基于安全与纠错算法的增强型蓝牙基带研究与实现

李振荣 庄奕琪 张 博 牛玉峰

(西安电子科技大学微电子学院 宽禁带半导体材料与器件教育部重点实验室 西安 710071)

摘 要 基于蓝牙在安全、纠错和抗干扰方面的不足,分析和改进了蓝牙协议数据链路层的跳频和纠错算法。分析了基于高级加密标准(AES)迭代型分组密码算法构造的新型跳频序列的性能,仿真结果表明该序列具有良好的安全性、均匀性和相关性。针对蓝牙DM分组,采用了融合交织编码和前向纠错的增强型纠错机制,并基于Gillbert-Elliott信道模型进行了仿真。结果表明该增强型纠错机制大大提高了数据传输的抗干扰能力。提出了基于AES的跳频序列发生器和融合交织编码的增强型纠错机制的ASIC实现结构,并运用低功耗和资源优化技术,给出了VLSI实现结果。基于改进算法IP,实现了高安全、强纠错的增强型蓝牙基带,并结合标准蓝牙基带进行了性能分析。最后,采用基于平台的设计方法,搭建了蓝牙SoC系统平台,并进行了实测。

关键词 蓝牙,基带,安全性,纠错性,专用集成电路设计,片上系统平台

中图法分类号 TN918 **文献标识码** A

Research and Realization of Enhancing Bluetooth Baseband Based on Security and Error Correction Algorithm

LI Zhen-rong ZHUANG Yi-qi ZHANG Bo NIU Yu-feng

(Key Laboratory of the Ministry of Education for Wide Band-gap Semiconductor Materials and Devices, School of Microelectronics, Xidian University, Xi'an 710071, China)

Abstract The frequency hopping (FH) and error correction algorithms of Bluetooth were analyzed and improved for the defects of security and anti-jamming. The performance of FH sequences based on advanced encryption standard (AES) iterated block cipher was analyzed, and the results showed the sequences had good performance on uniformity, correlation, and security. An enhancing error correction mechanism (EECM) combining the forward error correction with interleaving was adopted for Bluetooth DM packets, and the simulation was carried out based on Gillbert-Elliott channel. The result showed the EECM could improve the anti-interference ability largely. The ASIC structures of FH sequences generator and EECM were proposed, and the realized results of these enhancing IPs were obtained by using low-power, low-cost VLSI design techniques. The performance of enhancing Bluetooth baseband was analyzed compared with the standard Bluetooth baseband. Finally, the Bluetooth system-on-chip was realized and tested by using platform-based design method.

Keywords Bluetooth, Baseband, Security, Error correction, ASIC, System on chip platform

近几年,随着无线通信技术在商业、金融、军事等领域的应用不断增加,人们对无线通信技术的性能要求也急剧提升[1]。蓝牙作为一种无线数据与语音通信的开放性全球规范,是WPAN关键技术之一,具有低功率、低成本、组网简单和适宜语音传输等突出优点[2],成为近年来发展最快的无线通信技术之一。但由于纠错能力、安全性和抗干扰性等方面的不足,使其在商业、金融等领域的应用大大受限。如要进一步加强蓝牙技术在无线通信领域的优势,就必须对现有蓝牙技术进行改进,尤其是在安全能力和抗干扰能力方面。

本文将分析标准蓝牙的技术特点,针对蓝牙的安全和纠错算法进行研究,提出相应的增强型算法或改进策略,并采用低功耗、低成本的VLSI设计方法,实现高安全性和强纠错能力的增强型蓝牙基带芯片。

1 蓝牙技术及算法分析

蓝牙是一种开放性短距离无线通信技术,它以低成本的近距离无线连接为基础,为固定与移动设备通信环境建立一个特别连接。蓝牙采用快速跳频和时分多址技术[3],提供两种不同形式的链路,即支持数据流量的异步无连接链路和支持语音流量的同步面向连接链路。数据链路层是蓝牙通信系统的核心组成部分。为满足基本的安全和抗干扰性能需求,采用了蝶型跳频选择算法和前向纠错机制,具体功能在蓝牙基带中实现。

1.1 蝶形跳频选择算法

蓝牙采用TDD(Time-Division Duplex)时分双工方式进行通讯[4],ISM频段被划分为79/23个带宽为1MHz的频

到稿日期:2009-09-23 返修日期:2009-12-21 本文受国家自然科学基金项目(60676053)资助。

李振荣(1979-),男,博士生,主要研究方向为短距离无线通信芯片系统设计等,E-mail:allen_lzr@126.com;庄奕琪(1957-),男,博士,教授,博士生导师,主要研究方向为通信与功率系统集成、短距离无线通信芯片设计等;张 博(1983-),男,博士生,主要研究方向为射频与微波芯片设计;牛玉峰(1976-),男,博士生,主要研究方向为无线通信纠错算法。

点，跳频速率为 1600/3200 跳/s。以 79 跳模式为例，跳频系统在 2.402GHz 到 2.480GHz 之间进行跳频，载频为(2402+k)MHz(k=0,1,2,…,78)。如图 1 所示，跳频选择算法包括两个步骤：首先生成一个伪随机数，构造可以有效避免频段内干扰的跳频频点。在蓝牙基带中，跳频序列由本地时钟和蓝牙设备地址两个输入变量通过蝶型运算产生。第二阶段完成从伪随机数到跳频频点的映射，由射频模块中的频率合成器实现。尽管目前基于蝶形运算的跳频选择算法实现简单，硬件开销小，但是该算法过于简单，已无法满足目前跳频通信系统较高的安全性和抗干扰性要求[5-7]，尤其是在军事、金融等领域。

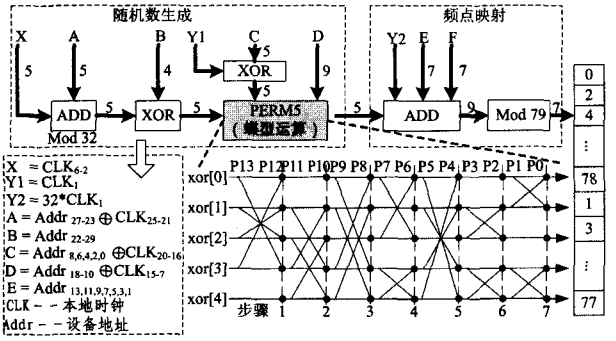

图 1　蓝牙跳频选择算法原理

1.2　FEC 纠错算法

标准蓝牙数据采用两种纠错机制[4]，分别是 1/3FEC 和 2/3FEC，在数据传输中配合信道质量灵活采用。FEC 纠错机制能够在一定程度上保证数据传输的准确性，但也会降低平均传输速率。1/3FEC 编码方式是一种较简单的纠错码方式，将要传输的数据重复传输 3 次即可。解码时采用多数表决的方法即可解码。2/3FEC 编码是一个(15,10)的截短汉明码，应用于蓝牙 DM 数据分组，编码时的生成多项式为：

$$g(D)=(D+1)(D^4+D+1)=D^5+D^4+D^2+1$$

解码校验矩阵为：

$$H=[x^{14^{-T}},x^{13^{-T}},x^{12^{-T}}\cdots x^{2^{-T}},x^{1^{-T}},x^{0^{-T}},](\mathrm{mod}\ g(x))$$

1/3FEC 和 2/3FEC 对于信道中较少且独立的突发错误，有较好的纠错能力，但在实际的无线信道中，往往存在突发的连续干扰，此时 FEC 纠错能力会十分有限。

2　基于 AES 的跳频选择算法分析

跳频序列对跳频通信系统的性能有着决定性影响，标准蓝牙基于蝶型运算构造的跳频序列在安全性、均匀性和随机性等方面已无法满足金融、军事等领域的通信需要。寻求具有理想特性的跳频序列，已成为跳频通信的重要课题之一[5]。尽管在一些文献中[6,7]已经对基于 DES 等密码理论构造的跳频序列性能进行了一定的分析，但随着通信系统对于安全性、功耗和成本的要求不断提高，设计一个具有更高安全性和跳频特性，且具有高速、低硬件开销特点的跳频序列发生器成为一个巨大挑战。本文分析了基于高级加密标准(AES)迭代型分组密码构造的新型跳频序列的性能，并基于分析结果，提出了一种应用于蓝牙的高速跳频、低功耗和低成本的新型跳频序列发生器。

2.1　安全性分析

基于 AES 算法构造的跳频序列，其安全性是由 AES 算法的安全机制决定的。AES 标准是由美国国家标准与技术研究院(NIST)于 2002 年制定的高级加密标准，用于替代美国数据加密标准(DES)算法。根据 Shannon 提出的密码设计“混淆”和“扩散”原则，AES 算法的设计策略是针对差分分析和线性分析提出的宽轨迹策略(Wide Trail Strategy)，算法采用替代/置换网络，符合“混淆”和“扩散”原则，具有很高的安全性[8,9]。S-Box 构造中有限域 GF(2^8)逆操作使线性逼近和差分分布表中的各项趋于均匀分布，对差分分析和线性分析具有良好的免疫力。总之，对于已知攻击而言，AES 算法具有极高的安全性，因而基于该算法的跳频序列也具有良好的安全性。

2.2　均匀性分析

对于跳频系统，可根据卡方分布检验[6,7]，用式(1)衡量跳频序列的均匀性。卡方值越小，分布状态越符合均匀分布。

$$\chi^2_{k-1}=\sum_{t=1}^{k}\frac{(N_f-LP_t)^2}{LP_t},P_t=\frac{1}{k}\qquad(1)$$

假定跳频信道数 k 为 64，置信度 α 为 0.05，分别采用 $\chi^2_{k-1}=82.244$，$\chi^2_{k^2-1}=4244.7$ 作为等分布检验和连续性检验标准。随机选取 10 组序列进行仿真，均通过测试，如图 2 所示。说明基于 AES 算法的跳频序列具有良好的均匀性。

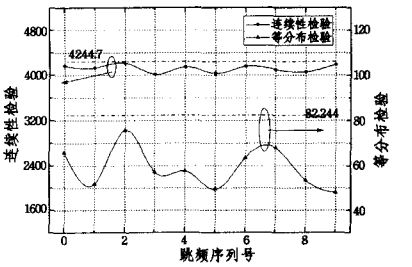

图 2　跳频序列均匀性分析

2.3　汉明相关性分析

跳频通信系统的相互干扰由各系统所采用的跳频序列的汉明相关性决定，可由式(2)表示：

$$H_{XY}(\tau)=\sum_{i=0}^{N-1}h(X_i,Y_{i+\tau}),h(x,y)=\begin{cases}1, & X_i=Y_{i+\tau}\\ 0, & X_i\neq Y_{i+\tau}\end{cases}\qquad(2)$$

式中，X,Y 为跳频序列，$0\leqslant\tau\leqslant N-1$，$N$ 表示($i+\tau$)的模。若 X,Y 为相同序列，运算结果表示序列的汉明自相关值，否则表示序列的互相关值。文献[7,10,11]的分析方法，假设序列长度为 10000，信道数为 64，算得序列的自相关和互相关值均应小于 $\chi^2_{10000-2}(0.05)=10231.46$。随机选取 20 组数据，对加密后的密文序列进行分析。仿真结果如图 3 所示，证明基于 AES 的跳频序列具有良好的汉明相关性。

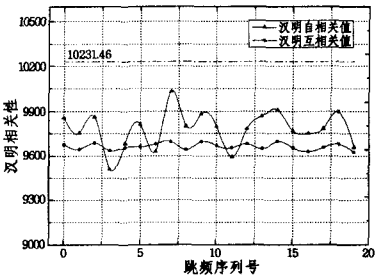

图 3　汉明相关性分析

3　融合交织编码和 FEC 的纠错算法研究

3.1　算法描述

标准蓝牙对于 DM(包括 DM1,DM3,DM5)数据分组的载荷定义了基于 2/3FEC 的纠错机制,适合纠正少量相对独立的差错,对于会导致连续误码的突发干扰,纠错能力有限。针对此缺陷,本文采用了融合交织编码和 FEC 的纠错算法。交织编码是将数据在发送前排列成 M 行 N 列再按行读出,在遇到突发干扰时,可把一个较长的突发差错离散成随机差错。若干扰片的尺寸为 m,交织编码后的干扰片尺寸就变为 m/M。只要 m/M 小于差错控制电路的纠错范围,便可克服干扰的影响。蓝牙传输的 DM 数据首先经交织编码处理,可有效克服衰落信道中突发性干扰[12],之后采用能够纠正随机差错的 2/3FEC 编码技术和出错重传机制来消除随机差错,从而达到提高纠错概率、降低信道误码率、改善传输特性的目的[13]。下面基于 Gillbert-Elliott(G-E)信道[14,15]对该纠错机制进行仿真分析。

3.2 G-E 信道模型及吞吐率仿真

G-E 信道是一阶、离散的静态马尔可夫链,具有 Good 和 Bad 两个状态。如图 4 所示,Pgb,Pbg,Pbb,Pgg 分别表示信道在 Good 和 Bad 两种状态下的相应转换概率[14,15]。

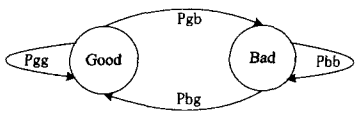

图 4 G-E 信道模型

对于长度 n,可纠正 t 个随机错误的编码字$[n,t]$,在连续 n 个状态中有 d 个错误的概率如式(3)所示[15]:

$$P_n(d)=\begin{cases}P(G)(1-P_{gb})^{n-1}, & d=0\\ P(G)(P_n(d|GG)+P_n(d|GB))+\\ \quad P(B)(P_n(d|BG)+P_n(d|BB)), & 1\leqslant d<n\\ P(B)(1-P_{bg})^{n-1}, & d=n\end{cases} \tag{3}$$

蓝牙数据传输吞吐量可表示为信道状态变化概率的函数。在 G-E 信道中,分别在融合交织编码前后的两种纠错机制下,对蓝牙 DM 数据分组的传输吞吐量进行了仿真(分别表示为 DM 和 DME)。在不同信道状态变化概率下,得到数据传输吞吐量与信道变化概率的关系曲线,如图 5 所示。表明 DM 数据包增加交织编码运算后,能大大提高纠错性能以及传输中抗突发错误和多径效应影响的能力,从而提高数据传输吞吐率。

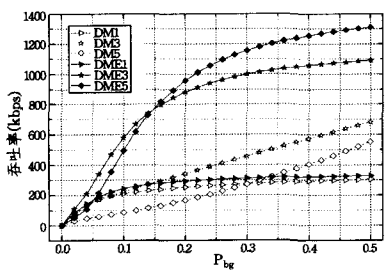

图 5 基于 G-E 信道的吞吐量仿真

4 增强型蓝牙基带实现

4.1 AES 跳频选择 IP 实现

上述理论分析证明,基于 AES 分组加密算法构造的跳频序列具有良好的安全性、均匀性和汉明相关性,可构造出性能突出的跳频序列。但由于 AES 算法复杂度较高,资源消耗较大,且蓝牙基带对低功耗和低成本有较高要求,因此将该跳频序列发生器集成到增强型蓝牙基带时需考虑 VLSI 优化实现。本文结合 AES 算法硬件实现原理[16],实现了基于 AES 算法的快速、低功耗和低成本的跳频序列发生器 IP,结构如图 6 所示。

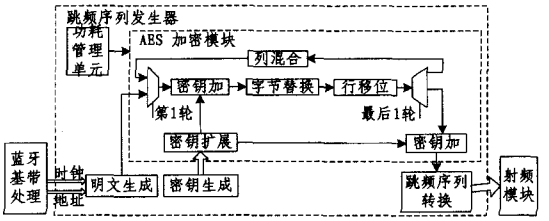

图 6 基于 AES 算法的跳频序列发生器结构图

字节变换模块是 AES 算法的核心模块,也是 AES 算法硬件实现资源开销最大的模块之一。为了便于将该跳频发生器 IP 集成到蓝牙基带中,本文对 AES 算法的字节变换操作进行了优化,在提高算法处理速度的同时尽可能降低资源开销。

字节变换是一个利用替换表(S-box)进行的非线性字节替换操作。针对每个字节,该运算包含两个步骤:首先在有限域 $GF(2^8)$ 中求得乘法逆,然后进行仿射变换,描述如下:

$$b_i'=b_i\oplus b_{(i+4)\bmod 8}\oplus b_{(i+5)\bmod 8}\oplus b_{(i+6)\bmod 8}\oplus b_{(i+7)\bmod 8}\oplus c_i \tag{4}$$

替换表(S-Box)的 VLSI 实现涉及较复杂的逻辑运算,资源开销大。因此,如何减少逻辑资源,是设计 S-Box 的关键因素。目前主要有两种 S-Box 的实现方式:查找表(Look-Up Table)和有限域运算。在本文中,采用了有限域运算的方法来达到降低硬件开销的目的[17],即采用基于有限域 $GF((2^4)^2)$ 的 S-Box 高效实现,结构如图 7 所示。这样,复杂的有限域 $GF(2^8)$ 运算被映射到规模较小的子有限域 $GF(2^4)$ 上,从而加速和简化了有限域 $GF(2^8)$ 的计算,同时能够大大降低硬件实现的复杂度和资源消耗。此外,密钥扩展模块也需要用到 S-Box 模块。

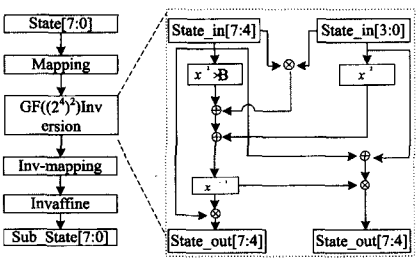

图 7 字节替换结构优化实现

此外,在该跳频发生器 IP 中,结合 VLSI 资源复用技术和低功耗技术,采用了基于动态门控时钟技术的层次化功耗管理策略[18]。最终实现的跳频发生器 IP 最大功耗为 0.033mW/MHz,等效逻辑门为 9.9k,最大跳频速率为 1098901 跳/s,完全能够满足蓝牙最高 3200 跳/s 的高速跳频要求,且延时很短,跳频序列性能大大提高。

4.2 融合交织编码和 FEC 的增强型纠错 IP 实现

标准蓝牙对 DM 数据分组的 FEC 纠错处理在基带部分完成。因此,在增强型蓝牙基带中集成上述增强型纠错机制,需在蓝牙基带与上层接口间增加交织/解交织模块。当蓝牙设备处于发送状态时,下行数据先经过交织运算,再进行基带

处理；而对于接收状态，上行数据经过基带接收处理后，再经过解交织运算，才能传送给上层接口。整体的数据处理流程和交织编码基本操作如图 8 所示。

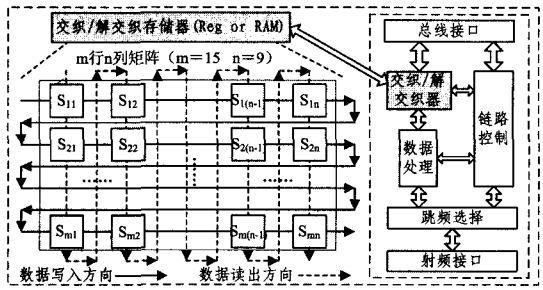

图 8　具有交织器的纠错机制结构图

蓝牙通信系统通过 DM 数据分组进行数据传输的实时性要求较低，因此在数据处理过程中增加交织编码运算后引入的硬件处理延时对系统数据传输影响不大。本文中，交织器 IP 基于存储器的矩阵转置变换操作实现，逻辑操作简单，考虑到 VLSI 实现过程中交织深度与引入的硬件开销成正比，采用了 15×9 存储矩阵进行交织运算，增加的硬件开销在可接受范围内。本文采用寄存器结构作为交织存储器（也可基于双端口 RAM 实现），最大功耗为 0.031mW/MHz，等效逻辑门为 8.2k，易于集成，满足增强型蓝牙基带要求。

4.3　增强型基带实现及性能

标准型和增强型蓝牙基带基于 SMIC 0.18um 标准工艺库，进行门级综合和功耗分析。图 9 为增强型蓝牙基带 IP 各子模块的面积和功耗开销分布。

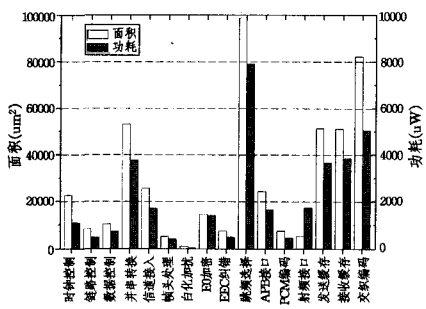

图 9　增强型基带各模块功耗和面积分布

标准型和增强型蓝牙基带实现的整体性能对比评估如表 1 所列，包括最高频率、面积、功耗、等效门数指标以及基于 FPGA 进行功能验证的资源开销对比。虽然整体设计采用了低功耗和资源优化技术，但由于引入的增强型改进算法在提高性能的同时引起了部分模块资源和功耗的增加，导致增强型蓝牙基带整体功耗和面积开销比标准基带有所增加，但仍属于可接受范围内。

表 1　标准型和增强型蓝牙基带性能比较

参数	ASIC(0.18um)			FPGA(Xc2v8000)		
	A/mm²	P/mW	f/MHz	Slice	P/mW	f/MHz
标准基带	0.32	25.1	133	1995	337	95
改型基带	0.47	35.4	105	3900	427	84

蓝牙 SoC 是由基带、射频收发、处理器、固件等组成的复杂片上系统。本文采用了基于平台设计（Platform-Based Design，PBD）的方法[19,20]集成增强型蓝牙基带，并编写蓝牙固件，快速构建了蓝牙 SoC 系统的设计、验证和测试平台，如图 10 所示，其中 SoC 平台和射频模块为实物图。

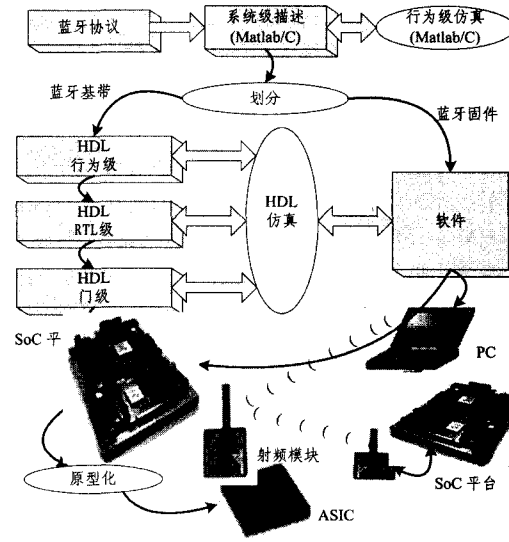

图 10　基于 PBD 的蓝牙 SoC 设计流程

蓝牙 SoC 平台内 ARM9 处理器运行蓝牙固件，控制逻辑板加载的增强型蓝牙基带进行数据处理，通过射频芯片实现数据收发，最终完成增强型蓝牙基带的验证和蓝牙 SoC 软硬件协同设计。通过不同平台相互通信来完成增强型基带功能和传输性能的测试，以典型时隙分组 DM1，DM3 和 DM5 为例进行测试，结果表明，在有较大干扰的情况下，本增强型基带仍具有良好的传输性能，且安全性大大提高。

结束语　针对蓝牙在商业、军事等领域的应用，研究了蓝牙技术的安全性和纠错能力，提出并实现了基于 AES 加密算法构造的新型跳频序列发生器 IP，融合了交织编码和前向纠错技术的增强纠错 IP，从而大大提高了蓝牙的纠错性能、安全性和抗干扰性；在开发标准蓝牙基带基础上，实现了基于以上改进算法的高安全性、强纠错增强型蓝牙基带芯片。最后结合标准蓝牙基带，对增强型基带芯片实现结果进行了性能分析，并基于 PBD 方法进行了蓝牙 SoC 平台实测。芯片设计中采用了低功耗、资源优化技术，但对于系统功耗、面积的最优有待多角度进一步研究。

参 考 文 献

[1] Cook J A, Kolmanovsky I V, McNamara D, et al. Technologies for the Twenty-First Century Model T[C]// Control, Computing and Communications Proceedings. IEEE, 2007: 334-355

[2] Sairam K V S S S S, Gunasekaran N, Redd S R. Bluetooth in wireless communication[J]. IEEE Communications Magazine, 2002, 40(6): 90-96

[3] McDermott-Wells P. What is Bluetooth [J]. IEEE Potentials, 2004, 23(5): 33-35

[4] Bluetooth SIG. Specification of the Bluetooth System Core, Core Specification v2.0 + EDR[S]. 2004

[5] 梅文华，杨义先，周炯. 跳频序列设计理论的研究进展[J]. 通信学报，2003，24(2)：92-101

[6] Li Zan, Chang Yilin, Jin Lijun. A novel family of frequency hopping sequences for multi-hop Bluetooth networks[J]. IEEE Transactions on Consumer Electronics, 2003, 49(2): 1084-1089

（下转第 151 页）

况是能达到 SQL 的表达水平。

参 考 文 献

[1] Gregor K, Lamping J, Mendhekar A, et al. Aspect-oriented Programming[C]// Proceedings of the European Conference on Object-Oriented Programming. vol 1241: 220-242

[2] http://eclipse.org/aspectj/

[3] http://aspectwerkz.codehaus.org/

[4] http://jboss.org/jbossaop/

[5] http://www.aspectc.org/

[6] http://wwwiti.cs.uni-magdeburg.de/iti_db/forschung/fop/featurec/

[7] http://www.castleproject.org/aspectsharp/

[8] http://www.facultyresourcecenter.com/curriculum/pfv.aspx?ID=6801

[9] Douglas B, Torsten S. Solving the Java Object Storage Problem [J]. Computer, 1998, 31(11): 33-40

[10] Java Data Objects Specification[S]. Version: 2.0, 2005

[11] SUN Microsystems. Enterprise JavaBeans[S]. Version 2.0, Final Release, August 2001

[12] SUN Microsystems. Enterprise JavaBeans[S]. Version 3.0, Final Release, 2006

[13] Hibernate Reference Documentation[EB/OL]. Version: 3.2.3.ga, http://www.hibernate.org

[14] Rashid A. On to Aspect Persistence[C]// GCSE Syrup. LNCS 2177. Springer-Verlag, 2000: 26-36

[15] Rashid A. Weaving Aspects in a Persistent Environment[C]// ACM SIGPLAN Notices. Feb. 2002

[16] Rashid A, Loughran N. Relational Database Support for Aspect-Oriented Programming[C]// Proceedings of NetObjectDays. LNCS 2591. Springer-Verlag, 2002: 233-247

[17] Rashid A, Sawyer P. Dynamic Relationships in Object Oriented Databases: A Uniform Approach[C]// DEXA. LNCS 1677. Springer-Verlag, 1999: 26-35

[18] Rashid A, Chitchyan R. Persistence as an Aspect[C]// Proc. of AOSD'03. Boston, USA, 2003: 120-129

[19] Filman R, Friedman D. Aspect-oriented Programming is Quantification and Obliviousness[C]// OOPSLA Workshop on Advanced Separation of Concerns. 2000

[20] Al-Mansari M, Hanenberg S, Unland R. Orthogonal persistence and AOP: a balancing act[C]// Proceedings of the 6th Workshop on Aspects, Components, and Patterns for Infrastructure Software. Vancouver, British Columbia, Canada, March 2007: 12-16

[21] Al-Mansari M, Hanenberg S. Path Expression Pointcuts: Abstracting over Non-Local Object Relationships in Aspect-Oriented Languages[C]// NODe'06. Erfurt, Germany, 2006

[22] Campbell R, Habermann A. The Specification of Process Synchronization by Path Expressions[C]// Sym. on Operating Systems. Springer-Verlag, 1974: 89-102

[23] Elmasri R, Navathe B. Fundamentals of Database Systems(3rd ed)[M]. Addison-Wesley, 2000

[24] 陈兴润，滕腾，黄罡，等. 一种对象/关系映射隐式持久化框架[J]. 电子学报，2007，35(B12)：179-185

[25] Java Persistent Aspect[EB/OL]. http://sourceforge.net/projects/jpa/

[26] Gamma E, Helm R, Johnson R, et al. Design Patterns: Elements of Reusable Object-oriented Software[M]. Reading, MA: Addison-Wesley, 1995

[27] http://db.apache.org/ojb/

(上接第 110 页)

[7] Guo Feng, Zhuang Yi-qi, Hu Bin. Structure of Frequency Hopping Sequences Family Based on Stream Cipher[J]. Chinese Journal of Electron Devices, 2007, 30(5): 1696-1699

[8] Ho Yean Li, Samsudin A, Belaton B. Heuristic cryptanalysis of classical and modern ciphers Networks[C]// 7th International Conference on Communication. Malaysia: IEEE, 2005: 6

[9] Nadeem A, Javed M Y. A Performance Comparison of Data Encryption Algorithms Information and Communication Technologies[J]//First International Conference on Information and Communication Technologies. Karachi, Pakistan: IEEE, 2005: 84-89

[10] Chu W, Colbourn C J. Optimal frequency-hopping sequences via cyclotomy[J]. IEEE Transactions on Information Theory, 2005, 51(3): 1139-1141

[11] 王淑波，梅文华，毕笃彦. 蓝牙自适应跳频序列的性能分析[J]. 电波科学学报，2006，21(4)：612-618

[12] Nafaa A, Ahmed T, Mehaoua A. Unequal and interleaved FEC protocol for robust MPEG-4 multicasting over wireless LANs [C]// IEEE International Conference on Communications. 2004: 1431-1435

[13] Han Sunyoung, Kim Heemin, Son Kiwon, et al. Cross-correlated FEC Scheme for Multimedia Streaming over Wireless LAN[C]// 22nd International Conference on Advanced Information Networking and Applications. 2008: 217-222

[14] Gilbert E N. Capacity of a burst-noise channel[J]. Bell Syst. Tech. J, 1960, 39: 1253-1265

[15] Wilhelmsson L, Milstein L B. On the Effect of Imperfect Interleaving for the Gilbert-Elliott Channel[J]. IEEE Transactions on Communications, 1999, 47(5): 681-688

[16] Federal Information Processing Standards Publication (FIPS) 197. Specification for the Advanced Encryption Standard(AES) [S]. 2001

[17] Salomon D. Data Privacy and Security[M]. Beijing: Tsinghua University Press, 2005: 292-302

[18] Nakajima M, Yamamoto T, Yamasaki M, et al. Low Power Techniques for Mobile Application SoCs Based on Integrated Platform "UniPhier"[C]// IEEE Design Automation Conference. 2007: 649 - 653

[19] 熊志辉，李思昆，陈吉华，等. 支持平台设计方法的系统芯片协同设计环境[J]. 计算机辅助设计与图形学学报，2005，17(7)：1401-1406

[20] 章立生，韩承德. SoC 芯片设计方法及标准化[J]. 计算机研究与发展，2002，39(1)：1-8