"責任分配"概念下的金匙信託加密系統
A Key Escrow Encryption System with the Concept of Duties-Separation

詹進科、陳育毅
Jinn-Ke Jan and Yu-Yii Chen

中興大學應用數學研究所
Institute of Applied Mathematics,
National Chung Hsing University,
jkjan@amath.nchu.edu.tw

中文摘要

由於「金匙信託加密系統」是美國政府近年來在資訊安全上的主要政策[Den1,Den2,DB,DS,Gan1,Pow,WLED]，其將主導未來的加密系統之應用。所以在這篇文章中，吾人針對金匙信託加密系統設計上的缺失加以修正，擴大其應用層面，並解決了配合使用的問題、監控對象的確認、金匙託管的安全、監控行為的限制、及責作上的問題。

關鍵字：金匙信託加密系統

Abstract

Key-escrow encryption system is the main policy of information security of United Ststes government within these years[Den1,Den2,DB,DS,Gan1,Pow,WLEB]. Due to this reasearch might impact the applications of cryptography in the near future, we propose this paper for settling down all possible pitfalls of key-escrow encryption system including the issues on compliance, identification, wiretapping limitations, and key managements. Hopefully, our proposal might contribute to the main goal of practicability.

Keywords：Key Escrow Encryption System

§1. 重點介紹

密碼學可說是一種古老的藝術。在凱撒大帝的時代，就曾經對戰爭中的通訊以移位代換字母的方法加密之，以確保其機密性。到了現代，雖然網路上的通訊早已數位化成0與1的資料，但其保密的需求依然存在。

在1970年代時期，通訊的保密都是使用「單一金匙加密系統」來達成(最有名的就是DES系統[*DES*])，其設計上都是只用一個相同的金匙來完成加密與解密的動作，而其缺點也就在於通訊的雙方如何確保事前能夠安全地協調出共同的金匙。

到了1976年，Whitfield Diffie與Martin Hellman發表了「公開金匙加密系統」的概念[*DH*]。在這個概念中，認為可以將加密系統的金匙以成對的方式設計，一個為公開金匙，一個為秘密金匙。當某人要傳送訊息給對方之前，先以對方的公開金匙將訊息加密，然後就只有知道秘密金匙的對方才可以解出該訊息。如此即可確保通訊的機密性，而且也不再需要事先協調共同金匙的過程。

當此概念被提出後，Ron Rivest, Adi Shamir, Len Adlemen三人即很快地設計出符合此一精神的加密系統(即現今所稱的RSA系統[*RSA*])。

雖然是為了資訊安全的理由而對通訊資料加密，但相對地，不法份子也可利用其來反制政府的監控，藉由密碼系統之協助，可以對其非法行為進行秘密通訊而逍遙法外。因此，「金匙信託加密系統」的概念便應運而生。所謂的金匙信託加密系統就是允許在"特定情況下"，由特定單位在可信賴金匙託管中心的協助下，能夠將通訊密文解開，以便加以監控。這樣的系統設計必須提供足夠的安全通訊，但在必要時又能讓政府進行監控。

在1993年4月16日，美國總統柯林頓頒佈通過第一項有關「金匙信託加密系統」(Key-Escrow Encryption System, 簡稱KES)的法案[*WH1*]。在該法案中，宣佈採用Clipper晶片為先期導入之標準，作為美國政府對金匙信託加密系統所跨出的第一步。到了1994年2月，美國政府更進一步公佈信託加密的標準(Escrowed Encryption Standard, 簡稱EES)[*NIST1*]，其以Clipper晶片為基礎而制訂出來的一個廣義規範，作為美國聯邦在未來的語音、傳真、電子資料...等通訊上的一個資訊處理準則。它提供對具有敏感性但卻非機密性之通訊的一個重要標準，讓民眾能在獲得方便的私密性通訊外，政府也能對從事非法活動的嫌疑者進行監控，期使人民的隱私權與政府維護治安的公權力得以平衡。

目前，有關金匙信託加密系統之設計，已有許多研究及產品問世[*BELW,BKOSW,Cae,Des1,Des2,FMW,FY2,Gan2,HD,KL1,KL2,LWY,Mad,Mah,Mic,MS,Ne,WB,WLEBB*]，但總是無法在安全性方面達成滿意之成果[*Bla,FY1*]。所以，在吾人的研究中將針對各種缺失的修正方向加以說明與改進。

§2. 吾人提出的方法

在吾人的方法中，系統之組成為：

- 第一金匙信託中心：負責通訊設備之註冊及金匙託管。
- 第二金匙信託中心：負責個人之帳號申請及金匙託管。
- 執法單位：負責執行監聽。
- 司法機關：負責授權監聽。
- 通訊設備：可供通訊的軟體與硬體。
- 通訊雙方：持有個人IC卡的使用者。

接下來，就針對金匙信託加密系統中，有關通訊雙方、金匙信託中心、及執法單位的互動關係分成五個部份敘述。

一. 通訊設備之註冊及金匙託管流程

Step 1： 通訊設備在開始啟用之前，必須向第一金匙信託中心註冊。

Step 2： 第一金匙信託中心會對每一個註冊的通訊設備選定兩個大質數p_S及q_S，並求出其乘積$n_S=p_S \cdot q_S$(且其值必須大於一特定臨界值h)。同時，設定其秘密金匙d_S，並求出其公開金匙e_S，使得其符合：

$$e_S \cdot d_S = 1 \bmod (p_S-1)(q_S-1) .$$

然後，將(e_S,d_S,n_S)燒錄在通訊設備上，並將(e_S,d_S,p_S,q_S)記錄下來。

二. 個人之帳號申請及金匙託管流程

Step 1： 使用者持IC卡向第二金匙信託中心辦理登記，第二金匙信託中心核對其IC卡上的身份資料及聯合發卡中心簽章，確認是否無誤。

Step 2： 第二金匙信託中心為其選定兩個大質數p_i及q_i，並求出其乘積$n_i=p_i \cdot q_i$(且其值必須小於一特定臨界值h)。同時，設定其秘密金匙d_i，並求出其公開金匙e_i，使得其符合：

$$e_i \cdot d_i = 1 \bmod (p_i-1)(q_i-1) .$$

然後，在使用者IC卡上開檔存入(e_i,d_i,n_i)，並將(e_i,d_i,p_i,q_i)記錄下來。

三. 送訊方的作業程序

Step 1： 使用者將個人的IC卡置入任一通訊設備，通訊設備便在$[1,n_i-1]$的範圍內隨機產生一個亂數Υ，並計算出：

$$cm = \Upsilon^{e_i} \bmod n_i .$$

cm是用來要求使用者證明其身份的一個質問訊息(Challenge Message)。

Step 2： 於是，使用者針對通訊設備的質問訊息計算出：

$$rm = cm^{d_i} \bmod n_i .$$

然後，將rm送交通訊設備。

Step 3： 通訊設備以IC卡所回應的rm對照原Υ值：

$$rm \stackrel{?}{\equiv} \Upsilon .$$

如果無誤，則代表該使用者使用了正確的d_i，其身份無誤。

Step 4： 於是，通訊設備要求使用者將通訊雙方事先協議好的通訊金匙ck輸入，通訊設備便會對通訊內容m以特定加密函數$E()$加密為密文c：

$$c = E_{ck}(m) .$$

Step 5： 為了要讓執法單位能夠在監聽過程中解得通訊內容，因此通訊設備要將該通訊金匙ck隱含其中。於是，通訊設備以其公開金匙e_S及使用者的公開金匙e_i，配合通訊日期$date$，透過下列的計算將通訊金匙ck隱含於eck之中：

$$eck = (ck^{e_i \cdot date} \bmod n_i)^{e_S \cdot date} \bmod n_S .$$

Step 6： 同時，為了確保通訊的完整性與安全性，通訊設備更進一步計算出兩個檢查值ea_1、ea_2。其中，將送訊方的現在時刻t，以通訊設備的秘密金匙d_S，加密為ea_1：

$$ea_1 = t^{d_S} \bmod n_S .$$

另外，將使用者公開金匙e_i、通訊設備公開金匙e_S、通訊密文c、通訊金匙ck及其加密值eck、及前述檢查值ea_1，以特定的單向赫序函數$f()$計算成介於$[1,n_S-1]$之值，並以通訊設備的秘密金匙d_S，加密為ea_2：

$$ea_2 = f(e_i,e_S,c,ck,eck,ea_1)^{d_S} \bmod n_S .$$

Step 7： 最後，將上述附加資訊組成LEAF $=(eck,e_i,e_S,ea_1,ea_2)$，將$(LEAF,c)$傳送給收訊方。

四. 收訊方的作業程序

Step 1： 首先，收訊方的通訊設備同樣會要求使用者將通訊雙方事先協議好的通訊金匙ck輸入。

Step 2： 不過，通訊設備在解出通訊明文之前，必須先核對檢查值以確保通訊的完整性與安全性。於是，以檢查值ea_1及傳送端的通訊設備公開金匙e_S，解出其傳送時間t：

$$\begin{aligned} & ea_1^{e_S} \bmod n_S \\ &= t^{d_S \cdot e_S} \bmod n_S \\ &= t . \end{aligned}$$

然後，比較其與收訊方的現在時刻t'之時差是否在規定的有限值ξ內。

$$t' - t \stackrel{?}{\leqq} \xi .$$

如果是在合理的時限內，則進一步以檢查值ea_2及送訊方的通訊設備公開金匙e_S，解出比較其值與$f(e_i,e_S,c,ck,eck,ea_1)$結果相符否：

$$f(e_i,e_S,c,ck,eck,ea_1) \stackrel{?}{\equiv} ea_2^{e_S} \bmod n_S .$$

如此即能確認LEAF與密文c的關聯性，確保通訊的完整性。

Step 3： 在確保通訊完整性與安全性的情況下，收訊方的通訊設備才會依使用者輸入的通訊金匙ck，以特定解密函數$D()$將密文c解密得出明文m：

$$m = D_{ck}(c) .$$

五. 通訊的監控程序

Step 1： 執法單位向司法機關提出申請，針對特定使用者e_i、在特定通訊設備e_S、及特定日期$date$的監聽授權。

Step 2： 第一金匙信託中心即根據授權憑證，依其通訊設備公開金匙e_S查出對應之p_S、q_S，求出符合下列公式的α值：

$$\alpha \cdot date = 1 \bmod (p_S-1)(q_S-1) .$$

再結合其託管金匙d_S，計算出部份解密金匙d_L如下：

$$d_I = d_S \cdot \alpha \bmod (p_S-1)(q_S-1) .$$

然後將此部份解密金匙d_I交予執法單位。

Step 3：同樣的，第二金匙信託中心根據授權憑證，依其監聽對象的公開金匙e_i查出對應之p_i、q_i，求出符合下列公式的β值：

$$\beta \cdot date = 1 \bmod (p_i-1)(q_i-1) .$$

再結合其託管金匙d_i，計算出部份解密金匙d_{II}如下：

$$d_{II} = d_i \cdot \beta \bmod (p_i-1)(q_i-1) .$$

然後將此部份解密金匙d_{II}交予執法單位。

Step 4：於是，執法單位即可以此二金匙d_I、d_{II}，配合其監聽通訊中的eck解得其通訊金匙ck：

$$\begin{aligned}&(eck^{d_I} \bmod n_S)^{d_{II}} \bmod n_i \\ &= (ck^{e_i \cdot d_i \cdot \beta \cdot date} \bmod n_i)^{e_S \cdot d_S \cdot \alpha \cdot date} \bmod n_S \\ &= ck .\end{aligned}$$

然後使用此通訊金匙ck，以特定解密函數$D()$將密文c解密，即可得出明文m：

$$m = D_{ck}(c) .$$

§3. 安全性與實用性之分析

在這個部份，將討論下列有關吾人所提出的金匙信託加密系統之安全性與實用性問題。

一．人們配合使用的問題(Compliance)

就配合使用的這個問題來說，可分為兩個層次討論：就技術層次而言，金匙信託加密系統的設計上，如何令參與的使用者能被監聽而無法逃避。就市場層次而言，一個金匙信託加密系統開發完成後，要如何才能吸引人們加以使用？

就技術層次來說，在吾人的方法中，為了確保通訊的完整性，避免送訊方除去LEAF資料而規避執法單位的監控，送訊方的通訊設備會在通訊內容中附上兩個檢查值ea_1、ea_2。

$$ea_1 = t^{d_1} \bmod n_S ,$$

$$ea_2 = f(e_i,e_S,c,ck,eck,ea_1)^{d_2} \bmod n_S .$$

而收訊方的通訊設備在解出通訊明文之前，會先核對檢查值。其中，以ea_1檢查LEAF的時效性(比較其與接收端的現在時刻t'之時差是否在規定的有限值ξ內)：

$$\begin{aligned}&ea_1^{e_2} \bmod n_S \\ &= t^{d_1 \cdot e_2} \bmod n_S \\ &= t .\end{aligned}$$

$$t' - t \overset{?}{\leqq} \xi .$$

然後，以ea_2檢查LEAF與密文c的關聯性：

$$f(e_i,e_S,c,ck,eck,ea_1) \overset{?}{\equiv} ea_2^{e_2} \bmod n_S .$$

所以，送訊方如欲除去LEAF資料而規避執法單位的監控，那麼將因為無法通過收訊方通訊設備的檢查而使用者無從得知其通訊明文。

更進一步來說，LEAF資料如果有可能遭到竄改而仍然通過收訊方通訊設備的檢查，執法單位便無法從偽造的LEAF中取得正確的通訊金匙，進而無法解得正確的通訊內容。就這方面來看，吾人方法中的LEAF=(eck,e_i,e_S,ea_1,ea_2)，其中隱含通訊金匙的eck、送訊方使用者公開金匙e_i、及通訊設備公開金匙e_S都有可能被意圖竄改，導致執法單位無法解得真正的通訊金匙ck，進而無法對監聽之通訊解得正確明文。然而，除非能夠同時偽造出對應之檢查值ea_2，才能順利通過收訊方通訊設備對ea_2之檢查並進而解得明文。不然，單單竄改eck、e_i、e_S是無法達成通訊之目的。但是，這在送訊方通訊設備的秘密金匙d_S不公開的情況下，要偽造出適當的檢查值ea_2，將是一件非常難的事，因為其相當於解factoring large numbers問題。

尤其是，吾人方法中的LEAF具有時效性，其隱含於檢查值ea_1之中。同樣在送訊方通訊設備的秘密金匙d_S不公開的情況下，要偽造出適當的檢查值ea_1也是非常困難。如此一來，要在合理的時限內竄改LEAF資料，而又能通過收訊方通訊設備的檢查，其機率是微乎其微!

除了技術面的探討外，就市場層面來說，如何提高人們的使用意願，才是金匙信託加密系統能否順利推展的重要因素。換句話說，在金匙信託加密系統中必須具備有益於使用者的功能而不是完全以監控為主要目的，如此才能吸引人們加以使用。

企業在安全的考量下，通常會令員工將每份文件加密存檔。然而，在加密金匙是由員工自由選擇的情況下，一旦員工忘記加密金匙，或是員工已經離職，那麼其加密的文件將難以還原。所以，如果採用金匙信託加密系統，則可讓員工或企業主管在必要時將加密的文件還原。而吾人方法中的各個角色很容易轉換到企業體系的運作，以符合這樣的商業應用。

- 在一個企業中，資訊室負責管理所有相關之電腦設施，非常適合扮演第一金匙信託中心的角色。於是，可以將吾人方法中有關設備的註冊與金匙託管的運作，交由資訊室負責。
- 另外，人事處是負責管理所有員工的相關資料，適合擔任第二金匙信託中心的角色。於是，可以將吾人方法中有關個人的帳號及金匙託管的運作，交由人事處負責。
- 企業裡的員工執行文件加密存檔的程序，將如同吾人方法中的送訊方作業程序。使用者同樣要通過電腦設備的身份驗證[Step 1]～[Step 3]步驟；並在[Step 4]輸入其選擇的加密金匙ck，讓電腦設備以該金匙將明文m加密為密文c；然後電腦設備同樣依[Step 5]～[Step 6]步驟結合本身的秘密金匙d_S、使用者的秘密金匙d_i、及日期$date$，產生完整的LEAF資料，連同密文一起存檔於該電腦設備中。
- 在正常的情況下，員工要解密出個人存檔的文件，只要輸入正確的金匙ck，即可令電腦設備解出明文。
- 然而，一旦員工忘記加密金匙，或是員工已經離職，那麼只要進行吾人方法中的監控程序，即可讓員工或企業主管在必要時將加密的文件還原。

從這樣的應用來看，迎合企業之架構與需求的金匙信託加密系統，確能提高人們的使用意願。而這也是吾人的設計中，之所以採取"人機分離"架構的重要考量。

二．監控對象的確認問題(Identification)

吾人的方法中，通訊設備會提出要求使用者證明其身份的質問訊息(Challenge Message)：

$$cm = \Upsilon^{e_i} \bmod n_i .$$

唯有使用真正的d_i才能計算出正確的rm：

$$rm = cm^{d_i} \bmod n_i$$
$$= \Upsilon^{e_i \cdot d_i} \bmod n_i .$$

如此，通訊設備無需與第二金匙信託中心連線即可驗證其身份。

在經過身份驗證後，便可毫無疑慮地將通訊資料與使用者身份建立明確的關係。而這在吾人的方法中，便是將送訊方使用者公開金匙e_i及其相關的檢查值ea_2加入通訊之中，而且難以竄改。如此一來，便符合美國聯邦調查局所提出的監聽對象確認之需求聲明，加強監聽證據之實質效力。

三．監控行為的限制(Wiretapping Limitation)

能解出通訊金匙ck的解密金匙是由通訊日期$date$、使用者秘密金匙d_i、及通訊設備的秘密金匙d_S共同組成的，執法單位必須在取得司法單位的授權後向兩個金匙信託中心提出申請，由第一金匙信託中心計算出部份解密金匙d_{I}：

$$\alpha \cdot date = 1 \bmod (p_S-1)(q_S-1) ,$$

$$d_{\text{I}} = d_S \cdot \alpha \bmod (p_S-1)(q_S-1) .$$

第二金匙信託中心計算出另一部份解密金匙d_{II}：

$$\beta \cdot date = 1 \bmod (p_i-1)(q_i-1) ,$$

$$d_{\text{II}} = d_i \cdot \beta \bmod (p_i-1)(q_i-1) .$$

執法單位取得此二解密金匙d_{I}、d_{II}後，才能解得其通訊金匙ck，進而得出明文m：

$$(eck^{d_{\text{I}}} \bmod n_S)^{d_{\text{II}}} \bmod n_i$$
$$= (ck^{e_i \cdot d_i \cdot \beta \cdot date} \bmod n_i)^{e_S \cdot d_S \cdot \alpha \cdot date} \bmod n_S$$
$$= ck .$$

$$m = D_{ck}(c) .$$

很明顯的，執法單位只能就特定使用者e_i、在特定通訊設備e_S、及特定日期$date$的通訊進行監聽。其取得的解密金匙是無法對授權條件之外的通訊進行解密，因此無需以強力的硬體防護加以管制(如美國政府的「敏感資料處理中心」)，即可達到對監控行為之限制。

同時，為了防止執法單位竄改監聽內容進行誣陷，在吾人的方法中加強了LEAF與密文c的關聯性：

$$ea_2 = f(e_i,e_S,c,ck,eck,ea_1)^{d_i} \bmod n_S .$$

如此一來，收訊方的通訊設備能確認通訊的完整性:

$$f(e_i,e_S,c,ck,eck,ea_1) \stackrel{?}{\equiv} ea_2^{e_i} \bmod n_S .$$

同樣的，在送訊方通訊設備的秘密金匙d_S不公開的情況下，執法單位難以竄改監聽內容並偽造出適當的檢查值ea_2，所以無法對監聽對象進行誣陷。

四．金匙管理的安全問題(Key Management)

在吾人的方法中，通訊雙方會在通訊之初協議出共同的通訊金匙ck，而這可以用任何的公開金匙分配方法(例如Diffie-Hellman Key Distribution Scheme)達到此一目的，沒有安全上的問題。

至於能解出通訊金匙ck的解密金匙d_{I}、d_{II}是由通訊日期$date$、使用者秘密金匙d_i、及通訊設備的秘密金匙d_S共同組成的，執法單位必須在取得司法單位的授權後向兩個金匙信託中心提出申請。解密金匙不但是無法對授權條件之外的通訊進行解密，執法單位也無法以此推導出使用者個人金匙d_i及通訊設備的秘密金匙d_S。因此，託管於兩個金匙信託中心的所有金匙都是安全無慮的。

另外，通訊設備的秘密金匙與使用者的個人金匙之產生及託管過程，是分別由兩個金匙信託中心獨立進行，沒有任何的交集。因此，不若Clipper或其他利用機密分享託管金匙的系統存在其危機，這是因為其解密金匙是靜態配置的，而且在託管過程中都有完整存在的一刻，在運作不當的情況下，仍有外洩之可能。但因為吾人方法中的解密金匙是結合了通訊設備的秘密金匙、使用者的個人金匙、及通訊日期而動態產生的，在通訊之前從未完整存在過，也因此不必擔心其安全問題。

五．實作的問題(Implementation)

在吾人的方法中，沒有任何不可公開的關鍵方法，而能夠將設計攤在陽光下接受公眾的檢驗，取得民眾之信任，進而增進使用之意願。

同時，既然沒有不方便公開的設計存在，就沒有必要一定以硬體的型式存在。以軟體的方式實作，同樣可以達成不被竄改的安全程度，而且其成本將遠低於硬體，更容易推廣普及。

§4. 文章總結

在吾人的方法中，加入了安全性與實用性兼顧的身份驗證程序，使得本方法為一完整的金匙信託加密系統。當然，吾人的方法也達成金匙信託加密系統之理想:

- 確保使用者配合使用
- 嚴謹的身份確認
- 監控行為的有效限制
- 確保金匙託管程序的安全
- 增進軟體實作之可能

在未來，若能針對其計算複雜度做更進一步的探討，提高金匙信託加密系統的效率與安全，達到快速、正確、有效之目的，則將是一種能為大眾所接受，極具有實用價值的金匙信託加密系統。

References

[Bla] M. Blaze, "Protocol Failure in the Escrow Encryption Standard", Proceedings of The 2nd ACM Conference on Computer and Communications Security, November, 1994, pp.59-67.

[BELW] D. M. Balenson, C. M. Ellison, S. B. Lipner, and S. T. Walker, "A New Approach to Software Key Escrow", Trusted Information Systems, Inc., 1995. (ftp://ftp.tis.com/pub/crypto/ske/paper)

[BKOSW] T. Beth, H. J. Knobloch, M. Otten, G. J. Simmous, and P. Wichmann, "Towards Acceptable Key Escrow Systems", Proceedings of The 2nd ACM Conference on Computer and Communications Security, November, 1994, pp.51-58.

[Cae] W. J. Caelli, "Commerical Key Escrow: An Australian Perspective", Cryptography: Policy and Algorothms Conference, Australia, July, 1995, pp.67-81.

[Den1] D. E. Denning, "The US Key Escrow Encryption Technology", Computer Communication Magazine, Vol.17, No.7, July, 1994, pp.51-58.

[Den2] D. E. Denning, "Key Escrow Encryption: The Third Paradigm", Computer Security Journal, Vol. 6, No.1, 1995, pp.43-52.

[Des1] Y. Desmedt, "Threshold Decryption: An Alternative to the Clipper Chip", Proceedings of the E.I.S.S. Workshop on Escrowed Key Cryptography, European Institute for System Security, University of Kerlsruhe, 1994, pp.138-150.

[Des2] Y. Desmedt, "Securing Traceability of Ciphertexts - Toeards a Secure Key Escrow System", Advances in Cryptology - EUROCRYPT'95 Proceedings, Springer-Verlag, 1996, pp.147-157.

[DB] D. E. Denning and D. K. Branstad, "A Taxonomy for Key Escrow Encryption Systems", Communication of the ACM, Vol.39, No.3, March, 1996, pp.34-40.

[DES] "Data Encryption Standard", Washington, DC: FIPS Pub.46, National Bureau of Standards, January 1977.

[DH] W. Diffie and M. E. Hellman, "New Directions in Cryptography", IEEE Transactions on Information Theory, Vol.IT-22, No.6, November 1976, pp.644-654.

[DS] D. E. Denning and M. Smid, "Key Escrow Now", IEEE Communications Magazine, September, 1994, pp.54-68.

[FBI] The FBI, "Law Enforcement REQUIREMENTS for the Surveillance of Electronic Communications", Prepared by the Federal Bureau of Investigations (FBI) in cooperation with federal, state, and local law enforcement menbers of the National Technical Investigation Association, June, 1994.

[FMW] N. Fefferies, C. Mitchell, and M. Walker, "A Proposed Architecture for Trusted Third Party Services", Cryptography: Policy and Algorothms Conference, Australia, July, 1995, pp.67-81.

[FY1] Y. Frankel and M. Yung, "Escrow Encryption Systems Visited: Attacks, Analysis and Designs", Advances in Cryptology - CRYPTO'95 Proceedings, Springer-Verlag, 1996, pp.222-235.

[FY2] Y. Frankel and M. Yung, "Designs of Escrow Encryption Systems: Models, Methodologies and Technologies", Available from the authors, 1994.

[Gan1] R. Ganesan, "How To Use Key Escrow", Communication of the ACM, Vol.39, No.3, March, 1996, pp.33.

[Gan2] R. Ganesan, "The Yaksha Security System", Communication of the ACM, Vol.39, No.3, March, 1996, pp.55-60.

[HD] J. He and E. Dawson, "A New Key Escrow Cryptosystem", Cryptography: Policy and Algorothms Conference, Australia, July, 1995, pp. 83-101.

[KL1] J. Kikian and T. Leighton, "Failsafe Key Escrow", Technical Report TR-636, MIT, August, 1994.

[KL2] J. Kilian and T. Leighton, "Fair Cryptosystems, Revisited", Advances in Cryptology - CRYPTO'95 Proceedings, Springer-Verlag, 1996, pp.208-221.

[KP] L. R. Knudsen and T. P. Pedersen, "On the Difficulty of Software Key Escrow", Advances in Cryptology - EUROCRYPT'96 Proceedings, Springer-Verlag, 1997, pp.237-244.

[LWY] A. K. Lenstra, P. Winkler, and Y. Yacobi, "A Key Escrow System with Warrant Bounds", Advances in Cryptology - CRYPTO'95 Proceedings, Springer-Verlag, 1996, pp.197-207.

[Mad] W. Madsen, "Good-bye Key Escrow, Hello Key Recovery", Computer Frauo and Security, November, 1996, pp.8-10.

[Mah] D. P. Maher, "Crypto Backup and Key Escrow", Communication of the ACM, Vol.39, No.3, March, 1996, pp.48-53.

[Mic] S. Micali, "Fair Public Key Cryptosystems", Advances in Cryptology - CRYPTO'92 Proceedings, Springer-Verlag, 1993, pp.113-138.

[MS] S. Micali and R. Sidney, "A Simple Method for Generating and Sharing Pseudo-Random Functions, with Applications to Clipper-like Key Escrow Systems", Advances in Cryptology - CRYPTO'95 Proceedings, Springer-Verlag, 1996, pp.185-196.

[Ne] J. Nechvatal, "A Public-Key-Based Key Escrow System", Journal of System and Software, No.35, 1996, pp.73-83.

[NIST1] National Institute of Standards and Technology, "Federal Information Processing Standards Publication 185, Escrowed Encryption Standard", Federal Information Processing Standards Publication, February 9, 1994, Washington, DC.

[NIST2] National Institute of Standards and Technology, " NIST Announces Process for Dialogue on Key Escrow Issues", NIST 95-24, August 17, 1995.

[NR] K. Nyberg and R. A. Rueppel, "A New Signature Schemes Based on the DSA giving Message Recovery", Proceedings of the 1st ACM Conference on Computer and Communications Security, Fairfax, Virginia, November 3-5, 1993.

[Pow] R. Power, "Point/Counterpoint: Phil Zimmerman and Dorothy Denning on Key Escrow and the Future of Crypto", Computer Security Journal, Vol. 6, No.1, 1995, pp.53-56.

[PH] S. C. Polig and M. E. Hellman, "An Improved Algorithm for Computing Logarithms over GF(P) and its Cryptographic Significance", IEEE Transactions on Information Theory, Vol.IT-24, No.1, January 1978, pp.106-110.

[RSA] R. L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", Communications of the Association for Computing Machinery, Vol.21, No.2, February 1978, pp.120-126.

[WB] S. T. Walker and D. M. Balenson, "A Software Key Escrow Approach", Proceeding of the E.I.S.S. Workshop on Escrowed Key Cryptography, European Institute for System Security, University of Kerlsruhe, 1994, pp.68-77.

[WH1] "The White House Press Release Regarding the Clipper", The White House Office of The Press Secretary, April 16, 1993.

[WH2] The White House, "Statement of the Vice President ", http://csrc.ncsl.nist.gov/keyrecovery, 1996.

[WLEB] S. T. Walker, S. B. Lipner, C. M. Ellison, and D. M . Balenson, "Commerical Key Recovery", Communication of the ACM, Vol.39, No.3, March, 1996, pp.41-47.

[WLEBB] S. T. Walker, S. B. Lipner, C. M. Ellison, D. K. Branstad, and D. M. Balenson, "Commerical Key Escrow: Something for Everyone Now and for The Future", Trusted Information Systems, Inc., 1995. (http://www.tis.com/crypto/ske/paper.html)