Master Thesis

Title of the Thesis

Student name

Date: date
Supervisor: name

Ruhr-University Bochum, Germany

Chair for Network and Data Security
Prof. Dr. Jörg Schwenk
Homepage: www.nds.rub.de

Erklärung

Ich erkläre, dass das Thema dieser Arbeit nicht identisch ist mit dem Thema einer von mir bereits für ein anderes Examen eingereichten Arbeit. Ich erkläre weiterhin, dass ich die Arbeit nicht bereits an einer anderen Hochschule zur Erlangung eines akademischen Grades eingereicht habe.

Ich versichere, dass ich die Arbeit selbständig verfasst und keine anderen als die angegebenen Quellen benutzt habe. Die Stellen der Arbeit, die anderen Werken dem Wortlaut oder dem Sinn nach entnommen sind, habe ich unter Angabe der Quellen der Entlehnung kenntlich gemacht. Dies gilt sinngemäß auch für gelieferte Zeichnungen, Skizzen und bildliche Darstellungen und dergleichen.

Ort, Datum	Unterschrift

Acknowledgements

The author would like to thank...

Abstract

The abstract goes here.

KEYWORDS: some key words

Contents

List of Figures

List of Tables

1 Caption of Chapter 1

Description of this chapter.

1.1 Position of figures

You can include the image as usual. You can include the image as usual. You can include the image as usual. You can include the image as usual. You can include the image as usual. You can include the image as usual.

Figure 1.1: SubBytes(normal figure)

You can include the image as usual. You can include the image as usual. You can include the image as usual. You can include the image as usual. You can include the image as usual. You can include the image as usual.

You can wrap the figure (align right). You can wrap the figure (align right). You can wrap the figure (align right). You can wrap the figure (align right). You can wrap the figure (align right).

You can wrap the figure (align right). You can wrap the figure (align right). You can wrap the figure (align right). You can wrap the figure (align right). You can wrap the figure (align right).

You can wrap the figure (align right). You can wrap the figure (align right). You can wrap the figure (align right). You can wrap the figure (align right). You can wrap the figure (align right).

Figure 1.2: SubBytes(Normal figure (align right))

Figure 1.3: SubBytes(Normal figure (align left))

You can wrap the figure (align left). You can wrap the figure (align right). You can wrap the figure (align left). You can wrap the figure (align left). You can wrap the figure (align left).

You can wrap the figure (align left). You can wrap the figure (align right). You can wrap the figure (align left). You can wrap the figure (align left). You can wrap the figure (align left).

You can wrap the figure (align left). You can wrap the figure (align right). You can wrap the figure (align left). You can wrap the figure (align left). You can wrap the figure (align left).

1.2 Multiple Figures and Tables Parallel

Two tables parallel.

A	B	C

Table 1.1: Caption of table

D	E	F

Table 1.2: Caption of table

Two figures parallel.

Figure 1.4: Caption of figure

Figure 1.5: Caption of figure

One figure and one table parallel

D	E	F

Table 1.3: Caption of table

Figure 1.6: Caption of figure

1.3 Algorithms

Algorithm

Algorithm 1 Key pair generation of ECDSA

Require: valid $PARAM$
Ensure: public key Q and secret key d
  while true do
    $d \Leftarrow_R [1,\mathrm{n}-1]$
    $Q = (x_Q, y_Q) \Leftarrow dG.$
    if $Q \neq O$ **then**
      return (Q, d)
    end if
  end while

1.4 Citations

artice [1]

manual [2, Section Nr.]

book [3, Section Nr.]

misc [4, Section Nr.]

phdthesis [5, Section Nr.]

inproceedings [6, Section Nr.]

standard [7, Section Nr.]

techreport [8, Section Nr.]

2 Conclusions

Conclusions.

A Caption of Appendix

A.1 Title of the first appendix section

You can embed the java source code as follows:

```
public boolean verify(byte[] signature){
 return true;
}
```

A.2 Caption of the second appendix section

BlaBla Blabla ...

Bibliography

[1] H. Drucker, D. Wu, and V. N. Vapnik, "Support vector machines for spam categorization," *IEEE Transactions On Neural Networks*, vol. 10, no. 5, pp. 1048–1054, 1999.

[2] *Smart Cards for Payment Systems: An Introductory Paper describing how Thales e-Security can help banks migrate to Smart Card Technology*, Thales eSecurity. [Online]. Available: http://www.thales-esecurity.com/Whitepapers/documents/Smart_cards_for_payment_systems.pdf

[3] C. R. Murthy and B. S. Manoj, *Ad Hoc Wireless Networks - Architectures and Protocols*. Person Education, 2004, pp. 299–364.

[4] Y. Hu, A. Perrig, and D. Johnson, "Wormhole Detection in Wireless Ad Hoc Networks," June 2002. [Online]. Available: citeseer.ist.psu.edu/hu02wormhole.html

[5] Y. Amir, "Replication Using Group Communication over a Partitioned Network," Ph.D. dissertation, Institute of Computer Science, The Hebrew University of Jerusalem, Jerusalem, Israel, 1995.

[6] W. Du, J. Deng, Y. S. Han, and P. K. Varshney, "A Pairwise Key Pre-Distribution Scheme for Wireless Sensor Networks," in *CCS '03: Proceedings of the 10th ACM conference on Computer and communications security*. ACM Press, 2003, pp. 42–51.

[7] J. Galvin, S. Murphy, S. Crocker, and N. Freed, *Security Multiparts for MIME: Multipart/Signed and Multipart/Encrypted*, IETF RFC 1847, Oct. 1995.

[8] "Email metrics program: The network operators' perspectivereport #3 - 2nd quarter 2006," Messaging Anti-Abuse Working Group(MAAWG), Tech. Rep., Nov. 2006. [Online]. Available: http://www.maawg.org/about/FINAL_2Q2006_Metrics_Report.pdf