TikZ for Cryptographers

Jérémie Jean
Jean.Jeremy@gmail.com

FSE 2016 Rump Session
March 22, 2016
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.

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.
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.
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
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,
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,
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.
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!
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.
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.

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

You look for the round function of the PRESENT block cipher.
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
  
  \[\texttt{http://www.di.ens.fr/~jean/latex_cipher/}\]

- 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/