

共通言語基盤上における暗号アルゴリズムの効率的な実装手法

Efficient Implementation Techniques of Cryptographic Algorithms for Common Language Infrastructure

及川 一樹* 児玉 英一郎* 王家宏* 高田 豊雄*
Kazuki Oikawa Eiichiro Kodama Jiahong Wang Toyoo Takata

キー 共通言語基盤, 共通鍵暗号, 公開鍵暗号, 楕円曲線暗号, 多倍長演算

近年, Microsoft が設計し, Ecma International や ISO, JIS などの標準規格でもある共通言語基盤を利用した開発が数多く行われている. この共通言語基盤は, 共通中間言語と呼ばれる中間言語を用いて, 仮想実行システムと呼ばれる仮想マシン上で実行する仕組みを採っている. そのため, 直接機械語にコンパイルする場合と比べるとパフォーマンスの点で劣ってしまうが, 言語に依存しないため, 言語間での相互運用性が高く, 豊富なクラスライブラリや, ガベージコレクションにより開発が容易といった利点を持っている.

一方, 近年のアプリケーション開発において, 情報やプライバシー保護の観点から, データを暗号化する必要性が高まっている. しかし, 高速かつ強度の高い共通鍵暗号アルゴリズムとして知られる Camellia[1] や Rijndael[2] においても, CPU に強く依存するアセンブラによる実装でなければ, ギガビットイーサネットワークなどの広帯域を生かすような, 高速な暗号化処理は望めない.

また, 公開鍵暗号系は計算量の多い多倍長演算を必要とするため, パフォーマンスに難がある共通言語基盤上で動作するプログラムと, 機械語から直接実行されるプログラムとでは, 性能差が大きくなってしまふ.

そのため, IPv6 の普及と共に今後登場するであろう, クライアント同士が相互に認証し, データをやりとりするような P2P アプリケーションや, PDA/スマートフォンのような, 様々なアーキテクチャが存在する携帯端末向けのネットワークを活用したアプリケーションなどでは, 暗号化や認証などの計算コストが無視できない割合を占めることになる.

そこで, 本稿では共通言語基盤上における暗号アルゴリズムの効率的な実装手法を提案する. 評価においては, 共通鍵暗号方式として良く知られた Camellia や Rijndael, 及び, 公開鍵暗号方式である楕円曲線を利用したデジタル署名方式である ECDSA(Elliptic Curve Digital Signature Algorithm)[3] に対し, 提案手法を適用して実装を行い, 性能評価を行った.

評価の結果, 本提案手法を利用して実装した Camellia と Rijndael の暗号化速度は, 本提案手法を利用しない実装と比べ, Camellia においては 40%, Rijndael においては 20% の速度の向上が認められた. 特に Camellia においては, NTT による C 言語の実装よりも 17% 高速という結果が得られた. また, 公開鍵暗号方式である ECDSA において, 本提案手法を利用した実装は, C 言語による実装とほぼ同等の処理時間で, 署名の作成と検証が行われることが分かった.

以上のように, 本提案手法により仮想マシン上で動くプログラムながら, 直接, 環境固有の機械語にコンパイルされる C 言語で記述されたプログラムに近い速度を達成できた.

参考文献

- [1] 市川哲也, 松井充, 中嶋純子, 時田俊雄, 青木和麻呂, 神田雅透, 盛合志帆, “128 ビットブロック暗号 Camellia アルゴリズム仕様書”, <http://info.isl.ntt.co.jp/crypt/camellia/dl/01jspec.pdf>
- [2] Joan Daemen, Vincent Rijmen, “AES submission document on Rijndael, Version 2”, <http://csrc.nist.gov/CryptoToolkit/aes/rijndael/Rijndael-ammended.pdf>
- [3] Certicom Research, Standards for Efficient Cryptography Group, “SEC1: Elliptic Curve Cryptography”, http://www.secg.org/download/aid-385/sec1_final.pdf

* 岩手県立大学, 〒 020-0193 岩手県岩手郡滝沢村滝沢字菓子 152-52, Iwate Prefectural University, 152-52, Sugo, Takizawa, Takizawa village, Iwate 020-0193