公開鍵暗号

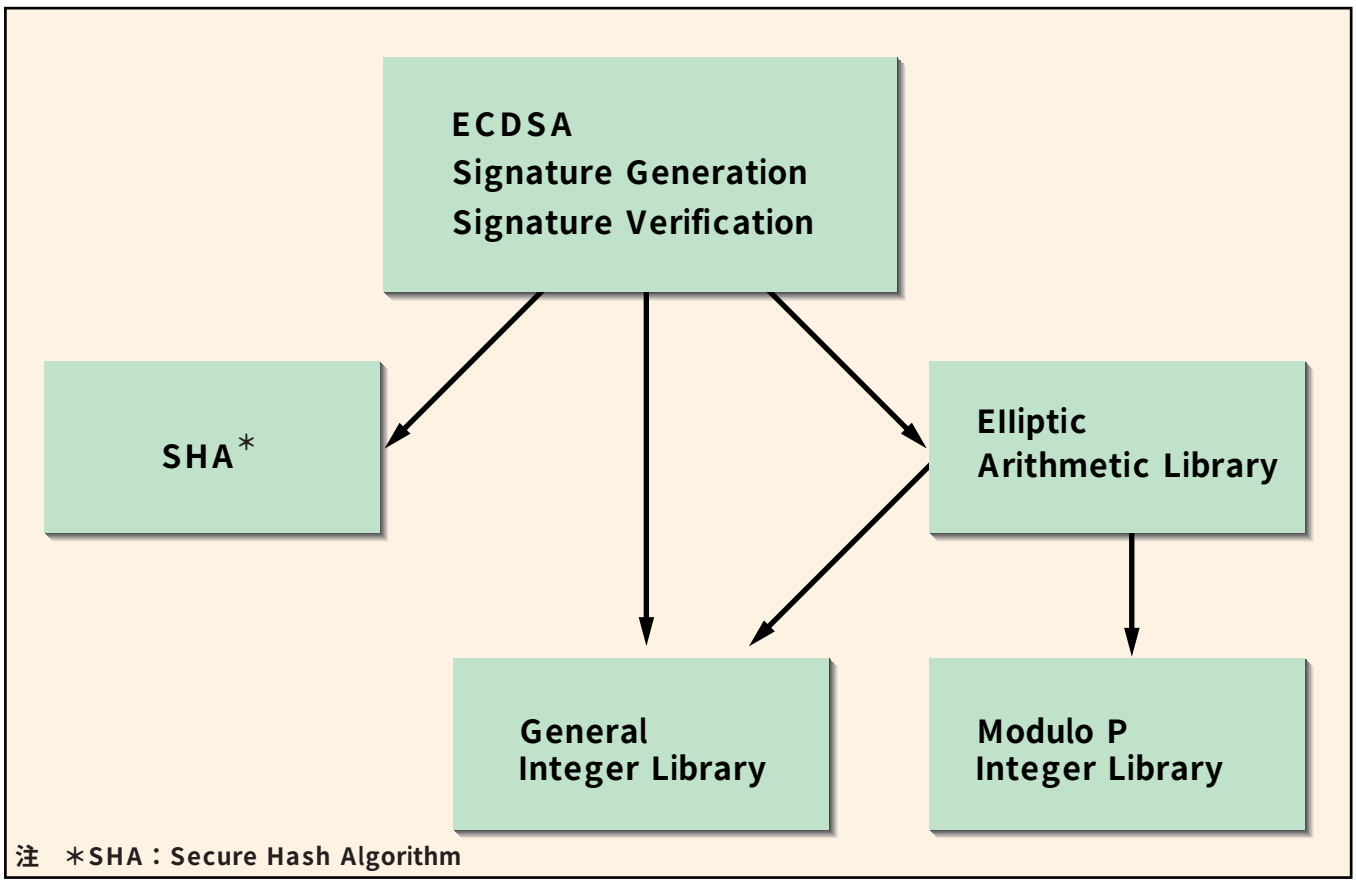
酒井康行*
長谷川俊夫*
中嶋純子**

要　旨

公開かぎ(鍵)暗号系の代表的アルゴリズムであるRSA暗号，だ(楕)円曲線暗号，及び超楕円曲線暗号の安全性と実装に関して考察する。RSA暗号の安全性の根拠は，素因数分解の困難さに置いているが，素因数分解対策を施さない鍵生成アルゴリズムによって生成された鍵は，512ビットの場合，パソコン１台で数十時間で解読される確率が低くないことを示した。また，最近その高速性から注目されている楕円曲線暗号において，標数Pの体上の曲線を用い，電子署名と検証を16ビットMPU上で世界で初めて実装した。ICカードは近年の情報セキュリティシステムにおいて重要な役割を果たしているが，実装に利用できるリソース(ROM／RAM)が少ないことから，プログラムサイズをいかに小さくするか，また速度とのトレードオフをいかにとるかが大きな問題となる。

本稿で述べる16ビットMPU上のソフトウェアは，小さいプログラムサイズで高速に電子署名や署名の検証を行えることから，ICカード上の実装に適したものである。また，楕円曲線暗号の拡張として，超楕円曲線暗号の基礎研究も近年活発である。超楕円曲線のヤコビ多様体上の離散対数問題を安全性の根拠とした，安全かつ実用的な暗号系を構成した。

これまで実用的速度が達成された超楕円曲線暗号はなかったが，本稿の公開鍵暗号は，スカラー倍算をAlpha 21164(250MHz)上のC言語で118msで実行でき，世界初の実用的超楕円曲線暗号である。



楕円曲線暗号ライブラリのソフトウェアアーキテクチャ

標数Pの体上の楕円曲線を用いた楕円曲線暗号ライブラリを作成した。楕円DSA署名，検証，ハッシュ関数の機能を搭載し，プログラムサイズ４Kバイトで高速に署名生成，検証が可能である。また，このライブラリは、RSA暗号にも利用可能である。

*情報技術総合研究所　**LSI事業推進センター