

LaTeX 레퍼런스 추가

한성대학교 서화정

LaTeX 레퍼런스 추가 설정

Menu

ICISC_AES

Review

Share

Submit

History

Chat

Source

Rich Text

Recompile

References

icisc.bib

aliascnt.sty

eijkel2.eps

history.txt

llncs.cls

llncs.tex

llncsdoc.pdf

llncsdoc.sty

llncsdoc.tex

llncsind.tex

readme.txt

remreset.sty

splncs03.bst

sprmindx.sty

subjidx.tex

typeinst.bbl

typeinst.tex

processor, however, optimizes the encryption time similar to that of lightweight cipher can be used as a lightweight cryptosystem that has more generality and security than conventional lightweight cryptosystem. In this paper, we propose the software optimization method which reduces the clock cycle of AES-CTR algorithm 128 / 256 bit to 2042 / 3010cc, which is faster than the previous implementations. In addition, we have added masking operation in order to protect the optimized AES against side channel attacks.

82

83 `\keywords{AES, Software Implementation, Lightweight Cryptography, Side Channel Attack}`

84 `\end{abstract}`

85

86

87 `\section{Introduction}`

88

89

90

91

92

93

94

95

96 `\bibliographystyle{abbrv}`

97 `\bibliography{References/icisc}`

98

99

100

101

102

103 `\end{document}`

104

sors. However, optimized AES with encryption time similar to that of lightweight cipher can be used as a lightweight cryptosystem that has more generality and security than conventional lightweight cryptosystem. In this paper, we propose the software optimization method which reduces the clock cycle of AES-CTR algorithm 128 / 256 bit to 2042 / 3010cc, which is faster than the previous implementations. In addition, we have added masking operation in order to protect the optimized AES against side channel attacks.

Keywords: AES, Software Implementation, Lightweight Cryptography, Side Channel Attack

1 Introduction

- 1) typeinst.bbl 파일을 추가한다.
해당 파일은 본문 tex파일과 이름을 동일하게 하고 확장자만 bbl로 해주면 된다.
- 2) 서브 디렉토리로 References를 추가한다.
그리고 레퍼런스 정보가 들어갈 파일을 추가한다. 예시에서는 icisc.bib로 작성하였다.
- 3) 마지막으로 tex 본문에 bib 파일 경로를 설정해준다. 예시는 아래와 같다.
`\bibliographystyle{abbrv}`
`\bibliography{References/icisc}`

CryptoCraft LAB

2

LaTeX 레퍼런스 추가

명시된 순서대로 논문을 검색 후 최종적으로
논문에 대한 정보를 확보하게 된다.

Google 학술검색

Announcing the advanced encryption standard (AES)

☒ 모든 언어 ☐ 한국어 웹

```
@article{standard2001announcing,  
  title={Announcing the advanced encryption standard (AES)},  
  author={Standard, NIST-FIPS},  
  journal={Federal Information Processing Standards Publication},  
  volume={197},  
  number={1-51},  
  pages={3--3},  
  year={2001}  
}
```

Google 학술검색 Announcing the advanced encryption standard (AES)

학술자료

모든 날짜
2019 년부터
2018 년부터
2015 년부터
기간 설정...

관련도별 정렬
날짜별 정렬

모든 언어
한국어 웹

☒ 특허 포함
☒ 서지정보 포함

[인용] Announcing the advanced encryption standard (AES)
NF Standard - Federal Information Processing Standards Publication, 2001
☆ 99 122회 인용 관련 학술자료

[인용] Announcing the advanced encryption standard (aes)
J Daemen, V Rijmen - Federal Information Processing Standards Publication, 2001
☆ 99 31회 인용 관련 학술자료

이 검색어에 대한 최상의 검색결과 표시 모든 검색결과 표시

인용

MLA Standard, NIST-FIPS. "Announcing the advanced encryption standard (AES)." *Federal Information Processing Standards Publication* 197.1-51 (2001): 3-3.

APA Standard, N. F. (2001). Announcing the advanced encryption standard (AES). *Federal Information Processing Standards Publication*, 197(1-51), 3-3.

ISO 690 STANDARD, NIST-FIPS. Announcing the advanced encryption standard (AES). *Federal Information Processing Standards Publication*, 2001, 197.1-51: 3.3.

BibTeX EndNote RefMan RefWorks

LaTeX 레퍼런스 추가

- 해당 정보를 긁어서 bib 파일에 추가한다.
- AES와 같은 대문자로 나타나야 하는 문구에는 중괄호 "{" , "}" 를 이용하여 묶어 주어야 대문자로 표기된다.

The screenshot displays the CryptoCraft LAB LaTeX editor interface. The top navigation bar includes 'Menu', 'ICISC_AES', 'Review', 'Share', 'Submit', 'History', and 'Chat'. The left sidebar shows a file explorer with 'References' and 'icisc.bib' selected. The main editor area is split into 'Source' and 'Rich Text' views. The 'Source' view shows a BibTeX entry for 'standard2001announcing' with fields for title, author, journal, volume, number, pages, and year. The title field contains the text 'Announcing the advanced encryption standard ({AES})', where the '({AES})' part is circled in red. The 'Rich Text' view on the right shows the rendered output of the document, including a paragraph of text and a 'Keywords' section listing 'AES, Software Implementation, Lightweight Cryptography, Side Channel Attack'. The bottom of the interface features a 'Recompile' button and a list of files in the project directory.

```
1 @article{standard2001announcing,  
2   title={Announcing the advanced encryption standard ({AES})},  
3   author={Standard, NIST-FIPS},  
4   journal={Federal Information Processing Standards Publication},  
5   volume={197},  
6   number={1-51},  
7   pages={3--3},  
8   year={2001}  
9 }
```

Keywords: AES, Software Implementation, Lightweight Cryptography, Side Channel Attack

1 Introduction

In the hyper-connected era, the utilization of the Internet of Things(IoT) have been increasing more than ever. At the same time, the publics interest in the security of the IoT is growing. Information transmitted between IoT devices may contain private information such as personal information and authentication information, therefore the communication between the devices must be performed in a secure state. Various kinds of encryption algorithms exist for such secure communication. The most widely used algorithm is a symmetric key encryption algorithm, of which AES[1] block cipher is the most representative.

References

LaTeX 레퍼런스 추가

- `\cite` 명령어로 해당 레퍼런스의 이름을 적어준다.

```
\section{Introduction}
```

In the hyper-connected era, the utilization of the Internet of Things(IoT) have been increasing more than ever. At the same time, the public's interest in the security of the IoT is growing.

Information transmitted between IoT devices may contain private information such as personal information and authentication information, therefore the communication between the devices must be performed in a secure state.

Various kinds of encryption algorithms exist for such secure communication. The most widely used algorithm is a symmetric key encryption algorithm, of which AES `\cite{standard2001announcing}` block cipher is the most representative.

LaTeX 레퍼런스 추가

- 컴파일을 수행 하면 해당 레퍼런스가 추가된다.

1 Introduction

In the hyper-connected era, the utilization of the Internet of Things(IoT) have been increasing more than ever. At the same time, the public's interest in the security of the IoT is growing. Information transmitted between IoT devices may contain private information such as personal information and authentication information, therefore the communication between the devices must be performed in a secure state. Various kinds of encryption algorithms exist for such secure communication. The most widely used algorithm is a symmetric key encryption algorithm, of which AES [1] block cipher is the most representative.

References

1. N.-F. Standard. Announcing the advanced encryption standard (AES). *Federal Information Processing Standards Publication*, 197(1-51):3-3, 2001.