

分类号 TP957

学号 0123456

UDC

密级 公开

工学硕士学位论文

国防科大学位论文 L^AT_EX 模板 使用手册

硕士生姓名 蓝宗骁

学 科 专 业 网络工程

研 究 方 向 网络工程

指 导 教 师 夏戈明 教授

国防科学技术大学研究生院

二〇一四年十月

面向规模化大数据传感网的数据认证关键技术研究

Candidate: Lan Zongxiao

Advisor: Associate Professor Xia Geming

A dissertation

Submitted in partial fulfillment of the requirements

for the degree of Master of Engineering

in Large-scale Wireless Sensor Network Data

Authentication

Graduate School of National University of Defense Technology

Changsha, Hunan, P. R. China

October 8, 2014

独 创 性 声 明

本人声明所呈交的学位论文是我本人在导师指导下进行的研究工作及取得的研究成果。尽我所知，除文中特别加以标注和致谢的地方外，论文中不包含其他人已经发表和撰写过的研究成果，也不包含为获得国防科学技术大学或其他教育机构的学位或证书而使用过的材料。与我一同工作的同志对本研究所做的任何贡献均已在论文中作了明确的说明并表示谢意。

学位论文题目：_____国防科学技术大学学位论文 L^AT_EX 模板_____

学位论文作者签名：_____日期：_____年____月____日

学位论文版权使用授权书

本人完全了解国防科学技术大学有关保留、使用学位论文的规定。本人授权国防科学技术大学可以保留并向国家有关部门或机构送交论文的复印件和电子文档，允许论文被查阅和借阅；可以将学位论文的全部或部分内容编入有关数据库进行检索，可以采用影印、缩印或扫描等复制手段保存、汇编学位论文。

（保密学位论文在解密后适用本授权书。）

学位论文题目：_____国防科学技术大学学位论文 L^AT_EX 模板_____

学位论文作者签名：_____日期：_____年____月____日

作者指导教师签名：_____日期：_____年____月____日

目 录

摘 要	i
ABSTRACT	ii
第一章 绪论	1
1.1 本文研究背景和意义	1
1.1.1 无线传感网概述	1
1.1.2 无线传感网数据交叉认证概述	1
1.2 本文研究内容	1
1.3 本文组织结构	1
第二章 相关研究	2
2.1 (2.1 题目)	2
2.1.1 (2.1.1 题目)	2
2.1.2 (2.1.2 题目)	2
2.2 (2.2 题目)	2
2.3 (2.3 题目)	2
第三章 多跳长路径上多节点联合数据认证	3
3.1 (2.1 题目)	3
3.1.1 (2.1.1 题目)	3
3.1.2 (2.1.2 题目)	3
3.2 (2.2 题目)	3
3.3 (2.3 题目)	3
第四章 多路径抗密钥失效	4
4.1 (2.1 题目)	4
4.1.1 (2.1.1 题目)	4
4.1.2 (2.1.2 题目)	4
4.2 (2.2 题目)	4
4.3 (2.3 题目)	4
第五章 密钥分配方案	5
5.1 (2.1 题目)	5
5.1.1 (2.1.1 题目)	5
5.1.2 (2.1.2 题目)	5

5.2	(2.2 题目)	5
5.3	(2.3 题目)	5
第六章	仿真实验与结果分析	6
6.1	(2.1 题目)	6
6.1.1	(2.1.1 题目)	6
6.1.2	(2.1.2 题目)	6
6.2	(2.2 题目)	6
6.3	(2.3 题目)	6
第七章	总结与展望	7
7.1	本文总结	7
7.2	未来工作于展望	7
致谢		8
参考文献		9
作者在学期间取得的学术成果		11
附录 A	模板提供的希腊字母命令列表	12

表 目 录

图 目 录

摘 要

国防科学技术大学是一所直属中央军委的综合性大学。1984 年,学校经国务院、中央军委和教育部批准首批成立研究生院,肩负着为全军培养高级科学和工程技术人才与指挥人才,培训高级领导干部,从事先进武器装备和国防关键技术研究的重要任务。国防科技大学是全国重点大学,也是全国首批进入国家“211 工程”建设并获中央专项经费支持的全国重点院校之一。学校前身是 1953 年创建于哈尔滨的中国人民解放军军事工程学院,简称“哈军工”。

关键词: 国防科学技术大学; 211; 哈军工

ABSTRACT

National University of Defense Technology is a comprehensive national key university based in Changsha, Hunan Province, China. It is under the dual supervision of the Ministry of National Defense and the Ministry of Education, designated for Project 211 and Project 985, the two national plans for facilitating the development of Chinese higher education.

NUDT was originally founded in 1953 as the Military Academy of Engineering in Harbin of Heilongjiang Province. In 1970 the Academy of Engineering moved southwards to Changsha and was renamed Changsha Institute of Technology. The Institute changed its name to National University of Defense Technology in 1978.

Key Words: NUDT; MND; ME

符号使用说明

HPC	高性能计算 (High Performance Computing)
cluster	集群
Itanium	安腾
SMP	对称多处理
API	应用程序编程接口
PI	聚酰亚胺
MPI	聚酰亚胺模型化合物, N-苯基邻苯酰亚胺
PBI	聚苯并咪唑
MPBI	聚苯并咪唑模型化合物, N-苯基苯并咪唑
PY	聚吡咙
PMDA-BDA	均苯四酸二酐与联苯四胺合成的聚吡咙薄膜
ΔG	活化自由能 (Activation Free Energy)
χ	传输系数 (Transmission Coefficient)
E	能量
m	质量
c	光速
P	概率
T	时间
v	速度

第一章 绪论

本章的主要内容与学校提供的 Word 模板中内容一致，图片与表格均采用原始设定大小，主要是为了说明格式的统一。但是， \LaTeX 的一些禁则，专业排版的能力，对公式及文献的处理都是得天独厚的，我们不必刻意去追求与 Word 的完美匹配。而且你将会发现，用 \LaTeX 书写论文的美！

1.1 本文研究背景和意义

正文内容

1.1.1 无线传感网概述

正文内容

正文内容

1.1.2 无线传感网数据交叉认证概述

正文内容

正文内容

1.2 本文研究内容

正文内容

正文内容

正文内容

正文内容

1.3 本文组织结构

本模板推荐使用 \LaTeX ，样式文件为 `bstutf8.bst`，符合学校的参考文献格式（如专利等引用未加详细测试）。看看这个例子，关于书的^[1, 2]，还有这些^[3-5]，关于杂志的^[6-8]，硕士论文^[9, 10]，博士论文^[11, 12]，标准文件^[13]，会议论文^[14, 15]，技术报告^[16]。中文参考文献^[17] **特别注意**，需要在 `bibitem` 中增加 `language` 域并设为 `zh`，英文此项可不填，之后由 `bstutf8` 统一处理（具体就是决定一些文献在中英文不同环境下的显示格式，如等、etc）。若使用 `JabRef`，则你可按下面步骤来设置：选择 **Options**→**Set Up General Fields**，在 `General:` 后加入 `language` 就可以了。

有时候不想要上标，那么可以这样^[11]，这个非常重要。

第二章 相关研究

本章的主要内容与学校提供的 Word 模板中内容一致，图片与表格均采用原始设定大小，主要是为了说明格式的统一。但是， \LaTeX 的一些禁则，专业排版的能力，对公式及文献的处理都是得天独厚的，我们不必刻意去追求与 Word 的完美匹配。而且你将会发现，用 \LaTeX 书写论文的美！

2.1 (2.1 题目)

正文内容

2.1.1 (2.1.1 题目)

正文内容

2.1.1.1 (2.1.1.1 题目)

正文内容

2.1.1.2 (2.1.1.2 题目)

正文内容

2.1.2 (2.1.2 题目)

正文内容

2.2 (2.2 题目)

正文内容

2.3 (2.3 题目)

第三章 多跳长路径上多节点联合数据认证

本章的主要内容与学校提供的 Word 模板中内容一致，图片与表格均采用原始设定大小，主要是为了说明格式的统一。但是， \LaTeX 的一些禁则，专业排版的能力，对公式及文献的处理都是得天独厚的，我们不必刻意去追求与 Word 的完美匹配。而且你将会发现，用 \LaTeX 书写论文的美！

3.1 (2.1 题目)

正文内容

3.1.1 (2.1.1 题目)

正文内容

3.1.1.1 (2.1.1.1 题目)

正文内容

3.1.1.2 (2.1.1.2 题目)

正文内容

3.1.2 (2.1.2 题目)

正文内容

3.2 (2.2 题目)

正文内容

3.3 (2.3 题目)

第四章 多路径抗密钥失效

本章的主要内容与学校提供的 Word 模板中内容一致，图片与表格均采用原始设定大小，主要是为了说明格式的统一。但是， \LaTeX 的一些禁则，专业排版的能力，对公式及文献的处理都是得天独厚的，我们不必刻意去追求与 Word 的完美匹配。而且你将会发现，用 \LaTeX 书写论文的美！

4.1 (2.1 题目)

正文内容

4.1.1 (2.1.1 题目)

正文内容

4.1.1.1 (2.1.1.1 题目)

正文内容

4.1.1.2 (2.1.1.2 题目)

正文内容

4.1.2 (2.1.2 题目)

正文内容

4.2 (2.2 题目)

正文内容

4.3 (2.3 题目)

第五章 密钥分配方案

本章的主要内容与学校提供的 Word 模板中内容一致，图片与表格均采用原始设定大小，主要是为了说明格式的统一。但是， \LaTeX 的一些禁则，专业排版的能力，对公式及文献的处理都是得天独厚的，我们不必刻意去追求与 Word 的完美匹配。而且你将会发现，用 \LaTeX 书写论文的美！

5.1 (2.1 题目)

正文内容

5.1.1 (2.1.1 题目)

正文内容

5.1.1.1 (2.1.1.1 题目)

正文内容

5.1.1.2 (2.1.1.2 题目)

正文内容

5.1.2 (2.1.2 题目)

正文内容

5.2 (2.2 题目)

正文内容

5.3 (2.3 题目)

第六章 仿真实验与结果分析

本章的主要内容与学校提供的 Word 模板中内容一致，图片与表格均采用原始设定大小，主要是为了说明格式的统一。但是， \LaTeX 的一些禁则，专业排版的能力，对公式及文献的处理都是得天独厚的，我们不必刻意去追求与 Word 的完美匹配。而且你将会发现，用 \LaTeX 书写论文的美！

6.1 (2.1 题目)

正文内容

6.1.1 (2.1.1 题目)

正文内容

6.1.1.1 (2.1.1.1 题目)

正文内容

6.1.1.2 (2.1.1.2 题目)

正文内容

6.1.2 (2.1.2 题目)

正文内容

6.2 (2.2 题目)

正文内容

6.3 (2.3 题目)

第七章 总结与展望

本章的主要内容与学校提供的 Word 模板中内容一致，图片与表格均采用原始设定大小，主要是为了说明格式的统一。但是， \LaTeX 的一些禁则，专业排版的能力，对公式及文献的处理都是得天独厚的，我们不必刻意去追求与 Word 的完美匹配。而且你将会发现，用 \LaTeX 书写论文的美！

7.1 本文总结

正文内容

7.2 未来工作于展望

正文内容

致 谢

衷心感谢导师 xxx 教授和 xxx 副教授对本人的精心指导。他们的言传身教将使我终生受益。

感谢 NudtPaper，它的存在让我的论文写作轻松自在了许多，让我的论文格式规整漂亮了许多。

参考文献

- [1] Knuth D E. The \TeX Book [M]. 15th ed. Reading, MA: Addison-Wesley Publishing Company, 1989.
- [2] Goosens M, Mittelbach F, Samarin A. The \LaTeX Companion [M]. Reading, MA: Addison-Wesley Publishing Company, 1994.
- [3] Krasnogor N. Towards robust memetic algorithms [M] // Hart W, Krasnogor N, Smith J. Recent Advances in Memetic Algorithms Vol.166. New York: Springer Berlin Heidelberg, 2004: 2004: 185–207.
- [4] 阎真. 沧浪之水 [M]. 人民文学出版社, 2001: 185–207.
- [5] 班固. 苏武传 [M] // 郑在瀛, 汪超宏, 周文复. 传记散文英华: 第2卷. 武汉: 湖北人民出版社, 1998: 1998: 65–69.
- [6] Chafik El Idrissi M, Roney A, Frigon C, et al. Measurements of total kinetic-energy released to the $N = 2$ dissociation limit of H_2 — evidence of the dissociation of very high vibrational Rydberg states of H_2 by doubly-excited states [J]. Chemical Physics Letters. 1994, 224 (10): 260–266.
- [7] Mellinger A, Vidal C R, Jungen C. Laser reduced fluorescence study of the carbon-monoxide nd triplet Rydberg series-experimental results and multichannel quantum-defect analysis [J]. J. Chem. Phys. 1996, 104 (5): 8913–8921.
- [8] Shell M. How to Use the IEEEtran \LaTeX Class [J]. Journal of \LaTeX Class Files. 2002, 12 (4): 100–120.
- [9] 猪八戒. 论流体食物的持久保存这是一个很长很长的题目用来测试 \LaTeX 会不会出现乱码貌似北邮的 \LaTeX 工作的很好 [D]. 北京: 广寒宫大学, 2005.
- [10] Jeyakumar A R. Metamori: A library for Incremental File Checkpointing [D]. Blacksburg: Virginia Tech, 2004.
- [11] 沙和尚. 论流沙河的综合治理 [D]. 北京: 清华大学, 2005.
- [12] Zadok E. FiST: A System for Stackable File System Code Generation [D]. USA: Computer Science Department, Columbia University, 2001.
- [13] IEEE Std 1363-2000. IEEE Standard Specifications for Public-Key Cryptography [M]. New York: IEEE, 2000.
- [14] Kim S, Woo N, Yeom H Y, et al. Design and Implementation of Dynamic Process Management for Grid-enabled MPICH [C]. In the 10th European PVM/MPI Users' Group Conference. Venice, Italy, sep 2003.

- [15] Kocher C, Jaffe J, Jun B. Differential Power Analysis [C]// Wiener M. In Advances in Cryptology (CRYPTO '99). August 1999: 388–397.
- [16] Woo A, Bailey D, Yarrow M, et al. The NAS Parallel Benchmarks 2.0 [R/OL]. 1995. <http://www.nasa.org/>.
- [17] 贾宝玉, 林黛玉, 薛宝钗, 等. 论刘姥姥食量大如牛之现实意义 [J]. 红楼梦杂谈. 1800, 224: 260–266.

作者在学期间取得的学术成果

发表的学术论文

- [1] Zongxiao Lan, Geming Xia, Aolong Zhou. Communication cost optimized session key transmission scheme for WSN based on non-perfect secret sharing. ICITMI, 2014.

附录 A 模板提供的希腊字母命令列表

大写希腊字母:

Γ \Gamma	Λ \Lambda	Σ \Sigma	Ψ \Psi
Δ \Delta	Ξ \Xi	Υ \Upsilon	Ω \Omega
Θ \Theta	Π \Pi	Φ \Phi	
Γ \varGamma	Λ \varLambda	Σ \varSigma	Ψ \varPsi
Δ \varDelta	Ξ \varXi	Υ \varUpsilon	Ω \varOmega
Θ \varTheta	Π \varPi	Φ \varPhi	

小写希腊字母:

α \alpha	θ \theta	\omicron \omicron	τ \tau
β \beta	ϑ \vartheta	π \pi	υ \upsilon
γ \gamma	ι \iota	ϖ \varpi	ϕ \phi
δ \delta	κ \kappa	ρ \rho	φ \varphi
ϵ \epsilon	λ \lambda	ϱ \varrho	χ \chi
ε \varepsilon	μ \mu	σ \sigma	ψ \psi
ζ \zeta	ν \nu	ς \varsigma	ω \omega
η \eta	ξ \xi	\kappaappa \kappaappa	\digamma \digamma
α \upalpha	θ \uptheta	o \mathrm{o}	τ \uptau
β \upbeta	ϑ \upvartheta	π \uppi	υ \upupsilon
γ \upgamma	ι \upiota	ϖ \upvarpi	ϕ \upphi
δ \updelta	κ \upkappa	ρ \uprho	φ \upvarphi
ϵ \upepsilon	λ \uplambda	ϱ \upvarrho	χ \upchi
ε \upvarepsilon	μ \upmu	σ \upsigma	ψ \uppsi
ζ \upzeta	ν \upnu	ς \upvarsigma	ω \upomega
η \upeta	ξ \upxi		

希腊字母属于数学符号类别, 请用\bm 命令加粗, 其余向量、矩阵可用\mathbf。