment shall the designed module be used in?

The main aim of every security module is to defeat certain vulnerabilities of a target system (for example an online banking application) to lower risks coming from potential threats. For this purpose, the threat is defined as an event which could cause a certain loss of subjects incorporated in using the particular application (here, it could be a threat of stealing an access to somebody's banking account, etc.). The vulnerability is then defined as a set of conditions which allow the particular threat to harm the system (here, it could be a security hole in an authentication module, etc.). Since the set of concrete threats together with their characteristics is given mainly by a concrete environment in which the designed module will be used, it is absolutely necessary to answer the first question mentioned above and to make up an accurate threat model. In such a model, we must then carefully examine as many properties of the module as we can to verify whether the module will really remove all those vulnerabilities or not. Moreover, we must also check if there are not some new vulnerabilities which would be introduced by applying this module. Otherwise, it may happen that the designed module will have such property that

would turn out to be a serious vulnerability allowing disastrous threat to occur. Although it may seem as nothing more than just repeating basis of the best designing practice, the reality shows that most of devastating attacks are possible mainly because of the fact that this code of best practice is being constantly underestimated and overlooked. For instance, ignoring physical properties of cryptographic modules (i.e. the environment which surrounds every physical device) motivated the development of a brand new, rapidly developing area of cryptanalytical techniques called *side channel cryptanalysis*. Roughly speaking, introduction of this theory (by Paul Kocher around 1996 [56]) was the time when devastating attacks returned back to the papers presented at conferences on cryptology. We may really say that it was a revolution in contemporary cryptology which, hopefully, changed the way of viewing and modeling cryptographic modules [50]. However, it will probably take some time until this theory becomes also practice. At the time of completing the thesis (spring-summer of 2004), side channel attacks are still very dangerous and very few modules can be regarded as reasonably protected against them. Therefore, most of the papers included in this thesis are focused on side channel attacks to deeply illustrate their nature and some techniques to defeat them.

The second key question is:

What is the easiest problem an attacker has to solve to break the module in some way?

As security architects, we should answer this question when we have an accurate threat model constructed in the previous step. It is important to note that, for example, identifying potential side channels would be of no benefit if we underestimate the way they would help an attacker to break into the system. The core is that traditional theoretical cryptanalysis tends to be focused on well-known, "well-hard" problems (such as factorization, discrete logarithm, etc. c.f. [64], [103]), while the particular problems an attacker has to solve in practice to be able to say that "she broke the system" are often essentially easier. Consequences of overlooking this aspect can be again easily seen from unusually good results obtained by side channel attacks. However, side channels are not the only one area where we can see that. As an example, we have also included in chapter G (see organization notes bellow) a new kind of attack on the well-known signature schemes DSA and ECDSA [33], [64], [103]. This is not a side channel attack, but it can also introduce serious weaknesses in certain systems based on a growing phenomenon of electronic signatures. Furthermore, we did not have to solve any from those "well-hard" problems (here namely the discrete logarithm problem) to do our attack. What we actually did is that we exploited such a property of these schemes which tends to be constantly overlooked by many researchers.

Certain evidences, that answering the above mentioned questions is of a crucial importance, can be seen if we look carefully at the attacks studied and presented at various conferences in the past and nowadays. The attacks discussed in the past were almost solely focused on cryptanalysis of intercepted cryptograms, while the ones presented nowadays are somehow mentioning playing an interactive game between an attacker and her victim. This naturally reflects the way in which cryptosystems are implemented into practical applications. Being in the role of the attacker, we do not have to rely solely on randomly intercepted cryptograms any more. Playing the interactive game with our victim, we can "adjust" the conditions of our attack to finally get as easiest mathematical problem to solve as possible. Although it can be perhaps a bit "disgusting"

for a beautiful mathematical mind, this subject must be studied and understood properly to tightly grasp what the contemporary cryptology is all about, which is then necessary to be able to fight with modern attackers as effectively as possible. Author's opinion here is that even in this area of so-called *theory of applied cryptography*, one can find very interesting problems for any taste of mathematical complexity and-or engineering practice. This is the main motto behind the papers written and completed in this thesis.

2. Goals of the Doctoral Thesis

The main goals of the dissertation are:

- To investigate several selected security standards which are widely used in contemporary security modules in order to see if they are designed properly according to particular key issues of modern cryptology (c.f. §1.2 above).
- To propose, elaborate, and describe possible practical attacks based on vulnerabilities found in these standards. The main focus is on the area of side channel cryptanalysis which is highly promising and rapidly growing part of contemporary cryptanalysis.
- To design and-or suggest effective countermeasures against discovered attacks.
- To contribute to a general theory of side channel cryptanalysis. Since this kind of cryptanalysis is the main tool used in the thesis, together with the fact that it is still rapidly growing, it would be desirable to try to independently generalize certain new ideas which were discovered for the purpose of the attacks presented here. We note that this goal is mainly achieved in the overviewing part of the thesis (c.f. organization of the thesis bellow) where a practical enhancement of classification methodology is proposed. Certain general results and observation are also pointed out in detailed descriptions of particular attacks.

3. Organization of the Thesis and Results Summary

The thesis consists of extended versions of papers which reflect author's results obtained during his PhD research. Each paper represents one chapter of the thesis indexed as A, B, …, G. The relevant information on how and where particular papers were published, is included as footnotes at their relevant starting pages. Short abstracts of each chapter showing the main author's results obtained follow.

3.1 Chapter A. Side Channel Cryptanalysis – An Overview

Growing theory of the side channel cryptanalysis shows the necessity of building and using general models of cryptographic modules when their security has to be examined. Traditional approach, which was used before, was to examine these modules as abstract mathematical functions without their connection to the objective physical reality. It shows that particular physical properties can prominently spread the set of vulnerabilities and available cryptanalytic techniques. From here follows their impact on the security. The information available due to particular physical properties is referred to as *side information*. The means, which the side information is transmitted by, are then referred to as *side channels*. Practically, side channels are often represented as physical magnitudes, which are in some ways related to an activity of the cryptographic module being examined (the amount of time it takes to perform some operation, the power trace, the electromagnetic emanation, etc.). This overviewing chapter presents various general aspects of the theory of side channel cryptanalysis. It introduces particular types of side channels, which are known up to now, and it sketches, how these side channels can be used for cryptanalytic purposes. It also proposes a general classification methodology which allows practically useful distinguishing between various channels and their analyses. Furthermore, it separates the terms channel, signal, analysis, and information which should also be practically beneficial.

3.2 Chapter B. Attack on Private Signature Keys of the OpenPGP format, PGP™ programs and other applications compatible with OpenPGP

In this chapter, we describe an attack on the OpenPGP format [87], which leads to a disclosure of private signature keys of the DSA [33] and RSA [89] algorithms. The OpenPGP format is used in a number of applications including PGP, GNU Privacy Guard and other programs specified on the list of products compatible with OpenPGP, which is available at http://www.pgpi.org/products. Therefore all these applications shall undergo the same revision as the actual program PGP™. The success of the attack was practically verified and demonstrated on the PGP™(*) program version 7.0.3 with a combination of the AES [34] and DH/DSS algorithms [87]. As the private signature key is the basic information of the whole system which is kept secret, it is encrypted using the strong cipher. However, we show that this protection is weak, as the attacker has neither to

(*) PGP is registered trade mark of Network Associates, Inc. All other registered and not registered trade marks listed in this document are owned by their appropriate owners.

attack this cipher nor user´s secret passphrase. A modification of the private key file in a certain manner and subsequent capturing of one signed message is sufficient for a successful attack. A vulnerability coming from an insufficient protection of the integrity of the public as well as private parts of signature keys in the OpenPGP format is analyzed. On the basis of this, a procedure of attacks is shown on both DSA and RSA private signature keys. The attacks apply to all lengths of parameters (modules, keys) of RSA and DSA. The cryptographic countermeasures for correction of the OpenPGP format as well as the PGP™ format are proposed.

3.3 Chapter C. Further Results and Considerations on Side Channel Attacks on RSA

The research presented in this chapter contains three parts. In the first part, we present a new side channel attack on a plaintext encrypted by EME-OAEP PKCS#1 v.2.1 [76]. In contrast with recent well-known Manger's attack [61], we attack directly that part of the plaintext, which is shielded by the OAEP method. In the second part, we remind that Bleichenbacher's [16] and Manger's attack on the RSA encryption scheme PKCS#1 v.1.5 and EME-OAEP PKCS#1 v.2.1 can be converted to an attack on the RSA signature scheme with any message encoding (not only PKCS). In the third part, we deploy a general idea of fault-based attacks (we introduce a notion of confirmation oracle) on the RSA-KEM [92] scheme which was suggested as a possible solution to implementation attacks (e.g. side channel attacks) which seem to be constant problems of the schemes from [76]. We present two particular attacks as examples to show that this solution is clearly not a definite one. The result of these attacks is the private key instead of the plaintext as with attacks on PKCS#1 v.1.5 and v.2.1. These attacks should highlight the fact that the RSA-KEM scheme is not an entirely universal solution to problems of RSAES-OAEP implementation and that even here the manner of implementation is significant.

3.4 Chapter D. Strengthened encryption in the CBC mode

Vaudenay [106] has presented a side channel attack on the CBC mode of block ciphers ([74], [86]), which use padding according to the PKCS#5 standard [77]. One of the countermeasures, which he assumed, consisted of the encryption of the message $M' = M \,||\, padding \,||\, hash(M \,||\, padding)$ instead of the original M, where *hash* is an appropriate cryptographic hash function. This can increase the length of the message by several blocks compared with the present padding. Moreover, Wagner [106] showed a security weakness in this proposal. The next correction, which Vaudenay proposed ("A Fix Which May Work") has a general character and doesn't solve practical problems with the real cryptographic interfaces used in contemporary applications. In this article we propose three variants of the CBC mode. From an external point of view, they behave the same as the present CBC mode with the PKCS#5 padding, but they prevent Vaudenay's attack. In this chapter, we also make use of the notion of confirmation oracle which has been introduced in chapter C.

3.5 Chapter E. Side Channel Attacks on CBC Encrypted Messages in the PKCS#7 Format

As shown by Vaudenay in [106] and also discussed in chapter D in this thesis, a CBC encryption mode ([74], [86]) combined with the PKCS#5 padding [77] scheme allows an attacker to invert the underlying block cipher, provided she has an access to a valid-padding oracle which for each input ciphertext tells her whether the corresponding plaintext has a valid padding or not. Having in mind the countermeasures against this attack, different padding schemes have been studied in [15]. The best one is referred to as the ABYT-PAD. It is designed for byte-oriented messages. It removes the valid-padding oracle, thereby defeating Vaudenay's attack, since all deciphered plaintexts are valid in this padding scheme. In this chapter, we try to combine the well-known cryptographic message syntax standard PKCS#7 [78] with the use of ABYT-PAD instead of PKCS#5. We also make use of a generalized notion of the confirmation oracle introduced in chapter C. Let us assume that we have access to a $\text{PKCS\#7}_{\text{CONF}}$ confirmation oracle that tells us for a given ciphertext (encapsulated in the PKCS#7 structure) whether the deciphered plaintext is correct or not according to the PKCS#7 (v1.6) syntax [79]. This is probably a very natural assumption, because applications usually have to reflect this situation in their behavior. It could be a message for a user, an API error message, an entry in the log file, different timing behavior, etc. We show that an access to such an oracle again enables an attacker to invert the underlying block cipher. The attack requires single captured ciphertext and approximately 128 oracle calls per one ciphertext byte. It shows that we cannot hope to fully solve problems with side channel attacks on the CBC encryption mode by using a “magic” padding method or an obscure message-encoding format. Strong cryptographic integrity checks of ciphertexts should be incorporated instead.

3.6 Chapter F. Attacking RSA-based Sessions in SSL/TLS

In this chapter, we present a practically feasible attack on RSA-based sessions in SSL/TLS protocols [85], [83]. These protocols incorporate the PKCS#1 (v. 1.5) [76] encoding method for the RSA encryption of a *premaster-secret* value. The *premaster-secret* is the only secret value that is used for deriving all the particular session keys. Therefore, an attacker who can recover the *premaster-secret* can decrypt the whole captured SSL/TLS session. We show that incorporating a version number check over PKCS#1 plaintext used in the SSL/TLS creates a side channel that allows the attacker to invert the RSA encryption. The attacker can then either recover the *premaster-secret* or sign a message on behalf of the server. Practical tests showed that two thirds of randomly chosen Internet SSL/TLS servers were vulnerable. The attack is an extension of Bleichenbacher’s attack on PKCS#1 (v. 1.5) [16]. We introduce the concept of a *bad-version oracle* (BVO) that covers the side channel leakage, and present several methods that speed up the original algorithm. Our attack was successfully tested in practice and the results of complexity measurements are presented here. Plugging a testing server (2x Pentium III/1.4 GHz, 1 GB RAM, 100 Mb/s Ethernet, OS RedHat 7.2, Apache 1.3.27), it was possible to achieve a speed of 67.7 BVO calls per second for a 1024 bits RSA key. The median time for a whole attack on the *premaster-secret* could be then estimated as 54 hours and 42 minutes. We also propose and discuss countermeasures, which are both cryptographically acceptable and practically feasible.

3.7 Chapter G. Key-collisions in (EC)DSA: Attacking Non-repudiation

A new kind of attack on the non-repudiation property [59] of digital signature schemes is presented. We introduce a notion of key-collisions, which may allow an attacker to claim that the message (presented to a judge) has been signed by someone else. We show how to compute key-collisions for the DSA and ECDSA signature schemes [33] effectively. The main idea of these attacks has been inspired by the well-known notion of message-collisions, where an attacker claims that the signature presented at the court belongs to a different message ([64], [103]). Both of these collision-based attacks significantly weaken the non-repudiation property of signature schemes. Moreover, they weaken the non-repudiation of protocols based on these schemes. It is shown that key-collision resistance of the (EC)DSA schemes requires the incorporation of a mechanism ensuring honest generation of (EC)DSA instances. The usage of such a mechanism shall be verifiable by an independent third party without revealing any secret information. We propose and discuss basic general countermeasures against key-collision attacks on the (EC)DSA schemes. We also show that the whole notion of key-collisions can be regarded as a platform for generalization of attacks discussed by Massias, Serret Avila, and Quisquater in [62]. The fact, that the area of key-collision attacks is not solved by the standard [33] itself, again emphasizes the main motto of modern cryptology saying that standards are clearly not enough.

Bibliography Used in the Thesis

1. Agrawal, D., Archambeault, B., Rao, J.-R., and Rohatgi P.: *The EM Side-Channel(s)*, in Proc. of CHES 2002, pp. 29-45, 2002
2. Agrawal, D., Rao, J.-R., and Rohatgi, P.: *Multi-channel Attacks*, in Proc. of CHES 2003, pp. 2-16, 2003
3. Akkar, M.-L., Bevan, R., Dischamp, P., and Moyart, D.: *Power Analysis, What Is Now Possible...*, in Proc. of ASIACRYPT 2000, pp. 489-502, 2000
4. Alexi, W., Chor, B., Goldreich, O., and Schnorr, C.: *RSA and Rabin functions: Certain parts are as hard as the whole*, SIAM Journal on Computing, 17(2), pp. 194-209, 1988
5. Anderson, R. and Kuhn, M.: *Low Cost Attacks on Tamper Resistant Devices*, in Proc. of Security Protocols '97, pp. 125-136, 1997
6. Anderson, R. and Kuhn, M.: *Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations*, in Proc. of Information Hiding '98, pp. 124-142, 1998
7. Anderson, R. and Kuhn, M.: *Tamper Resistance – a Cautionary Note*, in Proc. of 2nd USENIX Workshop On Electronic Commerce, pp. 1-11, 1996
8. Anderson, R.: *Security Engineering*, John Wiley & Sons, Inc., 2001
9. Aumüller, C., Bier, P., Fischer, W., Hofreiter, P., and Seifert, J.-P.: *Fault Attacks on RSA with CRT: Concrete Results and Practical Countermeasures*, in Proc. of CHES 2002, pp. 260-275, 2002
10. Bao, F., Deng, R.-H., Han, Y., Jeng, A., Narasimhalu, A.-D., and Ngair, T.: *Breaking Public Key Cryptosystems on Tamper Resistant Devices in the Presence of Transient Faults*, in Proc. of Security Protocols '97, pp. 115-124, 1997
11. Bellare, M. and Rogaway, P.: *Random Oracles are Practical: A Paradigm for Designing Efficient Protocols*, October 20, 1995, originally published in Proc. of the First ACM Conference on Computer and Communications Security, ACM, November 1993
12. Bellare, M. and Rogaway, P.: *The Exact Security of Digital Signatures – How to Sign with RSA and Rabin*, in Proc. of EUROCRYPT '96, pp. 399-416, 1996
13. Biham, E. and Shamir, A.: *Differential Fault Analysis of Secret Key Cryptosystems*, in Proc. of CRYPTO '97, pp. 513-525, 1997
14. Bishop, M.: *Computer Security – Art and Science*, Addison-Wesley, 2003
15. Black, J. and Urtubia, H.: *Side-Channel Attacks on Symmetric Encryption Schemes: The Case for Authenticated Encryption*, In Proc. of 11th USENIX Security Symposium, San Francisco 2002, pp. 327-338
16. Bleichenbacher, D.: *Chosen Ciphertexts Attacks Against Protocols Based on the RSA Encryption Standard PKCS#1*, in Proc. of CRYPTO '98, pp. 1-12, 1998
17. Blömer, J. and May, A.: *New Partial Key Exposure Attacks on RSA*, in Proc. of CRYPTO 2003, pp. 27-43, 2003
18. Boneh, D., DeMillo, R.-A., and Lipton, R.-J.: *On the Importance of Checking Cryptographic Protocols for Faults*, in Proc. of EUROCRYPT '97, pp. 37-51, 1997
19. Boneh, D.: *Twenty Years of Attacks on the RSA Cryptosystems*, Notices of the American Mathematical Society, vol. 46, no. 2, pp. 203-213, 1999

20. Brown, D.-R.-L.: *Generic Groups, Collision Resistance, and ECDSA*, IEEE 1363, February 2002
21. Canvel, B., Hiltgen, A., Vaudenay, S., and Vaugnoux, M.: *Password Interception in a SSL/TLS Channel*, In proc. of CRYPTO '03, pp. 583-599, 2003
22. Chari, S., Jutla, C.-S., Rao, J.-R., and Rohatgi, P.: *Towards Sound Approaches to Counteract Power-Analysis Attacks*, in Proc. of CRYPTO '99, pp. 398-411, 1999
23. Chari, S., Rao, J.-R., and Rohatgi, P.: *Template Attacks*, in Proc. of CHES 2002, pp. 13-28, 2002
24. Clavier, C., Coron, J.-S., and Dabbous, N.: *Differential Power Analysis in the Presence of Hardware Countermeasures*, in Proc. of CHES 2000, pp. 253-263, 2000
25. Clulow, J.: *On the Security of PKCS #11*, In proc. of CHES 2003, pp. 411-425, 2003
26. Coron, J.-S. and Goubin, L.: *On Boolean and Arithmetic Masking against Differential Power Analysis*, in Proc. of CHES 2000, pp. 231-237, 2000
27. Dhem, J.-F., Koeune, F., Leroux, P.-A., Mestré, P., and Quisquater, J.-J. and Willems, J. - L.: *A Practical Implementation of the Timing Attack*, Technical Report CG-1998/1, 1998
28. EESSI - *The European Electronic Signature Standardization Initiative*, c.f. the homepage at http://www.ict.etsi.org/eessi/EESSI-homepage.htm
29. ElGamal, T.: *A public key cryptosystem and a signature scheme based on discrete logarithms*, IEEE Transactions on Information Theory, Vol. 31, pp. 469–472, IEEE, 1985
30. E-SIGN - *The Electronic Signatures in Global and National Commerce Act*, enacted on June 30, 2000, c.f. http://www.cybercrime.gov/esign.htm
31. FIPS PUB 140-2: *Security Requirements for Cryptographic Modules*, National Institute of Standards and Technology, Issued May 25 2001, http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
32. FIPS PUB 180-1: *Secure Hash Standard (SHA-1)*, National Institute of Standards and Technology, January 2001
33. FIPS PUB 186-2: *Digital Signature Standard (DSS)*, National Institute of Standards and Technology, January 27, 2000, update: October 5, 2001
34. FIPS PUB 197: *Advanced Encryption Standard (AES)*, National Institute of Standards and Technology, November 26, 2001
35. Fischlin, R. and Schnorr, C.-P.: *Stronger Security Proofs for RSA and Rabin Bits*, in Proc. of EUROCRYPT '97, pp. 267-279, 1997
36. Fischlin, R. and Schnorr, C.-P.: *Stronger Security Proofs for RSA and Rabin Bits*, Journal of Cryptology, Vol. 13, No. 2, pp. 221-244, IACR, 2000
37. Fouque, P.-A., Martinet, G., and Poupard, G.: *Attacking Unbalanced RSA-CRT Using SPA*, in Proc. of CHES 2003, pp. 254-268, 2003
38. Fujisaki, E., Okamoto, T., Pointcheval, D., and Stern, J.: *RSA-OAEP Is Secure under the RSA Assumption*, in Proc. of CRYPTO 2001, pp. 260-274, 2001
39. Gandolfi, K., Mourtel, C., and Olivier, F.: *Electromagnetic Analysis: Concrete Results*, in Proc. of CHES 2001, pp. 251-261, 2001
40. Goubin, L. and Patarin, J.: *DES and differential power analysis*, in Proc. of CHES '99, pp. 158-172, 1999

41. Håstad, J. and Näslund, M.: *The Security of Individual RSA Bits*, in Proc. of FOCS '98, pp. 510 - 521, 1998
42. IEEE P1363: *Standard Specifications for Public Key Cryptography*, August 1998. c.f. http://grouper.ieee.org/groups/1363
43. ITU-T Recommendation X.680 (1997), ISO/IEC 8824-1:1998, *Information Technology - Abstract Syntax Notation One (ASN.1)*: Specification of Basic Notation
44. ITU-T Recommendation X.690 (1997), ISO/IEC 8825-1:1998, *Information Technology - ASN.1 Encoding Rules*: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)
45. Johnson, D., Menezes, A.-J., and Vanstone, S.-A.: *The Elliptic Curve Digital Signature Algorithm (ECDSA)*, International Journal of Information Security, Vol 1, Issue 1, pp. 36-63, Springer-Verlag, 2001
46. Jonsson, J. and Kaliski, B.-S., Jr.: *On the Security of RSA Encryption in TLS*, in Proc. of CRYPTO '02, pp. 127 -142, 2002
47. Joy, M., Lenstra, A.-K., and Quisquater, J.-J.: *Chinese Remaindering Based Cryptosystems in the Presence of Faults*, Journal of Cryptology, Volume 12, Number 4, pp. 241-245, Autumn 1999
48. Joye, M. and Quisquater, J.-J.: *Faulty RSA Encryption*, Technical Report CG-1997/8, 1997
49. Joye, M., Koeune, F., and Quisquater, J.-J.: *Further results on Chinese Remaindering*, Technical Report GC-1997/1, 1997
50. Joye, M., Koeune, F., Preneel, B., Rohatgi, P., Seifert, J.-P., and Walter, C.: *Are software and hardware counter-measures winning the war against side-channel leakage?*, panel session at CHES 2003, 2003
51. Joye, M., Lenstra, A.-K., and Quisquater, J.-J.: *Chinese remaindering cryptosystems in the presence of faults*, Journal of Cryptology, Volume 12, Number 4, pp. 241-245, Autumn 1999
52. Kelsey, J., Schneier, B., Wagner, D., and Hall, C.: *Side Channel Cryptanalysis of Product Ciphers*, in Proc. of ESORICS '98, pp. 97-110, 1998
53. Kiayias, A. and Yung, M.: *Breaking and Repairing Asymmetric Public-Key Traitor Tracing*, in Proc. of the 2002 ACM Workshop on Digital Rights Management, 2002
54. Kocher, P., Jaffe, J., and Jun, B.: *Differential Power Analysis: Leaking Secrets*, in Proc. of CRYPTO '99, pp. 388-397, 1999
55. Kocher, P., Jaffe, J., and Jun, B.: *Introduction to Differential Power Analysis and Related Attacks*, Technical Report, 1998, http://www.cryptography.com/dpa/technical
56. Kocher, P.: *Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems*, in Proc. of CRYPTO '96, pp. 104-113, 1996
57. Kömmerling, O. and Kuhn, M.: *Design Principles for Tamper-Resistant Smartcard Processors*, in Proc. of USENIX Workshop on Smartcard Technology, pp. 9-20, 1999
58. Krawczyk, H.: *The Order of Encryption and Authentication for Protecting Communications (or: How Secure Is SSL?)*, CRYPTO' 01, pp. 310 - 331, Springer-Verlag, 2001

59. Landwehr, C.-E.: *Computer Security*, International Journal of Information Security, Vol 1, Issue 1, pp. 3-13, Springer-Verlag, 2001
60. Lenstra, A.-K.: *Memo on RSA signature generation in the presence of faults*, manuscript, Sept. 28, 1996, available from author, partially published in [51]
61. Manger, J.: *A Chosen Ciphertext Attack on RSA Optimal Asymmetric Encryption Padding (OAEP) as Standardized in PKCS #1*, in Proc. of CRYPTO'01, pp. 230-238, 2001
62. Massias, H., Serret Avila, X., and Quisquater, J.-J.: *Timestamps: Main issues on their use and implementation*, In Proc. of IEEE 8th International Workshop on Enabling Technologies: Infrastructures for Collaborative Enterprises-Fourth International Workshop on Enterprise Security, pp. 178-183, June 1999
63. Mayer-Sommer, R.: *Smartly Analyzing the Simplicity and the Power of Simple Power Analysis on Smartcards*, in Proc. of CHES 2000, pp. 78-92, 2000
64. Menezes, A.-J., van Oorschot, P.-C., and Vanstone, S.-A.: *Handbook of Applied Cryptography*, CRC Press, 1996
65. Messegers, T.-S., Dabbish, E.-A., and Sloan, R.-H.: *Investigations of Power Analysis Attacks on Smartcards*, in Proc. of USENIX Workshop on Smartcard Technology, pp. 151-161, 1999
66. Messerges, T.-S., Dabbish, E.-A., and Sloan, R.-H.: *Power Analysis Attacks of Modular Exponentiation in Smartcards*, in Proc. of CHES '99, pp. 144-157, 1999
67. Messerges, T.-S.: *Securing the AES Finalists Against Power Analysis Attacks*, in Proc. of FSE 2000, pp. 150-164, 2000
68. Messerges, T.-S.: *Using Second-Order Power Analysis to Attack DPA Resistant Software*, in Proc. of CHES '00, pp. 238-251, 2000
69. Microsoft: *MSDN Library - July 2001*, Platform SDK Documentation, Security, Cryptography, 2001
70. Millen, J.: *20 Years of Covert Channel Modeling and Analysis*, in Proc. of the 1999 IEEE Symposium on Security and Privacy, pp. 113-114, 1999
71. Millen, J.: *Covert Channel Capacity*, in. Proc. of 1987 EEE Symposium on Research in Security and Privacy, pp. 60-65, 1987
72. Muir, J.-A.: *Techniques of Side Channel Cryptanalysis*, A thesis presented to the University of Waterloo, Canada, 2001, available at http://www.math.uwaterloo.ca/~jamuir/sidechannel.htm
73. Nguyen, P.-Q. and Shparlinski, I.-E.: *The Insecurity of the Digital Signature Algorithm with Partially Known Nonces*, Journal of Cryptology, Vol. 15, 3/2002, pp. 151-176, Springer-Verlag, 2002
74. NIST Special Publication: *SP 800-38A 2001 ED - Recommendation for Block Cipher Modes of Operation*, December 2001
75. OpenSSL: *OpenSSL ver. 0.9.7*, http://www.openssl.org/, December 31, 2002
76. PKCS#1 v2.1: *RSA Cryptography Standard*, RSA Labs, DRAFT2, January 5 2001
77. PKCS#5 v2.0: *Password-Based Cryptography Standard*, RSA Laboratories, March 25, 1999
78. PKCS #7 v1.5: *Cryptographic Message Syntax Standard*, RSA Laboratories, November 1, 1993
79. PKCS #7 v1.6 (DRAFT): *Extensions and Revisions to PKCS #7*, An RSA Laboratories Technical Note, May 13, 1997

80. Pohlig, S.-C. and Hellman, M.-E.: *An improved algorithm for computing logarithms over GF(p) and its cryptographic significance*, IEEE Trans. Inform. Theory, 24 (1978), 106-110
81. Quisquater, J.-J. and Samyde, D.: *Eddy current for magnetic analysis with active sensor*, In Proc. of Esmart 2002, 3rd edition, 2002
82. Rao, J.-R and Rohatgi, P.: *EMpowering Side-Channel Attacks*, preliminary technical report, May 11 2001, available from authors
83. Rescorla, E.: *SSL and TLS: Designing and Building Secure Systems*, Addison-Wesley, New York, 2000
84. RFC 1321: Rivest, R.: *The MD5 Message-Digest Algorithm*, April 1992
85. RFC 2246: Allen, C. and Dierks, T.: *The TLS Protocol*, Version 1.0, January 1999
86. RFC 2268: Baldwin, R. and Rivest, R.: *The RC5, RC5-CBC, RC5-CBC-Pad, and RC5-CTS Algorithms*, October 1996
87. RFC 2440: Callas, J., Donnerhacke, L., Finney, H., and Thayer, R.: *OpenPGP Message Format*, November 1998
88. RFC 2631: Rescorla, E.: *Diffie-Hellman Key Agreement Method*, June 1999
89. Rivest, R., L., Shamir, A., and Adleman, L.: *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*, Communications of the ACM, 21, pp. 120-126, 1978
90. Rosen, K.-H., Michels, J.-G., Gross, J.-L., Grossman, J.-W., and Shier, D.-R.: *Handbook of Discrete and Combinatorial Mathematics*, CRC Press, 2000
91. RSA Labs: *Prescriptions for Applications that are Vulnerable to the Adaptive Chosen Ciphertext Attack on PKCS #1 v1.5*, RSA Laboratories, http://www.rsasecurity.com/rsalabs/pkcs1/prescriptions.html
92. Shoup, V.: *A Proposal for an ISO Standard for Public Key Encryption (version 2.0)*, September 17, 2001
93. Shoup, V.: *OAEP Reconsidered (Extended Abstract)*, in Proc. of CRYPTO 2001, pp. 239-259, 2001
94. Schaumont, P. and Verbauwhede, I.: *Domain-Specific Codesign for Embedded Security*, Computer, April 2003, Vol. 36, No. 4, pp. 68-74, IEEE Computer Society, 2003
95. Schindler, W.: *A Timing Attack against RSA with the Chinese Remainder Theorem*, in Proc. of CHES 2000, pp. 109-124, 2000
96. Schneier, B. and Wagner, D.: *Analysis of the SSL 3.0 Protocol*, The Second USENIX Workshop on Electronic Commerce Proceedings, USENIX Press, November 1996, pp. 29 - 40
97. Schnorr, C.-P.: *Efficient Signature Generation by Smart Cards*, Journal of Cryptology, Vol. 4, pp. 161–174, Springer-Verlag, 1991
98. Simons, G.-J.,: *The History of Subliminal Channels*, IEEE Journal of Selected Areas in Communications, vol. 16, n. 4, pp. 452-462, April 1998
99. Skorobogatov, S.: *Copy Protection in Modern Microcontrollers*, Technical Report, 2000, http://www.cl.cam.ac.uk/~sps32/mcu_lock.html
100. Skorobogatov, S.-P. and Anderson, R.-J.: *Optical Fault Induction Attacks*, In proc. of CHES 2002, pp. 2-12, Springer-Verlag, 2003
101. Smulders, P.: *The Threat of Information Theft by Reception of Electromagnetic Radiation from RS-232 Cables*, Computers & Security vol. 9, pp. 53-58, 1990

102. Stern, J., Pointcheval, D., Malone-Lee, J., and Smart, N.-P.: *Flaws in Applying Proof Methodologies to Signature Schemes*, in Proc. of CRYPTO 2002, LNCS 2442, pp. 93-110, Springer-Verlag, 2002
103. Stinson, D., R.: *Cryptography – Theory and Practice*, CRC Press, 1995
104. van Eck, W.: *Electromagnetic Radiation from Video Display Units: an Eavesdropping Risk?*, Computers & Security vol. 4, pp. 269-286, 1985
105. Vaudenay, S.: *Hidden Collisions on DSS*, in Proc. of CRYPTO '96, pp. 83-88, Springer-Verlag, 1996
106. Vaudenay, S.: *Security Flaws Induced By CBC Padding - Application to SSL, IPSEC, WTLS...*, EUROCRYPT '02, pp. 534-545, Springer-Verlag, 2002
107. X509: ITU-T Recommendation X.509 (06/97) - *Information Technology - Open System Interconnection - The Directory*: Authenticantion Framework, ITU, 1997
108. Yen, S.-H., Moon, S.-J., Ha, J.-C.: *Permanent Fault Attack on the Parameters of RSA with CRT*, In Proc. of ACISP 2003, pp. 285-296, 2003
109. Young, A. and Yung, M.: *Kleptography: Using Cryptography Against Cryptography*, in Proc. of EUROCRYPT '97, pp. 62-74, 1997

Bibliography of Author Related to the Thesis

Side Channel Cryptanalysis

A1. Rosa, T.: *Vliv architektury kryptografických modulů na bezpečnost (Kryptografie v klidu a bezpečí)*, CHIP 2/2001, str. 137–139, 2001

A2. Rosa, T.: *Kocherův útok (Kryptografie v klidu a bezpečí (2))*, CHIP 3/2001, str. 140-142, 2001

A3. Rosa, T.: *Diferenciální časová analýza (Kryptografie v klidu a bezpečí (3))*, CHIP 4/2001, str. 179-181, 2001

A4. Rosa, T.: *Napěťově-proudové postranní kanály (Kryptografie v klidu a bezpečí (4))*, CHIP 6/2001, str. 180 – 182, 2001

A5. Rosa, T.: *Analýza typu OBA (Kryptografie v klidu a bezpečí (5))*, CHIP 7/2001, str. 148-150, 2001

A6. Rosa, T.: *Chybové postranní kanály (Kryptografie v klidu a bezpečí (6))*, CHIP 9/2001, str. 172-175, 2001

A7. Klíma, V., Rosa, T.: *Útok na privátní podpisové klíče PGP: Czech attack*, CHIP 5/2001, str. 164-167, 2001 (60%)

A8. Klíma, V. and Rosa, T.: *Attack on Private Signature Keys of the OpenPGP format, PGP (TM) Programs and Other Applications Compatible with OpenPGP*, IACR ePrint archive, 2002/076, http://eprint.iacr.org, 2001 (60%)

A9. Rosa, T.: *O ochraně privátních klíčů v bezpečnostních systémech*, ve sborníku semináře Bezpečnost dat v počítačových systémech, DCD Publishing, Praha, 24.4. - 25.4. 2001

A10. Rosa, T.: *Future Cryptography: Standards are not Enough*, in Proc. of Security and Protection of Information 2001, Military Academy in Brno, pp. 237-245, Brno, NATO-IDET 9.5. - 11.5. 2001

A11. Rosa, T.: *O postranních kanálech v kryptoanalýze*, ve sborníku XVIII. konference EurOpen.CZ, EurOpen.CZ, Malá Úpa, 11.6 - 13.6. 2001

A12. Rosa, T.: *Kryptoanalýza s využitím postranních kanálů*, ve sborníku příspěvků Vojenská kryptografie IV, konference pořádaná Vojenským bezpečnostním úřadem Praha a Vojenskou akademií v Brně, str. 113 – 156, Brno, 30.10. - 31.10. 2001

A13. Klíma, V., Rosa, T.: *O postranních kanálech, nové maskovací technice a jejím konkrétním využití proti Mangerovu útoku na PKCS#1*, ve sborníku MKB2001, str. 57–72, Ecom-monitor, 2001 (60%)

A14. Klíma, V., Rosa, T.: *Postranní kanály a RSAES-OAEP (RSA v novém světle (1))*, CHIP 11/2001, str. 172-175, 2001 (60%)

A15. Klíma, V., Rosa, T.: *Postranní kanály a RSAES-OAEP (RSA v novém světle (2))*, CHIP 12/2001, str. 180-183, 2001 (60%)

A16. Klíma, V., Rosa, T.: *Postranní kanály a RSAES-OAEP (RSA v novém světle (3))*, CHIP 1/2002, str. 126-129, 2002 (60%)

A17. Klíma, V., Rosa, T.: *Postranní kanály a RSAES-OAEP (RSA v novém světle (4))*, CHIP 2/2002, str. 134-137, 2002 (60%)

A18. Klíma, V., Rosa, T.: *Vybrané aspekty moderní kryptoanalýzy*, Sdělovací technika 3/2003, str. 3-7, 2003 (50%)

A19. Klíma, V., Rosa, T.: *Postranní kanály - moderní hrozby informačních a komunikačních systémů*, konference Informačná bezpečnosť 2002, Bratislava, 6.11. 2002 (60%)
A20. Klíma, V. and Rosa, T.: *Further Results and Considerations on Side Channel Attacks on RSA*, In proc. of CHES 2002, San Francisco Bay, USA, August 2002, pp. 245-260, Springer-Verlag, 2003 (60%)
A21. Klíma, V. and Rosa, T.: *Side Channel Attacks on CBC Encrypted Messages in the PKCS#7 Format*, In Proc. of 2nd International Scientific Conference: Security and Protection of Information, pp. 75-83, NATO PfP/PWP, Brno, Czech Republic, 28. - 30.4. 2003 (60%)
A22. Klíma, V. and Rosa, T.: *Side Channel Attacks - Highly Promising Directions in Modern Cryptanalysis*, TATRACRYPT '03, The 3rd Central European Conference on Cryptology, Bratislava, Slovakia, June 26-28, 2003 (50%)
A23. Klíma, V., Pokorný, O., and Rosa, T.: *Attacking RSA-based Sessions in SSL/TLS*, in Proc. of CHES '03, Cologne, Germany, September 7-11, pp. 426-440, Springer-Verlag, 2003 (60%)

General Cryptanalysis

A24. Rosa, T.: *Faktorizace velkých čísel pomocí TWINKLE (Na to vezmi LED!)*, CHIP 8/99, str. 40-43, 1999
A25. Rosa, T.: *Řešení problému diskrétního logaritmu pomocí TWINKLE (Na to vezmi LED! (2))*, 9/99, str. 34-37, 1999
A26. Rosa, T.: *Faktorizace RSA-155 (Jde to i bez Twinklu)*, CHIP 10/99, str. 30-30, 1999
A27. Klíma, V. a Rosa, T.: *Luštění šifry A5 v GSM (1) (Šifra v GSM prolomena! (1))*, CHIP 2/2000, str. 38-41, 2000
A28. Klíma, V. a Rosa, T.: *Luštění šifry A5 v GSM (2) (Šifra v GSM prolomena! (2))*, CHIP 3/2000, str. 42-44, 2000
A29. Rosa, T.: *Hledání kolizí hašovacích funkcí hrubou silou (Podpis k narozeninám)*, CHIP 8/2001, str. 131-133, 2001
A30. Rosa, T.: *On Key-collisions in Signature Schemes*, in Proc. of the workshop VKB 2002 (Czech language), pp. 14-26, Brno, April 3.-4., 2002
A31. Rosa, T.: *Klíčové kolize v podpisových schématech – upozornění na nedostatky slovenské vyhlášky č. 542/2002 Z.z.*, konference Informačná bezpečnosť 2002, Bratislava, 6.11. 2002
A32. Rosa, T.: *Hrozba klíčových kolizí v podpisových schématech (Kdopak se to vlastně podepsal?!)*, CHIP 12/2002, str. 170 – 173, 2002
A33. Rosa, T.: *On Key-collisions in (EC)DSA Schemes*, CRYPTO 2002 Rump Session, IACR ePrint archive 2002/129, Santa Barbara, USA, August 2002
A34. Rosa, T.: *Nepopiratelnost digitálních podpisů*, přijato na vědecko-pedagogickou konferenci Právní regulace společnosti informačních sítí, Západomoravská vysoká škola, Třebíč, 27. září 2004

Applied Cryptography

A35. Klíma, V., Rosa, T.: *O generátoru pseudonáhodných čísel Yarrow (Rukavice hozená hackerům)*, CHIP 5/2000, str. 50-53, 2000 (50%)
A36. Rosa, T.: *Obecné principy digitálního podpisu (Podpis pro pokročilé)*, CHIP 11/2000, str. 174-178, 2000
A37. Rosa, T.: *Obecné principy digitálního podpisu 2 (Podpis pro pokročilé 2)*, CHIP 12/2000, str. 172 – 176, 2000
A38. Rosa, T.: *Vybrané problémy podpisových schémat*, CHIP 1/2001, str. 134-137, 2001
A39. Klíma, V. and Rosa, T.: *Strengthened Encryption in the CBC Mode*, IACR ePrint archive 2002/061, May 2002 (50%)
A40. Klíma, V., Rosa, T.: *Kryptologie pro praxi - úvodní seznámení*, Sdělovací technika 6/2003, str. 19-19, 2003 (50%)
A41. Klíma, V., Rosa, T.: *Kryptologie pro praxi - druhy schémat*, Sdělovací technika 7/2003, str. 16-16, 2003 (50%)
A42. Klíma, V., Rosa, T.: *Kryptologie pro praxi - asymetrická schémata*, Sdělovací technika 8/2003, str. 22-22, 2003 (50%)
A43. Klíma, V., Rosa, T.: *Kryptologie pro praxi - symetrická schémata*, Sdělovací technika 9/2003, str. 16-16, 2003 (50%)
A44. Klíma, V., Rosa, T.: *Kryptologie pro praxi - formátování a bezpečnost*, Sdělovací technika 10/2003, str. 16-17, 2003 (50%)
A45. Klíma, V., Rosa, T.: *Kryptologie pro praxi - nejpoužívanější šifry*, Sdělovací technika 11/2003, str. 16-17, 2003 (50%)
A46. Klíma, V., Rosa, T.: *Kryptologie pro praxi - tipy a triky*, Sdělovací technika 12/2003, str. 18-19, 2003 (50%)
A47. Klíma, V., Rosa, T.: *Kryptologie pro praxi - funkce HMAC*, Sdělovací technika 2/2004, str. 17-17, 2004 (50%)
A48. Klíma, V., Rosa, T.: *Kryptologie pro praxi - metoda RSA*, Sdělovací technika 3/2004, str. 17-17, 2004 (50%)
A49. Klíma, V., Rosa, T.: *Kryptologie pro praxi - DSA, ECDSA*, Sdělovací technika 4/2004, str. 17-17, 2004 (50%)
A50. Klíma, V., Rosa, T.: *Kryptologie pro praxi - protokol D-H*, Sdělovací technika 5/2004, str. 16-16, 2004 (50%)
A51. Klíma, V., Rosa, T.: *Kryptologie pro praxi - schémata ElGamal*, Sdělovací technika 6/2004, str. 16-16, 2004 (50%)
A52. Klíma, V., Rosa, T.: *Kryptologie pro praxi - volba klíče*, Sdělovací technika 7/2004, str. 16-17, 2004 (50%)

Others

A53. Rosa, T.: *Elementární principy bezpečnostních kódů (V klidu a bezpečí (1))*, CHIP 10/99, str. 184-187, 1999
A54. Rosa, T.: *Elementární principy bezpečnostních kódů 2 (V klidu a bezpečí (2))*, CHIP 11/99, str. 162-164, 1999
A55. Rosa, T.: *Lineární kódy (V klidu a bezpečí (3))*, CHIP 12/99, str. 174-176, 1999

A56. Rosa, T.: *Hammingovy kódy (V klidu a bezpečí (4))*, CHIP 1/2000, str. 142-144, 2000
A57. Rosa, T.: *Golayovy kódy (V klidu a bezpečí (5))*, CHIP 2/2000, str. 147-149, 2000
A58. Rosa, T.: *Úpravy parametrů bezpečnostních kódů (V klidu a bezpečí (6))*, CHIP 4/2000, str. 182-185, 2000
A59. Rosa, T.: *Reedovy-Mullerovy kódy (V klidu a bezpečí (7))*, CHIP 5/2000, str. 178-180, 2000
A60. Rosa, T.: *Algebraické struktury pro cyklické kódy (V klidu a bezpečí (8))*, CHIP 6/2000, str. 178-180, 2000
A61. Rosa, T.: *Konstrukce cyklických kódů (V klidu a bezpečí (9))*, CHIP 7/2000, str. 162-165, 2000
A62. Rosa, T.: *Efektivní algoritmy pro cyklické kódy 1(V klidu a bezpečí (10))*, CHIP 8/2000, str. 162-165, 2000
A63. Rosa, T.: *Efektivní algoritmy pro cyklické kódy 2 (V klidu a bezpečí (11))*, CHIP 9/2000, str. 178-181, 2000
A64. Rosa, T.: *Problematika shlukových chyb (V klidu a bezpečí (12))*, CHIP 10/2000, str. 186-190, 2000
A65. Rosa, T.: *Čipové karty jako autentizační prostředky*, Security Magazín, červenec-srpen/2000, str. 44-47, 2000
A66. Rosa, T.: *Význam modulu CSP pro bezpečnost IS, reakce na nové trendy v kryptografii*, ve sborníku konference Současnost a budoucnost krizového managementu, kapitola 25, Praha, 29.11. - 30.11. 2000
A67. Kupča, V. a Rosa, T.: *Theory and Perspectives of Quantum Computers*, in Proc. of Workshop 2001 - Part A, CTU Prague, 2001 (75%)
A68. Rosa, T.: *Kvantové počítače a kryptografie (Od bitů ke qubitům (1))*, CHIP 3/2002, str. 148 – 152, 2002
A69. Rosa, T.: *Kvantové počítače a kryptografie (Od bitů ke qubitům (2))*, CHIP 4/2002, str. 154 – 158, 2002
A70. Rosa, T.: *Kvantové počítače a kryptografie (Od bitů ke qubitům (3))*, CHIP 5/2002, str. 138 – 141, 2002
A71. Rosa, T.: *TWINKLE jako nestandardní řešení faktorizace*, zvaná přednáška na semináři Kvantové počítání, Ústav informatiky, Akademie věd ČR, 2. května 2002
A72. Rosa, T.: *Comment on Quantum Cryptography*, short column in the IEEE Spectrum, September 2002
A73. Klíma, V., Kratochvíl, L., Rosa, T.: *Postranní kanály, sémantická bezpečnost komunikačních protokolů a zařízení BOB*, konference Technické aspekty informační války, Vojenská akademie v Brně, 10.12. 2002 (33%)
A74. Rosa, T.: *Bezpečnostní politika – dokument mnoha tváří a účelů*, ve sborníku konference IT Security 2004, Insitute for International Research, Wien, Praha 30.-21. března 2004

Responses and Citations

[A8] The article received worldwide attention, it was echoed in the New York Times (http://www.nytimes.com/2001/03/21/technology/21CODE.html), on international PGP page http://www.pgpi.org, and on several other PGP security related web pages, including the well-known and respected page http://www.mccune.cc/PGPpage2.htm. As a consequence of the attack presented, PGP 8.0.2 has been updated to prevent this kind of attack. Inherent countermeasures were also included in the project GnuPG (http://www.gnupg.org).

> Cited in: Clulow, J.: *On the Security of PKCS #11*, In proc. of CHES 2003, pp. 411-425, Springer-Verlag, 2003

[A20]

> Cited in: Clulow, J.: *On the Security of PKCS #11*, In proc. of CHES 2003, pp. 411-425, Springer-Verlag, 2003
>
> Dottax, E.: *Fault and chosen modulus attacks on some NESSIE asymmetric primitives*, the NESSIE initiative research document, 2003
>
> Dottax, E.: *Fault Attacks on NESSIE Signature and Identification Schemes*, the NESSIE initiative research document, 2003
>
> Oswald, E. and Preneel, B.: *A Survey on Passive Side-Channel Attacks and their Countermeasures for the NESSIE Public-Key Cryptosystems*, the NESSIE initiative research document, 2004

[A23] The article received worldwide attention, several cryptographic libraries were patched, including the OpenSSL project which was a prime target of the attack (http://www.openssl.org/news/secadv_20030319.txt). In the world, it has become known as “Klima-Pokorny-Rosa attack” or simply “KPR-attack”.

[A30] The article received the best presentation award from the program committee of the workshop VKB 2002. The ideas presented here were independently experimentally verified and extended later on by a team led by Prof. Otokar Grošek, Slovak University of Technology in Bratislava, Faculty of Electrical Engineering and Information Technology, Department of Mathematics – CRYPTOGROUP (grosek@kmat.elf.stuba.sk).

[A33]

> Cited in: Granboulan, L.: *PECDSA - How to build a DL-based digital signature scheme with the best proven security*, the NESSIE initiative research document NES/DOC/ENS/WP5/022/1, 2002
>
> Федюкович, В.: *Совпадения электронных подписей*, 24 декабря 2003 г. Author shows an extension of the original attack on the Ukraine standard DSTU 4145-2002.

[A74] According to an audience vote, the article received grade 1.8 on the interval <1, 6>, where 1 means excellent. Mean value of the audience vote was 1.9 counted over all articles presented on the workshop. Source: a signed letter from the Institute of International Research, Wien.

Summary

The results collected in the thesis show that a proper design of a particular cryptosystem in an *abstract mathematical form* is one thing, but its implementation into a physical device is another one. The main security risk here comes from evaluating only the mathematical properties of the designed cryptosystem, while at the same time underestimating the physical properties the system will have after its implementation in the *real world*. It has been also shown that another possible risk comes from evaluating only certain selected properties of the cryptosystem while omitting some essential aspects closely related to concrete demands of particular information system in which the cryptosystem shall be used. Such problems occur, for instance, in applications where cryptographic mechanisms enter an area of law. A good example of such a service is the worldwide growing initiative of *electronic signature standards and laws*. It turns out here that contemporary cryptographic mechanisms must not only protect data, but also be judiciously sound.

The biggest issue of real-world cryptographic applications probably follows from a threat of *side channels*. Almost all physical properties (including an electromagnetic emanation) of the cryptographic module that can be precisely measured or carefully altered can be used for some kind of *side channel attack*. These attacks, however, are not visible in the pure mathematical description of the given cryptosystem. The discovery of side channels is definitely one of the most significant events in the recent cryptanalysis. In the rapidly nascent side channels general theory, it becomes obvious that the cryptology (especially its important area called *applied cryptography*) is a very multidisciplinary science that combines a very wide range of purely mathematical disciplines together with certain knowledge about physics, computer science, and electrical engineering. Briefly speaking, the cryptology itself balances on the edge between mathematics and physics. If we exaggerate a little bit, we can rather talk about sort of *physical mathematics* here, where we borrowed the term *mathematical physics* and reversed the order of the disciplines names.

The side channels theory also significantly influences some of the well-established cryptographic principles. As one example for all, let us mention the concept of a *perfect secrecy* (also known as an *absolute security*). Informally speaking, this term refers to cryptographic constructions for which the possibility of cryptoanalysis can be totally eliminated regardless of the attacker's computing power. From this point of view, the *Vernam's Cipher* has become renowned which is absolutely secure if applied properly. However, if we do not consider side channels effect when evaluating a system, the concept of the perfect secrecy is not very beneficial for us. Information that we suppose not to be available to an attacker can actually leak out unnoticed from one of the side channels. Of course, this does not mean that the perfect secrecy term will necessarily die out. What it means is that constructing the proof of absolute security always has to be based on such a description of the evaluated cryptosystem, which corresponds with the physical reality (i.e. includes an accurate description of threatening side channels).

The general conclusion of the thesis is that the security of a particular cryptographic module does not depend only on the cryptographic standards employed. It is also a question of the way in which these standards are implemented as well as of the environment in which the module is to be used. Therefore, we can conclude that standards are clearly not enough in themselves for developing really secure security modules.

Resumé

Výsledky prezentované v disertační práci ukazují, že korektní návrh daného kryptosystému v *abstraktní matematické formě* je jedna věc, zatímco jeho správná implementace do konkrétního zařízení podléhajícího fyzikálním zákonům je věc druhá. Hlavní bezpečnostní riziko zde vyplývá z vyhodnocení pouze matematických vlastností navrhovaného systému, přičemž fyzikální vlastnosti, které systém bude mít po jeho implementaci v *reálném světě*, jsou podceněny. Dále je ukázáno, že existuje i riziko vyplývající ze zaměření se na určité vybrané vlastnosti kryptosystému, zatímco jiné podstatné aspekty úzce spojené s konkrétními požadavky informačního systému, ve kterém má být schéma nasazeno, jsou opomenuty. Takové problémy vznikají například v aplikacích, kde se kryptografické mechanizmy dostávají do spojení s právním systémem. Příkladem zde může být celosvětově probíhající iniciativa v oblasti legislativy a standardizace *elektronického podpisu*. Zde se jasně ukazuje, že kryptografické mechanizmy musí nejen chránit data, ale navíc musí být ještě legislativně uchopitelné.

Nejpalčivější problém kryptografických aplikací v reálném světě pravděpodobně plyne z hrozby *postranních kanálů*. Téměř všechny fyzikální veličiny (včetně elektromagnetického vyzařování) týkající se nějakého kryptografického modulu, které mohou být přesně měřeny nebo citlivě upraveny, mohou být použity pro nějaký druh *útoku postranním kanálem*. Tyto útoky ovšem nejsou viditelné s použitím čistě matematického popisu daného modulu. Objev postranních kanálů je tak definitivně jednou z nejvýznamnějších událostí v současné kryptoanalýze. V rychle se rodící obecné teorii postranních kanálů se jasně ukazuje, že moderní kryptologie (zejména její důležitá část *aplikovaná kryptografie*) je značně multidisciplinární věda, která kombinuje velmi širokou řadu čistě matematických disciplín s určitými znalostmi z oboru fyziky, počítačů a elektroinženýrství. Stručně řečeno, kryptologie sama o sobě balancuje na rozhranní matematiky a fyziky. S trochou nadsázky zde můžeme hovořit o jistém druhu *fyzikální matematiky*, kde jsme si vypůjčili pojem *matematická fyzika*, ve kterém jsme zaměnili pořadí obou disciplín.

Teorie postranních kanálů rovněž významně ovlivňuje některé ze zavedených kryptografických fenoménů. Jako příklad si uveďme koncept *perfektního utajení* (rovněž znám jako *absolutní bezpečnost*). Jednoduše řečeno, tímto termínem označujeme kryptografické konstrukce, u kterých může být jakákoliv možnost kryptoanalýzy zcela vyloučena, bez ohledu na výpočetní prostředky útočníka. V tomto směru obecně proslula *Vernamova šifra*, která je za předpokladu správné implementace absolutně bezpečná. Celý koncept perfektního utajení pro nás ovšem není příliš přínosný, pokud v něm neuvažujeme vliv postranních kanálů. Informace, o které předpokládáme její nedostupnost pro útočníka, totiž může ve skutečnosti nepozorovaně unikat právě některým z postranních kanálů. To samozřejmě neznamená, že termín perfektního utajení je odsouzen k zániku. Znamená to však, že konstrukce důkazu o absolutní bezpečnosti musí být vždy založena na takovém popisu vyhodnocovaného kryptosystému, který koresponduje s fyzikální realitou (tj. zahrnuje přesný popis hrozících postranních kanálů).

Obecně platným závěrem disertační práce je, že bezpečnost konkrétního kryptografického modulu nezávisí jen na aplikovaných kryptografických standardech. Je to rovněž otázka způsobu, kterým jsou tyto standardy implementovány, a stejně tak i prostředí, ve kterém má být modul používán. Odtud můžeme uzavřít, že standardy samy o sobě pro návrh skutečně bezpečných bezpečnostních modulů rozhodně nestačí.