【 2 】

氏　　名	ｸﾞｪﾝ ﾀﾞｯﾄ ﾄｳｵﾝ
学位の種類	博　士（工学）
学位記番号	第６４１号
認定課程名	防衛大学校理工学研究科後期課程
学位授与年月日	令和２年５月２２日
論文題目	GPU を用いたハッシュ関数 Keccak の高速化に関する研究
審査担当専門委員	（主査）慶応義塾大学　教授　天野　英晴
	工学院大学　教授　浅野　太
	慶応義塾大学　教授　斎藤　英雄

審査の結果の要旨

情報化社会の発展に伴い、情報保護の必要性が高まり、ハッシュ関数を用いた暗号化を行う機会が増えている。ハッシュ関数 SHA-3 は、現在利用されている SHA-2 に代わって今後広く用いられる可能性が高く、Keccak は、その元となったハッシュ関数である。ハッシュ関数は、出力として与えられたハッシュ値を生成するメッセージを見つけることは計算量的に困難である点を利用して情報秘匿を実現する。この安全性を高めるためには、攻撃に利用可能な高速化実装技術を研究することで、その攻撃の可能性を定量的に評価し、防御技術を高める必要がある。

著者は、科学技術計算に広く利用され、その性能向上が著しい GPU（Graphics Processing Unit）を用いて 512 ビット長を出力する Keccak-512 の高速化実装を行った。次に、これを応用して、現在、最も進んだ攻撃手法の一つであるレインボーテーブル攻撃を高速化し、Keccak 関数に対する脅威の程度を調べた。

ハッシュ関数の高速化は、(1) ルックアップテーブルの再構成　(2) 定数テーブルのメモリ配置の最適化　(3) ブロック、スレッド数の最適化　(4) CUDA ストリームとのオーバーラップの 4 つの方法を組み合わせて、NVIDIA 社 P100 アーキテクチャを用いた GeForce GTX1080 GPU を用いて、既存手法をはるかに上回る 65.582GB/s を達成した。レインボーテーブルの高速化は、1 つのチェーンを GPU の 1 スレッドに割り当てると共に、還元関数にパスワード候補のチェーン内の一情報を追加して、重複を避ける工夫を行った。さらに提案したハッシュ関数の高速化手法を適用した。この結果、CPU のみでレインボーテーブルを生成する場合に比べて約 239 倍の高速化を達成した。

このように著者は、最近重要性が高まっているハッシュ関数の暗号化の脅威となり得る手法を明確化し、安全性を高めるための新たな知見を示したものである。よって、学術的価値は高く、博士（工学）として合格と判定した。