Announcing the Best Crypto Competition!

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

March 4th, 2014

The Need for Security

Emerging challenges in computer security calls for cryptographic solutions which are:

- Ultra-fast;
- Require very little resources;
- Offer adequate security

The Need for Security

Emerging challenges in computer security calls for cryptographic solutions which are:

- Ultra-fast;
- Require very little resources;
- Offer adequate security

Luckily, we already had AES, NESSIE, eSTREAM, SHA-3, and working on some more competitions — CAESAR and PHC.

The True Need for Security

- Despite all efforts, people are still using weak encryption

The True Need for Security

- Despite all efforts, people are still using weak encryption
- Various companies and organizations are promoting the use of such encryption, rather than the good stuff we already have

The True Need for Security

- Despite all efforts, people are still using weak encryption
- Various companies and organizations are promoting the use of such encryption, rather than the good stuff we already have
- Moreover, people are willing to use stuff which we all know is weak

The True Need for Security

- Despite all efforts, people are still using weak encryption
- Various companies and organizations are promoting the use of such encryption, rather than the good stuff we already have
- Moreover, people are willing to use stuff which we all know is weak
- This proves that as researchers we have no idea what the people want

The True Need for Security

- Despite all efforts, people are still using weak encryption
- Various companies and organizations are promoting the use of such encryption, rather than the good stuff we already have
- Moreover, people are willing to use stuff which we all know is weak
- This proves that as researchers we have no idea what the people want
- Hence, we are starting a competition to fill the much-needed gap...

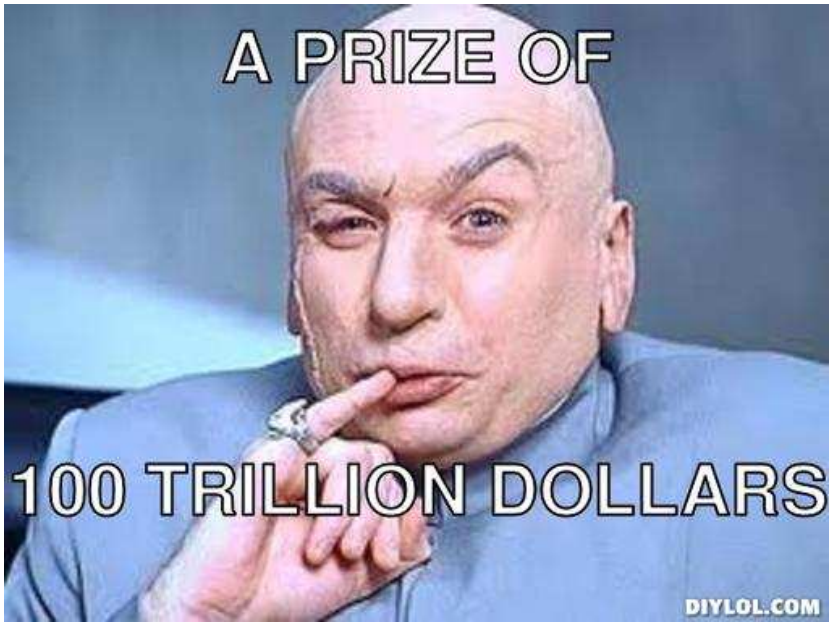
Introducing the Snake Oil Crypto Competition!

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)

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 a 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 a bottle of premium snake oil
- The **only crypto competition** to be supported by the information domination center, and his excellence, the emperor Alexander

Security Requirements

- Brute-forcing the key should be hard

Security Requirements

- Brute-forcing the key should be hard
- Distinguishing the C code from randomly generated code should be hard

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 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

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

Extra Features == Extra Points!

- Decryption being correct most of the time
- NSA endorsing your design
- Implementations on a wide range of platforms
- Should rely on patents
- Protection against front-channel attacks
- Paying companies to deploy your design
- Master keys stored on an internet-connected machine
- Inventing original backdoors
- Synergetic and multidisciplinary designs
- Published at TCC
- Protection against cash attacks
- Proof of knowledge of backdoor
- Protection against decryption misuse
- Zero-accuracy proof of security

Things which are NOT ACCEPTED

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

Timeline

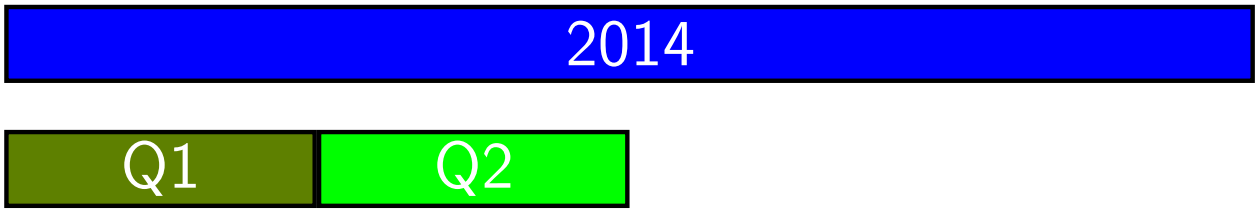
2014

Q1

Announcement

Set deadline to Q3

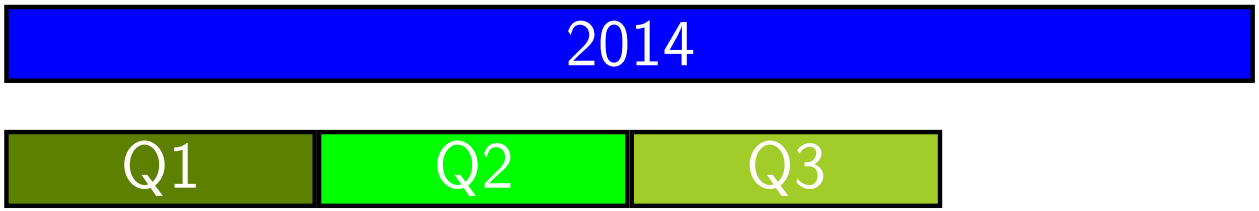
Timeline



CFP released

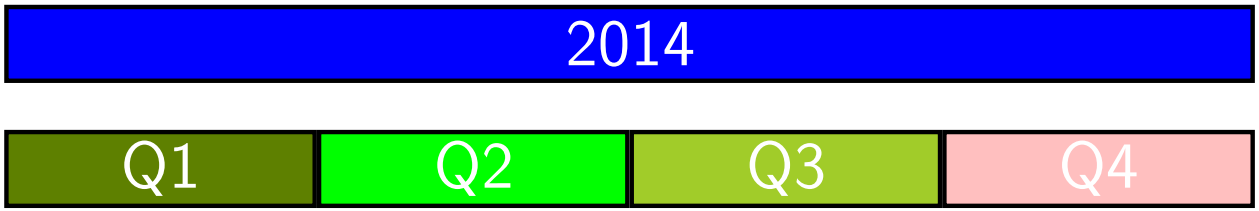
Postpone deadline to Q4

Timeline



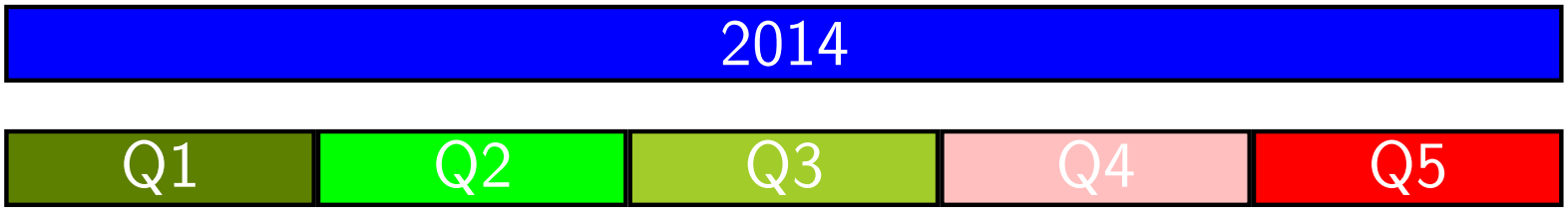
Push deadline back to Q2

Timeline



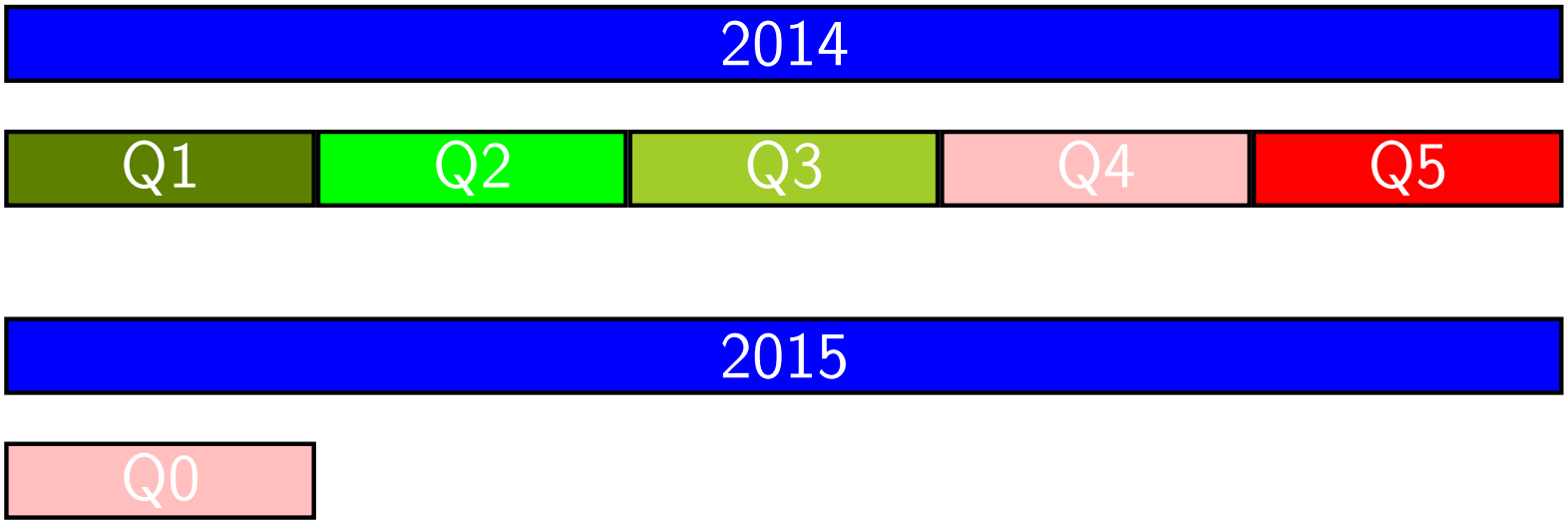
Open submission server

Timeline



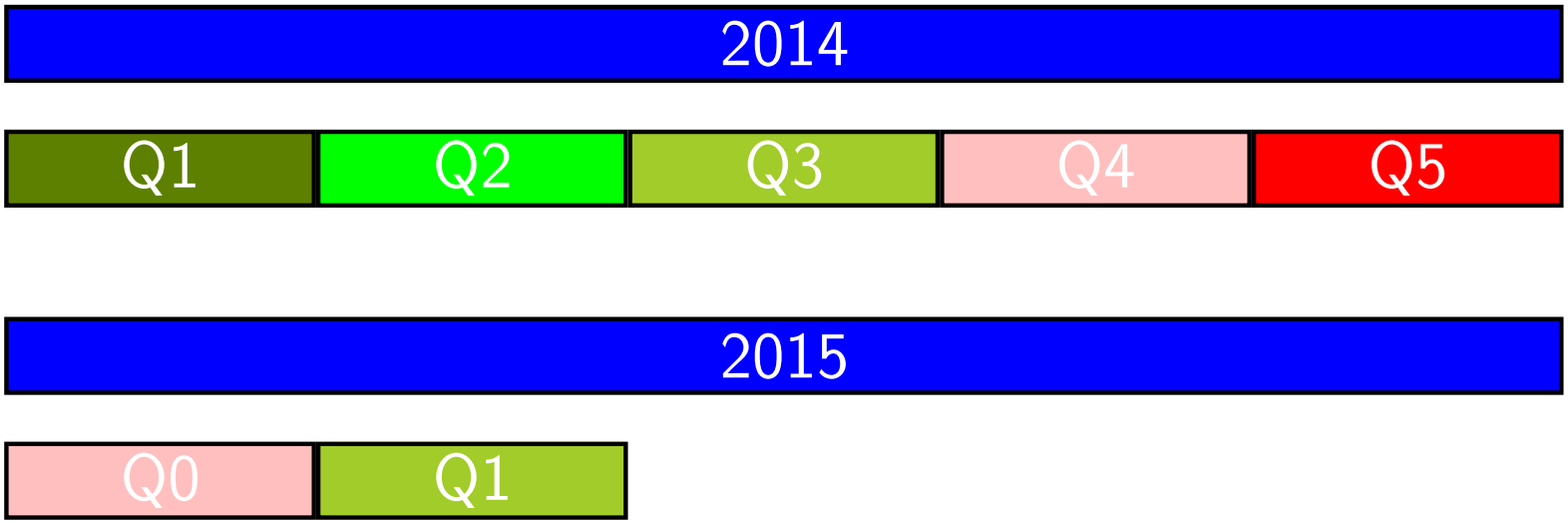
Ask for comments on call

Timeline



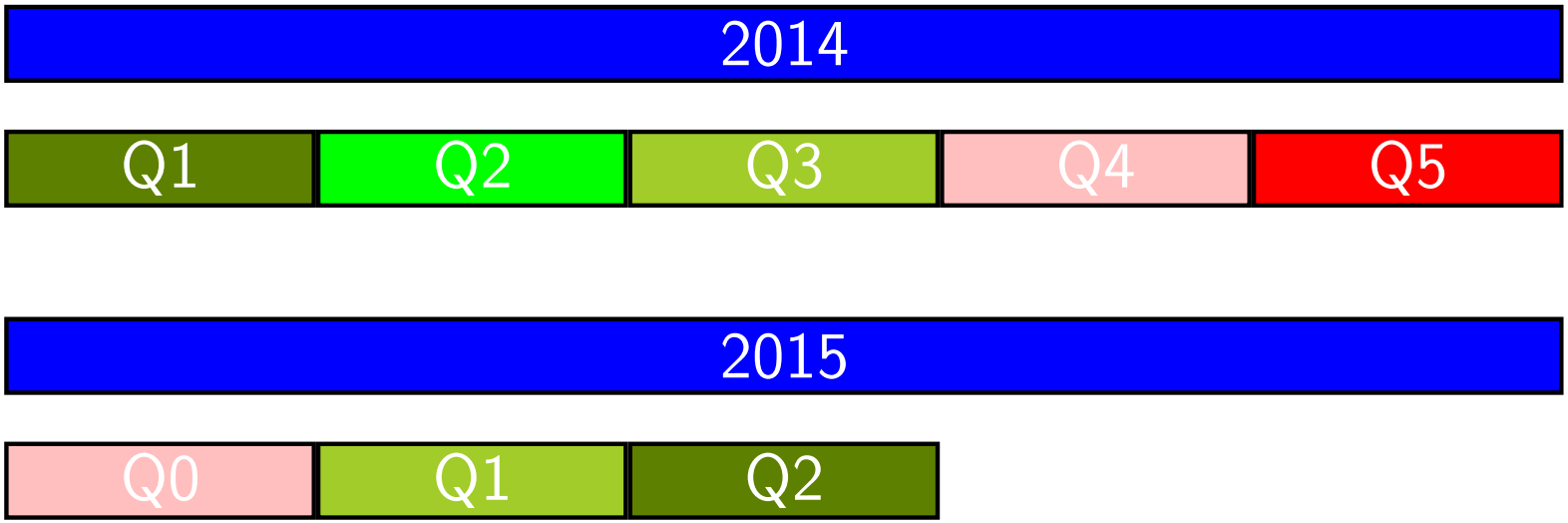
Tweaks

Timeline



Real deadline

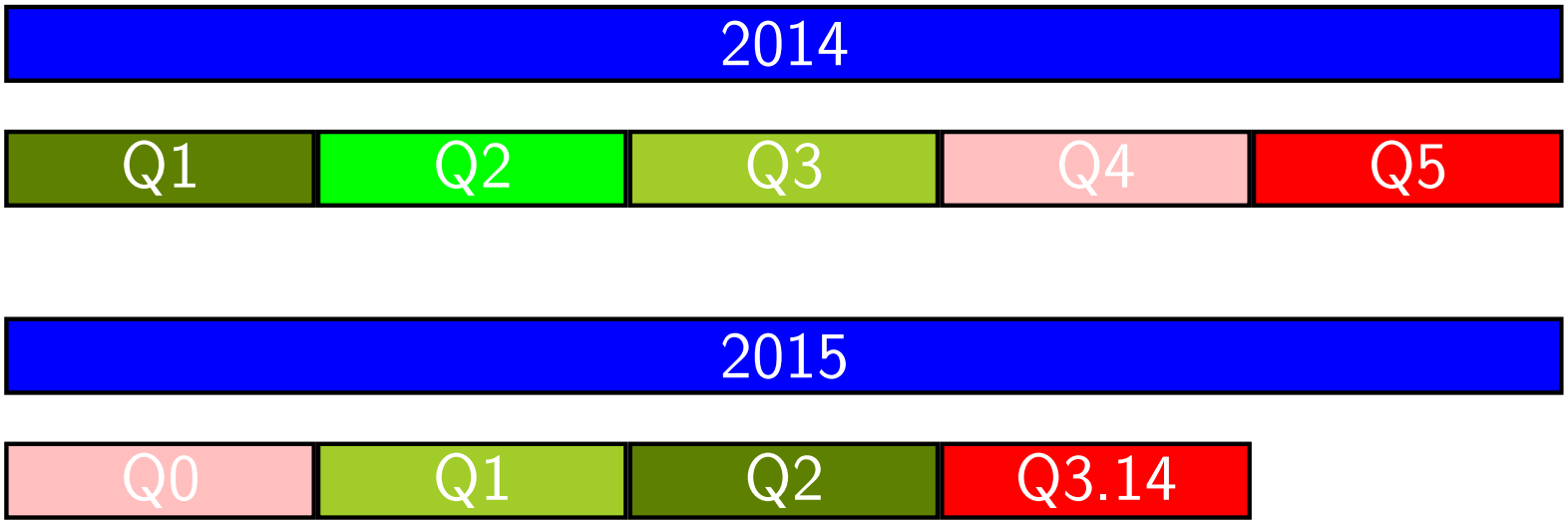
Timeline



Candidate workshop

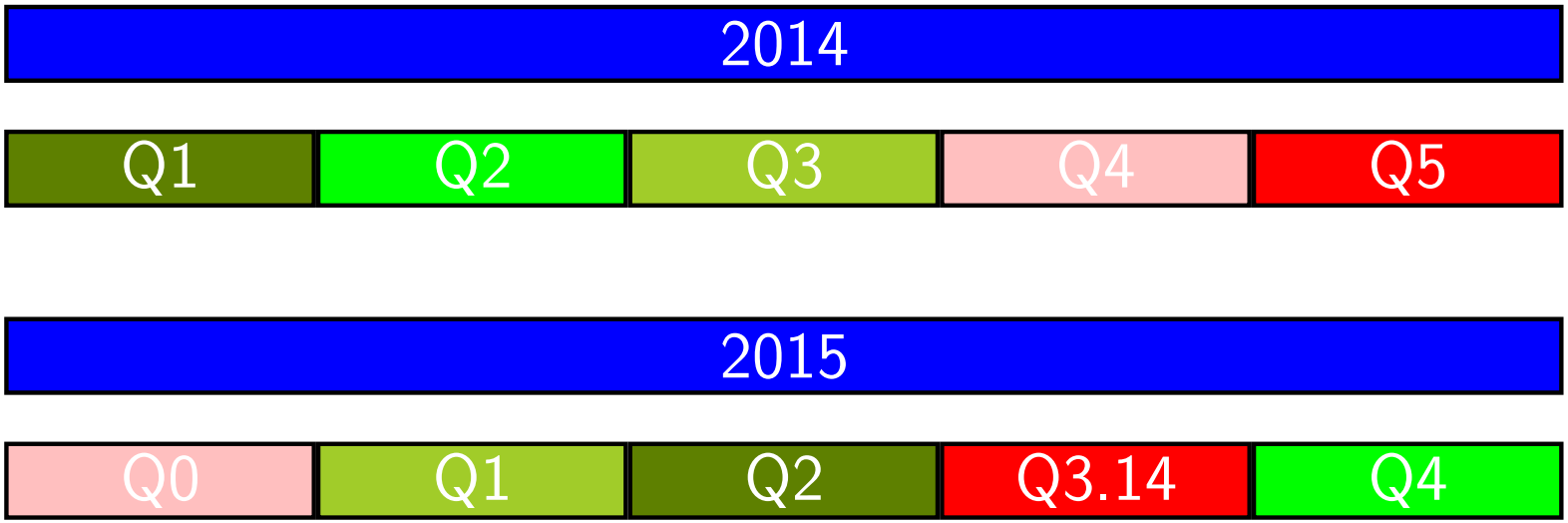
(collocation with Eurovision)

Timeline



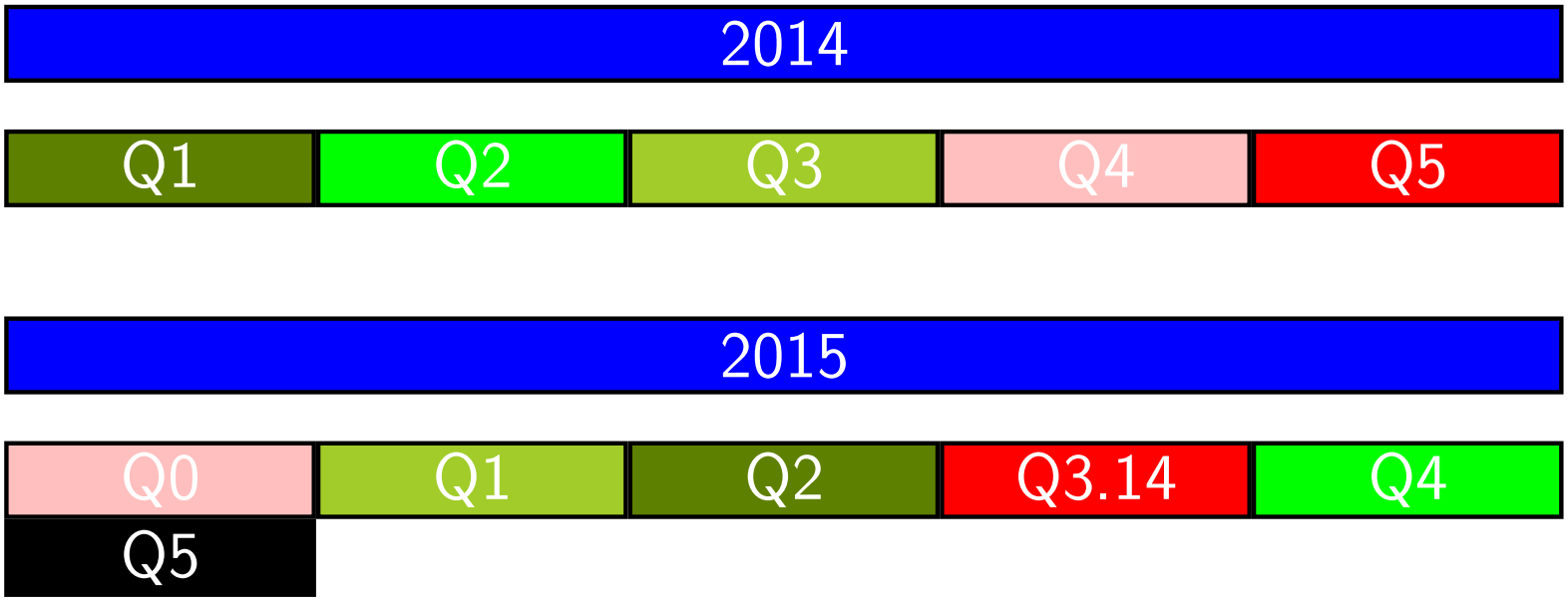
NSA comments
(private communication)

Timeline



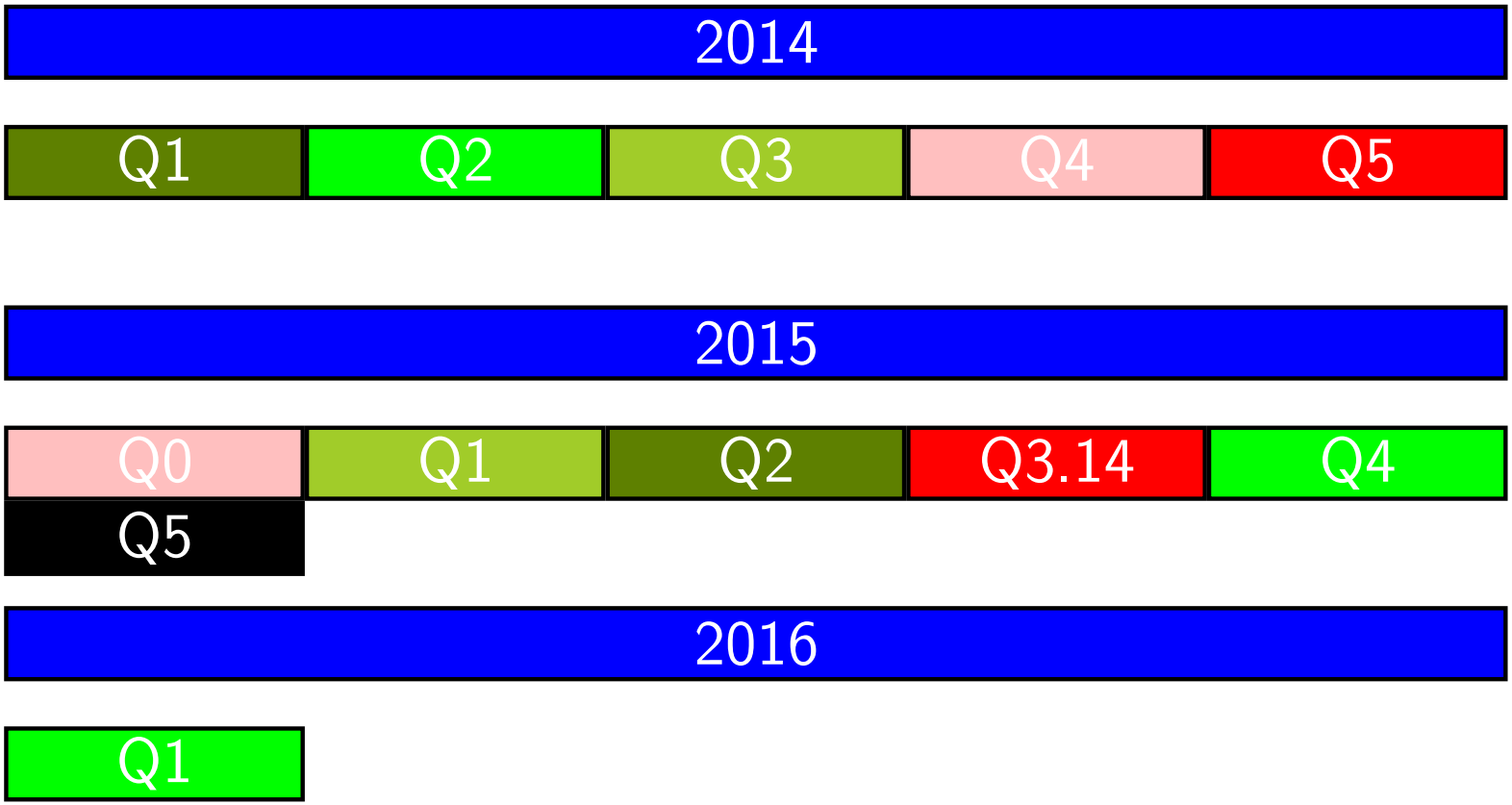
NSA comments (leaked)

Timeline



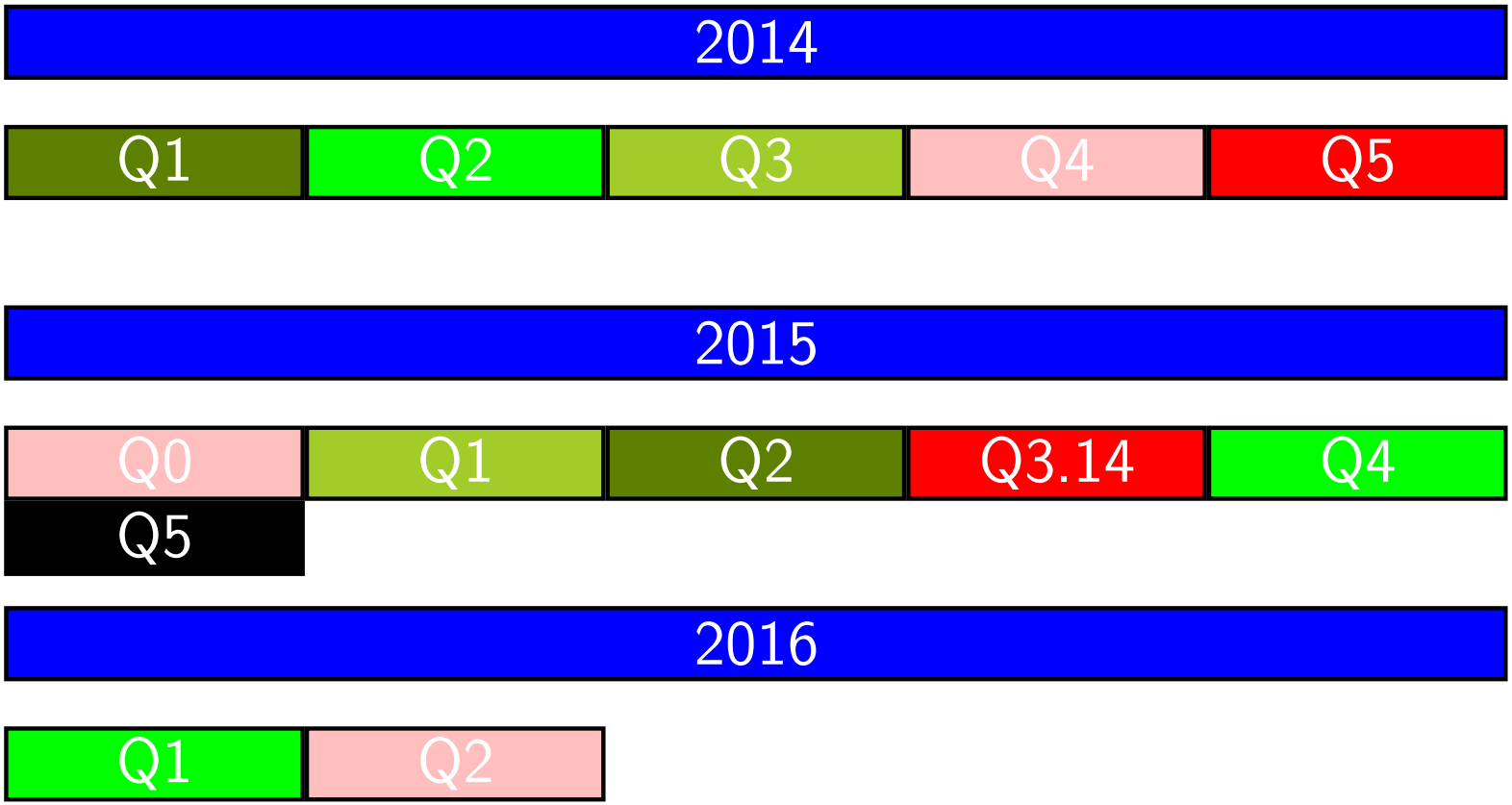
Winner selected!

Timeline



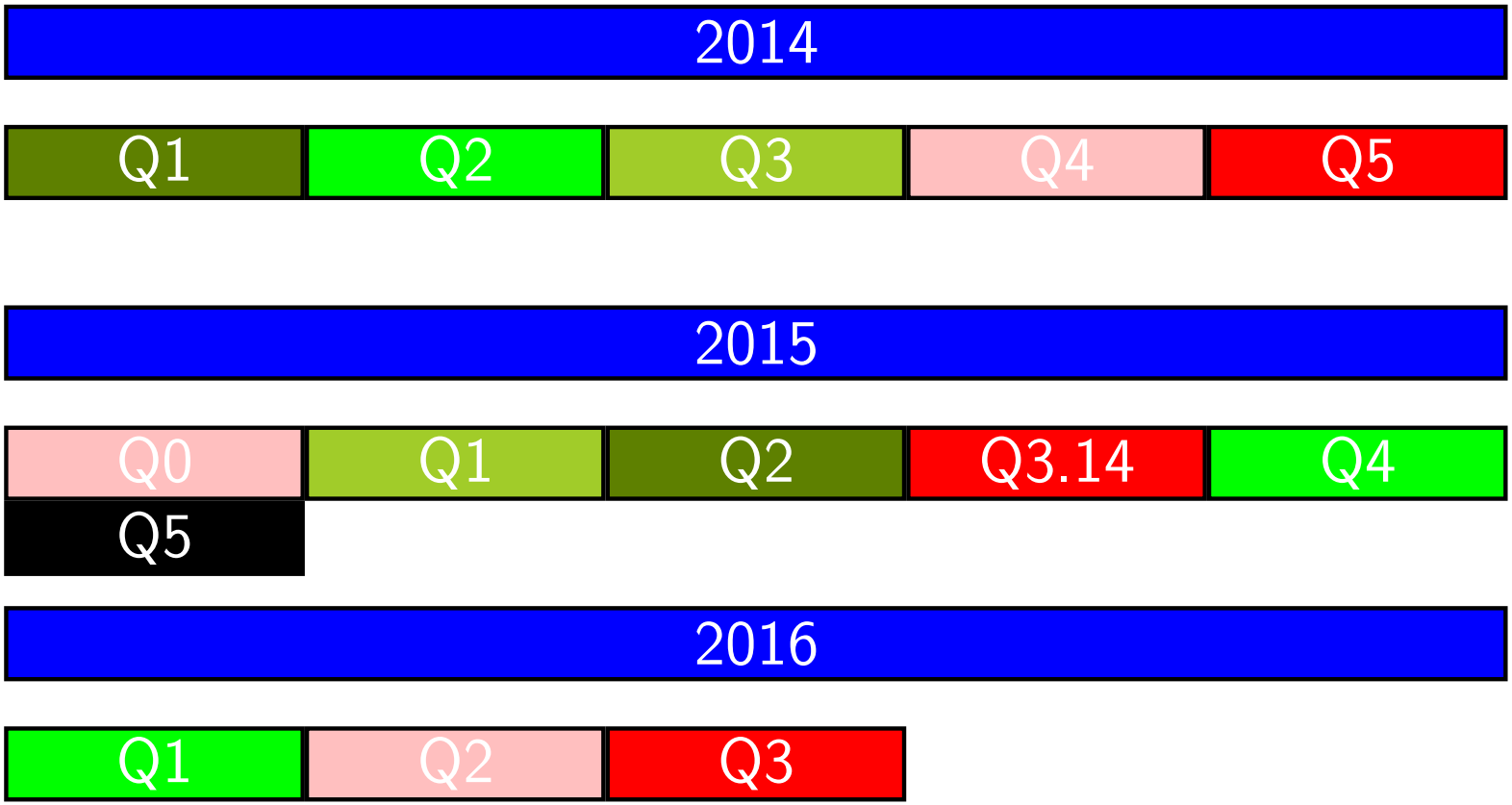
Altering winner's parameters

Timeline



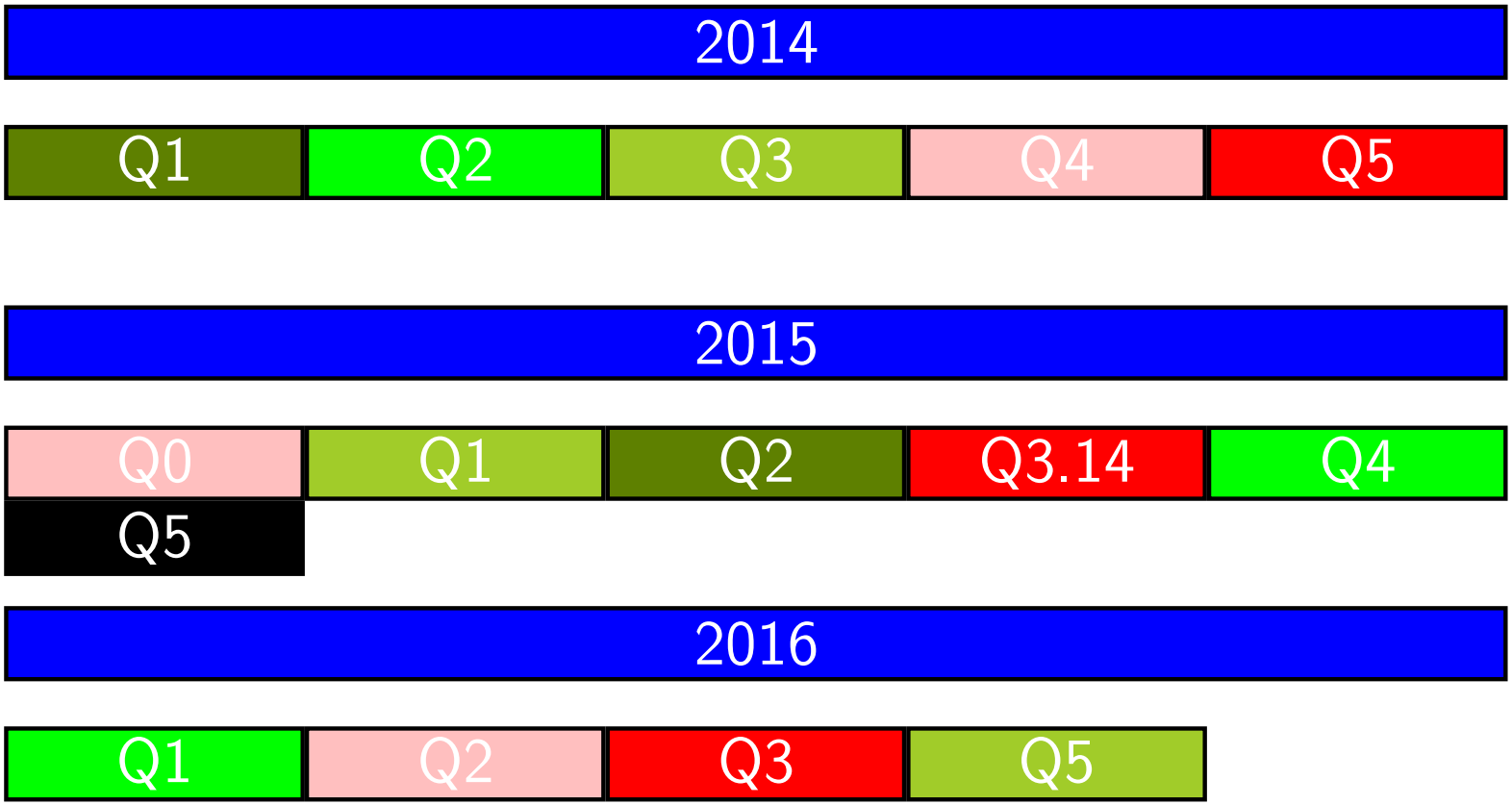
Altering winner's parameters to default ones

Timeline



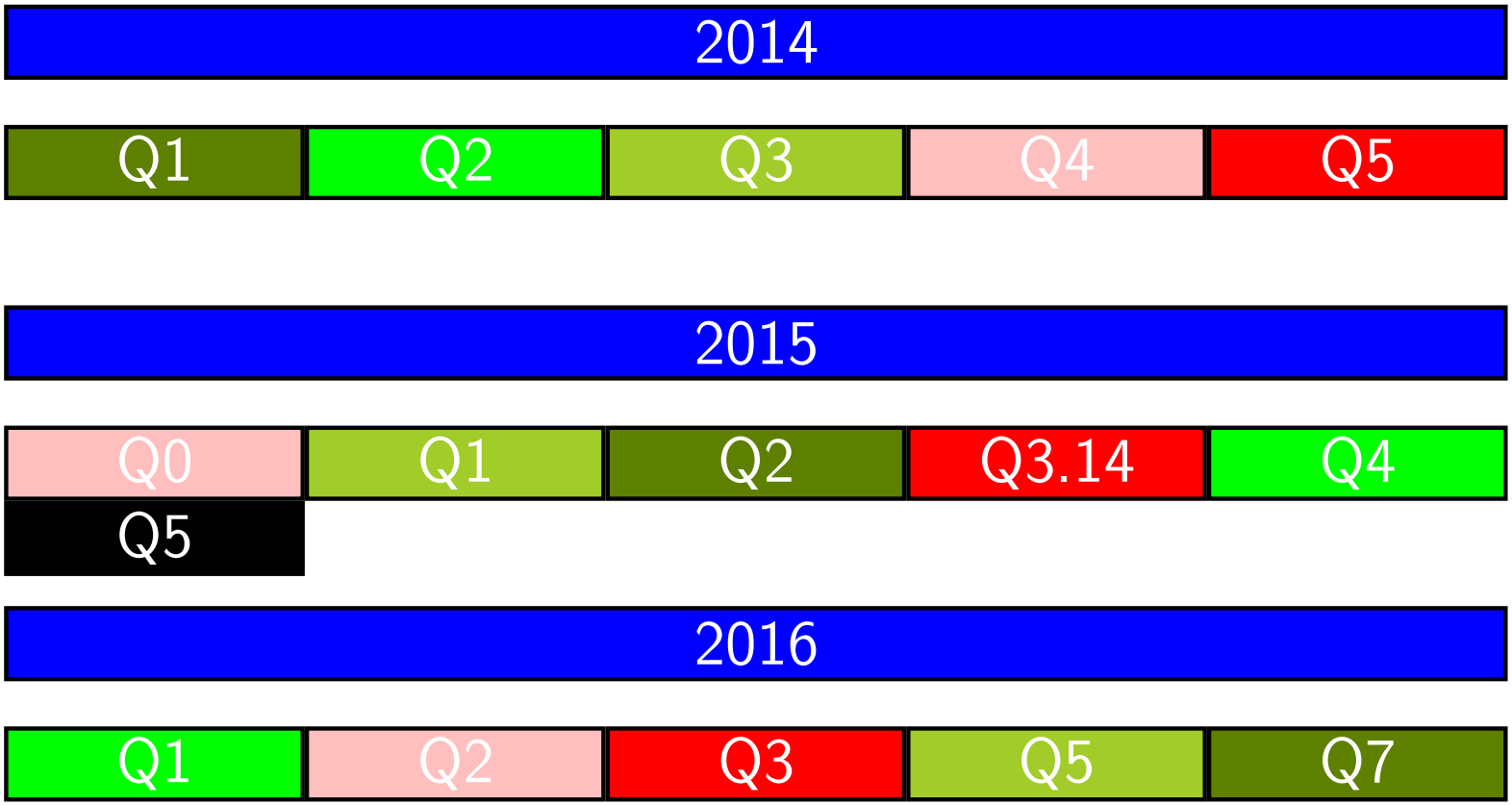
~~Altering winner's parameters to default ones~~

Timeline



Standard is out!

Timeline



Add missing $\lll 1$ to standard

More Information

For more information visit

snakeoil.cr.yp.to