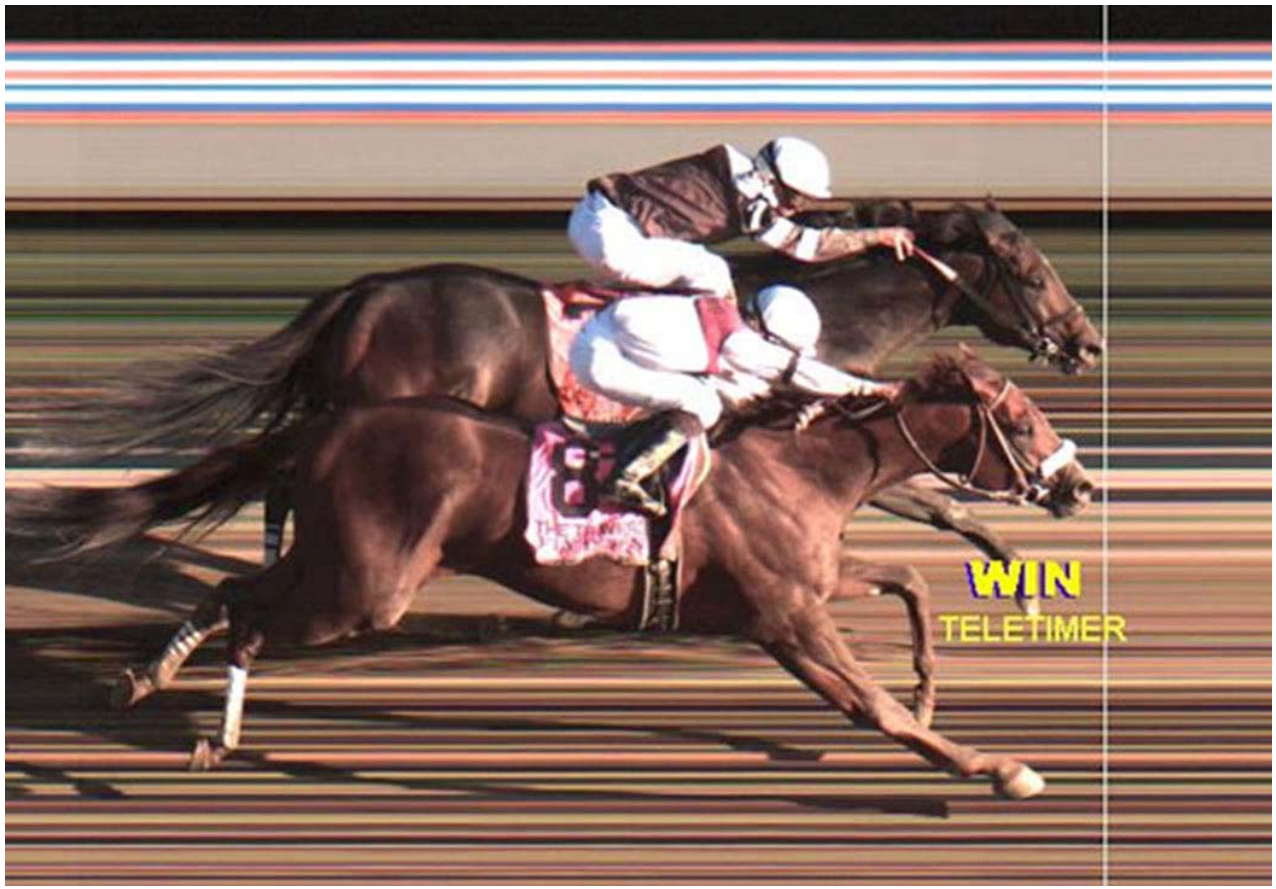
SHA-3 Update & NIST Thank You

Not the announcement

Bill Burr

Crypto 2012 Rump Session

Photo Finish



SHA-3: NIST appreciation

- Huge Crypto Community Contribution
- Far too many to name all in a rump session slot, if we even knew who they all were
  - 64 candidate submissions – every one a big effort
  - Many, many papers: cryptanalysis & implementation
  - Conferences and workshops
    - Participants and organizers

Our deepest appreciation to

The BLAKE Team

Jean-Philippe Aumasson
Luca Henzen
Willi Meier
Raphael C.-W. Phan

The Grøstl Team

Lars R. Knudsen
Praveen Gauravaram
Krystian Matusiewicz
Florian Mendel
Christian Rechberger
Martin Schläffer
Søren Steffen Thomsen

Our deepest appreciation to

The JH Designer

Hongjun Wu

The KECCAK Team

Guido Bertoni
Joan Daemen
Michaël Peeters
Gilles Van Assche

Our deepest appreciation to

The Skein Team

Niels Ferguson
Stefan Lucks
Bruce Schneier
Doug Whiting
Mihir Bellare
Tadayoshi Kohno
Jon Callas
Jesse Walker

Our deepest appreciation to

The KU Leuven COSIC Team

For help with the First SHA-3 Candidate Conference:

Bart Preneel

Sebastiaan Indesteege

The SHA-3 Zoo Team

Led by:

Christian Rechberger

Jean-Philippe Aumasson

Florian Mendel

Tomislav Nad

Martin Schläffer

Gilles Van Assche

Our deepest appreciation to

The Authors of the ECRYPT II SHA-3 Design and Cryptanalysis Report and the Intermediate Status Report

Christian Rechberger
Tor E. Bjørstad
Joan Daemen
Christophe De Cannière
Praveen Gauravaram
Dmitry Khovratovich
Willi Meier
Florian Mendel
Tomislav Nad
María Naya-Plasencia
Ivica Nikolić
Vincent Rijmen
Matt Robshaw
Martin Schläffer
Søren S. Thomsen
Elmar Tischhauser
Deniz Toz
Gilles Van Assche
Kerem Varici

Our deepest appreciation to

The eBASH Team

Led by:

Daniel J. Bernstein

Tanja Lange

The XBX Team

Led by:

Christian Wenzel-Benner

Jens Gräf

Our deepest appreciation to

The George Mason University ATHENa Team

Led by:

Kris Gaj

Jens-Peter Kaps

The Virginia Tech ECE Team

Led by:

Patrick Schaumont

Leyla Nazhand-Ali

The Eidgenössische Technische Hochschule Zürich (ETHZ) Team

Led by:

Frank K. Gürkaynak

Thank You All!

Many thanks to all of you who contributed in so many ways to the SHA-3 competition.