

電気・電子情報工学専攻		学籍番号	M145204	指導教員氏名	市川 周一 藤枝 直輝
申請者氏名	山内 涼				

論文要旨 (修士)

論文題目	Path ORAM におけるバンド幅削減手法の提案
------	---------------------------

Oblivious RAM (ORAM) はダミーアクセスやデータの再配置によってアクセスパターンを秘匿する技術である。ORAMにはメモリバンド幅に無視できないオーバーヘッドが伴うことが知られており、実用化にあたってはその削減が望まれている。

本研究では、ORAM アルゴリズムの一つである Path ORAMを対象としたバンド幅削減手法を提案する。はじめに評価基盤としてアルゴリズム再現用のシミュレータを作成し、その妥当性を評価した。次に提案手法を適用した場合のバンド幅削減率とストレージコストについて評価し、その有効性について論じた。

Path ORAMでは外部メモリに構成したバイナリツリーでデータブロックを管理する。ツリーにおけるルートからリーフまでの経路は Pathと呼ばれ、ブロックは配置先として 1つの Pathにマッピングされる。アルゴリズムではブロックへのアクセスは Path単位で実行され、かつ読み込みと書き込みをセットで行う。そのため、Pathに存在するブロック数の 2倍に相当するバンド幅オーバーヘッドが生じる。加えて、ツリーから読み込んだブロックを一時的に格納する内部メモリがストレージコストとして必要となる。

Path ORAMのバンド幅オーバーヘッドを削減するため、冗長なメモリアccessの省略を図る。連続したメモリリクエストが近接の Pathに対するものだった場合、書き込んだ直後のブロックを再び読み込む状況がしばしば発生する。本研究ではこのような無駄なメモリアccessを削減する手法として

Reuseと Delayを提案する。また、両手法のバンド幅削減率を向上する方法として Shuffleを提案する。Reuseでは直前に書き込まれたブロックのうち、次の Pathアクセスに含まれるものについては有効フラグをセットすることで再び参照可能にする。Delayでは直前の Pathアクセスにおけるブロックの書き戻しを次の Pathアクセスで実行する。これにより後続の Pathアクセス開始時には直前のアクセスで読み込まれたブロックが内部メモリに存在するため、重複したブロックアクセスを削減できる。Reuse, Delayの各手法においては削減できるメモリアccess数は連続する 2つの Pathが近接しているほど多くなる。Shuffleは Pathの近傍度によって複数の Pathアクセスを並び替えることで更なるバンド幅の削減を図る手法である。

評価基盤として Path ORAMアルゴリズムの振る舞いを再現するシミュレータを作成した。シミュレータの妥当性を検証するにあたり、Path ORAMの提案論文と、Maasらの論文で示された値を評価基準として用いた。シミュレータの出力結果と両論文で示された値を比較した結果、本研究で使用する上で十分信頼に足る性能であることを確認した。

提案手法の評価には DRAMシミュレータである USIMMに付属したメモリトレースを使用した。バンド幅削減率とストレージコストについて、メモリアccessが省略されなかった場合を基準として評価した。シミュレーションの結果、全てのアプリケーションで ShuffleとDelayを組み合わせた手法が最も高いバンド幅削減率を示し、最大で 27.0%、平均で 24.1%となった。同手法において、同じストレージコストにおけるバンド幅削減率は、Maasらの提案したオンチップメモリを追加する手法に比べ平均 10.3%高いことを確認した。