Postponing the Deadline of the Best Crypto Competition Ever!

Bart Preneel, Céline Blondeau, D. Julius B., Edward Snowden, Gaëtan Leurent, Greg Rose, Keith Alexander, Kenny Patterson, Kevin Igoe, Orr Dunkelman, Roberto Avanzi, Simon Speck, Stefan Lucks, Tanja Lange

August 19th, 2014

Motivation

- Flagship conferences become more and more theoretical;

Motivation

- Flagship conferences become more and more theoretical;
- New researchers in cryptography take the theoretical lane;

Motivation

- Flagship conferences become more and more theoretical;
- New researchers in cryptography take the theoretical lane;
- Cryptography is not really understood by computer security professionals (who prefer San Diego over Santa Barbara, go figure!);

Motivation

- Flagship conferences become more and more theoretical;
- New researchers in cryptography take the theoretical lane;
- Cryptography is not really understood by computer security professionals (who prefer San Diego over Santa Barbara, go figure!);
- Cryptographic competitions are the best way to inspire new results:
  - AES,
  - NESSIE,
  - eSTREAM,
  - SHA-3,

Motivation

- Flagship conferences become more and more theoretical;
- New researchers in cryptography take the theoretical lane;
- Cryptography is not really understood by computer security professionals (who prefer San Diego over Santa Barbara, go figure!);
- Cryptographic competitions are the best way to inspire new results:
    - AES,
    - NESSIE,
    - eSTREAM,
    - SHA-3,
    - Inefficient crypto competition (A.K.A. PHC)
    - Not really sure what we are doing competition (A.K.A. CAESAR, stay for DIAC!)

The True Need for Security

- At FSE 2014 and EUROCRYPT 2014 the best crypto competition was announced
- The competition will adhere to NIST's new guidelines for making trusted standards
- VCAT approved, NSA disapproved, generally disproved!
- Outcome to meet market demand and fill some much needed gaps in the literature!

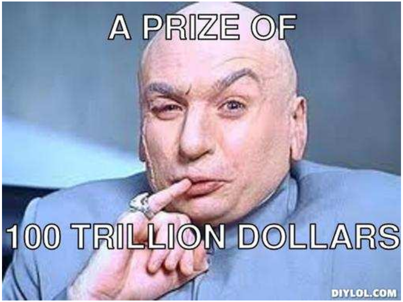
Introducing the Snake Oil Crypto Competition!

The Snake Oil Crypto Competition!

- Aims to extract first grade Snake Oil Crypto primitives
- Run by the “people”, for the “people”
- The only one that assures winners world fame

The Snake Oil Crypto Competition!

- Aims to extract first grade Snake Oil Crypto primitives
- Run by the "people", for the "people"
- The only one that assures winners world fame and 100 trillion dollar



The Snake Oil Crypto Competition!

- Aims to extract first grade Snake Oil Crypto primitives
- Run by the "people", for the "people"
- The only one that assures winners world fame and 100 trillion dollar (ZWR, i.e., third Zimbabwean dollar)

100 000 000 000 000
RESERVE BANK OF ZIMBABWE
I promise to pay the bearer on demand
ONE HUNDRED TRILLION DOLLARS
for the Reserve Bank of Zimbabwe
Dr. G. Gono Governor
HARARE 2008
AA3905431

The Snake Oil Crypto Competition!

- Aims to extract first grade Snake Oil Crypto primitives
- Run by the “people”, for the “people”
- The only one that assures winners world fame and 100 trillion dollar (ZWR, i.e., third Zimbabwean dollar) and **an empty(!)** bottle of premium snake oil

The Snake Oil Crypto Competition!

- Aims to extract first grade Snake Oil Crypto primitives
- Run by the "people", for the "people"
- The only one that assures winners world fame and 100 trillion dollar (ZWR, i.e., third Zimbabwean dollar) and **an empty(!)** bottle of premium snake oil
- The **only crypto competition** to be supported by the Information Dominance Center, and his excellence, the emperor Alexander

Security Requirements

- Brute-forcing the key should be hard
- Distinguishing the C code from randomly generated code should be hard
- The cipher should run in a finite amount of time on most inputs (security proofs are a plus)
- Security against some known and/or unknown attacks
- The cipher **must** make the user feel secure

Security Requirements

- Brute-forcing the key should be hard
- Distinguishing the C code from randomly generated code should be hard
- The cipher should run in a finite amount of time on most inputs (security proofs are a plus)
- Security against some known and/or unknown attacks
- The cipher **must** make the user feel secure, unless his with Al-Qaeda (then he must feel hunted down)

Security Requirements

- Brute-forcing the key should be hard
- Distinguishing the C code from randomly generated code should be hard
- The cipher should run in a finite amount of time on most inputs (security proofs are a plus)
- Security against some known and/or unknown attacks
- The cipher **must** make the user feel secure, unless his with Al-Qaeda (then he must feel hunted down) or with the EFF (then he must feel paranoid)

Things which are NOT ACCEPTED

- Chaos based cryptography
- Submissions form Joan Daemen and/or Vincent Rijmen
- Designs based on Serpent or the Cobra family or any related reptile family

Timeline

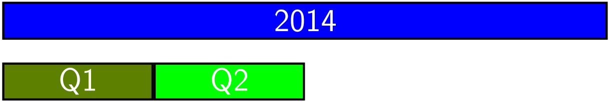
2014

Q1

Announcement ✓

Set deadline to Q3 ✓

Timeline



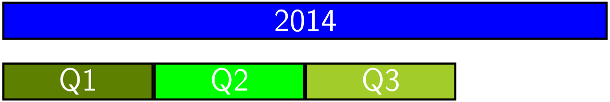
2014

Q1 Q2

CFP released ✓

Postpone deadline to Q4 ✓

Timeline

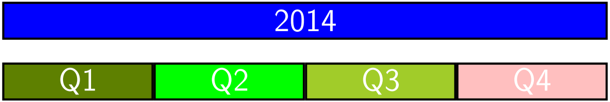


2014

Q1 Q2 Q3

Push deadline back to 2014Q2

Timeline

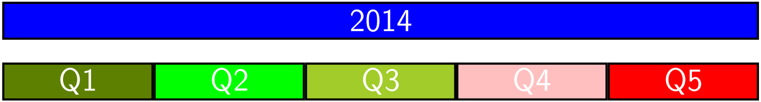


2014

Q1 Q2 Q3 Q4

Open submission server

Timeline



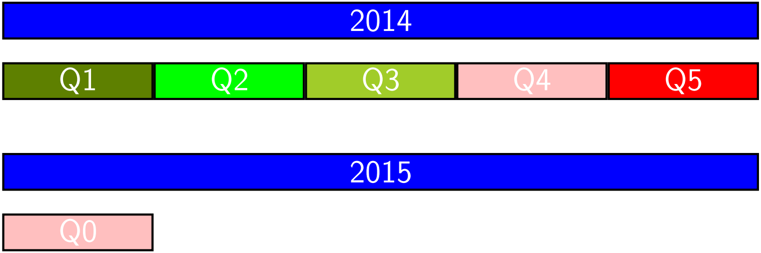
2014

Q1 Q2 Q3 Q4 Q5

Ask for comments on call

Ask for comments on process

Timeline



2014

Q1 Q2 Q3 Q4 Q5

2015

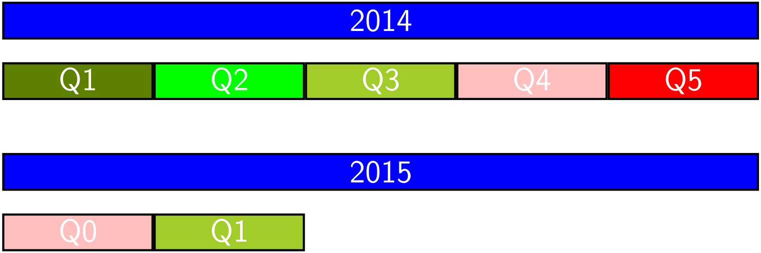
Q0

Tweaks

Disregard comments on call/process

Accept comments from IACR board

Timeline



2014

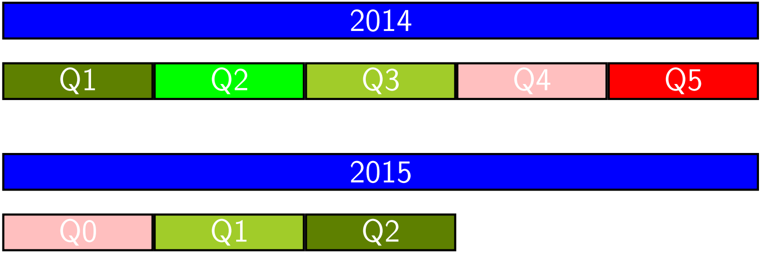
Q1 Q2 Q3 Q4 Q5

2015

Q0 Q1

Real deadline

Timeline



2014

Q1 Q2 Q3 Q4 Q5

2015

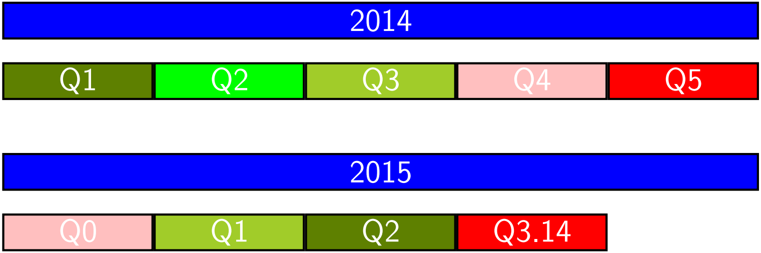
Q0 Q1 Q2

Candidate workshop

(collocation with Eurovision)

Deadline for calendarly-challenged

Timeline



2014

Q1 Q2 Q3 Q4 Q5

2015

Q0 Q1 Q2 Q3.14

NSA comments
(private communication)

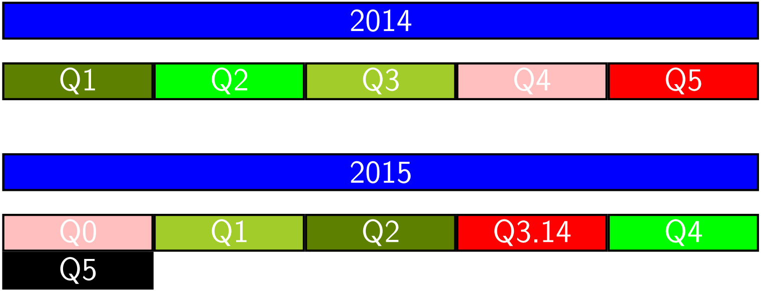
Timeline

2014				
Q1	Q2	Q3	Q4	Q5

2015				
Q0	Q1	Q2	Q3.14	Q4

NSA comments
(leaked)

Timeline



2014

Q1 Q2 Q3 Q4 Q5

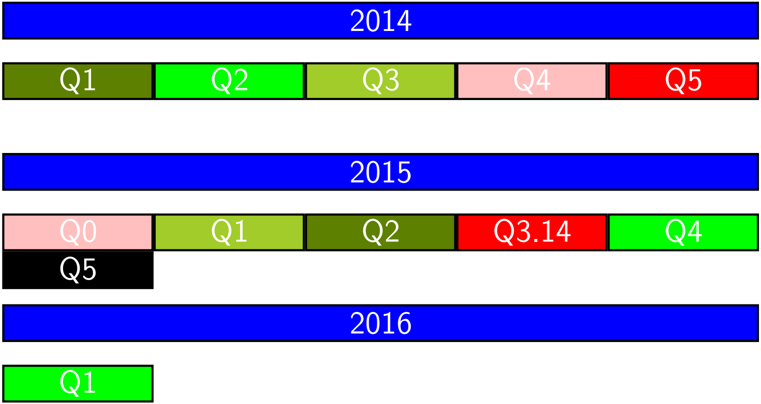
2015

Q0 Q1 Q2 Q3.14 Q4

Q5

Winner selected!

Timeline



2014

Q1 Q2 Q3 Q4 Q5

2015

Q0 Q1 Q2 Q3.14 Q4

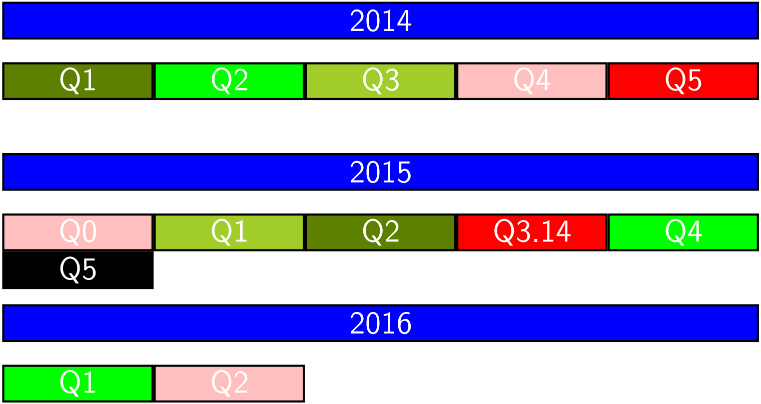
Q5

2016

Q1

Altering winner’s parameters

Timeline



2014

Q1 Q2 Q3 Q4 Q5

2015

Q0 Q1 Q2 Q3.14 Q4

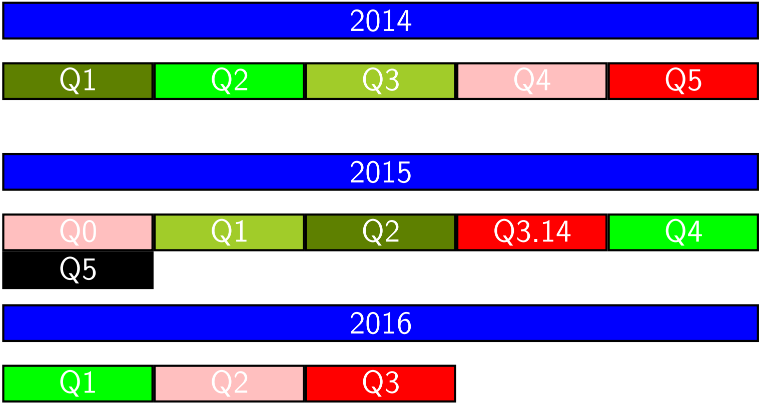
Q5

2016

Q1 Q2

Altering winner's parameters to default ones

Timeline



2014

Q1 Q2 Q3 Q4 Q5

2015

Q0 Q1 Q2 Q3.14 Q4

Q5

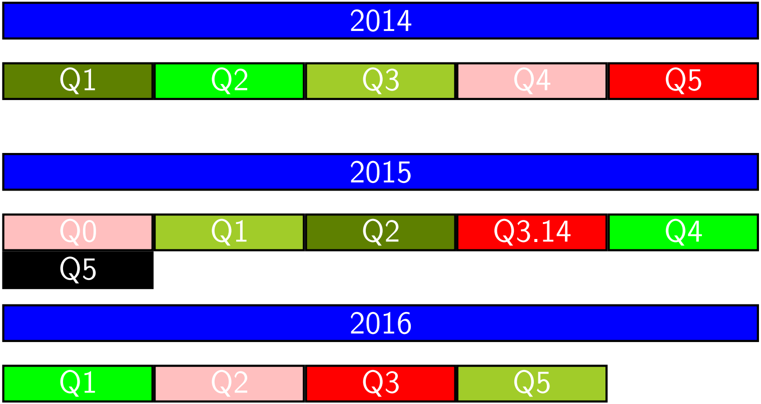
2016

Q1 Q2 Q3

~~Altering winner's parameters to default ones~~

Picking a different winner due to IP issues

Timeline



2014

Q1 Q2 Q3 Q4 Q5

2015

Q0 Q1 Q2 Q3.14 Q4

Q5

2016

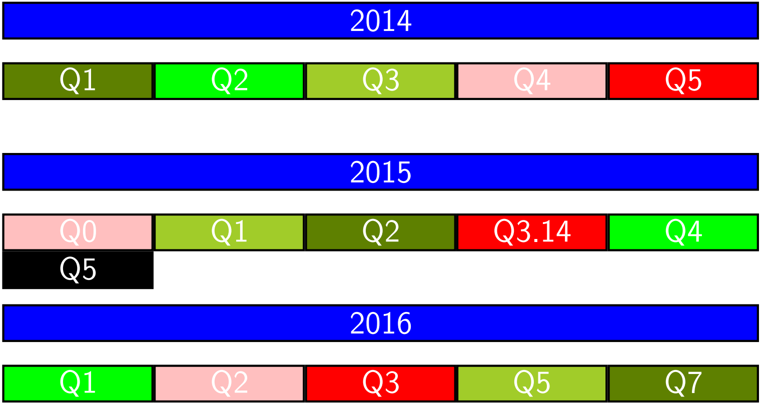
Q1 Q2 Q3 Q5

Standard is out!

Post-Snakeoil Cryptography

Pay EMC to implement

Timeline



2014

Q1 Q2 Q3 Q4 Q5

2015

Q0 Q1 Q2 Q3.14 Q4

Q5

2016

Q1 Q2 Q3 Q5 Q7

Add missing $\lll$ 1 to standard

Submit!

- So far, only two submissions.

Submit!

- So far, only two submissions.
- And an honorary submission (joint NSA/NIST submission — in process of leaving NSA to only submitters).

Submit!

- So far, only two submissions.
- And an honorary submission (joint NSA/NIST submission — in process of leaving NSA to only submitters).
- A team of bored experts are waiting just for you!

Submit!

- So far, only two submissions.
- And an honorary submission (joint NSA/NIST submission — in process of leaving NSA to only submitters).
- A team of bored experts are waiting just for you!
- To be published at Journal of Craptology and as NIST SP800-123.45!

Submit!

- So far, only two submissions.
- And an honorary submission (joint NSA/NIST submission — in process of leaving NSA to only submitters).
- A team of bored experts are waiting just for you!
- To be published at Journal of Craptology and as NIST SP800-123.45!
- To be immediately accepted into IEEE P1619, ANSI 9.52X, and of course, TLS 1.3.1.4!

Submit!

- So far, only two submissions.
- And an honorary submission (joint NSA/NIST submission — in process of leaving NSA to only submitters).
- A team of bored experts are waiting just for you!
- To be published at Journal of Craptology and as NIST SP800-123.45!
- To be immediately accepted into IEEE P1619, ANSI 9.52X, and of course, TLS 1.3.1.4!
- Theoretical submissions will be accepted in theory.

More Information

For more information visit

snakeoil.cr.yp.to