プロセッサ設計におけるセキュリティ向上の研究
(Study of security improvement in a processor design)

川口　聡
東海大学情報理工学部ソフトウェア開発工学科

山田　圀裕
東海大学専門職大学院組込み技術研究科

Satoshi Kawaguchi
TOKAI University School of Information Science and Technology, Department of Embedded Technology

Kunihiro Yamada
TOKAI University Professional Graduate School, Embedded Technology

要約—プロセッサ設計におけるセキュリティの向上を規模の小さいマイクロプロセッサで行っている。今回は、レジスタに重きをおいて研究を行った。レジスタ間のデータ転送に第二データバスを用いることによって、プロセッサやプログラムの機能を向上することが出来る見込みが得られた。

はじめに

近年、プロセッサ設計などのハードウェア開発では、FPGAやCADなどを用いて実際の配置配線をブラックボックス化した大規模な開発となっている[1]。これは、開発の効率化に大きく貢献してきた[2]。しかし、ブラックボックス化によって、応用技術の習得や使用といったことに重点が置かれ、基礎的なものが抜けてきた。そこで、開発の規模を非常に小さくした小マイクロプロセッサを用いることによって基礎を押さえ、大規模開発に応用でき得る技術の研究を行った。

プロセッサの構成

マイクロプロセッサ内部は、内部制御、演算、一時記憶などの機能で構成されている。これらは、一般的に制御線やデータバスで接続されている。すなわち、マイクロプロセッサは一度にひとつの処理を実行しているものとなっている。命令をひとつ実行している最中には、命令に関係していない演算や記憶などに関する機構のうち、すべてがデータの読み出しや書き込みを行っていない状態になる。そこで、今回はデータのやり取りなどを行うレジスタのデータバスを二重化することを行った。

第二データバス

データのやり取りなどを行う汎用レジスタのデータバスを第二データバスと呼ぶ。図1は第二データバスを用いた複数のレジスタ間のデータ転送の例の1つである。この第二データバスでは、4つのレジスタを持っている。Flag Gateは同時に動作し、ある特定のフラグが立っているときに開き、逆にフラグが立っていないときには閉じている。Data Bus 1でレジスタである、Reg AからReg Bへのデータ転送を実行する時、同時にData Bus 2でReg CからReg Dへデータ転送を行うときを考える。

先ず、フラグが立っていないときを考える。フラグが立っていないと、Flag Gateが閉じた状態になっている。これは、Data Bus1はデータのやりとりが出来るが、Data Bus2はデータのやり取りができない。この時に、データの転送はData Bus 1のReg AからReg Bは実行されるが、Data Bus 2ではFlag Gateが閉じており、Reg CからReg Dは実行されず、命令を実行した結果、Reg Aの中身がReg Bに格納され、そのほかのレジスタは前の状態が保持される。

次に、フラグが立っている時を考える。フラグが立っていると、Flag Gateが開いた状態になっている。これは、Data Bus 1もData Bus 2もデータのやりとりが出来ることを示している。この時に、データの転送はData Bus 1のReg AからReg Bの転送は実行され、Flag Gateが開いておりData Bus 2もReg CからReg Dのデータの転送は実行され、命令を実行した結果、Reg Aの中身がReg Bに格納され、また、Reg Cの中身がReg Dに格納される。

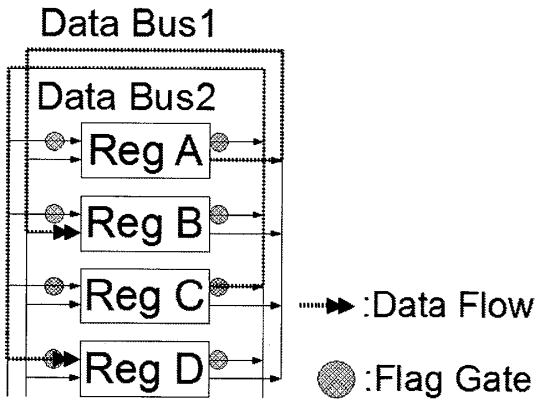

図1第二データバスとデータの流れ

Flag Gateの第二データバスを用いて、前述のデータ転送を行うと、通常のレジスタ間データ転送命令一つと条件付き分岐命令一つ、そして、条件付分岐命令の分岐先にあるレジスタ間データ転送命令一つが同時に実行される。これは、機械語の3つの命令が1つにまとめられていることを示すこととなる。

性能の向上へ

レジスタ間のデータの転送において、第二データバスとFlag Gateを用いると、特定の条件を満たしたときの命令の同時実行が可能となった。このときのFlag Gateは、特定のフラグが条件を満たしたことを示し、このフラグに対して動作を設定している。ここで、これを汎用レジスタの特定のビットを用いて動作させるときを考える。

普段はData Bus 1を用い汎用レジスタ間のデータ転送を行っている。また、Data Bus 2を用いた転送は、すべての汎用レジスタで実行できる。この、Data Bus 2のデータ転送の有無は、フラグの状態に依存し、Data Bus 1の汎用レジスタ間転送命令で隠れている状態となる。この時、フラグを意図しない状態で立てると、正規のレジスタ間転送の裏で、もう一つレジスタ間転送が実行され、レジスタ内のデータを破壊することとなる。これは、プログラム内では、変数の破壊といった現象が発生する。この現象を用いると、プログラム中に回避するための手段を組み込まないとプロセッサ上ではプログラムが正しく動作しないこととなる。これによって、ハードウェアとソフトウェアの間に、硬い関係が発生しプロセッサの不正使用といった面からセキュリティを向上させることができると考えられる。

まとめ

プロセッサ設計におけるセキュリティの向上を規模の小さいマイクロプロセッサで検討している。その中で、レジスタ間のデータ転送に二つのデータバスを用い、一つの命令で三つの命令分の実行を行うことができた。これによって、プログラムの密度の向上などができるようになった。

次の展開への考察として、レジスタ間で用いていた第二データバスをマイクロプロセッサ内のすべてのデータ転送に用いることがある。レジスタ間では、実行可能性の向上を得ることができた。また、低速なメモリやALUのデータ転送もほかの命令と同時に動作させることができる。このことより、マイクロプロセッサの更なる機能の向上を期待することができる。

参考文献

[1] 山田圀裕，坂本直史:“「システム技術と半導体」日本シミュレーション学会＆ゲーミング学会JASAG 2004年度周期全国大会”p.155-p.160

[2] 山田圀裕，坂本直史：“RENESAS SOLUTION SEMINAR 2004” P.255