부채널 분석 요약

2022 년 5 월 13 일

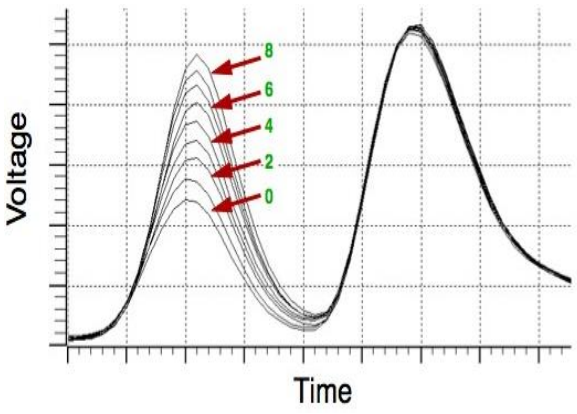
진성현

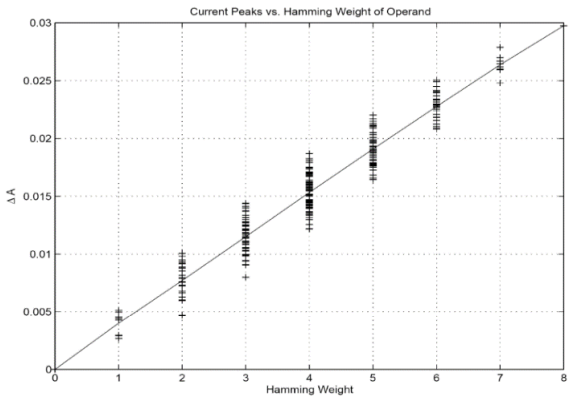
Side-Channel Analysis 요약

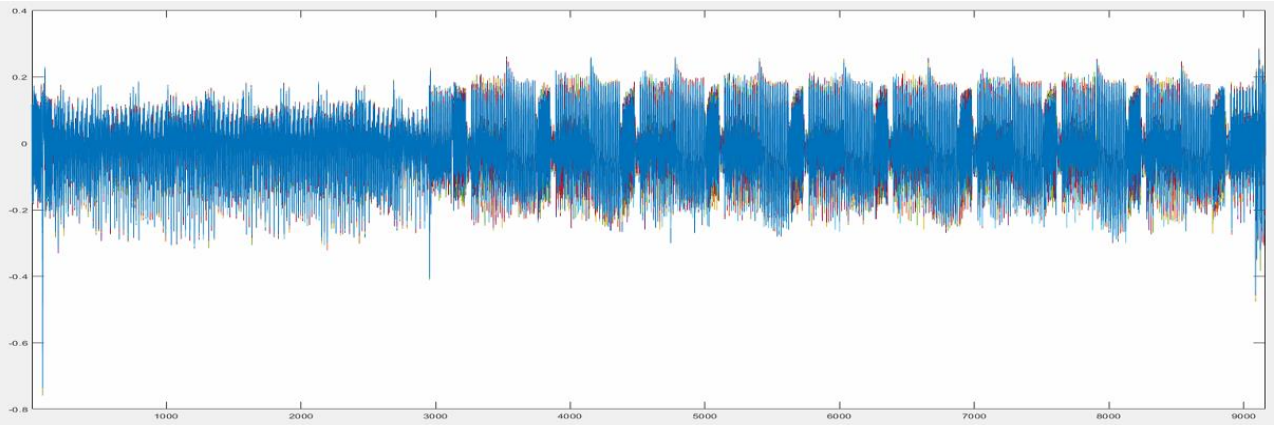
- 부채널분석은 구현물로부터 얻어낸 정보를 이용하여 특정 시스템을 공격하는 기법
- 반도체 회로의 동작 원리상 처리되는 데이터에 따른 전력 소모 발생

$$P = a \cdot f(D) + const + n \quad where \;\; n \in N(0, \sigma^2)$$

- 수직/수평 정보를 이용하여 암호분석 가능
- 대게, 장비들의 전력모델 f 는 해밍웨이트(HW) 또는 해밍디스턴스(HD) 모델을 따름이 알려짐







Differential Power Analysis (DPA) 요약

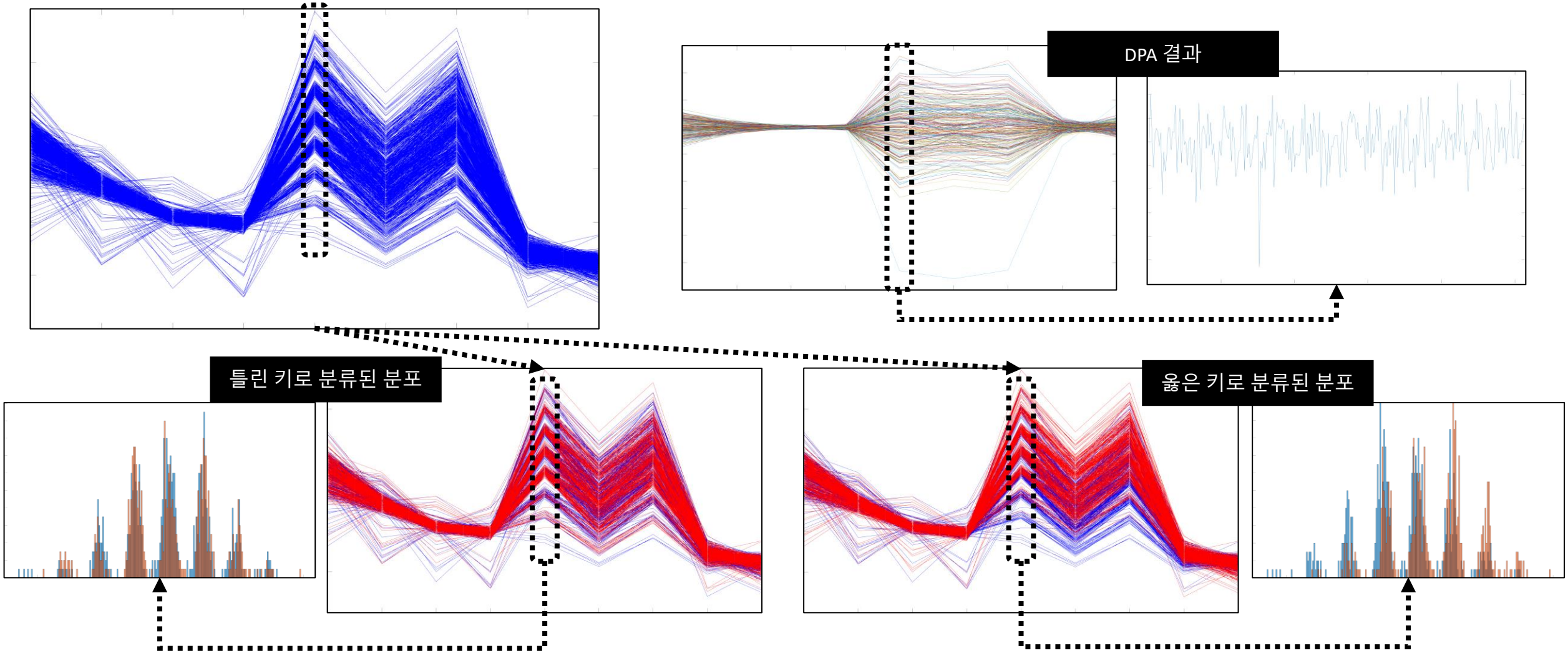
- 암호시스템의 중간값 중 극히 일부를 계산하기 위해서는 일부의 알려진 데이터와 비밀 데이터가 필요함
  - Example: AES 1라운드 첫번째 Subbytes 출력에 대한 부채널분석
    - 해당 출력을 계산하기 위해서는 평문과 마스터키 첫번째 바이트가 필요
    - 전력과 중간값은 아래와 같이 연관되어 있고 평문을 알고 있음

$$P \sim HW\left(S(P_1 \oplus K_1)\right)$$

- 비밀값 추측 통해 중간값 계산, 그 결과로 분포를 2개로 나누어 차이가 생기는지 확인
  - 옳은 추측을 할 경우에 올바르게 그룹화 되기 때문에 유의미한 2개의 분포가 생겨 차이가 커짐
  - 틀린 추측시 랜덤하게 그룹핑이 되기 때문에 분포 차이가 없어짐

Differential Power Analysis (DPA) 요약

- Example: AES 1라운드 첫번째 Subbytes 출력에 대한 부채널분석



Differential Power Analysis (DPA) 요약

- 구현 방법
  - For $gk \in |\mathcal{K}|$
    - For $t \in \{t_1, \dots, t_N\}$
      - 알려진 데이터와 추측한 키 값을 기반으로 타겟 중간값 $v = f_{alg}(d, gk)$ 계산
      - Assign t into set $\mathrm{T}_{LSB(v)\in\{0,1\}}$
    - $DPA\_Result[gk] = mean(T_0) - mean(T_1)$

KOREA UNIVERSITY

INSTITUTE OF CYBER SECURITY & PRIVACY

Korea University CIST Center for Information Security Technologies

Cryptographic Algorithm Laboratory

Q&A

Thanks

[mail] **sunghyunjin@korea.ac.kr** [web] **sunghyunjin.com** [twitter] **@mcsmonk_shj**

부채널 분석

DPA 실습 환경 구축

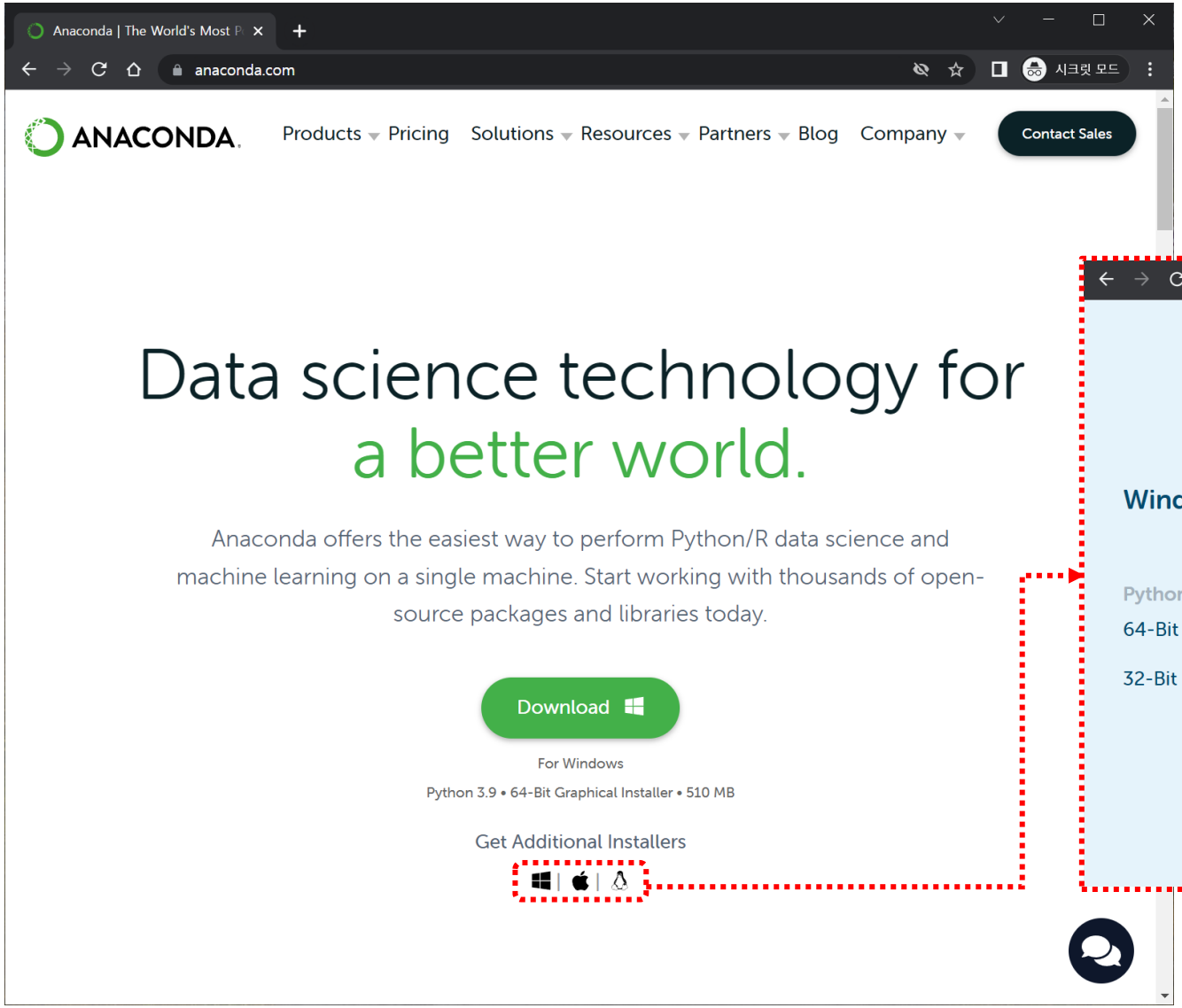
2022 년 5 월 6 일

진성현

Anaconda

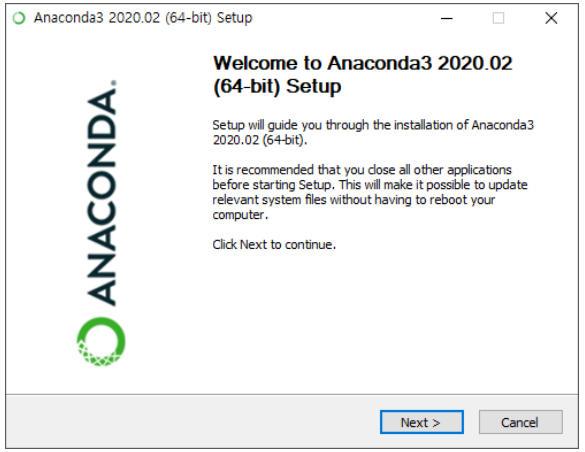
- Python/R 오픈소스 배포판
  - 데이터 과학 등의 과학 계산을 위한
  - 프로그래밍 환경, 패키지 관리 및 배포를 용이하게 하는
- https://www.anaconda.com/

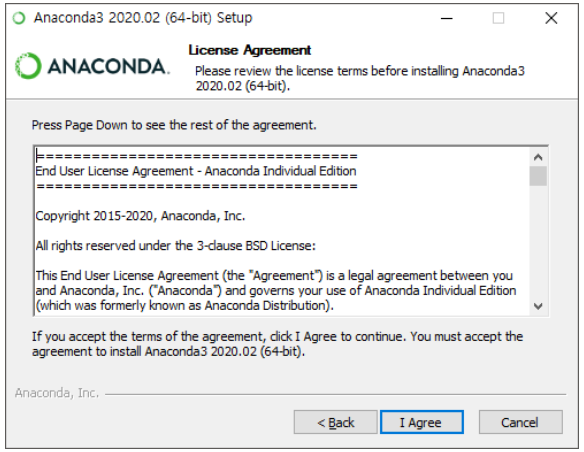
Anaconda 설치

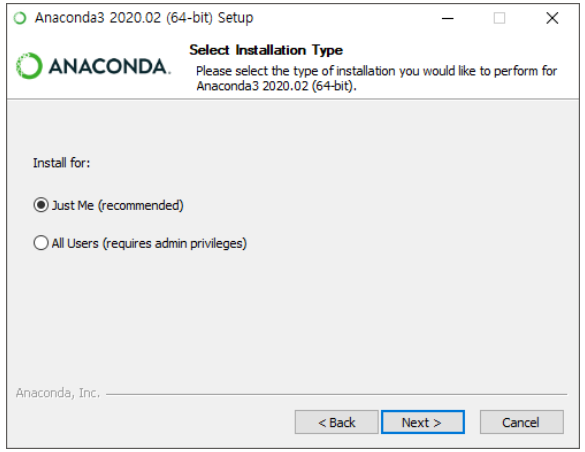

Anaconda | The World's Most P
anaconda.com
시크릿 모드
ANACONDA.
Products
Pricing
Solutions
Resources
Partners
Blog
Company
Contact Sales
Data science technology for
a better world.
Anaconda offers the easiest way to perform Python/R data science and machine learning on a single machine. Start working with thousands of open-source packages and libraries today.
Download
For Windows
Python 3.9 • 64-Bit Graphical Installer • 510 MB
Get Additional Installers

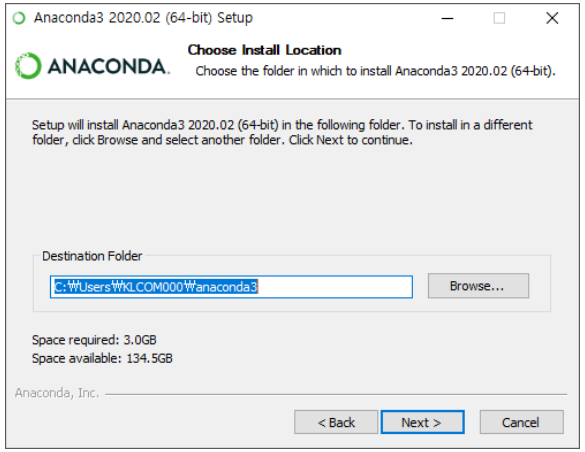

anaconda.com/products/distribution
시크릿 모드(창 2개)
Anaconda Installers
Windows
Python 3.9
64-Bit Graphical Installer (510 MB)
32-Bit Graphical Installer (404 MB)
MacOS
Python 3.9
64-Bit Graphical Installer (515 MB)
64-Bit Command Line Installer (508 MB)
Linux
Python 3.9
64-Bit (x86) Installer (581 MB)
64-Bit (Power8 and Power9) Installer (255 MB)
64-Bit (AWS Graviton2 / ARM64) Installer (488 MB)
64-bit (Linux on IBM Z & LinuxONE) Installer (242 MB)

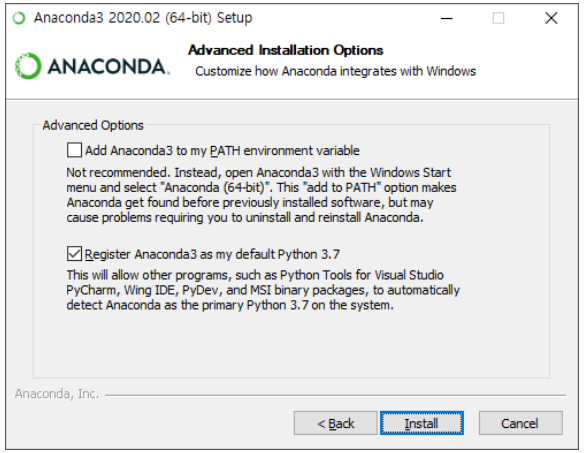
Anaconda 설치

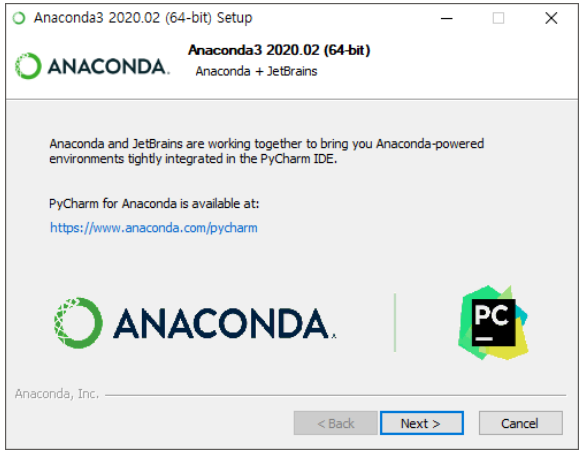

Anaconda3 2020.02 (64-bit) Setup
ANACONDA.
Welcome to Anaconda3 2020.02 (64-bit) Setup
Setup will guide you through the installation of Anaconda3 2020.02 (64-bit).
It is recommended that you close all other applications before starting Setup. This will make it possible to update relevant system files without having to reboot your computer.
Click Next to continue.
Next >
Cancel

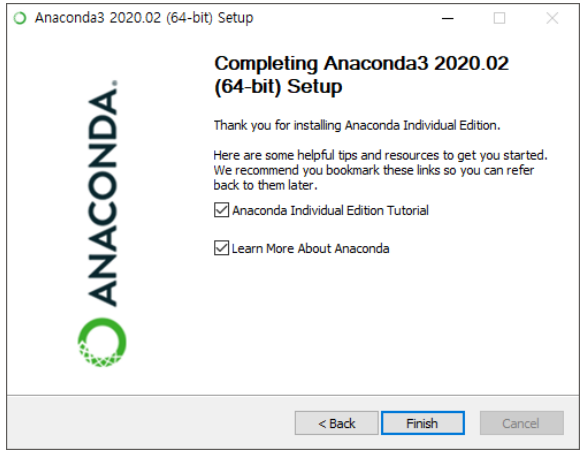

Anaconda3 2020.02 (64-bit) Setup
ANACONDA.
License Agreement
Please review the license terms before installing Anaconda3 2020.02 (64-bit).
Press Page Down to see the rotest of the agreement.
End User License Agreement - Anaconda Individual Edition
Copyright 2015-2020, Anaconda, Inc.
All rights reserved under the 3-clause BSD License:
This End User License Agreement (the "Agreement") is a legal agreement between you and Anaconda, Inc. ("Anaconda") and governs your use of Anaconda Individual Edition (which was formerly known as Anaconda Distribution).
If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install Anaconda3 2020.02 (64-bit).
Anaconda, Inc.
< Back
I Agree
Cancel


Anaconda3 2020.02 (64-bit) Setup
ANACONDA.
Select Installation Type
Please select the type of installation you would like to perform for Anaconda3 2020.02 (64-bit).
Install for:
Just Me (recommended)
All Users (requires admin privileges)
Anaconda, Inc.
< Back
Next >
Cancel


Anaconda3 2020.02 (64-bit) Setup
ANACONDA.
Choose Install Location
Choose the folder in which to install Anaconda3 2020.02 (64-bit).
Setup will install Anaconda3 2020.02 (64-bit) in the following folder. To install in a different folder, click Browse and select another folder. Click Next to continue.
Destination Folder
C:₩Users₩KLCOM000₩anaconda3
Browse...
Space required: 3.0GB
Space available: 134.5GB
Anaconda, Inc.
< Back
Next >
Cancel


Anaconda3 2020.02 (64-bit) Setup
ANACONDA.
Advanced Installation Options
Customize how Anaconda integrates with Windows
Advanced Options
Add Anaconda3 to my PATH environment variable
Not recommended. Instead, open Anaconda3 with the Windows Start menu and select "Anaconda (64-bit)". This "add to PATH" option makes Anaconda get found before previously installed software, but may cause problems requiring you to uninstall and reinstall Anaconda.
Register Anaconda3 as my default Python 3.7
This will allow other programs, such as Python Tools for Visual Studio PyCharm, Wing IDE, PyDev, and MSI binary packages, to automatically detect Anaconda as the primary Python 3.7 on the system.
Anaconda, Inc.
< Back
Install
Cancel

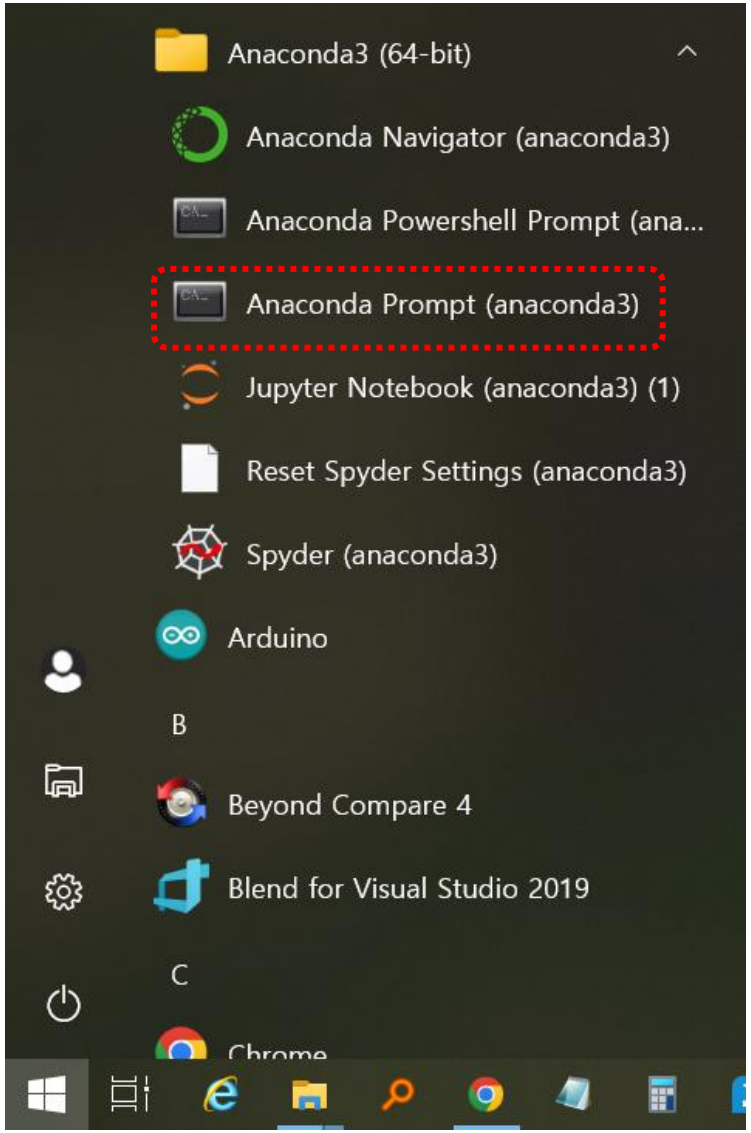

Anaconda3 2020.02 (64-bit) Setup
ANACONDA.
Anaconda3 2020.02 (64-bit)
Anaconda + JetBrains
Anaconda and JetBrains are working together to bring you Anaconda-powered environments tightly integrated in the PyCharm IDE.
PyCharm for Anaconda is available at:
https://www.anaconda.com/pycharm
ANACONDA.
PC
Anaconda, Inc.
< Back
Next >
Cancel


Anaconda3 2020.02 (64-bit) Setup
ANACONDA.
Completing Anaconda3 2020.02 (64-bit) Setup
Thank you for installing Anaconda Individual Edition.
Here are some helpful tips and resources to get you started. We recommend you bookmark these links so you can refer back to them later.
Anaconda Individual Edition Tutorial
Learn More About Anaconda
< Back
Finish
Cancel

Anaconda 설치

- 용량 부족시 miniconda 로 대체 설치 가능
  - Miniconda : Anaconda 최소 설치
    - https://docs.conda.io/en/latest/miniconda.html

Anaconda 실행 및 환경 구축



Anaconda Prompt (anaconda3)

```
(base) C:₩Users₩jin>_
```

Anaconda Prompt (anaconda3) - conda create -n dpa python=3.8 pip

```
(base) C:₩Users₩jin>conda create -n dpa python=3.8 pip
Collecting package metadata (current_repodata.json): done
Solving environment: done

## Package Plan ##

  environment location: C:₩Users₩jin₩anaconda3₩envs₩dpa

  added / updated specs:
    - pip
    - python=3.8


The following NEW packages will be INSTALLED:

  bzip2              conda-forge/win-64::bzip2-1.0.8-h8ffe710_4
  ca-certificates    conda-forge/win-64::ca-certificates-2021.10.8-h5b45459_0
  libffi             conda-forge/win-64::libffi-3.4.2-h8ffe710_5
  libzlib            conda-forge/win-64::libzlib-1.2.11-h8ffe710_1014
  openssl            conda-forge/win-64::openssl-3.0.2-h8ffe710_1
  pip                conda-forge/noarch::pip-22.0.4-pyhd8ed1ab_0
  python             conda-forge/win-64::python-3.8.13-hcf16a7b_0_cpython
  python_abi         conda-forge/win-64::python_abi-3.8-2_cp38
  setuptools         conda-forge/win-64::setuptools-62.1.0-py38haa244fe_0
  sqlite             conda-forge/win-64::sqlite-3.38.3-h8ffe710_0
  tk                 conda-forge/win-64::tk-8.6.12-h8ffe710_0
  ucrt               conda-forge/win-64::ucrt-10.0.20348.0-h57928b3_0
  vc                 conda-forge/win-64::vc-14.2-hb210afc_6
  vs2015_runtime     conda-forge/win-64::vs2015_runtime-14.29.30037-h902a5da_6
  wheel              conda-forge/noarch::wheel-0.37.1-pyhd8ed1ab_0
  xz                 conda-forge/win-64::xz-5.2.5-h62dcd97_1


Proceed ([y]/n)? _
```

설치할 패키지

환경 이름

Anaconda 실행 및 환경 구축

Anaconda Prompt (anaconda3)

```
done
#
# To activate this environment, use
#
#     $ conda activate dpa
#
# To deactivate an active environment, use
#
#     $ conda deactivate


(base) C:₩Users₩jin>conda env list
# conda environments:
#
base                  *  C:₩Users₩jin₩anaconda3
cw                       C:₩Users₩jin₩anaconda3₩envs₩cw
dpa                      C:₩Users₩jin₩anaconda3₩envs₩dpa
etc                      C:₩Users₩jin₩anaconda3₩envs₩etc
gnuradio                 C:₩Users₩jin₩anaconda3₩envs₩gnuradio
julia                    C:₩Users₩jin₩anaconda3₩envs₩julia


(base) C:₩Users₩jin>conda activate dpa

(dpa) C:₩Users₩jin>_
```

(base) C:\Users\jin>PATH
PATH=C:\Users\jin\anaconda3;…

(dpa) C:\Users\jin>PATH
PATH=C:\Users\jin\anaconda3\envs\dpa;…

Anaconda 실행 및 환경 구축

Anaconda Prompt (anaconda3) - conda deactivate - pip install numpy scipy tqdm h5py matplotlib bokeh jupyter

```
(dpa) C:₩Users₩jin>pip install numpy scipy tqdm h5py matplotlib bokeh jupyter
Collecting numpy
  Using cached numpy-1.22.3-cp38-cp38-win_amd64.whl (14.7 MB)
Collecting scipy
  Using cached scipy-1.8.0-cp38-cp38-win_amd64.whl (36.9 MB)
Collecting tqdm
  Using cached tqdm-4.64.0-py2.py3-none-any.whl (78 kB)
Collecting h5py
  Using cached h5py-3.6.0-cp38-cp38-win_amd64.whl (2.8 MB)
```

• • •

```
Installing collected packages: webencodings, wcwidth, Send2Trash, pywin32, pure-eval, pickleshare, mistune, ipython-genu
tils, fastjsonschema, executing, backcall, zipp, typing-extensions, traitlets, tornado, tinycss2, soupsieve, six, pyzmq,
 PyYAML, pywinpty, pyrsistent, pyparsing, pygments, pycparser, psutil, prompt-toolkit, prometheus-client, pillow, parso,
 pandocfilters, numpy, nest-asyncio, MarkupSafe, kiwisolver, jupyterlab-widgets, jupyterlab-pygments, fonttools, entrypo
ints, defusedxml, decorator, debugpy, cycler, colorama, attrs, tqdm, terminado, scipy, python-dateutil, packaging, matpl
otlib-inline, jupyter-core, Jinja2, jedi, importlib-resources, h5py, cffi, bleach, beautifulsoup4, asttokens, stack-data
, qtpy, matplotlib, jupyter-client, jsonschema, bokeh, argon2-cffi-bindings, nbformat, ipython, argon2-cffi, nbclient, i
pykernel, qtconsole, nbconvert, jupyter-console, notebook, widgetsnbextension, ipywidgets, jupyter
Successfully installed Jinja2-3.1.2 MarkupSafe-2.1.1 PyYAML-6.0 Send2Trash-1.8.0 argon2-cffi-21.3.0 argon2-cffi-bindings
-21.2.0 asttokens-2.0.5 attrs-21.4.0 backcall-0.2.0 beautifulsoup4-4.11.1 bleach-5.0.0 bokeh-2.4.2 cffi-1.15.0 colorama-
0.4.4 cycler-0.11.0 debugpy-1.6.0 decorator-5.1.1 defusedxml-0.7.1 entrypoints-0.4 executing-0.8.3 fastjsonschema-2.15.3
 fonttools-4.33.3 h5py-3.6.0 importlib-resources-5.7.1 ipykernel-6.13.0 ipython-8.3.0 ipython-genutils-0.2.0 ipywidgets-
7.7.0 jedi-0.18.1 jsonschema-4.4.0 jupyter-1.0.0 jupyter-client-7.3.0 jupyter-console-6.4.3 jupyter-core-4.10.0 jupyterl
ab-pygments-0.2.2 jupyterlab-widgets-1.1.0 kiwisolver-1.4.2 matplotlib-3.5.2 matplotlib-inline-0.1.3 mistune-0.8.4 nbcli
ent-0.6.2 nbconvert-6.5.0 nbformat-5.3.0 nest-asyncio-1.5.5 notebook-6.4.11 numpy-1.22.3 packaging-21.3 pandocfilters-1.
5.0 parso-0.8.3 pickleshare-0.7.5 pillow-9.1.0 prometheus-client-0.14.1 prompt-toolkit-3.0.29 psutil-5.9.0 pure-eval-0.2
.2 pycparser-2.21 pygments-2.12.0 pyparsing-3.0.8 pyrsistent-0.18.1 python-dateutil-2.8.2 pywin32-304 pywinpty-2.0.5 pyz
mq-22.3.0 qtconsole-5.3.0 qtpy-2.1.0 scipy-1.8.0 six-1.16.0 soupsieve-2.3.2.post1 stack-data-0.2.0 terminado-0.13.3 tiny
css2-1.1.1 tornado-6.1 tqdm-4.64.0 traitlets-5.1.1 typing-extensions-4.2.0 wcwidth-0.2.5 webencodings-0.5.1 widgetsnbext
ension-3.6.0 zipp-3.8.0

(dpa) C:₩Users₩jin>_
```

실습데이터

- 1. DES SW
  - https://www.dropbox.com/s/atq3tihqzs0sij2/220423_jinsunghyun_cw-xmega-des-5MHz-50MS-10ppc-N5000-comp1ppc--2022.04.07-18.50.58.h5?dl=0

- 2. DES HW
  - DPA Contest v1 : https://www.dpacontest.org/index.php
  - secmatv1_2006_04_0809
    - [Bin] https://www.dropbox.com/s/ca5i035woqhawkn/secmatv1_2006_04_0809.zip?dl=0
    - [mat] https://www.dropbox.com/s/ye2o0h7c2jo470k/secmatv1_2006_04_0809.mat?dl=0
    - [hdf5] https://www.dropbox.com/s/d3be01gv4elpkqy/secmatv1_2006_04_0809.h5?dl=0

KOREA UNIVERSITY

INSTITUTE OF CYBER SECURITY & PRIVACY

Korea University CIST Center for Information Security Technologies

Cryptographic Algorithm Laboratory

Q&A

Thanks

[mail] **sunghyunjin@korea.ac.kr** [web] **sunghyunjin.com** [twitter] **@mcsmonk_shj**

부채널 분석 실습

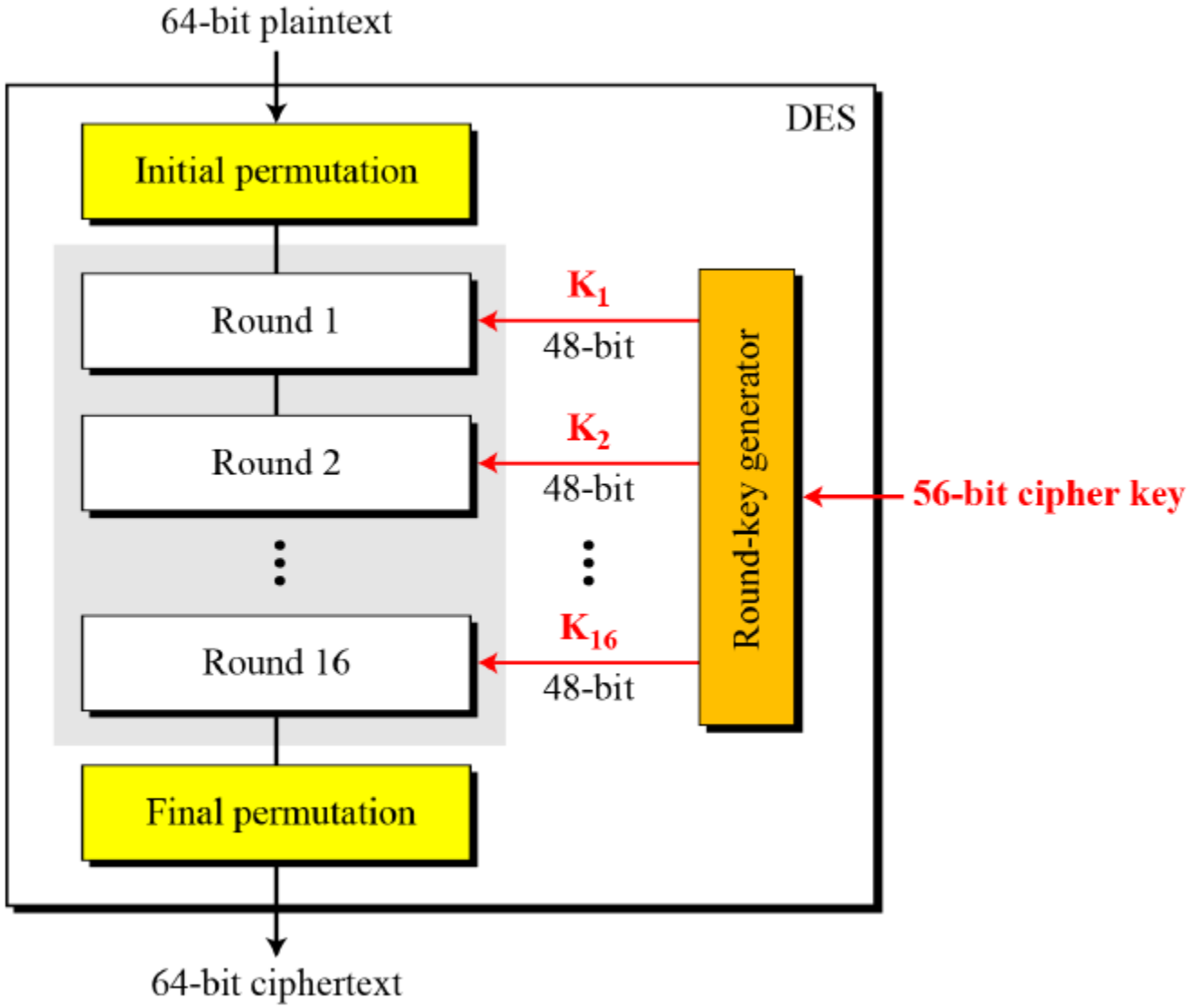
Differential Power Analysis on DES

2022 년 5 월 13 일

진성현

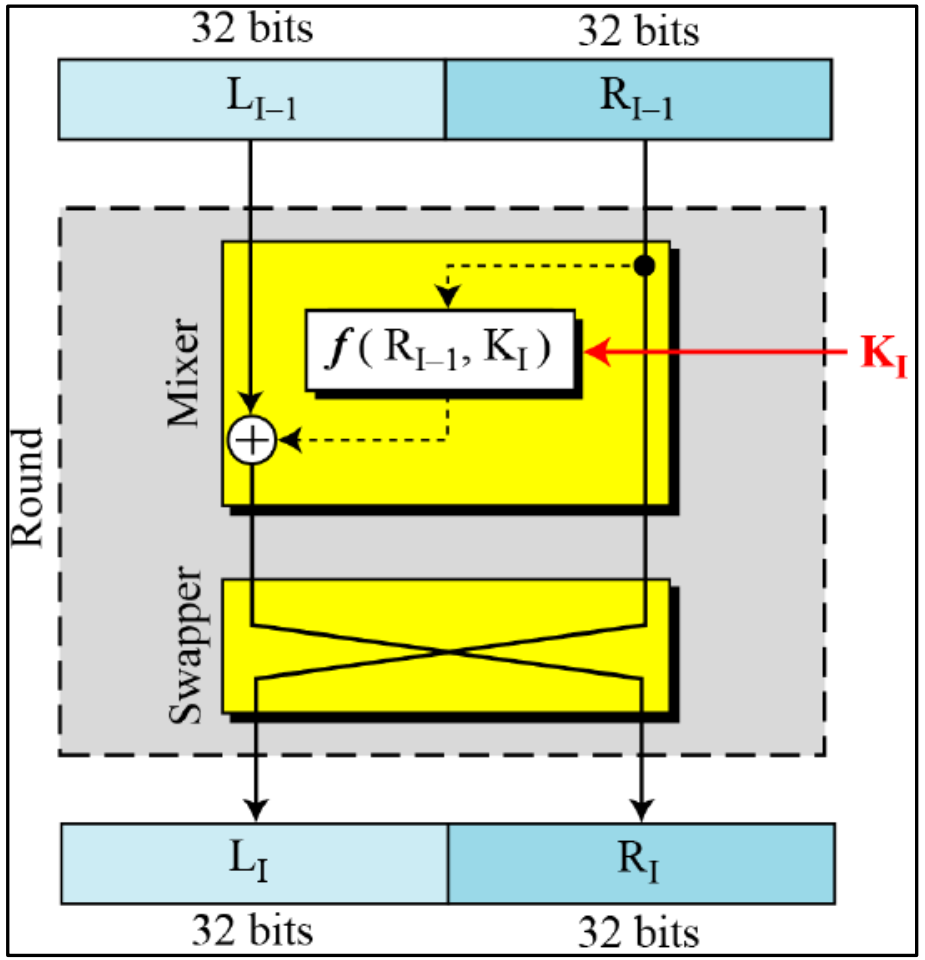
Data Encryption Standard

- 64-bit Block Cipher
- 56-bit Key
- 16 Round Feistel Structure

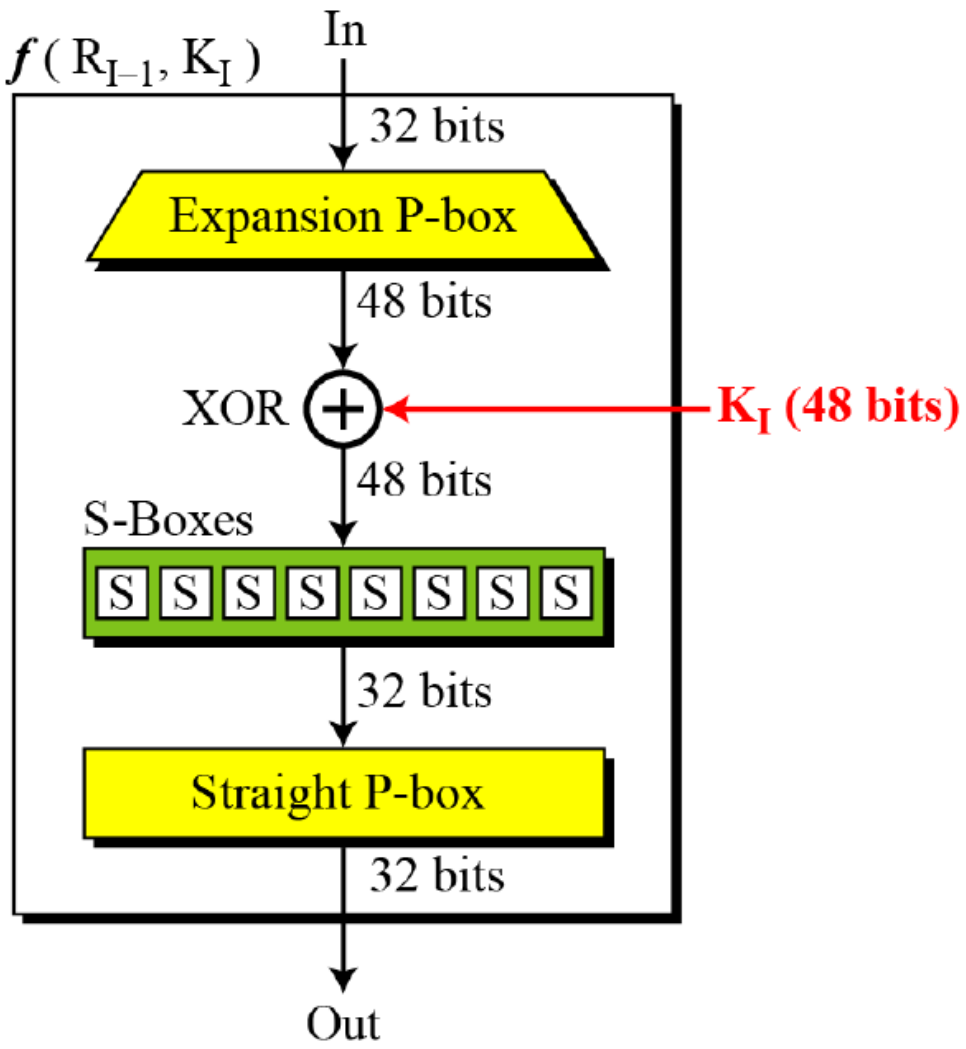


Data Encryption Standard

Round 함수

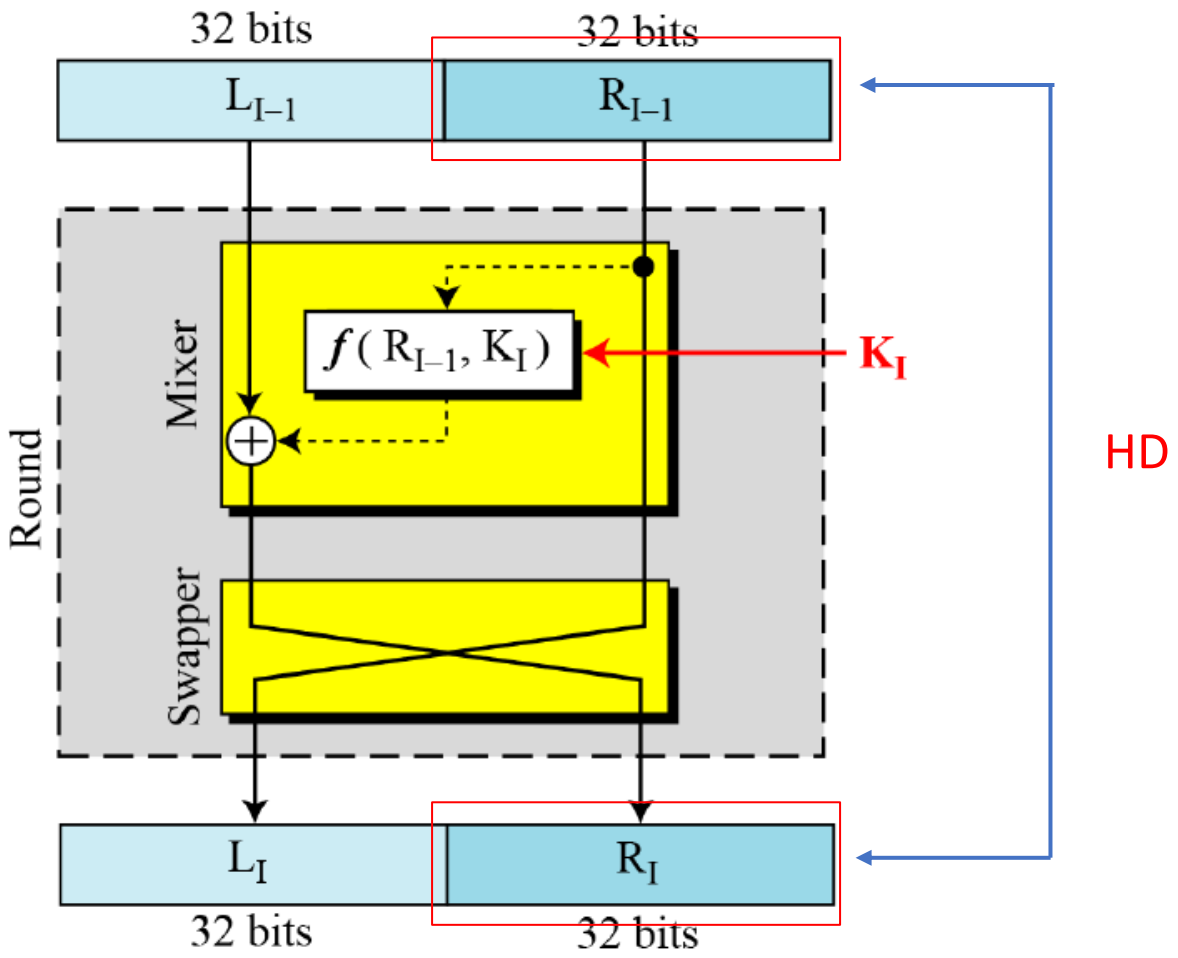


Round F-함수

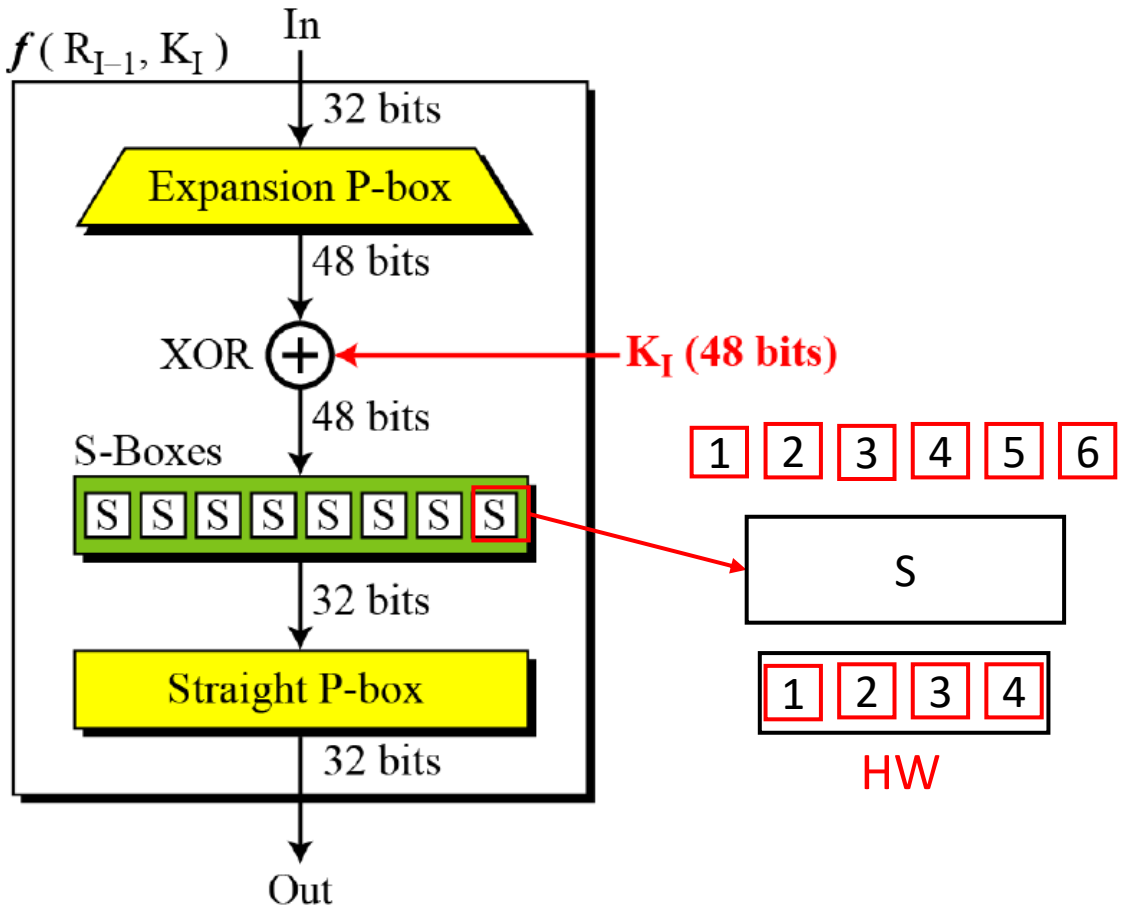


DES Target

Hardware Implementation



Software Implementation



Cryptographic Algorithm Laboratory

Reference

- Numpy
  - https://numpy.org/learn/
  - https://github.com/numpy
  - https://cs231n.github.io/python-numpy-tutorial/
- DPA tutorial code
  - https://github.com/mcsmonk/sca-tutorial-dpa-des

KOREA UNIVERSITY

INSTITUTE OF CYBER SECURITY & PRIVACY

Korea University CIST Center for Information Security Technologies

Cryptographic Algorithm Laboratory

Q&A

Thanks

[mail] **sunghyunjin@korea.ac.kr** [web] **sunghyunjin.com** [twitter] **@mcsmonk_shj**