GPU Parallelization of Cryptographic Primitives using Multivariate Quadratic Polynomials and its Security Evaluation

田中, 哲士

https://doi.org/10.15017/1500750

（別紙様式 5-2）

氏　　名	田中　哲士
論　文　名	GPU Parallelization of Cryptographic Primitives using Multivariate Quadratic Polynomials and its Security Evaluation （多変数二次多項式を用いた暗号プリミティブと その安全性評価の GPU 並列化）
論文調査委員	主査　九州大学　教　授　櫻井　幸一 副査　　〃　　〃　　岡田　義広 〃　　〃　　〃　　高木　剛

論　文　審　査　の　結　果　の　要　旨

本研究は、多変数二次多項式暗号の実用化に関する課題すなわち高速化と安全性評価についての課題の解決のために、GPU による並列処理を論じたものであり、情報工学上寄与するところが大きい。よって本論文は、博士（工学）の学位論文に値すると認める。