卒論チェックシート

学籍番号 7535079X 氏名 柚木孝文

目的

卒論本文に関して，以下の項目１）～５）に関する記述が必要です．５項目についての記述も卒論評価の１部とします．この卒論チェックシートを完成させ，卒論提出前に記入漏れがないことを確認してください．なお，このシートは卒論審査資料の一つとなります．卒論と同様にしっかり完成させ，卒論と一緒に主査と副査へ提出してください．

提出方法

1. チェック項目について明確・簡潔に回答を記入する．また，対応記述を含む本文のページ番号を明記する（例：3ページ，3,5,7ページ，3-10ページなど）．全ての項目について回答し，卒論チェックシートを完成させる．
2. 完成した卒論チェックシートを，卒論を収めたファイルの最後尾に綴じる．
3. 主査（１名）と副査（２名）に卒論と卒論チェックシートを綴じたファイルを提出する（従って，卒論とともに卒論チェックシートも３部用意する，卒論チェックシートの記述内容は3部とも同一で良い）．

1) 研究の目的・目標を明確に設定できる．（卒論評価項目１）

[チェック項目] 研究目的・目標を説明してください．

近年、IoTの普及に伴い、IoTセキュリティの需要が高まっている。SAS-L2はセンサ等のIoT機器に搭載する認証プロトコルとして開発されたワンタイムパスワード認証方式であり、被認証者側の計算負荷が削減されていることが特徴である。

本研究の目的は、SAS-L2を組込みデバイス上で実装し、SAS-L2に有意性があるかを検証すること、そして、実装上のSAS-L2の問題点を明らかにすることである。そのために本研究の目標を、SAS-L2によって鍵配送を行う暗号通信プログラムの実装およびその評価とする。

本文におけるページ番号：1,2ページ

2) 人類や社会に望まれ、貢献する研究目標を立てられる．（卒論評価項目２）

[チェック項目] 論文に示された研究目標が，情報工学を応用し人類・社会に貢献するものであることを説明してください．（社会との関わりなど）

SAS-L2は、センサ等の処理能力の低いIoT機器とそれらの機器を集約する装置の間で、ほぼ処理負荷なしに暗号通信の鍵配送実現できることが期待されている。本研究では、SAS-L2に関して、実装上の評価を行うことによって、IoTシステムにおける暗号通信の鍵配送を実用化するための足掛かりとなる。

本文におけるページ番号:1,2ページ

（裏にもあります）

3) **研究の目的・目標を実現するための具体的研究方法を示し、実行できる．（卒論評価項目３）**

[チェック項目] 論文に示された研究方法の具体性や，研究目的・研究目標の達成を目指すためにどのような意味がありそのような研究方法を採用したのか説明してください.

SAS-L2と比較する従来のSAS認証方式として、本研究ではSAS-2を用いた。SAS-L2によって、認証機器の処理負荷が削減できることを確認する必要があるため、評価項目をCPU時間とリソース使用量(CPU使用率、メモリ使用量)とし、実装したプログラムをJetson nanoに搭載して評価項目の測定を行った。

本文におけるページ番号：2,29-31ページ

4) **研究の内容が，情報工学技術の発展や応用に貢献するものである．（卒論評価項目４）**

[チェック項目] 論文で示された研究内容が，情報工学技術の発達や応用に貢献するものであることを説明してください．（研究内容の新規性など）

SAS-L2は、現段階では理論上の評価に限られるため、SAS-L2を組込みデバイス上で動作させ、評価実験を行うことに新規性がある。実験を通してIoT機器にSAS-L2を搭載する意義が示されれば、IoTセキュリティ技術の応用に貢献するものとなる。

本文におけるページ番号：2ページ

5) **卒業論文，卒業論文発表において，卒業研究の目的・目標，研究方法，研究成果が論理的に述べられる．（卒論評価項目６）**

[チェック項目] 論文で示された研究成果について説明してください.

本研究では、SAS-2、SAS-L2を組込みデバイス上で動作させて評価実験を行った。実験を通して、SAS-L2ではメモリの使用量と演算処理のCPU負荷が削減されていることがわかった。従来のSAS認証方式と比較し、運用時に求められる機器のスペックが抑えられるため、IoT機器のような限られたリソースの中にSAS-L2認証方式を搭載する意義が示された。

本文におけるページ番号：33-35ページ

[チェック項目] 卒業研究の目的・目標，研究方法，研究成果がどのような章立てで述べられているか説明してください.

第1章で研究目的・目標を述べ、第2章、第3章で実装したプログラムの構成要素となる技術の原理を述べる。第4章で実装したプログラムの構成を述べ、第5章で評価実験の方法及び結果、考察を述べ、第6章で研究成果のまとめを行う。

以上