

TikZ for Cryptographers

Jérémy Jean

Jean.Jeremy@gmail.com

FSE 2016 Rump Session

March 22, 2016

Facts

- Papers/presentations using **Figures** can only be better.
 - They illustrate textual arguments.

Facts

- Papers/presentations using **Figures** can only be better.
 - They illustrate textual arguments.
 - Complex ideas can often be simply explained using pictures.

Facts

- Papers/presentations using **Figures** can only be better.
 - They illustrate textual arguments.
 - Complex ideas can often be simply explained using pictures.
 - People prefer pictures over text anyway.

Facts

- Papers/presentations using **Figures** can only be better.
 - They illustrate textual arguments.
 - Complex ideas can often be simply explained using pictures.
 - People prefer pictures over text anyway.
- However, drawing them can be

Facts

- Papers/presentations using **Figures** can only be better.
 - They illustrate textual arguments.
 - Complex ideas can often be simply explained using pictures.
 - People prefer pictures over text anyway.
- However, drawing them can be
 - tedious,

Facts

- Papers/presentations using **Figures** can only be better.
 - They illustrate textual arguments.
 - Complex ideas can often be simply explained using pictures.
 - People prefer pictures over text anyway.
- However, drawing them can be
 - tedious,
 - frustrating,

Facts

- Papers/presentations using **Figures** can only be better.
 - They illustrate textual arguments.
 - Complex ideas can often be simply explained using pictures.
 - People prefer pictures over text anyway.
- However, drawing them can be
 - tedious,
 - frustrating,
 - time consuming.

Facts

- Papers/presentations using **Figures** can only be better.
 - They illustrate textual arguments.
 - Complex ideas can often be simply explained using pictures.
 - People prefer pictures over text anyway.
- However, drawing them can be
 - tedious,
 - frustrating,
 - time consuming.
- But: there exist tools to draw them straight from LaTeX
 - **TikZ!**

Facts

- Papers/presentations using **Figures** can only be better.
 - They illustrate textual arguments.
 - Complex ideas can often be simply explained using pictures.
 - People prefer pictures over text anyway.
- However, drawing them can be
 - tedious,
 - frustrating,
 - time consuming.
- But: there exist tools to draw them straight from LaTeX
 - **TikZ!**
 - The results usually look really good.

Facts

- Papers/presentations using **Figures** can only be better.
 - They illustrate textual arguments.
 - Complex ideas can often be simply explained using pictures.
 - People prefer pictures over text anyway.
- However, drawing them can be
 - tedious,
 - frustrating,
 - time consuming.
- But: there exist tools to draw them straight from LaTeX
 - **TikZ!**
 - The results usually look really good.
 - It can produce reusable PDF images.

Contribution

An online repository of TikZ figures.

L^AT_EX

101 TikZ figures

Search...

AE 7

AES 13

Block ciphers 12

Construction 11

Cryptanalysis 20

Feistel 4

General 1

Hash Functions 26

Models 4

Modes 3

TikZ for Cryptographers

What is TikZ?

PGF/TikZ is a tandem of languages for producing vector **graphics** from a geometric/algebraic description. PGF is a lower-level language, while TikZ is a set of higher-level macros that use PGF. The top-level PGF and TikZ commands are invoked as TeX macros. Together with the LaTeX language, it is the most efficient way to write **research papers**.

[More from Wikipedia.](#)

How to contribute

Do you have any TIKZ code that you are willing to **share**? If yes, please do not hesitate to send me an **email** with the images, and I will look into including them into this repository.

News

- 2015-02-23 Added 4 figures.
- 2015-02-20 Added 12 figures.
- 2015-02-07 Added 84 figures.
- 2015-02-07 Website is up.

How to use this repository

You can browse the available figures by using the left menu, either selecting one of the **categories**, or by **searching** for a keyword in the dedicated field. A sublist of the corresponding figures will then appear, and choosing any will display the actual compiled image (in low-quality for efficiency reasons) together with its associated LaTeX code generating it. From there, you can download the actual code and/or PDF, as well as some custom packages.

Free of use

All the TikZ images and codes available of this website are **free of use**. You can use them to create your owns, modify them as much as you want, and include them in any documents. Nevertheless, we would be grateful if you could **cite** this repository as a source of inspiration. :-)

Contact

My name is **Jérémy Jean**, and you can contact me about this repository at this email address: [JJean\(at\)ntu\(dot\)edu\(dot\)sg](mailto:JJean(at)ntu(dot)edu(dot)sg).
My webpage is online here: <http://www.di.ens.fr/~jean/>.

http://www.di.ens.fr/~jean/latex_crypto/
(temporary)

Example

You look for the round function of the PRESENT block cipher.

L^AT_EX

101 TikZ figures

Search...

AE 7

AES 13

Block ciphers 12

Construction 11

Cryptanalysis 20

Feistel 4

General 1

Hash Functions 26

Models 4

Modes 3

Block cipher black-box representation

Key-alternating cipher

LBlock F-function

LBlock round function

LED-128 block cipher

LED-64 block cipher

PRESENT block cipher

PRINCE block cipher

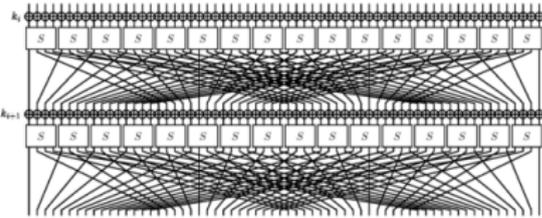
Piccolo F-function

Piccolo RP Permutation

Piccolo block cipher

TWINE round function

Title: PRESENT block cipher.
Author: Jérémie Jean.
Date: February 2015.
Section: Block ciphers.
Required packages  : crypto symbols • custom arrows.
Download files: PNG • PDF • TEX.



```
\documentclass{standalone}

%% Common TikZ libraries
\usepackage{tikz}
\usetikzlibrary{calc}
\usetikzlibrary{positioning}

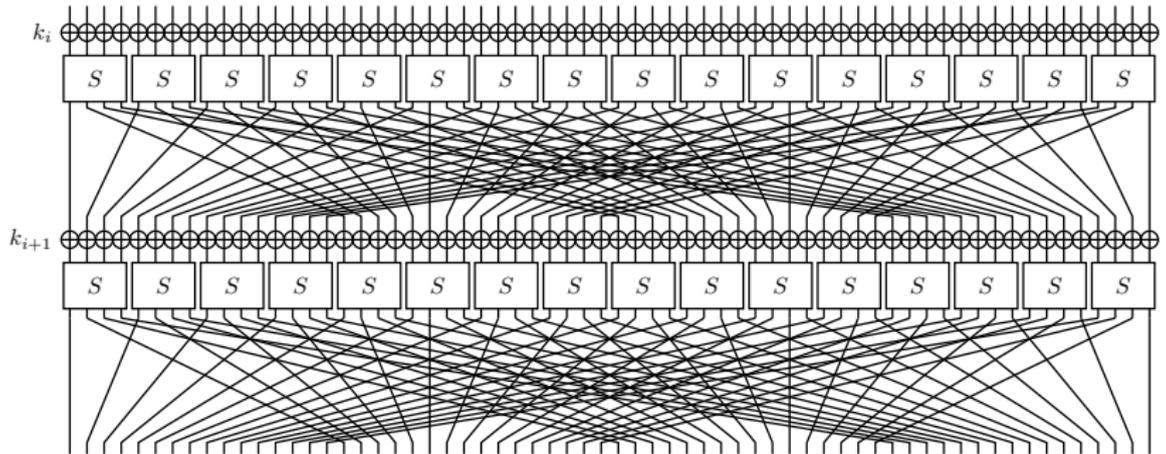
%% Custom TikZ addons
\usetikzlibrary{crypto.symbols}
\tikzset{shadows=no} % Option: add shadows to XOR, ADD, etc.

%% Document
\begin{document}
\begin{tikzpicture}
```

Example

```
12 %% Document
13 \begin{document}
14 \begin{tikzpicture}
15
16   %% Subkey XORs
17   \foreach \z in {0,...,63} {
18     \node[XOR, scale=0.8] (xor\z) at ($\z*(0.75em, 0)$) {};
19     \node[XOR, scale=0.8] (xorr\z) at ($\z*(0.75em, 0)+(0,-9em)$) {};
20   }
21
22   %% Nodes positions
23   \foreach \z in {0,...,63} {
24     \node (i\z) [above = 0.75em of xor\z] {};
25     \node (o\z) [below = 2.5em of xor\z] {};
26     \node (ii\z) [above = 0.25em of xorr\z] {};
27     \node (oo\z) [below = 3em of xorr\z] {};
28     \node (t\z) [below = 4em of oo\z] {};
29     \draw[thick] (i\z) -- (xor\z);
30   }
31
32   %% Permutation layer
33   \foreach \z [evaluate=\z as \zz using {int(mod(16*\z,63))}] in {0,...,62} {
34     \draw[thick] (xor\z) -- (o\z.center) -- (ii\zz.center) -- (xorr\zz) -- (oo\zz);
35     \draw[thick] (oo\z.north) -- (t\zz.south) -- +(0,-0.5em);
36   }
37   \draw[thick] (xor63) -- (o63.center) -- (ii63.center) -- (xorr63) -- (oo63);
38   \draw[thick] (oo63.north) -- (t63.south) -- +(0,-0.5em);
39
40   %% SBoxes
41   \foreach \z in {0,...,15} {
42     \node[draw,thick,minimum width=2.75em,minimum height=2em,fill=white] (p4) at ($\z*(3em,0) + (1.1em,-2em)$) {$$$};
43     \node[draw,thick,minimum width=2.75em,minimum height=2em,fill=white] (p4) at ($\z*(3em,0) + (1.1em,-11em)$) {$$$};
44   }
45
46   \node[left = 0em of xor0] {$k_{i}$};
47   \node[left = 0em of xorr0] {$k_{i+1}$};
48
49 \end{tikzpicture}
50 \end{document}
```

Example



Details

- Already online

`http://www.di.ens.fr/~jean/latex_crypto/`

Details

- Already online

`http://www.di.ens.fr/~jean/latex_crypto/`

- Currently

Details

- Already online

`http://www.di.ens.fr/~jean/latex_crypto/`

- Currently
 - About 100 different pictures.

Details

- Already online

`http://www.di.ens.fr/~jean/latex_crypto/`

- Currently
 - About 100 different pictures.
 - All share (almost) the same look.

Details

- Already online

`http://www.di.ens.fr/~jean/latex_crypto/`

- Currently
 - About 100 different pictures.
 - All share (almost) the same look.
 - Mostly symmetric-key related content.

Details

- Already online

`http://www.di.ens.fr/~jean/latex_crypto/`

- Currently
 - About 100 different pictures.
 - All share (almost) the same look.
 - Mostly symmetric-key related content.
- Goals

Details

- Already online

`http://www.di.ens.fr/~jean/latex_crypto/`

- Currently

- About 100 different pictures.
- All share (almost) the same look.
- Mostly symmetric-key related content.

- Goals

- Help the crypto community write better papers.

Details

- Already online

`http://www.di.ens.fr/~jean/latex_crypto/`

- Currently

- About 100 different pictures.
- All share (almost) the same look.
- Mostly symmetric-key related content.

- Goals

- Help the crypto community write better papers.
- Gather all crypto-related pictures in a single place.

Details

- Already online

`http://www.di.ens.fr/~jean/latex_crypto/`

- Currently

- About 100 different pictures.
- All share (almost) the same look.
- Mostly symmetric-key related content.

- Goals

- Help the crypto community write better papers.
- Gather all crypto-related pictures in a single place.
- **Encourage you to submit and share your crypto figures!**

http://www.di.ens.fr/~jean/latex_crypto/