ユーザに対して秘匿される秘密情報の受け渡し

2G－6

井熊 徹　西垣 正勝　曽我 正和　田窪 昭夫
静岡大学大学院　静岡大学　岩手県立大学　三菱電機
理工学研究科　情報学部　ソフトウエア情報学部　情報システム製作所

1. はじめに

プログラムの不正コピー防止のために，著者らはすでにプログラムのスクラッチング（汚染）と動的復元によるバイナリプログラムの不正コピー防止方式を示した[1]。スクラッチング（汚染）はプログラムの一部のみを暗号化することにより，プログラムの実行速度を落とすことなく，プログラムのセキュリティを保つ方法である。この方法においては，各CPUが公開鍵暗号方式の鍵のペア（配信用公開鍵，配信用秘密鍵）を持つことが仮定されている。そして，CPUにはセキュアレジスタと呼ばれる安全なレジスタが付加される。セキュアレジスタは，その内容を読み出す機械語命令が用意されておらず，セキュアレジスタ内の情報はユーザにさえ隠蔽される。プログラム中のスクラッチ（汚染）を修復するための情報（クリーナ情報）は，購入者が使用する計算機の配信用公開鍵により暗号化され，計算機に送られる。配信用秘密鍵およびクリーナ情報は各CPUのセキュアレジスタに格納され，封印される。また，一連の復号は「セキュアファームウェア」により実装される。セキュアファームウェアによる処理は通常のCPUの処理とは完全に独立し，処理途中のデータや結果はセキュアレジスタ以外のいかなる記憶装置上にも残らない。以上により，プログラムを修復して正しく実行できるのは購入者の使用する計算機のみとなり，プログラムの不正コピーは無意味となる。

しかし，この方法ではユーザの使用できる計算機が固定されてしまうという問題が残った。本稿ではこの問題を解決するための方法を提案する。本稿では，クリーナ情報を格納するデバイスとしてICカードを選んだ。ICカードはユーザごとに用意され，ユーザは使用する計算機に自分専用のICカードを差し込んで使用することとする。クリーナ情報はICカード内に封印されており，プログラムの実行に前もってCPU内のセキュアレジスタに転送される。したがって，クリーナ情報をCPUに安全に転送することが本稿の命題となる。

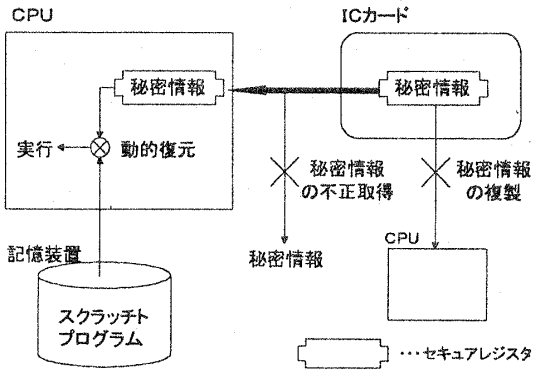

図1：秘密情報を用いた不正コピー防止方法

なお，本方式は，クリーナ情報に限らず，ICカード内の何らかの秘密情報をCPU内のセキュアレジスタに転送するための方法として使用できる。したがって，以下ではクリーナ情報を秘密情報（SI）という言葉で表す。

2. 前提

1. CPUとICカードは内部にセキュアレジスタを持つ。
2. CPUとICカードは内部にセキュアファームウェアを持つ。本手法における暗号化等の処理はすべてセキュアファームウェアにより行われる。
3. 各ユーザは個人認証用の鍵を持つ。この鍵のペアをユーザ公開鍵（Up），ユーザ秘密鍵（Uq）と呼ぶ。Uqは各ユーザが秘密裡に保管するものであるが，ICカード内のセキュアレジスタにも保存されている。
4. 認証局と呼ばれる公の機関が存在する。認証局の持つ鍵のペアを認証局公開鍵（Ep），認証局秘密鍵（Eq）と呼ぶ。ICカードは内部にEpを保有する。
5. 各ICカードは製造時に，鍵を割り当てられる。この鍵のペアをIC公開鍵（Ip），IC秘密鍵（Iq）と呼ぶ。Iq

A protocol for secure transportation of secret information
Tohru Ikuma , Masakatsu Nishigaki ,
Faculty of Information , Shizuoka University ,
3-5-1 Johoku Hamamatsu 432-8011 , Japan .
E-mail:nisigaki@cs.inf.shizuoka.ac.jp
Masakazu Soga , Iwate Prefectural University .
Akio Takubo , Mitsubishi Electric Corp .

はICカード内のセキュアレジスタに保管される。

6. 各CPUは製造時にIDと鍵を割り当てられる。これらをそれぞれ，CPU－ID(CID)，CPU公開鍵(Cp)，CPU秘密鍵(Cq)と呼ぶ。CqはCPU内のセキュアレジスタに保管される。CPUは内部にCIDを保有する。Cpは認証局によって保管・管理される。
7. CPUはセキュアな乱数生成機構を持つ。生成された乱数(R)は直接，セキュアレジスタに格納される。また，Rはエミュレート等により予測されない。
8. 本稿においては，鍵Kによりメッセージを暗号化したものをK(M)と記す。

3. 動作手順

3.1. 著作者からICカードへの秘密情報の送信

1. 購入者は著作者にEq(Ip)を送信する。
2. 著作者はEpにより署名を確認し，Ipを得る。
3. 著作者は秘密情報(SI)をIp(SI)の形で，購入者の所有するICカードに送信する。
4. ICカードはIp(SI)をIqで復号し，SIをICカード内のセキュアレジスタに保存する。

3.2. 前処理

本方式では以下の手順を前処理として行なう。これにより，ICカードはCpを認証局の保証の元に得ることができる。本方式では，前処理部分のみがネットワークによる通信を必要とする。あらかじめ前処理を行うことにより，ユーザはネットワークを利用できない状態であってもコンテンツの利用を妨げられない。

1. CPUはCIDをEp(Kq(CID))の形で認証局に送る。
2. 認証局はKpで署名を確認し，CIDを得る。
3. 認証局はCIDに対応するCpをEq(Kp(Cp))の形でICカードに送る。
4. ICカードはEq(Kp(Cp))をEp，Kqにより復号することでCpを得る。

3.3. ICカードからCPUへの秘密情報の転送

1. CPUはICカードにCIDを送ることで秘密情報を要求する。このとき，ICカードは暗証番号の押下等により本人からの要求であることを確認する。
2. ICカードはIpをCp(Ip)の形でCPUに送る。
3. CPUはCp(Ip)を復号し，Ipをセキュアレジスタに格納する。
4. CPUは手順3と同時にRを生成する。そして，IpとRを対応させ，ロックをかける。ロックは新たにCp(Ip)を受け取るまで外れない。すなわち，Ip，Rは片方のみが変更されることを許されない。
5. CPUはRをCq(Ip(R, M1))の形でICカードに送る。ここで，M1はRの送信を意味する予約語である。
6. ICカードはCq(Ip(R, M1))を復号し，Rをセキュアレジスタに格納する。
7. ICカードは秘密情報をCp(R(SI))の形でCPUに送信する。同時に，ICカードは秘密情報にロックをかける。このロックは後述の解除手順を終了するまで外されない。これにより，悪意を持つ正規ユーザが複数の秘密情報を同時に流出させることを防ぐ。
8. CPUはCp(R(SI))を復号し，秘密情報をセキュアレジスタに格納する。

3.4. 秘密情報のロック解除手順

1. CPUはCq(Ip(R, M2))をICカードに送信すると同時にCPU内の秘密情報，および，IC公開鍵と乱数を消去する。ここで，M2は秘密情報の開放を意味する予約語である。
2. ICカードはCq(Ip(R, M2))を復号し，Rが正しいことを確認する。これによりICカードはCPU内の秘密情報の消去を確認し，秘密情報のロックを解除する。

4. まとめ

正規ユーザにすら知られてはならない秘密情報をICカードからCPUに転送するための一手法を示した。本方式により，文献[1]の方法におけるユーザの使用できる計算機が限定されるという欠点が克服される。

今後は本方式の安全性に対して検討を重ねる。

参考文献

[1]井熊，曽我，西垣，田窪：データの汚染と動的復元による実行形式プログラムの不正コピー防止方式，1999 年暗号と情報セキュリティシンポジウム予稿集，pp.445-450，1999 年 1 月．