5T−1

暗号応用機能を強化したICカードの開発

武藤義弘　、　高木伸哉
松下電器産業（株）事業推進センター

1. はじめに

昨今いずれの分野においてもパソコン通信・LANなどを用いて電子的にデータが処理され、それらシステムには高いセキュリティが求められるようになってきた。現在ICカードの多くはDESあるいはFEALなどの秘密鍵暗号を搭載しており、金融、通信などのセキュリティが要求される分野では有効的な手段と考えられる。しかしこれらICカードには秘密鍵暗号を利用した暗号関連のコマンドが少なく、セキュリティを要するアプリケーションに十分に対応することができない。そこで秘密鍵暗号を用いた種々のアプリケーションに対応できるようにまた国際標準ISOに準拠するようにICカード内の基本プログラムを設計し、豊富な暗号関連のコマンドを有するICカードの開発を行った。

本報では、最初に暗号機能について、次いで秘密鍵暗号の秘密鍵の管理方法について述べる。

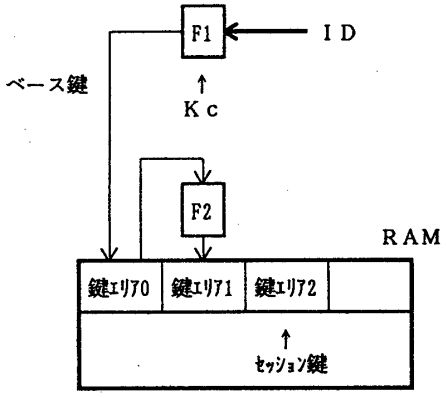
2. 暗号機能

秘密鍵暗号を用いた場合の電子資金移動やデータ通信においては以下に示す暗号機能が必要と思われる。これら各機能で使用される鍵は表1に示すISO10202のPart 3（鍵の諸関係）に準拠した。

1）エンティティ認証
　通信相手の正当性をチェックする
2）メッセージ認証
　メッセージの完全性をチェックする
3）データの暗号化・復号
ICカード内メモリデータに対して
4）暗号化読出し
　秘密の固定データを暗号化して読み出す
5）復号書込み
　暗号化データを復号して書き込む
6）証明書付読出し
　読み出しデータに加え、該ICカードの証明書を付けて読み出す
7）証明書データの確認
　受信したデータとそのデータの証明書の正当性をチェックする

表1　鍵の種類

鍵	使用できる機能	格納場所
Kaut1	相互認証	RAM
Kaut2	相互認証：Kaut1の対鍵	E²PROM
Kmac	メッセージ認証子の生成	RAM
Kcer	取引証明書の生成	RAM
Kenc	データの暗号化・復号	RAM
Kctl	鍵の管理	RAM
Kadf	ファイル管理	RAM
Kc	鍵の生成	E²PROM
Kp	PINの伝送	E²PROM



第1図　鍵管理

Development of IC Card with Ciphering Process
Yoshihiro MUTOH, Nobuya TAKAGI
MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.

3. 鍵管理方式

通信相手と同じ鍵を持つ必要がある秘密鍵暗号においては、その通信システムを利用する全員が同じ鍵を持つか、全ての通信相手の鍵を複数持つか、の2通りが考えられる。前者はその鍵が漏洩した時にシステム全体に影響を及ぼし、また後者は表1に示す複数の鍵を通信相手分所持するため記憶容量に負担がかかる。

ＩＣカードが任意の通信相手との間で上記機能を達成するために、本ＩＣカードでは暗号処理で使用される秘密の鍵を第1図に示すように生成する。

1）通信相手のＩＤを受信し、センターの秘密鍵Ｋｃと関数Ｆ1を用いてベース鍵を生成する。

2）暗号関連のコマンドを受信する度に、前記ベース鍵と関数Ｆ2を用いて各コマンドで使用する秘密の鍵を生成する。

ここで、鍵ＫｃはＩＣカード発行時に書換え可能な不揮発性メモリに格納されている。また生成された通信相手の秘密の鍵は全て揮発性メモリに格納され、取引が終了した時点で消えるようになっているため安全性が高い。

これら生成された鍵はセンター鍵Ｋｃあるいは関数Ｆが変更されない限り、ひとつのＩＤに対して同一の鍵を生成する。しかしアプリケーションによってはその処理にだけ有効な秘密鍵（セッション鍵）を利用したい場合がある。本ＩＣカードでは、図2に示すように相互に認証を行うことで通信者間でセッション鍵が共有でき、お互いに認証できた場合のみ使用することができる。ここでＩＣカードのＫaut1および通信相手のＫaut2はそれぞれ相手のＩＤより生成される。

また不正防止のためセッション鍵は少なくとも以下の成分を含む必要がある。

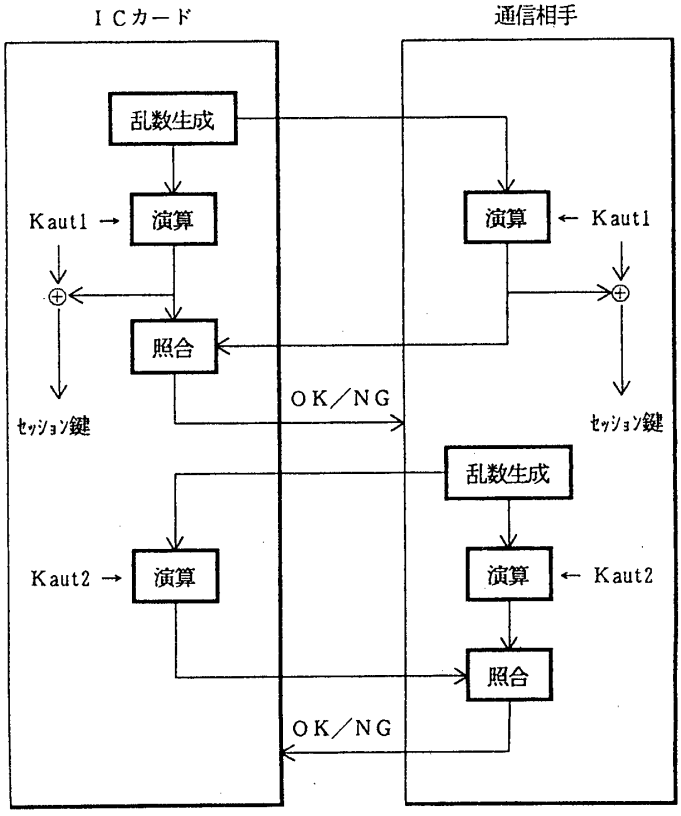
a）内部保持している値　　b）秘密情報　　c）乱数成分

4. まとめ

セキュリティを要するアプリケーションで利用するための豊富な暗号機能を有するＩＣカードのソフト設計を完了した。現在国際標準ＩＳＯでは審議進行中であり実際のコーディングを見送ったが、標準が決まり次第すぐに対応可能である。

これら暗号応用機能を用いれば容易に電子的資金移動システムが構築でき、また単にデータを暗号化・復号する機能もあるため、データ通信の分野にも利用できる。

今後の課題としては、ＩＣカードの国際標準が主にＩＣカードとＩＣカード受入れ端末間での取り決めであるため、アプリケーションを構築する上でホストをも含めたシステム全般的な暗号処理を考える必要がある。



第2図　相互認証