2F-3

楕円署名アルゴリズムの実装と評価(1)
ー楕円署名ライブラリ ー

齋藤 和美 、辻 宏郷 、太田 英憲
三菱電機(株) 情報技術総合研究所

1. はじめに

PKI(Public Key Infrastructure)は、公開鍵暗号技術を用いて暗号化や電子署名を実現するための基盤技術である。我々は、PKIに必要な各種機能を実装したPKI暗号ライブラリ[1]を開発中であるが、今回、公開鍵暗号アルゴリズムに、既存の RSA アルゴリズムに加えて、米国標準 ANSI X9.62[2]に準拠した楕円署名暗号アルゴリズムを実装した楕円署名ライブラリを開発した。本稿では、同ライブラリの構成及び特徴について報告する。

2. PKI暗号ライブラリ

PKI暗号ライブラリは、PKIの構成要素である各種機能を実現するライブラリ群から構成される。ライブラリ群は、公開鍵暗号や共通鍵暗号等の暗号アルゴリズムの実装に加えて、公開鍵や公開鍵証明証の管理機能、署名・暗号化メッセージ形式の作成機能等を実現する。PKI 暗号ライブラリは、以下に示す特徴を持つ。

(1) PKI に必要な機能を、基本暗号処理、電子署名処理、証明証管理、鍵管理、証明証検証、パスワードベース暗号処理、暗号化・鍵交換処理、ASN.1 符号化の各機能に分割し、ライブラリとして実装した。

(2) 暗号処理、証明証やメッセージ形式は、国際標準規格や業界標準規格に準拠している。

(3) 各機能は、暗号アルゴリズムから独立したAPIと実際に暗号処理を行う CSP の交換によって、暗号アルゴリズムの種類や強度、公開鍵や証明証の格納デバイス、証明証の検証方法等の変更や拡張が可能である。

3. 従来の署名ライブラリ

PKI暗号ライブラリが実現する各機能の中で、電子署名処理を実現する署名ライブラリには、RSA 暗号アルゴリズムを適用した RSA 署名ライブラリがある。暗号アルゴリズム及びデータ形式は、業界標準であるPKCS #1に準拠している。RSA署名ライブラリは、RSA 公開鍵対生成機能、署名生成機能、署名検証機能の他に、公開鍵及び秘密鍵のデータ変換機能を保有する。鍵のデータ形式は、public exponent や modulus 等構成要素を含む構造体形式と、PKCS #1 に規定された ASN.1 符号化形式を利用可能である。各々の形式は相互に変換可能である。RSA 署名ライブラリの構成を以下に示す。

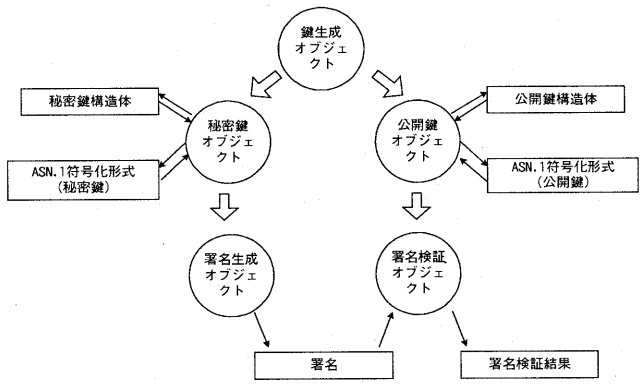

図1 RSA 署名ライブラリの構成

RSA 署名ライブラリは、鍵オブジェクト、鍵生成オブジェクト、署名生成オブジェクト、署名検証オブジェクトの 4 オブジェクトから構成される(図1)。

(1) 鍵オブジェクト

鍵オブジェクトは、公開鍵オブジェクトと秘密鍵オブジェクトからなる。鍵オブジェクトを用いて、鍵データを、構成要素を含む構造体形式と PKCS #1 準拠の ASN.1 符号化形式にて設定及び取得可能である。また、各々のデータ形式を相互に変換可能である。

(2) 鍵生成オブジェクト

鍵生成オブジェクトは、鍵長や public exponent 等の鍵生成情報から公開鍵対を生成し、公開鍵オブジ

Application of Elliptic Curve Digital Signature Algorithm to Cryptographic Library for Public Key Infrastructure (1) – Elliptic Curve Digital Signature Library –

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

ェクトと秘密鍵オブジェクトを作成する。

(3) 署名生成オブジェクト

署名生成オブジェクトは、秘密鍵オブジェクトと署名対象のデータを用いて、署名を生成する。

(4) 署名検証オブジェクト

署名検証オブジェクトは、公開鍵オブジェクト、署名対象のデータ及び署名を用いて、署名を検証し、検証結果を出力する。

4. 楕円署名アルゴリズムの適用

今回、署名ライブラリに楕円署名アルゴリズムを適用し、ANSI X9.62 に準拠する楕円署名(ECDSA)の公開鍵対生成、署名生成及び署名検証を実現する楕円署名ライブラリを開発した。同ライブラリの構成及び特徴を以下に示す。

4.1. 構成

楕円署名ライブラリは、鍵オブジェクト、鍵生成オブジェクト、署名生成オブジェクト、署名検証オブジェクトから構成される(図2)。鍵オブジェクトは、公開鍵オブジェクトと秘密鍵オブジェクトからなり、楕円曲線パラメータと鍵の構成要素を含む構造体あるいはASN.1 符号化形式で設定及び取得が可能である。但し、秘密鍵の ASN.1 形式は、現在の仕様では未公開のため利用不可である。鍵オブジェクトは、構造体形式とASN.1形式の相互変換も可能である。鍵生成オブジェクトは、指定された楕円曲線パラメータに基づき、公開鍵対を生成し、公開鍵オブジェクトと秘密鍵オブジェクトの対として作成する。署名生成及び署名検証オブジェクトは、ANSI X9.62 に準拠した署名アルゴリズムを用いて、署名を生成・検証する。署名データ形式は、構成要素を含む構造体形式と ASN.1 形式のいずれでも取得可能である。

4.2. 特徴

楕円署名ライブラリの特徴を以下に示す。

(1) 既存の署名ライブラリAPIと等価

ライブラリの構成や関数の処理手順は、既存の RSA 署名ライブラリとほぼ同一である。これにより、従来からのライブラリ利用者も容易に理解することができ、開発効率も向上する。

(2) ANSI仕様準拠の標準形式

鍵生成や署名生成、署名検証アルゴリズムに加えて、鍵データや署名データのデータ形式をANSI仕様に規定されている ASN.1 形式を利用可能とした。これにより、PKIへの組み込みが容易となる。

(3) 楕円曲線パラメータの指定方法の簡素化

楕円曲線パラメータの指定方法を簡易にした。利用可能な曲線は、ANSI仕様に例として記載されている楕円曲線パラメータを含む全 15 種類である。各パラメータを設定する代わりに、オブジェクト識別子を用いて鍵生成オブジェクトや鍵オブジェクトに指定すれば良い。

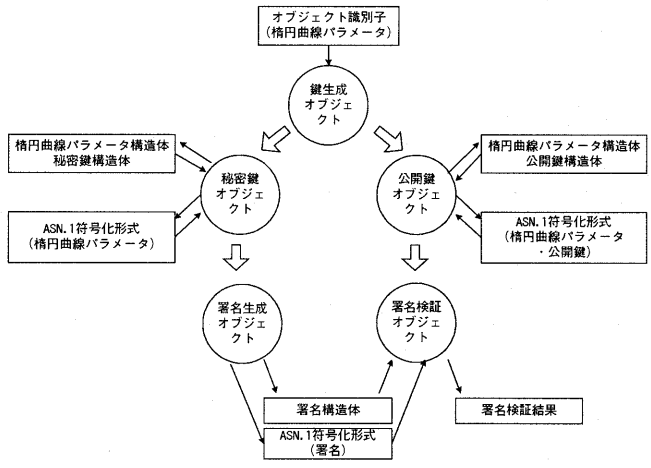

図 2 楕円署名ライブラリの構成

5. おわりに

本稿では、楕円署名アルゴリズムのPKI暗号ライブラリへの適用について述べた。今後は、各楕円曲線パラメータの設定も可能とし、利用者の用途を拡大する。また、楕円暗号を用いた鍵交換や暗号処理のPKIへの適用についても検討する。

参考文献

[1] H.Tsuji, K.Saito, H.Sakakibara, T.Yoneda, "Cryptographic Library Architecture for Secure Application Development", 電子情報通信学会研究報告 ISEC97-47, 1997.

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

[3] 辻・齋藤・太田, "楕円署名アルゴリズムの実装と評価(2) – PKI への適用 –", 情報処理学会第61回全国大会 2F-4, 2000.