商用目的に適した鍵回復システムの開発

6F－5

(株)日立製作所[1] 日立電子サービス(株)[2] (株)富士通北陸システムズ[3]
(株)富士通研究所[4] 東北大学[5] 北陸先端科学技術大学院大学[6]
道明誠一[1],梅木久志[1],土屋宏嘉[1],川井亨[2],谷田武[3],鳥居直哉[4],満保雅浩[5],岡本栄司[6]

1 はじめに

企業資産を取り扱うファイルやメッセージを暗号化する分野では，業務や部署別に多数の暗号鍵を使い分ける要求が増えている．その際に，鍵を格納したICカードを紛失したり，鍵の所有者が部署を離れることで，企業資産が回復できない可能性があり，その場合の経済的損失が指摘されている．

企業資産として，(a)ファイル共有：部署別に共用するファイル(たとえば顧客名簿，帳簿)．(b)電子メール：担当者あてのメッセージ(たとえば注文書，見積書，契約書)の二種類の電子文書をとりあげる．このような電子文書における課題は，つぎのとおり．(1)アクセス管理の点で暗号化した状態[*1]で保存することが望ましいが，その反面，資産管理者や監査者が内容を参照できることをいかに保障するか．(2)電子文書の保存期間(たとえば7年)は，公開鍵の有効期間(1年)にくらべ長期であり，利用が終わった秘密鍵について，鍵所有者の自主的な保管に期待することは難しい．

以上の課題を解決する手段の一つとして，利用者の秘密鍵をバックアップし，企業内システムで一元管理するメカニズムを検討した[1]．開発したメカニズム(鍵回復システム)の設計方針[2]はつぎのとおり．(a)鍵所有者の情報を蓄積しない匿名性．(b)秘密分散(secret sharing)という暗号技術を用いた秘密鍵の秘匿性．(c)エンベロープデータ形式[*1]を実装する上での，業界標準な規格PKCS#7[*2]を採用する相互接続性．

本稿では，(b)の秘密分散技術を応用した鍵回復方式の目的と，秘密鍵を分割保管したままでデータ鍵を合成する手順について説明する．さらに，実験システムでの測定をもとに，秘密鍵の分割数とデータ回復の処理性能との関係について報告する．

2 秘密分散技術と鍵回復方式

まず，秘密分散技術について説明する．秘密分散とは，(1)分配者が秘密Sをn個の情報に分割し，それぞれn人の保管者に配る．(2)n人の保管者が，分割された情報$(S_1,S_2,\cdots,S_n)$を持ちよることで，元の秘密Sを復元できる暗号技術である．このとき，保管者のうちに不正者がいた場合に，いかなる分割情報S_iを用いても元の秘密Sが復元できないことを保証する．

秘密分散技術を鍵回復方式，とくに鍵保管装置に応用する目的はつぎのとおり．(a)鍵保管装置への不正者の侵入に対し，秘密鍵の漏洩を困難とする．(b)鍵所有者が，暗号化する電子文書のカテゴリや機密度を考慮し，鍵の保管先および分割数を指定できる．

3 鍵回復システムの構成

3.1. システム概要

提案する鍵回復システムは，利用者装置，鍵登録装置，鍵保管装置，鍵回復装置で構成する[2]．鍵回復プロトコルは，(1)秘密鍵バックアップ，(2)データ鍵合成，(3)データ回復の三つの手順に分類できる．利用者(鍵所有者)は，手順(1)を用いて，秘密鍵をバックアップし，引き換えとして預かり証を入手する．利用者(資産管理者，監査者)は，手順(2)(3)を用いて，預かり証とエンベロープデータより，暗号データを復号する[*3]．

3.2. 鍵回復プロトコル

図1と図2(分割数 k=2)を用いて，鍵回復プロトコルの手順を説明する．利用者Aの公開鍵をUsr_Apub，秘密鍵をUsr_Apriとし，平文Mを暗号化・復号する共通鍵(データ鍵)をSとする．なお，以下の説明では，鍵Kを用いてデータXを暗号化することをE[K](X)，鍵Kを用いてデータYを復号することをD[K](Y)と記す．

<u>秘密鍵のバックアップ</u>

①鍵所有者Aによる秘密鍵の分割

公開鍵Usr_Apubとペアの秘密鍵Usr_Apriをk分割．

②分割した秘密鍵の配送

鍵所有者が任意の鍵保管装置$KS_i(i=2,\cdots,k)$を選択．分割秘密鍵Usr_Apri_iを鍵保管装置の公開鍵を用いて暗号化したE[KS_ipub](Usr_Apri_i)を鍵保管装置に送付．

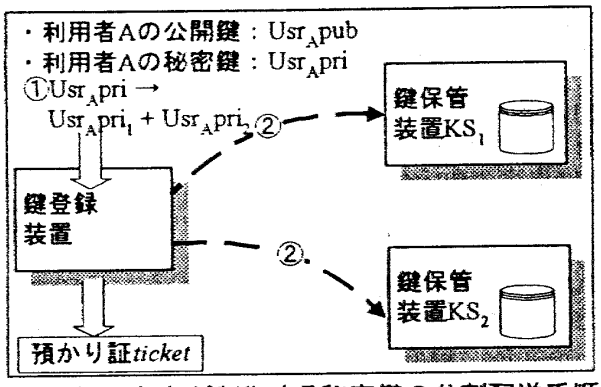

図1. 鍵所有者が制御する秘密鍵の分割配送手順

データ鍵合成とデータ回復

③暗号化したデータ鍵の送付

エンベロープデータの E[Usr_Apub](S)を抽出し，鍵保管装置(i=2,…,k)に送付.

④データ鍵の部分回復

分割秘密鍵 $Usr_A pri_i$ を用いて E[Usr_Apub](S)を復号.

⑤部分回復したデータ鍵の返信

鍵保管装置(i=2,…,k)より D[$Usr_A pri_i$](E[Usr_Apub](S))を返信.

⑥データ鍵の合成

D[$Usr_A pri_i$] (E[Usr_Apub](S))の積を計算. RSA 暗号アルゴリズムの特性を利用し，データ鍵 S を合成.

⑦データ回復

データ鍵 S を用いて E[S](M)より，平文 M を復号.

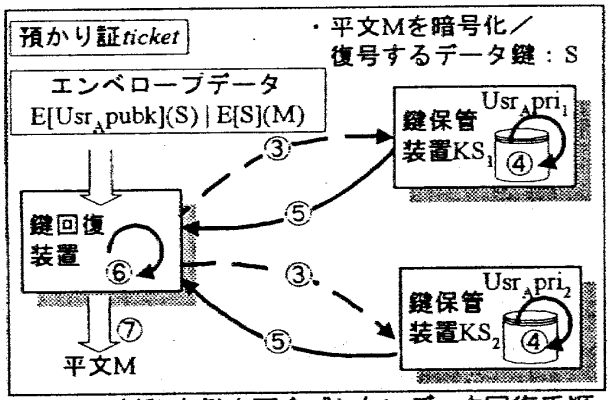

図2. 分割秘密鍵を再合成しないデータ回復手順

4　評価

PC/AT 互換機を配した実験システムにおいて，条件 Usr_Apri:1024bit,S:64bit,M:0.5Mbyte のもと，秘密鍵の分割数(k=3,…,10)と，データ鍵合成およびデータ回復のターンアラウンドタイム t との関係を調べた.

実験システムでは，暗号処理(ステップ⑦)にくらべ，他の処理のコストが高くついている. たとえば，(1)手順による要因:部分回復したデータ鍵を合成する(⑥)のに，k 回の乗算処理，(2)実装方式による要因:各鍵回復装置と鍵保管装置の間の，k回のデータ鍵の部分回復処理(③～⑤)*4，があげられる. これらの要因によって，ターンアラウンドタイム t が，分割数 k に対し，計算量 O(k)で増加することを確認した.

電子文書の鍵管理という観点で提案方式を評価する. 鍵所有者は，機密度の高い電子文書を扱う鍵ほど，安全性の向上のために分割数を増加させたい. したがって，機密度の高い文書の回復時間は増加する. 一方，資産管理者や監査者は，電子文書の機密度に関係なく，データ回復時間を一定の範囲内としたい. この両者の要求を踏まえ，企業のセキュリティ方針として，秘密鍵分割の適正な値を定めておく必要がある.

5　おわりに

秘密鍵の分割数(電子文書の機密度)とデータ回復時間がトレードオフの関係にあることを確認した. 今後は，実システムと組合わせる過程で，実現方式の改善点を明らかにしたい.

参考文献

[1]田渕:プライバシー保護に適した鍵回復方式の研究開発，創造的ソフトウェア育成事業中間成果発表論文誌 pp.492-496, 情報処理振興事業協会, June 1997

[2]谷田，土屋他:鍵回復システムの設計と実装，第 55 回情報処理全国大会予稿集 2T-01, 3-645, Sept. 1997

---

*1 本稿において，電子文書を保存する形式として，共通鍵(データ鍵)を用いて平文(データ)を暗号化し，さらに利用者の公開鍵を用いてデータ鍵を暗号化し，暗号文に添付する形式を採用した. 一般に，このような形式をエンベロープデータ形式とよぶ.

*2 Cryptographic Message Syntax Standard An RSA Laboratories Technical Note Version 1.5 Revised November 1,1993

PKCS は，RSA Data Security 社の登録商標です.

*3 データの秘匿性の観点から，鍵回復方式の多くは，鍵回復は鍵回復装置，データ回復は利用者装置と分業する構成をとる. しかし，長期保存の用途では，復号プログラムが利用者装置に存在してない可能性がある. そこで，復号プログラムを要した鍵回復装置が，エンベロープデータの形式を解釈し，データを回復する仕様とした.

*4 鍵回復装置での待ち処理を簡略化する目的で，各鍵保管装置の処理を順次，依頼する仕様とした.