SHA-1を使った電子取引の安全保証

暗号化能力を持った携帯電子機器を使って、非常に安全なネットワーク真正証明、仮想私的ネットワーク、販売機レギュレーション、料金徴収、従業員又は市民の識別を行う傾向が世界的に強くなっています。こうした携帯機器(又はトークン)の設計には、暗号化装置がデリケートなデータ及び金銭情報が真正であることを証明し、保護する方法を注意深く研究する必要があります。もちろんeキャッシュ(識別トークン)は持ち運び可能で、長持ちし、安全が保証される必要がありますが、安全保証トークンはさらにいくつかの暗号化、電気的及び物理的条件を満たさなければならないことがすぐに明らかになってきます。

真の安全保証トークンが持つべき最も重要な機能は真正証明機能です。トークンは、発行者(サービスプロバイダ)から認可されていること及び本物であることを証明できなければなりません。そのトークンが認可されているということは、発行権限所有者だけが作成できる暗号化情報を持っているということだけで証明できます。しかし、安全保証付真正証明ははるかに難しい問題です。デバイスは自らが偽物や複製でないことを証明しなければなりませんが、これには非常に特殊なハードウェア機能が必要とされます。デバイスの設計を自由に調べることができなければ、そのデバイスは信用されないため、設計や機能の秘密は保つことができません。デバイスの内部のしかけが公表されて周知である場合、十分な技術を持った人なら誰でもそのデバイスの模造品を作り、デバイスのハードウェアが課する特別なコントロールの一部をバイパスすることができます。分かり難さで安全を保証しようとするトークン設計は必ず失敗します。

暗号法の世界では、真の安全保証真正証明は「チャレンジ・アンド・レスポンス」という方法で扱われます。この方法は、正当なトークンとホストにしか知られていない秘密と、トークンがその秘密を知っていることを証明して本物であることを自ら証明する方法から成っています。もちろん、このプロセスの中で秘密が知られてしまってはいけません。ここで、「ゼロ・ノレッジ・プルーフ」という暗号概念が使用されます。トークンは自らがその秘密を知っていることを、その秘密に関する情報を全く暴露することなく証明するメカニズムをサポートしなければなりません。一見、これは不可能に見えます。しかし、これは安全保証付暗号システムにおいて普通に行われていることです。この方式は次のように機能します。問題のトークンが来ると、ホストシステムは非常に大きな数(チャレンジと呼ばれます)を全くランダムに作ってトークンに送ります。トークンはこのチャレンジを受け取って、これに対して内部に保存された秘密を使って複雑な数学演算を行います。そして、その演算の結果をホストに返します(図1を参照)。ホストも同じ秘密を知っているので、同じ数学演算を内部で行い、結果を比較します。トークンからのレスポンスがホスト内で計算されたものと一致すれば、トークンは秘密を暴露することなくその秘密を知っていることを証明したことになります(これがゼロ・ノレッジ・プルーフの本質です)。秘密を知らない攻撃者がこの会話を盗み聞きしても、何の役にも立ちません。これは、チャレンジがランダムに生成され、毎回異なるからです。次のチャレンジが何であるかは全く予想できません。秘密は安全にトークン内に保持され、ホストはそのトークンが本物であることを知ります(本物のトークンだけが秘密を知っているからです)。

もちろん、使用される複雑な数学アルゴリズムは不可逆なものであることが必須です。さもないと攻撃者はその演算を逆に実行して秘密を引き出すことができるからです。実際、チャレンジ・アンド・レスポンス方式の安全保証を審査する上で最も重要な要因はどのアルゴリズムを選択するかということかもしれません。過去には、自家製アルゴリズム、ストリームサイファー、ローリングコードあるいはこの目的用に短縮された暗号アルゴリズムを使った電子トークンが作られてきましたが、これらは広く受け入れられていません。問題なのは、広範な同業者による検討なしには、これらのアルゴリズムが攻撃に対して安全を保証できるかどうかが保証できないことです。また、これらのアルゴリズムにデバイスメーカだけが知っている(意図的、あるいは偶然の)「裏口」がないという保証もありません。

真の安全保証暗号トークンを作るには、選択したアルゴリズムがよく知られていて、信用があり、長期に渡って試されていて、しかも世界中の暗号技術者による検討がなされたものでなければなりません。入力データから非可逆的にそのデータのダイジェスト版を作るアルゴリズムは、一方向ハッシュ(ごたまぜ)関数と呼ばれます。最もよく研究され、信用されている一方向ハッシュ関数はSHA-1(安全保証ハッシュアルゴリズム)です。このアルゴリズムは政府から認可されていて(FIPS 180-1)、現代のディジタル署名及び書類保護方式の基礎になっています。また、暗号技術者の世界で長い歴史を持ち、検討され、広く信用されているものです。

しかし、SHA-1は複数の32ビット5方向加算、複雑な論理関数、データシフト及び非常に多数の繰り返しを含む複雑なアルゴリズムです。シリコンでSHA-1アルゴリズムを実現するには従来大きなチップ面積を必要とし、

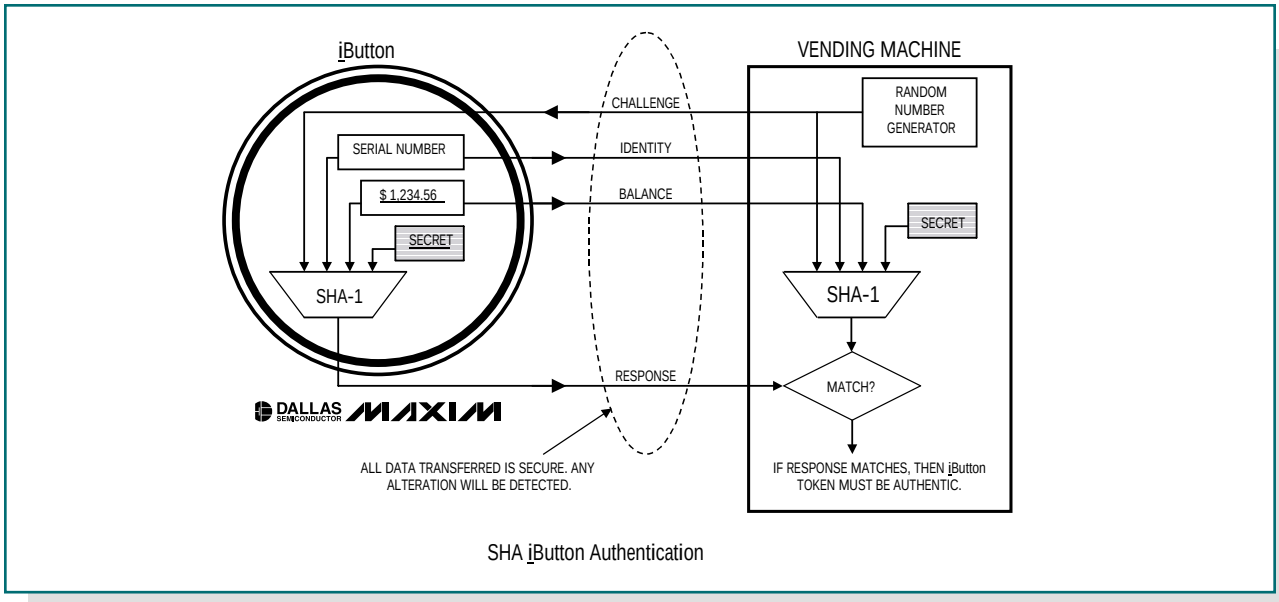

図1．SHA iButton真正証明

トークンがかなり高価になっていました。このアルゴリズムをシリアル式に実行する新しい方法が工夫されたことで、チップ面積が10分の1以下になり、妥当な価格のSHA-1式トークンが可能になりました。

真の安全保証トークンのもう一つの必須条件は、世界的に唯一独自で変更不能なアイデンティティを持っていることです。唯一のトークンシリアル番号を真正証明アルゴリズムの追加入力として含めることにより、物理的なトークンとその内容が結びつけられるため、トークン間で金銭値や信用証明を複製することが不可能になります。

金銭的アプリケーションで安全保証トークンが使用される時、そのトークンが含む情報(おそらく口座預金高)は動的になります。なぜなら、デバイスが使用される度に重要な値が読み取られ、借方記入され、それから再び書き込まれるからです。こういった使い方にもとづいて、暗号技術者がリプレーアタックと呼ぶタイプの攻撃が可能になります。攻撃者はトークンからの値のデータを読取り、「正当に買い物をして」そのトークンを空にします。それから、元のデータを復元(又はリプレー)することでトークンの金銭値を復元して何度も使えるようにします。このリプレーを防ぐためには、トークンが使用される度に含まれるデータをそれぞれ唯一独自のものにするようなメカニズムを持っている必要があります。従って、真の安全保証金銭トークンは特別なカウンタを持っています。このカウンタはデバイスに書込みがある度にカウントが上がり、循環、リセット、カウントダウン又はリロードができないようになっています。このカウンタ値を真正証明アルゴリズムの入力に含めることにより、金銭的データ、デバイスのアイデンティティ、及び金銭的な事例が全て一緒にまとめられます。デバイスからデータを取って後で書き戻した場合、カウンタが変化しているために無効とみなされます。同じ値ですが、その値の事例が異なるからです。

チャレンジ・アンド・レスポンス真正証明プロセスの興味深い特長は、トークンからホストに至るルートにおいてもデータが保護されているということです。データ、トークンのアイデンティティ及び事例カウンタの全てがSHA-1アルゴリズム入力に含まれているため、トークンとホストの間の通信経路でデータビットを変更あるいは注入しようとすれば、その取引は無効になります。すなわち、このチャレンジ・アンド・レスポンスデータ交換を数々の信用できない仲介者が扱ったとしても、プロセスの安全保証は保たれます。遠隔地にあるインターネットのサーバーが、数知れぬルーター、ブリッジ、ハブ及び盗聴者を通じて家庭にあるユーザのトークンの真正証明を行う場合でも、安全保証が全く損なわれません。

安全保証付真正証明トークンにおいてもう一つ重要な条件は、そのトークンが保持している秘密を保護する能力を持っていることです。シリコンチップを埋め込んだプラスチックカードは物理的な攻撃を受けやすく、また通常のメモリデバイスは秘密が保持されている保存エリアを保護する特別な手段を持っていません。安全保証付トークンは、含まれている秘密を保護するために高レベルの物理的な安全保証手段を提供しなければなりません。

暗号技術が提供するもう一つの方法は、各デバイスの秘密が、デバイスに保存されていない別のマスター秘密

と唯一独自のデバイスアイデンティティの組み合わせから引き出されるというものです。これにより、各デバイスに唯一独自の秘密が提供され、ある一つのデバイスの秘密が破れてもシステム全体のブレーク(クラスブレークと呼ばれます)を防止することができます。また、金銭システムは一般にトークンの真正証明用に一つの秘密(トークンの中に保存)を使用し、別の秘密(トークンに保存されない)をトークンに保存されている金銭値の確認用に使用しています。これにより、トークンを物理的に攻撃してもその一つのトークンを模倣できるだけになるため、物理的な攻撃で得られる利益が大きく制限されます。

しばしば見過ごされる攻撃経路は、サービスプロバイダの施設で不謹慎な従業員が真正証明に使用される重要な秘密を知ってしまうことです。この問題を克服するために、暗号技術者はシークレットシェアリングと呼ばれる方法を提供しています。実際の秘密は存在せず、その代わりに2つ以上の部分的な秘密を結合した計算の結果が存在します。サービスプロバイダはこれらの部分的な秘密を離れた場所の別々のシステムに保存し、誰も2つ以上の部分にアクセスできないようにします。全ての部分的な秘密を正しい順番で使用しない限り、実際の秘密を計算することができません。真に効果的な安全保証トークンは、これらの部分的な秘密を全てトークンの中で結合して、最終的な秘密が人間に観察可能な場所に決して存在しないようにしなければなりません。トークンがサービスプロバイダの初期化プロセスの中を進むにつれて、後に続く各々の部分的秘密が注入され、実際の秘密は各デバイスの内側だけで計算されます。最終ステップとして、唯一独自のデバイスアイデンティティがプロセスに注入されるため、その結果得られるデバイスの秘密はそのデバイスの唯一独自のものとなり、マスター秘密は損なわれる可能性のある場所には決して存在しません。

強力な真正証明が可能な安全保証付電子トークンは、ドアロック、アクセス制御機器及び機器制御ロックアウト用の非常に安全保証度の高いキーになります。チャレンジ・アンド・レスポンスを使った電子キーは複製や改変が不可能であり、盗聴しても無益です。このアプリケーションにおいてはデータは静的であるといわれます。なぜなら、eキャッシュアプリケーションと違って使用する度に変化することがないからです。トークンを差し出す人間の真正証明をそのトークンに行わせることにより、(そうしたPIN又はパスワード保護機能を持たないシステムの場合でも)システムの安全保証がさらに強くなります。

対等(ピアツウピア)真正証明アプリケーションにより、ネットワークで結合された電気製品同士が互いに真正確認を行うことができます。これにより、外部の者が操作するのを防ぐことができます。真正確認を迅速に行い、内部の秘密を保護するトークンを使うと、電気製品に必要な物理的な安全保証対策がずっと少なくて済みます。また、トークンを使って制御コマンド又はデリケートなデータを暗号化する唯一独自のセッションキーを生成することができます。

ダラスセミコンダクタのDS1963S iButtonはこれらの要求条件を全て満たす安全保証付の電子トークンです。各トークンは世界的に唯一独自の出荷時レーザ処理済みの64ビットアイデンティティ、リチウム電池でバックアップされた512バイトのNV RAMデータ保存エリア及び8つの保護付64ビット秘密を備えています。これらの全てが小型で頑丈なステンレススチール容器に収められています。このデバイスとの双方向通信は単一データ導体を使って最大140kbpsで行われ、SHA-1は内部で500マイクロ秒以内に実行されます。秘密のサイズが64ビットであるということは、力づくで破るのに約9,223,000,000,000,000,000回の試行を要することを意味するため、力づくの攻撃は非現実的です。iButtonは装身具のように身に付けたり、IDカード又はバッジに付けたり、あるいは鍵のように持ち運ぶことができます。容器や製品あるいは出荷カートンに張りつけることもできます。コンピュータや回路基板に埋め込むことも可能です。

ダラスセミコンダクタのDS1961S iButtonはDS1963SのEEPROMバージョンです。本製品は128バイトのメモリを持ち、デバイスを改変するにはホストシステムがSHA真正証明に合格しなければならないようにした書込み保護方式を提供しています。

また、DS1963Sはホスト側の処理能力と速度に制限のある自動販売機や料金徴収システムにおいてコプロセッサとして貢献します。コプロセッサとして使用された場合、DS1963Sはシステムの秘密を安全に保存・保護し、SHA-1アルゴリズムを非常に迅速に実行し、徴収された料金を安全に保存するほか、徴収ボックス又は自動販売機を識別する世界的に唯一独自のシリアル番号を提供します。コプロセッサとしてのDS1963S iButtonは、ホストが使用する重要な設定及び価格データを保持することもできます。ホストの電子機器は単にiButton間でデータを動かすだけです。eキャッシュシステムにおいては、ここで説明した安全保証機能の全てを使って金銭取引を一通り実行するのに要する時間が50ミリ秒以下です。

DS1961Sはチップの形でも提供されていて、ネットワーク化されたデバイスに埋め込むこともできます(通信は僅か1つのポートで可能です)。これにより、ネットワーク化されたデバイス間での強力な暗号化真正証明が可能になり、インターネットを使ってそれらのデバイスに対する質問や制御を行う新しい可能性が開けました。ネットワーク化されたデバイスは、迅速で信頼性の高い相互真正証明と、データ暗号化用の乱数ベースセッションキー生成の全てを、1つのメッセージを交換するだけで行うことができます。システムの秘密は保護付EEPROMに安全に保存され、ほとんどオーバーヘッドなしでネットワーク化されたデバイスに強力な暗号化安全保証を付加することができます。