氏　　名	Camille Vuillaume
学　位　名	博士（システム情報科学）
学位記番号	第３号
学位授与年月日	平成１９年９月２８日
学位論文題目	Low-cost high-speed public key cryptosystems
論文審査委員	主査　高木　剛
	副査　高橋　修
	副査　三木　信弘
	副査　三浦　守
	副査　顔　嵩銘（台湾国立中央大学）

論　文　要　旨

審査結果の要旨

提出論文はユビキタスディバイスにおける楕円曲線暗号の高速実装技術に関するもので，ディバイスに対する消費電力攻撃（サイドチャンネル攻撃）に対して，Koblitz曲線を用いた安全な高速アルゴリズムを提案している．

上記の研究テーマにおいて，電子情報通信学会英文論文誌2編，Springer LNCSレベルの国際会議論文4件に採録されている．これらに加え，ジャーナル論文2編が査読中であり，この他にも国内での学会研究会およびシンポジウムなどで7件の講演発表を行っている．

これらは，システム情報科学分野の学位論文として十分な学術的成果を有していると認められ，「合」と判定する．