2F-4

楕円署名アルゴリズムの実装と評価(2)
－PKIへの適用 －

辻　宏郷 、齋藤 和美 、太田 英憲
三菱電機(株) 情報技術総合研究所

1. はじめに

今回、PKI暗号ライブラリを拡張し、公開鍵暗号アルゴリズムに楕円署名(ECDSA)アルゴリズムを適用した楕円署名ライブラリを開発した[1]。本稿では、ライブラリを実装する過程において生じた、PKIへの楕円署名アルゴリズム適用の際の留意点を述べる。また、既存のRSA署名ライブラリと楕円署名ライブラリの速度面における比較結果も併せて報告する。

2. 楕円署名アルゴリズムのPKIへの適用

米国標準ANSI X9.62 仕様[2]に準拠する楕円署名ライブラリの実装にあたり、特に以下に示すデータ形式に留意して、PKIへの適用を図った。

2. 1. 公開鍵データ形式

楕円署名ライブラリを用いると、公開鍵は、鍵オブジェクトから設定及び取得可能である。データ形式は、楕円曲線パラメータと公開鍵を、各構成要素を含む構造体形式とASN.1 符号化形式のいずれも利用できる。ASN.1 符号化形式を利用すると、公開鍵証明証内部の保持形式と同一なので、証明証作成時や証明証から公開鍵を取得する場合に、容易に用いる事ができる(図1)。

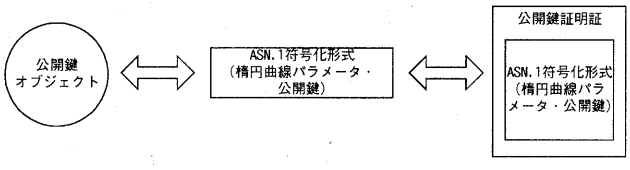

図1 公開鍵の証明証への適用

2. 2. 署名データ形式

署名データは、署名生成オブジェクトから取得可能、また署名検証オブジェクトから設定可能である。署名データの構成要素は、(r,s)の整数の組により表わされる。PKIに適用される署名メッセージ形式として組み込むには、オクテット列へ変換する必要がある。本ライブラリでは、公開鍵と同様に ASN.1 符号化形式での設定及び取得が可能なので、メッセージ形式への組み込みやメッセージ形式からの取得も容易となる(図2)。

図2 署名のメッセージ形式への適用

3. RSA 署名ライブラリと楕円署名ライブラリの比較

RSA アルゴリズムと楕円署名アルゴリズムの速度面での比較を行うために、既存の RSA 署名ライブラリと今回実装した楕円署名ライブラリの各処理時間の測定を行った。

3. 1. 測定方法

公開鍵対の生成処理、20 バイトの平文を用いた書名生成処理、署名検証処理の 3 処理について、その処理時間を測定した。測定に使用した鍵の長さは、RSA アルゴリズムの場合、512、1024、1536、2048、3072ビットである。楕円署名アルゴリズムの場合、鍵の長さと楕円曲線パラメータは、ANSI 仕様に例として記載されている prime192v1、prime192v2、prime192v3、prime239v1、prime239v2、prime239v3、prime256v1を用いた。署名アルゴリズム及びデータ形式は、RSA の場合、PKCS #1 仕様[3]に準拠し、楕円署名の場合、ANSI X9.62 仕様に準拠している。

3. 2. 測定結果

測定は、Pentium II 266MHz の AT 互換機の計算機で行った。公開鍵対の生成処理、署名生成処理、署名検証処理の順に、RSA アルゴリズム(以下、RSA 方式)と楕円署名アルゴリズム(以下、楕円署名

Application of Elliptic Curve Digital Signature Algorithm to Cryptographic Library for Public Key Infrastructure (2) – Applying to Public Key Infrastructure –

Hirosato TSUJI, Kazumi SAITO , Hidenori OHTA
Information Technology R&D Center, Mitsubishi Electric Corporation

方式)それぞれ対応する鍵長毎に処理時間(単位:秒)を示す(表 1、表 2、表 3)。鍵長の対応は、SECG (The Standards for Efficient Cryptography Group)の SEC2[4]を参照した。

RSA方式		楕円署名方式	
鍵長	速度(秒)	速度(秒)	鍵長
512	0.413	-	
1024	2.522	-	
1536	10.848	0.041	prime192v1
		0.040	prime192v2
		0.039	prime192v3
2048	22.093	-	
-		0.146	prime239v1
		0.143	prime239v2
		0.142	prime239v3
3072	137.075	0.153	prime256v1

表1 公開鍵対生成処理時間測定結果

RSA方式		楕円署名方式	
鍵長	速度(秒)	速度(秒)	鍵長
512	0.011	-	
1024	0.032	-	
1536	0.087	0.073	prime192v1
		0.072	prime192v2
		0.073	prime192v3
2048	0.179	-	
-		0.282	prime239v1
		0.289	prime239v2
		0.283	prime239v3
3072	0.507	0.305	prime256v1

表2 署名生成処理時間測定結果

RSA方式		楕円署名方式	
鍵長	速度(秒)	速度(秒)	鍵長
512	0.002	-	
1024	0.005	-	
1536	0.007	0.048	prime192v1
		0.048	prime192v2
		0.047	prime192v3
2048	0.003	-	
-		0.160	prime239v1
		0.161	prime239v2
		0.160	prime239v3
3072	0.013	0.173	prime256v1

表3 署名検証処理時間測定結果

4. 考察

公開鍵対生成処理については、楕円署名方式の方が高速である。署名の検証処理については、RSA 方式の方が高速ではあるが、署名生成処理は、RSA 1536 ビット未満で、ほぼ同等、1536 ビット以上では楕円署名方式の方が高速であった。結論として、公開鍵対生成処理については、楕円署名方式の有効性が認められる。署名の生成及び検証については、RSA 方式では行われていない署名データの ASN.1 符号化及び復号処理が影響しているためか、RSA 方式と同等以下という結果となった。しかし、RSA 方式と比較して短い鍵長を利用して、より低性能の計算機への利用は容易である。また、公開鍵をセッション鍵として利用する場合は、セッション毎に異なる鍵を用いるため、頻繁に鍵生成が行われる。このような場合、楕円署名方式の方が有効である。

5. おわりに

本稿では、楕円署名アルゴリズムのPKIへの適用に際しての留意点と、実装したライブラリを用いて、RSAアルゴリズムと楕円署名アルゴリズムの鍵生成処理、署名生成処理、署名検証処理速度の比較を行った。

参考文献

[1] 辻・齋藤・太田, “楕円署名アルゴリズムの実装と評価(1) – 楕円署名ライブラリ –”, 情報処理学会第 61 回全国大会 2F-3, 2000.

[2] ANSI X9.62-1998, “Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm(ECDSA)”, 1999.

[3] RSA Laboratories, “PKCS #1:RSA Cryptography Standard”, Version 2.0, Oct. 1998.

[4] SECG, “SEC2:Recommended Elliptic Curve Domain Parameters”, Working Draft Version 0.6, Oct. 1999.