



elektor

射频识别：

应用中的MIFARE和
非接触式智能卡

（影印版）

RFID:

MIFARE and Contactless Smartcards in Application

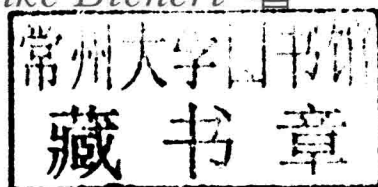
Gerhard H. Schalk , Renke Bienert 著



东南大学出版社
SOUTHEAST UNIVERSITY PRESS

射频识别：
应用中的 MIFARE 和非接触式智能卡
(影印版)

Gerhard H. Schalk, Renke Bienert 著



南京 东南大学出版社

图书在版编目(CIP)数据

射频识别:应用中的 MIFARE 和非接触式智能卡:
英文/(德)沙尔克(Schalk, G.H.), (德)比奈特(Bienert, R.)
著. —影印本. —南京:东南大学出版社, 2015.9

书名原文:RFID:MIFARE and Contactless Smartcards
in Application

ISBN 978-7-5641-5947-4

I. ①射… II. ①沙… ②比… III. ①射频-无
线电信号-信号识别-英文 IV. ①TN911.23

中国版本图书馆 CIP 数据核字(2015)第 170009 号

© 2013 by Elektor International Media BV

Reprint of the English Edition, jointly published by Elektor International Media BV and Southeast University Press, 2015. Authorized reprint of the original English edition, 2015 Elektor International Media BV, the owner of all rights to publish and sell the same.

All rights reserved including the rights of reproduction in whole or in part in any form.

英文原版由 Elektor International Media BV 出版 2013。

英文影印版由东南大学出版社出版 2015。此影印版的出版和销售得到出版权和销售权的所有者——Elektor International Media BV 的许可。

版权所有,未得书面许可,本书的任何部分和全部不得以任何形式重制。

射频识别:应用中的 MIFARE 和非接触式智能卡(影印版)

出版发行:东南大学出版社

地 址:南京四牌楼 2 号 邮编:210096

出 版 人:江建中

网 址:<http://www.seupress.com>

电子邮件:press@seupress.com

印 刷:常州市武进第三印刷有限公司

开 本:787 毫米×980 毫米 16 开本

印 张:30.25

字 数:592 千字

版 次:2015 年 9 月第 1 版

印 次:2015 年 9 月第 1 次印刷

书 号:ISBN 978-7-5641-5947-4

定 价:89.00 元

Preface

Dr. Thomas Wille

RFID technology, which uses radio frequency to identify people or objects, opens up pathways to newer and more expansive applications. From easier access control using contactless (RFID) cards to public transport fare tickets to bank cards to use in passports as well as in the new German identity cards, the applications are becoming more complex and require ever more computing power.

One of the reasons for contactless technology's success is the cards' ease of use and convenience. Simply placing an RFID device, without any special orientation, within a few centimeters of the reader suffices, and a transaction is completed in a fraction of a second.

Another advantage of this technology is its robustness. RFID devices are now highly integrated and measure just a few square millimeters in area. The coupling antennas are connected directly to the ICs' antenna terminals, resulting in minimal anisotropic connections. The antenna and IC may then be housed very stably within a card enclosure. By minimizing the required electrical connections in this manner, there are no further mechanical-electrical connections that, from a quality perspective, could present weaknesses. It is only possible by means of this robust construction, to achieve life spans of over ten years, and to use the technology in extreme environments.

All of these advantages are enabled with the design of more complex contactless interfaces on the cards and readers. In contrast with serial contact card interfaces with their 8 contacts, data coding for RFID carriers is more complex and the high positioning tolerance in regard to the reader device is made possible by complex and robust analog interface circuitry design. Optimization of the reader-card system is also crucial for optimal implementation and robust dimensioning of RFID technology.

This book gives the reader a simple and understandable introduction to the fundamentals of RFID technology and explains the relevant international standards. Then, in a separate chapter, the security aspects of the technology are discussed. Further, all RFID system components are systematically presented and explained in detail, from RFID antenna design to the different card and tag types to the design of an RFID reader, including the antenna design.

The design of a reader, particularly the Elektor RFID Reader, is very carefully described to the user, from software/firmware to user interface. However, for the user, practical application and associated problems are the key. This is where extensive description of some Elektor RFID Reader use cases and useful tips, tricks and solutions for problem

situations comes in. The chapters that follow fully describe the included reader software for an access control system functionally. The book also explains the user interface standards.

This book is thus a systematic introduction to the RFID arena that leads the user through the design of a practical card-reader system. In addition, the book is an indispensable guide for any user who wants to conceptualize, design and optimize RFID systems, and offers the crucial assistance required for the often complex problems inherent in RFID system design.

With this book, the authors have closed the loop for users, hopefully aiding the continuous march of RFID technology to further, unimagined extents. For this, we owe the authors a large debt of gratitude.

Hamburg, January 2011

Dr. Thomas Wille

Senior Director Architecture & Technology

Business Unit Identification, NXP Semiconductors

About the authors

Gerhard Schalk has been an application engineer at NXP Semiconductors (formerly Philips Semiconductors) since 2001. In this role, he supports global clients in developing smartcard operating systems. He is also a freelance lecturer at the FH-Hagenberg and FH-Campus 02 (Graz) technical colleges.

Renke Bienert has also been an application engineer at NXP Semiconductors since 2001. He supports global clients in developing readers and systems that use contactless smartcards. He was involved, among other things, with the introduction of electronic tickets for the 2006 FIFA World Cup, as well as electronic travel passes.

Acknowledgments

When we began this project, we had no idea how much blood, sweat and tears would be required to physically nail down all of these concepts in writing. It's perhaps good that we didn't know that in advance.

For technical assistance, we want to thank all of our colleagues and former colleagues in the Identification Team at NXP, from Hamburg (Germany), Gratkorn (Austria), Caen (France), Eindhoven (The Netherlands), Leuven (Belgium), Singapore, Shanghai (China) and all other locations!

We also thank all collaborators in standardization, especially the members of SC17/WG8 and of the DIN working group, as well as all of our customers throughout the world. Without NXP's support, this book would not have been possible.

Special thanks go to Dr. Thomas Wille, Dipl.-Ing. Reinhard Szoncsó, Ing. Martin Möstl, Dr. Ute Merkel and Mag. Annemarie Brunner for intensive proofreading, as well as Raimund Krings for the supervision and support of Elektor Publishing.

February 2011, Gerhard H. Schalk and Renke Bienert

My special thanks go to my dear wife, Annemarie Brunner, and my two sons, Maximilian and Simon. Without the patience and support of my family, my contribution to this book would not have been possible.

February 2011, Gerhard H. Schalk

My sincere thanks go to all who have tolerated and supported me during the writing of this book, especially my wife, Ute Merkel.

February 2011, Renke Bienert

Contents

Preface	13
 1 RFID Fundamentals	 17
1.1 Introduction to RFID	17
1.1.1 RF	17
1.1.2 ID	18
1.1.3 RFID system classification	19
1.1.3.1 Frequencies and transmission principles	19
1.1.3.2 Applications	20
1.2 RFID system components	22
1.2.1 Card (PICC)	22
1.2.2 Reader (PCD)	23
1.3 ISO/IEC 14443 application example	24
1.3.1 Public transport ticketing	24
1.3.2 Employee identification cards	25
1.3.3 Electronic passports and identity cards	26
1.3.4 Other applications	27
1.4 Physical fundamentals	27
1.4.1 Energy transmission	27
1.4.2 Data transmission from PCD to PICC	29
1.4.2.1 Amplitude modulation	29
1.4.2.2 Standard data rate (106Kb/s)	29
1.4.2.3 Higher data rates (up to 848Kb/s)	31
1.4.3 Data transmission from PICC to PCD	32
1.4.3.1 Load modulation	33
1.4.3.2 Subcarrier modulation: Manchester encoding using ASK	33
1.4.3.3 Subcarrier modulation: NRZ encoding with BPSK	34
 2 Overview of the Relevant Standards	 35
2.1 ISO/IEC 14443	35
2.1.1 Part 1: physical properties	36
2.1.2 Part 2: RF properties and signals	37
2.1.3 Part 3: Card selection and activation	38
2.1.3.1 Type A: UIDs	38
2.1.3.2 Type A: card activation	40
2.1.3.3 Type A: SAK encoding	42
2.1.3.4 Type A: collision-detection and conflict resolution	44
2.1.3.5 Type B card activation	46
2.1.3.6 Type B: Card activation parameters	48

2.1.4	Part 4: communication protocol	49
2.1.4.1	Protocol activation	49
2.1.4.2	T=CL protocol block structure	56
2.1.5	Information Block (I Block)	56
2.1.5.1	Receive-ready Blocks (R Blocks)	58
2.1.5.2	Supervisory Blocks (S Blocks)	59
2.1.6	Electromagnetic disturbance (EMD)	61
2.1.6.1	Rest period	62
2.1.6.2	Rest level	63
2.1.6.3	Distinction between invalid card response and EMD	63
2.1.6.4	The MFRC522 reader IC and EMD	63
2.2	ISO/IEC 10373-6 test methods	64
2.2.1	Test equipment	65
2.2.1.1	Calibration coil	65
2.2.1.2	Test PCD assembly	65
2.2.1.3	ReferencePICC	66
2.2.2	Tuning and calibration	68
2.2.2.1	Tuning	68
2.2.2.2	Calibration	68
2.2.3	Measurements at the reader	69
2.2.3.1	Range measurement	69
2.2.3.2	Measurement effort	69
2.2.4	Tests for Layer 3 and 4	70
2.3	Near Field Communication (NFC)	70
2.3.1	Introduction	70
2.3.2	NFC air interface	71
2.3.2.1	NFC device as card	71
2.3.2.2	NFC device as a reader	71
2.3.2.3	NFC device in 'active' mode	72
3	RFID Antenna Design	73
3.1	Theoretical Fundamentals	73
3.1.1	Antenna as Resonant Circuit	73
3.1.2	Transformer Model	77
3.1.3	The Biot-Savart Law	79
3.1.4	Optimal Antenna Size	80
3.2	Reader Antennas	83
3.2.1	Antenna Quality	83
3.2.1.1	Data Transmission Bandwidth	83
3.2.1.2	Stability Against Detuning	86
3.2.2	Electrically Conductive Surfaces in the Vicinity of the Antenna	89
3.2.2.1	Ferrites	90
3.2.3	Balanced and Unbalanced Antennas	92
3.2.3.1	Balanced Antenna	93
3.2.3.2	Unbalanced Antenna	96

3.3	Card Antennas	98
3.3.1	Standard Cards (ID-1)	98
3.3.2	Tokens with Smaller Inlays (Smaller than ID-1)	100
3.4	Impedance Measurements with the miniVNA	101
3.4.1	miniVNA User Software.	102
3.4.2	Disadvantages and Limitations of the miniVNA	102
3.4.2.1	Lack of Sign for Imaginary Numbers	102
3.4.2.2	Lack of Calibration and Compensation	102
3.4.3	How Do I Find the Correct Compensation?	103
3.4.4	Coil Inductance Measurement	105
4	Security and Cryptography	109
4.1	Protection Objectives	109
4.1.1	Keeping Data Secure	109
4.1.2	Data Integrity	111
4.1.3	Privacy Protection	112
4.2	Attacks on Smartcards	112
4.2.1	Logical Attacks	112
4.2.1.1	Unauthorized Reading of Data.	112
4.2.1.2	Unauthorized Manipulation of Data	113
4.2.1.3	'Replay' Attack	114
4.2.1.4	'Relay' Attack	114
4.2.1.5	'Man-in-the-Middle' Attack	116
4.2.1.6	Denial-of-Service Attack	116
4.2.2	Physical Attacks.	116
4.2.2.1	Side Channel Attacks and Power Analysis	116
4.2.2.2	Reverse Engineering	118
4.2.2.3	Light and Laser Attacks	119
4.2.2.4	Temperature and Frequency.	120
4.2.3	Combined Attacks	120
4.3	Cryptography	120
4.3.1	Asymmetric Cryptography.	120
4.3.2	Symmetric Cryptography	122
4.3.3	Block and Stream Cipher	123
4.3.4	Encryption Standards: DES and AES	124
4.3.5	DES Cascading.	125
4.3.6	Operation mode.	127
4.3.6.1	Electronic Code Book (ECB)	127
4.3.6.2	Cipher Block Chaining (CBC).	127
4.4	Application of Cryptography.	129
4.4.1	Mutual Authentication.	129
4.4.2	Data Encryption.	131
4.4.3	Message Authentication Code (MAC)	131
4.4.4	Key Management	132
4.4.4.1	Dynamic Keys	132
4.4.4.2	Key Diversification.	132
4.4.5	Secure Application Module (SAM).	135
4.4.6	Security Assessment	135

5	Introduction to Cards and Tags	137
5.1	Overview	137
5.1.1	Memory Cards and Microcontroller Cards	137
5.1.2	Advantages and Disadvantages of Contactless Cards	138
5.1.2.1	Robustness	138
5.1.2.2	Longevity	138
5.1.2.3	Usability	138
5.1.2.4	Infrastructure	138
5.1.2.5	Contact Between Card and Reader	139
5.1.3	Dual-Interface Cards	139
5.2	MIFARE	139
5.2.1	MIFARE Overview	139
5.2.1.1	Success Story	140
5.2.1.2	MIFARE Clone	140
5.2.1.3	MIFARE Hack	140
5.2.1.4	MIFARE Product Overview	140
5.2.2	MIFARE Ultralight	141
5.2.2.1	Instruction Set	142
5.2.2.2	Memory Organization	144
5.2.2.3	Security Functions	144
5.2.3	MIFARE Ultralight C	145
5.2.3.1	Instruction Set	146
5.2.3.2	Memory Organization	147
5.2.3.3	Security Functions	147
5.2.4	MIFARE Classic	148
5.2.4.1	Instruction Set	150
5.2.4.2	Memory Organization	151
5.2.4.3	Security Functions	152
5.2.5	MIFARE Plus	152
5.2.5.1	Memory Organization	152
5.2.5.2	MIFARE Plus S and MIFARE Plus X	152
5.2.5.3	Security Levels	153
5.2.6	MIFARE DESFire (EV1)	156
5.2.6.1	Memory Organization	156
5.2.6.2	File Types	157
5.2.6.3	Data File	157
6	Reader Antenna Design	159
6.1	MF RC522 Reader Module	159
6.1.1	Digital Interfaces	160
6.1.1.1	UART	160
6.1.1.2	SPI	160
6.1.1.3	I ² C	160
6.1.2	Oscillator	161
6.1.3	Analog Interfaces	161
6.1.3.1	Transmitter Outputs	161
6.1.3.2	Receive Input	165

6.1.4	Test Signals	169
6.1.4.1	MFOUT	170
6.1.4.2	AUX1 and AUX2	171
6.1.5	Miscellaneous	173
6.1.5.1	Power Supply and GND	173
6.1.5.2	Tolerances	173
6.2	Antenna Design	173
6.2.1	Coil Design	174
6.2.1.1	Measuring the Coil Parameters	175
6.2.1.2	Determine the Q Factor and the Series Resistance	176
6.2.2	Matching: Calculating the Initial Values	176
6.2.2.1	Parallel Equivalent Circuit	176
6.2.2.2	Partitioning and Simplifying the Circuit Diagram	177
6.2.2.3	Low-Pass Filter	177
6.2.2.4	Matching Network	178
6.2.3	Matching: Simulation and Measurement	179
6.2.4	Measurements on the Transmitted Pulse	181
6.2.5	Measurement and Adjustment of the Receive Path	183
6.2.6	Eliminating Interference	183
6.2.7	Range Checking	185
7	The Elektor RFID Reader	187
7.1	Introduction	187
7.2	Reader Hardware	190
7.2.1	Power Supply	192
7.2.2	The P89LPC936 Microcontroller	193
7.2.3	The MF RC522 Reader IC	194
7.2.4	The FT232R USB/RS-232 Converter	197
7.2.4.1	Configuring the FT232R	199
7.2.4.2	USB Driver Modification	201
7.3	Construction and Operation	202
7.3.1	Installing the USB Driver	202
7.3.2	Reader Firmware Update	203
7.3.3	Firmware Version Control	205
7.4	Reader Modes	205
7.4.1	Terminal Mode	205
7.4.2	PC Reader Mode	207
7.4.2.1	Activating the PC Reader Mode	207
7.5	The Firmware	208
7.5.1	The Software Architecture	208
7.5.2	The Main Program	208
7.5.3	The PC_ReaderMode() Function	210
7.5.3.1	The RS-232 Communication Protocol	210
7.6	The PC Development Tools	212
7.6.1	Elektor RFID Reader Programming in .NET	212
7.6.2	Smart Card Magic.NET	214
7.6.2.1	It's Usable without Programming	214

7.6.2.2	A Scripting Tool or a C# Compiler?	215
7.6.2.3	Our First Program: "Hello World".	216
7.6.2.4	Compiling and Running.	219
7.6.2.5	User Input from the Console Window	220
7.6.2.6	Are There Really No Breakpoints?	222
7.6.3	Visual C# 2012 Express Edition	223
7.6.3.1	Creating a Simple Console Application	223
7.6.3.2	Integrating the Elektor RFID Reader Library	225
8	Cards and Tags in Application	227
8.1	ISO/IEC 14443 Type A Card Activation	228
8.1.1	Card Types from the Perspective of Card Activation	228
8.1.2	The Activation Sequence.	230
8.1.2.1	The Request and Wake-Up Commands	230
8.1.2.2	The Anti-collision and Select Commands	233
8.1.2.3	The HALT Command	234
8.1.3	Elektor RFID Reader Library: Card Activation	236
8.1.4	Program Examples	241
8.1.4.1	Card Activation	241
8.1.4.2	Reader Selection	243
8.1.4.3	Polling for Cards	244
8.1.4.4	Simplified Card Activation	247
8.1.4.5	Testing the Reading Range	249
8.1.4.6	Listing All Cards in the Reader's Field	250
8.2	MIFARE Card-Type Detection	254
8.2.1	Program Example.	255
8.3	The MIFARE Ultralight Card	258
8.3.1	Memory Organization	258
8.3.3	Function of the One-Time-Programmable (OTP) Bytes	261
8.3.3.1	Lock Bits Functionality	262
8.3.4	Elektor RFID Reader Library: MIFARE Ultralight.	263
8.3.5	Program Examples	264
8.3.5.1	Writing and Erasing Data	264
8.3.5.2	Reading the Entire Memory Contents	265
8.3.5.3	Reading and Writing Strings	267
8.3.5.4	A Simple Ticket Application	268
8.3.5.5	Cloning the Memory Content	271
8.3.5.6	Secure Data Storage	273
8.4	The MIFARE Classic Card	281
8.4.1	MIFARE Classic 1K Card Memory Organization.	281
8.4.2	MIFARE Classic 4K Card Memory Organization.	281
8.4.3	MIFARE Mini Card Memory Organization.	282
8.4.4	Instruction Set.	282
8.4.5	The MIFARE Value Format	286
8.4.6	Decrement, Increment, Restore and Transfer	289
8.4.7	Changing the Keys and Access Condition	290
8.4.8	Elektor RFID Reader Library: MIFARE Classic	294

8.4.8.1	The MifareClassicUtil Class	294
8.4.8.2	The IMifareClassic Interface	297
8.4.9	Program and Case Studies	300
8.4.9.1	Writing and Erasing Data	300
8.4.9.2	Reading the Entire Memory Contents.	301
8.4.9.3	Optimizing the Read and Write Speeds	303
8.4.9.4	Optimized Reading of the Entire Memory Contents	307
8.4.9.5	The Problem of Data Corruption	310
8.4.9.6	The MIFARE Value Format Methods	314
8.4.9.7	Electronic Purse with Backup Management.	316
8.5	The MIFARE Ultralight C Card	322
8.5.1	Memory Organization	322
8.5.2	Instruction Set.	324
8.5.3	Triple-DES Authentication	324
8.5.4	Elektor RFID Reader Library: MIFARE Ultralight C	327
8.5.5	Programming Examples	327
8.5.5.1	The MIFARE Ultralight C Authentication Sequence	327
8.5.5.2	MIFARE Ultralight C Card Personalization	333
8.6	The T=CL Transmission Protocol	337
8.6.1	T=CL Protocol Activation and Deactivation	338
8.6.1.1	Multi-Card Activation	341
8.6.2	Data Exchange.	341
8.6.2.1	Smart Card Magic.NET – Exchange Mode.	342
8.6.2.2	Block Chaining	343
8.6.2.3	Waiting Time Extension	344
8.6.2.4	Error Detection and Correction	344
8.6.3	Elektor RFID Reader Library: T=CL	345
8.6.4	Example Programs	350
8.6.4.1	T=CL Protocol Activation and Deactivation	350
8.6.4.2	Multi-Card Activation	352
8.7	The MIFARE DESFire EV1 Card	355
8.7.1	MIFARE DESFire EV1 Commands	356
8.7.2	DESFire Native Command Structure	357
8.7.2.1	Card Command Structure.	357
8.7.2.2	Card Response Structure	357
8.7.2.3	DESFire Block Chaining	358
8.7.3	The DESFire File System	359
8.7.3.1	File Types	359
8.7.3.2	Data File Structure	360
8.7.3.3	Directory Names	361
8.7.3.4	File Names	362
8.7.4	Data Structure	362
8.7.5	Elektor RFID Reader Library: MIFARE DESFire EV1.	362
8.7.6	Example Programs	363
8.7.6.1	Creating a DESFire Application	363
8.7.6.2	Standard Data File: Reading and Writing Data	366
8.8	Application Protocol Data Units (APDUs)	368
8.8.1	Command APDU Data Structure.	368

8.8.1.1	Class Byte (CLA)	369
8.8.1.2	Instruction Byte (INS)	369
8.8.1.3	Parameter Bytes P1 and P2	369
8.8.1.4	Coding of Length Fields Lc and Le	369
8.8.2	Response APDU Data Structure	371
8.8.3	Examples of ISO/IEC 7816-Compatible APDUs	372
8.8.3.1	The SELECT Command	372
8.8.3.2	The READ BINARY Command	373
8.8.3.3	The Update Binary Command	375
8.8.4	Elektor RFID Reader Library: APDU	376
8.8.5	Accessing an ISO/IEC 7816 File System	378
8.8.5.1	Example Program	380
9	Elektor RFID Projects	385
9.1	Programming the MF RC522 Reader IC	385
9.1.1	Elektor RFID Reader Library: MF RC522	386
9.1.2	Program Examples	386
9.1.2.1	Changing the RF Parameter Configuration	386
9.1.2.2	MF RC522 SFR Programming — Card Activation	387
9.2	RFID Access Control Systems.	396
9.2.1	Online Systems	396
9.2.2	Offline Systems	396
9.2.3	Elektor RFID Reader as Access Control System	396
9.2.3.1	Functional Description	397
9.2.3.2	Access Control Manager	398
9.2.3.3	Microcontroller Firmware	399
9.2.3.4	Reading and Deleting from the P89LPC936 EEPROM	404
9.3	An Electronic ID Card	406
9.3.1	Personalization.	406
9.3.2	Reading the ID Card Data	407
9.4	Launching a Windows Application	408
10	Smart Card Reader API Standards.	411
10.1	Introduction	411
10.2	Card Terminal API (CT-API)	412
10.3	Open Card Framework (OCF)	412
10.4	Personal Computer/Smartcard (PC/SC)	413
10.4.1	The PC/SC Architecture.	413
10.4.1.1	Integrated Circuit Card (ICC)	414
10.4.1.2	Interface Device (IFD)	414
10.4.1.3	Interface Device Handler (IFD Handler)	414
10.4.1.4	ICC Resource Manager (RM)	415
10.4.1.5	Service Provider	416
10.4.1.6	ICC-Aware Applications	417

11	PC/SC Readers	419
11.1	Contactless Cards	419
11.1.1	Contactless Microcontroller Smartcards	419
11.1.2	Contactless Memory Cards	419
11.1.2.1	PC/SC-Compliant APDUs	420
11.1.3	Answer To Reset (ATR)	422
11.1.3.1	Contact-type Card Activation Sequence	422
11.1.3.2	ATR Structure of a Contact-Type Smartcard	424
11.1.3.3	Contactless Smartcard Pseudo-ATR Structure	425
11.2	The Microsoft WinSCard API	427
11.2.1	WinSCard API Programming	428
11.2.1.1	Programming the WinSCard API in C	430
11.3	Java and PC/SC	438
11.3.1	JPC/SC Java API	438
11.3.2	Java Smartcard I/O API	440
11.4	The CSharpPCSC Wrapper for .NET	441
11.4.1	How Does One Create an API Wrapper?	441
11.4.2	The WinSCard Class	442
11.4.3	The PCSCReader Class	445
11.4.4	Program Examples	447
11.4.4.1	"Hello Contactless Card"	447
11.4.4.2	Determine All Installed PC/SC Drivers	449
11.4.4.3	Getting the Reader and Card Properties	451
11.4.4.4	Testing the Reading Range	452
11.4.4.5	Determining the Type of Contactless Memory Card	455
11.4.4.6	MIFARE Classic 1K/4K and MIFARE Ultralight	456
11.4.4.7	MIFARE DESFire EV1	459
12	List of Abbreviations	465
13	Bibliography	469
14	Index	471

射频识别：
应用中的 MIFARE 和非接触式智能卡
(影印版)

Gerhard H. Schalk, Renke Bienert 著

南京 东南大学出版社

图书在版编目(CIP)数据

射频识别:应用中的 MIFARE 和非接触式智能卡:
英文/(德)沙尔克(Schalk, G.H.), (德)比奈特(Bienert, R.)
著. —影印本. —南京:东南大学出版社, 2015.9

书名原文:RFID:MIFARE and Contactless Smartcards
in Application

ISBN 978-7-5641-5947-4

I. ①射… II. ①沙… ②比… III. ①射频-无
线电信号-信号识别-英文 IV. ①TN911.23

中国版本图书馆 CIP 数据核字(2015)第 170009 号

© 2013 by Elektor International Media BV

Reprint of the English Edition, jointly published by Elektor International Media BV and Southeast University Press, 2015. Authorized reprint of the original English edition, 2015 Elektor International Media BV, the owner of all rights to publish and sell the same.

All rights reserved including the rights of reproduction in whole or in part in any form.

英文原版由 Elektor International Media BV 出版 2013。

英文影印版由东南大学出版社出版 2015。此影印版的出版和销售得到出版权和销售权的所有者——Elektor International Media BV 的许可。

版权所有,未得书面许可,本书的任何部分和全部不得以任何形式重制。

射频识别:应用中的 MIFARE 和非接触式智能卡(影印版)

出版发行:东南大学出版社

地 址:南京四牌楼 2 号 邮编:210096

出 版 人:江建中

网 址:<http://www.seupress.com>

电子邮件:press@seupress.com

印 刷:常州市武进第三印刷有限公司

开 本:787 毫米×980 毫米 16 开本

印 张:30.25

字 数:592 千字

版 次:2015 年 9 月第 1 版

印 次:2015 年 9 月第 1 次印刷

书 号:ISBN 978-7-5641-5947-4

定 价:89.00 元

本社图书若有印装质量问题,请直接与营销部联系。电话(传真):025-83791830

此为试读,需要完整PDF请访问: www.ertongbook.com