RSA チップによる SSL の高速化実験

6F－9

櫛間 英樹 * kushima@cs.titech.ac.jp
新島 秀人 ** nijima@jp.ibm.com
丸山 宏 *** maruyama@jp.ibm.com, maruyama@cs.titech.ac.jp
*東京工業大学情報理工学研究科 **日本アイ・ビー・エム(株)東京基礎研究所

1. はじめに

近年，情報通信ネットワーク上で，WWW サーバを利用した情報共有システムが普及しつつある．このようなネットワークを用いた情報のやりとりは多大な利便性とコストダウンを提供した．その一方で，WWW サーバへの不正なアクセスや情報の漏洩・改ざんなどのセキュリティ問題が表面化している．その対策として，WWW サーバと WWW クライアントとの間の通信について，認証や暗号化などを用いた技術が使用され始めている．その 1つに Netscape Communication 社が提唱している SSL(Secure Socket Layer) プロトコル[1]を使用した HTTPS通信がある．HTTPS通信では，通常の HTTP セッションの前に，ネゴシエーションと呼ばれる，セッション内で使用される暗号仕様や デジタル署名のためのアルゴリズムなどの取り決めを行う．これらの取り決めを元に，相互認証を行った後，HTTP 通信が開始される．このように，単純なデータの送受信のみでなく，ネゴシエーションプロセスとデータの暗号化が必要となるので，それを処理するための時間及び CPU パワーが 余分に必要になる．この SSL プロトコル技術には RSA アルゴリズム[2]が使用されているが，このアルゴリズムには多くの CPU 時間が必要であり，それが通信速度の低下につながっている．通信速度の低下は WWW サーバ，WWW クライアント双方に対して大きな負担となる．

そこで本研究では，WWW サーバ側において必要な RSA 計算を専用のハードウェアアクセラレータ上で処理することで，SSL を 実装した WWW 通信の高速化を図る．

2. ハードウェアアクセラレータ

図 1 は本研究で RSA 計算に使用するハードウェアカードである．このカードは RSA アクセラレータ[3]の評価用として製作されたものである．

この評価用 RSA カードは RICO と呼ばれる RSA アクセラレータチップが搭載されていて，以下のような特性をもつ．

- 1024-bit までの RSA 計算が可能
- 1024-bit RSA 計算が 40MHz 動作で 27msec 以下という高速処理
- 33MHz 動作において電力消費は 100mA 以下

図の左側に位置するチップ (RICO) により RSA 計算が行なわれる．図の右側に位置するチップは ISA のバスコントローラである．

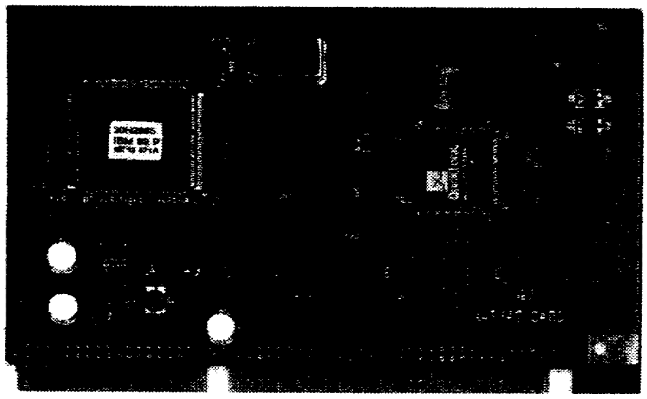

図 1. 評価用 RSA カード

今回のハードウェアはチップの評価用のため，ハードウェア割り込み機能を実装していない．現在開発中の PCI 版のカードにおいてはその点の改善がなされる予定である．

3. システム構成

図 2 に本研究で取り扱う WWW サーバのシステム構成を示す．本研究では WWW サーバとして Apache を使用した．そしてこの WWW サーバに SSL 接続をインプリメントするツールとして SSLeay[4] を使用した．

本研究において，通常 SSLeay 上で行なわれる RSA

Performance improvement of SSL using RSA hardware accelerator, Hideki Kushima, Tokyo Institute of Technology, Hideto Niijima, IBM Research, Tokyo Research Laboratory, and Hiroshi Maruyama, IBM Research, Tokyo Research Laboratory and Tokyo Institute of Technology

計算 (m^d mod N) を，ハードウェアを用いて処理する．ところで，今回の WWW サーバマシンとして用いた Windows NT4.0 では，特権がなければ自由にハードウェアにアクセスすることができない．そこで今回，直接ハードウェアに対してデータを転送するためのデバイスドライバを作成した．RSA 計算が必要な場合，デバイスドライバに m, d, M を渡し，計算終了確認後，結果が SSLeay に渡されるという仕組みになっている．

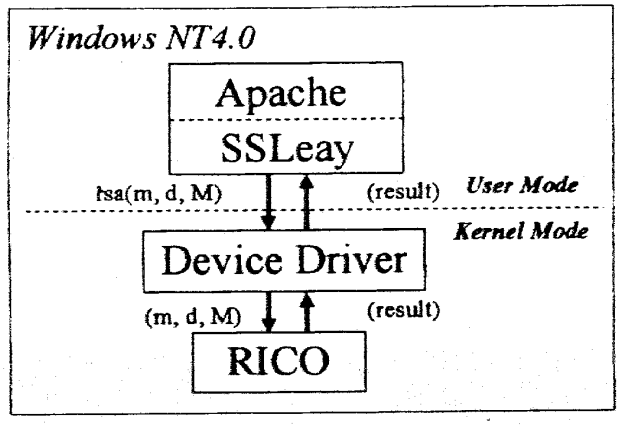

図 2. システム構成

4. 実験

Pentium-200MHz マシン上において SSLeay を使用して，SSL のネゴシエーションにかかるサーバ側の CPU 時間を測定した．使った CipherSuite は RSA 1024-bit + RC4-64-MD5 である．今回，クライアント認証を行わない SSL2での実験を行った．測定はクライアント側からSSL 接続を 500 回繰り返して行った．OS は Windows NT4.0 を使用している．

図 3 に実験の結果を示す．図の中で 純粋な RSAの復号計算を除く部分をSSLネゴシエーションのオーバーヘッドとしてある．ソフトウェア版では中国人の剰余定理(CRT)を使う方法と，使わない方法の 2 種類を示した．

図が示すとおり，SSLのネゴシエーションにおいてかなりの部分を RSA計算が占めていることが分かる．また Pentium-200MHz マシンにおいては，1024-bit の RSA 計算は中国人の剰余定理を使用すればハードウェア版と変わらないぐらい速いことが分かった．

5. 考察

今回の評価用カードは，ハードウェア割り込みを実装していなかった．このため，カーネル内においてポーリングのための無駄な CPU 時間が使われてしまっていた．このため RSA 計算をハードウェア化することの性能上のメリットは小さいということが分かった．現在開発中の PCI 版ではその点が改善される．すなわち，RSA計算をハードウェア上で実行中，CPUが他の処理を行うことができるようになるため，システム全体のスループットの向上が最大約 70% 期待できる．

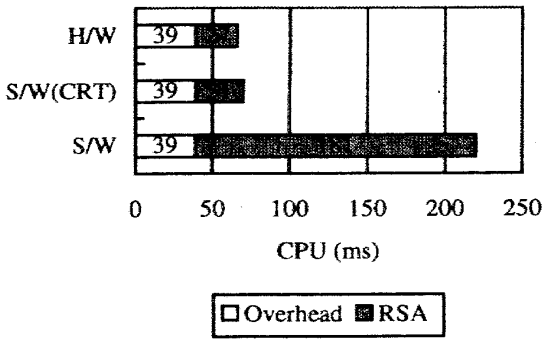

図3. 1回のネゴシエーションにかかる CPU 時間

RSA 計算をハードウェア化するメリットとして，ほかに WWW サーバの秘密鍵管理の問題がある．現在，SSL 接続が可能な Web サイトでは，SSL の接続要求がある度に WWW サーバの秘密鍵を使わなければならない．この秘密鍵が外部からアクセスされる可能性のある環境に存在することは，セキュリティ上大きな問題となり得る．現在開発中の PCI 版においては，一旦キーをカードの中にインプットしてしまえば 外部からのキーを読み出しが不可能になっている．

6. 今後の課題

HTTPS は広く使われるようになってきているが，クライアント認証の有無，ネゴシエーションの頻度，X.509 証明書の構造など，性能評価に与えるパラメータが非常に複雑である．今後は HTTPSのパフォーマンスを正確に計るためのベンチマークの提案と，それを用いた実環境のテストを行っていきたい．

7. 参考文献

[1] http://home.netscape.com/eng/ssl3/ssl-toc.html, Internet Draft.

[2] http://www.rsa.com/rsalabs/pubs/PKCS/, RSA Data Security, Inc.

[3] A. Satoh, Y. Kobayashi, H.Nijima, N.Munetoh, and S.Sone: "A High-Speed Small RSA Encryption LSI with Low Power Dissipation," 1997 Information Security Workshop, pp.99-105, Sept. 1997.

[4] http://www.cryptsoft.com/, CryptoSoft Pty Ltd.