# ISO/IEC 9796-2 (Scheme 1) 署名の偽造の報告に関する分析

株式会社富士通研究所 セキュアコンピューティング研究部
産業技術総合研究所 情報セキュリティ研究センター

2009 年 11 月 13 日 (初版)

## 1 概要

国際会議 CRYPTO 2009 (2009 年 8 月 16–20 日) において、電子署名方式の国際標準のひとつである ISO/IEC 9796-2 (Scheme 1) [ISO97, ISO02] の安全性の問題点を指摘する論文 [CNTW09] が発表されました。本稿においては、その解説を行い、それが社会に与える影響を分析します。特に、やむを得ない場合を除き、ISO/IEC 9796-2 (Scheme 1) を使用すべきでないことを指摘し、また、同方式を利用せざるを得ない場合の運用上の注意点を述べます。さらに、ISO/IEC 9796-2 (Scheme 1) の重要な応用先である、次世代 IC 旅券やある種の金融カード (EMV カード) などの安全性を議論し、これらの安全性が直ちに損なわれるわけではないが、可能であればより信頼できる方式に移行するべきであることを指摘します。

本章においては本稿全体の概要を述べ、2 章では [CNTW09] において提案がなされた ISO/IEC 9796-2 (Scheme 1) への攻撃手法の詳細を説明し、3 章では次世代 IC 旅券と EMV カードの安全性について議論を行い、4 章でより一般的な応用における対策を述べます。最後に、5 章で全体のまとめを行います。

### 1.1 ISO/IEC 9796-2 (Scheme 1) について

ISO/IEC 9796-2 (Scheme 1) は、ISO/IEC において国際標準として制定されている電子署名方式の一つであり、メッセージ復元型署名とよばれるものの一種です。しかしながら、この方式は 1999 年にすでに、署名の不正な偽造が理論的に可能であることが指摘されており [CNS99]、2002 年からは、すでに稼働済みで仕様の変更が困難なシステムとの互換性のためだけに ISO/IEC の国際標準として残された形になっております。なお、ISO/IEC では、互換性の問題のためにやむを得ない場合を除き、ISO/IEC 9796-2 (Scheme 2) の利用を推奨しており、また、なんらかの理由で署名者側での乱数生成が難しい場合は、ISO/IEC 9796-2 (Scheme 3) の利用を奨めています。

### 1.2 ISO/IEC 9796-2 (Scheme 1) の安全性に関するこれまでの歴史的経緯

ISO/IEC 9796-2 (Scheme 1) は基本的 に RSA 署名 [RSA76] の実装の一形態であり、したがって、RSA 暗号を本質的に完全解読できない限り、同方式における署名の偽造も不可能となることが期待された設計がなされています。

一方、1985 年に、Desmedt と Odlyzko は、慎重な設計が十分になされていないような RSA 署名の実装に

おいては、RSA 暗号の本質的な完全解読を回避しつつ、署名の偽造を行うことが可能である場合があることを示しています [DO85]。Desmedt と Odlyzko は、署名対象となるデータのハッシュ値に対して単純に (基本的) RSA 署名を施すような実装に対し、同ハッシュ値のサイズがある程度小さい (たとえば、160 ビット) 場合は、いくつか元となるデータのハッシュ値を合成した値を、別のデータのハッシュ値に一致させることが可能であることを利用して署名の偽造を行っています (この攻撃法を Desmedt-Odlyzko 攻撃と呼ぶものとします)。ここで、もし、元となるデータについての署名を得ることが可能であれば、これらの署名を合成した値を、同様に、別のデータの署名に一致させることが可能となります。すなわち、署名の偽造に成功したことになります (この攻撃法を Coron-Naccache-Stern 攻撃と呼ぶものとします)。

さらに、上記のとおり、1999 年には、すでに国際標準化されていた ISO/IEC 9796-2 (Scheme 1) についても類似の攻撃が「理論的」に適用可能であることが示されています。ISO/IEC 9796-2 (Scheme 1) では、Desmedt-Odlyzko 攻撃を踏まえ、サイズの小さなハッシュ値に単純に署名を施すのではなく、同ハッシュ値と既定のデータを連結し、合計サイズが RSA 暗号における法のサイズと同程度に十分に大きくなるようにすることで安全性を高めてはいるものの、ある種の式変形によってそのような効果を取り除くことが可能であることを Coron, Naccache, Stern [CNS99] が明らかにしています。

この結果や、同時期の別の暗号技術に対する諸々の安全性解析の成果をうけて、それ以降では安全性の検証が十分になされた方式以外は積極的に利用すべきでないというコンセンサスが得られています。実際に ISO/IEC 9796-2 (Scheme 2) は、証明可能安全性をもつ、すなわち、RSA 暗号を本質的に完全解読ができない限り署名の偽造が不可能であることが証明されている RSA-PSS-R [BR96] に基づく方式となっています。

## 1.3 Coron-Naccache-Tibouchi-Weinmann 攻撃

ISO/IEC 9796-2 (Scheme 1) は、1999 年の時点ですでに署名の偽造が理論的に可能であることが示されており、利用は推奨されていません。しかしながら、これまで実際に署名の偽造がなされたわけではないことから、既存の稼働済みのシステムとの互換性が必要とされる場合を考慮して、国際標準として現在まで残っています。

それに対し、Coron, Naccache, Tibouchi, Weinmann は、Coron-Naccache-Stern 攻撃を改良し、同攻撃が単に理論的なものではなく、現実的なものとなりうることを示そうと試みています。それが、今回の新たな結果となります。この攻撃では、Coron-Naccache-Stern 攻撃に新たにいくつかの計算テクニックを効果的に導入して、計算速度を飛躍的に向上させることで、1.2 で述べられたような「いくつか元となるデータのハッシュ値を合成した値を、別のデータのハッシュ値に一致させること」を実際に成功させています (この攻撃法を Coron-Naccache-Tibouchi-Weinmann 攻撃と呼ぶものとします)。

したがって、あとはその「元となるデータ」に対する署名さえなんらかの方法で入手することができれば、上述のとおり、「別のデータ」に対する署名を不正に偽造することが可能となります。以上の議論から、Coron-Naccache-Tibouchi-Weinmann 攻撃が機能するためには、

- [攻撃用の署名の入手条件]: 攻撃者が自由に選んだ、署名偽造の対象となるデータを除く任意のデータに対して、その正当な署名を希望通りにいくらでも得られるような状況であること
- [偽造対象データの条件]: 署名を偽造可能なデータは、上記の「元となるデータのハッシュ値」を合成した値と同一のハッシュ値をもつ「別のデータ」に厳しく限定されるため、そのような偽造でも意味をもつような状況であること

の二つの条件を同時に満足する必要があることがわかります。

### 1.4 Coron-Naccache-Tibouchi-Weinmann 攻撃への対策

電子署名の利用がなされている多くの注意深く設計されたアプリケーションにおいては、1.3 で述べられている Coron-Naccache-Tibouchi-Weinmann 攻撃を実行させるための二つの条件は現実的には成立せず、当該攻撃がただちに実利用上の脅威になるものとは必ずしもならないと思われます。たとえば、次世代 IC 旅券や EMV カードにおいても、Coron-Naccache-Tibouchi-Weinmann 攻撃を実行することは困難と考えられます。これらについてのより詳細な議論は、3 章にて行います。

しかしながら、別の言い方をすれば、ISO/IEC 9796-2 (Scheme 1) では自身が内包する数学的な欠点が運用によって守られているとも解釈でき、したがって、同方式を利用する場合は証明可能安全性をもつような他の方式に比べ格段に慎重な扱いが必要となります。

以上を鑑みるに、

- すでに ISO/IEC 9796-2 (Scheme 1) を利用した稼働がなされていて、仕様の変更が困難なシステムについては、1.3 で述べた様な二つの条件が成立しないように細心の注意を払う
- そのような事情がなく、利用する電子署名方式を柔軟に選択できるのであれば、証明可能安全性をもつような、十分に安全性の検証がなされた別の方式を利用する

ことで、対策可能です。より詳細については、4 章において説明を行います。

そのような信頼性の高い電子署名方式については、CRYPTREC [CRY] において電子政府推奨暗号として挙げられているもの (たとえば RSA-PSS [BR96]) などがあります。また、ISO/IEC 9796-2 で制定されているものであれば、上記のとおり RSA-PSS (より正確には、RSA-PSS の亜種である RSA-PSS-R) に基づく方式である ISO/IEC 9796-2 (Scheme 2) も利用可能です。

殊に CRYPTREC において制定された電子政府推奨暗号は、多数の有識者により安全性の検証がなされている技術であるため可能な限り積極的に利用されることを強くお奨めします。

## 2 Coron-Naccache-Tibouchi-Weinmann 攻撃の詳細

### 2.1 Desmedt-Odlyzko 攻撃

1985 年、Desmedt と Odlyzko [DO85] は RSA 署名に対する興味深い攻撃手法を提案しました。この攻撃によれば、署名の対象となるデータの (短い) ハッシュ値を直接 RSA 関数への入力にすることで電子署名を作成するタイプの方式については、RSA 暗号の本質的な解読を回避しながら、署名の偽造が可能となっています。

具体的には、$[d, N, u(\cdot)]$ を署名鍵 (ただし、$u(\cdot)$ は出力長が 160 ビット程度のハッシュ関数) として、署名対象データ $m$ に対する署名を次のように作成する署名方式を考えます:

$$\sigma = u(m)^d \bmod N$$

これに対し、次の要領で署名の偽造を試みます。

まず、ある上界 $B$ を定め、$\{p_1, \ldots, p_L\}$ を $B$ より小さいすべての素数の集合とします。また、$u(m_i)$ が上記集合に含まれる素数の積で表現できるようなメッセージ $m_i$ を (少なくとも) $L+1$ 個探します。これら

$L+1$ 個のうちのひとつ $u(m_j)$ を選び、他の $L$ 個の $u(m_i)$ の線形結合として表現します。さらに、$m_j$ を除く、$L$ 個のメッセージ $m_i$ に対応する $L$ 個の電子署名をなんらかの方法で入手します (与えられたメッセージに対して、その正しい署名を返答する存在は「署名オラクル」と呼ばれています (4.2 を参照))。

これらの署名情報を用いて、以下の要領でメッセージ $m_j$ に対する署名を偽造します。まず、ある値 $x$ のすべての素因数が $B$ より小さくなるとき、$x$ が $B$-smooth であると呼ぶことにします。このとき、上記のように得られた $u(m_i)$ は $B$-smooth となります。そのような $m_i$ の総数を $\tau$ とすると、任意の $m_i$ $(1 \leq i \leq \tau)$ に対して、以下の等式が成り立ちます。

$$u(m_i) = \prod_{z=1}^{L} p_z^{v_{i,z}}$$

次に、公開鍵 (に含まれる) $e$ と 各 $u(m_i)$ に対して、次の $L$ 次元ベクトルを定義します:

$$V_i = (v_{i,1} \bmod e, \ldots, v_{i,L} \bmod e)$$

$\tau \geq L+1$ のとき、あるベクトル (たとえば $V_\tau$) を他のベクトルでの線形結合として表現できます。つまり、ある $\Gamma = (\gamma_1, \ldots, \gamma_L) \in \mathbb{Z}^L$ が存在し、$V_\tau = \Gamma \cdot e + \sum_{i=1}^{\tau-1} \beta_i V_i$ として表すことが出来ます。すなわち、$v_{\tau,z} = \delta_z \cdot e + \sum_{i=1}^{\tau-1} \beta_i \cdot v_{i,z}$ となります。従って、$\delta = \prod_{z=1}^{L} p_z^{\delta_z}$ とおくと、$u(m_\tau)$ は、次のように表すことが出来ます。

$$u(m_\tau) = \delta^e \cdot \prod_{i=1}^{\tau-1} u(m_i)^{\beta_i}$$

最後に、各メッセージ $m_i$ の署名を用いて次のようにメッセージ $m_\tau$ の署名 $\sigma_\tau$ を偽造します:

$$\sigma_\tau = u(m_\tau)^d = \delta \cdot \prod_{i=1}^{\tau-1} (u(m_i)^d)^{\beta_i} = \delta \cdot \prod_{i=1}^{\tau-1} \sigma_i^{\beta_i} \bmod N$$

## 2.2 ISO/IEC 9796-2 (Scheme 1)

ISO/IEC 9796-2 (Scheme 1) では、メッセージの (小さいサイズの) ハッシュ値を直接署名するのではなく、適当な長さになるようにパディングを施したうえで RSA 署名の生成がなされています。より具体的には、ISO/IEC 9796-2 (Scheme 1) において、メッセージを RSA 署名の対象に変換するためのエンコーディング関数 $u(\cdot)$ は次のとおりとなっています (HASH は SHA-1 等のハッシュ関数):

$$u(m) = \mathtt{6A}_{16} \,||\, m[1] \,||\, \mathrm{HASH}(m) \,||\, \mathtt{BC}_{16}$$

ここで、HASH 出力の長さは $k_h$、RSA の法 $N$ の長さは $k$ ビットとします。また、メッセージ $m$ の上位 $k - k_h - 16$ ビットを $m[1]$ とします。

先頭の 1 バイトを $\mathtt{6A}_{16}$ としているのは、前述の Desmedt-Odlyzko 攻撃が直接適用できないよう、$u(m)$ を (素因数分解を困難な程度の) 十分大きい値にするためです。この対策により、Desmedt-Odlyzko 攻撃は直接には ISO/IEC 9796-2 (Scheme 1) に適用できないと考えられます。

## 2.3 Coron-Naccache-Stern 攻撃

上記のとおり、$u(m)$ のサイズが大きくなるような工夫が施されており、Desmedt-Odlyzko 攻撃を直接的に ISO/IEC 9796-2 (Scheme 1) に対して適用することは難しいと考えられています。しかし、逆にいえば、$u(m)$ に対して何らかの変換を施し、そのような工夫の効果を取り除くことができれば、ISO/IEC 9796-2

(Scheme 1) に対して Desmedt-Odlyzko 攻撃が実行可能となります。Coron, Naccache, Stern [CNS99] はそのような変換方法を発見し、ISO/IEC 9796-2 (Scheme 1) が依然として脅威にさらされていることを明らかにしています。Coron-Naccache-Stern 攻撃では、メッセージ $m_i$ のエンコーディング $u(m_i)$ が十分に大きかったとしても、それそのものを素因数分解するのではなく $u(m_i)$ の定数倍の剰余をとることで素因数分解の対象のサイズを小さくしています。

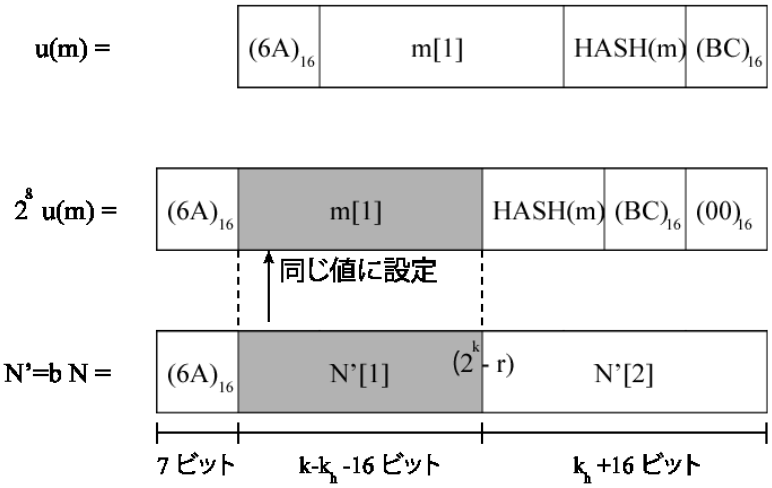


図 1　Coron-Naccache-Stern 攻撃

具体的な手順はつぎのようになります (図 1 に処理の概観を示します)。

1. まず $a = 2^8$ とします。また、ユークリッドの互除法により、次式を満足する整数 $b$ と $r$ $(0 \leq r < N < 2^k)$ を求めます: $(\mathtt{6A}_{16} + 1) \cdot 2^k = b \cdot N + r$
2. 次に、$N' = b \cdot N$ と定義すると、$N' = \mathtt{6A}_{16} \mid\mid N'[1] \mid\mid N'[2]$ と表現できます。この時、$N'$ と $N'[1]$ の長さはそれぞれ $k + 7$、$k - k_h - 16$ ビットとなります。
3. さらに、$m[1]$ を $N'[1]$ と同じ値とします。つまり、$m[1] = N'[1]$ となります。
4. 最後に、$t = N'[2] - (\mathrm{HASH}(m) \mid\mid \mathtt{BC00}_{16})$ とすると、その長さは $k_h + 16$ 以下になります。

HASH 出力の長さは 160 ビット (つまり $k_h = 160$) の場合、$t$ は最長でも 176 ビットとなります。このような変換がなされたデータ $t$ に対して、Desmedt-Odlyzko 攻撃を適用することで RSA 暗号の完全解読を回避して、署名の偽造を行うことが可能となります。たとえば、ハッシュ値の長さが 160 ビットの場合、ISO/IEC 9796-2 (Scheme 1) は 61 ビット安全性しかもたないことがわかりました。ただし、この時点では実際の署名偽造までは至っていませんでした。

ここで、$X$ ビット安全性とは、直感的には、$2^X$ 回の基本的計算処理を繰り返し実行しない限り署名の偽造に成功しないことが保証可能であることをいいます。現状では、実用に耐えうる安全性として、多くのシステムにおいて最低でも 80 ビット安全性が要求されています。1024 ビットの RSA 暗号の完全解読に対する安全性も、80 ビット安全性とほぼ等価であると考えられています。

## 2.4 Coron-Naccache-Tibouchi-Weinmann 攻撃

### 2.4.1 Coron-Naccache-Stern 攻撃との差分

[CNS99] において、Coron らは ISO/IEC 9796-2 (Scheme 1) の安全性が 80 ビット安全性を下回ることを示しましたが、それが実際に現実的な計算時間で実行可能であるかまでは、よくわかっていませんでした。それに対し、2009 年 8 月の国際会議 CRYPTO'09 において、Coron, Naccache, Tibouchi, Weinmann は、Coron-Naccache-Stern 攻撃における各計算ステップを高速に実行するための手法を示し、一般的に使用可能な計算資源のみを用いて同攻撃が実行可能であることを明らかにしました。なお、漸近的な計算コストについては、Coron-Naccache-Stern 攻撃から大きく改善されたわけではありません。

### 2.4.2 効率の改良

Coron, Naccache, Tibouchi, Weinmann は、Coron-Naccache-Stern 攻撃の高速実装に関し、以下の四つの手法が効果的であることを示しました。

- Smoothness 検知アルゴリズムの利用: Desmedt-Odlyzko 攻撃を実行する際、膨大な数のハッシュ値に対し、これらの中から多数の $B$-smooth なハッシュ値を集める必要がありました。これについて、Bernstein [Ber04] によって提案がなされた Smoothness Detection Algorithm (SDA) を利用することで、与えられたハッシュ値が $B$-smooth であるかを高速に判定可能となります。[CNTW09] によれば、この判定処理を従来より約 1000 倍程度高速化可能であるようです。
- Large Prime Variant 法の利用: Bach と Peralta [BP96] により提案された Large Prime Variant 法を用いると、$B$-smooth (に近い) ハッシュ値をもつメッセージの収集をさらに約 1.4 倍高速化可能となります。
- $a$, $b$ の値の最適な選択: 上記の Coron-Naccache-Stern 攻撃においては、最適性をあまり吟味することなく $a = 2^8$ としていますが、より適切な $a$ の値を慎重に選択することで、$t_i$ のサイズを若干小さくすることができます。この手法により、ランダムに作成したハッシュ値が $B$-smooth となる確率が高まり、結果として約 2 倍高速化可能となります。
- 探索空間の拡大: ランダムなハッシュ値の生成をより広範囲に行い、特殊なハッシュ値をもつメッセージのみを探索することでのサイズがより小さくなるようにします。これにより、やはり同様に、そのハッシュ値が $B$-smooth となる確率がさらに高まり、約 2 倍高速化可能となります。

### 2.4.3 Coron-Naccache-Tibouchi-Weinmann 攻撃の評価

Coron-Naccache-Tibouchi-Weinmann 攻撃は、Coron-Naccache-Stern 攻撃に必要となる計算時間を実際に実行可能となるように、必要な各計算処理の高速実装法を示したものといえます。したがって、Coron-Naccache-Tibouchi-Weinmann 攻撃は、Coron-Naccache-Stern 攻撃や Desmedt-Odlyzko 攻撃と同様に、その性質上、それが現実的な社会的被害を引き起こす状況は限られています (詳細については、4 章および 3 章において説明します)。しかしながら、[CNTW09] によれば、2048 ビットの $N$ と出力長が 160 ビットであるような HASH に対し、わずか 2 日の計算時間と 800 米ドルの計算コストで署名の偽造を行うためのデータの作成に成功しています。これらのデータに対応した正規の署名さえ手に入れることさえできれば (ただし約 $2^{20}$ 個必要)、それら以外にもメッセージと署名のペアを、署名鍵を用いることなく作成可能となりえます。

また、Coron らは、彼らの計算実験を Amazon EC2 上で行っており、このような誰でも利用可能な計算資源のみを用いて、しかもわずか 800 米ドルのみで、ここまでの成果を得たことも注目に値します。

# 3 具体的応用における安全性

本章では、ISO/IEC 9796-2 (Scheme 1) の関連技術の利用がなされている具体的応用先として、次世代 IC 旅券と EMV カードを取り上げ、これらの安全性について議論を行います。

## 3.1 次世代 IC 旅券の能動的認証

次世代 IC 旅券 (所謂、電子パスポート) では、正規パスポートの複製 (つまり、ある正規パスポートについて、それと同一の機能を持つものの不正な作成) を防止するための技術として、電子署名を用いた能動的認証プロトコルの導入の検討がなされています [ICAO]。耐タンパー性を持つ IC チップに署名鍵を格納することで、この署名鍵の複製が困難となるようにし、それを利用してパスポート全体の複製も困難にしています。

この能動的認証プロトコルでは、基本的に検証者が選ぶデータ (チャレンジ) に対応した署名を証明者が作成することで、署名鍵の所持を証明しています。前述のとおり ISO/IEC 9796-2 (Scheme 1) で単純にこれを行うと署名オラクルが存在してしまう可能性がありますが、実際には署名の対象となるデータ (チャレンジ) として、検証者が選んだ値だけでなく、証明者自身が選んだ値も部分的に反映させることで、検証者が自由に選んだデータそのものに対応した (ISO/IEC 9796-2 (Scheme 1) における) 署名を検証者が得ることを防いでいます。

より具体的には、この能動的認証プロトコルに対して Coron-Naccache-Tibouchi-Weinmann 攻撃を行う際、攻撃の過程において攻撃者の選択の余地が (ほとんど) なく 848 ビットのある値 M1 が自動的に定まり ($N$ が 1024 ビットの場合)、攻撃を成功させるためには、攻撃者は署名オラクルから先頭 848 ビットが M1 であるようなデータに対する署名を膨大な数だけ受け取る必要があります。しかしながら、このプロトコルでは、(ISO/IEC 9796-2 (Scheme 1) における) 署名の対象となるデータの先頭 848 ビットは検証者ではなく、証明者である IC チップが内部でランダムに選ぶことになっているため、(検証者の立場である) 攻撃者は先頭 848 ビットが M1 であるようなデータに対する署名を受け取ることができません。したがって、検証者を Coron-Naccache-Tibouchi-Weinmann 攻撃が実行するために有効な情報を引き出すための署名オラクルとして利用することが出来ていないことがわかります。

ただし、本プロトコルにおいて、仮に、なんらかの方法で署名対象データの先頭 848 ビットを IC チップの外部から制御することが可能であれば、これが M1 となるように操作することで、Coron-Naccache-Tibouchi-Weinmann 攻撃を実行することが可能となります。しかし、そのような操作を行うためには IC チップの耐タンパー性を破る必要があるため、実際にそれを実行することは容易ではありません。別の言い方をすれば、電子パスポートにおける能動的認証プロトコルでは、署名の対象となるデータの先頭 848 ビットを外部から制御できないような耐タンパー性が重要な役割を担っていることがわかります。

以上をまとめると、電子パスポートに関し、現在までに検討されている ISO/IEC 9796-2 (Scheme 1) を用いた能動的認証プロトコルに対して、Coron-Naccache-Tibouchi-Weinmann 攻撃をただちに適用することは困難であると思われます。しかし、上記のとおり、それほど自明と言えない処理やそれを支える耐タンパー性によって署名オラクルの実効的な利用が防がれていることがその根拠となっていますので、運用する際はそのような仕組みを理解し、それが正しく機能しているかを常に把握しておくことが重要であると考えられます。

また、ISO/IEC 9796-2 (Scheme 1) は安全性の証明がついていないため、今後どのような新たな脅威にさらされるかについて不確実です。そのようなことからも、可能であればたとえば 4.1 で紹介されているような信頼性の高い方式への移行も検討すべきと思われます。次世代 IC 旅券の Coron-Naccache-Tibouchi-Weinmann 攻撃に対する安全性は [SIT+09] でも議論されています。

### 3.2 EMV 署名

クレジットカード決済等の電子商取引に利用するための IC カードの仕様として、EMV 仕様がよく知られています。EMV とは、Europay International, MasterCard International, Visa International の頭文字を並べたものであり、これら 3 社によって定められ、その後、これに JCB と American Express が加わっています。(Europay International は 2002 年に MasterCard と合併。)

EMV 仕様においては、IC カードの正当性の保証のために内部の複数の箇所で、ISO/IEC 9796-2 (Scheme 1) に準拠した電子署名方式を利用しています。しかしながら、これらの対して Coron-Naccache-Tibouchi-Weinmann 攻撃を実行するためには署名オラクルの自由な利用が必要となり、実際にはそれは極めて困難です。これは、署名の対象となるデータの形式は厳しく定められているために、攻撃を成功させるためにはどのようなデータに対する署名を得られれば都合が良いかがわかっていても、そのような恣意的な (おそらく意味をもたない) データに対する署名を、正当な署名者に作成させることはほとんど不可能であることによります。また、[CNTW09] の文中にも、そのような処理上の理由によって、EMV 仕様による IC カードの安全性が実際に脅かされることはないと述べられています。しかしながら、攻撃手法のさらなる改良などにより、今後も安全性が維持される保証はなく、もし可能であるならばより信頼性の高い方式への移行が望まれます。

## 4 一般的な対策について

本章では、Coron-Naccache-Tibouchi-Weinmann 攻撃を回避するための一般的対策について議論を行います。

### 4.1 より信頼できる方式の利用

Coron-Naccache-Tibouchi-Weinmann 攻撃を回避するための最も確実な対策は、そもそも ISO/IEC 9796-2 (Scheme 1) を利用せず、より高い信頼性をもつ方式を利用することです。その際、特に CRYPTREC によって制定された電子政府推奨暗号リストなどを参考に、すでに有識者によって詳細な安全性の検証が行われている暗号技術を適切に選択することが重要となります。2009 年 9 月現在、電子政府推奨暗号リストに記載される電子署名方式は、DSA, ECDSA, RSA-PSS, RSASSA-PKCS1 v1_5 となっていますが、RSASSA-PKCS1 v1_5 に関しては、ISO/IEC 9796-2 (Scheme 1) と同様に「既存システムとの整合性をとる目的以外では使用されるべきではない。(p.6, http://www.cryptrec.go.jp/report/c08_listguide2008_signature_v7.pdf)」とされていますので、 DSA, ECDSA, RSA-PSS のうちのいずれかを用いるのがよいと考えられます。

### 4.2 署名オラクルの排除

ISO/IEC 9796-2 (Scheme 1) に強く依存して稼働しているシステムで、他のより信頼性の高い方式への移行が困難な場合は、Coron-Naccache-Tibouchi-Weinmann 攻撃が実行可能な状況であるかを慎重に確認する

必要があります。特に、署名オラクルとなるものが存在しないことを精査することが肝要です。

署名オラクルとは、攻撃者によって選ばれたデータが送信されると、それに対する正しい署名を回答するような存在を言います。Coron-Naccache-Tibouchi-Weinmann 攻撃を実行するためには、攻撃者が署名オラクルを利用可能でなければなりません。署名オラクルが利用可能であるような状況は起こりえないようにも感じられますが、その一方で絶対に起こりえないとも言い切れません。署名対象となるデータが、署名者の意志だけによって定まるとは限らない場合は、署名オラクルが潜在的に生じやすい状況となるので特に注意が必要となります。

署名オラクルとなるものが生じないようにするためには、どのようなデータが署名対象となりうるか、また、それらについて署名者の意志だけに依存していない部分がどこであるかを把握することが必要です。たとえば、検証者側がランダムに作成したデータ (チャレンジ) $C$ を証明者に送り、証明者側が $C$ に対する電子署名を返答することで、正しい署名鍵を所持していることを証明するような認証プロトコルを考えます。すると、悪意ある検証者がチャレンジ $C$ をランダムに選ばず、自分自身が興味がある値を恣意的に選択することで証明者を署名オラクルとして利用できていることがわかります。したがって、この認証プロトコルにおいて、ISO/IEC 9796-2 (Scheme 1) 署名を単純に利用した場合、安全とはならない恐れがあります。

### 4.3 署名対象データのフォーマットの厳格化

仮に署名オラクルとなりうるものが存在し、Coron-Naccache-Tibouchi-Weinmann 攻撃が実行可能であったとしても、攻撃者は任意のデータに対する署名を自由に作成できるわけではありません。したがって、実際に署名の対象となりうるデータのフォーマットを厳格に定め、そのフォーマットから外れたものを正当なデータとみなさないことで Coron-Naccache-Tibouchi-Weinmann 攻撃を無力化することも可能です。(しかしながら、本来であれば署名鍵が無い限り作成不可能なデータを、第三者が作成可能であること自体、不安を抱かせるものです。したがって、それさえも回避することが望まれます。)

## 5 結論

本稿では、一定の条件が整えば Coron-Naccache-Tibouchi-Weinmann 攻撃により、電子署名方式の国際標準の一つである ISO/IEC 9796-2 (Scheme 1) において、実行可能な計算時間で署名の偽造を行うことができることを述べました。ここで求められる条件は、あまり現実的なものではないため、ISO/IEC 9796-2 (Scheme 1) に基づくすべてのシステムが直ちに利用できなくなるわけではありません。また、具体的な応用先である次世代 IC 旅券や EMV カードに対しても、この攻撃を単純に適用することが困難であることも確認しました。しかしながら、Coron-Naccache-Tibouchi-Weinmann 攻撃の存在は、ISO/IEC 9796-2 (Scheme 1) の今後の使用について不安を抱かせるに十分な脅威と考えられます。したがって、特段の理由がない限り ISO/IEC 9796-2 (Scheme 1) の利用は避け、CRYPTREC で制定された電子政府推奨暗号リストに記載の電子署名方式やそれと同等レベルと考えられるもののみを利用することを強くお奨めします。稼働済みのシステムで、他の署名方式への移行が難しいものについては、Coron-Naccache-Tibouchi-Weinmann 攻撃の適用可能性について慎重に検討を行っていく必要があります。

## 参考文献


[BP96] E. Bach, R. Peralta, Asymptotic semismoothness probabilities, Mathematics of Computation 65(216), 1996, pp. 1701–1715.

[BR96] M. Bellare and P. Rogaway, The Exact security of digital signatures: How to sign with RSA and Rabin, Proceedings of EUROCRYPT '96, LNCS, vol. 1070, Springer-Verlag, 1996, pp. 399–416.

[Ber04] D.-J. Bernstein, How to find smooth parts of integers (2004/05/10), preprint.

[CNS99] J.-S. Coron, D. Naccache and J.P. Stern, On the security of RSA padding, Proceedings of CRYPTO '99, LNCS, vol. 1666, Springer-Verlag, 1999, pp. 1–18.

[CNTW09] J.-S. Coron, D. Naccache, M. Tibouchi and R.-P. Weinmann, Practical cryptanalysis of ISO/IEC 9796-2 and EMV signatures, Proceedings of CRYPTO 2009, LNCS, vol. 5677, Springer-Verlag, 2009, pp. 428–444. Full version available from IACR eprint archive http://eprint.iacr.org/2009/203

[CRY] Cryptography Research and Evaluation Committees, Japan. http://www.cryptrec.go.jp/

[DO85] Y. Desmedt and A. Odlyzko, A chosen text attack on the RSA cryptosystem and some discrete logarithm schemes, Proceedings of CRYPTO '85, LNCS, vol. 218, Springer-Verlag, 1986, pp. 516–522.

[ICAO] ICAO NTWG, PKI for Machine Readable Travel Documents Offering ICC Read-Only Access, Technical Report, Version 1.1, October 01, 2004.

[ISO97] ISO/IEC 9796-2, Information technology – Security techniques – Digital signature scheme giving message recovery, Part 2: Mechanisms using a hash-function, 1997.

[ISO02] ISO/IEC 9796-2:2002, Information technology – Security techniques – Digital signature schemes giving message recovery – Part 2: Integer factorization based mechanisms, 2002.

[RSA76] R. Rivest, A. Shamir and L. Adleman, A method for obtaining digital signatures and public key cryptosystems, Communications of the ACM, vol. 21, 1978, pp. 120–126.

[SIT+09] 酒見, 伊豆, 武仲, 野上, 森川, 署名偽造攻撃の次世代電子パスポートへの適用, コンピュータセキュリティシンポジウム 2009 予稿集, B5-3, 2009.


### 担当著者


- 花岡 悟一郎 (産業技術総合研究所 情報セキュリティ研究センター セキュリティ基盤技術研究チーム)
- Attrapadung, Nuttapong (産業技術総合研究所 情報セキュリティ研究センター セキュリティ基盤技術研究チーム)
- 崔 洋 (産業技術総合研究所 情報セキュリティ研究センター セキュリティ基盤技術研究チーム)
- 伊豆 哲也 (株式会社富士通研究所 ソフトウェア＆ソリューション研究所 セキュアコンピューティング研究部)
- 武仲 正彦 (株式会社富士通研究所 ソフトウェア＆ソリューション研究所 セキュアコンピューティング研究部)
- 酒見 由美 (岡山大学大学院 自然科学研究科 情報伝送学研究室)
- 渡辺 創 (産業技術総合研究所 情報セキュリティ研究センター セキュリティ基盤技術研究チーム)

- 大岩 寛 (産業技術総合研究所 情報セキュリティ研究センター ソフトウェアセキュリティ研究チーム)
- 山口 利恵 (産業技術総合研究所 情報セキュリティ研究センター セキュリティ基盤技術研究チーム)
- 古原 和邦 (産業技術総合研究所 情報セキュリティ研究センター 主幹研究員)

**本稿に関する連絡先**

- security_white_paper@ml.fujitsu.com