ISSN: 2150-8194 (Print), 2150-8208 (Online) Vol. 1, No. 1, July 2009

Intelligent Information Management

智能信息管理 國際期刊

Editor-in-Chief: Dr.Bin Wu

www.scirp.org/journal/iim

Scientific Research

Journal Editorial Board

ISSN: 2150-8194 (Print), 2150-8208 (Online)

http://www.scirp.org/journal/iim

Editor-in-Chief

Dr.Bin Wu **National Library of China, China**

Editorial Board (According to Alphabet)

Dr. Xilin Chen	Chinese Academy of Sciences, China
Prof. Zhoujun Li	Beihang University, China
Prof. Zhendong Niu	Beijing Institute of Technology, China
Prof. Yigang Sun	National Library of China, China

Intelligent Information Management, 2009, 1-63
http://www.scirp.org/journal/iim

Scientific Research

Table of Contents

The Analysis and Amendment of Security System in 3G.....**01**
Min ZHAO, Ling SHI

Investigations on Simultaneously Secure IBE Scheme and Security Proofs under RO and Non-RO Model.....**06**
Zhengtao JIANG, Yongbin WANG, Yong WANG, Yumin WANG

Total Domination Number of Generalized Petersen Graphs.....**15**
Jianxiang CAO, Weiguo LIN, Minyong SHI

Henan Cultural Information Resources Sharing Project Persistent Effect Mechanism Research.....**19**
Weigong CUI, Hui JIAN, Yuan GAN, Zhen ZHANG, Yanfeng LIU

Reasoning with Ontology Model Based on Jena.....**25**
Jing WU, Yongxin HUANG

Design of Collaborative Platform on Clustering Applications for Governments.....**32**
Xue-Wang ZHANG, Zhou-Jun LI, Wei SHEN

A New Method for Calculating Similarity between Sentences and Application on Automatic Abstracting.....**38**
Wenqian JI, Zhoujun LI, Wenhan CHAO, Xiaoming CHEN

Application of a Sign Language Synthesis System in Digital Library Services.....**46**
Jing WAN, Bin WU, Yingxin QIAO

Virtual Home Library System.....**54**
—— Let every Chinese family having their own libraries
Bin WU, Shu SONG, Jianxiang CAO, Wen RU

The Design of the Minimum Spanning Tree Algorithms.....**60**
Zhicheng LIU, Bo JIANG

Copyright © 2009 SciRes

Intelligent Information Management (IIM)

Journal Information

SUBSCRIPTIONS

The *Intelligent Information Management* (Online at Scientific Research Publishing, www.SciRP.org) is published quarterly by Scientific Research Publishing, Inc., USA.

E-mail: service@scirp.org

Subscription rates: Volume 1 2009
Print: $50 per copy.
Electronic: free, available on www.SciRP.org.
To subscribe, please contact Journals Subscriptions Department, E-mail: service@scirp.org

Sample copies: If you are interested in subscribing, you may obtain a free sample copy by contacting Scientific Research Publishing, Inc. at the above address.

SERVICES

Advertisements
Advertisement Sales Department, E-mail: service@scirp.org

Reprints (minimum quantity 100 copies)
Reprints Co-ordinator, Scientific Research Publishing, Inc., USA.
E-mail: service@scirp.org

COPYRIGHT

Copyright© 2009 Scientific Research Publishing, Inc.

All Rights Reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except as described below, without the permission in writing of the Publisher.

Copying of articles is not permitted except for personal and internal use, to the extent permitted by national copyright law, or under the terms of a license issued by the national Reproduction Rights Organization.

Requests for permission for other kinds of copying, such as copying for general distribution, for advertising or promotional purposes, for creating new collective works or for resale, and other enquiries should be addressed to the Publisher.

Statements and opinions expressed in the articles and communications are those of the individual contributors and not the statements and opinion of Scientific Research Publishing, Inc. We assumes no responsibility or liability for any damage or injury to persons or property arising out of the use of any materials, instructions, methods or ideas contained herein. We expressly disclaim any implied warranties of merchantability or fitness for a particular purpose. If expert assistance is required, the services of a competent professional person should be sought.

PRODUCTION INFORMATION

For manuscripts that have been accepted for publication, please contact:
E-mail: iim@scirp.org

Intelligent Information Management, 2009, 1-5
doi:10.4236/iim.2009.11001 Published Online July 2009 (http://www.scirp.org/journal/iim)

The Analysis and Amendment of Security System in 3G

Min ZHAO, Ling SHI
Computer Department, East China University of Science and Technology, Shanghai, China

Abstract: This paper analyses security mechanism and authentication, key agreement protocol of 3G system amply, puts forward a amelioration scheme. This scheme assures security communications without credible VLR. This paper analyses ameliorative protocol and resolves the security communications problem between MS and HLR.

Keywords: 3G Security, 3G Security Structure, 3G authentication and key agreement protocol Security arithmetic

3G 系統安全體制分析與協議改進

趙　敏，史　令
華東理工大學 計算機系 200237

摘　要：本文對 3G 系統安全體制和認證、密鑰分配協議進行了詳細分析，提出了對協議的改進方案，從而保證有不完全可信 VLR 參與的保密通信，並對改進方案進行了分析，解決了 MS 到 HLR 之間的通信安全問題。

關鍵詞：3G 安全，3G 安全體制，3G 認證與密鑰協商，安全算法

1. 引 言

在第三代移動通信系統中，除了傳統的話音業務外，電子商務、電子貿易、網路服務等新型業務將成為 3G 的重要業務內容。目前，2G 網路已經投入了大量資金和設備，廢棄 2G 網路在一種新的安全體制之上開發 3G 網路是不現實的作法。移動通信中 3G 網路與 2G 網路的共存是目前移動通信向 3G 過渡必然要經歷的階段。因此，3G 網路要繼承 2G 網路，無法改變建立在對稱密碼安全體制之上的 2G 安全體制。從 1996 年起，歐洲電信標準學會著手開發 3G 移動系統，並逐漸由 3GPP 取代，其目的是制定一個全球統一的移動應用規範。3G 安全的設計宗旨是在 2G 安全的基礎上有所提高，以提供新的安全性能與服務。因此，在移動通信系統中，資訊的加密仍將採用對稱密碼體制，為實現資訊的加密傳輸，通信雙方必須首先進行身份認證，協商會話密鑰[1]。在現有 2G 網路中引入 3G 接入設備和網路實體時,要在儘量不改變原有 2G 網路實體的基礎上,實現與現有 2G 網路的交互，使移動網路能為雙模式手持設備用戶提供通過使用 SIM 卡或 USIM 卡在 2G 和 3G 網路的接入和服務[2]。

3G 安全體制不是端到端的安全機制, 給密級較高的應用帶來困難。比如, 如果 VLR 在一個不被信任的網路域中，由於在 3G 系統中它可以獲取通信所需的 CK 和 IK 的，這樣對 VLR 而言，就沒有什麼秘密可言。

2. 3G 安全體制

3G 的安全目標是: 保證由用戶產生的或與用戶相關的資訊能夠得到充分保護，防止被誤用或盜用；保證由服務網路或歸屬環境提供的資源和業務能夠得到充分保護，防止被誤用或盜用；保證標準化的安全特徵至少應有一個可以在世界範圍的基礎上輸出的加密

Copyright © 2009 SciRes

演算法；保證安全特徵被充分的標準化，以確保世界範圍內互操作與不同的服務網路之間的漫遊；保證提供給用戶和業務供應者的保護級別比現代固定和移動網路提供的高；保證 3GPP 安全特徵、機制和實現能被擴展和加強[3]。

3G 安全體制的總體結構分為 3 個層面和 5 個部分：

⑴ 網路接入安全：提供安全接入 3G 服務網的機制，並抵禦無線鏈路攻擊。這一部分功能包括：用戶身份保密、認證和密鑰分配、資料加密和完整性等。認證過程也融合了加密、完整性保護等措施。

⑵ 網路域安全：保證網內信令的安全傳送並抵禦對有線網路的攻擊。

⑶ 用戶域安全：主要保證對移動台的安全接入，包括用戶與智慧卡間認證、智慧卡與終端的認證及其鏈路的保護。

⑷ 應用域安全：使用戶域與服務提供商的應用程式間能夠安全的交換資訊。

⑸ 安全特性的可視性及可配置能力：主要指用戶能獲知安全特性是否在使用以及服務提供商提供的服務是否需要以安全服務為基礎[4]。

加密和完整性保護是實現安全通信的核心，認證與密鑰分配是實現安全通信的重要保證。3G 系統的安全體制是建立在 2G 的基礎上，GSM 及其他 2G 系統中已被證明是必須和穩健的安全元素將繼續被採用，3G 還將改進 2G 中的安全弱點，最終提供全新的安全性能和業務。3G 相關安全協議很多，本文針只對其中的核心部分，認證與密鑰分配協議進行分析與改進。

3. 3G 認證與密鑰分配協議分析與改進

3G 安全系統定義了一些安全演算法，下面只介紹本文所用到的安全演算法：

f1=>MAC：產生消息認證碼；

f2=>XRES：用於消息認證中計算期望回應值；

f3=>CK：產生加密密鑰；

f4=>IK：產生完整性密鑰；

f5=>AK：產生匿名密鑰；

3G 認證與密鑰分配由 f1~f5 實現。

3G 規範中 UMTS 鑒權過程是建立在每個用戶唯一的用戶鑰匙 K 的基礎上的，K 存儲在 USIM 和用戶環境歸屬 AuC 中。MS：移動站；AKA：認證與密鑰分配；UE：用戶終端；HLR：歸屬位置寄存器；VLR：訪問位置寄存器；HE：本地環境；AV：認證向量，AV=RAND||XRES||CK||IK||AUTH ； XRES=f2(K ，RAND)；CK=f3(K，RAND)；IK=f4(K，RAND)；AUTH=SQN ⊕ AK||MODE||MAC；MODE：移動性管理標識；MAC=f1(K，SQN||RAND||MODE)。

3.1 協議過程分析

認證協定分為以下幾個步驟：

⑴ MS➔VLR：IMSI||HLR；

⑵ VLR➔HLR：IMSI；

⑶ HLR➔VLE：認證向量 AV；

⑷ VLR➔MS：RAND||AUTH；

⑸ MS➔VLR：RES

首先 VLR 收到 MS 的註冊請求，MS 發送用戶自己的 IMSI 和 HLR 資訊給 VLR；

VLR 接收到該請求後，將 IMSI 轉發給 MS 的 HLR；

HLR 接到 IMSI 後產生 SQN，RAND，按照上述公式計算認證向量 AV，併發送給 VLR；

VLR 接收到 AV 後，將解析到的 RAND 和 AUTH 轉發給 MS；

MS 接收到認證請求回應後，計算 XMAC= f1(K，SQN||RAND||MODE)，比較是否等於 MAC，如果不同，則向 VLR 發送拒絕認證消息並放棄該過程。接下來檢測 SQN 是否在合理的範圍內，如果不在合理範圍內，就向 VLR 發送“同步失敗”消息，放棄該過程。如果上面檢測都通過了，MS 計算 RES、CK 和 IK，並將 RES 發送給 VLR；

VLR 接收到 RES 後，與 XRES 比較，如果 RES 與 XRES 相同，認證成功，否則認證失敗。協定流程如圖 1 所示。

3.2 安全性分析

前面已經提到 MS 與 HLR 之間共用一個密鑰 K，該密鑰的安全是 3G 安全體制的基本保障。因為 3G 安全體制建立在對稱密碼體制基礎上，所以對稱密鑰的安全顯得尤為重要。

⑴ 認證安全分析：我們已經知道，3G 安全認證是雙向認證，MS 需要認證 HLR，VLR 需要認證 MS。

VLR 接收到來自 HLR 的認證向量中包含了期望 MS 產生的應答 XRES=f2(K，RAND)。若 MS 是合法用戶，在接收到 VLR 返回的 RAND 後，只有合法的

Copyright © 2009 SciRes

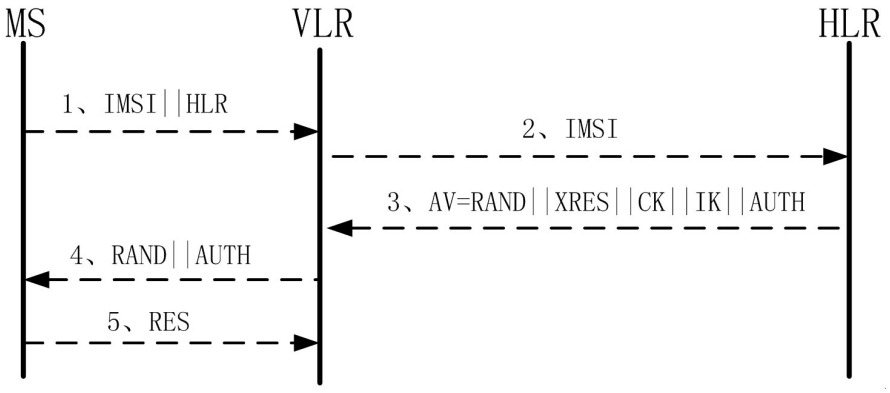


圖 1. 認證與密鑰分配過程
Figure 1. Authentication & key distribution process

MS 才能計算出 RES=f2(K, RAND), 且 RES=XRES。因為 K 由 MS 和其歸屬的 HLR 所掌握，所以別人無法計算得出 RES。這樣, 就實現了 VLR 對 MS 的認證。

MS 對 HLR 的認證是通過消息認證碼 MAC 來實現的。MS 接收到 VLR 轉發的來自 HLR 的 MAC=f1(K, SQN||RAND||MODE)，計算 XMAC=f1(K，SQN||RAND ||MODE)，在保證 SQN 的正確性前提下，MAC=XMAC，則認證成功。因為對稱密鑰 K 在 HLR 也掌握，隨意只有合法的 HLR 才能計算出與 MS 計算得到相同的 MAC 值，這樣就實現了 MS 對 VLR 和 HLR 的認證。

⑵ 加密和完整性密鑰每次會話都更新

MS 與 VLR 之間每次通信均採用不同的密鑰 CK 與 IK。由於每次通信前的認證選擇了不同的認證向量, 保證每次通信採用的 CK 和 IK 是採用不同的亂數得到的。而每次使用的消息認證碼 MAC 是由不斷遞增的序列號 SQN 作為其輸入參數之一, 保證了認證消息的新鮮性，從而確保密鑰的新鮮性，但在一次會話建立後直到該會話結束 CK 與 IK 不會改變。

⑶ 資料完整性

通過在消息中包含哈希值來進行完整性驗證。在認證和密鑰分配過程中，通信雙方協商了完整性密鑰 IK，通過 IK 可以保證資料沒有被修改。

⑷ MS 與 VLR 之間的密鑰分配安全性

VLR 接收到來自 HLR 的認證向量中包含了加密密鑰 CK 與完整性密鑰 IK，合法用戶在收到正確的亂數 RAND 後，能正確產生 CK=f3(K，RAND)，CK 與 IK 未在無線介面中傳輸，確保了密鑰的安全性。也就是說，CK 與 IK 在 HLR 和 MS 端分別產生，由於有共用密鑰 K，所以雙方產生的 CK 和 IK 是一致的。

3.3 協議改進

從上面分析可以看出, 目前 3G 通過在 MS 和 HLR 共用密鑰, 達到 MS 與 VLR 之間加密通信。也就是說, MS 可以用與 VLR 之間協商的 CK 和 IK 進行加密通信，但無法從 3G 安全協議本身保證從 VLR 和 HLR 之間的安全通信，VLR 和 HLR 之間的安全通信是通過網路域的保密措施來保證的, 3G 協議本身並未對次進行定義。

3G 的認證與密鑰分配協議在假定 HLR 與 VLR 之間安全的前提下，實現了用戶終端對網路 HLR/VLE 的認證和網路對用戶的認證，同時也實現了在 UE 與 VLR 之間的密鑰分配。從協議上看，3G 認證與密鑰分配協議不是一種端到端的安全協議, 在 VLR 和 HLR 之間是通過網路域安全來保證的。

如果第三方在 VLR 和 HLR 之間對資訊進行竊取，就可以獲取 HLR 傳送給 VLR 的認證向量 AV，從而可以獲取 CK 和 IK。這樣，MS 的加密資料對入侵者而言就沒有秘密可言。

針對上述分析，有兩種方案進行改進：

⑴ 對可信的 VLR 而言，增加 HLR 與 VLR 之間的共用密鑰 K2；

通過增加 HLR 與 VLR 共用密鑰，實現 HLR 和 VLR 之間重要資訊的加密傳輸，保證了傳輸資訊的機密性，使第三方無法獲取認證向量 AV，保證通信的安全[5]。

本方法解決了在 VLR 和 HLR 之間的安全傳輸問題，雖然這可以用網路域的安全方案給予解決，但本方案從 3G 協議本身入手，解決了第三方竊取通信資

Copyright © 2009 SciRes

料的問題。

⑵ 對不完全可信的 VLR 而言，利用 MS 與 HLR 之間共用的密鑰 K 進行加密通信，VLR 只作轉發工作，這適用於密級較高的應用。

從圖 1 可以看出，在 VLR 和 HLR 之間部分傳輸資料對不可信 VLR 是敏感的，比如：認證向量 AV。如果不希望 VLR 見到敏感資料, 可以利用共用密鑰 K 進行處理。假設對稱加密演算法為 E(●)；對稱解密演算法為 D(●)；

① MS➔VLR：IMSI||HLR；

② VLR➔HLR：IMSI；

③ HLR➔VLE：E(K，AV)||XRES；

④ VLR➔MS：E(K，AV)；

⑤ MS➔VLR：RES

注：AV= RAND|| AUTH

在改進協議中，HLR 利用與 MS 共用的密鑰 K 對 AV 加密處理，並計算 XRES，把 E(K，AV)||XRES 傳送給 VLR。由於 VLR 無法掌握密鑰 K，也就無法掌握認證向量 AV。VLR 把 E(K，AV)轉發給 MS，由於 MS 掌握密鑰 K，所以可以得到認證向量 AV。從 AV 中可以獲取 RAND 和 AUTH, MS 計算得到 CK 和 IK 用於加密通信, 計算 RES= f2(K, RAND)返回給 VLR。VLR 比較 XRES 與 RES，如果相等就認證成功。此過程見圖 2。

此方法解決了如果在 VLR 不可信的基礎上, 如何保證端到端的資料加密通信。第三方或不可信的 VLR 無法獲取敏感通信資料。

安全性分析：

加密通信過程中，用密鑰 CK 進行加密，完整性驗證用密鑰 IK。CK 和 IK 由 RAND 和共用密鑰 K 產生, 而 K 只有 MS 和 HLR 掌握, 所以只有 MS 和 HLR 能夠產生正確的 CK 和 IK，從而保證通信安全。

假設，建立會話後進行後續通信的資料為 Data，對稱加密演算法為 E(●)；對稱解密演算法為 D(●)；MS 把 Data 進行對稱加密結果 E(CK，Data)||HLR 發送給 VLR，VLR 轉發給 HLR。HLR 利用 CK 進行解密得到 Data。這樣，在通信線路中傳輸的為密文，從而確保安全。

假設某個 VLR 不可信, 由於它無法計算得到加密密鑰 CK，從而無法得到加密通信資料 E(CK，Data)的明文 Data, 資料就可以安全通過 VLR 到達 HLR 了。

假設竊聽者在通信線路上截取通信資料，與 VLR 一樣，它也無法計算得到加密密鑰 CK，也無法獲取通信資料的明文。

該協定繼續沿用了 3GPP 標準中該協議的安全特性：對 MS 和 HLR/VLR 進行雙向認證；在認證過程中進行密鑰分配和協商；資料完整性驗證等。

此協定中，只是把 VLR 作為通信資料轉發站來看，VLR 和任何想截獲通信資料的第三方都無法得到通信資料明文，從而有效的防止了第三方竊取和 VLR 不可信的問題，但這會增加一些計算量，對通信效率有所影響。對密級較高的通信，損失一些速度而保證安全也是可取的。

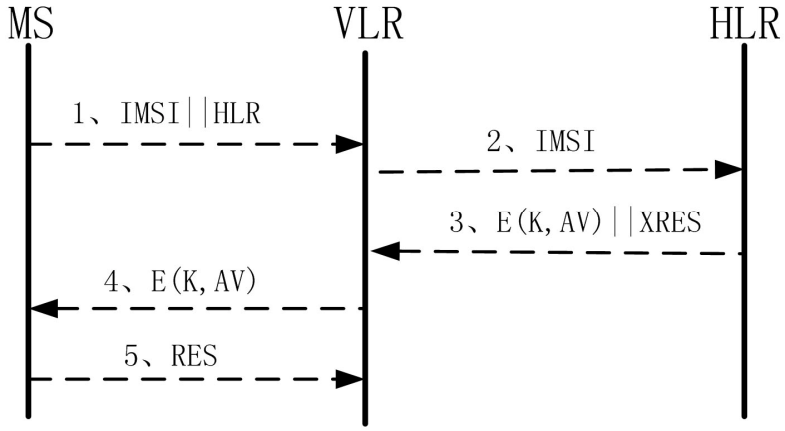


圖 2. 改進的認證與密鑰分配協定

Figure 2. Improved authentication & key distribution agreements

Copyright © 2009 SciRes

4. 結論

目前 3G 相關的協議和標準正在不斷完善過程中，本文從理論角度提出瞭解決在不完全可信 VLR 參與情況下安全通信的問題。目前 3G 系統中 HLR 和 VLR 之間網路傳輸的安全特性定義在網路域的安全協定中，本文從 3G 協議本身出發，提出了建立在對稱密碼機制基礎之上結合 3GPP 相關協議的安全認證與密鑰分配協議的新思路。

該安全協議有如下特點：

繼承 3G 認證與密鑰分配協議的優點，不損害原有協議安全性；

從協議自身增強 VLR 與 HLR 之間的通信安全性；能夠抵抗中間人攻擊。

REFERENCES

[1] Zhu li-qi, Huang ben-xong. improvement and formal analysis of 3G authentication and key distribution protocol. Electronics Engineers, 05/2004(In Chinese) (朱裏奇，黃本雄. 3G 認證和密鑰分配協議的形式化分析與改進. 電子工程師, 5/2004).

[2] Liu zi-long, lu Zheng-xin, huang zhai-lu. 2G and 3G mobile network system security and user authentication. Telecommunications technology, 02/2002(In Chinese)(劉子龍，盧正新，黃載祿. 2G 與 3G 移動網系統安全性及用戶鑒權. 電訊技術, 2/2002).

[3] Li xiang, 3G Security Architecture. Telecommunications Technology, 10/2002(In Chinese)(李翔. 3G 的安全體系結構. 電信技術, 10/2002).

[4] Lin de-jing, lin bai-gang, lin de-qing. research and analysis of 3G system-wide network security. ZTE Technology. 02/2003 (In Chinese)(林德敬，林柏剛，林德清. 3G 系統全網安全體制的探討與分析. 中興通訊技術, 2/2003).

[5] Liu dong-shu, wei bao-dian, wang xin-mei. improvement of the 3G authentication and key distribution protocol. Journal of Communication, 05/2002(In Chinese)(劉東蘇，韋寶典，王新梅. 改進的 3G 認證與密鑰分配協定 通信學報. 5/2002).

Copyright © 2009 SciRes

Intelligent Information Management, 2009, 6-14
doi:10.4236/iim.2009.11002 Published Online July 2009 (http://www.scirp.org/journal/iim)

Investigations on Simultaneously Secure IBE Scheme and Security Proofs under RO and Non-RO Model

Zhengtao JIANG [1], Yongbin WANG [1], Yong WANG [2], Yumin WANG [3]
[1] *School of Computer Science, Communication University of China, Beijing* 100024*, China*
[2] *School of Computer Science, Beijing University of Technology, Beijing* 100022*, China*
[3] *National Key Lab. of Integrated Service Networks, Xidian University, Xi'an* 710071*, China*

Abstract: Investigations on the proof theory and methods of simultaneously provable security under multi-model helps to construct formally secure cryptographic scheme under multi-environments. Further research is provided on the construction of efficient IBE scheme and provable security under CCA model. Elementary investigations on pairing-based CCA secure IBE scheme which is provably secure based on RO and non-RO model were provided. It avoided the induction inefficiency in the previous proofs. Based on the standard DBDH problem, its provable security under both models is argued. The proposed scheme has low parameter and ciphertext size, which were composed of four group element respectively. The induction of security proof is more concise and tight.

Keywords: IBE, bilinear pairing, DBDH, multi-model security, IND-CCA secure, IND-sID secure

RO 和無 RO 模型下同時安全 IBE 體制及安全證明的研究

姜正濤 [1]，王永濱 [1]，王勇 [2]，王育民 [3]

[1] 中國傳媒大學 計算機學院，北京 10024；[2] 北京工業大學 計算機學院，北京 100022
[3] 西安電子科技大學 綜合業務網國家重點實驗室，陝西 西安 710071

摘　要：探討多模型下同時安全的體制構造、證明理論與方法有助於構造多環境下形式化安全的密碼體制，本文進一步研究了高效的 IBE 體制構造和 CCA 模式下的可證明安全，基於所構造的體制探討了 RO 和無 RO 模型下的安全證明，並避免了本文指出的以往證明中在規約效率方面的不足，基於標準 DBDH 問題在兩種模型下證明體制的可證明安全性，另外該體制的特點是參數規模和密文長度更小，分別為 4 個群元素，安全證明規約更簡化和緊致。

關鍵詞: IBE，雙線性對，DBDH，多模型安全，IND-CCA 安全，IND-sID 安全
中圖分類號: TP309

1. 引 言

基於身份的加密體制(IBE)以主體身份 ID 作為主體的公鑰，如 Email、電話號碼等，這一方法避免了 PKI 環境下 CA 證書傳輸、驗證以及證書管理的複雜維護等問題[1][2]，基於 RSA 假設，A. Shamir 在 1984

基金專案：國家"211 工程"資助專案、國家自然科學基金資助項目(90412011).

Copyright © 2009 SciRes

年提出了基於身份公鑰密碼系統的概念[3]，自然地解決公鑰和實體身份的綁定問題，簡化公鑰證書的管理。IBE 通常分為 4 個步驟：(1) Setup，生成系統公開參數和主密鑰 MK；(2) Extract，運用 MK 為主體生成私鑰；(3) 加密；(4) 解密。與 PKI 不同的是，只要在階段(1)建立的公開參數後，即使主體還未建立自己的私鑰，成員也可以使用主體的身份對消息加密。隨後研究者對 IBE 及其簽名應用等領域進行了廣泛深入的研究[4-8]。

2001 年 D. Boneh 等利用雙線性線對構造了第一個安全有效的 IBE 體制，並定義了 IBE 體制的選擇明文(IND-ID-CPA)和選擇密文安全性(IND-ID-CCA)，目前 IND-ID-CCA 逐漸成為被普遍接受的安全定義，其中的攻擊者可以適應性選擇成員身份（公鑰）和密文分別進行私鑰提取和解密詢問，基於判斷雙線性對 Diffie-Hellman (DBDH)問題，在隨機預言(RO)模型下證明瞭體制的 IND-ID-CPA 安全性，並進一步把體制改進成具有 IND-ID-CCA 安全性，其語義安全等價於 DBCH 問題[9]。

R. Canetti 等運用雙線性對基於他們所提出的選擇身份(sID)安全定義[10][11]，在無 RO 模型下構造了一個可證明安全的層次 IBE 體制，在安全證明中，攻擊者可以適應性地選擇身份和密文進行解密預言詢問，但是其中的攻擊者需要在系統生成公開參數之前承諾(commit)攻擊目標的身份，另外私鑰詢問階段所選擇的身份既不能是攻擊目標身份也不能是該身份的任何首碼，D, Boneh 等稱其為 IND-sID-CCA 安全[12]。這是一種基於相對弱的安全模型的證明方法，在體制的解密過程中，對應於身份串的每一比特均要執行一次對運算，實現效率比較低。

D. Boneh 和 X. Boyen[12][13]對 R. Canetti 等[10]的 IND-sID-CCA 安全模式作了進一步限制，給出選擇選擇身份、選擇明文的安全性(IND-sID-CPA)定義，在 IND-sID-CPA 安全模式中，攻擊者不能進行解密預言詢問。基於 IND-sID-CPA 攻擊模式，D. Boneh 等在無 RO 模型下對兩個 IBE 體制及安全證明進行了研究，第一個為層次身份加密(HIBE)體制，證明瞭其 IND-sID-CPA 安全性基於 DBDH 問題，但其主體私鑰、公鑰以及密文規模比較大，加解密效率比較低。第二個體制在 D. Boneh 等定義的一個非標準的問題假設下(判斷雙線性 DH 逆問題 q-DBDHI)證明瞭體制的 IND-sID-CPA 安全性[12]。

B. Waters 對文[12]中的 IBE 體製作了進一步研究[14]，根據主體身份逐比特在橢圓曲線群中執行群運算，縮短了密文長度，提高了效率，在標準模型下把適應性選擇身份-選擇明文(IND-ID-CPA)安全性規約到 DBDH 問題，攻擊者在攻擊之前不需要承諾攻擊目標的身份，是在比較弱的非 CCA 攻擊模式下證明的，另外系統參數規模仍然比較大，安全證明規約不夠緊致，每次模擬只能以比較低的概率成功，安全證明中也存在不足。針對 IBE 參數規模和安全證明規約存在的上述問題，B. Waters 在文[14]最後提出了兩個進一步研究的問題：降低 IBE 體制的公開參數規模以及在無 RO 模型下更緊致的安全證明。目前對密碼體制的可證明安全研究，大都基於單一的安全模型，探討多模型下可證明安全的理論與方法可以為密碼體制的安全性提供更多的安全論證，是可證明安全領域有意義的研究內容[15][14][9]。

針對上述幾方面問題，本文進一步研究了雙線性對上構造公開參數規模小的選擇密文(CCA)可證安全的 IBE 體制，以及探討在 RO 和無 RO 兩種模型下可證明安全的體制的構造和證明方法，基於 DBDH 問題假設，嘗試分別在 RO 模型和無 RO 模型下證明體制的安全性，避免以往證明中的一個不足，系統參數規模小，公開參數與密文長度分別為 4 個群元素，證明規約更簡化和緊致，多模型下同時安全的體制構造和證明的理論與方法還處於研究初步階段，還沒有完善的證明，這一問題的研究有助於構造多攻擊環境下形式化安全的密碼體制，是可證明安全領域的一項有意義的研究內容。

2. 雙線性對與安全性定義

設 G_1 為 q 階加群，G_2 為 q 階乘群，其中 q 為素數，P 為 G_1 的生成元，定義在 $G_1 \times G_1$ 上的對是一個映射 $e: G_1 \times G_1 \to G_2$，滿足以下條件[16-18]：

1. 雙線性：對任意的 $Q, R, W \in G_1$，有
$$e(P, Q+R) = e(P, Q) \cdot e(P, R),$$
$$e(P+Q, R) = e(P, R) \cdot e(Q, R)。$$

2. 非退化：$e(P, P) \neq 1$。

Copyright © 2009 SciRes

3. e 可有效計算：對任意的 $Q,R \in G_1$，$e(Q,R)$ 可有效計算。

e 可以通過有限域上超奇異橢圓曲線中的 Weil 對 Tate 對來實現。

定義 1 雙線性參數生成器 Param-*Gen* 一個雙線性參數生成器 Param-*Gen* 為一個概率多項式時間演算法，輸入安全參數 k，輸出一個雙線性五元組 (q,G_1,G_2,e,P) 作為雙線性參數，其中 q 為大素數滿足 $q \geq 2^k$，G_1 為 q 階加群，G_2 為 q 階乘群，P 為 G_1 的生成元，$e: G_1 \times G_1 \to G_2$ 是一個雙線性對。

定義 2 計算雙線性 Diffie-Hellman (CBDH) 問題 給定 $P,aP,bP,cP \in G_1$，對於隨機的 $a,b,c \in Z_q^*$，計算 $e(P,P)^{abc} \in G_2$。

演算法 A 成功計算 CBDH 問題的概率記為：

$$Succ_{Gen,\mathcal{A}}^{CBDH} = \Pr[e(P,P)^{abc} \leftarrow A(P,aP,bP,cP)]$$

這裏 a,b,c 是 Z_q^* 中的亂數。

CBDH 問題假設：對於隨機選取的 $a,b,c \in Z_q^*$，不存在有效的多項式時間演算法 A，使得對於某個不可忽略的 ε，滿足 $Succ_{Gen,\mathcal{A}}^{CBDH} \geq \varepsilon$。

定義 3 判斷雙線性 Diffie-Hellman (DBDH)問題實例生成器 DBDH-*Gen* 一個判斷雙線性 Diffie-Hellman 問題實例生成器 DBDH-*Gen* 為一個概率多項式時間演算法，輸入一個雙線性五元組 (q,G_1,G_2,e,P)，輸出判斷雙線性五元組 $(P,a_iP,b_iP,c_iP,T_i) \in G_1^4 \times G_2$，這裏 $a_i,b_i,c_i (i=1,2...,n)$ 是 Z_q^* 中的亂數，T 為 G_2 中的亂數。

定義 4 判斷雙線性 Diffie-Hellman (DBDH)問題 輸入一個判斷雙線性五元組 $(P,a_iP,b_iP,c_iP,T_i) \in G_1^4 \times G_2$，判斷 $T_i = e(P,P)^{a_ib_ic_i}$ 是否成立。

演算法 A 成功判斷 DBDH 問題的概率記為：

$$Succ_{Gen,\mathcal{A}}^{DBDH} = \Pr[1 \leftarrow A(P,aP,bP,cP,e(P,P)^{abc})]$$

這裏的 $a_i,b_i,c_i (i=1,2...,n)$ 是 Z_q^* 中的亂數，T 為 G_2 中的亂數。

定義 5 DBDH 問題假設 對於隨機選取的 $a,b,c \in Z_q^*$ 和 $T \in G_2$，不存在演算法 B 可以在 t 時間內以不小於 ε 的優勢解決 DBDH 問題，即不存在演算法 B 使得 $Succ_{Gen,\mathcal{A}}^{DBDH} \geq \varepsilon + \frac{1}{2}$，此時稱 (t,ε) -DBDH 假設成立。

定義 6 RO 模型下 $(t,q_{ID},q_E,q_D,\varepsilon)$ -IND-ID -CCA 安全稱一個 IBE 體制是 $(t,q_{ID},q_E,q_D,\varepsilon)$ -IND-ID-CCA 安全的，如果不存在在適用性選擇密文攻擊者可以在 t 時間內、經過 q_{ID} 次身份預言詢問、q_E 次私鑰提取預言詢問和 q_D 次解密預言詢問，以不小於 ε 的優勢成功攻擊體制的語義安全性。

3. RO 和無 RO 模型下的安全 IBE

Setup: 密鑰生成中心 KGC 輸入安全參數 k，由雙線性參數生成器 Param-*Gen* 輸出一個雙線性五元組 (q,G_1,G_2,e,P)，這裏 G_1 為 q 階加群，G_2 為 q 階乘群，其中 q 為素數，P 為 G_1 的生成元，$e: G_1 \times G_1 \to G_2$ 是一個雙線性對。

$H: \{0,1\}^* \to G_1^*$ 為把一 bit 串映射到 G_1 中元素，滿足當 $x \neq y$ 時，有 $H(x) \neq H(y)$。

隨機選取 $\alpha \in Z_q$，計算 $P_1 = \alpha P$，隨機選取 $P_2, P_3 \in G_1$，生成主密鑰 $MK: \alpha P_2$，公開參數 $Params = < q, G_1, G_2, e, P, P_1, P_2, P_3 >$。

KeyGen: 設主體的身份為 ID，向 KGC 申請私鑰；KGC 計算 $Q_{ID} = H(ID)$，隨機選取 $r \in Z_q$，計算主體 ID 的私鑰

$$d_{ID} = < \alpha P_2 + rP_2 + rQ_{ID} + rP_3, rP >,$$

並安全發送給主體 ID。

Encryption: 待加密的消息為 M，加密者隨機選取 $t \in Z_q$，計算密文

$$C = < e(P_1,P_2)^t M, tP, tP_2 + tQ_{ID} + tP_3 >$$

Decryption: 解密者收到 $C = < C_1, C_2, C_3 >$，根據自己的私鑰 $d_{ID} = < d_1, d_2 >$，計算得到明文

$$M = C_1 \frac{e(d_2, C_3)}{e(d_1, C_2)}$$

Copyright © 2009 SciRes

4. 可行性分析與安全證明

4.1 可行性分析

4.1.1 私鑰生成有效性

主體 ID 收到私鑰

$d_{ID}=(d_1,d_2)=<\alpha P_2+rP_2+rQ_{ID}+rP_3,rP>$，通過以下計算驗證私鑰 d_{ID} 是否的確是由 KGC 為自己生成的有效私鑰：

$$\frac{e(d_1,P)}{e(d_2,Q_{ID})e(d_2,P_3)}\stackrel{?}{=}e(d_2,P_2)e(P_2,P_1)$$

事實上，

$$\frac{e(d_1,P)}{e(d_2,Q_{ID})e(d_2,P_3)}=\frac{e(\alpha P_2+rP_2+rQ_{ID}+rP_3,P)}{e(rP,Q_{ID})e(rP,P_3)}$$
$$=e(d_2,P_2)e(P_2,P_1)。$$

4.1.2 解密可行性

解密者通過計算 $C_1\frac{e(d_2,C_3)}{e(d_1,C_2)}$ 可以得到相應的明文。

事實上，

$$C_1\frac{e(d_2,C_3)}{e(d_1,C_2)}$$
$$=e(P_1,P_2)^tM\frac{e(rP,tP+tQ_{ID}+tP_3)}{e(\alpha P_2+rP_2+rQ_{ID}+rP_3,tP)}$$
$$=M。$$

4.1.3 效率分析

加密需要一個對運算（可預計算），二個橢圓曲線上標量乘法運算，一個有限域上乘法運算，一個有限域上指數計算。

解密需要兩個對運算，一個有限域上乘法運算，一個有限域上除法運算。

4.2 RO 模型下的安全性證明

定理 1 在 RO 模型下，如果 $(t+O(q_{ID}+q_E+q_D),\varepsilon)$-DBDH 假設成立，則該 IBE 體制是 $(t,q_{ID},q_E,q_D,\varepsilon)$-IND-CCA 安全的，這裏攻擊者 A 進行 q_{ID} 次身份 Oracle 詢問，q_E 次私鑰提取 Oracle 詢問、q_D 次解密 Oracle 詢問。

證明 由判斷雙線性 DH 問題實例生成器 DBDH-*Gen* 隨機生成一個判斷雙線性五元組 (P,aP,bP,cP,T)，A 為 $(t,q_{ID},q_E,q_D,\varepsilon)$-IND-CCA 攻擊者，在 RO 模型下攻擊者 A 隨機選擇身份與模擬者 B 進行私鑰提取和解密詢問攻擊遊戲，模擬者 B 返回相應的私鑰作為對 A 私鑰詢問的應答，並對提交的密文進行解密應答，充分利用了 A 的攻擊能力，經過 q_{ID} 次身份 Oracle 詢問，q_E 次私鑰提取詢問、q_D 次解密詢問和一次挑戰，最後 A 以不可忽略的概率成功攻擊 IBE 體制的 IND-CCA 安全性，那麼存在一個演算法運用 A 的攻擊能力，可以不可忽略的概率成功解決 DBDH 問題，從而證明體制的安全性。

Setup: 密鑰生成中心 KGC 輸入安全參數 k，由雙線性參數生成器 Param-*Gen*，輸出一個雙線性五元組 (q,G_1,G_2,e,P)。

由判斷雙線性 DH 問題實例生成器 DBDH-*Genn* 生成一個判斷雙線性五元組實例 $(P,A,B,C,T)=(P,aP,bP,cP,T)$。

B 構造 IBE 體制，令 $P_1=A=aP$，$P_2=B=bP$，隨機選取 $P_3\in G_1$，相應的公開參數為 Params=$<q,G_1,G_2,e,P,P_1,P_2,P_3>$。

Phase 1: 攻擊者 A 與模擬者 B 執行 l $(<q_{ID})$ 次身份 Oracle 詢問-應答、n $(<q_E)$ 次私鑰 Oracle 詢問-應答和 u $(<q_D)$ 次解密 Oracle 詢問-應答。

B 構造一個身份 Oracle 應答列表 T_{ID-H}，初始為空。

1) 攻擊者 A 提交一個身份 ID_i 進行身份 Oracle 詢問：

如果 ID_i 已被 A 詢問過，B 從列表 T_{ID-H} 中直接讀取；

否則，B 隨機選取 $m_i\in Z_q$，令 $H(ID_i)=Q_i=m_iP-P_3$ 發給 A，並把身份詢問-應答 $<ID_i,Q_i>$ 添加到 T_{ID-H} 中。

由於 $m_i\in Z_q$ 是由 B 隨機選取的，Q_i 與 G_1 中隨機元素不可區分。

如果攻擊者 A 需要對主體 ID_i 進行私鑰 Oracle 詢問，執行下麵的 2）。

2) 攻擊者 A 提交一個身份 ID_i 進行私鑰 Oracle 詢問：

Copyright © 2009 SciRes

如果身份 ID_i 在 1)中被詢問過, 則 B 直接從 T_{ID-H} 讀取 $H(ID_i)$，否則隨機生成新的 $H(ID_i)=Q_i=m_iP-P_3$ 發送給 A，並把新的身份詢問-應答對 $<ID_i,Q_i>$ 添加到 T_{ID-H} 中。

B 隨機選取 $r_i\in Z_q$，輸出二元組 $d_i=(d_{i,0},d_{i,1})$ $=(-m_iP_1+r_iP_2+r_iQ_i+r_iP_3,r_iP-P_1)$。

事實上，

$$d_{i,0}=-m_iP_1+r_iP_2+r_iQ_i+r_iP_3$$

$$=aP_2+(-a)P_2+-m_iP_1+r_iP_2+r_iQ_i+r_iP_3$$

$$=aP_2+(r_i-a)(P_2+Q_i+P_3)$$

$$d_{i,1}=r_iP-P_1=(r_i-a)P$$

令 $r_i'=r_i-a$，則 $d_i=(d_{i,0},d_{i,1})$ $=(aP_2+r_i'P_2+r_i'Q_i+r_i'P_3,r_i'P)$。

攻擊者 A 可以通過以下等式驗證私鑰應答的正確性：

$$\frac{e(d_{i,1},P)}{e(d_{i,2},Q_i)e(d_2,P_3)}=\frac{e(-m_iP_1+r_iP_2+r_iQ_i+r_iP_3,P)}{e(r_iP-P_1,Q_i)e(r_iP-P_1,P_3)}$$

$$=e(d_{i,2},P_2)e(P_2,P_1)$$

所以，

$d_i=(d_{i,0},d_{i,1})=(-m_iP_1+r_iP_2+r_iQ_i+r_iP_3,r_iP-P_1)$ 是身份 $Q_i=H(ID_i)$ 對應的有效私鑰。

如果攻擊者 A 需要對主體 ID_i 進行解密 Oracle 詢問，執行下麵的 3)。

3) 攻擊者 A 選擇一條明文 M, 構造合法的密文，進行解密 Oracle 詢問：

攻擊者 A 選擇一個身份 ID_i，如果身份 ID_i 在 1), 2) 中被詢問過, 則 A 直接生成合法密文, 否則把身份 ID_i 提交給 B，B 隨機選取 $m_i\in Z_q$ 並生成新的 $H(ID_i)=Q_i=m_iP-P_3$ 發送給 A, 並把新的 $<ID_i,Q_i>$ 添加到 T_{ID-H} 中。

A 隨機選取 $t\in Z_q$，生成合法密文 $C=<C_1,C_2>=<e(P_1,P_2)^tM,tP,tP_2+tQ_i+tP_3>$ 發送給模擬者 B。

模擬者 B 收到密文 C 後，如果 A 在 2)對身份 ID_i 進行過私鑰 Oracle 詢問，則直接使用已生成的私鑰進行解密，否則針對身份 ID_i，B 隨機選取 $r_i\in Z_q$ 生成新的 $d_i=(d_{i,0},d_{i,1})$ $=(-m_iP_1+r_iP_2+r_iQ_i+r_iP_3,r_iP-P_1)$ 進行解密：

B 計算

$$C_1\frac{e(d_{i,2},C_3)}{e(d_{i,1},C_2)}$$

$$=e(P_1,P_2)^tM\frac{e(r_iP-P_1,tP_2+tQ_i+tP_3)}{e(-m_iP_1+r_iP_2+r_iQ_i+r_iP_3,tP)}$$

=M

並把 M 發送給 A。

由於 1),2),3)中對於新的身份 ID_i 和新的私鑰詢問，$m_i,r_i\in Z_q$ 是由 B 隨機生成的，攻擊者 A 能夠得到滿意的身份、私鑰和解密 Oracle 應答，模擬者 B 成功模擬攻擊者 A 在 Phase1 階段的詢問。

A 分別重複 1), 2),3) l $(<q_{ID})$ 次、n $(<q_E)$ 次和 u $(<q_D)$ 次，完成 Phase1。

Challenge: 類比者 B 對 DBDH 問題實例 $(P,A,B,C,T)=(P,aP,bP,cP,T)$ 的判斷沒有任何優勢，B 所能做的是構造適於 A 展開攻擊的場景，充分利用 A 的 IND-CCA 能力。

攻擊者 A 提交兩條明文 $M_0,M_1\in\{0,1\}^n$ 和一個身份 ID_{ch}，為充分運用 A 的攻擊能力，對 ID_{ch} 唯一的要求是沒有在 Phase1 進行過私鑰詢問。模擬者 B 收到 M_0,M_1 和 ID_{ch} 後, 根據 DBDH 問題實例 (P,A,B,C,T) 構造合法密文。

模擬者 B 隨機選取 $k\in Z_q$，計算 $Q_{ch}=kP-P_2-P_3$，令 $H(ID_{ch})=Q_{ch}$，把 $H(ID_{ch})=Q_{ch}$ 發送給 A，並在 T_{ID-H} 中添加 $<ID_{ch},Q_{ch}>$。

模擬者 B 構造合法密文：

B 擲幣隨機選取 $\gamma\in\{0,1\}$，構造密文 $Z=(T\cdot M_\gamma,C,kC)$，併發送給 A。

事實上，如果 $(P,A,B,C,T)=(P,aP,bP,cP,T)$ 是 DBDH 問題五元組，即 $T=e(P,P)^{abc}$，則有

$$Z=(T\cdot M_\gamma,C,kC)=(e(P_1,P_2)^cM_\gamma,cP,c\cdot kP)$$

$$=(e(P_1,P_2)^cM_\gamma,cP,c\cdot P_2+c\cdot Q_{ch}+c\cdot P_3)$$

是明文 M_γ 對應的有效密文。

Copyright © 2009 SciRes

另外，由於 $k \in Z_q$ 隨機選取，在攻擊者 A 看來，Q_{ch} 與從 G_1 中隨機選取的元素隨機性不可區分。

Phase 2: 類似 Phase1，攻擊者 A 與模擬者 B 分別重複執行 $q_E - l - 1$ 次身份 Oracle 詢問-應答、$q_E - n$ 私鑰 Oracle 詢問-應答和 $q_D - u$ 解密 Oracle 詢問-應答，唯一限制是 A 不能對主體身份 ID_{ch} 進行私鑰和解密 Oracle 詢問。

Quess: 最後，攻擊者 A 輸出對 γ 的猜測 γ'。

4.3 無 RO 模型下的安全性證明

下麵的證明擴展了 R. Canetti 等基於 DBDH 問題在無 RO 模型下構造的選擇身份（sID）安全證明，攻擊者除了擁有文[10]中描述的攻擊能力外，還可以選擇 DBDH 問題實例（也可固定），攻擊者完成第一階段的選擇身份、選擇 DBDH 問題實例的私鑰和解密預言詢問後，在 challenge 階段攻擊者選擇目標 DBDH 問題實例和身份進行挑戰，模擬者在對 DBDH 問題沒有任何優勢的情況下，基於問題參數生成合法密文，在攻擊遊戲結束後，模擬者利用攻擊者的選擇身份、選擇 DBDH 問題實例的 CCA（IND-sID||sIN-CCA）攻擊能力，回答 DBDH 問題。

定理 2 在無 RO 模型下，如果 $(t+O(q_{ID}+q_{IN}+q_E+q_D),\varepsilon)$ -DBDH 假設成立，則該 IBE 體制是 $(t,q_{ID},q_{IN},q_E,q_D,\varepsilon)$ -IND-sID||sIN-CCA 安全的，這裏攻擊者 A 進行 q_{ID} 次身份選擇、q_{IN} 次實例選擇、q_E 次私鑰提取 Oracle 詢問、q_D 次解密 Oracle 詢問。

證明 由判斷雙線性 DH 問題實例生成器 DBDH-*Gen* 隨機生成 n 個判斷雙線性五元組 (P,a_iP,b_iP,c_iP,T_i) , $i=1,2,...,n$，A 為攻擊者，類比者 B 根據 A 選擇攻擊實例和身份構造適合 A 展開攻擊的攻擊場景，以充分運用 A 具有的攻擊能力，攻擊者 A 隨機選擇身份和DBDH問題實例與類比者B進行私鑰提取詢問和解密詢問攻擊遊戲，模擬者 B 提交相應的私鑰和明文分別作為對 A 私鑰詢問和解密詢問的應答，充分利用了 A 的攻擊能力，在時間 t 內，進行 q_{ID} 次身份選擇、q_{IN} 次實例選擇、q_E 次私鑰提取 Oracle 詢問、q_D 次解密 Oracle 詢問和一次挑戰，最後 A 以不可忽略的概率成功攻擊 IBE 體制的語義安全性，B 把 A 的這一適應性攻擊能力規約到 DBDH 問題的解決，從而在無 RO 模型下證明體制安全性。

Setup: 密鑰生成中心 KGC 輸入安全參數 k，由雙線性參數生成器 Param-*Gen*，輸出一個雙線性五元組 (q,G_1,G_2,e,P)。

根據體制的建立階段，設元素變換函數 $H(\cdot)=h(\cdot)P \in G_1$ 為 $\{0,1\}^* \to G_1^*$ 的抗碰撞 Hash 函數，$h:\{0,1\}^* \to Z_q$ 為一密碼學 Hash 函數，如 SHA-1 等，實現把不同的身份 ID 映射為 G_1 中不同的群元素，記 $H(ID)=h(ID)P=h_{ID}P$。

由判斷雙線性 DH 問題實例生成器 DBDH-*Genn* 生成 n 個判斷雙線性五元組實例 (P,a_iP,b_iP,c_iP,T_i) , $i=1,2,...,n$。

對於 A 提交一個 DBDH 問題實例 (P,a_iP,b_iP,c_iP,T_i)，相應的公開參數為 *Params*= $<q,G_1,G_2,e,P,P_1,P_2,P_3>$，其中 $P_1=a_iP, P_2=b_iP$，$P_3 \in G_1$ 為由 B 根據 DBDH 問題實例隨機選取的元素。

Phase 1: 攻擊者 A 隨機選取 l $(<q_{ID})$ 個身份、k $(<q_{IN})$ 個 DBDH 問題實例 (P,a_iP,b_iP,c_iP,T_i)、與模擬者 B 執行 n $(<q_E)$ 次私鑰 Oracle 詢問-應答和 u $(<q_D)$ 次解密 Oracle 詢問-應答。

1) 攻擊者 A 隨機選擇 DBDH 問題實例 (P,a_iP,b_iP,c_iP,T_i) 和身份 ID_j。

類比者 B 根據 A 選擇的參數構造合法的 IBE 實例 *Params*= $<q,G_1,G_2,e,P,P_1,P_2,P_3>$，其中 $P_1=A_i=a_iP, P_2=B_i=b_iP$，B 隨機選取 $m \in Z_q$，計算 $P_3=mP$*，由於 $m \in Z_q$ 是由 B 隨機選擇的，在 A 看來 P_3 與 G_1 中的隨機元素不可區分。

如果攻擊者 A 需要對主體 ID_j 進行私鑰 Oracle 詢問，執行下麵的 2）。

2) 攻擊者 A 提交一個身份 ID_j 進行私鑰 Oracle 詢問：

B 隨機選取 $r_j \in Z_q$，輸出二元組 $d_j=(d_{j,0},d_{j,1})$ $=(-mP_1-h_jP_1+r_jP_2+r_jQ_j+r_jP_3, r_jP-P_1)$。

事實上，

$$d_{j,0}=-mP_1-h_jP_1+r_jP_2+r_jQ_j+r_jP_3$$
$$=aP_2+(-a)(P_2+Q_j+P_3)+r_jP_2+r_jQ_i+r_jP_3$$

*這裏 $P_3=mP$ 也可以在 Phase1 階段之前由模擬者 B 隨機選定.

Copyright © 2009 SciRes

$= aP_2 + (r_j - a)(P_2 + Q_j + P_3)$

$d_{j,1} = r_j P - P_1 = (r_j - a)P$

令 $r'_j = r_j - a$，則 $d_j = (d_{j,0}, d_{j,1})$ $= (aP_2 + r'_j P_2 + r'_j Q_j + r'_j P_3, r'_j P)$ 是關於 IBE 實例 $Params = < q, G_1, G_2, e, P, P_1, P_2, P_3 >$，身份 ID_j 對應的有效私鑰。

如果攻擊者 A 需要進一步對主體 ID_j 進行解密 Oracle 詢問，執行下麵的 3)。

3) 攻擊者 A 選擇一條明文 M, 構造合法的密文，進行解密 Oracle 詢問：

攻擊者 A 選擇一個身份 ID_j，隨機選取 $t \in Z_q$，生成密文

$C = < C_1, C_2 > = < e(P_1, P_2)^t M, tP, tP_2 + tQ_j + tP_3 >$ 發送給模擬者 B。

模擬者 B 收到密文 C 後，如果 A 在 2)中對身份 ID_j 進行過私鑰 Oracle 詢問，則直接使用已生成的私鑰進行解密，否則針對身份 ID_j，B 隨機選取 $r_j \in Z_q$ 生成新的私鑰 $d_j = (d_{j,0}, d_{j,1})$ $= (-mP_1 - h_j P_1 + r_j P_2 + r_j Q_j + r_j P_3, r_j P - P_1)$ 進行解密：

B 計算

$$C_1 \frac{e(d_{j,1}, C_3)}{e(d_{j,0}, C_2)}$$

$$= e(P_1, P_2)^t M \frac{e(r_j P - P_1, tP_2 + tQ_j + tP_3)}{e(-mP_1 - h_j P_1 + r_j P_2 + r_j Q_j + r_j P_3, tP)}$$

=M

並把 M 發送給 A。

關於 IBE 實例 $Params = < q, G_1, G_2, e, P, P_1, P_2, P_3 >$，由於 1),2),3)中對於身份 ID_j 和私鑰詢問，$r_j \in Z_q$ 是由 B 隨機生成的，攻擊者 A 能夠得到滿意的私鑰和解密 Oracle 應答，模擬者 B 成功模擬攻擊者 A 在 Phase1 階段的私鑰和解密 Oracle 詢問。

A 分別重複 1),2),3)，隨機選取 l $(< q_{ID})$ 個身份、k $(< q_{IN})$ 個 DBDH 問題實例 $(P, a_i P, b_i P, c_i P, T_i)$、與模擬者 B 執行 n $(< q_E)$ 次私鑰 Oracle 詢問-應答和 u $(< q_D)$ 次解密 Oracle 詢問-應答，完成 Phase1。

Challenge: 攻擊者 A 提交兩條明文 $M_0, M_1 \in \{0,1\}^n$ 和一個主體身份 ID_{ch}，並從 DBDH 問題實例中隨機選取 $(P, A, B, C, T) = (P, a_i P, b_i P, c_i P, T_i)$，相應的公開參數為 $Params = < q, G_1, G_2, e, P, P_1, P_2, P_3 >$，其中 $P_1 = a_i P, P_2 = b_i P$，$P_3 \in G_1$ 由 B 隨機選取, 這裏對 ID_{ch} 的唯一限制是在 Phase1 針對實例 $(P, a_i P, b_i P, c_i P, T_i)$ 沒有對 ID_{ch} 進行過私鑰詢問。

為充分利用攻擊者 A 的攻擊能力, 模擬者 B 隨機選擇 $k \in Z_q$，計算 $P_3 = kP - P_2 - Q_j$，令 $C = c_i P$，B 擲幣隨機選取 $\gamma \in \{0,1\}$，構造密文 $Z = (T \cdot M_\gamma, C, kC)$。

事實上，如果 $(P, A, B, C, T) = (P, a_i P, b_i P, c_i P, T_i)$ 是 BDH 五元組，即 $T = e(P, P)^{abc}$，則有

$Z = (T \cdot M_\gamma, C, kC) = (e(P_1, P_2)^c M_\gamma, cP, c \cdot kP) = (e(P_1, P_2)^c M_\gamma, cP, c \cdot P_2 + c \cdot P_3 + c \cdot P_3)$

是明文 M_γ 對應的有效密文。

另外，由於 $k \in Z_q$ 隨機選取，在攻擊者 A 看來，P_3 與從 G_1 中隨機選取的元素 $P'_3 \in G_1$ 隨機性不可區分。

Phase 2: 類似 Phase1 重複進行 $q_{ID} - l - 1$ 個身份選取、$q_{IN} - k - 1$ 個 DBDH 問題實例選取、$q_E - n$ 次私鑰 Oracle 詢問-應答和 $q_D - u$ 次解密 Oracle 詢問-應答，唯一限制是 A 不能針對 DBDH 問題實例 $(P, a_i P, b_i P, c_i P, T_i)$ 對主體身份 ID_{ch} 進行私鑰詢問。

Quess: 最後，攻擊者 A 輸出對 γ 的猜測 γ'。

分析：

對任意的 DBDH 問題實例 $(P, a_i P, b_i P, c_i P, T_i)$, $i = 1,2,...,n$，類比者 B 在沒有判斷優勢的情況下，通過類比適於 A 展開攻擊的場景，充分利用 A 的攻擊能力，最終回答 DBDH 問題。

(1) 在 Phase2 階段，對攻擊者 A 的唯一限制是 A 不能對 Challenge 階段的 < 實例, 身份 > 對 $< (P, a_i P, b_i P, c_i P, T_i), ID_{ch} >$ 私鑰詢問，即只要 $< (P, A, B, C, T), ID_i > \neq < (P, a_i P, b_i P, c_i P, T_i), ID_{ch} >$，$< (P, A, B, C, T), ID_i >$都可以在 Phase1,2 階段執行私鑰 Oracle 詢問-應答和解密 Oracle 詢問-應答，這種情況包含了文[14][10]安全證明中的私鑰提取詢問過程。

(2) 在 Challenge 階段，對於 DBDH 問題實例

(P,a_jP,b_jP,c_jP,T_j)，模擬者 B 沒有任何優勢，對於 A 隨機選擇的兩條明文 $M_0,M_1\in\{0,1\}^n$，B 通過構造有效的密文，利用攻擊者 A 的攻擊能力，並把這一能力規約到解決 DBDH 問題：(P,A,B,C,T) 是 BDH 五元組，當且僅當 A 可以正確判斷 $\gamma\in\{0,1\}$。

注：本文初步探討了同時在 RO 和無 RO 模型下的安全體制構造與安全證明，目前對密碼體制的構造和安全性證明大都基於單一的安全模型，多模型下的體制構造、安全模型與證明方法的研究還不成熟，還需要進一步做大量的研究。定理 2 中無 RO 模型下的安全證明中，其安全模型可以看作是 sID-CCA 安全的一個擴展，進一步研究參數規模小、多模型下可證安全的體制構造與證明方法對於構造多攻擊環境下安全的高效密碼體制具有重要意義。

4.4 相關工作分析

本文主要在B. Waters等對的IBE體制研究的基礎上做進一步研究[14][10](本文 IBE 體制同樣也可進一步構造 RO 和無 RO 模型下可證安全的簽名體制)，主要包括：對公開參數規模簡化（ RO 模型下可以令 $P_3=O$，進一步簡化系統參數而不影響證明)；把 CPA 模式下的安全改進到 CCA 模式下的安全；在此基礎上，探討同時在 RO 和無 RO 模型下安全的 IBE 體制構造與規約緊致的安全證明，並避免了文[14]證明中的一個不足。

在 B. Waters 的安全證明中[14]，模擬者選取的公開參數 $u'=g_2^{p-km+x'}g^{y'}$, $u_i=g_2^{x_i}g^{y_i}$， $i=1,2,...,n$，其中 $x',x_i\in[0,m-1]$， $y',y_i\in Z_p$， $m=4q$， q 為攻擊者的私鑰詢問次數， m,n,k 均為多項式有界量，攻擊者可以以不可忽略的概率猜得所有的 x' 和 x_i ($i=1,2,...,n$)（攻擊者也可以在 Phase1,2 階段，通過 $K(v)$ 的值，構造 n+1 組 $x'+\sum_{i\in V^*}x_i=0(\mathrm{mod}\,m)$ 同餘線性方程組求得 x' 和 x_i ($i=1,2,...,n$))。

另外，在獲得 x' 和 x_i ($i=1,2,...,n$)後，公開參數指數部分包含 x' 和 x_i 成分起不到保密作用，而且額外增加計算量；另外在攻擊者 A 獲得 x' , x_i ($i=1,2,...,n$) 後，在 Challenge 階段，A 可以選擇身份 v^* 並計算 $F=x'+\sum_{i\in V^*}x_i$，如果 $F\neq km$，就把 v^* 提交給模擬者，這樣模擬者中斷模擬的概率為 1，而不是 $1-\frac{1}{8(n+1)q}$。類似地在 Phase1 或 Phase2 階段，利用已知的 x' , x_i ($i=1,2,...,n$)，攻擊者可以選擇身份 v^* 並計算 $E=x'+\sum_{i\in V^*}x_i \bmod m$, 若 $E=0$, 提交身份 v^* 進行私鑰詢問，同樣模擬者會以概率 1 中斷模擬，而不是 $1-\frac{1}{8(n+1)q}$。出現這一情況的主要原因是安全規約的參數構造階段 x' , x_i ($i=1,2,...,n$)的選擇範圍較小，不能很好隱藏冪指數，攻擊者 A 可以獲得 x' , x_i ($i=1,2,...,n$), 但是如果 x' , x_i ($i=1,2,...,n$)的選擇範圍過大（ m 比較大)，對於隨機選擇的身份 v^*，在 Challenge 階段攻擊遊戲中斷的概率同樣趨向於 1，對攻擊者來說參數和所選擇的身份不能看作是完全隨機的。

5. 結 論

本文基於 B. Waters 提出的兩個公開有待研究的問題和目前安全證明模型單一的問題，對雙線性對上構造 RO 與無 RO 模型下安全有效的 IBE 體制和安全證明做了進一步研究，用小規模的參數構造基於 RO 與無 RO 的 CCA 模式下可證安全 IBE 體制，避免以往證明中的一點不足，安全證明規約更簡化和緊致，基於 DBDH 假設，在 RO 和無 RO 模型下分別證明瞭體制的安全性，探討多安全模型下構造同時可證安全的密碼體制與證明方法是一個比較新穎和有意義的研究內容，有利於形式化保證密碼體制在多應用環境下的安全，其理論與方法還不成熟，還需要展開深入的研究。

REFERENCES

[1] Wang Yu-Min, Liu Jian-Wei. Communication network security-Theory and technique. Xidian University Press, 2002, 5 (王育民, 劉建偉. 通信網的安全—理論與技術. 西安電子科技大學出版社, 2002, 5).

[2] PKI. http://www.pki-page.org/

[3] Shamir A.. Identity-based cryptosystems and signature schemes. Advances in Cryptology-Crypto'84, LNCS 196, 1984, Berlin: Springer-Verlag, 47-53.

Copyright © 2009 SciRes

[4] Tanaka H.. A realization scheme for the identity-based cryptosystem. Advances in Cryptology-Crypto'87, LNCS 293, 1987, Berlin: Springer-Verlag, 341-349.

[5] Hühnlein D., Jacobson, M. Weber D.. Towards practical non-interactive public key cryptosystems using non-maximal imaginary quadratic orders. Selected Areas in Cryptography, LNCS 2012, 2000, Berlin: Springer-Verlag, 275-287.

[6] Sakai R., Ohgishi K., Kasahara M.. Cryptosystems based on pairing. Symposium on Cryptography and Information Security-SCIS'00, 2000, Okinawa, Japan, 26-28.

[7] Ma Chun-Bo, Ao Jun, He Da-Ke. Multi-Signature and Group Signature Based on Bilinear Pairing. Chinese Journal of Computers, 2005, 28(9): 1558-1563 (in Chinese) (馬春波, 敖珺, 何大可. 基於雙線性映射的多重簽名與群簽名. 電腦學報, 2005, 28(9): 1558-1563).

[8] Boyen X., Waters B. Full-domain subgroup hiding and constant-size Group signatures. Advances in Cryptology-PKC'07, LNCS 4450, 2007, Berlin: Springer-Verlag, 1-15.

[9] Boneh D., Franklin M.. Identity-based encryption from the weil pairing. Advances in Cryptology-Crypto'01, LNCS 2139, 2001, Berlin: Springer-Verlag, 213-22.

[10] Canetti R., Halevi S., Katz J. A forward-secure public-key encryption scheme. Advances in Cryptology-EUROCRYPT'03, LNCS 2656, 2003, Berlin: Springer-Verlag, 255-271.

[11] Canetti R., Halevi S., Katz J. Chosen-ciphertext security from identity-based encryption. Advances in Cryptology-EUROC RYPT'04, LNCS 3027, 2004, Berlin: Springer-Verlag, 207-22.

[12] Boneh D., Boyen X. Efficient selective-ID secure identity based encryption without random oracles. Advances in Cryptology-EUROCRYPT'04, LNCS 3027, 2004, Berlin: Springer-Verlag, 223-238.

[13] Boneh D., Boyen X. Secure identity based encryption without random oracles. Advances in Cryptology-CRYPTO 2004, LNCS 3152, 2004, Berlin: Springer-Verlag, 443-59.

[14] Waters B. Efficient identity based encryption without random oracles. Advances in Cryptology-EUROCRYPT'05, LNCS 3494, 2005, Berlin: Springer-Verlag, 114-127.

[15] Goyal V. Reducing Trust in the PKG in Identity Based Cryptosystems. Advances in Cryptology – CRYPTO'07, NCS 4622, Berlin: Springer, 2007, 430-447.

[16] Washington L. C.. Elliptic Curve Number Theory and Cryptography. New York, CRC Press, 2003.

[17] Boneh D., Franklin M.. Identity-based encryption from the weil pairing. SIAM Journal of Computing, 2003, 32(3): 586-615.

[18] Ming Yang. Study and design of universal designated verifier signature schemes [Ph. D. dissertation]. Xi'an: Xidian University, 2007, 12 (in Chinese) ([明 07] 明洋. 廣義指定驗證者簽名體制的研究和設計[博士論文]. 西安電子科技大學, 2007, 12).

Copyright © 2009 SciRes

Intelligent Information Management, 2009, 15-18
doi:10.4236/iim.2009.11003 Published Online July 2009 (http://www.scirp.org/journal/iim)

Total Domination Number of Generalized Petersen Graphs

Jianxiang CAO[1], Weiguo LIN[2], Minyong SHI[3]

[1] *School of Computer Science, Communication University of China, Beijing* 100024, *China*

[2] *School of Computer Science, Communication University of China, Beijing* 100024, *China*

[3] *School of Animation, Communication University of China, Beijing* 100024, *China*

Abstract: Generalized Petersen graphs are an important class of commonly used interconnection networks and have been studied . The total domination number of generalized Petersen graphs P(m,2) is obtained in this paper.

Keywords: generalized Petersen graphs, total domination set, total domination number, regular graph, domination set, domination number

廣義 Petersen 圖的全控制數

曹建香[1]，林衛國[2]，石民勇[3]

[1] 中國傳媒大學計算機學院，北京 100024；[2] 中國傳媒大學計算機學院，北京 100024；

[3] 中國傳媒大學動畫學院，北京 100024

摘　要：廣義 Petersen 圖是一類重要的並被廣泛研究的互聯網絡拓撲結構，控制數是圖論中的一個重要參數，而全控制數是控制數的一個變形，本文確定了廣義 Petersen 圖的全控制數。

關鍵詞：廣義 Petersen 圖，全控制集，全控制數，正則圖，控制集，控制數

1. 引 言

互聯網路具有廣泛的含義，泛指元件集合與通信通道集合按照一定的點對點方式相互連接所形成的系統。網路中的元件和元件之間的連接方式成為該網路的拓撲結構，人們通常把網路中的元件抽象成一個點，把通信通道抽象成兩點之間的連線，該網路中的拓撲結構就被抽象成一個圖。例如，一個通信網路可以用圖做模型，網路中的站點作為圖中的點，站點之間的連接作為圖中的邊。出於通信的需要，人們在站點安置發射器，利用某個站點上的發射器，可以把資訊發送到所有與該站相鄰的站點。為了覆蓋整個網路必須適當選取一些站點來放置發射器，使得每個站點都能接收到來自這些發射器的信號。在這裏抽象成圖論問題就是站點的選取相當於尋找圖中的控制集，出於經濟的考慮，發射器越少越好，這就是要去找圖中的最小控制集，所需要發射器的數目就是圖中的控制數。

上面提到的概念僅僅是控制這個概念的最原始的形式，在現實問題中很多問題都與控制的概念有關係，根據實際問題的不同，對控制的概念做了不同的變形，這裏要介紹的一種是——全控制數。然而對任意的圖確定其全控制數是 NP-完全問題，所以一般只能確定某些特殊圖類的全控制數，如在[1]中研究了兩類特殊圖廣義 De Bruijn 和廣義 Kauta 的全控制數。這裏我們主要求解廣義 Petersen 圖的全控制數。廣義 Petersen 圖是 Petersen 圖的推廣，是一類重要的互聯網

Copyright © 2009 SciRes

路, 因而受到廣泛的研究, 在[2]中研究了廣義 Petersen 圖的 Hamiltonian 圈，在[3]中研究了廣義 Petersen 圖的交叉數（crossing number），在[4]中給出了廣義 Petersen 圖 P(m,2)的直徑和寬直徑，在[5][6]中求出了廣義 Petersen 圖的控制數的一個上界。本文求出了廣義 Petersen 圖的全控制數。

2. 基本概念

所謂圖(graph)指的是一個二元組(V, E)，其中 V 是圖的頂點集(vertex-set)，它的元素稱為圖的頂點(vertex)，而 E 是圖的邊集(edge-set)，它的元素稱為圖的邊(edge), 一般用 V(G)和 E(G)來表示圖 G 的頂點集和邊集，以區別於其他的圖。一條邊 e 和兩個頂點相關聯(incident)，即 e=(u, v)，其中 u, v∈V, 此時稱 u, v 為 e 的端點(end-vertex), 並稱 u, v 是相鄰的(adjacent)。直觀地看，頂點就是空間中的點，而邊就是兩點之間的連接.若這樣的連接沒有方向，即對圖中每條邊都有(u, v)=(v, u)，那麼稱這樣的圖為無向圖 (undirected graph)，其中的邊稱為無向邊，並可用 u v 這種形式來表示。若 W⊆V(G),則 W 在 G 中的導出子圖記為<W>, 設 v∈V(G), 令 N(v)={u∈V(G)| uv∈E(G)} 和 N[v]={v}∪N(v); 設 A⊆V(G),令 N[A]={v|v∈A 或 ∃u∈A 使 uv∈E(G)}; 其中與頂點 u 相鄰接的頂點數稱為 u 的度，若一個圖中各個頂點的度都是 k，則稱該圖為 k 正則圖。

定義 1 廣義 Petersen 圖，記為 P(m, a),其定義如下：P(m, a)的頂點集為 U∪W,其中 U={$u_1,u_2,\ldots,u_m$}, W={$w_1,w_2,\ldots,w_m$}; P(m, a) 的邊集為 (u_i, w_i)(1≤i≤m),(u_i,u_{i+1})(i≥1,u_i=u_j, 如果 i≡j(mod m))和(w_i, w_{i+a})(i≥1,w_i=w_j, 如果 i≡j(mod m))。稱 U 中的點為外圈點，W 中的點為內圈點。廣義 Petersen 圖是 Coxter 於 1951 年引入的，顯然 Petersen 圖即為 P(5, 2)。

定義 2 若(u,v)是圖 G 中的一條邊，則稱點 u 全控制點 v。如果 T⊆V(G)能夠全控制所有 G 的頂點，則稱 T 是 G 的全控制集。所含頂點最少的全控制集稱為最小全控制集，其中的頂點數稱為全控制數，記作 γ_t (G)。

不難看出，全控制集就是不含孤立點的控制集，並且對任意圖，全控制集也肯定是控制集。文中所討論的圖 G 都是無向簡單圖, 用$\lceil x \rceil$表示不小於 x 的最小整數, 文中其他未加說明的概念和術語均參見文獻[7]。

3. 主要結論

為了證明主要定理，先給出一個引理。

引理 1 若 G 是一個具有 n 個頂點的 k 正則圖，則 γ_t (G) ≥$\left\lceil \frac{n}{k} \right\rceil$。

證明：由全控制數的定義知道，每個頂點可以控制除自身之外的 k 個頂點, 若設 T 是 G 的最小全控制集，設 u,v∈T，且 uv 是一條邊，在最好的情況下，N(u)∩N(v)=ϕ, 則此時 T 中每個點恰好控制了 k 個點，故 T 中頂點數不小於$\left\lceil \frac{n}{k} \right\rceil$。

定理 1 廣義 Petersen 圖 P(m,2)的全控制數為：

$$\gamma_t\,(\mathrm{P}(m,2)) = \begin{cases} 2k & m=3k \\ 2(k+1) & m=3k+1 \\ 2(k+1) & m=3k+2 \end{cases}$$ 其中 k≥2。

證明：證明過程主要是找出 P(m,2)的一個最小全控制集。下麵根據廣義 Petersen 圖的結構分三種情況討論：

情形 1 當 m=3k 時，證 γ_t (P(3k,2))=2k, k=1,2,…

取 T={$u_1,w_1,u_4,w_4,\ldots,u_{3k-2},w_{3k-2}$},|T|=2k, 下面分兩種情形來證明 T 就是 P(3k,2)的一個最小全控制集。

子情形 1.1 當 k 為偶數時

此時 P(3k,2)的內圈點構成了兩個長度為 3k/2 的內圈，外圈點構成一個長度為 3k 的外圈, 記外圈 C=$u_1u_2u_3\ldots u_{3k}u_1$。兩個內圈分別用 C_1，C_2 來表示：

C_1=$w_1w_3w_5\ldots w_{3k-1}w_1$;

C_2=$w_2w_4w_6\ldots w_{3k}w_2$.

因為(u_i, w_i)(1≤i≤m)是 P(3k,2)中的邊, 所以 T 中的頂點已被全控制。同時 T 中的外圈點 u_{3i-2}(1≤i≤k)全控制了外圈上的點 u_{3k},u_2, u_{3i-3} , u_{3i-1}，其中 2≤i≤k, 這些點及 T 中的外圈點恰好是全部外圈上的點，即外圈上的點全部被全控制。

對於 T 中內圈 C_1 上的點 $w_1,w_7,\ldots,w_{3k-5}$ 全控制了 C_1 上的 $w_{3k-1},w_3,w_5,\ldots,w_{3k-4}$。類似的對於 T 中內圈 C_2 上的點 $w_4,w_{10},\ldots,w_{3k-2}$ 全控制了 C_2 上的 $w_2,w_6,w_8,w_{10},\ldots,w_{3k}$。因此 T 是一個全控制集，故 γ_t (P(3k,2))≤|T|=2k。

又因為 P(3k,2)是一個 3 正則圖，由引理 1 知，γ_t (P(3k,2))≥(2×3k)/3=2k。綜上可得 γ_t (P(3k,2))=2k。

Copyright © 2009 SciRes

子情形 1.2 當 k 為奇數時

此時 P(3k,2)的外圈點跟子情形 1.1 一樣，用 C 來表示，內圈點構成了一個長度為 3k 的內圈，記為 $C_1=w_1w_3w_5\ldots w_{3k}w_2w_4w_6\ldots w_{3k-1}w_1$. 類似子情形 1.1, 易知 T 中的外圈點 $u_{3i-2}(1\le i\le k)$全控制了外圈上的點 $u_{3k},u_2, u_{3i-3}, u_{3i-1}$，其中 $2\le i\le k$, 這些點及 T 中的外圈點恰好是全部外圈上的點，即外圈上的點全部被全控制。

對於 T 中內圈 C_1 上的點 $w_1,w_4,\ldots,w_{3k-2}$ 全控制了 C_1 上的 $w_{3k},w_3, w_5, \ldots,w_{3k}$.被全控制。因此無論內圈點還是外全點都可由 T 中的點全控制，即 T 是一個全控制集，故 γ_t (P(3k,2))≤|T|=2k。

又因為 P(3k,2)是一個 3 正則圖，由引理 1 知，γ_t (P(3k,2))≥(2×3k)/3=2k。綜上可得 γ_t (P(3k,2))=2k。

綜合子情形 1.1 和 1.2 可知，當 m=3k，k≥1 時，有 γ_t (P(3k,2))=2k。證畢!

情形 2 當 m=3k+1 時,證 γ_t (P(3k+1,2))=2(k+1), k=1,2,…。

下麵分三種情形來討論：

子情形 1.1 當 k=1 時，此時 P(4,2)的結構比較特殊，只有外圈，沒有內圈，頂點集 $W=\{w_1,w_2,w_3,w_4\}$ 構成的子圖只有兩點邊(w_1,w_3)和(w_2,w_4)。假設 T 是 P(4,2)的最小全控制集，又由於 P(4,2)是 3 正則圖，故由引理 1 知γ_t (P(4,2))$\ge\left\lceil\frac{2\times4}{3}\right\rceil$=3。若 γ_t (P(4,2))=3, 即|T|=3，由全控制的定義知，T 的導出子圖不能含有孤立點，故 T 中的 3 點構成的子圖必須是連通的，分析 P(4,2)的結構知道，這樣的 3 個點生成的子圖中有兩條邊，下麵分 4 種情況來討論：

(1) 若該 3 點是外圈上的點，則 W 中的除與該 3 點相鄰的剩下的一個點不能被全控制；

(2) 若 T 中該 3 點中有 2 個是外圈上的點，另一個是內圈上的點，不失一般性，不妨設 $T=\{u_1,u_2,w_1\}$, 則此時 w_4 不被全控制；

(3) 若 T 中有 1 個點是外圈點，另 2 個點為 W 中的點，不失一般性，設 $T=\{u_1,w_1,w_3\}$,則，此時有 w_2,w_4 不被全控制；

(4) T 中的 3 個點不可能為 W 中的點，因為 $W=\{w_1,w_2,w_3,w_4\}$導出的子圖中只有兩條邊, 該子圖是不連通的，所以不存在 3 個點構成的連通子圖。

由上面 4 種情況的討論可知，P(4,2)不可能由 3 個點全控制，而存在四個點 w_1,w_2,w_3 及 w_4 可全控制 P(4,2)。故 γ_t (P(4,2))=4=2(k+1)。

當 k≥2 時，此時分兩種情況來討論，k 為偶數和 k 為奇數。

子情形 1.2 當 k 為偶數時

此時 P(3k+1,2)有一個外圈 C 和一個內圈 C_1，分別為

$C=u_1u_2u_3\ldots u_{3k}u_1$；

$C1=w_1w_3w_5\ldots w_{3k+1}w_2w_4w_6\ldots w_{3k}w_1$；

因為 P(3k+1,2)是一個 3 正則圖, 故由引理 1 得 γ_t (P(3k+1,2))$\ge\left\lceil\frac{2(3k+1)}{3}\right\rceil$=2k+1。

現令 $T_1=\{u_1,w_1,u_4,w_4,\ldots,u_{3k-2},w_{3k-2},u_{3k-1},u_{3k+1}\}$，此時 T_1 中的點 u_i 與 w_i 相互全控制,且 u_1 全控制了 u_{3k+1} 和 u_2,u_{3k+1} 全控制了 u_{3k}。其他的 T_1 中的 u_i 全控制了 u_{i-1} 和 u_{i+1}, 這裏 i=4,7,…,3k-2; 類似地, w_1 全控制了 w_{3k},w_3, T_1 中的 w_i 全控制了 w_{i-2} 和 w_{i+2}，這裏 i=4,7,…,3k-2，同時 u_{3k-1} 和 u_{3k+1} 分別全控制了 w_{3k-1} 和 w_{3k+1}。即 T_1 是 P(3k+1,2)的一個全控制集，而$|T_1|=2(k+1)$，故 γ_t (P(3k+1,2))≤2(k+1)，結合 γ_t (P(3k+1,2))$\ge\left\lceil\frac{2(3k+1)}{3}\right\rceil$=2k+1。可得 2k+1≤ γ_t (P(3k+1,2))≤2(k+1)。

下麵來證明 γ_t (P(3k+1,2))≠2k+1，從而得出 γ_t (P(3k+1,2))=2(k+1)。

反證法，假設 γ_t (P(3k+1,2))=2k+1。則∃一個最小全控制集 T，滿足|T|=2k+1。

因為 T 是最小全控制集，所以 T 中沒有孤立頂點，由廣義 Petersen 圖的結構性質知，T 中至少存在 3 個頂點，這 3 個頂點導出的子圖是一條路，這 3 個頂點要麼都是相鄰的外圈點或內圈點，要麼 2 個點是外圈點一個點是內圈點或反之。若 3 個點都是內圈點或者外圈點, 不失一般性, 不妨設該 3 點為 w_3, w_5, w_7, 這 3 個點相互全控制並且控制了外圈點 u_3, u_5, u_7 和內圈點 w_1, w_9，此時外圈上，u_3, u_4, u_5, u_6, u_7 是連續相鄰的點，但 u_4, u_6 未被控制，故要麼由內圈上的 w_4, w_6 來全控制, 要麼至少由 u_5 來全控制, 若是前者, 即 w_3, w_5, w_7, w_4, w_6 共控制了 14 個頂點，故剩下的 2(3k+1)-14 個頂點，至少需要 2(3k+1)-14/3=2k-4 個點來全控制，此時滿足這個最少數的條件是 T 中其他的任 2 個點都沒有公共鄰接點, 但是在 $w_{11},\ldots,w_{3k+1}$ 之間共有(3k-8)/2 個點未被全控制，要使這些點被全控制，其中不能有

Copyright © 2009 SciRes

相鄰的點在 T 中，否則這樣兩個相鄰的點控制了外圈上間隔為 1 的點，要使這個間隔點被全控制必然導致有兩個 T 中點有公共鄰接點, 這與 2k-4 個全控制點矛盾。因此要使 $w_{11},\ldots,w_{3k+1}$ 被控制，T 中控制這些點的相鄰點只能一個在外圈上一個在內圈上，但這至少需要(3k-8)/(2×3)個點，顯然這也導致 T 中有 2 個全控制點有共同的鄰域。所以這 3 個點其中有 2 個是外圈(或內圈) 點另一個點是內圈 (或外圈) 點，不失一般性，不妨設這 3 個點為 u_3,w_3,w_5, 這 3 個點全控制了 $u_2, u_3, u_4, w_1, w_3, w_5, w_7$, 這樣還有 3k+1-3+3k+1-4=6k-5 未被全控制,又因為每個點度為 3 只能全控制 3 個點, 故這 6k-5 個點至少需要 2k-1 個點來控制, 這樣全控制點至少有 2k-1+3=2k+2 這與|T|=2k+1 矛盾。綜上所述可知，不存在 2k+1 個點全控制 P(3k+1,2)。故 γ_t (P(3k+1,2))=2(k+1)。

子情形 1.3 當 k 為奇數時

在此種情況下有兩個內圈，證明類似子情形 1.2，這裏不再討論。

綜合上面的情況可知故 γ_t (P(3k+1,2))=2(k+1)，情形 2 證畢!

情形 3 當 m=3k+2 時，k≥1

此時，由引理 1 可得 γ_t (P(3k+2,2))≥ $\left\lceil \frac{2(3k+2)}{3} \right\rceil$=2k+2。

要證明 γ_t (P(3k+2,2))=2k+2, 只要證明存在一個全控制集 T⊆V(P(3k+2,2)),且|T|=2k+2 即可。

子情形 1.1 當 k 為偶數時

此時類似前面可知 P(3k+2,2)的外圈點構成一個長度為 3k+2 的外圈，記外圈 $C=u_1u_2u_3\ldots u_{3k+2}u_1$。P(3k+2,2)的內圈點構成了兩個長度為 3k/2 的內圈, 兩個內圈分別用 C_1，C_2 來表示：

$C_1=w_1w_3w_5\ldots w_{3k+1}w_1$;

$C_2=w_2w_4w_6\ldots w_{3k+2}w_2$.

取 $T=\{u_2, w_2, u_5, w_5,\ldots, u_{3k-1}, w_{3k-1}, u_{3k}, u_1\}$, 顯然 T 中的點 u_i 和 w_i 相互全控制，這裏 i=2,5,…,3k-1. 且 u_i 全控制了 u_{i-1} 和 u_{i+1}，u_{3k} 全控制了 u_{3k+1}，u_1 全控制了 u_{3k+2}，即外圈上的點可由 T 中的點全控制。由於 T 中的點 w_{3i+2} 全控制了內圈 C_1 上的 w_{3i} 和 w_{3i+4}，這裏 i=1,3,…,k-1，而 u_1 又控制了 w_1，故內圈 C_1 上的點可由 T 中的點全控制。對於內圈 C_2，T 中的點 w_2 全控制了內圈 C_2 上的 w_{3k+2} 和 w_4 ,T 中的點 w_{3i+2} 全控制了內圈 C_2 上的 w_{3i} 和 w_{3i+4}，這裏 i=2,4,…,k-2，而 u_{3k} 又控制了 w_{3k}，故內圈 C_2 上的點也可由 T 中的點全控制。綜上所述 T 是 P(3k+2,2)的一個全控制集，並且因為|T|=2k+2。故 T 是最小控制集。所以 γ_t (P(3k+2,2))=2(k+1)。

子情形 1.2 當 k 為奇數時。

此時 P(3k+2,2)的外圈仍記為 $C=u_1u_2u_3\ldots u_{3k+2}u_1$，內圈點只構成了一個長度為 3k 的內圈，記為 $C_1=w_1w_3w_5\ldots w_{3k+2}w_2w_4w_6\ldots w_{3k+1}w_1$。

取 $T=\{u_2, w_2, u_5, w_5, \ldots, u_{3k-1}, w_{3k-1}, u_{3k}, u_1\}$,類似子情形 1.1 可證 T 是 P(3k+2,2)最小控制集。所以 γ_t (P(3k+2,2))=2(k+1)。

綜合這兩種情形，得到當 m=3k+2 時，γ_t (P(m,2))=2(k+1)。證畢!

REFERENCES

[1] Huang Jia, On Domination-Stability of Graphs. The doctoral dissertation of the Univerisity of Science and Technology og China.(in Chinese) (黃佳, 圖的控制穩定性研究. 中國科技大學博士論文, 2007).

[2] Bnaani K. Hamiltonian cycles in generalized Petersen graphs [J]. J Combinatorial Theory, 1978, 181-183.

[3] Exoo G, Harary F, Kabell J. The crossing numbers of some generalized Petersen graphs [J]. Math Scand, 1981, 184-188.

[4] Hou Xin-min, Wang Tian-ming. Wide diameters of generalized Petersen graphs [J]. Journal of Mathematical Research and Exposition, 2004, 24(2): 249-253.

[5] QI Deng-ji, Domination Number of Generalized Petersen Graphs (m is odd) , Journal of Qingdao University of Science and Technology , Vol . 26 No. 1 Apr . 2005, 92-94(in Chinese) (齊登記. 廣義 Petersen 圖的控制數——當 m 是奇數時 P(m,2)的控制數[J]. 青島科技大學學報（自然科學版）, 2005, 26(1): 92-94).

[6] QI Deng-ji, Domination Number of Generalized Petersen Graphs (m is even) , Journal of Qingdao University of Science and Technology , Vol . 26 No. 2 Apr . 2005, 181-183(in Chinese)(齊登記. 廣義 Petersen 圖的控制數——當 m 是偶數時 P(m,2)的控制數[J]. 青島科技大學學報（自然科學版）, 2005, 26(2): 181-183).

[7] Bondy J A, Murty U S R. Graph theory with applications [M]. New York: North-Holland, 1976.

Copyright © 2009 SciRes

Intelligent Information Management, 2009, 19-24
doi:10.4236/iim.2009.11004 Published Online July 2009 (http://www.scirp.org/journal/iim)

Henan Cultural Information Resources Sharing Project Persistent Effect Mechanism Research

Weigong CUI[1], Hui JIAN[1], Yuan GAN[1], Zhen ZHANG[2], Yanfeng LIU[3]
[1]*Henan Provincial Department of Culture, Zhengzhou* 450000, *China*
[2]*Zhengzhou University, Zhengzhou* 450000, *China*
[3]*Zhengzhou Vcom Science & Technology Co., Ltd., Zhengzhou* 450001, *China*

Abstract: National Cultural Information Resources Sharing Project is a project which is benefit people and welcomed by people. Since this project started in 2002, it has got great achievements. However, with continuous expansion of the coverage, new problems has coming up. Henan cultural information resources sharing project group not only considering those new problems, but also thinking and exploring a long—term machanism for the project. The group choose resources and management system, as well as forming a guiding principle named guided by government, managed by enterprises, and benefit the people. It works as an intentive mechanism, which will monilize enthusiasm of grass-roots staff, and save the cost of network access for county extensio center through the project operation. With the integration of "data network, voice network and radio/television network", the group did some research and practices on sharing cultural information resources service on television netwoek, internet and 3G mobile network.

Keywords: cultural information resources sharing project, long-term mechanism, IPTV, digital library, cultural industry

河南省文化信息資源共享工程的長效機制研究

崔為工[1]，翦　輝[1]，甘　源[1]，張　震[2]，劉延鋒[3]

[1]河南省文化廳 鄭州 450000；[2]鄭州大學 鄭州 450000；
[3]鄭州威科姆科技股份有限公司 鄭州 450001

摘　要: 全國文化信息資源共享工程是是深受人民群眾歡迎的惠民工程。項目從 2002 年啟動實施以來取得了輝煌的成就，但是隨著覆蓋面的不斷擴大也發現了一些新的問題。河南省文化信息資源共享工程針對存在的問題的同時對項目發展的長效機制進行了思考和探索，項目組在選擇資源平臺建設、傳輸網絡建設、播放平臺建設和運行管理體系的同時，從戰略高度出發，以政府指導、企業運營、群眾得實惠為指導方針,形成一套激勵機制調動基層人員工作的積極性運營方案，同時通過項目的運營合作解決縣支中心網絡接入費用。隨著"三網"融合的實現，對文化共享工程資源在電視網、互聯網和 3G 移動網絡的共享服務也做了一些探討和嘗試。

關鍵詞: 文化信息資源共享工程，長效機制，數字圖書館，IPTV 模式，文化產業

1. 引 言

全國文化資訊資源分享工程（以下簡稱文化資訊資源分享工程）是新形勢下貫徹落實科學發展觀、構建公共文化服務體系、惠及千家萬戶的一項重要文化基礎工程，是政府提供公益性服務的重大文化專案，是實現廣大人民群眾基本文化權益的重要途徑，是解

Copyright © 2009 SciRes

決落後地區資訊閉塞，縮小“數位鴻溝”的有效舉措，對提高廣大人民群眾的科學文化素質，推進社會主義文化大發展大繁榮與建設和諧社會具有重要作用。

河南省文化資訊資源分享工程啟動於 2002 年, 河南省文化廳針對本省實際，以點帶面，全面推進文化資訊資源分享工程。在項目建設中堅持突出河南省特色文化資源建設、基層隊伍建設和文化資訊資源分享工程基層網點覆蓋面建設。工程實施七年來取得了顯著的成就，創造性地將文化資訊資源分享工程與黨員幹部現代遠端教育網共建共用。2007 年 2 月，中共河南省委組織部、河南省黨員幹部現代遠端教育試點工作領導協調小組、河南省文化廳、河南省財政廳聯合下發了《關於加強全省農村黨員幹部現代遠端教育與文化資訊資源分享工程資源整合工作的通知》正式啟動了全省農村黨員幹部現代遠端教育與共用工程資源整合工作，提出了明確要求，並做出了全面安排和部署。文化資訊資源分享工程與農村黨員幹部現代遠端教育共建共用，主要包括：一是整合基礎設施資源。兩大網路在省級技術平臺上進行資源對接，實現農村黨員幹部現代遠端教育資源庫與共用工程資源庫的互聯互通。農村黨員幹部現代遠端教育終端接收站點和共用工程基層網點採用“寬頻網路＋機頂盒＋電視機”建設模式，依託聯通的寬頻網路傳輸和播放資源。二是整合基層網點組織管理資源。在兩大網路基層網點的組織管理上，實行統一規劃，相互協調，共同管理，共同服務，實現人力資源的有效整合。管理人員的培訓，由各級遠端辦、文化部門、財政部門共同負責組織實施，確保教學管理和組織活動健康有效開展，形成了基層網點正常運行和維護的長效機制，走出了全國文化資訊資源分享工程的“河南模式”。

2. 實施進展及發現的問題

河南省文化資訊資源分享工程從開始至今一直受到省委、省政府的高度重視，是省委、省政府向全省人民承諾的十件實事之一。到 2010 年將建成 1 個省分中心、159 個縣級支中心、4.8 萬個村級基層服務點，實現縣縣都有支中心、村村都有基層服務點的全覆蓋目標，初步形成一個覆蓋河南全省的文化資訊資源分享工程服務網路，全省 6000 萬農村群眾可從中受益。河南省文化資訊資源分享工程省級分中心現已具備資源接收、製作、發佈、人員培訓的能力，並通過 IPTV 網路可以為群眾提供的數位資源總量已達到 10TB, 群眾將可以共用到相當於 1600 萬冊圖書、60000 小時視頻節目的優秀文化資源，滿足了農民“求知、求富、求樂”的需求，豐富了農民群眾的精神文化生活，有力的推進了全省公共文化服務體系建設和新農村建設。與此同時，我們也清醒地認識到，河南省的文化資訊資源分享工程仍處於起步階段，還存在許多困難和不足，在延伸服務的過程中我們發現了以下問題：

1) 部分貧困縣的財政比較困難, 不能按照國家要求撥付額定配套資金，後期的運行費用（電費、網路使用費、人員工資等）也無法保障，影響了共用工程的可持續發展。

2) 各級公共圖書館、鄉鎮文化站和村級文化大院技術人才匱乏，對伺服器等設備維護有困難比較大。

3) 隨著站點數量的不斷增加, 現有的人工上報服務情況的管理模式耗費時間長且資料不準確，難以適應目前專案發展要求。

4) 沒有健全的激勵機制做保障, 致使基層服務點工作人員積極性不高，造成了共用工程資源和設備使用率低，影響了基層文化活動的開展。

5) 河南全省基層網點的數量達到 4.8 萬個左右，基層服務隊伍的培訓工作開展成為一大難題。

6) 由於文化資訊共用工程資源的不斷擴充, 農村黨員幹部現代遠端教育平臺給予的存儲空間已經遠遠不能滿足專案發展的需求，需要在農村黨員幹部現代遠端教育平臺的基礎上擴充文化資訊資源分享工程的資源存儲及播放平臺。

針對以上幾個問題，河南省文化廳和河南省共用工程分中心通過積極的調研分析，並進行了思考和探索，初步形成了一套科學、可行的建設思路。

3. 發展目標

在“十一五”期間，按照文化部對文化資訊資源分享工程建設的要求，河南省文化資訊資源分享工程在河南省文化廳的領導下，以資源建設為中心，農村基層服務點為重點，取得了飛速的發展。為了實現文化資訊資源分享工程的良性可持續發展，打造文化資訊資源分享工程的“河南模式”，河南省文化資訊資源分享工程制定了如下目標：

1) 爭取各級財政的支援, 將文化共用工程各級中心、基層服務點的運行費用列入財政預算，確保工程

Copyright © 2009 SciRes

的日常運行。加強與企業進行合作，利用文化資訊資源分享工程的資源優勢與一些企業的業務相結合，互惠互利，在不增加農村群眾負擔的基礎上開展一些增值業務，產生的效益可納入共用工程管理經費，確保工程的可持續發展。

2) 通過與電信運營商進行合作，增強維護管理隊伍的技術能力。並通過網路培訓系統和業務考核系統實現工作人員的線上培訓和線上考核，保證了培訓效果，降低培訓的難度和成本。

3) 針對文化資訊資源分享工程的需求開發一套可自主運營和管理的運行系統，實現業務開展規範化和資料統計精確化。在省文化廳、市/縣文化局等主管部門創建運行管理平臺，在各級中心構建運營平臺，實現從專案建設管理、行政區劃管理、基層服務站點管理、業務培訓計畫制訂、培訓情況查詢、活動組織統計和資源回饋評價的全過程管理。

4) 建立文化資源分享工程的資源建設體系，整合國家資源、本地資源和互聯網資源，國家資源實現一點接收全省共用，本地資源實現省、市、縣特色資源插入，全省共用；並結合數位圖書館建設實現數位圖書的網路化服務。

5) 通過與黨員幹部現代遠端教育的基礎平臺、傳輸網路和基層站點建設的結合，在實現網路站點全覆蓋的基礎上加快推進共用工程資源的全覆蓋。主要包括建立文化資訊資源分享工程的資源存儲及播出平臺，包括省分中心和市支中心的節目製作、存儲、管理平臺和市、縣兩級存儲及播出平臺，並通過 CDN 資源智慧分發與調度手段，實現區域定制化服務。

6) 建設可擴展的應用平臺，在機頂盒+電視機模式的基礎上實現投影機+機頂盒、PC+終端點播軟體、3G 手機+資源點播軟體等多種服務模式，滿足城鄉村各種用戶需求，進一步拓展文化資訊資源工程的服務範圍。

最終要建設成一套河南省文化資訊資源分享工程的資源建設體系、運行管理體系和運營保障體系，形成可運營、可管理、可拓展的“河南模式”文化資源分享工程。

4. 河南省文化資訊資源分享工程的探索

河南省文化廳結合本省實際情況，在資訊資源分享工程的建設中，以科學發展觀為指導，緊緊抓住“以人為本”這一核心，提出“公益性事業，社會化管理，市場化運作”的發展思路，在系統平臺建設中採用支援未來 3G 移動應用的技術架構，在運營中大膽創新統籌兼顧，規範地植入一些市場元素，把有能力、有責任的企業介入到文化資訊資源分享工程的建設運營中來，通過政府扶持、企業參與、群眾得實惠的原則，逐步構建河南省農村公共文化服務體系，以確保文化資訊資源分享工程健康、可持續發展。

4.1 平臺建設

首先加強省分中心的建設，建設資源的加工、存儲、發佈平臺。在共用農村黨員幹部現代遠端教育平臺節目分發、網路管理、資料獲取、播出管理等系統的基礎上在各縣區部署資源存儲點播平臺，逐步實現縣支中心、鄉鎮文化站、街道/社區/村級基層服務網點的接入。該模式終端接入靈活快捷，設備操作簡單，實用性強。並隨著互聯網技術與 3G 移動網路的融合，文化資訊資源分享工程資源在 3G 移動網路平臺的應用將成為未來重要的傳播管道之一。系統平臺網路部署結構如圖 1 所示，在省分中心建設了獨立的資源接收、資源加工、資源存儲。

4.2 運行管理

河南省文化資訊資源分享工程運行管理系統是文化資源分享工程的重要組成部分，運行管理系統採用 B/S 架構，實現省、市、縣、鄉、村（社區）五級管理網路，完成了從站點開戶、建設管理、行政區劃管理、業務培訓計畫制訂、培訓情況查詢、文化活動管理、互動需求回饋、活動資料統計和資源評價的全過程管理，能夠讓文化資源分享工程工作從流程上形成一個閉環，為文化資源工程的推廣和完善提供支撐。系統模組組成如圖 2 所示:

4.3 終端服務

村級基層服務點是基層服務點建設的主要內容。它用來接收省(市)縣播出平臺播出的文化資訊資源，供站點使用。同時，也可通過電視圖文和數位圖書館的方式，為廣大群眾提供各種網站圖文資訊和圖書閱讀等服務。河南省文化資訊資源分享工程根據基層服務特點，有針對性的開發出了“文化共用機頂盒+投影機”和“PC+PC 資源播放用戶端軟體”的服務模式。可以廣泛應用於電子閱覽室、農村文化大院、農村文化活動室等多種應用。可以實現線上下載離線播放、卡拉 OK、數位圖書館等業務，同時還支援各種外接移動存儲設備，方便流動服務。

Copyright © 2009 SciRes

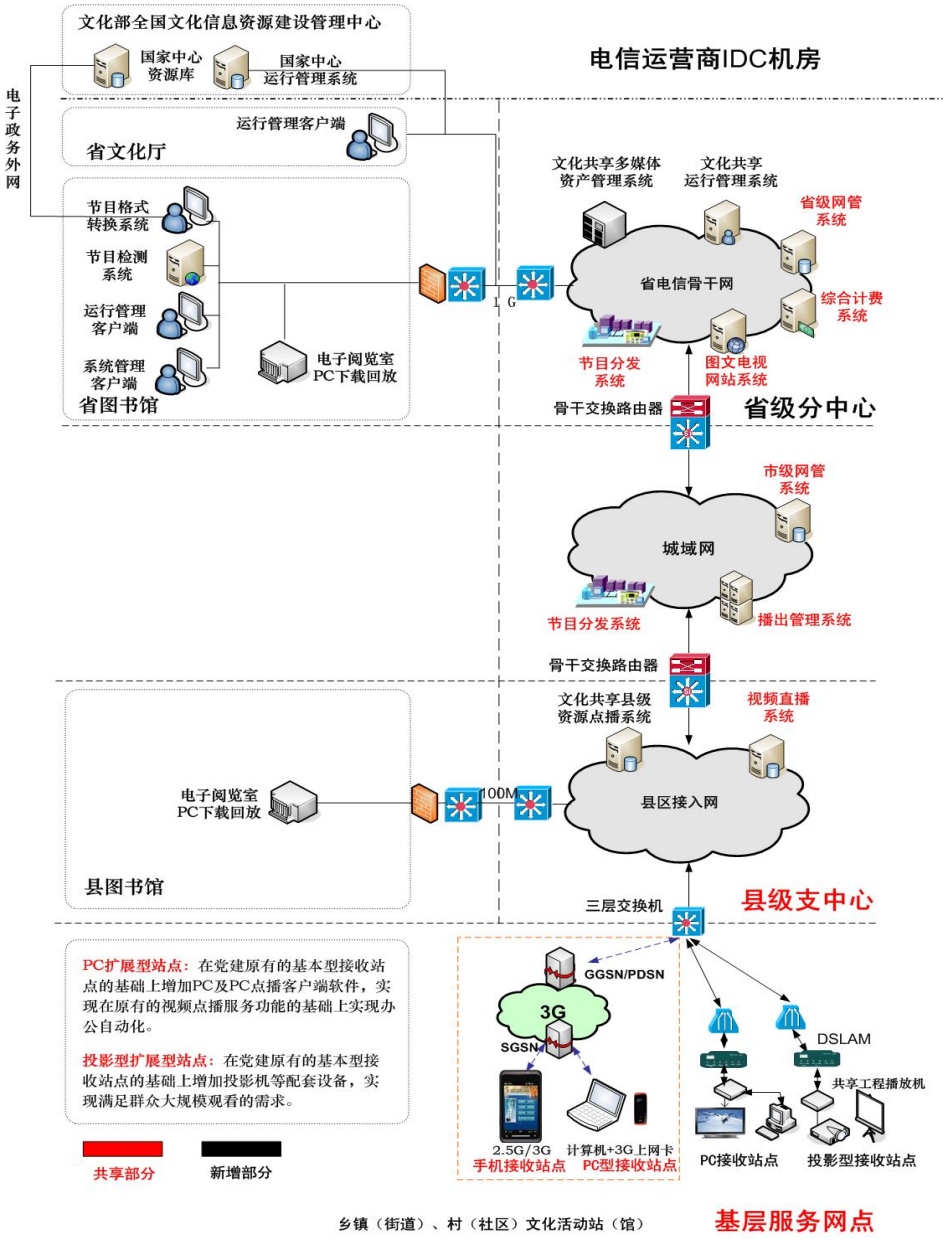


圖 1. 河南省文化信息資源共享工程網絡結構圖
Figure 1. Henan cultural information resources sharing project network structure

4.4 技術保障

通過 IPTV 平臺提供文化共用工程技術培訓和考核為一體的綜合平臺，可以有效的解決大量基層服務人員的培訓問題，保證了培訓的效果。同時通過與電信運營商進行合作，有效的解決了縣級支中心、鄉鎮文化站、村級基層站點技術力量薄弱問題，保障了系統的正常運行。

5. 平臺特點

5.1 低投入

可以共用農村黨員幹部現代遠端教育的省級網管系統、綜合計費系統、圖文網站系統、省級節目分發系統；市平臺的市級網管系統、市級節目分發系統；村級終端站點的相關場地、人員和設備，通過資源整

Copyright © 2009 SciRes

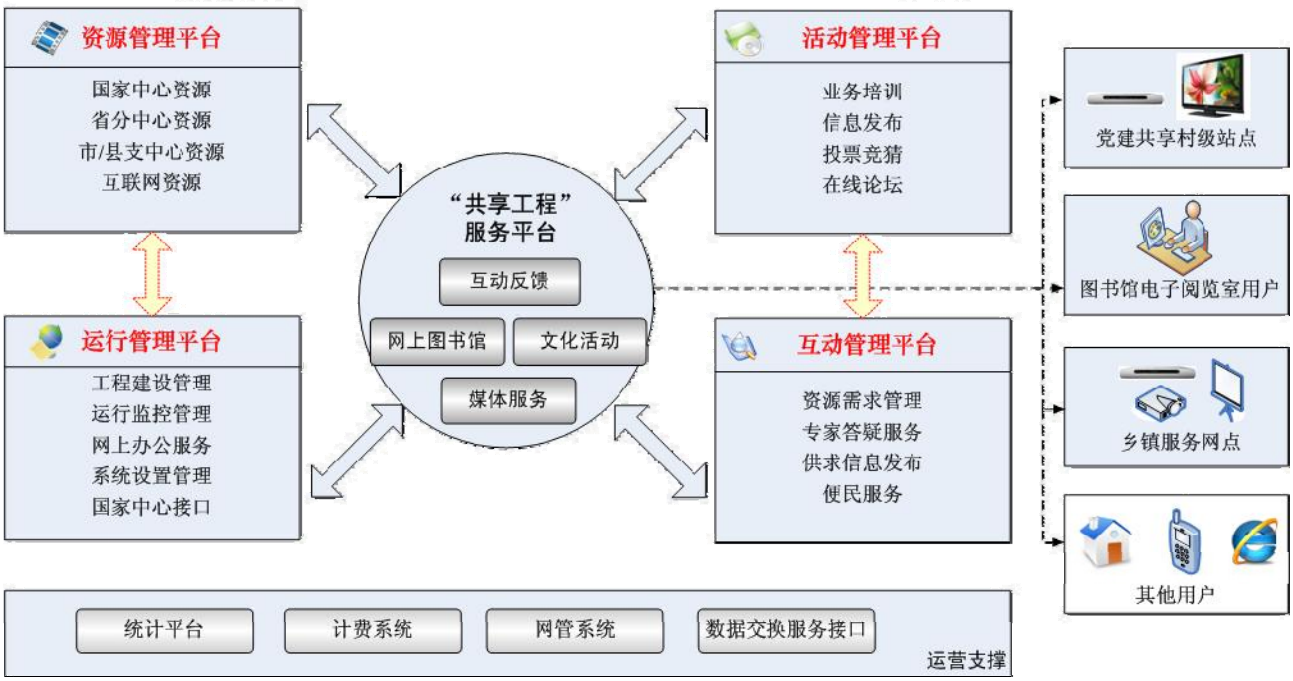


圖 2. 系統模塊組成圖
Figure 2. System modules

合、機構調整、資訊共用節約了大量的建設經費和維護經費。

5.2 易維護

省分中心、縣支中心的資源存儲和視頻點播伺服器都託管於聯通機房，減少了工作人員的維護難度和工作量；終端機頂盒支援網路自動升級，避免了後續功能擴展的問題。

5.3 實用性強

具有卡拉 OK、線上播放、離線播放等功能，適用於農村群眾組織室內或廣場搞文化、科技教育活動。

5.4 支援運營

平臺具有廣告等增值業務的支援能力，可以實現目前的互聯網運營和未來的 3G 網路運營。

5.5 功能擴展性強

支援電視機、投影機、PC、手機等設備上展現數位圖書館、數位博物館、網上書畫展等業務，且可以支援互動培訓和線上考試等功能。

6. 業務創新

6.1 卡拉 OK 功能

為了農村群眾的業餘生活，省分中心加工了一批群眾喜聞樂見的卡拉 OK 資源和非物質文化遺產中的一些優秀曲目，基層群眾可以通過機頂盒實現點歌、唱歌、原唱和伴唱自由切換，活躍了農村的文化生活也傳承和發揚了本省的特色文化。

6.2 資源更新服務

通過 IPTV 網路，基層服務點實現了共用工程資源的網路更新、線上播放和離線播放。

6.3 片頭插入功能

通過資源管理平臺設置，機頂盒可首先會預下載需要插播的視頻，存儲於本地，在節目正片播放前快速進行片頭插播。

6.4 虛擬數字圖書館

在機頂盒+電視機構建一個虛擬的“圖書館”和虛擬的讀書氛圍，為用戶提供拓展的數位圖書館服務。

Copyright © 2009 SciRes

6.5 滾動字幕

伺服器可以控制機頂盒滾動字幕播發內容，播發時間及播發次數，通過該平臺可以為基層群眾提供重要的農業預警類的即時資訊、政府相關公告和天氣預報等公共服務資訊。

6.6 手機移動播放

用戶可以通過 3G 手機點播文化資訊資源分享工程的電影、電視劇、戲曲等豐富多彩的精彩視頻節目。

7. 效益分析

河南省文化共用工程的實施，將開闢一條不受地域、時間限制的嶄新的文化傳播管道，將豐富的文化資源以先進的傳播方式傳輸到廣大基層群眾，尤其是欠發達地區的農民群眾手中，對於打破落後地區資訊閉塞的狀況，消除“數位鴻溝”，提高廣大人民群眾的科學文化素質，加強基層精神文明建設，促進經濟、社會協調發展、區域協調發展、城鄉協調發展將起到積極作用。主要體現在以下幾個方面：

1) 提出解決中西部經濟欠發達地區文化資訊資源分享工程開展過程中重建設、輕服務的難題的方法，保障了文化資訊資源分享工程的可持續發展。本項目的研究成果可推廣、複製到全國其他省、市，將帶動、促進全國文化共用工程的建設，引領建設方向，為此將產生重大的經濟和社會效益。

2) 促進農村經濟文化發展，保障了農民群眾的權益。通過與工商等單位合作，對假冒偽劣產品進行曝光，避免次品和過期產品危害群眾的利益。

3) 通過互惠互利，雙贏的思路拓展了文化共用的內涵。通過與萬村千鄉農家店工程、家電下鄉工程、金牧陽光工程進行合作，對一些產品品質好、市場信譽高的企業進行宣傳，對促進內需，拉動河南省農村市場經濟，農村物流體系建設，農村文化建設和社會和諧等都具有很大的意義。

4) 通過多種管道為農村群眾提供大量的農村實用技術、城鎮勞務資訊、農副商品產供銷資訊資源，幫助群眾瞭解新技術、新產品，開闢了農民發家致富的新途徑。

5) 隨著 3G 的應用，將可以帶動 1000 萬左右的城鄉手機用戶享受到文化共用工程的服務，有效的擴展了文化共用工程資源的服務範圍。

6) 通過互聯互通，數位圖書館建設打破原來的數字鴻溝，實現全省範圍內的“讀者共用”、“館員共用”、“數位資源分享”和“網路共用”，利用互聯網的傳遞和交互功能，把數位參考諮詢服務和各級圖書館的資訊資源實現了有效的整合，極大的改善公共圖書館、鄉鎮村文化站的公共資訊服務能力，全面提升、拓展城鄉一體化公共文化服務體系及其事業主體的多元化服務能力與社會效益。

8. 結 論

河南省文化資訊資源分享工程實施以來，始終堅持廣開管道、合作共贏、科學規劃、拓展服務的建設理念，不斷進行實踐和探索，結合全省公共文化體系建設找到了一條適合河南省實際情況的建設模式，形成了河南省文化資訊資源分享工程跨越式發展的長效機制，找出文化資訊資源分享工程可持續發展的一條新路子，取得了良好的服務效果。在豐富農村群眾精神文化生活、發展地方經濟建設和縮小城鄉之間文化發展差距發揮了重要作用。

REFERENCES

[1] 文化部關於做好 2008 年全國文化資訊資源分享工程建設工作的通知文社圖發[2008] 17 號 http://www.ccnt.gov.cn/gsjpd/shwh/sttsggz/t20080624_55325.htm.

[2] 全國文化資訊資源分享工程“十一五”規劃發展綱要 http://www.ccnt.gov.cn/gsjpd/shwh/sttsggz/t20061011_30821.htm

[3] 全國文化資訊資源分享工程情況 http://www.ccnt.gov.cn/gsjpd/shwh/sttsggz/t20080305_52104.htm.

[4] 中共河南省委組織部、河南省黨員幹部現代遠端教育試點工作領導協調小組、河南省文化廳、河南省財政廳. 關於加強全省農村黨員幹部現代遠端教育與文化資訊資源分享工程資源整合工作的通知. 豫組通[2007] l0 號.

[5] 全國文化資訊資源分享工程介紹 http://www.ndcnc.gov.cn/libpage/gxgc/index.htm.

Copyright © 2009 SciRes

Intelligent Information Management, 2009, 25-31
doi:10.4236/iim.2009.11005 Published Online July 2009 (http://www.scirp.org/journal/iim)

Reasoning with Ontology Model Based on Jena

Jing WU[1], Yongxin HUANG[2]
[1]*National Library of China, Beijing* 100081, *China*
[2]*Information Technology Institute, Beijing Union University, Beijing* 100101, *China*

Abstract: As the core of knowledge representation, reasoning plays an important role in the Semantic Web. In this paper, introduce Description Logic as the theoretical foundation of reasoning in the Semantic Web and OWL which needs to be expressive enough for representing knowledge and computationally tractable for inference of large-scale applications. Then construct an ontology model depicted with OWL by protégé and Jena API , and also prove the validity of reasoning with the model.

Keywords: OWL, description logic, jena, protégé

基於 Jena 的本體模型推理

吳　靜[1]，黃永欣[2]

[1]中國國家圖書館，北京 100081；[2]北京聯合大學，信息技術研究所，北京 100101

摘　要：推理作為知識表示的核心在語義 Web 中扮演著重要的角色。本文先介紹了語義 Web 中推理的理論基礎描述邏輯，以及提供較強知識表達能力並適合大規模應用推理的本體語言 OWL，然後結合建模工具 protégé 和語義網系統開發工具 Jena API 構建了一個用 OWL 語言描述的本體模型，並實現了對此模型的有效推理。

關鍵詞：本體網絡語言，描述邏輯，Jena，protégé

1. 背景和介紹

本體被定義成“概念模型的顯示表示”[1]，目前本體的應用熱點集中在語義 Web (Semantic Web) 中，本體實現了對 Web 內容的形式化與結構化描述，使得電腦也能夠在“理解”的前提下更好地處理、利用 Web 上的資訊和知識。因此,本體是語義 Web 的基石[2]。

本體語言如 RDF、DAML+OIL、OWL[3][4]是基於 XML 標準的，XML 是元資料(描述資料的資料)實現的技術手段,從資料與文檔的底層實現格式化。RDF 資源描述框架(Resource Description Framework)是建立在 XML 標準之上來描述元資料以及元資料與元資料之間的關係，其定義了一個簡單的資料模型，通過性質(property)和值(value)來描述資源以及資源與資源之間關係，因此 RDF 模型可以看成一個實體關係圖。RDF 是一種相對原始的語言，為了更詳細的描述資源，需要更強的表達能力，只有擁有自動推理功能這些描述機制才能在自動化處理中得到應用。基於以上考慮推動了 DAML+OIL 和 OWL 等本體語言的發展。這些本體語言是建立在描述邏輯研究的基礎上引入了 Web 的特點而建立起來的。其中 OWL 是 W3C 工作組在 2001 年創建的 Web 本體語言，2004 年 2 月 10 日起已正式成為 W3C 推薦標準[5]。

各種各樣的本體編輯工具也推動了本體技術進一步的發展,目前主要有 1)由美國 Manchester 大學開發的 OILEd[6]，它使用 OIL(DAML 十 OIL)本體語言來構建本體，較好地結合了框架表示(Frame

Copyright © 2009 SciRes

Representation) 和描述邏輯(Description Logical)表示兩者的長處。OILEd 編輯後的本體以 DAML 的檔形式存儲,載入了 FaCT(Fast Classification of Terminologies)推理機,可實現類的分層推理功能。2) 由美國 Stanford 大學開發的 Protege2000[7],它是用 Java 開發的一個開源專案，它採用 Plugin 機制使結構容易擴展，Protege 2000 beta 版開始以 OWL 插件的形式支持 OWL 格式的本體，此 OWL 插件以 Java 開發，用 Jena[8]包(HP 實驗室開發的 Java API)支援 OWL 文檔的讀取。Protege2000 工具本身沒有嵌入推理工具，不能實現推理，但該工具很容易嵌入其他的系統或與其他系統聯繫使用。本文使用外掛 Racer[9]推理機進行推理。3) 由英國 Knowledge Media Institute of the Open University 開發的 WebOnto[10]，它支持本體的協作創建和編輯，目的就是容易使用，也更容易地擴展形成大的本體，WebOnto 中本體的建模語言是 OCML。

根據實際需要，本文採用 Protégé 本體建模工具創建和編輯本體，利用 Jena 開發工具包對基於 OWL 語言描述的本體模型在應用程式中進行推理。

2. 描述邏輯

描述邏輯（Description Logic, DL）又稱為術語邏輯（Terminological Logic）或類 KL-ONE 系統，是在命題邏輯(Propositional Logical)和一階謂詞邏輯(First Order Logic, FOL)上發展起來的,是本體語言推理的重要設計基礎。描述邏輯的目的是在表達能力和推理複雜度之間取得平衡，便於提供自動推理服務，尤其是一致性（satisfiability）和歸約(subsumption)關係檢查。

一個標準的描述邏輯系統的體系結構由四個部分組成：(1)表示概念和關係(角色 Role)的構造集；(2)TBox (Terminology Box)一個描述領域結構的公理集,包含概念定義 (如: Wife≡Woman ∩ hasHusband. Man ，即 Wife 定義為“有丈夫的女人”)及公理(如:Woman Man)；(3)ABox (Assertional Box)一個描述關於具體個體事實的公理集，包含概念斷言(如：實例 Woman (marry),marry 是 woman)和關係斷言(如：hasHusband (Marry, Jack) Marry 的丈夫是 Jack)；(4)TBox 和 ABox 上的推理機制。一個基於 DL 的知識庫就是 K=TBox+ABox，簡寫成 KB(T,A)。

定義 1 知識庫解釋：對 KB(T,A)的解釋記為 I，$I=(\Delta^I,\cdot^I)$。其中 Δ^I 為 $\cdot^I$ 的論域，$\cdot^I$ 為映射函數，每個概念映射為 Δ^I 的子集，把關係映射為 $\Delta^I\times\Delta^I$ 一個子集，把實例映射為 Δ^I 的一個元素。一個描述邏輯主要依賴於構造運算元在簡單概念和關係的基礎上構造複雜的概念和關係。構造運算元如表 1 所示：根據構造運算元的不同對 DL 進行分類，最基本的 DL 是 ALC，它只包含合取∩、析取∪、非¬、存在量詞∃、全稱量詞∀這些構造運算元。SHIQ .DL 是在 ALC 的基礎上包含了原始關係/角色傳遞閉包，稱這種類型的 DL 為 S 是因為它和 the proposition (multi) modal logic S4(m)有關係，增加了逆 (inverse Role I)、關係/角色層次(role hierarchies H)、數量約束(Q)這幾種構造運算元,所以稱之為 SHIQ 。OWL DL 就是基於 SHIQ .DL[11]。

綜上所述描述邏輯是一種用來描述概念和概念層次關係的知識表示語言，儘管大多數本體模型採用的一階邏輯具有很強的表達能力，但其推理過程複雜不利於本體模型的檢驗，而描述邏輯可以看成謂詞邏輯的子語言，雖沒一階邏輯的表達能力強，但推理複雜度可知且更適合本體檢驗，而且 DL 的語法容易轉換成 XML/RDF 形式，因此基於 DL 的本體模型更適合 Web 環境下概念建模與知識共用。

表 1. DL 算子的語法與語義
Table 1. Syntax and semantics of DL

構造算子	語法	語義
原子概念	C,D	$C\subseteq\Delta^I$, $D\subseteq\Delta^I$
原子關係	R	$R^I\subseteq\Delta^I\times\Delta^I$
合取	$C\cap D$	$(C\cap D)^I=C^I\cap D^I$
析取	$C\cup D$	$(C\cup D)^I=C^I\cup D^I$
非	$\neg C$	$(\neg C)^I=\Delta^I\setminus C^I$
存在量詞	$\exists R.C$	$(\exists R.C)^I=\{x\mid\exists y.(x,y)\in R^I \text{ and } y\in C^I\}$
全稱量詞	$\forall R.C$	$(\forall R.C)^I=\{x\mid\forall y.(x,y)\in R^I \text{ inplies } y\in C^I\}$
數量約束	$\geq nR.C$	$(\geq nR.C)^I=\{x\mid\#\{y.(x,y)\in R^I \text{ and } y\in C^I\}\geq n\}$
	$\leq nR.C$	$(\leq nR.C)^I=\{x\mid\#\{y.(x,y)\in R^I \text{ and } y\in C^I\}\leq n\}$
逆	R^-	$(R^-)^I=\{(x,y)\mid(y,x)\in R^I\}$
傳遞閉包	R^+	$R^I=(R^I)^+$

Copyright © 2009 SciRes

3. Web 本體語言 OWL

OWL 是 W3C 推薦的標準本體表示語言，它的最大特點是關聯描述邏輯，這就意味著描述邏輯推理機可以推理 OWL 本體。OWL 是未來的 web 本體語言標準，它是建立在已有的 RDFS 和 DAML+OIL 技術之上的。OWL 通過對概念、概念屬性及其相互間關係的描述，構成概念的複雜關係網絡。

OWL 中的概念由類 Class 來表示，它可以是名字（如 URI）或運算式，而且提供大量的構造運算元來建立運算式，這裏的構造運算元與描述邏輯中的構造運算元相對應，OWL 強大的表達能力正是由它所支持的概念構造運算元、性質構造運算元以及各(Axioms)所決定的。

OWL 是用於在 Web 上描述本體的標準語言，有 3 個表達能力遞增的三個子語言：OWL Lite、OWL DL、OWL Full[12]。

（1）OWL Lite 提供了類層次的能力和簡單的約束能力。支持基數為 0 或 1 的基數約束。語言構造運算元可以分以下 6 個類別：

- RDF 模式特性包括類(Class)、子類（rdfs:subClassOf)、屬性(rdfs:property)、子屬性(rdfs:subPropertyOf)、域(rdfs:domain)、範圍(rdfs:range)和個體(individual)
- 相等/不相等包括類相等(equivalentClass)、屬性相等(equivalentProperty)、個體相同(sameIndividualAs)、不同於(differentFrom)、全不同(allDifferent)、區分成員(distinctMembers)
- 性質特徵包括類屬性(ObjectProperty)、資料類型屬性（Datatype Property）、逆反（inverseOf）、傳遞(transitiveProperty）、對稱（sysmetricProperty）、函數式（FunctionalProperty）、反函數式（InverseFunctionalProperty）
- 性質限制包括限制（Restriction）、限制於屬性（onProperty）、全部取值於(allValuesFrom)和一些取值於(someValuesFrom)
- 基數限制包括最小基數(minCardinality 0 或 1)和 最大基數(maxCardinality 0 或 1)
- 類相交(intersectionOf)

對於版本資訊、頭資訊和評注性質這裏不一一介紹。

（2）OWL DL（其中的 DL 表示描述邏輯）在保持計算完整性（computational completeness 所有的結論可以保證計算出來）和可判定性（decidability 所有的計算在有限時間內結束）的前提下，提供了盡可能大的表達能力，OWL 包含了 OWL 的全部語言構造成分但他們的使用受到一些限制（如一個類可以是許多類的子類，但不能是另一個類的實例）。OWL DL 的主要擴充是增加了布林邏輯運算操作，即邏輯否定和邏輯析取等。描述邏輯是 OWL 的形式化基礎，OWL DL 提供了描述邏輯的推理功能。

（3）OWL Full 包含 OWL 的全部語言構造成分並取消了 OWL DL 的限制，在 OWL Full 中一個類可以看成個體的集合，也可以看成是一個個體。由於 OWL Full 取消了 OWL DL 中的保證可計算的某些限制，在沒有計算保證的語法自由的 RDF 上進行最大程度表達，允許在一個 Ontology 在預定義的（RDF、OWL）辭彙表上增加辭彙，從而任何推理軟體均不能支援 OWL FULL 的所有特點，因此不存在完整的推理演算法支援 OWL Full 的全部特性。

OWL DL 和 OWL Full 中用來擴展 OWL Lite 的構造運算元如下分為 3 類：

- 類公理包括枚舉類型（one of,dataRange）、分離(disjointWith)、類相等（equivalentClass 用於類運算式）、子類(rdfs:subClassOf 用於類運算式)
- 任意基數限制包括最小基數(minCardinality)和最大基數(maxCardinality)
- 類運算式的布林組合包括析取（unionOf）、合取(intersectionOf)和取反（complementOf）
- 填充資訊包括擁有值（hasValue）

4. 開發工具介紹

Protégé[7]是一個斯坦福大學開發的本體編輯器，為開放源碼軟體，具有優秀的設計和眾多的插件，是目前使用最廣泛的本體編輯器之一。它採用圖形化介面，介面上以多個 Tab 分別支持 Classes,Slots,Forms,Instances,Queries 的編輯。它的結構容易擴展，Protege 2000 beta 版開始以 OWL 插件的形式支持 OWL 格式的本體，此 OWL 插件以 Java 開發，用 Jena 包(HP 實驗室開發的 Java API)支援 OWL 文檔的讀取如圖 1 所示。

Protege 的安裝是獨立的。它可支援多種格式的本

Copyright © 2009 SciRes

體檔的輸入編輯和編輯後的輸出，類(Concept)的編輯是分層的，有具體類和抽象類。Protégé 可以根據使用者的需要進行定制，如可以定制用戶的介面以更好地適應新語言的使用；具有可擴展的結構，可根據需要添加所需要的功能模組。Protégé 2000 工具本身沒有嵌入推理工具，不能實現推理，但該工具有良好的可擴展結構，很容易嵌入其他的系統中或與其他系統聯繫使用，如直接與外部的具有推理功能的語義模組聯繫[14]，本文的例子採用外掛 Racer 推理機。

一般來說，我們在 Protégé 這樣的編輯器裏構建了本體，就會想在應用程式裏使用它，這就需要一些開發介面。用程式操作本體是很必要的，這裏我們使用 Jena API。Jena[8]是惠普實驗室語義網研究項目的開放資源，是一個基於 W3C 的 RDF、DAML/OIL、OWL 進行語義網建模和推理的 Java API 開發包。Jena 框架主要包括如下幾部分：

（1）An RDF API：用於對 RDF 檔和模型進行處理的 RDF 應用程式介面，其主要功能包括創建和讀、寫、操作和檢索 RDF 模型，語義網應用程式可以通過 Jena 提供的 RDF API 在 RDF 檔（例如用本體建模工具 Protégé 建立的或是網路上已經存在的 RDF 檔）和 RDF 模型之間實現轉換，並且用戶可以對 RDF 模型實施簡單而必要的操作和檢索，這是整個應用程式開發的基礎支撐條件。

（2）ARP：Jena 的 RDF/XML 解析器是隨 Jena 發佈內嵌的重要功能，解決了對基於 XML 語法和格式的 RDF 文檔的解析問題，通常在調用 Jena API 的 Read 方法時會調用解析器的功能，為獲取 RDF 文檔中的資訊以及創建 RDF Model 提供支援。

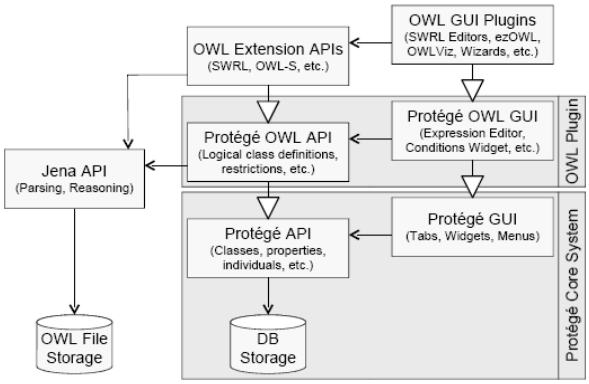


圖 1. Protégé 的 owl plugin
Figure 1. Owl plugin of Protégé

（3）Persistence：持續化功能，除了在記憶體中存儲 RDF、RDFS、OWL 等資料模型，對於資料量較大的本體模型可以通過 Jena 提供的資料庫引擎將其模型存儲到關聯資料庫中，用戶可以用 Jena 的查詢語言 RDQL API 將這些資料從資料庫中檢索出來從而創建 RDF 模型以供進一步使用和處理。目前 Jena 2 資料庫引擎支援 MySQL、Oracle 和 ProtegeSQL 等資料庫，支援 Linux 和 Windows XP 等作業系統。

（4）Reasoning subsystem：推理子系統，Jena 提供基於規則的推理機（如 RDFS Reasoner、OWL Reasoner 等），它包含了一般的推理功能，此外用戶還可以根據需要自定義推理規則，也可以註冊使用第三方推理引擎（例如：本文採用的是 Racer 推理機）。

Jena 是 RDF 和 OWL 的 API，也提供 OWL 和 RDF 的推理功能，Jena 核心只是提供了有限的查詢元語。DL 推理機的實現比較複雜，而 Racer 提供了一個很好的 DL 推理機（描述邏輯推理機），而且還提供標準的 DIG interface 支援。但目前的 DIG interface 只支援標準的 DL 推理服務，尚未支援 OWL 推理。Racer 剛剛開始試驗性的支持推理 OWL 不是一個推理查詢語言最多能用 OWL 描述本體，但不能用 OWL 來詢問本體。這就需要對 OWL 和 DIG 作適當的結合。就推理方面，Jena 自身提供的是基於規則的推理機，是通過規則來實現對 OWL 的推理，不能對所有的推理功能支援，性能上也比不過 Racer，Racer 算是 DL 推理機裏性能最強悍的了，可以支援工業使用，Jena 裏的 Rule Reasoner 性能並不是很理想。Racer 使用的是 DIG 介面，需要通過 HTTP 或是 TCP 訪問，如果知識庫不是很複雜的話，可能會由於通信的時間消耗反而使性能下降。另一方面 Racer 一定程度來說只是單純的推理機，它不對知識庫的存儲做很多考慮，而 Jena 對知識庫的存儲乃至持久化支援的都很完整（可以把知識庫直接存在關聯資料庫中）新版的 Jena 2.2 已經開始支援集成使用 DIG 介面的 Reasoner 了。Jena 是一定要用的，用不用 Racer 要看知識庫的複雜程度和對推理功能的要求。在推理方面可以通過 DIG 介面連接專門的推理機，由於推理需要 DL 推理機，所以這裏我們採用 Racer，通過 Dig 介面 Racer 直接使用 jena 進行編碼實現推理。

Copyright © 2009 SciRes

5. 本體推理應用實例

實例使用 Protégé 本體建模工具建立本體模型，該本體描述了六個原始概念（原始類 primitive class）：人（people）、男人（man）、女人（woman）、父親（father）、母親（mother）和父母（parent），一個屬性（關係）：有孩子（hasChild），三個實例：Jim、Marry 和 Terry 和一個定義類（defined class）：誰有孩子（WhoHasChild），用 OWLViz（Protege3.1 版本的一個 plugin）顯示結果本體模型如圖 2 所示：

Man、Woman 和 Parent 均是 People 的子類，Man 和 Woman 兩個類沒有交集是互斥關係（用 Disjoint 來聲明），Parent 至少存在一個 hasChild 關係（最小基數 minCardinality 為 1）說明有孩子的個數大於等於 1 的 People 是 Parent，Father 是 Man 和 Parent 的共同子類，Mother 是 Woman 和 Parent 的共同子類和 Father 沒有交集，這樣就定義了只有既是 Man 同時也是 Parent 的 People 才是 Father，同理既是 Woman 同時也是 Parent 的 People 才是 Mother。聲明三個實例：Terry、Marry 和 Jim，三個實例均為 People 類的實例，同時定義了 Marry 有孩子是 Jim（通過屬性 hasChild 關聯），Terry 是 Parent.最後定義一個 Definded 類 WhoHasChild（用 equivalentClass 來聲明）用於推理，它的充要條件是 WhoHasChild≡hasChild.People≥1。本例主要根據給定的實例描述得出哪些 People 有孩子，也就是推理機 Racer 推理後劃分在 WhoHasChild 類下的實例既是我們想要的結果。圖 3 是在 Protégé 運行 Compute inferred types 命令後得到的推理前與推理後的類結構對比圖。

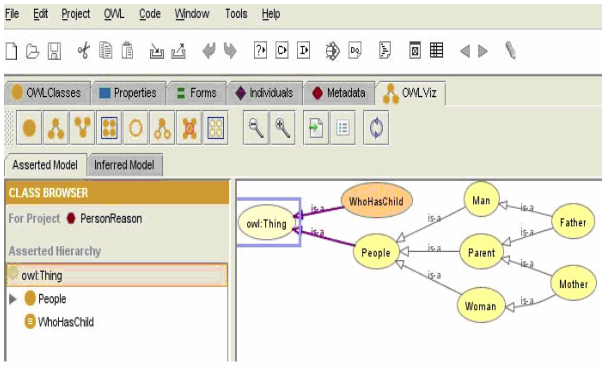


圖 2. 本體模型可視化顯示
Figure 2. Visualization of the ontology model

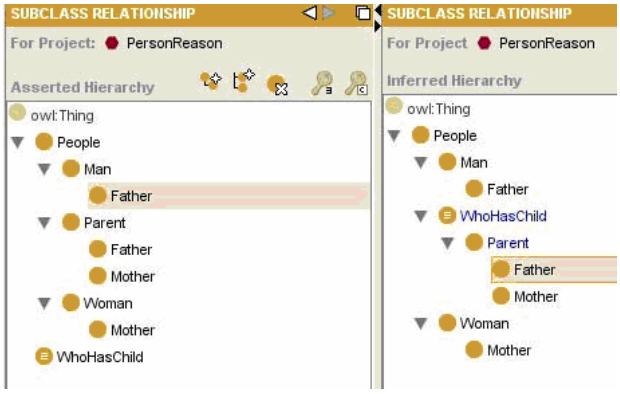


圖 3. protégé 中的斷言類結構和推理類結構對比
Figure 3. Contrast between asserted hierarchy and inferred hierarchy of Protégé

可以看出獲取本體中的知識包含兩個方面：

（1）獲取 TBox 中類的關係和屬性的關係，具體來說就是獲得類的子類集（就是包含推理）、屬性的子屬性集、屬性的特徵、屬性的定義域和值域等等，它更接近於概念的查詢，因此推理可靠性較高，不能出現概念錯誤。本例中對應的是推理後將 Parent 類劃分到 WhoHasChild 類下（因為 Parent 類的屬性 hasChild≥1 符合 WhoHasChild 類的充要條件），說明屬於 Parent 類的概念一定屬於 WhoHasChild 類的概念，同時將 WhoHasChild 類作為 People 的子類。

（2）獲取 ABox 中的資訊，具體來說有獲得一個類的所有實例、實例的屬性、獲得滿足條件的所有實例等等，它更接近於實例的檢索和資訊的流覽，因此推理的速度和效率要求較高，所獲得資訊的完整性就成為次要需求。本例中對應的是推理後 WhoHasChild 類下的實例為 Marry (實例 Marry 是 People 同時又存在 hasChild 關係，則 Marry 是 Parent，而 Parent 又是 WhoHasChild 的子類，則 Marry 是 WhoHasChild 類的實例)，這就是實例規類，目的是把一個描述好的實例歸入一個最具體的、最能反映它特徵的類中。

上述推理過程採用 Jena API 實現代碼如下(只寫出核心代碼)：

```
public class Reason {
//Racer 推理機所需的 URL
  string REASONER_URL="http://localhost:8080";
ProtegeOWLReasoner  reasoner=null;
//該 OWLModel 模型是從 owl 檔中讀取建立的
//該檔對應的本體模型是在 Protégé 中建立
```

Copyright © 2009 SciRes

```
public void reason(OWLModel model)
throws DIGReasonerException{
//如果連接不上推理機直接返回
if(this.isConnected(model)==null)  return;
//得到推理後 People 下的子類
Collection inferredSubClass=
reasoner.getSubclasses(peopleClass,null);
for (Iterator iter = inferredSubClass.iterator();
iter.hasNext();) {
OWLNamedClass cls =
(OWLNamedClass) iter.next();
System.out.println("inferredSubClass
name:"+cls.getName());
//得到某類所有實例(包含推理出來的)
Collection Individuals=
reasoner.getIndividualsBelongingToClass(cls,null);
for (Iterator iterator = Individuals.iterator();
iterator.hasNext();) {
OWLIndividual element =
(OWLIndividual) iterator.next();
System.out.println("—individualsBelongingTo
Classname:"+element.getName());
}
}
//推理機是否鏈結成功
Private ProtegeOWLReasoner
isConnected(OWLModel model){
//從推理機管理工廠中獲得推理機實例
ReasonerManager reasonerManager
=ReasonerManager.getInstance();
reasoner=
reasonerManager.getReasoner(model,true);
reasoner.setURL(REASONER_URL);
//連接推理機是否成功注意 Race 推理機一定要啟
動
if(reasoner.isConnected()){
DIGReasoner Identityidentity
=reasoner.getIdentity();
return reasoner;
}else{//列印連接失敗資訊
return null;}
}
}
```

運行結果:

```
inferredSubClass name:Woman
inferredSubClass name:Man
inferredSubClass name:WhoHasChild
--individualsBelongingToClass name:Marry
--individualsBelongingToClass name:Terry
```

可以看出Marry和Terry是有孩子的People.

6. 結論和展望

本文我們概括的介紹了在 Web 語義推理中所需要理解掌握的一些知識如描述邏輯、本體描述語言 OWL、本體建模工具 Protégé、推理機 Racer 和開發工具包 Jena。在此基礎上我們用一個簡單例子說明了這些知識在推理中的作用。需要指出的是：在應用本體時,除了這些基本的推理，還可以定義很多附加規則來實現高層次的推理，這些上層次的推理主要是針對具體領域、具體應用的。本例中的實例是存儲在 owl 檔中的也就是將實例和概念存儲在一起，在 ontology 中針對海量實例可以把實例和其他概念分開存儲，例如把實例存儲在關聯資料庫中，Jena 本身提供了持久化存儲方案,還有開源項目 The OWL Instance Store 也提供了針對 ABox 推理的海量資料問題的解決方案[13]。推理作為知識表示的核心在語義 Web 中扮演著重要的角色，隨著 OWL 語言在語義 Web 領域中廣泛應用，會有很多基於這種語言的推理技術出現，這將會進一步引發 Web 上本體應用的快速發展，各種推理的應用將會被用來輔助建立和應用 Web 上的本體。Jena 作為惠普實驗室開發的開放資源是實現語義 Web 應用系統的有力工具，Stanford 大學開發的 Protégé 工具使我們更加方便的建立本體模型，借助這些工具我們可以加深對 ontology 等研究物件的理解和認識，推動語義 Web 技術的發展。

REFERENCES

[1] Gruber T R. A Translation Approach to Portable Ontology Specifications[S]. Knowledge Acquisition, 5/1993: 199−200.

[2] Chen Kai,He Keqing,Li Bing,Liang Peng. Research on Ontology Modeling Using Object-Oriented Technology.Computer Engineering and Applications, 2005, 41(2): 40-43 (in Chinese)(陳凱, 何克清, 李兵, 梁鵬. 面向對象的本體建模研究[J], 電腦工程與應用[J],2005, 41(2): 40-43).

Copyright © 2009 SciRes

[3] Asunción Gómez-Pérez, Oscar Corcho. “Ontology Specification Languages for the Semantic Web. [S]” IEEE Intelligent Systems, 2002, 17(1), 54−60.

[4] Gao Qi,Chen Huajun.Comparison And Analysis Of Web Ontology Languages And Reasoning. Computer Applications and Software,2004,21(10) (in Chinese)(高琦, 陳華鈞. 互聯網Ontology語言和推理的比較和分析[J]. 電腦應用與軟體,2004, 21(10)).

[5] Frank Manola, Eric Miller. RDF Primer[EB/OL]. W3C Working Draft, 2004-02-10. http://www.w3.org/TR/2004/REC-rdf- primer -20040210/.

[6] Bechhofer S, Horrocks I, Goble C, *et al*. OILEd: A reasonable ontology editor for the semantic web[R]. Joint German/Austrian conference on Artificial Intelligence, 2/2001, 174: 396−408.

[7] Knublauch, H., Fergerson, R. W., Noy, N. F., Musen, M. A.: The Protégé OWL Plugin: An Open Development Environment for Semantic Web Applications [R], Third International Semantic Web Conference - ISWC 2004, Hiroshima, Japan, 2004.

[8] restol.Jena2.ASemanticWebFramework[EB/OL].http://Jena.Sourceforge.net (Accessed Oct.12, 2004).

[9] V. Haarslev, R. Möller, A.-Y. Turhan. RACE User’s Guide and Reference Manual Version 1.1[R]. Technical report, University of Hamburg, Computer Science Department, 1999.

[10] Domingue J. Tadzebao. WebOnto: Discussing, browsing, and editing ontologies on the web[R]. Proceedings of the 11th Knowledge Acquisition for Knowledge-Based Systems. Workshop, 1998.

[11] I. Horrocks, U. Sattler, S. Tobies. Reasoning with individuals for the description logic shiq[J]. In D. MacAllester, editor, Proc. of the 17th Conf. on Automated Deduction (CADE-17), number 1831 in Lecture Notes in Computer Science, Germany, 2000. Springer-Verlag.

[12] Mike Dean, Guus Schreiber. OWL Web ontology language reference [EB/OL]. W3C Working Draft, http://www.w3c.org/TR/2003/WD-owl-ref-200330331/, 2003.

[13] Instance Store website. [EB/OL] http://instan- cestore. man.ac.uk.

[14] Tao Wan,LIAO Ahu-mei.Analysis and research of current ontology editing tools.Computer Engineering and Design,2005,26(3)(in Chinese)陶皖，廖述梅.當前本體編輯工具的分析與研究[J].電腦工程與設計,2005,26(3)).

Copyright © 2009 SciRes

Intelligent Information Management, 2009, 32-37
doi:10.4236/iim.2009.11006 Published Online July 2009 (http://www.scirp.org/journal/iim)

Design of the Collaborative Platform on Clustering Applications for Governments

Xuewang ZHANG[1,2], Zhoujun LI[2], Wei SHEN[3]
[1]*College of Software, Chongqing University of Posts and Telecommunications, Chongqing* 400065*, China*
[2]*School of Computer Science and Engineering, Beihang University, Beijing* 100191*, China*
[3]*Chongqing South China Zenith Information Technology Co.,Ltd, Chongqing* 400039*, China*

Abstract: The collaborative platform on clustering applications for governments consists of six large-scale systems, including the clustering Government Internet portal system, clustering public-mailboxes collaboration system, clustering government affairs portal system, clustering emergency information collaboration system, clustering office automation collaboration system, and clustering messages collaboration systems. The application and technique architectures of the collaborative platform are elaborated in this paper，and the major key technologies on the platform are also expounded, which includes realization of many governments applications' scale integration and collaborative application, business model driven software development platform based on SOA, SSO, tans-departmental and cross-level multi-engine clustering protocol. Based on the "clustering application" design, to maximize the utilization of hardware, software resources and administrative resources of the provincial government collaborative platform, rural districts and counties can build their own platforms based on the provincial platform. The platform having been running for over 2 years shows that the planning of urban and rural e-governments' construction and maintenance is achieved, thus reducing costs greatly and improving governments' functions and efficiencies.

Keywords: clustering applications, collaborative applications, single sign on, components, e-government

集群政務協同業務平臺的設計

張學旺[1,2]，李舟軍[2]，沈　偉[3]
[1]重慶郵電大學軟件學院 重慶 400065；[2]北京航空航天大學計算機學院 北京 100191；
[3]重慶南華中天信息技術有限公司 重慶 400039

摘　要：集群政務協同平臺包括六大系統，本文論述了該平臺的總體應用架構和總體技術架構的設計，闡述了它的主要關鍵技術：多個政務應用的規模集成和協同應用，業務模型驅動的 SOA 架構通用開發平臺，單點登錄技術，跨部門、跨層級的多引擎集群協議。基於"集群化應用"設計思想，集群政務協同平臺能夠最大限度地整合利用省（市）級政務平臺的軟硬件資源和政務業務資源，使農村區縣基於省（市）級平臺構建各自的政務平臺。某省（市）2 年多的運行實踐表明，該平臺實現了政務平臺的城鄉統籌建設和維護，經濟效益和社會效應巨大。

關鍵詞：集群應用，協同應用，單點登錄，構件，電子政務
中圖法分類號：TP393　　**文獻標識碼：**A

1. 引 言

在國家主導建設下，中國的電子政務基礎設施和應用系統都取得了較大進展，中央和地方政府分別建立了大量的政務應用系統，在政務資訊公開和政府工作開展中發揮了重要作用。但是，中國的政務應用系

本文受國家自然科學基金重大研究計劃項目（90718017）和重慶市重大產業開發技術項目（渝發改技[2007]1110 號）資助。
張學旺（1974-），男，講師，主研方向：網絡信息安全、軟件工程；李舟軍（1963-），男，教授，博導，主研方向：高可信軟件與理論、信息安全理論與技術、數據挖掘與文本挖掘技術；沈偉（1974-），男，總經理助理，主研方向：企業信息化。

Copyright © 2009 SciRes

統建設還存在著下列較突出的問題：

1）政務資訊孤島嚴重，政務資訊交換與共用平臺建設滯後；

2）重複建設較普遍，很多政務資訊系統沒有發揮出應有的作用；

3）政務資訊系統建設城鄉差距大；

4）政務資訊化專業技術人員不足，尤其在區縣等基層政府中表現相當突出。

為了促進政務平臺城鄉統籌建設和維護，我們根據某省（市）的政務資訊化建設的需要，設計並實現了集群政務協同業務平臺。

2. 集群政務協同業務平臺的架構設計

2.1 總體應用架構

集群政務協同業務平臺由六大系統組成，總體應用架構如圖 1 所示。

1）集群政府公眾門戶系統。是集群政務業務協同平臺實現政務資訊服務的核心，是政府在 Internet 上的視窗和服務平臺。集群政府公眾門戶系統既非單一站點，也不是簡單的將各部門站點鏈結起來，而是基於集群應用的立體化的綜合門戶。它實現以下功能：

① 省（市）政府對各級機關網站進行統一規劃，將所有分散的資訊與網上服務集中到集群政府公眾門戶網站，讓公眾能夠在一個地方就可以流覽所有的資訊和得到所有的政務網上服務。

② 各級機關利用集群內容管理系統進行自建網站專業化網站設計、內容發佈、資訊管理，以準確掌握資訊的合理性和對資訊進行及時的更新。

③ 省（市）政府集群網站群管理系統實現網站群的管理。集群站點群管理主要實現四方面功能：一是實現網站群站點彙集，二是實現資料共用和同步，三是在資料整合基礎上實現服務的整合，四是實現網站群統一部署、即時跟蹤資訊的變更情況、統一評測。流程控制和許可權控制貫穿整個過程。

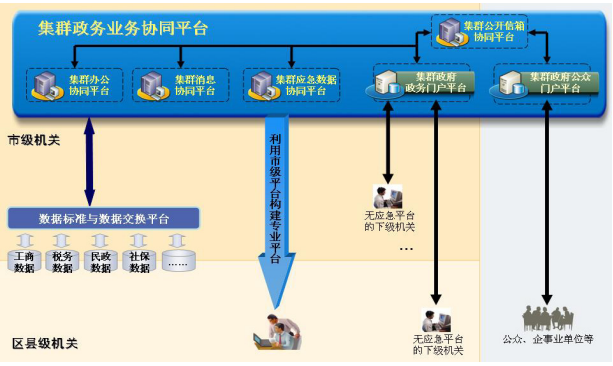


圖 1. 集群政務協同平臺的總體應用架構

Figure 1. The application architecture of the collaborative platform on clustering applications for governments

2）集群公開信箱協同系統。遵循“分級負責、屬地管理”原則，在辦理工作中實行“集中受理、歸口辦理、集中公示、統一監管”制度，在省（市）級政府各部門間實現對市民問題的協同辦理。集群應用表現在政府各網站有集群公開信息協同平臺的統一入口，市民可統一使用一個平臺；各級機關可直接登錄省（市）政府集群公開信箱協同系統或建立自己的內部集群公開信箱系統、對市民來信協同辦理；政府及主管部門對信件處理過程進行監控、向市民回饋處理結果等業務應用，實現市民來信的“日記日清、有問必答”。

3）集群政府政務門戶系統。主要實現三大功能目標：一是省（市）政務外網用戶統一身份認證，實現“單點登錄，全網通行”；二是集成省（市）政府各委辦廳（局）政務業務系統；三是成為全省（市）政務工作人員的工作平臺，實現跨機關的工作辦理。核心是實現省（市）政務外網用戶統一身份認證。

4）集群應急資料協同系統。既可實現應急資料協同，也可實現應急業務平臺集群。應急資料協同，即由省（市）政府資料交換中心的交換伺服器和公安、衛生、安檢、環保等各共建單位的交換前置機通過政務網連接，各委辦廳（局）通過省（市）政府系統提供的接入功能，實現部門應急資料的採集和匯總，並在此基礎上整理、合併、清洗後形成統一的應急中心資料庫，實現應急資料的整合利用與資源分享。應急資料獲取協同建設包括建立應急資料交換標準和目錄、建立應急資料交換平臺兩方面。

應急業務平臺集群，即在建成應急中心資料庫與應用系統的基礎上，下級機關利用集群應急資料協同系統構建本單位的專業化或區域應急平臺，直接利用省（市）級應急資料中心的整合資料，並通過系統定制的基礎服務實現如動態監測、預測預警、應急指揮、災後評估和恢復重建、任務派發、應急資訊發佈等應急業務應用。

Copyright © 2009 SciRes

5）集群辦公協同系統。旨在實現橫向區域、縱向行業間交錯繁雜的政務公文資訊集群應用，通過利用省（市）政府資訊中心（簡稱 GDC）完善的硬體資源（網路設備、伺服器設備等）、軟體資源（中間件、資料庫、政務辦公系統等），實現區域、行業中的集群辦公及協同應用。

6）集群消息協同系統。整合了集群辦公協同系統的集群即時通訊產品，除具有一般 RTX 平臺產品（如騰訊 QQ、MSN 等）的即時溝通交流、短信發送（支援雙向收發）、狀態展示（支援聯繫人狀態關注）、聯繫人分組、聯繫人資料管理、快速搜索（支援模糊查找）、歷史消息查看、視頻通訊（640*480 高清晰視頻）、群組語音通訊（支援 6 人）、群組文字通訊（支援 80 人）、RTX 電話（USB Phone）、遠端登錄、自動升級、個性化界面等功能外，還具有以下兩方面特色功能：根據省（市）政府組織結構設置分組，用戶可清晰看到即時更新的由樹型目錄（LDAP）表達的多層次機關組織架構電子通訊錄，從而極大地方便相關業務處室間即時通訊對口管理；集成辦公協同系統資訊，可在消息系統中集成其他各集群政務協同系統的消息（如待辦事宜、工作提示等）。

2.2 總體技術架構

集群政務協同業務平臺的軟體架構基於 J2EE 標準和 SOA 架構，使流覽、邏輯、業務、資料各層合理劃分，讓系統整體構架更加優化。總體技術架構分為門戶層（服務管道層）、應用支撐層、應用層、資訊資源層四層架構，如圖 2 所示。

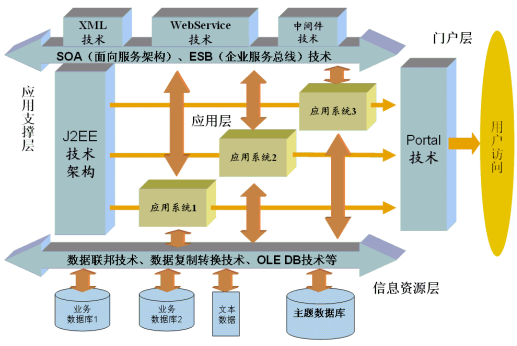


圖 2. 集群政務協同平臺的總體技術架構

Figure 2. The technique architecture of the collaborative platform on clustering applications for governments

1）應用支撐層。用 J2EE 的應用服務中間件，採用面向服務（SOA）的體系結構，結合 Web Service 技術、XML 技術、消息中間件等具體技術，實現應用整合、內容管理和應用系統構件化開發等。

2）應用層。用 J2EE 技術開發構件化的通用業務功能平臺，以業務功能平臺為基礎組裝業務應用系統。需要對外提供的服務進行 Web Service 封裝。

3）門戶層。將各種資料資源綜合起來形成複雜頁面，以易於用戶接收的表單形式返回給用戶。封裝各種應用服務，以使用戶可按角色規定的許可權獲得個性化的應用服務。

4）資訊資源層。依託資料中心實現關聯式資料的整合，統一管理關聯式、非關聯式資料。

通過採用圖 2 所示的架構，整個平臺的多層劃分便於將各層構件置於不同的物理伺服器上，各層的負載可分擔到各自的後臺伺服器上，並且在業務層、資料層還可以用集群方式（如採用分區資料庫方式），這些措施可以極大地提高系統的運行效率。

平臺相容性方面，應用程式、Web 服務總控程式（Servlet）和系統業務資料處理層（EJB、JavaBean）都是通過 JDBC 方式聯接後臺資料庫，這樣，對提供 JDBC 訪問界面的各類通用資料庫系統都支援。在各層 JVS（Java 虛擬機）的支持下，實現了平臺無關性與可跨平臺應用。伺服器端的作業系統可用 UNIX、Windows NT 以及 Linux。伺服器端的資料庫則可用 DB2、SQL Server、Oracle 等多種通用資料庫。

3. 集群政務協同業務平臺的主要關鍵技術

3.1 實現多個政務應用系統的規模集成與協同應用

集群政務協同平臺，首先建設 SOA 架構平臺；然後在 SOA 架構平臺上建立六大系統；最後六大系統共同構成省（市）級協同電子政務平臺（包括 Internet 企業公眾服務平臺與政務業務協同平臺），其中 Internet 企業公眾服務平臺包括集群政府公眾門戶系統和集群公開信箱協同系統，政務業務協同平臺包括集群政府政務門戶系統、集群應急資料協同系統、集群辦公協同系統和集群消息系統。

1）協同應用。即各政府機關業務在政府部門間統一的工作平臺上按統一業務規則政務業務資訊的交換

Copyright © 2009 SciRes

和處理。包括從操作和應用層面建立全省（市）政府機關電子化和網路化協同資訊流管理、協同消息體系、協同業務流管理。

協同資訊流管理，指對政務業務資訊流進行統一的規劃和治理，實現橫（同級機關間）、縱（上下級機關間）兩個方向實現文檔資料與表格資料等的快速收集和即時處理，形成全省（市）政府機關間資訊流交換和共用的支撐體系。

協同業務流管理，指形成橫、縱兩個方向即時、有效、便於多種應用相集成的統一業務流。例如全省（市）各政務機關統一跨機關的公文延續辦理，公文流轉實現橫（不同政府部門之間）、縱（上下級政府）間有序的全電子化流轉。協同應用可擴展至任意的跨機關業務處理，從而可以在應用架構上建立各類跨機關的應用系統，實現全省（市）政府機關間協同工作業務處理和快速回應工作體系。

協同消息體系，指在全省（市）政府機關間，多種形式的消息傳遞、接收、回饋和監控支撐體系，對協同資訊流和協同業務流構成輔助支撐。

“協同應用”設計思想旨在提升全省（市）政府機關協同業務處理和快速回應能力，是集群政務協同業務平臺建設的核心。

2）集成展現。通過採用統一資源管理平臺、內容管理技術、單點登錄技術，採用有條件的授權方式在網路門戶上查看到所有網路業務系統的資料和整合後的資料。集成展現包括“對內”和“對外”兩方面，“對內”在集群政府政務門戶系統上集成政務業務管理資訊，便於相關領導提供及時全面的政務決策支援資訊，便於業務管理人員一目了然地把握相關工作動態；“對外”在集群政府公眾門戶系統上為政務業務服務物件和公眾提供盡可能全面、便捷的政務業務資訊和公共服務資訊，提升政務服務效率，便於業務網路服務管道的普及推廣。

集成展現是集群應用、協同應用的設計思想的最終目的與效果展現。

3.2 SOA 架構的通用開發平臺

SOA 架構的通用開發平臺是基礎，它強調業務模型驅動（BMD）。

1）業務模型驅動。體現“以業務模型為中心”的思想，這一思想要求基於企業工程理論和業務模型體系使用基於 SOA 的業務建模模式，並將業務模型構件作為管理軟體發展的主體產品。業務建模的關鍵基礎是業務模型體系；業務模型體系是從企業資訊化的需要出發，針對企業的業務和管理所做的一種體系性抽象和描述，它可以為資訊系統的設計和開發提供科學、合理的導向和依據。業務建模的過程，是從業務和管理的現實和知識出發，參照業務模型體系，採用業務建模工具，設計並構建出相關的業務模型構件；業務模型構件是業務建模的主要產品。

我們把基於 SOA 的政務業務模型總結為包括業務領域（一組相互關聯比較密切的可以作為一個整體看待的業務功能的組合）、業務過程（一個完整的業務行為，也即一項業）、業務活動（一個可以賦予一個物件進行操作的業務動作）三個層次。業務領域可以包含低一個層次的業務領域或業務過程；一個業務過程可以為服務物件提供一個完整的服務，由於業務的多變性和複雜性，同時一個業務中會存在與其他業務的協作，一個業務也可能包含其他的業務過程，甚至其他業務領域中的業務過程；業務活動也稱為一個原子業務，它是一個可獨立操作的業務元素，業務活動組成業務過程。

在基於 SOA 的政務業務模型調整中我們觀察到這樣的規律：業務活動不隨業務模型調整的變化而變化，業務模型調整的一般是業務領域、業務過程。因此，基於業務活動構建業務模型構件能夠很好地解決業務模型調整導致的變化需求；業務模型就可以適用新的業務改變。所以，業務模型構件應是針對業務活動的，這種業務活動是原子化的，不可再分。

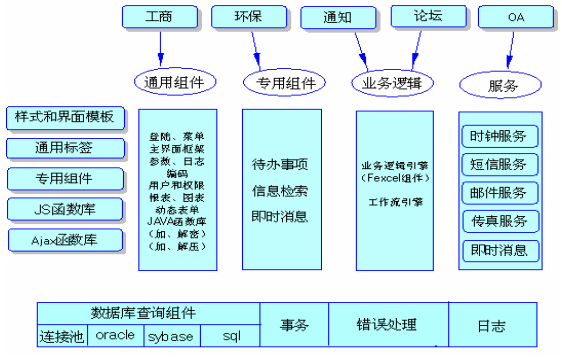


圖 3. 業務模型構件結構

Figure 3. The structure of business models' components

Copyright © 2009 SciRes

2）業務模型構件。包括應用的分層結構、層次之間的資訊傳遞和控制機制、相關的配置檔的設置、錯誤控制、日誌管理、事務和緩存的管理控制機制等內容。集群政務協同業務平臺的業務模型構件結構如圖 3 所示，基礎服務構件包含資料庫查詢構件、事物處理、錯誤處理、日誌等，時鐘服務，系統服務構件包括短信服務、郵件服務、傳真服務等。

業務邏輯引擎是最重要的核心構件，由我們自主設計實現的類微軟 EXCEL 構件的、基於 J2EE 的 Web 構件 FEXCEL 充當，FEXCEL 構件採用 DSL（Domain Specific Language，領域專用語言）的方式描述業務邏輯，融合面向物件、面向方面和面向服務這三種開發方法的優點，擴充 EXCEL 功能使之具有強大的資料處理功能和複雜的業務邏輯處理能力，並實現了企業級應用的主要功能需求：異構資料源支援，大資料量輸入的複雜界面、資料展現界面和資料輸出處理，複雜業務邏輯處理，併發資料訪問，資料安全，不同用戶的個性化需要。它大大簡化了 Java 等主流通用編程語言開發基於 J2EE 的 Web 應用相同的軟體功能的難度和複雜度，通過配置能夠生成相應的業務處理代碼，以適應不斷變化的用戶需求。

我們採用基於 SOA 的 J2EE 的 MVC 架構，利用 Ajax 標籤（例如：文本框、下拉式列表框、日曆控制項、按鈕、樹型控制項、圖形按鈕等界面元素標籤控制項）、頁面範本（包括多套主頁模版、功能表模版、界面模版）、應用構件（包括用戶管理、許可權管理、登錄和註冊管理、編碼管理、參數管理、日誌管理、工作流、通用查詢、通用報表、圖表分析、動態表單、通用資料轉入和轉出等應用服務構件），建立業務模型構件，再利用構件組裝技術把業務模型構件組裝為業務過程、業務領域，從而實現業務模型，來建立應用系統。

3）構件組裝。服務構件組裝技術是基於構件的軟體發展的核心技術。如何將構件組裝形成應用系統卻受到構件模型、體系結構、構件粒度、運行環境等因素的制約；反過來，使這些因素要盡可能地有利於構件的組裝，則更為關鍵和重要。在基於 SOA 的通用開發平臺我們採用“基於匯流排”與“基於連接器”相結合的方法，實現構件組裝；能夠使適應於業務需求不同與變化的新應用構件，可方便地融入該開發平臺。

基於體系結構連接器的構件組裝方法開發軟體發展，首先根據用戶需求和實現環境的要求確定系統的體系結構，定義系統中的構件及構件之間的關係。其次在可複用構件庫和連接器庫中查找符合要求的構件與連接器，必要時開發新的滿足要求的構件、連接器。最後通過組裝工具把這些構件和連接器組裝起來，生成新的應用系統。基於該體系結構的構件組裝框架如圖 4 所示。

3.3 SSO 技術

SSO（Singe Sign On，單點登錄）是集群政務協同業務平臺的核心技術之一，用來整合各政府部門業務系統中存在的大量孤立、分散的身份管理，實現跨平臺的單點登錄管理。單點登錄被設計成一個獨立的 Web 應用，通過運行在 HTTPS 伺服器上的多個系統服務進程加以實現，外部認證訪問界面主要是通過 URL 進行。

SSO 的主要功能如下：

1）集中身份資訊存放及維護。提供統一的身份資訊存儲，實現用戶的統一管理，包括註冊、組織調換、登出等常見用戶管理操作，用戶的排序顯示、並能維護排序依據等。提供用戶分組維護，方便用戶授權管理。

2）子系統用戶分級管理。各功能子系統中需要存放本系統的所有的用戶標識資訊，這些用戶標識資訊需要與集中存放的身份相對應，因此在維護時需要與集中存放身份庫同步。關於用戶的許可權角色等功能屬於功能子系統功能，SSO 不涉及這方面的內容，也不進行集中許可權管理，這是 SSO 的精華。用戶分級管理需要實現兩步操作：本功能子系統用戶的增加和統一身份庫中用戶的增加，是一個用戶同步的問題。

3）用戶憑證映射管理。憑證映射是實現統一身份庫中用戶與各功能子系統中用戶實現關聯的方法。要實現用戶關聯，憑證映射管理首先需要實現對常見身份存儲的訪問，如目錄服務、關聯資料庫等。其次需要提供統一身份庫和功能子系統身份庫中用戶的流覽視圖，方便用戶實現關聯操作。自動映射時需要用戶提供映射依據（如用戶編號），手動映射時需要用戶在

Copyright © 2009 SciRes

統一身份庫和子系統身份庫選擇用戶，系統根據用戶情況實現映射操作。

4）統一登錄界面及登錄界面管理。提供統一登錄界面，登錄後其他功能子系統直接存取登錄資訊而不需要再次登錄，從而實現單點登錄。各功能子系統利用集中存放的身份與各子系統存放的身份之間的映射資訊確定登錄者在該系統中的具體許可權。

5）統一用戶註銷管理。提供各功能子系統的退出功能，為保證系統安全與系統的方便實用，用戶在使用各功能子系統的過程中可以隨時退出登錄，再次訪問被保護資源時需要顯示登出是否成功資訊。根據用戶的當前登錄資訊，調用 SSO 提供的註銷功能，清除用戶登錄後的憑證資訊，以實現用戶登出。

新增系統可以方便地集成到目前的 SSO 系統中。原系統可以兩種方式實現集成：一種方式是將原系統與活動目錄中的用戶進行映射，此時原系統需要有自己的用戶資訊庫；另一方式是以統一用戶庫中的用戶作為本系統的用戶庫，原系統中需要有許可權資訊表作為系統許可權控制的依據。

3.4 跨部門、跨層級多引擎集群協定

考慮類 DNS“跨部門、跨層級多引擎集群協定”把政務門戶、公開信箱、公文、業務資料等形成的“縱（跨層級）橫（跨部門）交錯”的條塊互通體系所需的各自相關引擎形成一個整體。其協定內容主要有：

1) 功能變數名稱協議：定義位址的規則。

2) 資料傳輸協議：通過調用 Web Service，資料以基於 HTTP 的 SOAP 協定傳輸，該協定是通過 80 埠傳輸，不受防火牆限制，並支援跨平臺、跨編程語言調用。並確定資料傳輸安全性協議。

3) 資料格式協定：針對不同的應急應用系統，定義 XML 資料交換格式。

4) 界面規則協定：定義通用的及不同的應急應用系統專用的界面函數。

4. 結束語

集群政務協同業務平臺歷時 3、4 年研發，已經成功地在某省（市）投入應用，兩年多的運行表明，該平臺取得了多項集成創新，能夠最大限度地整合利用省（市）級協同政務平臺的網路、服務存儲平臺、軟體資源和政務業務資訊資源，使農村區縣直接基於該協同政務平臺構建各自的政務平臺，實現了政務平臺城鄉統籌建設和維護，大大降低了某省（市）政務建設成本和維護成本，產生的經濟效益和社會效益都很大。以經濟效益為例，據保守估算（僅算總量的 40%），一個委辦廳（局）機關平均可節約 20 萬元/年，某省（市）每年可降低直接行政成本 2000 萬元左右；抑制了電子政務建設中較為普遍存在的重複建設和無效建設，進一步保證了某省（市）每年至少 8000 萬元投入的有效性。

REFERENCES

[1] Marijn Janssen, Soon Ae Chun, J. Ramon Gil-Garcia. Building the next generation of digital government infrastructures[J]. Government Information Quarterly, 2009,26(2): 233-432

[2] Yusong QI. Research on System of Service Web_Oriented E-government[PhD]. Nanjing University of Technology, 2007 (in Chinese) (戚玉松. 面向服務的電子政務系統研究[PhD]. 南京：南京理工大學, 2007)

[3] Alexandros Kaliontzoglou, Panagiotis Sklavos, Thanos Karantjias, et al.. A secure e-Government platform architecture for small to medium sized public organizations [J]. Electronic Commerce Research and Applications, 2005,4(2): 174-186

[4] LI Chang-yun, YANG Ai-min, MAN Jun-feng, et al.. An Approach to Constructing Business Model for Services Integration According to Requirement[J]. Chinese Journal of Computers, 2006, 29(7): 1095-1104 (in Chinese) (李長雲, 陽愛民, 滿君豐等. 一種面向按需集成服務的業務模型構造方法[J]. 計算件學報, 2006, 29(7): 1095-1104)

[5] LIN Bo, ZHOU Ming-hui, LIU Tian-cheng, et al.. A Web Container Integration Framework in J2EE Application Servers[J]. Journal of Software, 2006,17(5): 11958-11203 (in Chinese) (林泊, 周明輝, 劉天成等. 一個 J2EE 應用伺服器的 Web 容器集成框架[J]. 軟體學報, 2006, 17(5): 11958-11203)

[6] YUE Kun, WANG Xiao-ling, ZHOU Ao-ying. Underlying Techniques for Web Services: A Survey[J]. Journal of Software, 2004,15(3): 428-442 (in Chinese) (嶽昆, 王曉玲, 周傲英. Web 服務核心支撐技術:研究綜述[J]. 軟體學報, 2004, 15(3): 428-442)

Copyright © 2009 SciRes

Intelligent Information Management, 2009, 38-45
doi:10.4236/iim.2009.11007 Published Online July 2009 (http://www.scirp.org/journal/iim)

A New Method for Calculating Similarity between Sentences and Application on Automatic Abstracting

Wenqian JI, Zhoujun LI, Wenhan CHAO, Xiaoming CHEN
Department of Computer Science and Technology, BeiHang University，Beijing 100191*, China*

Abstract: Sentence similarity computing plays an important role in machine question-answering systems, machine-translation systems, information retrieval and automatic abstracting systems. This article firstly sums up several methods for calculating similarity between sentences, and brings out a new method which takes all factors into consideration including critical words, semantic information, sentential form and sentence length. And on this basis, a automatic abstracting system based on LexRank algorithm is implemented. We made several improvements in both sentence weight computing and redundancy resolution. The system described in this article could deal with single or multi-document summarization both in English and Chinese. With evaluations on two corpuses, our system could produce better summaries to a certain degree. We also show that our system is quite insensitive to the noise in the data that may result from an imperfect topical clustering of documents. And in the end, existing problem and the developing trend of automatic summarization technology are discussed.

Keywords: sentence similarity, automatic abstracting, lexrank, sentence-weight computing, redundancy resolution

句子相似度計算及其在自動文摘系統中的應用

紀文倩，李舟軍，巢文涵，陳小明
北京航空航天大學計算機學院 北京 100191

摘　要：計算句子的相似度在自動問答、機器翻譯、信息檢索和自動文摘等系統中有著非常重要的作用。本文首先歸納了句子相似度計算的方法，提出了一種新的句子相似度計算方法，綜合考慮了關鍵詞特徵、語義特徵、句式特徵和句子長度特徵等信息。並以此為基礎，實現了一個基於 LexRank 算法的自動文摘系統，同時對句子權重計算方法以及冗餘處理等方面進行了改進。我們實現的文摘系統，可以對中文或英文的單文本或多文本進行自動文摘。通過在哈工大和 DUC 的測評語料上進行實驗，測試結果表明該系統在一定程度上改進了文摘的質量，在多文本文摘中的抗噪聲方面也有一定的優越性。最後，文章討論了自動摘要研究存在的問題，並指出自動文摘的研究趨勢。

關鍵詞：句子相似度，自動文摘，LexRank，句子權重計算，冗餘處理

1. 引 言

在自然語言處理領域，句子相似度計算是一項基礎而核心的研究課題，長期以來一直是人們研究的一個熱點和難點。句子相似度的計算在自然語言處理的各個領域都有著非常重要的作用，在基於實例的機器翻譯中，相似度主要用於衡量文本中詞語的可替換程度[1]；在資訊檢索中，相似度更多的是反映文本與用戶查詢在意義上的符合程度；在自動問答中，相似度反映的是句子之間語義上的匹配程度；而在多文檔文摘系統中，相似度可以反映出局部主題資訊的擬合程度[2]。

自動文摘是隨著互聯網上的資訊急劇膨脹而發展起來的文本資訊處理技術，它利用電腦自動地從文本或文本集合中提煉出能準確、全面地反映文本主要內容的精簡、連貫的短文[10]，以滿足用戶快速獲取知

Copyright © 2009 SciRes

識的要求。

本文給出了一種計算句子相似度的新方法，並給出了該方法在自動文摘系統中的應用，設計並實現了一種基於 LexRank 的改進的自動文摘系統。

2. 句子相似度計算方法

在自然語言處理的許多領域，句子相似度計算是一項應用廣泛的技術，並發揮著重要作用。隨著這些領域的發展，句子相似度計算也誕生了很多方法。不同方法很大程度上依賴於句子的不同表示形式[3]。目前研究句子相似度的方法有基於關鍵字的方法，使用語義詞典的方法[4]，使用語義依存的方法[5]，計算編輯距離的方法[6]，基於預警框架的方法[7]，基於屬性論的方法[8]以及基於統計的方法[9]等。

2.1 基於句子不同特徵的相似度計算

通過對句子的深入分析，句子相似度計算歸結起來可以概括為三類方法：基於詞特徵的句子相似度計算，基於語義特徵的句子相似度計算以及基於句法分析特徵的句子相似度計算。

2.1.1 基於詞特徵的句子相似度計算

基於關鍵字特徵的句子相似度的計算通常採用基於向量空間模型的方法。文本中每個句子表示成一個 n 維向量 V=(d_1,d_2,…,d_n)，d_i 是對應單詞的 tf*idf 值；句子之間的相似度就等於對應向量的 Cosine 值。設兩個句子 A 和 B，它們所有有效詞構成向量空間為 $V=\{X_1,X_2,X_3,...,X_n\}$，句子 A 對應的向量為 $V_1=\{w_1,w_2,w_3,...,w_n\}$,其中 w_i 為句子 A 中有效詞 X_i 的 TF*IDF 值；同樣的句子 B 對應的向量為 $V_2=\{\varphi_1,\varphi_2,\varphi_3,...,\varphi_n\}$，其中 φ_i 為句子 B 中有效詞 X_i 的 TF*IDF 值。則兩個句子的相似度為：

$$Similarity(A,B)=\frac{\sum_{i=1}^{n} w_i * \varphi_i}{\sqrt{\sum_{i=1}^{n} {w_i}^2} * \sqrt{\sum_{i=1}^{n} {\varphi_i}^2}} \quad (1)$$

這種方法只是單獨地考慮了句子的物理特徵，沒有考慮句式特徵、句子長度以及語義特徵，因此具有一定的局限性。

本文工作得到國家自然科學基金項目(60573057)資助

2.1.2 基於語義特徵的句子相似度計算

基於語義特徵的句子相似度計算，需要一定的語義知識庫作為基礎，中文常採用 HowNet 或《同義詞詞林》，英文一般採用 WordNet。通過詞與詞之間的語義相似度，計算句子間的語義相似度。設兩個句子 A 和 B，設 A 包含關鍵字為 x_1，x_2，□，x_m，句子 B 包含的詞為 y_1，y_2，□，y_n。詞 $x_i(1\le i\le m)$和 $y_i(1\le j\le n)$之間的相似度用 $s(x_i,y_j)$ 來表示，這樣我們得到一個語義相似度矩陣：

$$X=\begin{bmatrix} s(x_1,y_1),s(x_1,y_2),\Lambda,s(x_1,y_n) \\ s(x_2,y_1),s(x_2,y_2),\Lambda,s(x2,y_n) \\ ..... \\ s(x_m,y_1),s(x_m,y_2),\Lambda,s(x_m,y_n) \end{bmatrix} \quad (2)$$

則 A，B 句子之間的語義相似度為：

$$Similarity(A,B)=\frac{1}{2}*(\frac{\sum_{i=1}^{m} a_i}{m}+\frac{\sum_{i=1}^{n} b_i}{n}) \quad (3)$$

其中 $a_i=\max(s(x_i,y_1),s(x_i,y_2),\dots,s(x_i,y_n))$，$b_i=\max(s(y_i,x_1),s(y_i,x_2),\dots,s(y_i,x_m))$。這種方法充分考慮了句子中每個詞的深層語義資訊，使得表面不同，深層意義相同的詞被挖掘出來，而基於關鍵字特徵的相似度計算就不可識別這類資訊。但是由於詞典的不全面和一些未登錄詞的詞義代碼的缺失，也給計算帶來一定的誤差，另外這種方法也沒有考慮結構資訊。

2.1.3 基於句法分析特徵的句子相似度計算

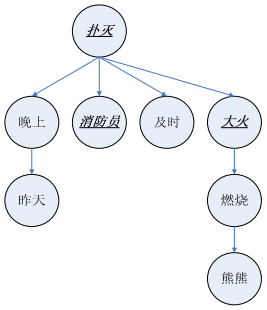
基於句子句法特徵的句子相似度計算需要考慮句子的句法結構資訊。一個完整的句子是由句子的主幹成分和修飾成分所構成，人們往往從主幹成分就可以瞭解句子的主要意思，所以在利用依存結構進行相似度計算時，只考慮那些有效搭配對之間的相似程度。有效搭配對是指全句核心詞和直接依附於它的有效片語成的搭配對，這裏有效詞定義為動詞、名詞和形容詞。全句核心詞為依存樹的根節點。例如下麵兩個句子：

例句 1　昨天晚上，消防隊員及時撲滅了熊熊燃燒的大火。

例句 2　晚上 11 點左右，熊熊燃燒的大火才徹底熄滅。

上圖中標記為斜體的詞代表了句子的主要意思，

Copyright © 2009 SciRes



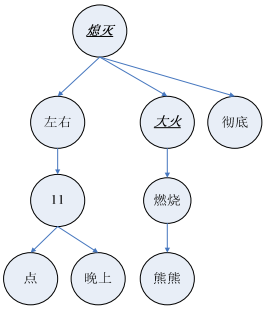


圖 1. 例句 1 的依存樹 **圖 2. 例句 2 的依存樹**

Figure 1. The dependency structure of example sentence 1

Figure 2. The dependency structure of example sentence 2

即句子 1 的有效搭配對為: 撲滅_消防員、撲滅_大火; 句子 2 的有效搭配對為: 熄滅_大火。兩個句子之間的相似度計算方法為:

$$Similarity(A,B)=\frac{Match(PairCount)}{\text{Max}\{PairCount_1,PairCount_2\}} \quad (4)$$

其中，$Match(PairCount)$ 為句子 1 和 2 有效搭配對的匹配數，$PairCount_1$ 為句子 1 的有效搭配對數，$PairCount_2$ 為句子 2 的有效搭配對數。

這種方法從句法深度進行考慮，考慮到了詞與詞之間的依存關係，對句子的理解更加充分，從而更準確的得到句子的相似度。但是，現有的句法分析技術還不夠成熟，無法將所有句法資訊特徵全部考慮進去，所以就產生了一定的誤差。

2.2 改進的句子相似度計算

由上一部分可知: 基於關鍵字特徵的方法體現了句子的表面資訊，基於語義特徵的方法考慮了組成句子的每個詞的深層的語義資訊，基於句法特徵的方法結合了詞與詞之間的依存關係。我們將關鍵字特徵和語義特徵相結合，同時引入句式特徵、句長特徵的影響，從而對句子相似度計算方法進行了改進。

向量空間模型（VSM）中，所有句子的關鍵字個數為 N，它們所有有效詞構成向量空間為 $V=\{X_1,X_2,X_3,...,X_n\}$。

首先，擴展向量空間到 N+1 維，第 N+1 維為 0 或 1 表示句子的句式特徵，當該句為肯定句時為 1，否定句為 0。

其次，考慮句子的關鍵字特徵，設句子 A 對應的向量為 $V_1=\{w_1,w_2,w_3,...,w_n,\ w_{n+1}\}$，其中 w_i (1≤i≤n) 為句子 A 中有效詞 X_i 的 TF*IDF 值；同樣的句子 B 對應的向量為 $V_2=\{\varphi_1,\varphi_2,\varphi_3,...,\varphi_n,\ \varphi_{n+1}\}$，其中 φ_i (1≤i≤n)為句子 B 中有效詞 X_i 的 TF*IDF 值。

然後考慮句子語義特徵，如 2.12 章所述，通過計算詞與詞之間的語義相似度，得到語義相似度矩陣，如公式(2)所示。根據句子的關鍵字特徵和語義特徵，我們可以得到句子 A 和 B 的語義相似度:

$$SemSim(A,B)=\frac{\sum_{i=1}^{n} w_i * a_i}{\sum_{i=1}^{n} w_i}+\frac{\sum_{i=1}^{n} \varphi_i * b_i}{\sum_{i=1}^{n} \varphi_i} \quad (5)$$

其中 $a_i=\max(s(x_i,y_1),s(x_i,y_2),\dots,s(x_i,y_n))$，$b_i=\max(s(y_i,x_1),s(y_i,x_2),\dots,s(y_i,x_n))$。

再次，我們考慮句子的長度相似性，通過公式(6)計算得到:

$$LenSim(A,B)=1-\left|\frac{Length(A)-Length(B)}{Length(A)+Length(B)}\right| \quad (6)$$

因此，最後的句子相似度計算公式為:

$$Sim(A,B)=(w_{n+1}\otimes\varphi_{n+1})*(\alpha*SemSim(A,B)+\beta*LenSim(A,B)) \quad (7)$$

其中，w_{n+1} 和 φ_{n+1} 表示句子 A 和 B 的句式特徵，當 w_{n+1} 和 φ_{n+1} 不同時 $(w_{n+1}\otimes\varphi_{n+1})$ 結果為 0，當二者相同時則等於 1。

這樣在句子相似度的計算中，不僅考慮了詞語的出現的頻率、句子長度等物理特徵，還考慮了詞語之間的語義關係。因此，計算得到的相似度更具合理性。

3. 自動文摘系統

自動文摘的研究始於 1958 年，由美國 IBM 公司的 Luhn 開創了自動摘要研究的先河[10],接著馬裏蘭州大學的 Edmundson[11][12]、美國俄亥俄州立大學的 Rush[13]、英國蘭開斯特大學的 Paice 等[14]選取字詞的不同特徵作為提取摘要的關鍵。隨後，有的學者開始引入文檔的結構特徵和語義特徵。美國耶魯大學的 Schank[15]、以及 GE 開發中心的 Rau 等[16]通過分析和推理得到文檔的摘要。Sasha Blair-Goldensohm 等提出了 SC 演算法[17]，其核心思想是: 包含越多句子的類的代表句子就越重要。因此，首先將句子聚類，根

Copyright © 2009 SciRes

據每個類中的句子數目決定類的重要度，抽取重要的類的代表句子作為文摘。

我國對自動文摘的研究起步較晚，中文文摘系統的研究在 20 世紀 90 年代才發展起來。上海交通大學 1997 年研製了 OA 中文文獻自動摘要系統[27]。該系統集成了位置法、指示短語法、關鍵字法和標題法等多種方法；復旦大學提出了一種基於統計的文本自動綜述方法，該方法利用文檔內和文檔之間段落的語義相關性，實現多文檔的自動綜述[25]；哈爾濱工業大學從各級文本單元的話語關係研究入手,研究跨文本單元的相似關係識別、文本時間資訊抽取以及事件的時序關係識別、文本內部修辭結構識別以及文本集合的層次主題的識別等, 並提出了基於修辭結構理論的多文檔文摘方法[26][28]。此外，還有很多大學和研究機構都取得了許多重要理論成果，實現了一批應用系統。

3.1 LexRank 演算法

自動文摘是通過選取原始文本中一組最重要的句子實現的。這裏如何定量地評定句子的重要度（本文中稱為權重）成為文摘選取的關鍵。密西根大學的 Gunes Erkan 和 Dragomir R Radev 提出的 LexRank 演算法[18]是一種在句子的圖形表示下計算句子權重的方法，他們認為如果一個句子與很多其他句子相似，那麼這個句子就是比較重要的。

首先把給定的文檔分句，並計算句子之間的相似度，如果兩個句子之間的相似度大於給定的閾值，就認為這兩個句子語義相關並將它們連接起來。按照這種方法，可以得到一個無向圖 $G=(S,E)$，圖中的每個節點 $s\in S$ 對應一個句子，而邊 $(s_i,s_j)\in E$ 表示句子 s_i 與 s_j 是相關的。節點 s 的度 d 是與 s 相連的邊的數目, 反映了其所對應句子所包含資訊的重要程度: d 越大，則對應句子所關聯的句子數目越多，那麼這個句子所包含的資訊越重要；反之亦成立。另一方面，如果一個節點的度比較大, 那麼與之相關聯的句子也相應的比較重要。這樣通過計算句子間的相似度構建圖 G，然後根據句子間的連接迭代計算句子所包含的信息量，再從中選取包含信息量最多的一組句子作為文摘。

在這個過程中我們發現，句子相似度計算的好壞對最後結果有較大的影響。原有演算法是根據句子的關鍵字特徵來計算相似度的，我們使用上文中改進的相似度計算方法，加入了語義和句子長度、句式特徵等資訊。同時，我們在計算句子權重時不僅考慮了句子通過 LexRank 得到的結果，而且加入了句子位置、指示性短語、句子長度等多個特徵；對於多文本文摘冗餘的問題也做了相關的改進工作。

3.2 改進的自動文摘系統

上一部分中已經介紹了 LexRank 演算法的核心思想，下面將介紹我們的自動文摘系統，其中將對句子權重計算方法以及去冗餘處理模組進行詳細講述。系統是在向量空間模型(Vector Space Model, VSM)上實現的，其基本流程如圖 3 所示。包含以下六個步驟：

1）預處理：將輸入的文本或文本集的內容切分成句子並標號，對不可能成為文摘句的疑問句、反問句等進行句子過濾，分詞、去除停用詞；

2）計算句子的相似度，得到句子的相似度矩陣；

3）計算句子的權重：其中將結合 LexRank 及其它特徵。

4）根據句子的權重抽取句子，並去除冗餘；

5）轉到 4）直到抽取的句子數目滿足條件；

6）結合專家文摘對文摘結果進行評測。

3.2.1 句子權重的計算

得到句子的相似度矩陣之後，通過 LexRank 演算法可以計算得到句子的權重，我們記作 LexRankSco- re。但是這樣得到的權重沒有涉及到句子位置、指示性短語等相關資訊。我們的權重計算過程如圖 4 所示。

句子位置對文摘結果有一定的影響，據統計每段首句所包含的信息量較大。我們用 PositionScore 表示句子位置的加分，如果句子 i 不是首句，PositionScore 等於 0。

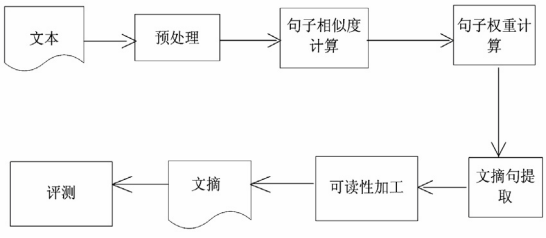


圖 3. 文摘的自動抽取流程圖

Figure 3. The workflow diagram of automatic abstracting

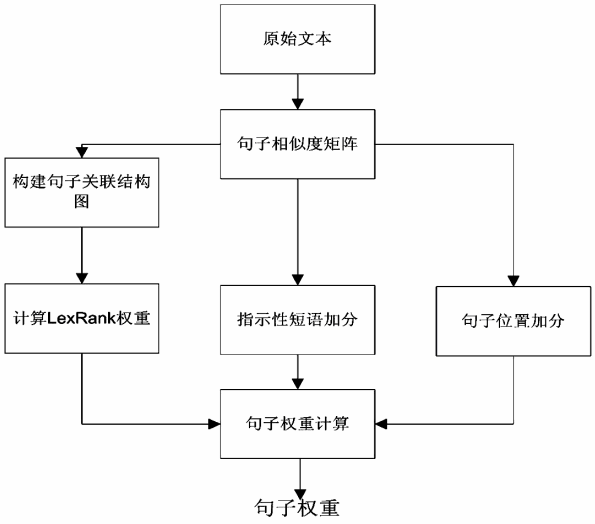


圖 4. 句子權重計算圖

Figure 4. The workflow for computing sentence-weight

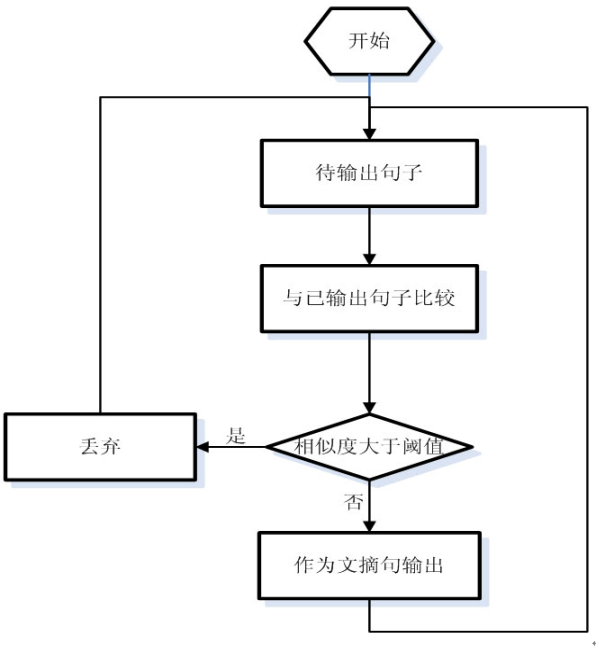


圖 5. 冗餘處理流程圖

Figure 5. The workflow for redundancy resolution

文章中常常有一些特殊的指示性短語(例如 in this paper…the purpose of the article…等), 它們對文章主題具有明顯的提示作用，可以利用它們來獲取文章的主題資訊。我們使用 InforScore 表示指示性短語所在的句子的加分，如果句子 i 中不包含指示性短語，其對應的 InforScore 等於 0。

綜上計算得到三個結果之後，我們使用使用公式(8)計算句子的權重 q_i。

$$q_i = LexRankScore + PositionScore + InforScore \quad \textbf{(8)}$$

3.2.2 冗餘處理

在自動文摘過程中，如果被抽取的句子意思相同，會影響最後的文摘所包含的信息量，這就是我們所說的冗餘問題。在多文本文摘中冗餘的消除是影響文摘結果的一個重要方面. 我們消除冗餘的步驟如下:

1） 根據句子權重計算結果，對句子的重要度由高到低排序，得到候選的句子列表 $S = \{s_1, s_2, \ldots, s_n\}$，文摘集合 A 為空。

2） 權重最大的 s_i 作為文摘輸出，$A = \{s_i\}$，$S = S - \{s_i\}$；

3） 依次選舉 S 中的 s_i ($i \geq 2$), 如果 s_i 與 A 中所有句子的相似度小於等於設定的閾值 threshold，$A = A + s_i$；否則丟棄 s_i；

4） 迴圈步驟 3, 直到抽取的句子數到達一定長度。

4. 實驗

系統可以處理中文（英文）的單文本（多文本）文摘。由於測評語料的限制，我們的實驗分為三個部分，第一部分是中文單文本文摘，包括語料庫的建設和結果測評；第二部分實驗是借助於 2004 年 DUC 英文多文本文摘的測評語料進行的；第三部分主要是針對系統的抗雜訊能力進行測評。測評採用的是 2004 年 DUC 採用的 ROUGE 方法。

4.1 ROUGE 方法

ROUGE 是由 Chin-Yew Lin 等人提出的自動文摘評價方法[19]，它是通過電腦器產生的文摘和專家文摘間重疊的單詞數目來評價文摘品質的。DUC2004 採用了三種 ROUGE 評價方法，分別是 ROUGE-N，ROUGE-L，ROUGE-W[20]。ROUGE-N 計算的是機器摘要與一組人工摘要中 n-gram 的 Recall 值, 它的計算公式如下：

$$\text{ROUGE-N} = \frac{\sum_{s \subset (modelSummaries)} \sum_{gram_n \subset s} Count(Match(gram_n))}{\sum_{s \subset (modelSummaries)} \sum_{gram_n \subset s} Count(gram_n)} \quad \textbf{(9)}$$

Copyright © 2009 SciRes

其中，n 代表 n-gram 的長度，$Match(gram_n)$表示同時出現在系統文摘和專家文摘中的 n-gram 的數目。ROUGE-L 是根據最長公共子序列來電腦器文摘和人工文摘的相似程度，而 ROUGE-W 是帶權重的最長公共子序列。這兩個評價方法的計算都比較複雜，在此不做贅述。

4.2 中文單文本文摘測評

我們使用的是哈爾濱工業大學的《哈工大資訊檢索研究室單文檔自動文摘語料庫》。包含語料共計 211 篇，分為不同體裁。其中各體裁文章數為：奧運，57 篇；記敍文，40 篇；說明文，40 篇；議論文，46 篇；應用文，18 篇；03 年 863 評測語料，10 篇。並由 5 個人分別人工按照原文 10%以及 20%文摘句。

我們依照 2004 年 DUC 的測評方法，將這五個人人工標注的 10%句子和 20%句子分詞後分別作為 10%專家文摘和 20%專家文摘。將我們系統生成的文摘與專家文摘使用 ROUGE-N 方法測評，這裏的 n-gram 是以中文分詞後的單個詞語為單位。表 1 給出了使用詞特徵的句子相似度計算方法、使用語義特徵的句子相似度計算方法和我們改進後句子相似度計算方法對文摘結果影響的比較。結果表明改進的句子相似度計算方法使得生成的文摘品質有一定的提高。

4.3 英文多文本文摘測評

我們採用的是 DUC 2004 年的多文本測評語料。DUC 提供了五十個 TDT 英文文本集，每個文本集包含十篇同一話題的文章。要求每個文本集自動生成不超過 665 位元組的文摘。並提供了專家文摘，採用 ROUGE 方法對文摘進行評價。表 2 給出了使用詞特徵的句子相似度計算方法、使用語義特徵的句子相似度計算方法和我們改進後句子相似度計算方法對文摘結果影響的比較。

同樣，我們可以看到，使用了改進的句子相似度計算方法的系統生成的文摘品質要好於單純使用詞特徵的句子相似度計算方法或使用語義特徵的句子相似度計算方法。測評結果表明 ROUGE-1 分別提高了 9.5%、6.8%，ROUGE-2 分別提高了 16.3%、12.5%，文摘品質有了一定的提高。

表 1. 中文單文本語料測評結果

Table 1. The evaluation results on Chinese single-document corpus

	10%壓縮率		20%壓縮率	
句子相似度計算方法	ROUGE-1	ROUGE-2	ROUGE-1	ROUGE-2
TF*IDF	0.2898	0.1557	0.4011	0.2235
語義特徵	0.3184	0.1703	0.4076	0.2219
改進後的方法	0.3404	0.2057	0.4668	0.2835

4.4 抗雜訊能力測評

當處理多文本文摘時，LexRank 把所有文本看作一個整體，句子重要性的判斷是根據所有文章內容，而不是局部某一篇文章。所以 LexRank 方法對雜訊資料不敏感。我們的系統由於結合了 LexRank 演算法，在多文本文摘的抗雜訊方面有著一定的優越性。

為了觀察結果，我們對 DUC2004 年的多文本測評語料庫進行了兩種修改：第一種，每個文本集的十篇文章中我們刪除其中一篇文章，再加入一篇與該主題不相關的文章，雜訊資料為 1/10=10%；第二種，在每個文本集中加入兩篇不相關的文章，雜訊為 2/12=16.7%。實驗結果如表 3 所示，結果表明兩種情況下，文摘品質都沒有明顯下降。

5. 結束語

本文介紹了句子相似度計算的幾種方法，並根據其不足提出了一種新的句子相似度計算方法，綜合考慮了句子的關鍵字特徵、語義特徵、句式特徵和句子長度特徵等資訊。在此基礎上實現了一個基於 LexRank 演算法的自動文摘系統，並從句子權重計算

表 2. 英文多文本語料測評結果比較

Table 2. The evaluation results on English multi-document corpus

句子相似度計算方法	ROUGE-1	ROUGE-2
TF*IDF	0.3433	0.0814
語義特徵	0.3521	0.0842
改進後的方法	0.3759	0.0947

表 3. 加入噪聲數據後文摘的測評結果

Table 3. The evaluation results on English multi-document corpus with certain percent of noisy data

語料庫	ROUGE-1			ROUGE-2		
噪聲數據	min	max	average	min	max	average
無	0.3213	0.4245	0.3759	0.0511	0.1465	0.0947
10%	0.3078	0.4164	0.3677	0.0504	0.1367	0.0903
16..7%	0.2747	0.4049	0.3465	0.0487	0.1198	0.0843

Copyright © 2009 SciRes

和冗餘處理等方面進行了改進。該系統可以對中文或英文的單文本或多文本進行自動文摘，通過在哈工大和 DUC 的測評語料上進行實驗，測試結果表明該系統在一定程度上改進了文摘的品質，在多文本文摘中的抗雜訊方面也有一定的優越性。

但是，對於多文本文摘，文摘句輸出順序問題仍沒有解決；而且實際上句子作為文摘的最小單元不是最理想的。這是由於有時在一個句子中還會包含冗餘資訊，有時一個句子表達的意思還不夠完整。於是有人提出了對句子進行壓縮和融合[23]，就是通過句法分析和統計的方法，對句子進行裁剪，使文摘更加精煉。

中文自動文摘由於缺乏大規模統一的測評語料以及測試平臺，不利於它的研究和發展。隨著更多的中文自然語言資源庫的健全和開放，中文句法分析和等自然語言處理技術的成熟，中文自動文摘會有更大的發展。

REFERENCES

[1] Hu Guo-Quan, Chen Jia-Jun, Dai Xin-Yu. A Examle-based Chinese-English Machine Translation Strategy [J]. Computer Engineering and Design, 2005, 26(4): 900-903. (in Chinese) (胡國全, 陳家俊, 戴新宇. 一種基於實例的漢英機器翻譯策略[J]. 電腦工程與設計, 2005, 26(4): 900-903.)

[2] Zhang Qi, Huang Xuan-Jing, Wu Li-De. A New Method for Computing Similarity between Sentences and Application on Automatic Text Summarization [J]. Journal of Chinese Information Processing. 2005, 19(2): 93-99.(in Chinese) (張奇, 黃萱菁, 吳立德. 一種新的句子相似度度量及其在文本自動摘要中的應用[J]. 中文資訊學報, 2005, 19(2): 93-99.)

[3] K. Chidananda Gowda, E. Diday. Symbolic Clustering Using a New Similarity Measure[J]. IEEE Transactions on System, Man and Cybernetic, 1992, 22(2).

[4] Li S, Zhang J. Journal of Computer Science and Technology, 2008, 17(6): 933-939.

[5] Wei Zhi-Fang, Yu Shi-Wen. A Dependency-based Model for Sentence Similarity Computing [C]. ICCIP'98, 1998. (in Chinese) (魏志方, 俞士汶. 基於骨架依存樹的句子相似度計算模型[C]. 中文資訊處理國際會議. (ICCIP'98), 1998.)

[6] Che Wan-Xiang. Similar Chinese Sentence Retrieval based on Improved Edit-Distance [J]. Chinese High Technology Letters. 2004. (In Chinese) (車萬翔等. 基於改進編輯距離的中文相似度句子檢索[J]. 高技術通訊. 2004.)

[7] Jin Yao-Hong. Text Similarity Computing Based on Context Framework Model [J]. Computer Engineering and Application. 2006(16). (In Chinese) (晉耀紅等. 基於語境框架的文本相似度計算[J]. 電腦工程與應用. 2006(16).)

[8] Pan Qian-Hong. Text Similarity Computing based on Attribute Theory [J]. Chinese Journal of Computer. 1999: 22(6). (In Chinese) (潘謙紅等. 基於屬性論的文本相似度計算[J]. 電腦學報. 1999: 22(6).)

[9] Chatterjee N. A Statistical approach for similarity measurement between sentences for EBMT. 1999.

[10] Luhn H P. The Automatic Creation of Literature Abstracts [J]. IBM Journal of Research and Development, 1958: 159-165.

[11] Edmundson, Wyllys. Automatic Abstracting and Indexing: Survey and Recommendations. Communication of the ACM, 1961, 4(5): 226-234.

[12] Edmundson. New methods in automatic abstracting [J]. Journal of the Association for Computing Machinery, 1996, 16(2): 264-285.

[13] Pollock J J, Zamora A. Automatic Abstracting Research at Chemical Abstracts Service [J]. Journal of Chemical Information and Computer Sciences, 1975, 15(4): 226-232.

[14] Paice C D. The Automatic Generation of Literature Abstracts: An Approach Based on the Identification of Self-Indicating Phrases. Information Retrieval Research.

[15] Schank C, Abelson P. Scripts, Plans, Goals, and Understanding: An Inquiry into Human Knowledge Structures [J]. Lawrence Erlbaum Associates, Hillsdale, New Jersey, 1977.

[16] Lisa F Rau, Jacobs P S. SCISOR: Extracting Information Online News[J]. Communication of the ACM, 1990, 33(11): 88-97.

[17] S Blair-Goldensohn. Columbia University at DUC 2004[C]. In DUC '04, 2004.

[18] Gunes Erkan, Dragomir R Radev. LexRank: Graph-Based Centrality as Salience in Text Summarization [J]. Journal of Artificial Intelligence Research 22(2004), 12/2004.

[19] Lin, Chin-Yew, E. H. Hovy. Automatic Evaluation of Summaries Using N-gram Co-occurrence Statistics [J]. In Proceedings of 2003 Language Technology Conference (HLT-NAACL 2003), Canada, 2003.

[20] Zajic, David, Bonnie Dorr, Richard Schwartz. BBN/UMD at DUC-2004: Topiary. In Proceedings of the Fourth Document Understanding Conference (DUC '04), 2004: 112-119.

[21] Huang Li-Qiong. Research on Chinese Automatic Summarization and Its Evaluation Method [D]. Chongqing University, 2007. (In Chinese) (黃麗瓊. 中文自動文摘及評價方法的研究[D]. 重慶大學, 2007).

[22] Chin-Yew Lin, Eduard Hovy. The Potential and Limitations of Automatic Sentence Extraction for Summarization [J]. University of Southern California, 2008: 73-80.

[23] Lin, C. Y. Improving summarization performance by sentence compression: A pilot study[C]. In Proceedings of the Sixth International Workshop on Information Retrieval with Asian Languages. 2003: 1-9.

[24] Qin Bing, Liu Ting, Li Sheng. Summarization Based on Physical Features and Logical Structure of Multi Documents[J]. High Technology Letters, 2005, 11(2): 133-136.

[25] Zheng Yi, Huang Xuan-Jing, Wu Li-De. Research and Implementation of Automatic Multi-Document Summarization System [J]. Journal of Computer Research and Development. 2003, 40(11): 107-110. (In Chinese) (鄭義，黃萱菁，吳立德. 文本自

Copyright © 2009 SciRes

動綜述系統的研究與實現[J]. 電腦研究與發展. 2003, 40(11): 107-110.)

[26] Xu Yong-Dong. Research on Key Technology of Multiple Documents Automatic Summarization [D]. Harbin Institute of Technology, 2007. (In Chinese) (徐永東. 多文檔自動文摘關鍵技術研究[D]. 哈爾濱工業大學, 2007.)

[27] Wang Yong-Cheng, Xu Hui-Min. OA Automatic Abstracting System on Chinese Documents [J]. Journal of the China Society for Scientific and Technical Information, 1997, 16(2): 128-132. (In Chinese) (王永成, 許慧敏. OA 中文文獻自動摘要系統[J]. 情報學報, 1997, 16(2): 128-132.)

[28] Xu Yong-Dong, Xu Zhi-Ming, Wang Xiao-Long. Multi-Document Automatic Summarization Technique based on Information Fusion [J]. Chinese Journal of Computers, 2007, 30(11): 2049-2054. (In Chinese) (徐永東, 徐志明, 王曉龍. 基於資訊融合的多文檔自動文摘技術[J]. 電腦學報, 2007, 30(11): 2049-2054.)

[29] Wang Ji-Cheng, Wu Gang-Shan, Zhou Yuan-Yuan, Zhang Yan-Fu. Research on Automatic Summarization of Web Document Guided by Discourse [J]. Journal of Computer Research and Development. 2003, 40(3): 398-405. (In Chinese) (王繼成, 武港山, 周源遠, 張福炎. 一種篇章結構指導的中文 Web 文檔自動摘要方法[J]. 電腦研究與發展. 2003, 40(3): 398-405.)

[30] Wang Meng. Research of Chinese Text Automatic Summarization Based on Conceptual Vector Space Model [D]. Department of Computer Science Central China Normal University, 2005. (In Chinese) (王萌. 基於向量空間模型的中文自動文摘研究[D]. 華中師範大學, 2005.)

[31] Xiaohua Zhou, Xiaodan Zhang, Xiaohua Hu. Dragon Toolkit: Incorporating Auto-learned Semantic Knowledge into Large-Scale Text Retrieval and Mining [C]. In proceedings of the 19th IEEE International Conference on Tools with Artificial Intelligence (ICTAI). 2007: 29-31.

Copyright © 2009 SciRes

Intelligent Information Management, 2009, 46-53
doi:10.4236/iim.2009.11008 Published Online July 2009 (http://www.scirp.org/journal/iim)

Application of a Sign Language Synthesis System in Digital Library Services

Jing WAN, Bin WU, Yingxin QIAO
Department of Computer and Network Systems, National Library of China, Beijing, 100081

Abstract: Information Accessibility for disabled people is one of the most important design criteria for the China National Digital Library (CNDL) development. Sign language synthesis systems are effective to provide information services for people with hearing and speech impairments. This paper presents a framework of a sign language synthesis system application in CNDL, as well as discusses the relevant technologies applied in the system. CNDL has been a real practice area for the sign language synthesis research.

Keywords: sign language synthesis, digital library, on-line seminar, sign language presentation

淺析手語系統在數字圖書館中的應用

萬　靜，吳　斌，喬穎欣

國家圖書館計算機與網絡系統部 北京 100081

摘　要：為殘疾人服務是國家數字圖書館建設的一個重要組成部分。其中，手語合成系統的應用將為聽力和語音障礙者（聾啞讀者）瀏覽數字圖書館資源（特別是在線講座等）提供信息無障礙的服務。本文論述了該手語合成系統的總體架構和採用的相關技術。國家數字圖書館的在線講座服務將是手語合成系統的一個重要的應用領域和實踐。

關鍵詞：手語合成，數字圖書館，講座，三維手語顯示

1. 背景簡介

為廣大殘疾人服務是國家數位圖書館建設的一個重要組成部分。

通常，傳統圖書館服務所面對的殘疾人群體可以分為肢體殘疾（多指輪椅使用者）、視覺殘疾（盲人）和語音聽覺殘疾（聾啞人）三類。由於數位圖書館的許多內容都是通過互聯網和個人電腦來提供閱覽，對於肢體殘疾的讀者來說，在電腦操作和網路使用上，應該同健全讀者無異，而數位圖書館"足不出戶"的使用特性，正好為他們提供了巨大便利。因此，相對於傳統圖書館面向服務的三類殘疾人群，視覺殘疾（盲人）和語音聽覺殘疾（聾啞人）兩類殘疾人群則是數字圖書館的要重點關注的物件，需要配以特殊的技術輔助。

對於盲人讀者，國家數字圖書館已與 2008 年 10 月開通了"中國盲人數位圖書館"的門戶網站，採用了多種比較成熟的資訊無障礙技術，本著公益服務、資訊讀取無障礙、邊建設邊服務、資源特色化與共建共用的原則，提供了大量的數位圖書和音頻數位資源，服務于盲人。同時，社會上也有很多成熟的讀屏軟體可供盲人在使用電腦時理解螢幕資訊。

相比而言，可供聾啞人使用的資訊無障礙產品則相對匱乏，許多音視頻資源無法供聾啞人使用。雖然現在大多數的解決方案是提供相應的字幕，但聾啞人對可視文字的理解速度要比手語慢得多。經研究表

Copyright © 2009 SciRes

明，聾啞人對手語的理解速度和健全人對語音語言的理解速度是相當的，手語可以說是聾啞人的“聽力系統”[1]。手語更直觀更迅捷，它是聾啞人最重要的交流手段[2]。

國內一些學者對聾啞人適用的資訊無障礙的相關技術，比如視頻編碼與分析、手語識別與合成、人臉識別等，正在做一些研究，並取得了一定的成果。但這些技術成果還處於實驗室階段，缺乏具體的應用領域[3-5]。正在建設中的“國家數字圖書館”為此提供了一個應用平臺。目前，國家圖書館正在進行如何將手語合成技術應用到國家數位圖書館服務領域的研究和實踐。本文將簡要介紹這一手語合成系統的構建思路和技術實現。

2. 手語合成系統在數位圖書館中的應用

正在建設中的國家數字圖書館，遵循“邊建設便服務”的原則，至今已有豐富的數位資源上線服務。對於電子圖書、古代文獻、圖片等“無聲”的數位資源，聽力和語音障礙者（聾啞人）在使用上沒有障礙；而對於視頻影像資源，聽力和語音障礙者就有障礙，需要經過“字幕”等加工處理才能讓他們理解。

國家圖書館有大量的講座視頻資源，比如“文津講壇”、“文津圖書沙龍”等已成為國圖的講座品牌，幾乎每週都有講座舉辦，並連續 3 年將國內外著名專家學者的精華講座製作成多媒體數位檔並發佈，現在已經有 387 場、近 100GB 的數字講座得到授權，在互聯網上發佈。這是國家數位圖書館數位資源的重要組成部分。然而對於聾啞人讀者來說，目前講座現場不提供字幕和手語翻譯支援，在講座錄製加工後，仍有一部份講座沒有字幕，這使得聽力和語音障礙者無法欣賞講座的精彩內容，更無法親身參與到現場的互動活動。

為了改善對聾啞殘疾人讀者的服務，更好地幫助他們理解到講座的內容，我們希望通過採用手語合成的技術，對視頻講座配以手語畫面（效果圖如圖 1），

圖 1. 三維手語示例效果圖（主畫面是國家圖書館名譽館長任繼愈先生的講座《中國哲學的未來》的視頻，右上角的三維模擬人通過手語對講座的內容進行同步翻譯）。

Figure 1. A 3D effect of a sign language demonstration (the main picture is a lecture video of the honorary director of the National Library of China Ren Jiyu on “the future of Chinese philosophy”,the right corner above shows a 3D dummy man interpreting the lecture simultaneously).

Copyright © 2009 SciRes

無論聾啞人讀者即時參與講座還是後來觀看網路數位錄影，都能夠快速地理解講座內容，和正常人一樣，真正做到資訊無障礙。手語合成系統在國圖講座中的應用，將是國家數位圖書館為聾啞人提供服務的一個重要的應用領域，將極大地提高他們獲取資訊的自立能力。從理論上講，該手語合成系統，可擴展應用到數位圖書館的任何凡有交流性質的服務中，為廣大聾啞讀者提供便利。

3. 手語合成系統的構建

3.1 總體流程

手語合成系統的總體流程是系統根據語音輸入（即時或多媒體影像）進行語音識，轉換成文本資訊，然後自動把文本資訊翻譯成對應的手語資訊，並採用圖像技術，把手語逼真地展示出來。

手語合成系統的總體流程如圖 2，包括語音識別、文本到手語碼的轉換、手語運動資料的建立、手語動作的合成、三維手語的顯示等主要環節。

語音信號的來源可以是現場麥克風採集的聲音，或者現場錄製成多媒體資源中的音頻。音頻信號經過語音識別轉化為文本資訊，對這些文本資訊進行自動切分，得到文本對應的分詞序列，實現從文本到手語碼的轉換。手語運動資料庫記錄了每個手語詞的手語運動資訊，涵蓋了中國基本手語詞、同義手語詞、指拼手語詞等。手語碼經由手語運動資料庫的“翻譯”，合成手語動作。系統將手語動作以三維圖像的方式展示，且生成的手語圖像能夠被聽力語音障礙者便捷準確地閱讀和理解。

3.2 語音識別

語音識別是指將人類的語音中的詞彙內容轉換為計算機可讀的輸入[6]。對於視頻講座的語音識別，主要是把講座的音頻轉化為文本，為下一步手語碼轉換提供信息。音頻的來源有兩種方式，見圖 3、圖 4。

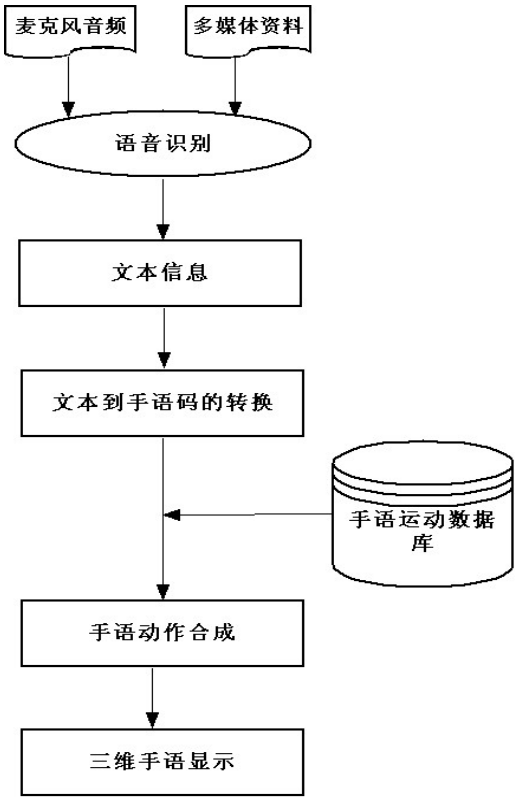


圖 2. 總體流程圖
Figure 2. Overall flow chart

Copyright © 2009 SciRes

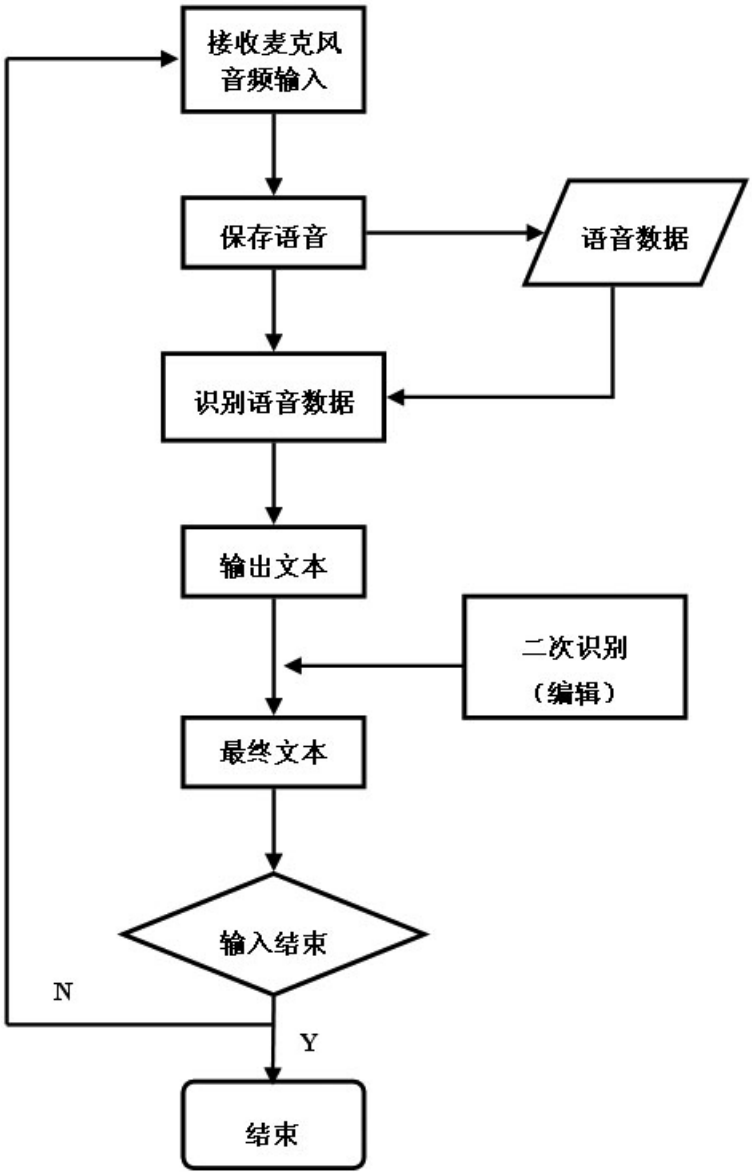


圖3. 即時語音識別的流程圖
Figure 3. A real time speech recognition flow chart

如圖 3 所示，說話人通過麥克風輸入語音，系統自動將當前聲音信號保存為語音數據，並對語音數據進行識別，實時輸出對應的文本。

語音識別是指將人類的語音中的辭彙內容轉換為電腦可讀的輸入[6]。對於視頻講座的語音識別，主要是把講座的音頻轉化為文本，為下一步手語碼轉換提供資訊。音頻的來源有兩種方式，見圖 3、圖 4。

如圖 3 所示，說話人通過麥克風輸入語音，系統自動將當前聲音信號保存為語音資料，並對語音資料進行識別，即時輸出對應的文本。

如圖4所示，系統輸入為多媒體資料檔，即視頻或音頻的編碼檔（視頻檔為Mpeg1/2/4和WMV格式，音頻為WAV/MP3格式），系統將檔解碼為原始語音資料，並將資料切分為若干小段，逐段進行語音識別，輸出對應的文本。

3.3 文本到手語碼的轉換

如圖5所示，文本句法分析到手語碼的轉換是手語合成中的關鍵環節，直接關係到手語內容的表意準確。中國手語是參考漢語制定的，但在基本詞彙、句子結

Copyright © 2009 SciRes

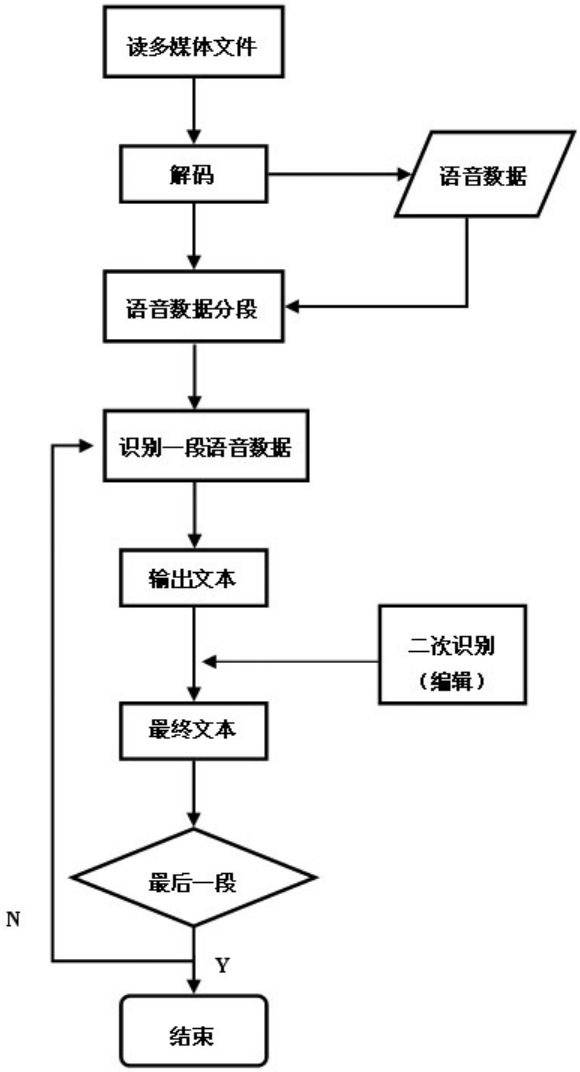


圖 4. 多媒體資料的語音識別流程圖
Figure 4. A multimedia speech recognition flow chart

構和構詞方法上有著明顯的區別。中國手語的辭彙由3330個手勢語組成，遠少於漢語十幾萬的辭彙量，手勢詞語與漢語的詞語不完全存在一一對應的關係。在句子結構和構詞方法上，手語句子的語序以主謂賓為主[7]，在一些時候與漢語句子的詞序有所不同。手語合成中的文本分析過程是在語音識別的漢語語句的基礎上，按照手語的規則提取和組合用來表意手語碼的辭彙，組成手語碼序列。

3.4 手語運動資料庫的建立

手語運動資料庫的建立流程如圖 6。手語運動資料庫記錄了每個手語詞的手語運動資訊，是手語合成的基礎。目前建立手語詞庫的方法有兩種：運動跟蹤方法[8][9]和手工編輯方法[10]。兩種方法各有利弊[3]，可以將這兩種方法結合，首先進行動作資料獲取，建立初始手語動作詞庫，然後對不準確的手語運動進行編輯修改。這樣可以獲得一個準確、逼真的手語詞庫，而且減少了工作量。

3.5 手語動作的合成

在經文本分析和手語運動資料檢索後，得到的手語符號序列中包含手語詞和手語運動參數，手語運動合成的目的是將這樣的符號序列轉換成手語動作。

如圖 7 所示，手語動作合成主要完成手語動作之

Copyright © 2009 SciRes

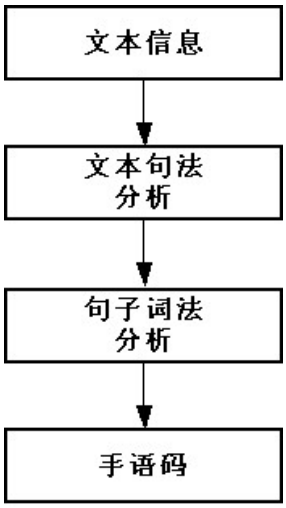


圖 5. 文本到手語碼轉換的流程圖
Figure 5. A text to sign language translation flow chart

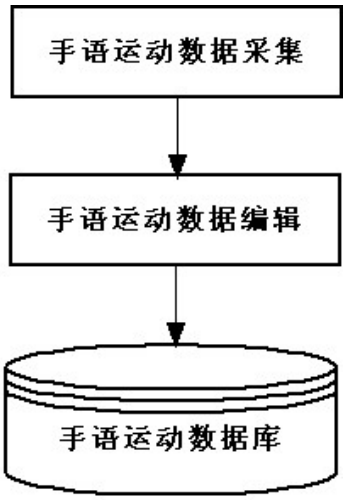


圖 6. 手語運動資料庫建立的流程圖
Figure 6. A hand signals database setup flow chart

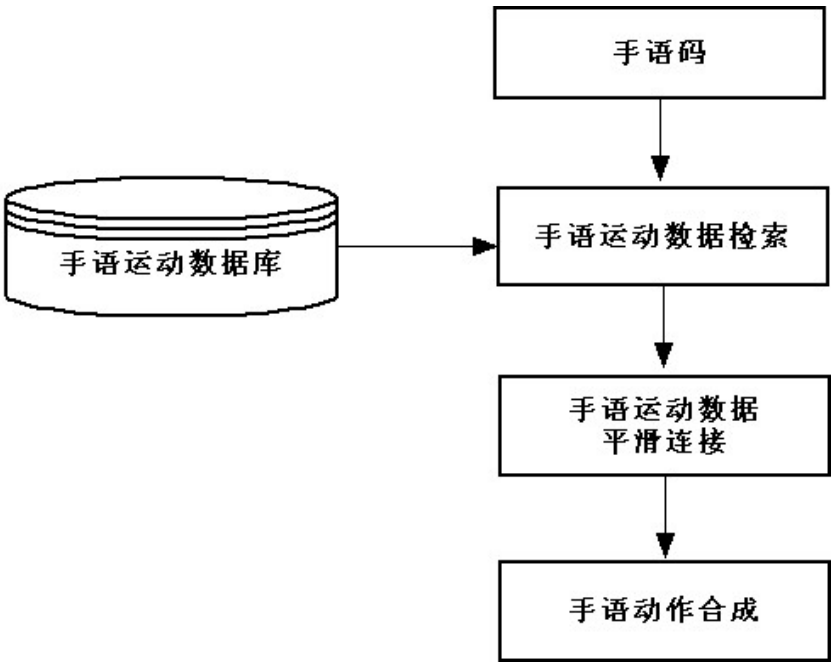


圖 7. 手語動作合成的流程圖
Figure 7. A hand signals synthesis flow chart

間的過渡和銜接，要求合成的手語運動序列具備連續性和平滑性，並要求不同的手語動作之間有較好的過渡動作。手語符號序列中的每個手語詞的手語運動資料可直接從手語詞運動資料庫中查詢得到，手語詞的錄製是完整且連貫的，因此其內部具有很好的運動逼真性和連續幀之間的運動相關性[3]。但，由於兩個連續的手語詞之間，前一個手語詞的最後一個手勢（最後一幀）與下一個手語詞的第一個手勢（第一幀）之間的差別是任意的，因此手語詞之間的平滑過渡則要更複雜。

3.6 三維手語的顯示

手語是一種人之間交流的可視語言，手語動作最終以三維虛擬人的動作展示給語音障礙者。

如圖 8 所示，系統能夠以三維的方式展示手語，

Copyright © 2009 SciRes

且生成的手語圖像能夠被聽力和語音障礙者便捷準確地進行閱讀和理解。一個手語運動是一個人體手勢的序列，按照預定的時間間隔連續顯示一個手語運動中的每一個手勢，既可以生成對應的手語運動。手語三維顯示實際上就是根據給定的手語運動表示，驅動虛擬人的上肢運動，以此顯示逼真的手語[4]。

三維手語的顯示除了要滿足手語顯示的連貫性和準確性要求，還要考慮檔傳輸的需求。對於線上講座直播的三維手語展示，希望能夠在互聯網上線上使用，一般三維動畫技術形成的圖像由於檔體積大，不適合網路應用。這就對可以使用三維動畫技術來實現手語動畫，但一般的三維動畫技術形成的圖像雖然可能滿足生動逼真的要求，卻不適合網路應用。Virtual Reality Modeling Language（VRML），是一種虛擬現實建模語言。它主要用於在 Internet 上表示並共用三維虛擬場景和虛擬物體[11]。在 VRML 中有一部分是專門用於描述三維人體模型 H-Anim 標準，根據此標準對虛擬人的定義，應用運動學的方法和電腦圖形學的方法就可以計算出虛擬人每個肢體的位置和方向，由此確定虛擬人的一個姿態，從而完成一系列動作[5]。

4. 結束語

本文論述了一個正在研究中的國家數位圖書館的手語合成系統。該系統通過手語合成技術對國家圖書館的線上講座、視頻資料、現場講座等數位視頻資源進行手語翻譯，並用三維虛擬人像手語展示，為廣大聾啞人做手語同步導視。這是手語系統的一個重要的應用領域和實踐，可以幫助有聽力和語音障礙的讀者和正常人一樣獲取國家數字圖書館的資源。

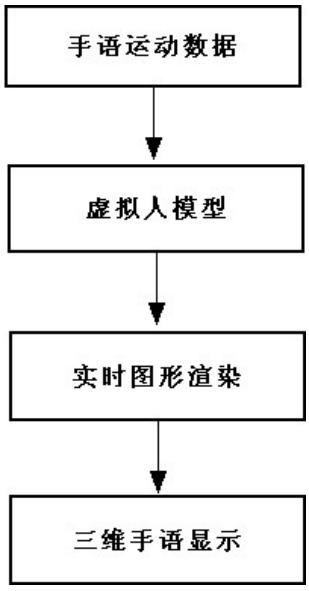


圖 8. 三維手語顯示的流程圖
Figure 8. A flow chart of sign language 3D display

5. 附錄：術語

聽覺和語音障礙者[1]：指那些由於疾病、傷害等各種原因導致聽力障礙和發音障礙的人，從而不能同一般人進行正常的話語交往活動，也即我們通常說的“聾啞人”。

語音識別：就是根據輸入的語音資料，系統自動地把語音翻譯成對應的文本。

手語合成：就是系統根據輸入的文本資訊，自動把文本資訊翻譯成對應的手語資訊，並採用圖形圖像技術，由電腦生成的虛擬人把手語逼真地展示出來。

REFERENCES

[1] Fu Yiting, Mei Cikai (1986). An Outline of Sign Language of the Deaf. (in Chinese) (付逸亭, 梅次開. 聾人手語概論. 學林出版社，1986.)

[2] China National Association of the Deaf (1988). Chinese Sign Language. (in Chinese) (中國聾人協會. 中國手語. 華夏出版社，1988.)

[3] Wang Zhaoqi, Gao Wenji (2002). The Synthesis Approches of Chinese Sign Language Based on Dummy Man Synthesis Technology, Journal of Software, 13(10), 2051-2056 (in Chinese) (王兆其, 高文基. 於虛擬人合成技術的中國手語合成方法. 軟件學報, 2002, 13(10), 2051-2056.)

[4] Wang Zhaoqi, Yang Changshui, Gao Wen (2003). 3D Display of Chinese Sign Language Based on VRML. Computer Study and Development. 40(3), 459-463. (in Chinese) (王兆其, 楊長水, 高文. 基於 VRML 的中國手語三維顯示 電腦研究與發展. 3/2003, 40(3), 459-463.)

[5] Gao Wei, Guo Jin, Zeng Peikai (2002). The Current Situation and Future Consideration of the Sign Language Research. Journal of IT Technology, 6-8. (in Chinese) (高偉, 郭瑾, 曾碚凱. 手語研究的方向與現狀. 電子技術應用, 11/2002, 6-8.)

[6] Wikipedia Editor : Speech Recognition 2009/06/02 23:08[2009/07/07.06:55] http://zh.wikipedia.org/w/index.php?title=E8%AF%AD%E9%9F%B3%E8%AF%86%E5%88%AB&oldid=10222296.) (in Chinese) (維琪百科編者. 語音識別[G/OL]. 維琪百科, 自由的百科全書, 2009 年 06 月 2 日 23:08 [2009 年 07 月 7 日 06:55]. http://zh.wikipedia.org/w/index.php?title=E8%AF%AD%E9%9F%B3%E8%AF%86%E5%88%AB&oldid=10222296.)

[7] Wikipedia Editor : Sign Language 2009/06/13 06:36[2009/07/02 06:32] http://zh.wikipedia.org/w/index.php?

Copyright © 2009 SciRes

title=%E6%89%8B%E8% AA%9E&oldid=10305654.) (in Chinese) (維琪百科編者. 手語[G/OL]. 維琪百科, 自由的百科全書, 2009 年 06 月 13 日 06:36 [2009 年 07 月 2 日 06:32] http://zh.wikipedia.org/w/index.php? title=%E6%89%8B%E8% AA%9E&oldid=10305654.)

[8] Erenshteyn, R., Laskov, P., Foulds, R., *et al*. Recognition approach to gesture language understanding. In: Kavanaugh, M. E., Werner, B., eds. Proceedings of the 13th International Conference on Pattern Recognition. Los Alamitors: IEEE Computer Society, 1996, 431-435.

[9] Fels, S., Hinton, G. Glove-TalkII: A neural network interface which maps gestures to parallel formant speech synthesizer controls. IEEE Transactions on Neural Networks, 1998, 9(1): 205-212.

[10] Noriko, T., *et al*. An alternative method for building a database for American sign language. In: Proceedings of the Technology for Persons with Disabilities Conference 2000. Los Angeles, CA, 2000. http://www.csun.edu/cod/conf/2000/proceedings/0071Tomuro.htm.

[11] VRML97 Specification ISO/ IEC DIS 14772.

Copyright © 2009 SciRes

Intelligent Information Management, 2009, 54-59
doi:10.4236/iim.2009.11009 Published Online July 2009 (http://www.scirp.org/journal/iim)

Virtual Home Library System
——Let every Chinese family having their own libraries

Bin WU[1], Shu SONG[1], Jianxiang CAO[2], Wen RU[1]
[1]*Nation Library of China, Beijing* 100081, *China*
[2]*Communication University of China, Beijing* 100024, *China*

Abstract: Virtual Home Library (VHL) is an integrated IT system that utilizes virtual reality technology and an IPTV set-top box (STB) to virtually construct a 'library' and the relevant reading environment on televisions in people's home. Unlike the online e-book reading applications, Virtual Home Library can be applied on televisions-the world's most convenient and most efficient communication tool. Providing extended digital library services, it will be a perfect group reading utility for family readers. The system has been investigated by a joint research team formed by the National Library of China and the Communication University of China, collaborating with a Chinese IPTV equipment manufacturer. This paper presents some preliminary investigations of the VHL system performed by the research team.

Keywords: virtual home library, IPTV, virtual reality, digital library

虛擬家庭圖書館
——讓每個中國家庭都擁有自己的“圖書館”

吳　斌[1], 宋　姝[1], 曹建香[2], 茹　文[1]

[1]中國國家圖書館 北京 100081; [2]中國傳媒大學 北京 100024

摘　要: 虛擬家庭圖書館簡稱 VHL (Virtual Home Library)，是一個採用虛擬現實技術和 IPTV 機頂盒構建的 IT 集成系統。它可通過電視機在讀者家裏構建一個虛擬的“圖書館”和虛擬的讀書氛圍。不同於網上在線的電子圖書閱覽器，虛擬家庭圖書館可以應用在目前世界上最方便、最普及的傳媒工具——電視上，並提供拓展的數字圖書館服務，從而成為可供家庭讀者單獨或群體閱讀的理想設施。國家圖書館和中國傳媒大學組成的研究團隊，聯合國內的 IPTV 廠商，正在對 VHL 系統進行前期調研。本文就是根據該團隊的前期調研結果對 VHL 系統做一個總體介紹。

關鍵詞: 虛擬家庭圖書館，IPTV，虛擬現實，數字圖書館
中圖分類號: G250.76

1. 背景介紹

在一個安靜愉悅的環境下讀書，大概是人類最普遍、最愜意的愛好之一。但是，在我國的部分地區，比如偏遠的西部農村地區，書籍和圖書館仍然是一種奢侈品。由於書籍的缺乏而引起得知識和教育的不足，是導致我國中西部地區、以及城鄉之間經濟發展不平衡的最主要的原因之一。即使對於發達地區的人們來說，有時候閱讀的需求也不能滿足。這可能有兩方面的原因，一是在當今社會巨大的工作壓力下，人們用來閱讀的時間極為有限；二是在今天這個資訊爆炸的時代，能找到合適的讀物或找到想要的資訊已經變得越來越困難。

“數字圖書館”以其顯著的優點成為解決上述問題

Copyright © 2009 SciRes

的極好方案，這些優點包括：大容量的數位資源、隨時隨地地讀取應用、高效的檢索技術、基於知識聚類和人工智慧的用戶介面、強大的資料管理功能等等。一個典型的應用例子就是讀者通過線上的閱讀軟體上網流覽各種數位圖書。

但用戶要使用數位圖書館的應用必須要具備三個基本條件：

・互聯網的接入設施
・電腦系統（包括硬體和軟體）
・電腦操作技能

雖然我國政府近幾年來已經投入了大量的財力致力於改善全國範圍內的網路設施，但不具備電腦操作的技能（缺乏相關的培訓）、需要購買電腦硬體設備和商業軟體等等都限制了線上閱讀軟體的應用，特別是在農村不發達地區。

本課題研究的“虛擬家庭圖書館”系統（Virtual Home Library，VHL），正是針對上述問題的一個很好的解決方案。它採用虛擬現實技術和 IPTV（Internet Protocol Television，互動式網路電視）機頂盒，形成一個軟硬體集成系統，並通過電視機在讀者家裏構建一個虛擬的圖書館和讀書氛圍（如圖 1，圖 2 所示）。

不同於網上線上的圖書閱覽器還需要電腦設備和相應的操作技能，“虛擬家庭圖書館”系統可以應用在目前世界上最方便、最普及的傳媒工具——電視上。

它的應用只需要兩個條件：

・互聯網的接入設施
・普通電視機

簡言之，只要可以上網，並有電視機，通過電視遙控器，就能使用“虛擬家庭圖書館”系統進行讀書和查閱資訊。

而電視機已經在我國普及，互聯網的普及程度隨著國家的基礎建設投入也逐年迅速提高，通過撥號、xDSL 或 LAN 的方式使用互聯網的家庭越來越多。特別的，在首都北京，上述這兩個條件，都已滿足。因而，在北京使用此項產品，已經沒有問題。

充足的數位資源和全國範圍的網路傳播設施是“虛擬家庭圖書館”系統應用的兩個基本條件。這兩個條件目前已由政府的不斷投入而得以保證。首先，正在建設中的“國家數位圖書館工程”到 2008 年底將會提供約 340TB 的數字資源，並且將保持每年至少 50TB 的增長速度[1]。其次，2004 年開始的“中國國家文化資訊共用工程”已逐步建立了一個有效的覆蓋了中國大陸 31 個行政地區的資料傳輸網路[2]。圖 2 是該資料傳輸網路的拓撲圖。

圖 1. VHL 系統的家庭應用
Figure 1. Home implementation of VHL system

Copyright © 2009 SciRes

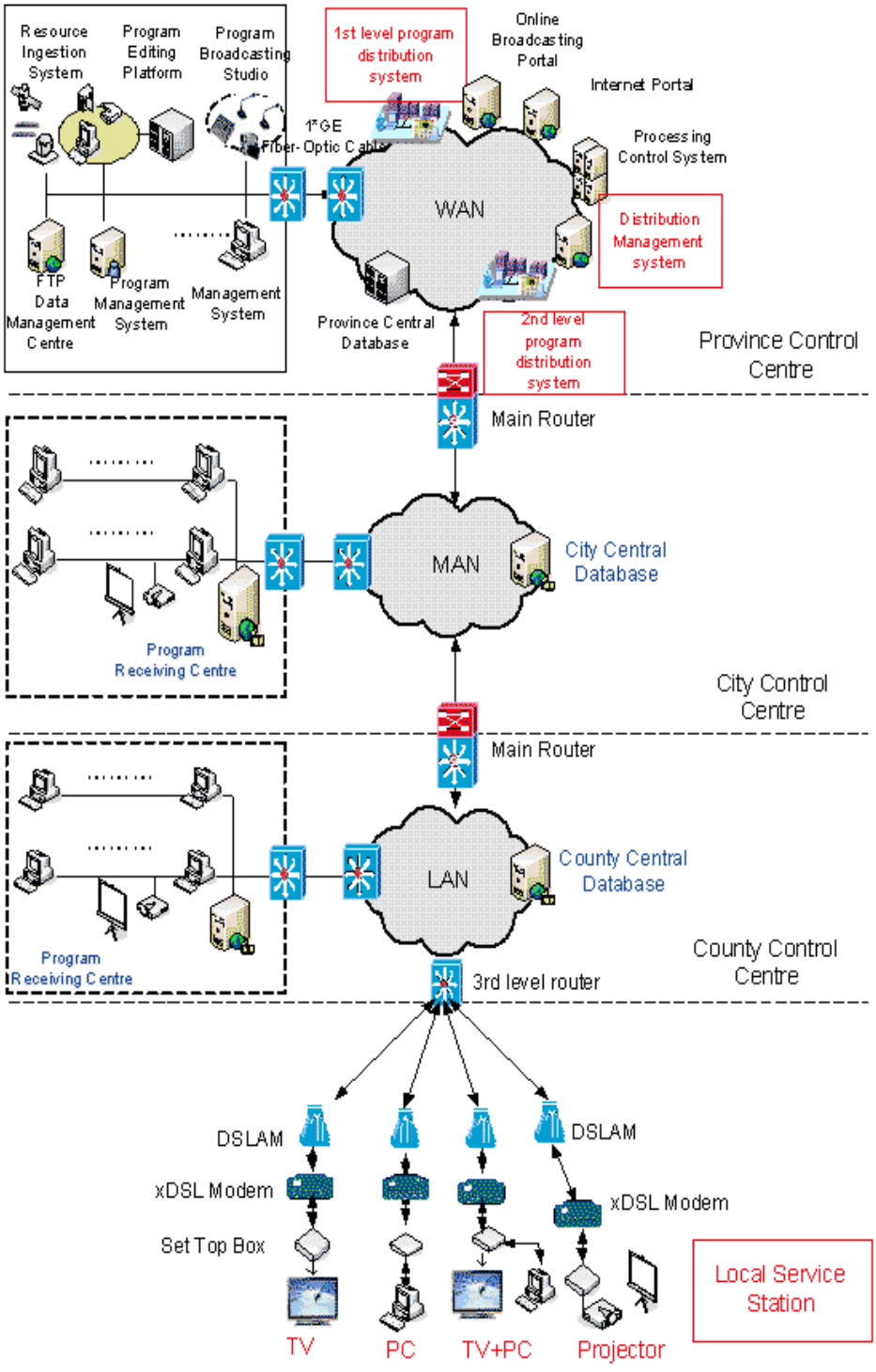


圖 2. 全國範圍的文化資源信息共享工程傳輸網絡拓撲圖

Figure 2. Topology of the nation-wide cultural resources information sharing transmission network

“虛擬家庭圖書館”是國家數位圖書館工程建設中《虛擬現實》子項目規劃中的一部分[3]，用以提供數位圖書館的拓展服務。其前期調研工作是由國家圖書館主導，並聯合中國傳媒大學和國內從事 IPTV 機頂盒研發的生產廠商共同組成的科研團隊進行的。目前研究工作的目標是要實現一個“虛擬家庭圖書館”的原

Copyright © 2009 SciRes

型系統。本文就是對該系統和相關的研究作一個初步介紹。

2. 虛擬家庭圖書館（VHL）系統和相關的研究內容

一個虛擬家庭圖書館系統由以下兩部分組成：

硬體: 一個具有 CPU 處理器和電視/互聯網介面、並能對無線控制信號做出反應的 IPTV 機頂盒 STB(Set Top Box)，見圖 3。

·軟體: 可對控制者的操作做出回應的嵌入式虛擬現實應用軟體。

研究小組將提交一份關於 VHL 系統的完整調研報告。該報告涉及的軟硬體技術細節主要包括以下幾個方面：

· 用戶需求分析
· 硬體相容性/功能操作分析
· 人機界面分析
· 服務功能分析
· 系統集成分析

根據這份研究報告，可以制定整個系統的設計綱要，並設計出原型系統。

目前的研究重點集中在以下兩點：

·“虛擬家庭圖書館”系統中相關軟硬體開發的技術問題。這些問題包括硬體相容性、嵌入式技術和人機交互介面等。

·“虛擬家庭圖書館”系統涉及到的數位圖書館服務相關的技術，比如：資料管理、基於知識聚類的檢索技術等。

3. 虛擬家庭圖書館（VHL）系統的優點

基於 IPTV 和虛擬現實技術的“虛擬家庭圖書館”系統將有以下幾個優點：

1) 低投入——該系統不需要任何電腦硬體，唯一一個硬體設備是一個可連接網路和普通電視的 IPTV 機頂盒（如圖 3 所示），用來切換數位信號轉和類比信號，並對用戶的操作做出相應的反應。該機頂盒的費用不到五百元人民幣。在一些省份的農村家庭和鄉村圖書館站已經由中央財政、地方政府和“全國文化資訊共用工程”三家提供了免費的機頂盒[2]。

2) 網路風險低——由於虛擬家庭圖書館系統的用戶端不具備上傳功能，並且用來傳輸的大多數數位資源的帶寬需求相對較低（約 800K－1M），因而網路

圖 3. VHL 系統使用的機頂盒原物圖
Figure 3. Set Top Box of VHL system

的安全及系統運行的可靠性能夠得到保證。

3) 易於維護——VHL 系統所涉及的所有資料的存儲和傳送都是由管理中心控制的，系統的升級也是由中央控制系統發送的進程來完成的。因而在 VHL 系統中無需用戶端做任何維護工作。

4) 不需要電腦操作技能——由於“虛擬家庭圖書館”系統是通過電視機來運行的，所以用戶只需會操作電視機的遙控器，不需要任何電腦作業系統的知識和技能。

5) 友好的用戶介面和個性化的功能——虛擬現實技術將提供給用戶一個自然的人機交互介面。每個家庭成員都可在家中定制自己的“書架”內容（見圖 4），享受個性化的閱讀環境。還有一些功能可以使得閱讀更加輕鬆，比如：通過語音輸出功能讓讀者在放鬆的時候或者在做其他事情的時候“聽”書。

6) 適合群體閱讀——由於“虛擬家庭圖書館”系統是通過電視機來實現的，它自然而然地繼承了電視機的播放特點和優勢（相對單個 PC 而言），比如可供多人一起進行閱讀、欣賞、娛樂等。

7) 有效快捷的讀取資源——作為數位圖書館的擴展服務，虛擬家庭圖書館系統可以擁有數位圖書館特有的強大服務功能，比如基於知識聚類的快捷檢索技術和智慧化的管理功能等。

4. 虛擬家庭圖書館（VHL）系統的創新點

概括來說，“虛擬家庭圖書館”系統的研發主要有兩方面的創新：一是數位圖書館在 IPTV 技術上的應用；二是虛擬現實的人機交互技術。

Copyright © 2009 SciRes

圖 4. 虛擬家庭圖書館系統中的“書架”圖書目錄

Figure 4. An example book selection menu of VHL

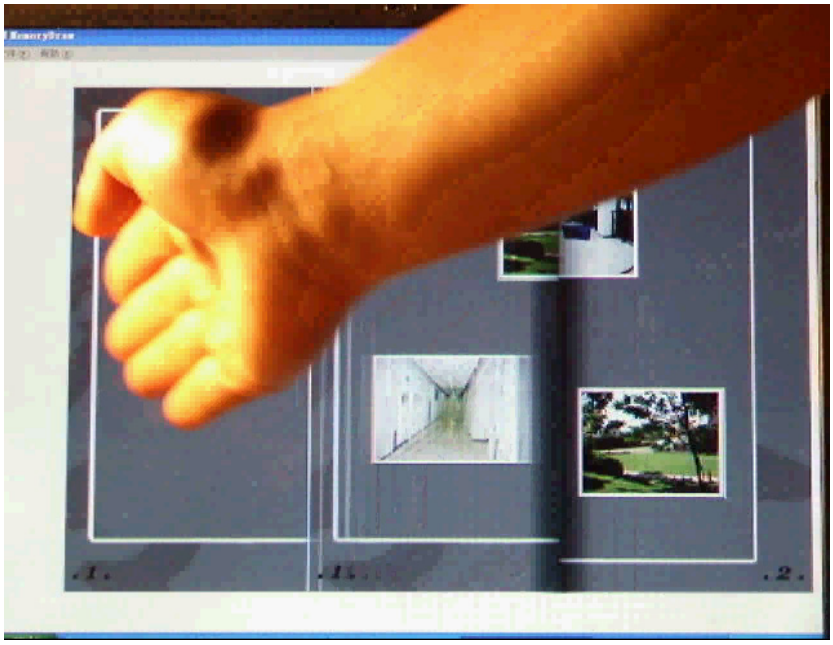


圖 5. 通過外接相機捕捉的手部動作實現翻頁功能

Figure 5. Hand turning pages without touching the screen (detected by a camera)

1) 數位圖書館的 IPTV 應用：“虛擬家庭圖書館”系統使得數位圖書館的服務可以應用到世界上最廣泛、最便捷的通訊工具上——電視上，而惠及千家萬戶。這是一個前所未有的創新。它具有操作簡單、易於維護、價格低廉等優勢，特別適用于普通中國家庭。

基於虛擬現實技術的人機交互介面: “虛擬家庭圖

Copyright © 2009 SciRes

書館”系統中虛擬現實技術的應用, 將會使讀者在電視上身臨其境地體驗真實“讀書”的效果。家庭中每個成員都可以在家裏的“虛擬閱讀環境”中享受讀書的樂趣。讀者可以建立一個屬於自己的虛擬“書架”, “擺放”從當地或國家數字圖書館借來的各種“圖書”。讀者可以隨時從該書架上“取”書並“翻開”進行閱讀。同時，一些新的體驗比如通過電視機的遙控器來實現“翻頁”功能，或者更自然地通過外接的攝像頭捕捉讀者的手部動作來實現閱讀時“翻頁”的功能（見圖 5）。此外，系統的語音輸出功能將會使閱讀的體驗更加輕鬆愜意，比如之前描述的“聽”書的功能。

5. “虛擬家庭圖書館”系統（VHL）的社會效益

1) 首先，“虛擬家庭圖書館”系統將有助於數位圖書館的服務拓展，可將知識傳播到更遠的地區，惠及更多的人群。

目前，中國是世界上電視機擁有量最多的國家。截止到 2006 年底, 我國國民家庭電視機擁有量大約為 3.2 億台，覆蓋了全國大約 94.8%的人口。特別是在農村地區，每百戶農村家庭平均擁有 108.6 台電視機，也就是說每戶農村家庭至少擁有一台電視機。作為國家重點資訊工程的“村村通網路”專案已在 2007 年 7 月啟動，目標是在下一個五年計劃中實現村村通網路。在“國家數位圖書館工程”、“全國文化資訊共用工程”、以及中央和地方各級政府的大力支持下，全國範圍內的資訊基礎設施和充足的數位資源已基本形成。因而，從理論上講，只要擁有電視機和互聯網接入的家庭都可以成為“虛擬家庭圖書館”的直接用戶。有了“虛擬家庭圖書館”系統，我們可以期待，無論在中國的城市還是鄉村，人們都可以方便、經濟、有效地通過電視機來檢索和閱讀圖書，**使圖書館走進千家萬戶，使全國人民都可以共用資訊和知識**。

2) 其次，“虛擬家庭圖書館”的建設將應用最新的技術，比如虛擬現實、人機自然交互介面及基於知識聚類的資訊檢索技術等。這使得該系統有著巨大的發展潛力，比如，可以融合到新一代的數位電視的發展以及未來“數位家庭”的發展[4]中。

6. 結 論

本文對虛擬家庭圖書館系統的前期調研做了一個總結。該項工作是由一個聯合的研發團隊實施的，將作為國家數位圖書館建設中的服務拓展的一部分。目前的研究目標是開發出一個融 IPTV 技術和虛擬現實技術於一體的“虛擬家庭圖書館”的原型系統。它能在讀者家中虛擬地構建 “圖書館”和相關的閱讀環境。由於可以提供充足的數位資源，“虛擬家庭圖書館”系統將可以使中國每個家庭都擁有自己的“圖書館”，足不出戶地閱讀和流覽各種圖書和資訊。

REFERENCES

[1] Sun, CJ. and Fu, P., Preliminary Design of the China National Digital Library Project, internal document, National Library of China, June 2005.（in Chinese） (孫承鑒, 富平, 孫衛, 等. 國家數字圖書館初步設計. 中國國家圖書館, 6/2005).

[2] Annual Report 2007, internal document, National Cultural Information Resources Sharing project, Home Page http://www.ndcnc.gov.cn), February 2008.(in Chinese) (全國文化資訊資源分享工程. 全國文化資訊資源分享工程 2007 年年報. http://www.ndcnc.gov.cn/).

[3] Wu, B., The Technical Framework of the China National Digital Library, Forum of the 10th Anniversary of the development of Digital Library in China, Shenzhen, China, November 2007.(in Chinese) (吳斌. 國家數位圖書館技術架構. 深圳. 中國數字圖書館 10 周年論壇, 11/2007).

[4] Introduction of China Digital Home project, media report: http://www.gd-emb.org/detail/id-38689.html, July 2007.(in Chinese)(中國數位元元元家庭工程介紹. http://www.gd-emb.org/detail/id- 38689. html, 07/2007).

Copyright © 2009 SciRes

Intelligent Information Management, 2009, 60-63
doi:10.4236/iim.2009.11010 Published Online July 2009 (http://www.scirp.org/journal/iim)

The Design of the Minimum Spanning Tree Algorithms

Zhicheng LIU[1], Bo JIANG[2]
[1]*Naval Aeronautical Engineering Institute, Yantai,* 264001*, China*
[2]*Shandong Institute of Business and Technology, Yantai,* 264005*, China*

Abstract: Based on the graphic theory and improved genetic algorithm, an improved genetic algorithm to search the minimum spanning trees is given. The algorithm uses binary code to represent the problem of minimum spanning trees. It designs the corresponding fitness function, operator and few controlling strategies to improve its speed and evolutionary efficiency. Only one solution can be gotten with running traditional algorithem atone time. The new algorithm can get a set of the solutions with higher probability in a shorter time. The experiment shows that it has a better performance than traditional methods.

Keywords: minimum spanning tree, genetic algorithm, pattern

一種最小生成樹算法設計

劉志成[1]，薑　波[2]
[1]海軍航空工程學院，[2]山東工商學院，山東　煙臺　264000

摘　要：以圖論和改進遺傳算法為基礎，提出了一種求最小生成樹的遺傳算法。該算法採用二進制表示最小樹問題，並設計出相應的適應度函數、算子以及幾種控制策略，以提高執行速度和進化效率。傳統算法一次只能得到一個候選解。用該算法對其求解，可以在較短的時間內以較高的概率獲得多個候選解。應用實例表明該算法優於傳統算法。

關鍵詞：最小生成樹，遺傳算法，模式

1. 引 言

圖論中已有一些經典的最小樹演算法，如 **Kruskal** 演算法、**Prim** 演算法、**Sollon** 演算法等，但都屬於貪心演算法，一般只能得到一個最小生成樹，而在實際應用中通常需要同時尋找出一組最小或次最小生成樹作為方案評價或選擇的依據。

遺傳演算法是一種類比自然進化過程的隨機搜索方法，在解決全局優化問題方面，顯示了廣泛的應用前景。為了能夠在較短的時間內以較高的概率獲得一組最小生成樹或次最小生成樹，本文提出一種基於改進遺傳演算法的最小生成樹演算法。

2. 遺傳演算法

遺傳演算法的基本思想來源於遺傳進化，主要是借助於生物進化機制與遺傳學

原理，按照自然選擇和適者生存的原則，利用簡單的編碼技術和繁殖機制，模擬自然界生物群體優勝劣汰的進化過程，實現對複雜問題的求解。遺傳演算法一般進過這樣幾個過程：首先隨機產生一定數目的初始染色體，然後以群體中個體的適應度為依據，對個體執行選擇、雜交和變異的操作，使群體中的個體不斷逼近問題的最優解。

選擇運算元是在當前種群選出優良的染色體。常用的選擇運算元有適應度比例法、最佳個體保留法、

Copyright © 2009 SciRes

期望值法等。雜交運算元按一定的概率隨機交換兩個個體的部分基因位元，它產生的兩個個體包含父代的遺傳物質，但與父代個體不同，因此雜交運算元擴大了搜索範圍。變異運算元以一個很小的隨機概率改變個體的某些基因位。它具有增加和恢復群體多樣性的功能，使遺傳演算法能進行非線性局部搜索。

3. 用遺傳演算法求最小生成樹的基本原理

設一無向圖 G=（N，E，W），其中 $W=\sum_{e\in E}\omega_e$ 為權函數，若樹 $T=(N,E_T,W_T)$ 包含了圖 G 的所有頂點，則樹 T 為 G 的一個生成樹，其中 $W_T=\sum_{e\in E}\omega_e$ 為樹 T 的權。圖 G 的生成樹不唯一，權最小的生成樹成為 G 的最小生成樹。

圖論中經典的最小生成樹演算法，一般情況下僅得到唯一的最小生成樹，對許多現實問題而言，不同形式的最小生成樹代表不同的設計方案。有時權值次小的生成樹，可能是一個較好的設計方案。如果任選其一，可能會丟棄或忽略更優的方案。因此，在實際應用當中希望能同時得到若干個最小或次小生成樹作為備選方案。對於一個完全圖 G，過 n 個頂點的樹的數目是 n^{n-2} 個，採用枚舉法計算量太大，有必要尋找更有效的演算法，在較短的時間內，以較高的概率確定出一批最小樹或次小樹。

考慮如下一個尋找最小樹的過程：根據圖論中樹的性質可知，一棵過 n 個頂點的樹必有 n-1 條邊，且是連通的。對於一個有 ND 個頂點、NP 條邊的圖 G 來說，從 NP 條邊中隨機選取 ND-1 條邊，則可構成一個子圖。利用深度優先搜索演算法（DFS）對該圖進行一次搜索，如果能搜索到 ND 個頂點，則 ND-1 條邊所構成的連接子圖是一個連通圖。過 ND 個頂點且有 ND-1 條邊的連通圖一定是該圖的一棵生成樹，即所選擇的 ND-1 條邊構成一個生成樹。如果能採用一定優先技術，搜索並評價盡可能多的生成樹，就可以尋找出一組權值最小或次最小的生成樹。

研究表明，遺傳演算法對組合優化問題的求解非常有效，能夠在短時間內，以較高的概率獲得一批最優或次最優方案。上述尋找最小生成樹的過程實際也是一個典型的組合優化問題。根據遺傳演算法的基本原理，結合最小生成樹的特點，可按照以下過程尋找生成樹：首先選擇一種合適的編碼方式表示最小樹問題，然後直接以樹的權值最小為優化目標函數，從一組隨機產生的初始解出發，以遺傳演算法控制優化搜索的過程，通過不斷搜索並評價可行的生成樹，逐漸進化到一組權值最小的生成樹，實現最小樹的優化求解。

設某一無向圖中共有 ND 個頂點和 NP 條邊，對圖中的節點和邊進行編號，以圖中的所有邊為編碼變數，各個編碼變數的取值為 0 或 1，則用一個長度為 NP 的二進位字元串可表示該圖的所有子圖；當字串中某位元上的字元值為 1 時，表示它所對應的一條邊是構成子圖的邊；當字元值為 0 時，表示它所對應的邊不是構成子圖的邊。

3.1 適應度函數的設計

設某一無向圖中各邊的權值為 $W_i(i=1,2,\wedge,NP)$，對於求權最小的生成樹問題，可定義其適應度函數為

$$F=\begin{cases}F_0-\sum WiZ_i & Z_i\in\{0,1\} \quad i=1,2\cdots NF\\ 0 & \text{其他}\end{cases}$$

式中 $F_0=(ND-1)\max(W_1,W_2,\wedge,W_{NP})$ 是一個正常數，保證個體適應值為正；W_i 為第邊的權值；Z_i 為個體編碼中第 i 位元的字元值（對應於圖中的第 i 條邊）為 0 或 1。

在遺傳過程中，必須對每一個個體所對應的子圖進行深度優先搜索。若能搜索到所有的頂點，則說明該個體是圖的一個生成樹，用所定義的適應度函數運算式計算該個體的適應度；否則令該個體的適應度為 0，使其在進化過程中的生存能力最低，逐漸從群體中淘汰出去。

3.2 遺傳運算元的設計

根據生成樹的特點可知：當用一個長度為 NP 的二進位字元串表示圖 G 的所有子圖時，為了避免進化過程中不可行方案的產生，必須控制所產生的個體只有 ND-1 個字元值為 1，使其具備成為可行解的必要條件，然後通過連通性檢驗確定是否是一個生成樹。

一般遺傳演算法主要通過雜交運算元和變異運算元產生新的個體。對於最小生成樹問題，變異運算元和雜交運算元都容易破壞個體的可行性，即他們所產生的新個體往往不能構成有效的生成樹，降低了遺傳演算法的搜索能力。為提高遺傳演算法搜索最小生成

Copyright © 2009 SciRes

樹的效率，結合生成樹的圖論特性，設計出新的運算元，即換位運算元和逆轉運算元。

換位運算元對所選擇個體的基因鏈上的任何一對基因進行交換，能使任何一個母體通過有限次基因換位生成新個體。通過這種基因重組方式可以從一個種群出發，以較高的概率搜索到解空間的各個可行解，能有效避免遺傳過程中無效個體的產生。

逆轉運算元則是將母體基因鏈上的一段基因進行逆轉，該段基因包含偶數個基因位元且所含字元“1”的個數為偶數。它一次性地將一個母體突變為一個新個體。與換位元運算元相比，它執行速度較快，有助於將母體中未突變的有效基因段, 直接移植到字體中。

改進後的遺傳演算法具有一個突出特點：在子代群體的生成過程中，所產生的個體不僅均為可行解，而且具有不同結構，可以提高對解空間的搜索能力。

3.3 控制策略的設計

為使遺傳進化過程以較快的速度向理想的優化方向前進，採用如下控制策略。

3.3.1 代間競爭與群體單一化策略

為保證群體性能的優越性，採用代間競爭機制，即在保持群體規模不變的情況下，選擇親代的若干個較優個體和新生成的個體組成進化群體，這樣既能保持群體的多樣性，又能保證群體性能不斷提高。

3.3.2 換位運算元和逆轉運算元隨機執行策略

在遺傳進化過程中換位運算元和逆轉運算元以一定得隨機概率執行。首先定義一個換位運算元的執行概率 P_t，用偽亂數 R_t 決定所要執行的運算元。$R_t \geq P_t$，執行換位運算元，否則執行逆轉運算元。

3.3.3 模式突變策略

同一基因位上等位基因的多樣性是指在種群中，染色體相同基因位的基因既有“0”又有“1” ,即在該基因位上基因全為“0”或“1”的概率為：

$$P(\text{“0”})=0 \qquad P(\text{“1”})=0$$

基因丟失指的是群體中所有個體在某基因位元上的字元值均相同，即整個群體在該基因位元上無互補字元值，即當前種群為一模式，而變異運算元無法有效保持同一基因位上基因的多樣性。一旦出現基因丟失，將會影響搜索效率，同時導致過早收斂與停滯現象的發生。

為避免上述情況，執行如下操作：

設個體 $e=(e_1 \quad e_2 \quad \wedge \quad e_n)$ $\qquad d=(d_1 \quad d_2 \quad \wedge \quad d_n)$

定義 $e \times d = g$ $\qquad g_i = \begin{cases} e_i & e_i = d_i \\ * & \text{其他} \end{cases}$

則稱 g 代表的模式為個體 e 和 d 的祖先模式。

（1）找到基因丟失位：取祖先模式，抽取模式，演算法如下：

$M_0 = a[1] \times a[2]$

For i=3 to N $\qquad M_0 = M_0 \times a[i]$

其中，$a[i]$ 為當前種群的個體， i=1 2…N。

（2）進行調節，演算法如下：

If M_0 中的字元不全是“*”then

對單個或多個基因丟失位執行逆轉運算

3.3.4 進化終止策略

遺傳演算法是一種反復迭代的演算法，必須事先給定最大遺傳代數。在進化過程中，通過觀察和比較群體平均適應度的變化，判斷進化狀態。如果群體平均適應度沒有變化且沒有達到控制代數時，則認為由出現進化停滯的跡象；如果群體平均適應度沒有變化且已經達到控制代數時，則認為進化已經停滯。

表 1. 用遺傳算法求得的最小生成樹

Table1. The minimum spanning trees based on genetic algorithm

方案	權	組成最小生成樹的邊								
1	60	1	2	7	10	11	15	17	19	23
2	60	1	2	5	7	10	11	15	19	23
3	60	2	5	7	10	11	15	17	19	23
4	61	2	4	7	10	11	15	17	19	23
5	61	1	2	5	7	10	11	15	19	23
6	61	2	5	10	11	15	17	18	19	23
7	61	1	2	7	10	11	15	16	19	23
8	61	1	2	7	10	11	15	17	19	23
9	61	1	2	5	7	11	15	17	19	23
10	61	2	5	7	11	15	17	18	19	23

Copyright © 2009 SciRes

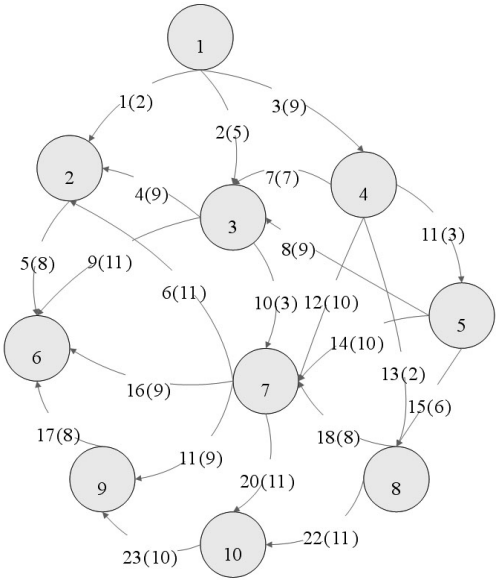


圖 1. 艦艇編隊通信網連接圖

Figure1. The network of communication of naval vessels

4. 實例應用

現有一艦艇編隊的初步組網方案，共有 10 艘艦艇，23 條可能的通信管道，擬求一組總長度最短的樹狀網佈局。首先將初步連接方案概化為如圖 1 所示的連接圖，各邊的編號及長度如圖 1 所示。對其進行優化，可獲得一組全最小或次最小的生成樹如表 1 所示。實驗表明：當換位運算元概率 Pt 在 0～0.5 之間變動時，共搜索和評價了 500 個方案，而採用圖論中 **Kruskal** 演算法只能得到一個最小生成樹，並且與表 1 中的方案 2 相同。

5. 結束語

基於改進遺傳演算法的最小生成樹演算法可用於不同類型的最小數研究，能夠在較短的時間內以較高的概率獲得一批最小樹或次小樹，為實際工作的方案評估和決策提供更多的依據。

該演算法所需資料少，操作簡單，收斂性和適應性較強，可根據不同工作需求，構建不同目標函數。如果能夠利用生成樹的啟發式資訊，就可以達到更快的收斂速度，這是有待進一步研究的問題。

REFERENCES

[1] Chen Guo-Liang,The Algorim of Genetic and The Application[M]. Beijing: People's post publishing house,1996.(in Chinese) (陳國良，遺傳演算法及應用 [M]. 北京：人民郵電出版社，1996).

[2] Xie Jin-Xing,Xing Wen-Xun. Optimization of the Network [M].BeiJing:the publishing of the QingHua University,2000(in Chinese) (謝金星，刑文訓. 網路優化[M]. 北京：清華大學出版社，2000).

Copyright © 2009 SciRes

9772150819004 01