行政院國家科學委員會專題研究計畫成果報告

網際網路安全串流密碼系統之設計

Design of Secure Stream Cipher Cryptosystem on Internet

計畫編號：NSC 90-2213-E-009-143

執行期限：90 年 08 月 01 日至 91 年 07 月 31 日

主持人：陳榮傑　國立交通大學 資訊工程系

計畫參與人員：胡鈞祥　國立交通大學 資訊工程系

黃凱群　國立交通大學 資訊工程系

林志信　國立交通大學 資訊工程系

劉穎駿　國立交通大學 資訊工程系

一、中文摘要

網際網路主要特色是無往弗屆的通訊本領，運用網際網路來達成視訊會議（net meeting）、網路電話（Voice over IP，簡稱 VoIP）等即時性的通訊機制（包括語音、影像等資料），已被普遍的使用在日常生活中。所謂的網路電話，是把語音當成數據資料加以封包(packetized)，透過網路從發話端送到收話端，此種技術有下面幾樣優點：對於擁有許多子公司的大型企業，可以藉由網路電話技術減少公司間的通話費；並不需要以特定的線路（circut）經由 PBX 與收端連線；可以更有效率地運用網路頻寬，避免傳統電訊所造成的閒置浪費。目前共有 Megaco（Media Gateway Control）、Sip（Session Initiation Protocol），以及 H.323 等三種網路電話規格。

網路電話雖然便利，但它以網路作為傳輸媒介，很容易被第三者竊聽，因此在上述的三種規格中均有定義保護封包的技術如 PGP、IPSec 等，這些方式都是以塊狀密碼系統（Block Cipher System）加密資料，然而塊狀密碼系統極為複雜且耗時，將它使用在即時系統中可能造成封包傳送上的延誤。而串流密碼系統（Stream Cipher System）有別於塊狀密碼系統，是種 架構相當簡單且加密速度非常快速的密碼系統，非常適用處理即時資料，目前在無線通訊 GSM 系統中的加密演算法 A5 即是使用此種系統架構。因此，我們亦想將串流密碼系統實際應用於網路電話上，計畫將針對串流密碼系統進行研究，探討構成系統的基本組成原件線性反饋移位暫存器（linear feedback shift register）、過濾函數（filter function）、組合函數（combination function）的特性，並對平衡（Balancedness）、非線性值（Nonlinearity）、代數級數（Algebratic Degree）、相關免疫性（Correlation Immunity）與傳播特徵（Progragation Charateristics）等必備性質加以分析研究，且針對串流密碼系統的攻擊方法 B-M 演算法、相關攻擊法與最佳仿射近似攻擊法提出合理可行的防範方式，以此建構出一個安全且有效率的串流密碼系統，接著將系統實際的運用在電話網路上，並給予安全性與效率分析。

關鍵詞：網路電話、串流密碼、塊狀密碼、串流密碼、線性反饋移位暫存器、過濾函數、組合函數、記憶體、平衡、非線性值、代數級數、相關免疫性、傳播特徵

Abstract

Internet provides peoples with infinit communication. Some real time communication services through internet, such as net meeting, Voice over IP(VoIP) etc., have been frequency used in our dialy life. VoIP involves transportation of voice messages over telephone lines and internet that uses technology offers the following

advantages：Reduce the cost of voice communications, repecially for companies with multiple office locations. Eliminates the need for extra circuits for private voice traffic by connecting your PBXs to one another. Use your existing Internet bandwidth more efficiently by running voice and Internet traffic on the same circuit.Currently, Megaco（Media Gateway Control）, Sip（Session Initiation Protocol） and the H.323 are main technologies on VoIP.

Although Internet Phone is very convenient, eavesdroppers can still easily hold up packets on public internet. VoIP technologies define protocols whose security relies on block cipher systems, such as PGP, IPSec etc. Those protocols can protect packets across public internet without interception. Because block cipher systems are too complicated, they could result in delay when systems send packets. Stream cipher systems, different form block cipher systems, Those are the most important ones which feature simple structures and high-speed encryption, to deal with real-time communication services. A good example is A5 Algorithm on GSM system. Therefore, we want to use stream cipher systems on internet phone. In this proposal, we will study LFSR(Linear Feedback Shift Register), filter function, combination function, balancedness, nonlinearity, algebratic degree, correlation immunity and progragation characteristics, and find effective methods to prevent the proposals of B-M algorithm, correlation attack and best affine approximation attack, in order to establish a new theory on stream cipher stability. Eventually, we will design a simple internet phone system , and do security analysis and efficiency analysis for it.

Keywords: Internet Phone、Block Cipher、Stream Cipher、LFSR、Filter function、Combination function、Balancedness、Nonlinearity、Algebratic Degree、Correlation Immunity、Progragation Charateristics

二、緣由與目的

近年來,隨著網際網路(Internet)與行動電話(Mobile Phone)的普及，人們已經習慣將許多的資料與訊息藉由網路與無線通訊系統來相互傳遞，這不僅提供人們生活上的便利，亦促使數位化的資料與訊息得以共享；1990 年，美國伊利諾州的硬體通訊實驗室，首先運用各人電腦在網路上傳送即時的語音與影像資訊，至目前為止，這方面的技術已有了長足的進步，如視訊會議（Net Meeting）、網路電話（Voice of Internet Phone）等應用。所謂的網路電話，是把語音當成數據資料加以封包(packetized)，透過網路從發話端送到收話端，並非以傳統交換電信網路（Public Switched Telephone Network，簡稱 PSTN）回路介接（Circuit Switch）來傳送語音訊息，我們可預見未來電信成本的下降及科技的進步，電信產業將會有一番新的革命與機會產生，且可以確認的是網路電話必成未來通訊主流。它有下面幾項優點：

1. 網路電話是透過語音封包繞路(routing)建立溝通的管道，傳輸成本遠低於傳統電信產業的 PSTN 網路，因此使用者所需負擔的通話費相對的也較低。
2. PSTN 網路必須使用交換機（personal business exchange，簡稱 PBX）建立一個通話端與對會端的固定連線，而網路電話並不需要特定的路徑來傳送語音訊息。
3. 在 PSTN 網路通話的同時，這條通路是專門且持續為使用者開設的，也就是說，如果使用者停頓不出聲音，或是談話內容中停頓的時間很長，計費仍然進行，而網路電話辦法偵測此種狀態的發生，並停止傳送封包，可以更有效率地運用網路頻寬，避免傳統電訊所造成的閒置浪費。

目前網路電話個規格技術共有三種，分別為由 IETF[35]（The Internet Engineering Task Force）所制訂的 Megaco[33]（Media Gateway Control）、SIP[32]（Session Initiation Protocol），以及 ITU[36]（International Telecommunication Union）所制訂的 H.323[36]。

網路電話雖然如此的便利，但它以網路作為傳輸媒介，很容易被第三者竊聽，

因此在上述的三種規格中均有定義保護封包的技術如 Megaco 中的 IPSec[34](Internet Protocol Security）安全協定，SIP 中的 PGP（Pretty Good Privacy）加密軟體，以及 H.323 中的 H.235[36]。IPSec 協定是分屬於網路 IP 層上的安全機制，將 IP 層以上的資訊加密起來，如下所示：其中加密所採用的的系統一般為 DES、Triple DES 等。SIP 網路電話規格中定義了三種加密的方式，其一為加密整個封包的方式來保護語音訊息；其二為讓竊聽者不知道封包是由誰送給誰之加密方式；其三為讓竊聽者連封包的傳送路徑也不曉得之加密方式；這三種加密的方法都是使用 PGP 來完成。PGP 是利用所謂的公開鑰匙密碼學（public-key cryptosystem）為基礎的加密方式，此種加密系統以 RSA 為主要代表。

然而 PGP 與 IPSec 等安全機制所選用的加密方法均屬於塊狀密碼系統（Block Cipher System）的範疇內，而塊狀密碼系統極為複雜且耗時，將它使用在即時系統中可能造成封包傳送上的延誤。串流密碼系統（Stream Cipher System）有別於塊狀密碼系統，是種 架構相當簡單且加密速度非常快速的密碼系統，非常適用處理即時資料，目前在無線通訊 GSM 系統中的加密演算法 A5 與微電腦（microprocessor）上面的軟體 SOBER 即是使用此種系統架構；串流密碼系統在密碼上的應用還有 1996 年由 Anderson 及 Biham 所提出的老虎雜錯函數（Tiger hash function）與 BBS 站常用來壓縮檔案的 PKZIP 軟體中的保密方式等。加密演算法 A5 是一種鐘控串流加密系統（clock control stream cipher），一般以晶片（chip）的方式存在行動電話與基地台中；而 SOBER 則是一個比 RC4 更快的加密軟體，也常運用於行動電話上；另外老虎雜錯函數是一種類似 DES 加密系統的雜錯函數，而此函數中的 S-box 與串流密碼中的組合函數（combination function）有相當密切的關係。有鑑於串流密碼系統如此被廣泛的應用與其快速且簡單的處理即時資訊，設計一個安全且實用的串流密碼系統已是一個重要的研究課題。

三、結果與討論

本計畫主要是研究有關串流密法的理論和實際的應用，依據安全與實用的因素去改良與設計出更好的串流密法系統。這些研究需有數論、密法學、網路安全、統計理論以及密碼系統設計等方面的知識加以整合。

串流密碼的核心元件通常是布林函數，所以布林函數在密碼學上的特性一直為研究的範疇，在此之前已經有許多學者提出相關的標準，用來檢測布林函數的密碼特性，其中我們將針對下面的標準來討論：(1)調和性 (2)代數冪級數 (3)非線性 (4)遺傳特性 (5)相關免疫性。

我們首先利用布林函數經華勒式-哈達瑪轉換在頻譜上的結果來分析，並研究及回顧目前對於這些密碼檢測標準間關係的研究，透過瞭解其相對關係，我們提出兩個同時考慮遺傳特性及相關免疫性標準下的布林函數建構方式。

據此，我們完成本計畫的目的，並針對串流密碼理論核心部分-布林函數提供兩種符合安全分析及檢測要求的建構方式。

四、計畫成果自評

依上節所提之結果，我們達成了此計畫預期的目標。此計畫的研究結果不僅針對串流密碼的核心技術提供理論上的安全檢測標準，更具體提出幾個建構的方向，未來不僅可以經由此結果設計出更安全的串流密碼系統，更可以將其應用在網際網路的通訊上。成果極具有學術上的價值與貢獻，相當適合學術期刊上發表。

五、參考文獻

[1] Zong-duo Dai, “Proof of Ruppel’s linear complexity conjecture,” submitted for publication to the IEEE Trans. on Info. Theory.

[2] E. P. Dawson, Design and cryptanalysis of symmetric ciphers, PhD Thesis, Queensland University of Technology, 1991.

[3] R. G. Gallager, Low-Density Parity-Check Codes, MIT Press, Cambridge, MA, 1963.

[4] S. W. Golomb, “Shift register sequences,” Holden-Day, San Francisco Calif., 1967.

[5] E. J. Groth, “Generation of binary sequences with

controllable complexity," IEEE Trans. on Info. Theory, Vol. IT-17, May 1971.
[6] F. G. Gustavson, "Analysis of the Berlekamp-Massey linear feedback shift-register synthesis algorithm," IBM J. Res. Develop., 1976.
[7] T. Herlestam, "On the complexity of functions of linear shift register sequences," Int. Symp. on Info. Th., LesArc, France, 1982.
[8] E. L. Key, "An analysis of the structures and complexity of nonlinear binary sequence generator," IEEE Trans. on Info. Theory, Vol. IT-22, Nov. 1976.
[9] C. H. Lin, S. C. Tsai and R. J. Chen, Spectral Analysis of Boolean Functions for Cryptographic Criteria, Master thesis, the National Chiao Tung University, 2002.
[10] C. H. Lin, S. C. Tsai and R. J. Chen, "Two New Constructions of Resilient Boolean Functions Satisfying Propagation Criterion," ICS 2002, to be accepted.
[11] J. L. Massey, "Shift-register synthesis and BCH decoding," IEEE Trans. Inform. Theroy, vol. IT-15, pp. 122-127, Jan. 1969
[12] A. Lempel and J. Ziv, "On the complexity of finite sequences," IEEE Trans. on Info. Theory, IT-22, Jan. 1976.
[13] W. Meier and O. Staffelbach, "Fast correlation attacks on stream ciphers," Advances in Cryptology—EUROCRYPT'88, Lecture Notes in Computer Science, Vol. 330, Springer-Verlag, 1988, pp. 301-314.
[14] W. Meier and O. Staffelbach, "Fast correlation attacks on certain stream ciphers," Journal of Cryptology, Vol. 1, 1989, pp. 159-176.
[15] M. Mihaljevic and J. Golic, "A fast iterative algorithm for a shift register initial state reconstruction given the noisy output sequence," Advances in Cryptology—AUSCRYPT'90, Lecture Notes in Computer Science, Vol. 453, Springer-Verlag, 1990, pp. 165-175.
[16] W. Penzhorn, "Correlation attacks on stream ciphers: Computing low weight parity checks based on error correcting codes," Fast Software Encryption, FSE'96, Lecture Notes in Computer Science, Vol. 1039, Springer-Verlag, 1996, pp. 159-172.
[17] K. C. Zeng, M. Q. Huang, and T. R. N. Rao, "An improved linear syndrome algorithm in cryptanalysis with applications," Proc. Crypto'90, Lecture Notes in Computer Science, Springer-Verlag.
[18] R.Forre, The strict avalanche critrion, "spectral properties of Boolean functions and on extended definition," Advances in cryptoloty-Crypt'88, Springer-Verlag, 1990, 450-468.
[19] B.Preneel etc, "Propagation characteristics of Boolean functions," Advances in Cryptoloty-Crypt'90, Springer-Verlag, 1991, 161-173.
[20] A.F.Webster, S.E.Tavares, "On the design of S-boxes," Advances in Cryptoloty-Crypt'85, Springer-Verlag, 1986, 523-534.
[21] P.Camion, etc al., "On correlation-immune functions," Advances in Cryptoloty-Crypt'91, Springer-Verlag, 1991, 86-100.
[22] J.Seberry, etal., "Construction and non-linearity of Correlation-immune functions," Advances in Cryptoloty, Proc. Eurocrypt'93, Springer-Verlag, 1993.
[23] J.Seberry, etal., "Non-linearity balanced Boolean functions and their propagation characteristic," Advances in Cryptoloty, Crypt ' 93, Springer-Verlag, 1994, Berlin, 6-12.
[24] C.Mitchell, "Enumerating Boolean functions of cryptographic signigicance, J. of Cryptology," 2(3)：1990, 155-170.

行政院國家科學委員會補助專題研究計畫成果報告

※※※※※※※※※※※※※※※※※※※※※※※※※※
※　　　　　　　　　　　　　　　　　　　　　　　　※
※　　　　網際網路安全串流密碼系統之設計　　　　※
※　　　　　　　　　　　　　　　　　　　　　　　　※
※※※※※※※※※※※※※※※※※※※※※※※※※※

計畫類別：☑個別型計畫　　□整合型計畫

計畫編號：NSC 90－2213－E－009－143－

執行期間：90 年 08 月 01 日至 91 年 07 月 31 日

計畫主持人：陳榮傑　國立交通大學 資訊工程系

共同主持人：

計畫參與人員：胡鈞祥　國立交通大學 資訊工程系

黃凱群　國立交通大學 資訊工程系

林志信　國立交通大學 資訊工程系

劉穎駿　國立交通大學 資訊工程系

本成果報告包括以下應繳交之附件：

□赴國外出差或研習心得報告一份

□赴大陸地區出差或研習心得報告一份

□出席國際學術會議心得報告及發表之論文各一份

□國際合作研究計畫國外研究報告書一份

執行單位：國立交通大學 資訊工程系

中　華　民　國　91 年　10 月　31 日