1L−6

マルチメディア通信に適したリニューアル可能な暗号認証システムの検討

栃窪 孝也† 遠藤 直樹† 岡本 栄司‡

†(株) 東芝 SI 技術開発センター ‡北陸先端科学技術大学院大学 情報科学研究科

1 はじめに

今日、ネットワークに接続されている様々な機器に機密保持のために暗号化技術が組み込まれている。組み込まれている暗号化技術を用いることで、ネットワークを介した電子商取引やコンテンツ配信事業などが盛んに行われているが、それらの事業は組み込まれている暗号化技術の安全性の基に成り立っている。このような背景から、安全かつ効率の良い暗号方式の設計に関する研究が盛んに行われている。その一方、安全な暗号方式の設計に関する研究と同時に暗号方式の安全性の評価のために暗号方式の解読法の研究も盛んに行われている。

また、従来の暗号化技術を組み込んだシステムは、規格標準化等によりシステム仕様が一度決まると、それと同時に、システムで使用する暗号方式が固定されるためシステムのセキュリティレベルも固定される。

したがって、システムで使用している暗号方式が解読されるといったことも現実に起こりうることであり、システムで使用している暗号方式が破られた場合、従来のシステムではもはやシステムをそのまま使用することができなくなる。仮に、すべての機器に対しシステムの暗号方式を更新する場合、ネットワークを介しての更新では、秘密情報の外部への流出などの安全性の面で問題があり、ネットワークを介さずの更新では、システムのすべての機器一台一台に変更を加えなければならないといった効率の面で問題がある。

さらに、従来のシステムでは、使用できる暗号方式が固定されているため、情報の価値を考慮した効率的な暗号化ができない。

以上のことから、小文では、情報の価値にふさわしい強度の暗号方式が使用でき、システムで使用できる暗号方式をネットワークを介して安全かつ効率よく更新することで、システムのセキュリティレベルの強度の維持・向上が可能な「リニューアル可能な暗号認証システム」および、暗号方式等の更新プロトコルを提案する。

2 リニューアル可能な暗号認証システム

提案システムは、システムで使用する暗号方式の登録、管理を行うセンターと複数の端末から構成される。

なお、以下では $E_K^x(y)$ によって暗号方式 x、鍵 K を用いたメッセージ y の暗号文を表し、$a|b$ によって a と b の連接を表す。

各端末は、システムで使用する暗号方式のアルゴリズム (プログラム) を複数保存する暗号アルゴリズムファイルと暗号通信に用いる秘密鍵などを保存する鍵情報ファイルを備える。そして、暗号通信の際に使用する暗号方式と秘密鍵をそれぞれ暗号アルゴリズムファイルおよび鍵情報ファイルから読み込み、暗号器・復号器でメッセージの暗号化、暗号文の復号化を行う。暗号アルゴリズムファイルに保存されている暗号アルゴリズム Al は暗号方式 E^2、暗号方式固有の鍵 K_{Al} によって暗号化されている。また、鍵情報ファイルに保存されている暗号方式固有の鍵 K_{Al} および、暗号通信に用いる秘密鍵は暗号方式 E^1、端末固有の鍵 K_i によって暗号化されている。

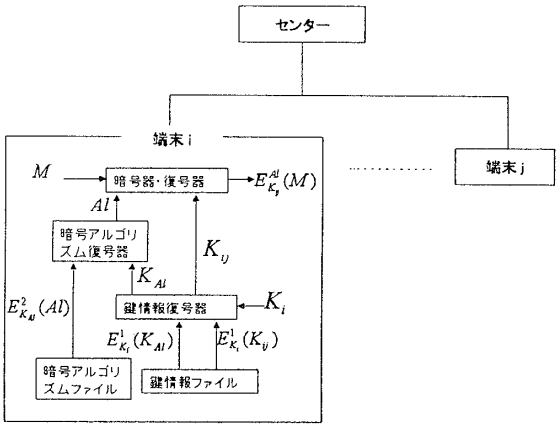

図 1: システムの構成

実際の通信は以下のように行われる。端末 i が端末 j へ暗号方式 Al でメッセージ M を送信する場合、鍵情報ファイルから暗号化された暗号方式固有の鍵 $E_{K_i}^1(K_{Al})$、$i-j$ 間の暗号通信用の秘密鍵 $E_{K_i}^1(K_{ij})$ を呼び出し、鍵情報復号器で端末固有の鍵 K_i によって復号化し、K_{Al} を暗号アルゴリズム復号器、K_{ij} を暗号器・復号器へ送る。また、暗号アルゴリズムファイルから $E_{K_{Al}}^2(Al)$ を呼び出し、暗号アルゴリズム復号器において K_{Al} によって復号化し、Al を暗号器・復号器へ送る。暗号器・復号器において、Al、K_{ij}、M から暗号文 $E_{K_{ij}}^{Al}(M)$ を作成し端末 j に送る。

本システムでは、暗号アルゴリズムが非公開な暗号方式に対するリニューアルをも考慮にいれるため、暗号アルゴリズムファイルには暗号アルゴリズムが暗号化さ

Renewable Authentication and Encryption Systems for Multimedia Communications

Kouya TOCHIKUBO† Naoki ENDOH† Eiji OKAMOTO‡

†SI Technology Center, TOSHIBA Corporation

‡School of Information Science, Japan Advanced Institute of Science and Technology

れて保存されているが、アルゴリズム公開の暗号方式に対しては暗号化せずに保存し、使用することも可能である。また、暗号アルゴリズムファイルに複数の暗号方式を保存しておくことで、情報の価値にふさわしい強度の暗号を使用可能である。さらに、暗号アルゴリズムや鍵情報等の秘密情報を暗号化して保存しているため、

- E_1 にアルゴリズムが非公開な暗号方式を用いる
- 端末固有の鍵 K_i の保存に IC カードを用いる

等で他人のみならず利用者本人からも秘密情報を保護することができ、外部および内部の不正利用を防止することができる。

3 暗号方式更新プロトコル

小文では、2つの暗号方式更新プロトコルを提案する。

更新プロトコル 1: センターに新規暗号方式 Al' および暗号方式固有の鍵 $K_{Al'}$ を要求

(i) 端末 i はセンターに、自分の ID 情報 ID_i、要求する暗号方式の ID 情報 $ID_{Al'}$ および更新の際に使用する暗号方式の ID 情報 ID_{Al} を送り更新要求を出す。

(ii) センターは、端末 i が暗号方式 Al' の使用が認められているかをチェックし、使用が認められている場合は、端末 i にセンターの ID 情報 ID_c、ID_{Al}、$E^{Al}_{K_{ci}}(ID_{Al'}|E^1_{K_i}(K_{Al'})|E^2_{K_{Al'}}(Al'))$ を送信する。

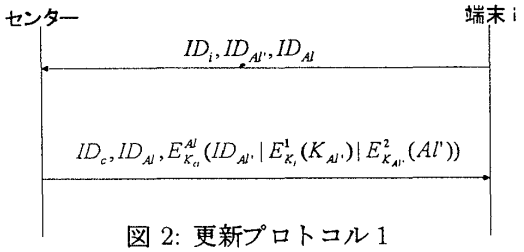

図 2: 更新プロトコル 1

更新プロトコル 2: 他の端末に新規暗号方式 Al'、センターに暗号方式固有の鍵 $K_{Al'}$ を要求

(i)-1 端末 i は端末 j に、自分の ID 情報 ID_i、要求する暗号方式の ID 情報 $ID_{Al'}$ および更新の際に使用する暗号方式の ID 情報 ID_{Al} を送り更新要求を出す。

(i)-2 端末 j は、端末 i に端末 j の ID 情報 ID_j、ID_{Al}、$E^{Al}_{K_{ij}}(ID_{Al'}|E^2_{K_{Al'}}(Al'))$ を送信する。

(ii)-1 端末 i はセンターに、自分の ID 情報 ID_i、要求する暗号方式固有の鍵の ID 情報 $ID_{K_{Al'}}$ および更新の際に使用する暗号方式の ID 情報 ID_{Al} を送り更新要求を出す。

(ii)-2 センターは、端末 i が暗号方式 Al' の使用が認められているかをチェックし、使用が認められている場合は、暗号方式固有の鍵 $K_{Al'}$ を暗号方式 E^2、端末固有の鍵 K_i によって暗号化し、端末 i にセンターの ID 情報 ID_c、ID_{Al}、$E^{Al}_{K_{ci}}(ID_{K_{Al'}}|E^1_{K_i}(K_{Al'}))$ を送信する。

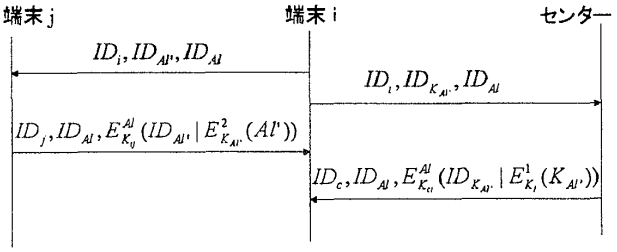

図 3: 更新プロトコル 2

どちらのプロトコルでも、端末は送られてきた更新情報に手を加えることなく、送られてきた更新情報をそのまま保存するだけで更新が可能である。また、更新プロトコル 2 は更新情報を分散して要求できるので、センターの負荷を減らすことができる。なお、暗号方式の更新の際に、センターは要求者が更新する暗号方式を使用可能かどうかチェックすることで、暗号方式の輸出規制等の暗号方式の管理にも対応可能である。

4 まとめ

小文では、情報の価値にふさわしい強度の暗号方式が使用でき、システムで使用できる暗号方式を更新することで、システムのセキュリティレベルの強度の維持・向上が可能な「リニューアル可能な暗号認証システム」および、暗号方式等の更新プロトコルを提案した。暗号方式の更新の際に、センターは要求者が更新する暗号方式を使用可能かどうかチェックすることで、暗号方式の輸出規制等の暗号方式の管理にも対応可能である。さらに、暗号アルゴリズムや鍵情報等の秘密情報を暗号化して保存しているため、外部および内部の不正利用を防止することができる。

本研究の一部は情報処理振興事業協会「独創的情報技術育成事業」の一環として行われたものである。

参考文献

[1] 栃窪 孝也, 遠藤 直樹, 岡本 栄司, “マルチメディア通信に適したリニューアル可能な暗号認証システムの調査研究,” 第 17 回 IPA 技術発表会論文集, vol.17 pp236-236, 1998.

[2] 南 向鎮, 岡本 栄司, 篠田 陽一, 満保 雅浩, “自己復号型秘密情報通信のためのプラットフォームの開発研究,” The 1996 Symposium on Cryptography and Information Security, SCIS96-01C, Jan. 29, 1996.

[3] 岡本 栄司, “暗号理論入門,” 共立出版株式会社, 1993.