Rump Session 2019

# The Fellowship of the Rump
# Crypto'19

A Celebration

Get ready: Sasha Boldyreva and Daniele Micciancio

Rump Session 2019



# Opening

Martijn Stam

Simula UiB

Get ready: Muthuramakrishnan Venkitasubramaniam

Helger says hello!

Rump Session 2019



# Borg Early Career Award (BECA)

Nadia Heninger (recipient of the award)

University of California, San Diego

Get ready: Douglas Stebila

Rump Session 2019



# Cards Against Cryptography

Anonymous

Anonymous

Get ready: Dankrad Feist

Rump Session 2019



# Cryptanalyzing the Legendre PRF

Dankrad Feist

Ethereum Foundation

Get ready: Greg Rose

Rump Session 2019



# Trivial Real World Crypto

Greg Rose

Deckard Technologies, Inc.

Get ready: Christian Cachin

Rump Session 2019



# The Grand Unified Theory of Cryptology

Christian Cachin

University of Bern

Get ready: Chris Peikert

Rump Session 2019



# He Gives C-Sieves on the CSIDH

Chris Peikert

University of Michigan

Get ready: Daniel Wichs

# Rump Session 2019



## New Conference on Information-Theoretic Cryptography

## (ITC)

Benny Applebaum, Ivan Damgård, Yevgeniy Dodis, Yuval Ishai, Ueli Maurer, Kobbi Nissim, Krzysztof Pietrzak, Manoj Prabhakaran, Adam Smith, Yael Kalai, Stefano Tessaro, Vinod Vaikuntanathan, Hoeteck Wee, Daniel Wichs, Mary Wootters, Chaoping Xing, Moti Yung

Rump Session 2019

# **Adjourment** of the 2019 Fellowship of the Rump

We reconvene: 20:45

Rump Session 2019

# **Adjourment** of the 2019 Fellowship of the Rump

We continue: now

Get ready: Edoardo Persichetti

Rump Session 2019



# PQC Wiki

Edoardo Persichetti

FAU

Get ready: Nicolas Sendrier

Rump Session 2019



# decodingchallenge.org

Julien Lavauzelle, Matthieu Lequesne, Nicolas Aragon

Université de Rennes 1, Sorbonne Université and Inria, Université de Limoges

Get ready: Michael Riabzev

Rump Session 2019



# STARK friendly hash challenge

Tomer Ashur, Eli Ben-Sasson, Lior Goldberg, Michael Riabzev

KU Leuven, StarkWare Industries

Get ready: Saravanan Musuwathi Kesavan

Rump Session 2019



# DH(E) and the leading zeros in the premaster secret in TLS 1.1/1.2

Saravanan Musuwathi Kesavan

F5 Networks

Get ready: Nadia Heninger

# Rump Session 2019



# 48ce563f89a0ed9414f5aa28ad0d96d6

Nadia Heninger, Travis Scholl, Dan Shumow

UC San Diego, UC Irvine, Microsoft Research

Get ready: Yongha Son

Rump Session 2019



# On parameter choices of Round5

Yongha Son

Seoul National University

Get ready: Mehdi Tibouchi

Rump Session 2019



# You are strong, FALCON,

## but we will break you!

Pierre-Alain Fouque, Paul Kirchner, Mehdi Tibouchi, Alexandre Wallet, Yang Yu

Univ Rennes and NTT Corporation

Get ready: Yevgeniy Dodis

Rump Session 2019



# Implementing Signal

Yi Tang, Yevgeniy Dodis

New York University

Get ready: Josh Benaloh

Rump Session 2019



# Microsoft's ElectionGuard

Josh Benaloh

Microsoft Research

Get ready: Dan Shumow

Rump Session 2019



# RSA Encraption

Dan Shumow, Brian LaMacchia

Microsoft Research

Get ready: Kelly Olson

Rump Session 2019



# Bringing Verifiable Delay Functions Into Production

Kelly Olson

Supranational, VDF Research

Get ready: Vassilis Zikas

Rump Session 2019



# OPA!!!

Muhammad Ishaq, Ana Milanova, Vassilis Zikas

University of Edinburgh, RPI

Get ready: Vassilis Zikas

Rump Session 2019



# PKC 2020 in Edinburgh

Vassilis Zikas

PKC General co-Chair

Rump Session 2019

# **Adjourment** of the 2019 Fellowship of the Rump

We reconvene: 22:00

Rump Session 2019

# **Adjourment** of the 2019 Fellowship of the Rump

We continue: now

Get ready: John Kelsey

Rump Session 2019



# NIST Update

John Kelsey, Luis Brandao, Meltem Sonmez Turan, Lily Chen, Dustin Moody, Elaine Barker

NIST

Get ready: Hilarie Orman

Rump Session 2019



# Key Words

Hilarie Orman

Purple Streak

Get ready: Chris Peikert

Rump Session 2019



# Algebraically Structured LWE, Revisited

Chris Peikert, Zachary Pepin

University of Michigan

Get ready: Erica Blum

Rump Session 2019




Synchronous Consensus with Optimal Asynchronous Fallback: The

# Crypto Chickens Go to the Beach

Erica Blum, Jonathan Katz, Julian Loss

University of Maryland College Park, University of Maryland College Park, Ruhr-Universität Bochum

Get ready: Christian Cachin

Rump Session 2019



# Asymmetric distributed trust

Christian Cachin, Björn Tackmann

University of Bern, IBM - Research

Get ready: Yun Lu

Rump Session 2019



# Collusion-Preserving Computation without a Mediator

Michele Ciampi, Yun Lu, Vassilis Zikas

University of Edinburgh

Get ready: Nikolaos Makriyannis

Rump Session 2019



# On the Round Complexity of Randomized Byzantine Agreement

Ran Cohen, Iftach Haitner, Nikolaos Makriyannis, Matan Orland, Alex Samorodnitsky

Northeastern, TAU, Technion, HUJI

Get ready: Joshua Baron

Rump Session 2019



# DARPA Cryptographic Research

Joshua Baron

DARPA

Get ready: Valeria Nikolaenko

Rump Session 2019



# Winkle: Protecting Proof-of-Stake Blockchains From Long-Range Attacks

Sarah Azouvi, George Danezis, Valeria Nikolaenko

Calibra-Facebook

Get ready: Olivier Blazy

Rump Session 2019



# A new Paradigm Shift for the Crypto BlockChain: Proof of Ability

Olivier Blazy, Orr Dunkelman

Université de Limoges, Haifa University

Get ready: Valeriya Idrisova

Rump Session 2019



# International Olympiad in Cryptography NSUCRYPTO

Valeriya Idrisova, Natalia Tokareva, Anastasiya Gorodilova et al.

Sobolev Institute of Mathematics, Novosibirsk State University

Get ready: Bram Cohen

Rump Session 2019



# The Chia Proof of Space construction and implementation competition

Bram Cohen

Chia Network

Rump Session 2019

# Disbandment of the 2019 Fellowship of the Rump