行政院國家科學委員會專題研究計畫　期中進度報告

行動代理人環境之入侵偵測系統之設計與實作(1/2)

計畫類別：個別型計畫
計畫編號：NSC92-2213-E-009-091-
執行期間：92 年 08 月 01 日至 93 年 07 月 31 日
執行單位：國立交通大學資訊工程學系

計畫主持人：葉義雄
共同主持人：林祝興

報告類型：精簡報告

處理方式：本計畫可公開查詢

中　華　民　國 93 年 8 月 6 日

行政院國家科學委員會補助專題研究計畫成果報告

行動代理人環境之入侵偵測系統之設計與實作

計畫類別：ˇ個別型計畫　　□ 整合型計畫
計畫編號：NSC 91-2213-E-009–084-
執行期間：　92 年　8 月　1 日至　93 年　7 月 31 日
計畫主持人：葉義雄教授
共同主持人：林祝興教授
計畫參與人員：李鎮宇、何明俞、胡家棟、王俊傑

成果報告類型(依經費核定清單規定繳交)：ˇ精簡報告　□完整報告
本成果報告包括以下應繳交之附件：
發表之論文一份

處理方式：除產學合作研究計畫、提升產業技術及人才培育研究計畫、
列管計畫及下列情形者外，得立即公開查詢
□涉及專利或其他智慧財產權，□一年□二年後可公開查詢

執行單位：國立交通大學資訊工程學系

中華民國　93 年　5 月　31 日

中文摘要：

在本報告中，提出將現今普及的可攜式行動代理人加入資料加密的功能，如此當提供可攜式行動代理人的廠商欲提供更多資訊給購買可攜式行動代理人的使用者時，可將資料經加密放於網際網路上，使用者下載下來後，經由可攜式行動代理人內建的金鑰作資訊的還原，除內建的金鑰外，使用者也可自行輸入金鑰作本地端資料的加解密用；因此除了擁有此設備及其內建金鑰的使用者，一般經由網路上獲得加密資料的使用者，無法窺視其內容。

在實現方面，我們運用目前常見的的元件，將其整合起來而具有有儲存、顯示、傳輸、加解密等基本功能的硬體，用來模擬我們所提出的應用以及一般可攜式行動代理人應有的基本功能。

關鍵字：行動代理人、加解密方法、非同步傳輸 UART

英文摘要：

In this thesis, we propose that ubiquitously and popularly portable agent nowadays include function of data cryptographic process. When vendor that provides portable agent would support more information to user that owns the portable agent, the information can be encrypted in advance and located on Internet. User who owns portable agent downloads the encrypted-data and recovery the information with embedded key corresponding the portable agent. In addition, user can also locally process data cryptography by user-defined key from external input. Except users who own the device within embedded key, end-user wouldn't decrypt ciphertext from plaintext.

In hardware implementation, we take common components and combine them to become device that has basic functions of storage, displaying, communication, and cryptographic process. The device will simulate our applied assumption and basic functions that portable agent include.

Keyword: portable agent, cryptography, asynchronous communication UART

前言：

Internet is ubiquitous and popular nowadays. Much information can be easily acquired. Here, we can image the normal situation that a consumer via unprotected channel, ie: Internet, to update or acquire important information that vendors provide. We think the model that vendors published should contains function of cryptography. In addition, the device also consists of embedded key which vendor supports. If vendors use embedded key to encrypt information, the consumer who owns the corresponding key can download and decrypt the encrypted- information from Internet. Any end-user without key corresponding the device would not observe the plaintext. We also can take user-defined key for data cryptographic. Therefore, the selection on key can be external from user-defined to local data cryptography or embedded key to decrypt ciphertext that vendor provides via Internet.

The electronic portable agent such as PDA, cellular phone etc. is more and more popular. Indeed, most of them are not used for cryptographic information. The digital context, ie E-book [1], does not hope to be read by other end-users except consumers of vendor. The application of protected-context is trend of future study.

研究目的：

We combine the techniques of mobile communication, network security and cryptography to design a secure environment for mobile agent. Therefore, we design protect the safe communication in mobile environment.

Cryptographic algorithms implemented by hardware are more physically secure, as hardware cannot easily be read or modified by an outside peeper [2][3] and we need not to memorize context of key. All we have to do is just use the key for cryptographic algorithms without recording the context of key [4]. The safety of key context may be enhanced by some procedures of key generation that vendor maybe supports.

研究方法：

Basing on the hardware with cryptographic data, we construct the architecture, as Figure 1, that included basic functions of implementing the device we considered.

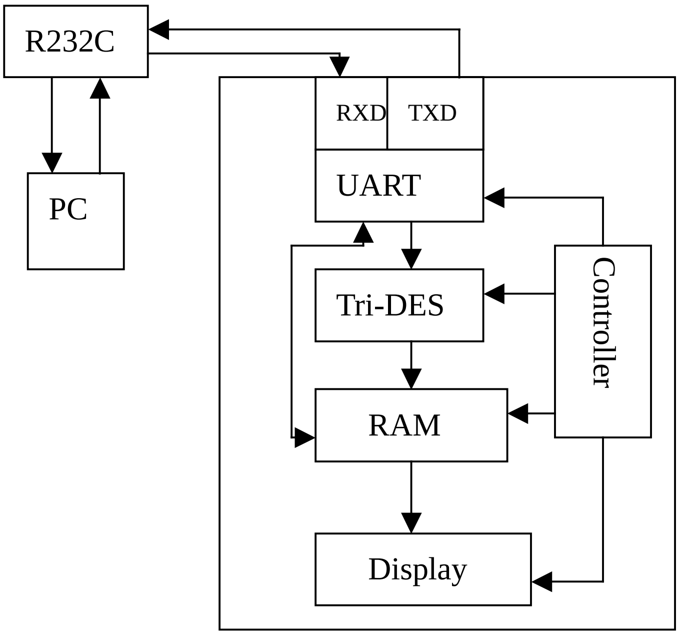

Figure 1 Designs Overview

The components of Figure 1 are describe as following:

- UART: the communication interface between receiver, device, and host-pc.
- DES^3: the process of cryptographic algorithm.
- RAM: used for storing data from UART or cryptographic process.
- Display: exhibits data that are stored in RAM.
- Controller: balance communication among components.

There are two ways to watch the plaintext: (1) the plaintext can be showed on computer via communication between device and computer. And (2) after the ciphertext is decrypted to plaintext and stored at storing component, the plaintext which read from storing device can be showed on display component in device.

結果與討論（含結論與建議）：

The system architecture is showing as following:

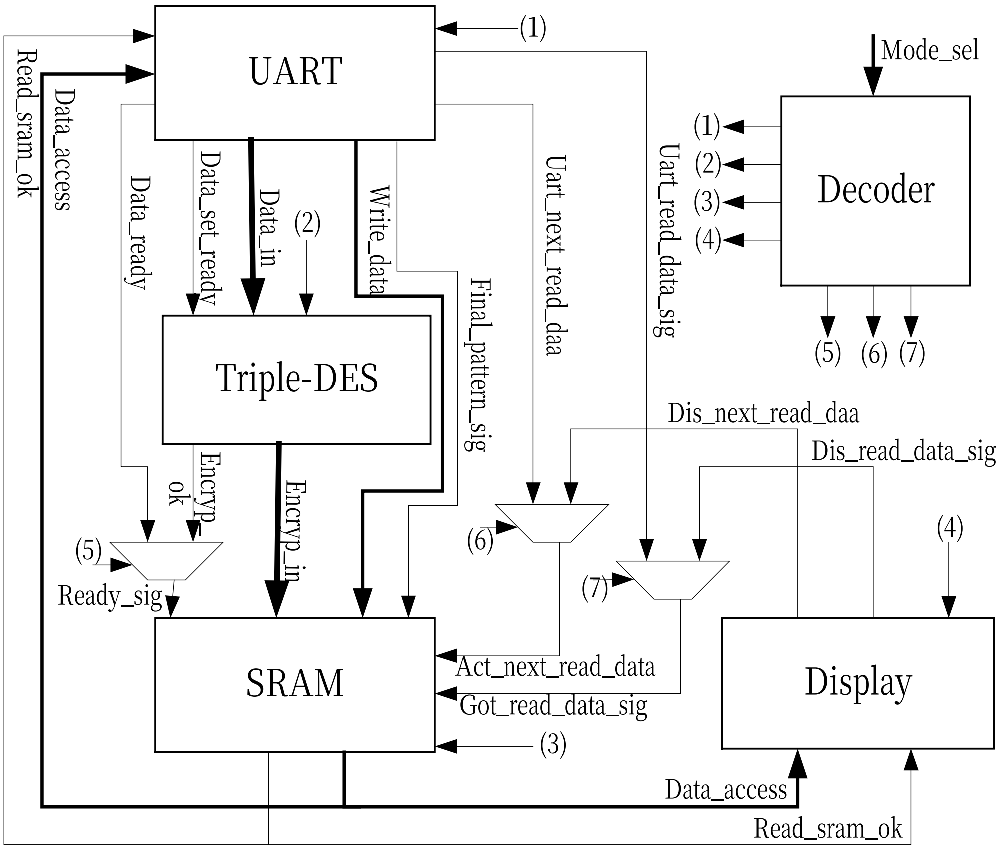

Figure 2 System Architecture

The function of device is decided by signal ‘Mode_sel’. The decode states, (1), (2), (3), and (4) in Figure 2.2 would make function corresponding component act. The decode states, (5), (6), and (7) controls communication among components.

The function in device included as following

1. UART Self testing
2. Display self testing
3. Data DES^3 process and store
4. UART receiver data and store

5. Reading data from storage and showing
6. Reading data from storage and transmitting to host-end
7. Loading key from user-defined

We constructed the device that is implemented by FPGA to verify that the entire component can work together and correctly. Here, we use EDA-tool and chip as:

Table 1 EDA tool

FPGA COMPLIER AND ANALYSIS	SYNPLIFY PRO 7.0
FPGA download for verify work	Altera Maxplus II 10.2
ALTERA FAMILY	FLEX10K

The Altera Maxplus II is used for downloading program into chip FLEX10K and verifying the device function, while Synplify Pro is used for producing netlist and feed into Maxplus II.

Table 2 Performance(Unit: MHz)

Element	UART	Displaying	Storage	Triple DES
Speed	46.94	25.83	35.46	12.85

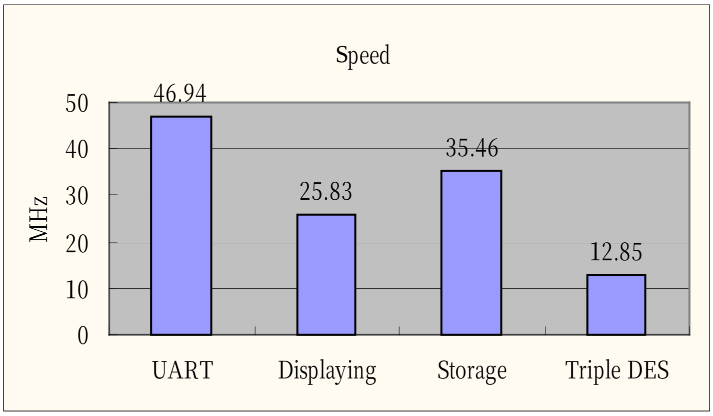

Figure 3 Performance Comparison

Table 3 Are Used (Unit: Logic Cells)

Element	UART	Displaying	Storage	Triple DES
Area	207	248	207	2,475

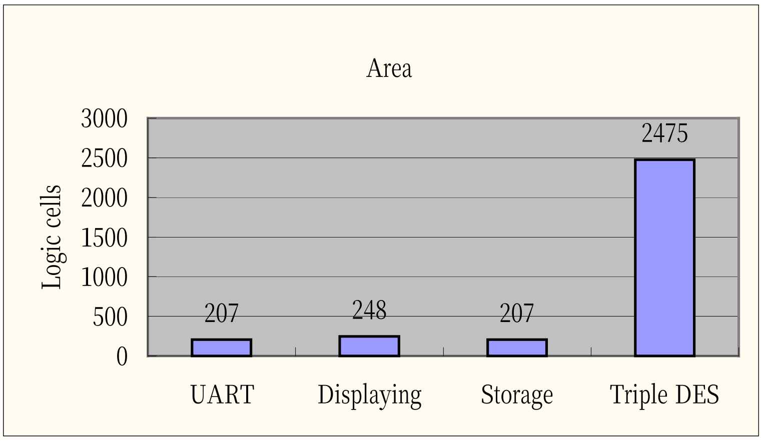

Figure 4 Area Comparison

As area view, we can see that Triple DES occupies most area than other function. Because many look-up Table, ie: P-box, S-box, E-box, FP, IP, would be implemented in single round Triple DES, we know that cost many logic cell since those look-up Tables are crated by pure flip-flop without RAM or ROM usage. The max stable transmitted-rate depends on transmitted-rate that transmitter setup.

Table 4 Throughput (Unit: BPS)

Element	UART	Displaying	Storage	Triple DES
Throughput	230,400(1)	24,390	3,125,000	1,803,013

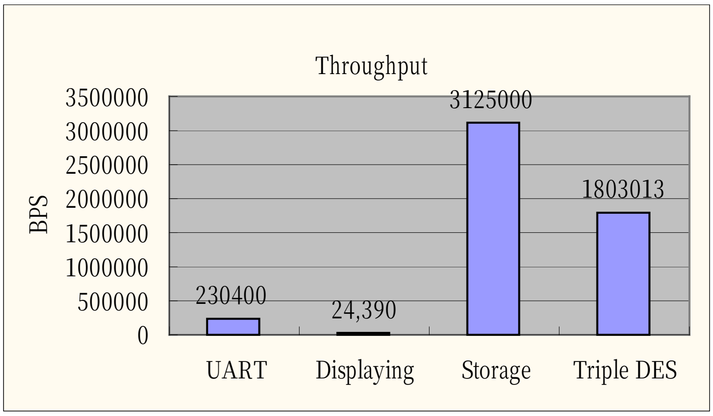

Figure 5 Throughput Comparison

The throughput is calculated by pure component alone, and thus not considered the condition of communication mechanism among component. Because of the characteristic of component, we know that device display has processed data for longer time and low throughput. The throughput in UART depends on the host-end BaudRate. As characteristic of storage component, the response time for processing data is much faster than other component. We can see the implementation result is the same as we predict before implementing.

參考文獻：

[1] Bryant, J. M., “The paperless book”, IEE Review, Vol. 41, Issue: 6, 16 Nov. 1995.

[2] R. Doud, “Hardware crypto solutions Boost VPN,” Electron. Eng. Times, pp. 57–64, Apr. 12, 1999.

[3] S. Brown and J. Rose, “FPGA and CPLD architectures: A tutorial,” IEEE Design Test Comput., vol. 13, no. 2, pp. 42–57, 1996.

[4] D. Runje and M. Kovac, “Universal strong encryption FPGA core implementation,” in Proc. Design, Automation, and Test in Europe, Paris, France, Feb. 1998, pp. 923–924.

[5] B. Schneier, Applied Cryptography, 2nd ed. New York: Wiley, 1996.

[6] Nation Institute of Standards and Technology (NIST), Data Encryption Standard (DES), National Technical Information Service, Sprinfgield, VA 22161, Oct. 1999.

[7] W. W. Peterson and E. J. Weldon, Jr., “Error-Correcting Codes,” MIT Press, Cambridge, MA, 2 edition, 1972.

[8] Axelson, Jan., “Serial port complete: programming and circuits for RS-232 and RS-485 links and networks”, Madison, WI :Lakeview Research, 1998.

[9] S. Brown and J. Rose, “FPGA and CPLD architectures: A tutorial,” IEEE Design Test Comput., vol. 13, no. 2, pp. 42–57, 1996.

[10] W. W. Peterson and E. J. Weldon, Jr., “Error-Correcting Codes,” MIT Press, Cambridge, MA, 2 edition, 1972.

[11] B. Chetwynd, “Universal block cipher module: Toward a generalized architectures for block ciphers,” Master’s thesis, ECE Dept., Worcester Polytechnic Inst., Worcester, MA, Nov. 1999.

[12] C. Phillips and K. Hodor, “Breaking the 10 k FPGA barrier calls for an ASIC-like design style,” Integrated Syst. Design, 1996.

計畫成果自評：

經由本計劃，我們除了探討了解行動代理人與入侵偵測系統相關技術，更對網路安全與密碼方法有深入的研究。進而規劃與設計相關的行動通訊與行動代理人環境以便於建立實驗系統環境。透過 UART、FPGA、RS-232 等硬體，實際建立安全的行動通訊與行動代理人環境，並測得其數據，撰寫成論文，投稿於國際期刊。

對於學術研究、國家發展及其他應用方面預期之貢獻：

1. 提供可預期未來行動代理人相關網路安全與入侵偵測技術之建立。
2. 提供可預期未來行動代理人相關網路安全與入侵偵測技術相關系統規劃與設計技術之建立。
3. 培植行動通訊之網路安全技術的研究能力。
4. 訓練行動通訊之網路安全技術相關人員。

對於參與之工作人員，預期可獲之訓練：

1. 對於行動通訊、行動代理人、網路安全與入侵偵測系統等各項相關技術瞭解與探討。
2. 對於行動通訊環境的安全系統有具體而完整的概念。
3. 對於各種行動通訊安全系統及系統整合的程式設計之磨練。
4. 對於行動通訊安全相關技術之建立。

可供推廣之研發成果資料表

˅　可申請專利　　□ 可技術移轉　　　　　　　　　　　　日期：93 年 5 月 31 日

國科會補助計畫	計畫名稱：行動代理人環境之入侵偵測系統之設計與實作 計畫主持人：葉義雄教授 計畫編號：NSC 91-2213-E-009–084-　學門領域：EA 資訊工程
技術/創作名稱	具加解密資料的應用硬體
發明人/創作人	葉義雄教授
技術說明	中文： 行動代理人環境加入資料加密的功能，如此當提供行動代理人的廠商欲提供更多資訊給購買行動代理人的使用者時，可將資料經加密放於網際網路上，使用者下載下來後，經由行動代理人內建的金鑰作資訊的還原，除內建的金鑰外，使用者也可自行輸入金鑰作本地端資料的加解密用。 英文： We propose that ubiquitously and popularly portable agent nowadays include function of data cryptographic process. When vendor that provides portable agent would support more information to user that owns the portable agent, the information can be encrypted in advance and located on Internet. User who owns portable agent downloads the encrypted-data and recovery the information with embedded key corresponding the portable agent.　In addition, user can also locally process data cryptography by user-defined key from external inputting.
可利用之產業 及 可開發之產品	Portable Agent such as PDA
技術特點	行動代理人環境加入資料加密的功能
推廣及運用的價值	可用於現今愈來愈廣泛的行動計算代理人(portable agent)，如PDA, notebook, cellular phone 等等。

※　1.每項研發成果請填寫一式二份，一份隨成果報告送繳本會，一份送　貴單位研發成果推廣單位（如技術移轉中心）。

※　2.本項研發成果若尚未申請專利，請勿揭露可申請專利之主要內容。

※　3.本表若不敷使用，請自行影印使用。