RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: **ACB-T11**

Cryptographic Agility: Anticipating, Preparing for and Executing Change

MODERATOR: **Dr. Lily Chen**
Manager of Cryptographic Technology Group
Computer Security Division
Information Technology Lab, NIST

PANELISTS:

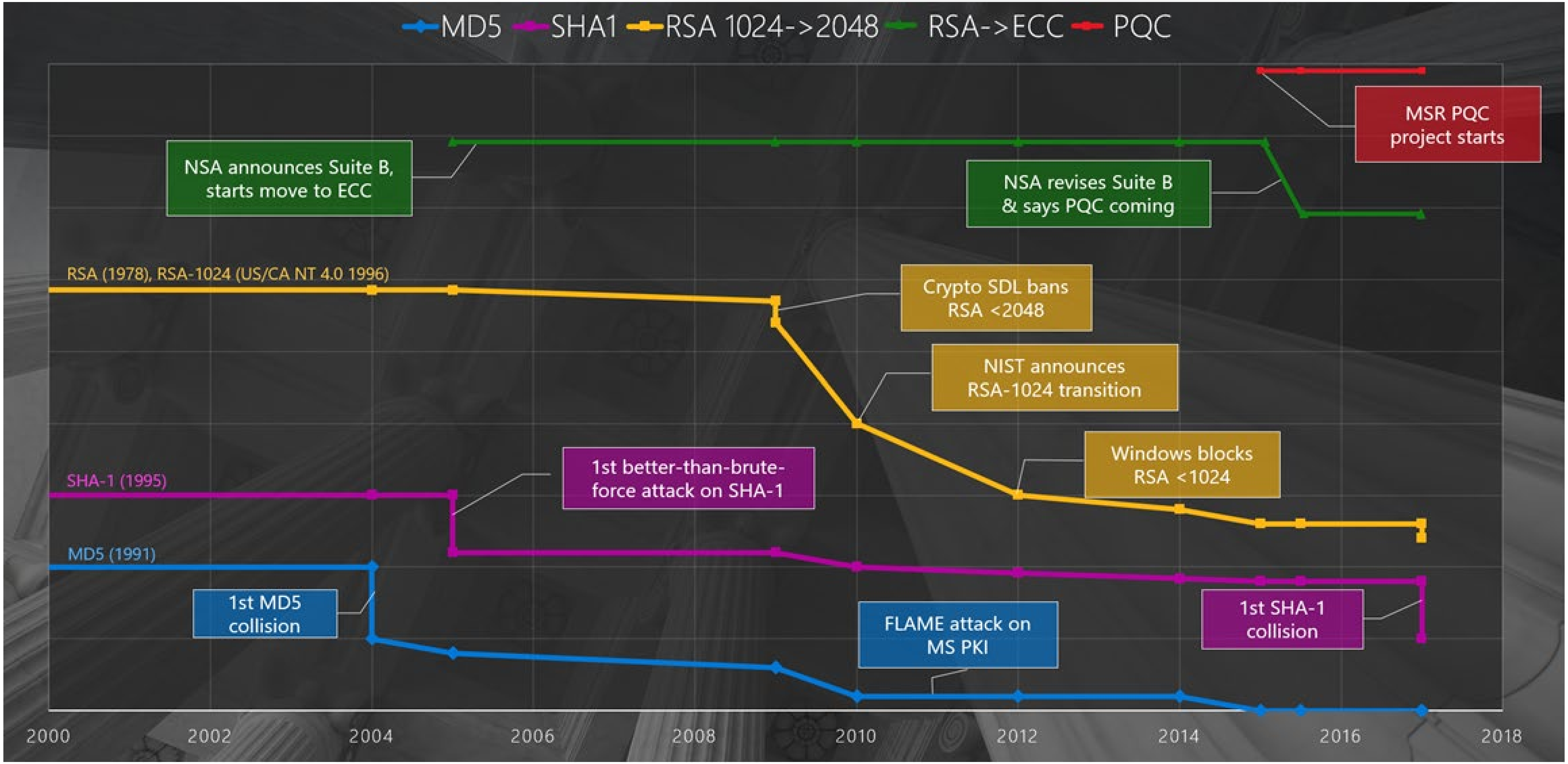
Dr. David Ott
Senior Staff Researcher and
Academic Program Director
VMware Research

Dr. Zulfikar Ramzan
Chief Technology Officer
RSA

Dr. Brian LaMacchia
Distinguished Engineer
Microsoft

#RSAC

Cryptography *Lifetime*: Algorithm Strength Over Time



NSA announces Suite B, starts move to ECC

MSR PQC project starts

NSA revises Suite B & says PQC coming

Crypto SDL bans RSA <2048

NIST announces RSA-1024 transition

Windows blocks RSA <1024

1st better-than-brute-force attack on SHA-1

1st MD5 collision

FLAME attack on MS PKI

1st SHA-1 collision

Cryptographic Agility: Addressing Change

Technology advancements and more sophisticated cryptanalysis empower attackers and increase threat levels

- Ex: Improvements in hash collision finding, future quantum computers

Cryptography needs to change over time

- Algorithms become deprecated and need removal
- New primitives and algorithms are introduced
- Larger key/signature/ciphertext sizes are needed
- Alternative parameter sets are introduced

Cryptographic Agility: a capability allowing us to make smooth transitions between algorithms and configurations

Cryptographic Agility: Discussion Topics

1. In the applications, products, or services your organization deploys, produces or provides, what does crypto agility mean and how has it been handled?
2. What have we learned from cryptography transitions in the past, and how might this motivate improvements?
3. What are the major challenges in dealing with transitions, for example, from the current adopted cryptosystems to new quantum-resistant algorithms? Possible technical paths for transition?
4. What strategies which you think might improve cryptographic agility?

Cryptographic Agility: What Can You Do Today

Build and maintain an inventory of current uses of cryptography in your systems and applications.

- Include algorithms, parameters, key sizes, protocols, etc.

Test transition ahead of time.

- For PQC, you can use Open Quantum Safe (OQS, https://openquantumsafe.org/) implementations to test candidate algorithms and PQC-enabled protocols.

Ask your suppliers for details on how they provide cryptographic agility in their systems and services.

Participate in industry forums discussing cryptography transition and the frameworks that will enable it.

- E.g., NIST PQC, IETF work on TLS hybrids