

# JAIST Repository Related Faculty & Research Search System < Operation Manual >

## 1. Enter a keyword.

Go to the search top page ([https://dspace.jaist.ac.jp/search/ir\\_search\\_eng.html](https://dspace.jaist.ac.jp/search/ir_search_eng.html)), and enter a keyword and click "Search".



Or

Go to the JAIST Repository topage (<https://dspace.jaist.ac.jp/dspace/index.jsp?locale=en>).

Choose "Faculty's Articles" and enter a keyword, and then click "Search".



## 2. Search results page shows as follows.

In the following search results page (Window1), you can see faculty members and articles that are related with the entered keywords. Faculty members and articles information shows on one page and it is possible to search again by a related keyword of the search results. (See ※2 for details of the "Related Keywords")

**Window1: Search Results Page**

Search: All of JAIST Repository  
 All  Faculty's Articles encryption

Results 1-5 of 8.

Refine results by Document Type | Related Keywords

Journal Article (36) | Conference Paper (9) | Technical Report (2) | Others (1) | Presentation (1) | Research Paper (4)

Atsuko Miyaji Professor | Faculty Profile | Link to the Faculty Profile .

1. A Timed-Release Proxy Re-Encryption Scheme and its Application to Fairly-Opened Multicast Communication

2. Ancestor Excludable Hierarchical ID-based Encryption and Its Application to Broadcast Encryption

3. Information Security for Privacy Protection

4. 初等的な環状経路を用いた匿名通信方式

5. Efficient Privacy-Preserving Data Mining in Malicious Model

6. Privacy-Preserving Data Mining in Presence of Covert Adversaries

7. A ciphertext-policy attribute-based encryption scheme with constant ciphertext length

8. Simple Certificateless Signature with Smart Cards

9. Success probability in chi-square attacks

10. サイドチャネル攻撃に対して安全な公開鍵暗号に関する研究

11. Toward Dynamic Attribute-Based Signcryption (Poster)

12. The security of PCE-assisted asymmetric chi-square test attack

Kazumasa Omote Associate Professor | Faculty Profile

1. Protection and Recovery of Disk Encryption Key Using Smart Cards

2. Practical and secure recovery of disk encryption key Using Smart Cards

3. A Timed-Release Proxy Re-Encryption Scheme and its Application to Fairly-Opened Multicast Communication

4. A ciphertext-policy attribute-based encryption scheme with constant ciphertext length

5. Simple Certificateless Signature with Smart Cards

**Window2: Faculty's Article List Page**

MST Repository >  
 宮地 光子 (ミヤジ アツコ) 教授  
 情報科学研究所

No. 書籍情報

1 Generalized RC4 Key Collisions and Hash Collisions / Chen, Jigeng, Miyaji, Atsuko, Lecture Notes in Computer Science, 6280/2010, pp.73-87, 2010-09, Springer

2 A ciphertext-policy attribute-based encryption scheme with constant ciphertext length / Emura, Keita, Miyaji, Atsuko, Omote, Kazumasa, Nomura, Akito, Soshi, Masakazu, International Journal of Applied Cryptography, 7(1), pp.45-59, 2010-07-02, Inderscience

3 New Analysis Based on Correlations of RC4 PRGA with Nonzero-Bit Differences / MIYAJI, Atsuko, SUKIGAWA, Masahiro, IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences, E93-A(6), pp.1066-1077, 2010-06-01, 電子情報通信学会

4 A Timed-Release Proxy Re-Encryption Scheme and its Application to Fairly-Opened Multicast Communication / Emura, Keita, Miyaji, Atsuko, Omote, Kazumasa, Lecture Notes in Computer Science, 6402/2010, pp.200-213, 2010, Springer

5 An Anonymous Designated Verifier Signature Scheme with Revocation: How to Protect a Company's Reputation / Emura, Keita, Miyaji, Atsuko, Omote, Kazumasa, Lecture Notes in Computer Science, 6402, pp.184-198, 2010, Springer

6 A New Class of RC4 Colliding Key Pairs With Greater Hamming Distance / Chen, Jigeng, Miyaji, Atsuko, Lecture Notes in Computer Science, 6047/2010, pp.30-44, 2010, Springer

7 Privacy-Preserving Data Mining in Presence of Covert Adversaries / Miyaji, Atsuko, Rahman, Mohammad Shahrir, Lecture Notes in Computer Science, 6440/2010, pp.429-440, 2010, Springer

**Window3: Article Details Page**

イテムの引用には次の識別子を使用してください: http://hdl.handle.net/10119/8481

タイトル: Protection and Recovery of Disk Encryption Key Using Smart Cards  
 著者: Omote, Kazumasa  
 Kato, Kazuhiko

発行日: 2008-04  
 出版者: Institute of Electrical and Electronics Engineers (IEEE)  
 誌名: Fifth International Conference on Information Technology: New Generations, 2008. ITNG 2008.  
 開始ページ: 106  
 終了ページ: 111  
 DOI: 10.1109/ITNG.2008.195

抄録: Information leakage has recently become a serious problem. Because a user's disk might contain a lot of confidential information, it should be encrypted and the encryption key protected securely. Disk security has been improved by storing the encryption key in a hardware token such as a smart card or USB device. There must be some way to recover the encryption key when the token is lost, but to prevent information leakage the encryption key should not be known by the system administrator and should not be able to be recovered by malicious users inside the system. Here we describe a scheme that can limit key recovery when the user's smart card is lost and can do so without the administrator knowing the key. The smart card is used for generating the key and for improving the user authentication.

Rights: Copyright (C) 2008 IEEE. Reprinted from Fifth International Conference on Information Technology: New Generations, 2008. ITNG 2008, 106-111. This material is posted here with permission of the IEEE. Such permission of the

(※1) **Refine results by Document Type:** To refine the results, click a document type such as "Journal Article", "Conference Paper" or etc.

(※2) **Related Keywords:** The results of "Related Keywords" listed below are extracted from the author keywords in search results of the above page (Windows1). It shows maximum 50 keywords sorted by the number of the articles that contain the entered keywords. For searching again faculty's articles that contain the same author's keywords, click to a related keyword.



(※3) **About Search Results:** The searching by entered keywords shows the articles that contain the same keywords in titles, authors, journals, author's keywords, abstracts or full texts. The results show the searched articles by each faculty member. (Sort ordering: in order of the number of searched articles by keyword.)