**SCIS 2008** The 2008 Symposium on
Cryptography and Information Security
Miyazaki, Japan, Jan. 22-25, 2008
The Institute of Electronics,
Information and Communication Engineers

# Research and Implementation of ID-based Encryption Scheme Based on Symmetric-Key Technique with a Trusted Device

林椿芳 Chun-Fung Lin [*]
楊中皇 Chung-Huang Yang [†]
櫻井幸一 Kouichi Sakurai [‡]

**Abstract—** IST is abbreviated from ID-based encryption scheme based on symmetric-key technique with a trusted device. IST scheme is differ from conventional security technical theory by unifying authentication and powerful encryption. In this scheme, users can encrypt their file by using identity information, and exchange any key is not necessary. The aim of this paper is to implement an IST scheme by using Java Card on Windows platform. Our implementation is created with Borland C++ Builder 6 to achieve user-friendly GUI interface, and may improve the security of key management by means of Java Card.

**Keywords:** Java card, symmetric-key, ID-based encryption scheme

## 1 Introduction

As home PC becomes widespread and the internet is growing up, nowadays people get many chances to transmit data and communication with other netizen, whereupon there are many problem of security appeared, such as stolen information, modified content, and so on. Therefore we have to consider how to achieve the security requirements of privacy, integrity, and authenticity. IST scheme, which is abbreviated from ID-based encryption scheme based on symmetric-key technique with a trusted device, saves users identity information in trusted device and uses these values for authentication without exchanging any key [1]. Two motives have combined to make us write a paper on IST: first, we review ID-based schemes and compare their advantage; and secondly, our purpose is to realize a user-friendly implementation of IST.

In this paper, detailed account of identity-based schemes are given in the next section, and then we design a tool to implement IST scheme in Section 3. Finally, our conclusion is given in Section 4.

## 2 Related Works

### 2.1 ID-based encryption

Shamir addressed identity-based cryptosystems and signature schemes [2]. A general idea of ID-based scheme is using a unique combination of users' identity information for authentication, even the users have no knowledge about cryptography, they can encrypt their information easily with this method. There are some differences between this scheme and others, for example, there is a Certificate Authority (CA) in Public Key Infrastructure (PKI) to management users' identity and keys, because of encrypting any ciphertext must use the keys, we must exchange keys with meticulous security; but in ID-based scheme, we can encrypt and decrypt only using users' identity information without exchange or conserve any key.

After Shamir's concept proposed, Desmedt et al. presented ID-based encryption with tamper-free device [3]. In other to provide physical protection to the keys, this scheme uses tamper-resistant device to improve its security. There are three main device in this scheme: encryption device $E$, decryption device $D$, and key generation $G$ which is tamper-resistant. Each user has a private key $k$ and a public key $K$ ($K = G(k)$). The security of this system is based on device $G$ which has a supersecret key $s$ to avoid malicious user to find the key. But if anyone knows a supersecret key $s$, he can attack all users of this system.

### 2.2 IST scheme

In the previous research, Fukaya and Sakurai presented a concept of ID-based encryption scheme based on symmetric-key technique with a trusted device (IST) [1]. IST uses a non-cloning device with unique value to generate encryption key, and users can enter a plaintext with their partner's ID to construct the ciphertext, and vice versa. As the symmetric-key is generated by users' ID information and the unique value in the non-cloning device is reliable, the secure key is not necessary to exchange or control. In a recent paper which proposed by Imamoto et al. use linear scheme to make enhancement of security [4]. Using unique device to make the ID stored in the device readable and unmodifiable is the difference between IST and the study issued by Desmedt et al.

IST technique could be implemented for many kinds of authentication system, like DRM [5], and so forth.

[*] Graduate Institute of Information and Computer Education, National Kaohsiung Normal University, 116, Ho Ping First Road, Kaohsiung 802, Taiwan. Email: veronica@icemail.nknu.edu.tw

[†] The same as *. Web: http://crypto.nknu.edu.tw/, Email: chyang@computer.org.

[‡] Faculty of Computer Science and Communication Engineering, Kyusyu University, 744 Motooka, Nishi-ku, Fukuoka 819-0395

### 2.3 Java Card

Java Card is one kind of smart card which includes both Java Card Virtual Machine (JCVM) and Java Card Runtime Environment (JCRE) so that it can manage Java classes and objects, execute Java Card applet, etc. [6] There are three main types of Java Card: JCOP10, JCOP20, JCOP30. The first dual-interface Java Card is JCOP30, which keep contact and contactless capabilities on the same chip, so that we can create much more applicability [7]. Because of all method and variables are controlled exactly, even any applets on the same Java Card couldn't access the other one to catch data, Java Cards could improve security for applications. There is one other thing that is important for us to use Java Card on our implementation: since we consider that users have to input their identity repeatedly and keep the symmetric key is difficult, Java Card provide a portable and reliable way to store information safely [8]. In order to achieve IST's personal security, we choose Java Card for the tamper-resistant device.

## 3 Implementation

In our study, we select Java Card (JCOP30) to manufacture trusted device with unique value. With the contact and contactless capabilities of JCOP30, users can use our tool by two ways to login for their convenience. Our concepts of encryption and decryption are shown in Figure 1 and Figure 2. For the consideration of security issue, we chose AES 256 to be the crypto algorithm because of its excellent performance.

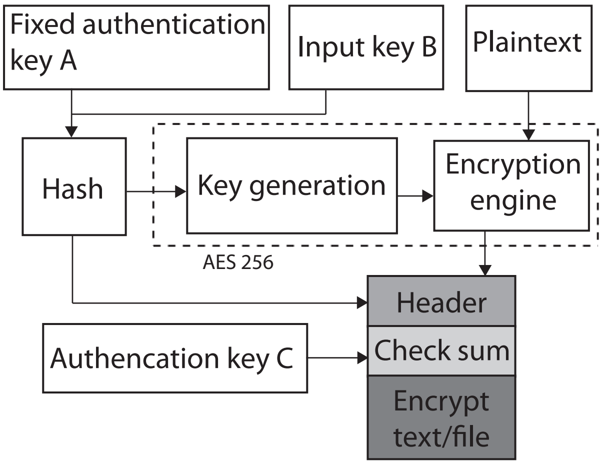


Figure 1: Concept of IST Encryption

As we want to illustrate our implement, we create three roles in the IST encryption/decryption scenario at first, included the sender $A$, the receiver $B$, and the administrator $M$.

1. The sender $A$: $A$ must know the receiver $B$'s public ID information before sending files, and use $B$'s ID and $A$'s own authentication information to encrypt the plaintext.

2. The receiver $B$: $B$ has to provide his Java Card to retrieve his own authenticate, then enter $A$'s ID information and his own authentication information to decrypt the ciphertext.

3. The administrator $M$: $M$ has a token which is a Java Card with special authority, so that he could putting information into the smart card by this software. $M$ can't generate any information into Java Card without the token.

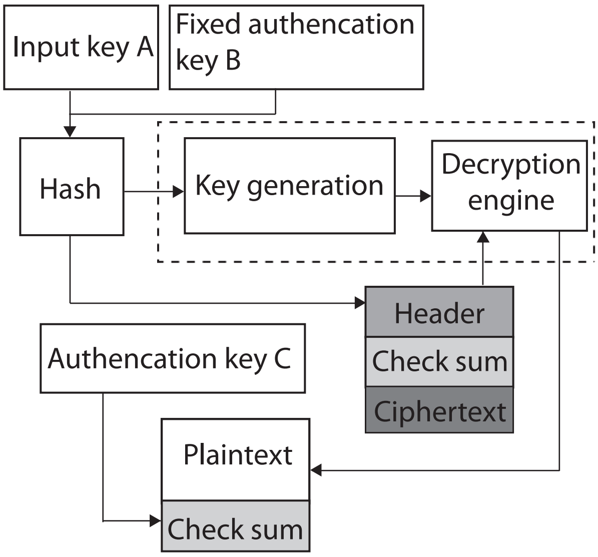
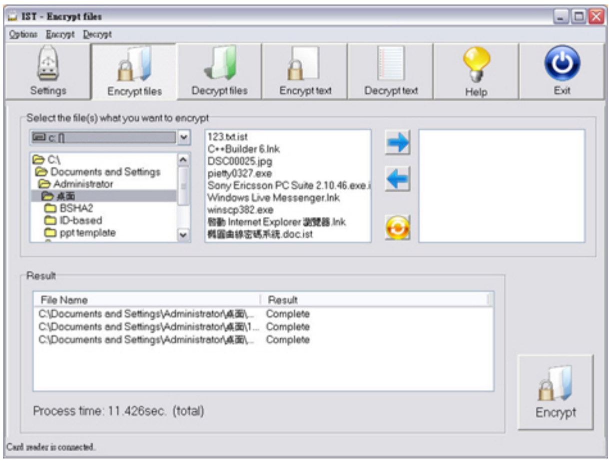


Figure 2: Concept of IST Decryption

When the software starts, the users ($A$ and $B$) should set their card reader and input the PIN of Java Card at first. If they are authenticated via Java Card, the software allows them to input their partner's ID information for preparing to encrypt/decrypt. Otherwise, the user who can't input PIN correctly is regarded as illegal.



Select the file(s) what you want to encrypt

c: []

C:\
Documents and Settings
Administrator
桌面
BSHA2
ID-based
ppt template

123.txt.ist
C++Builder 6.lnk
DSC00025.jpg
pietty0327.exe
Sony Ericsson PC Suite 2.10.46.exe.i
Windows Live Messenger.lnk
winscp382.exe
啟動 Internet Explorer 瀏覽器.lnk
橢圓曲線密碼系統.doc.ist

Result

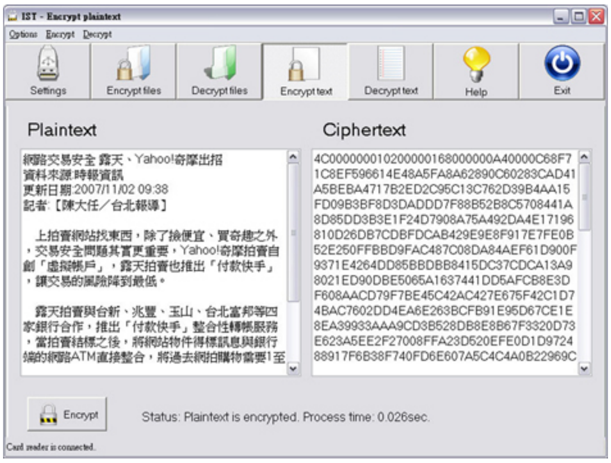
| File Name | Result |
|---|---|
| C:\Documents and Settings\Administrator\桌面\... | Complete |
| C:\Documents and Settings\Administrator\桌面\1... | Complete |
| C:\Documents and Settings\Administrator\桌面\... | Complete |

Process time: 11.426sec. (total)

Card reader is connected.

Figure 3: Encrypting batch of files

After all settings are completed, this software could retrieve fixed authentication *keyA* from Java Card. The system bundles fixed *keyA* and *keyB* which is based on receiver's ID for $H(ID(A), ID(B))$ to generate the secret key. This software accepts two kinds of plaintext: $A$ can select multiple files for encryption as Figure 3; or he can input what he want



Plaintext

網路交易安全 露天、Yahoo!奇摩出招
資料來源:時報資訊
更新日期:2007/11/02 09:38
記者:【陳大任／台北報導】

　上拍賣網站找東西，除了撿便宜、買奇趣之外
，交易安全問題其實更重要，Yahoo!奇摩拍賣自
創「虛擬帳戶」，露天拍賣也推出「付款快手」
，讓交易的風險降到最低。

　露天拍賣與台新、兆豐、玉山、台北富邦等四
家銀行合作，推出「付款快手」整合性轉帳服務
，當拍賣結標之後，將網站物件得標訊息與銀行
端的網路ATM直接整合，將過去網拍購物需要1至

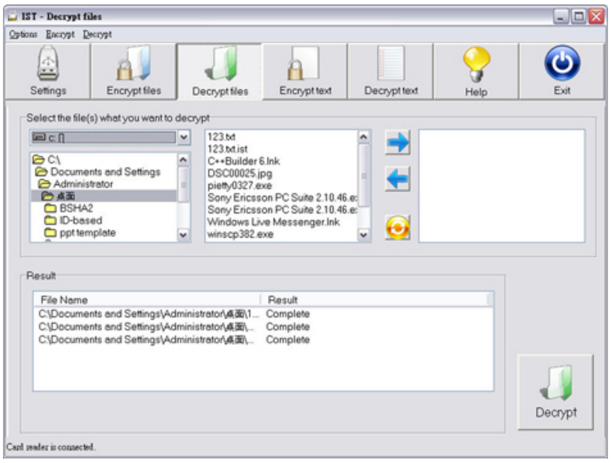
Ciphertext

```
4C000000010200000168000000A40000C68F7
1C8EF596614E48A5FA8A62890C60283CAD41
A5BEBA4717B2ED2C95C13C762D39B4AA15
FD09B3BF8D3DADDD7F88B52B8C5708441A
8D85DD3B3E1F24D7908A75A492DA4E17196
810D26DB7CDBFDCAB429E9E8F917E7FE0B
52E250FFBBD9FAC487C08DA84AEF61D900F
9371E4264DD85BBDBB8415DC37CDCA13A9
8021ED90DBE5065A1637441DD5AFCB8E3D
F608AACD79F7BE45C42AC427E675F42C1D7
4BAC7602DD4EA6E263BCFB91E95D67CE1E
8EA39933AAA9CD3B528DB8E8B67F3320D73
E623A5EE2F27008FFA23D520EFE0D1D9724
88917F6B38F740FD6E607A5C4C4A0B22969C
```

Status: Plaintext is encrypted. Process time: 0.026sec.

Card reader is connected.

Figure 4: Encrypting the text which user entered



Select the file(s) what you want to decrypt

c: []

C:\
Documents and Settings
Administrator
桌面
BSHA2
ID-based
ppt template

123.txt
123.txt.ist
C++Builder 6.lnk
DSC00025.jpg
pietty0327.exe
Sony Ericsson PC Suite 2.10.46.e:
Sony Ericsson PC Suite 2.10.46.e:
Windows Live Messenger.lnk
winscp382.exe

Result

| File Name | Result |
|---|---|
| C:\Documents and Settings\Administrator\桌面\1... | Complete |
| C:\Documents and Settings\Administrator\桌面\... | Complete |
| C:\Documents and Settings\Administrator\桌面\... | Complete |

Card reader is connected.

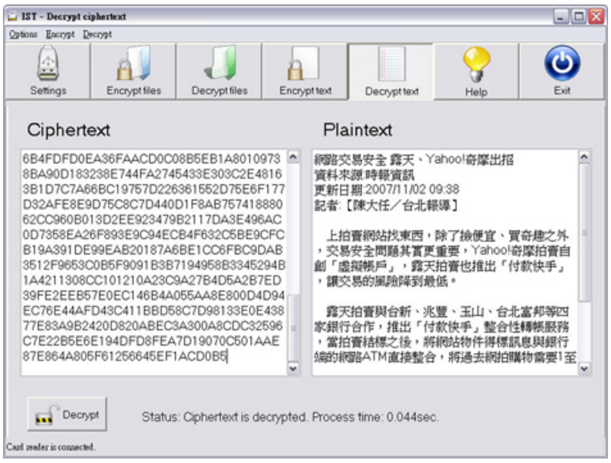
Figure 5: Decrypting batch of files

to encrypt just like Figure 4. While $A$ hits the "Encrypt" button and subsequently the files he selected or the text he inputted are ciphered. Finally, the system appends a fixed string $C$ which takes for checking decryption whether ciphertext is decrypt successfully, and suffixes a header which value is $H(ID(A), ID(B))$ to confirm the user who wants to decrypt the ciphertext is legitimate.

When $A$ sends ciphertext including the header and checksum to $B$, $B$ could choose to use files encryption (the screenshot shown as Figure 5) or text encryption (see Figure 6) up to the situation. Checking $B$ to verify the result of hashing fixed $keyB$ and input $keyA$ is necessary before decrypt the file or text. As the check is correct, the file/text decrypts for plaintext. Then the system checks the checksum $C$ in order to make sure of the integrity of plaintext.

Table 1: Experimental Results

| | | Process Time | |
|---|---|---|---|
| File Name | Size | Encryption | Decryption |
| file A | 783 KB | 0.165 sec. | 0.107 sec. |
| file B | 474 MB | 91.716 sec. | 73.053 sec. |



Ciphertext

```
6B4FDFD0EA36FAACD0C08B5EB1A8010973
8BA90D183238E744FA2745433E303C2E4816
3B1D7C7A66BC19757D226361552D75E6F177
D32AFE8E9D75C8C7D440D1F8AB757418880
62CC960B013D2EE923479B2117DA3E496AC
0D7358EA26F893E9C94ECB4F632C5BE9CFC
B19A391DE99EAB20187A6BE1CC6FBC9DAB
3512F9653C0B5F9091B3B7194958B3345294B
1A4211308CC101210A23C9A27B4D5A2B7ED
39FE2EEB57E0EC146B4A055AA8E800D4D94
EC76E44AFD43C411BBD58C7D98133E0E438
77E83A9B2420D820ABEC3A300A8CDC32596
C7E22B5E6E194DFD8FEA7D19070C501AAE
87E864A805F61256645EF1ACD0B5
```

Plaintext

網路交易安全 露天、Yahoo!奇摩出招
資料來源:時報資訊
更新日期:2007/11/02 09:38
記者:【陳大任／台北報導】

　上拍賣網站找東西，除了撿便宜、買奇趣之外
，交易安全問題其實更重要，Yahoo!奇摩拍賣自
創「虛擬帳戶」，露天拍賣也推出「付款快手」
，讓交易的風險降到最低。

　露天拍賣與台新、兆豐、玉山、台北富邦等四
家銀行合作，推出「付款快手」整合性轉帳服務
，當拍賣結標之後，將網站物件得標訊息與銀行
端的網路ATM直接整合，將過去網拍購物需要1至

Status: Ciphertext is decrypted. Process time: 0.044sec.

Card reader is connected.

Figure 6: Decrypting the text which user entered

The results of our implementation are shown as Table 1. We choose two files for testing, and the process time of encryption and decryption are reasonable.

## 4 Conclusion

There are three mainly kinds of cryptographic attacks [9]: the first is "cipher text-only attack," which means cryptanalysts steal ciphertext and find the rule of substitution out so that they can translate it into plaintext; the second trick is named "plaintext attack," cryptanalysts acquire plaintext and ciphertext at the same time, and then try corresponding to each other; and the third "brute force attack" is exhaustive calculation until find out the plaintext.

In this paper, the ciphertext which is generated by this implement is strong enough to resist cipher text-only attack because of it's confusion. Furthermore, we implement a ID-based encryption tool with Java Card and it can avoid brute force attack from the protection of PIN code. Finally, We leave user's identity information in Java Card therefore the user who use this tool does not require memorizing additional information, and it's not necessary to set PKI to manage users' identity and keys in our implementation thus could reduce the cost.

## References

[1] H. Fukaya and K. Sakurai, "Realization of the ID-based Encryption Scheme Based on Symmetric-key Technique with Device Characteristic Value," *IEICE Technical Report*, vol. 105, no. 662, pp. 97–102, 2006.

[2] A. Shamir, "Identity-Based Cryptosystems and Signature Schemes," in *Proceedings of CRYPTO 84 on Advances in cryptology*, pp. 47–53, 1985.

[3] Y. Desmedt and J.-J. Quisquater, "Public-key Systems Based on the Difficulty of Tampering (Is there a difference between DES and RSA?)," in *Proceedings of CRYPTO 86 on Advances in cryptology*, pp. 111–117, 1987.

[4] K. Imamoto, H. Fukaya, and K. Sakurai, "Cryptographic Infrastructures based on a Unique Device with

Tamper-Resistant," in *1st International Conference on Information Security and Computer Forensics*, pp. 41–47, 2006.

[5] H. Fukaya and K. Sakurai, "A Design of DRM Systems with Hardware-Based Authentication," *CSSIPSJ Research Report*, vol. 2006, no. 81, pp. 447–452, 2006.

[6] W. Rankl and W. Effing, *Smart Card Handbook*, 3rd ed. Wiley, 2003.

[7] IBM BlueZ. (2007, Sep 7). *JCOP30 Technical Brief* [Online]. Available FTP: ftp.software.ibm.com Directory: software/pervasive/info File: JCOP30Brief.pdf.

[8] Z. Chen, *Java Card Technology for Smart Cards*, Addison-Wesley, 2000.

[9] J. Slay and A. Koronios, *Information Technology Security and Risk Management*, Wiley, 2006.