平成 31 年 01 月 08 日

電気・電子情報工学専攻	学籍番号	M153257
申請者氏名	藤田 浩輝	

指導教員氏名	市川 周一 藤枝 直輝

論　文　要　旨（修士）

論文題目	Path ORAM の軽量実装とパスのランダム性に関する検討

Oblivious RAM (以下 ORAM) は，アクセスパターン解析をダミーアクセスやデータの再配置を用いて防ぐ技術である．特に軽量な ORAM プロトコルとして Path ORAM が広く研究されている．Path ORAM の帯域幅オーバーヘッドは大きいことが指摘されており，これを削減するための研究が広く行われている．しかし，削減手法を適用したことによる安全性の低下についての議論は少ない．本研究では，Path ORAM が用いる擬似乱数生成 (PRNG; Pseudo Random Numbers Generator) エンジンに着目し，安全性を定量的に評価することを目的とする．

Path ORAM 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．ブロックへのアクセスは Path 単位で実行され，かつ読み出しと書き戻しをセットで行う．各ブロックと Path の対応関係は，Position Map という領域によって管理され，ブロックはアクセスされるたびに PRNG による新たな Path に配置される．この働きによって，ブロックへのアクセス系列は，ブロックとは無関係のアクセス系列に置き換わり，アクセスパターンが秘匿される．

より軽量な PRNG エンジンでランダム性の高い Path の系列を生成出来れば，安全性を保ちながら Path ORAM アーキテクチャの軽量化が可能となる．本研究では，ブロックアクセスに対する Path の系列が十分なランダム性を持つ事をセキュリティ要件として定める．生成された乱数が低品質だとしても，Path の系列のランダム性が高ければ，Path ORAM のセキュリティを保つことが出来る．

評価のために，簡易的な Positon Map シミュレータを作成した．Positon Map の動作のみを再現し，入力されたアドレスに対応した Path の系列と，生成された乱数を出力する．生成した乱数と Path の系列を乱数テストにかけ，PRNG エンジンごとの Path の系列への影響を調査した．5 種類の PRNG エンジンを対象に，DRAM シミュレータ USIMM に付属するトレースファイルを用いて実験を行った結果，いくつかの PRNG エンジンにおいて，元の乱数系列が低品質であっても Path の系列のランダム性が保たれていることを確認した．また，より実際の Path ORAM に近い環境である ORAM シミュレータを用いて，帯域幅オーバーヘッド削減手法を適用した Path ORAM を想定し同様の実験を行った．これらは Path ORAM のツリーに対するキャッシュであり，キャッシュにヒットした場合ツリーへのアクセスは省略される．この場合にも，テストへの合格数の変化は誤差の範囲にとどまった．

最後に，ORAM コントローラのプロトタイプをハードウェア実装し，PRNG エンジンのうち軽量なもの 3 種類について，その選択がハードウェア使用量に与える影響を調査した．その結果，LUT，Flipflop 数の変化は最大でそれぞれ 193 個，130 個にとどまり，コントローラ全体に与える影響は軽微だった．これらの結果を踏まえて，安全性を満たしながら，より軽量な ORAM アーキテクチャを構築することが今後の課題である．