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,
  - frustating,

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,
  - frustating,
  - 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,
  - frustating,
  - time consuming.
- But: there exist tools to draw them straight from LaTeX
  - **TikZ!**

Facts

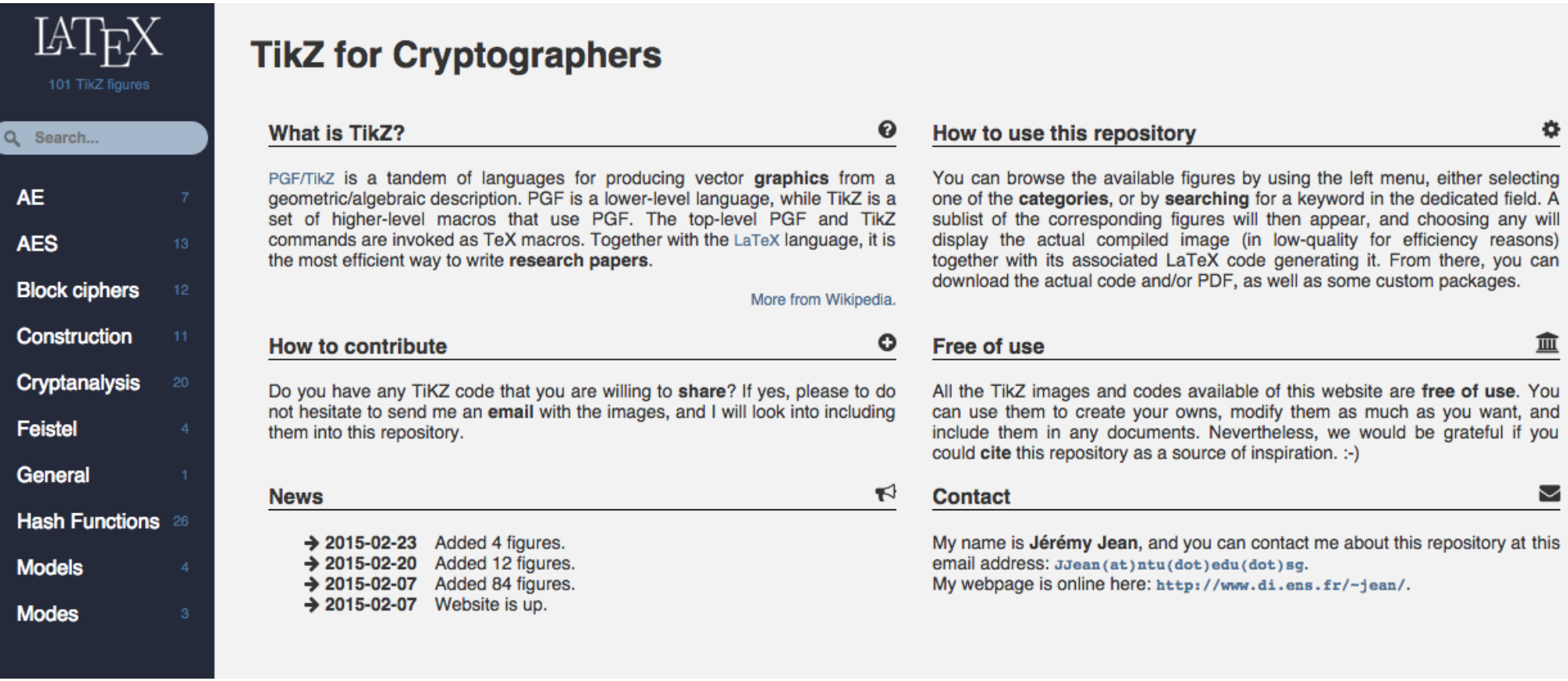
- Papers/presentations using **Figures** can only be better.
  - They illustrate textual arguments.
  - Complex ideas can often be simply explained using pictures.
  - People prefer pictures over text anyway.
- However, drawing them can be
  - tedious,
  - frustating,
  - time consuming.
- But: there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



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

(temporary)

Example

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

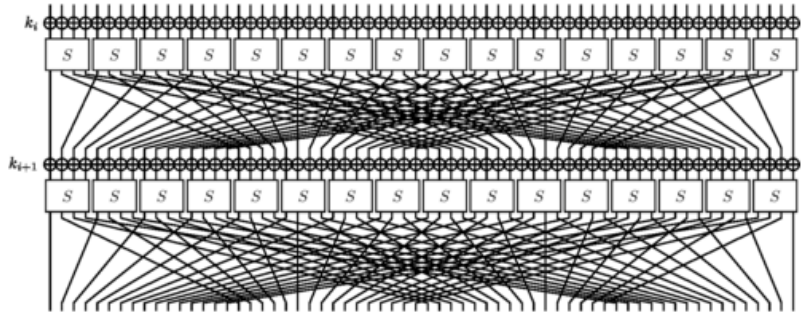
LaTeX
101 TikZ figures

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: Jérémy Jean.
Date: February 2015.
Section: Block ciphers.
Required packages : crypto symbols • custom arrows.
Download files: PNG • PDF • TEX.

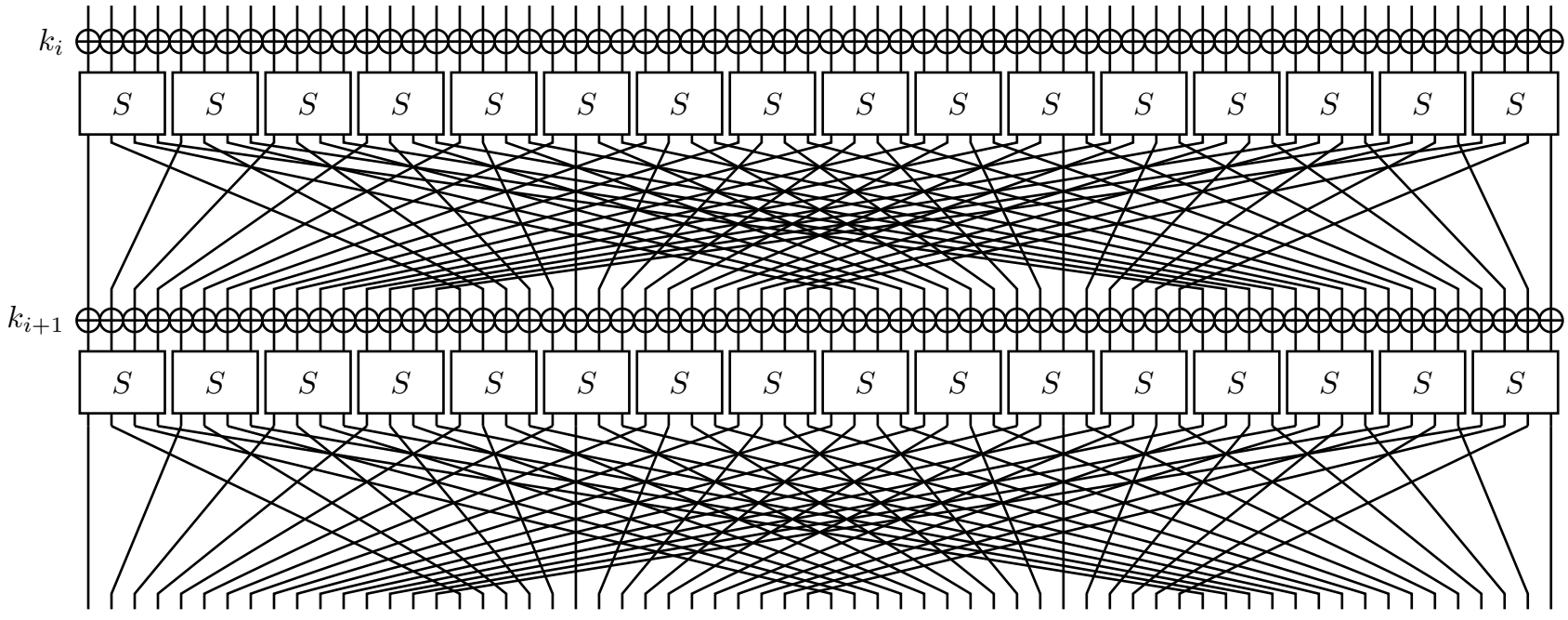



```
\documentclass{standalone}

%% 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

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

    %% Subkey XORs
    \foreach \z in {0,...,63} {
        \node[XOR, scale=0.8] (xor\z) at ($\z*(0.75em, 0)$) {};
        \node[XOR, scale=0.8] (xorr\z) at ($\z*(0.75em, 0)+(0,-9em)$) {};
    }

    %% Nodes positions
    \foreach \z in {0,...,63} {
        \node (i\z) [above = 0.75em of xor\z] {};
        \node (o\z) [below = 2.5em of xor\z] {};
        \node (ii\z) [above = 0.25em of xorr\z] {};
        \node (oo\z) [below = 3em of xorr\z] {};
        \node (t\z) [below = 4em of oo\z] {};
        \draw[thick] (i\z) -- (xor\z);
    }

    %% Permutation layer
    \foreach \z [evaluate=\z as \zz using {int(mod(16*\z,63))}] in {0,...,62} {
        \draw[thick] (xor\z)  -- (o\z.center)  -- (ii\zz.center) -- (xorr\zz) -- (oo\zz);
        \draw[thick] (oo\z.north)  -- (t\zz.south) -- +(0,-0.5em);
    }
    \draw[thick] (xor63) -- (o63.center) -- (ii63.center) -- (xorr63) -- (oo63);
    \draw[thick] (oo63.north) -- (t63.south) -- +(0,-0.5em);

    %% SBoxes
    \foreach \z in {0,...,15} {
        \node[draw,thick,minimum width=2.75em,minimum height=2em,fill=white] (p4) at ($\z*(3em,0) + (1.1em,-2em)$) {$S$};
        \node[draw,thick,minimum width=2.75em,minimum height=2em,fill=white] (p4) at ($\z*(3em,0) + (1.1em,-11em)$) {$S$};
    }

    \node[left = 0em of xor0] {$k_{i}$};
    \node[left = 0em of xorr0] {$k_{i+1}$};

\end{tikzpicture}
\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/