L-039

携帯電話を用いた電子印鑑システムの改良と出席通知システムへの適用実験

Improvements on a digital stamp using a mobile phone and its application to a roll call system

吉見 貴彦† 野口 健一郎‡
Takahiko Yoshimi Kenichiro Noguchi

1．はじめに

これまで携帯電話を利用した電子印鑑システムの作成実験を行ってきた[1]。本研究では、署名処理における PC と携帯電話の処理分担を不要にし、処理の全てを携帯電話上で実装し、使いやすさと安全性の向上を図った。また、署名計算処理部分の性能評価を行い改善を図った。

応用例として、携帯電話を利用した授業の出席通知システムの構築実験を行った。

2. システムの概要

(1) 電子印鑑システム

電子署名の信頼性を高めるため、署名のための秘密鍵を携帯電話に持たせる。携帯電話の SD メモリカード内の文書に秘密鍵を用いて署名処理を行い、署名された文書を再び SD メモリカードに出力する。署名処理は XML 署名規格[2]に従って行う。

(2) 出席通知システム

携帯電話を出席通知システムのクライアントに適用する。携帯電話のアプリケーションで入力フォームからの入力を元に XML 形式の出席通知文書を編集し、秘密鍵で署名後ネットワークを通じて管理サーバに送信する。

3. 研究課題

(1) 電子印鑑システムの使いやすさと安全性の向上
(2) RSA 署名計算速度の改善
(3) 携帯電話を使った出席通知システムへの応用

4. 電子印鑑システムの使いやすさと安全性向上

SD メモリカードを文書の移動媒体兼ストレージとして用いることと、携帯電話用 XML パーサである kXML などを実装することで PC と携帯電話の処理分担をなくし、携帯電話上で全ての処理を行うようにし、使いやすさと安全性の向上を図った(図 1)。

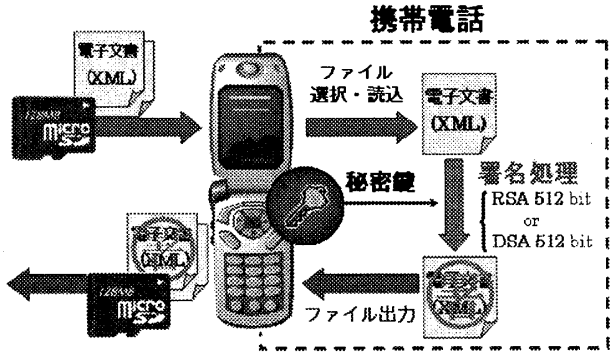

図 1 電子印鑑システムの概要

署名方式にはこれまで RSA だけを用いていたが、米国政府標準の電子文書認証方式である DSA を新たに実装することで署名方式の選択を可能にした。DSA の秘密鍵長は 512bit を採用した。

5. 署名計算速度の向上

(1) 多倍長整数演算プログラムの改善

これまでの多倍長整数演算プログラムについて、多倍長整数データの扱い方や四則演算などを作成し直すことで、演算処理性能の向上を図った。

(2) モンゴメリ乗算の適用

冪乗剰余算はバイナリ法を用いることにより高速化できる。バイナリ法では $a \cdot b \bmod N$ という計算を繰り返し行い、その際処理の重い剰余算を伴う。剰余算や除算を一切使うことなく加減乗算のみで $a \cdot b \bmod N$ を計算可能にする方法があり、それがモンゴメリ乗算である[3]。

冪乗剰余算に対してバイナリ法にモンゴメリ乗算を適用し実装することで、RSA 署名計算速度の更なる高速化を図った。

(a) モンゴメリ乗算に必要な値とその条件

モンゴメリ乗算を用いるためには、次の条件を満たす値が必要となる。

・ $R = 2^n$ (n : N のビット長、N は奇数)とモジュロ N におけるその逆元 R^{-1}, $0 < R^{-1} < N$
・ $R \cdot R^{-1} = N \cdot N' + 1$ を満たす N', $0 < N' < R$

(b) モンゴメリ乗算関数

モンゴメリ乗算では $a \cdot b \bmod N$ の計算を行う代わりに $A = aR \bmod N$, $B = bR \bmod N$ を求め、$ABR^{-1} \bmod N$ の計算を行う。$ABR^{-1} \bmod N$ の計算は次の関数で行える。

```
function REDC(A, B)
[Step 1] x = A · B
[Step 2] u = (x + (x · N' mod R) · N)/R
[Step 3] if(u ≥ N) then return u − N
         else return u
```

剰余算や除算が含まれているように見えるが、法 R は 2 の冪乗であるため、$\bmod R$ は剰余算は使わずに下位ビットから n ビットだけ残せばよい。また、$(x + (x \cdot N' \bmod R) \cdot N)$ は R で割り切れることが証明でき、除算を用いる代わりにシフト演算で済む。

(c) 冪乗剰余関数 ($a^e \bmod N$)

モンゴメリ乗算を使ったバイナリ法は次のようになる。[Step 3]のバイナリ法で乗算をモンゴメリ乗算にしている。

† 神奈川大学理学部情報科学科（現在 NEC ソフト株式会社）
‡ 神奈川大学理学部情報科学科

function $modPow(a, e, N)$
[Step 1] $A = REDC(a, R^2 \bmod N)$
[Step 2] $X = REDC(1, R^2 \bmod N)$
[Step 3] for $i = l-1$ downto 0
$X = REDC(X, X)$
if$(e_i = 1)$ then $REDC(X, A)$
[Step 4] return $x = REDC(X,1)$

6. 出席通知システムへの適用

携帯電話と管理サーバにより構成される（図 2）。管理サーバは Web サービスサーバとして実現した。

(1)携帯電話側の機能

①出席情報の入力による出席通知文書の作成

ユーザは出席通知アプリケーションの入力フォームに出席情報の入力を行い、出席通知文書を作成する。

②位置情報と時刻の取得による不在の防止

携帯電話に搭載される GPS 機能により、位置情報と時刻を自動的に取得する。この情報は通知文書に付加される。これにより教室外からの出席通知を防ぐ。

③電子署名による本人確認

作成された出席通知文書に携帯電話の固有 ID を加え、本人の秘密鍵で署名を行う。電子署名の非否認性により本人確認が可能となり、他者による代返を防止できる。

④管理サーバへの出席通知文書の送信

SOAP を利用して管理サーバに出席通知文書を送る。その後、受領通知を受け取るとそれを画面に表示する。

(2)管理サーバ側の機能

①出席通知文書の検証と保存

受信した出席通知を検証し、結果に応じて携帯電話側に受領通知を返し、通知文書とログをディスク上に出力する。

②座席表の作成

出席情報のログを元に、Web ブラウザから閲覧可能な座席表を作成する。教員や学生が管理サーバにアクセスすることでそれを確認できるようにした。

7. 評価

7.1 性能評価

多倍長整数演算プログラムの冪乗剰余算の性能を評価した(表 1)。$a^e \bmod N$ の測定において a:160bit の値に対して、e:166bit と N:169bit、e:510bit と N:512bit の 2 組を用いて、実機上で測定した。性能改善を確認できた。

表 1. 冪乗剰余算に要する時間の比較
①バイナリ法のみ(改善したプログラム)
②バイナリ法＋モンゴメリ乗算

N のビット長		169 bit	512 bit
実機 P903i	①	1978 ms	17347 ms
	②	93 ms	920 ms

7.2 出席通知システム

GPS 機能は屋内の教室では大きな誤差が出て、キャンパス内に居るかどうかの判定程度にしか使えない。

8. 今後の課題

(1) REDC( )内の乗算部分を in-line でコーディングするなどの高速化を図る

(2) XML 文書の正規化を実装する

謝辞

システム構築に際し、kXML および kSOAP、XmlPull Parser、The Bouncy Castle Crypto Package (DSA の実装) を使用しました。これらの開発者に感謝致します。

参考文献

[1] 星 耕平、野口 健一郎："携帯電話を利用した電子印鑑システムの作成実験", FIT(情報科学技術フォーラム) 2006.

[2] XML-Signature Syntax and Processing, W3C Recommendation, 2002.

[3] Çetin Kaya Koç, Tolga Acar, Burton S. Kaliski, Jr："Analyzing and Comparing Montgomery Multiplication Algorithms", IEEE Micro, pp.26-33, 1996.

[4] 琴浦 崇、宇田 隆哉、星 徹、松下 温："携帯電話を用いた出席率を向上させる出席管理システム", DICOMO 2006, pp.881-884.

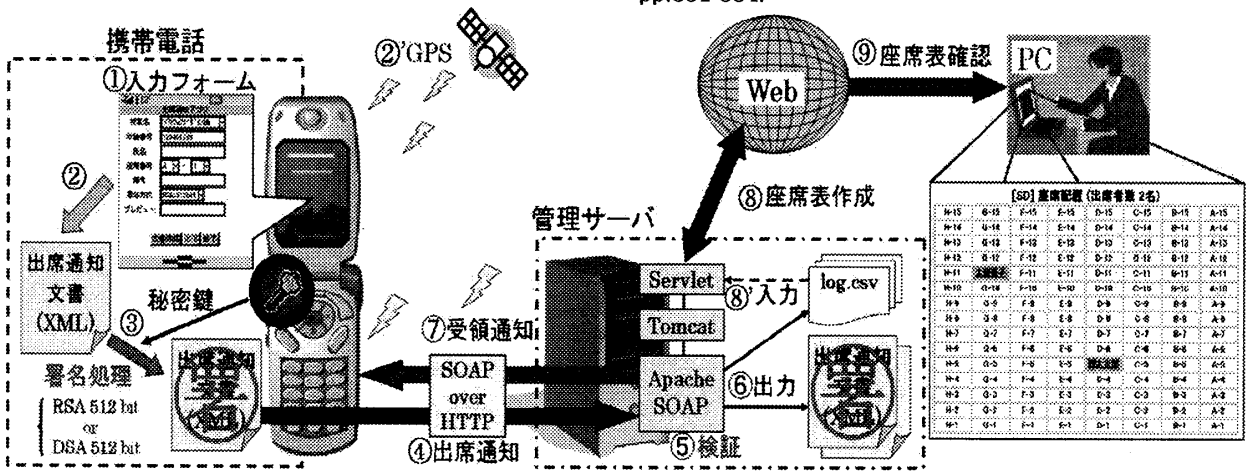

図 3. 携帯電話を用いた出席通知システムの概要