



# ***Applications of Trusted Computing***

Rick Wash

`rwash@citi.umich.edu`

CITI - University of Michigan

# ***TCPA Functions***

- ⑥ Public Key Functions
  - △ Key Generation
  - △ Signature
  - △ Encryption / Decryption
- ⑥ Trusted Boot
- ⑥ Initialization and Management

# TCPA Chip

Functional Units	Non-volatile Memory	Volatile Memory
<p>RNG</p>	<p>Endorsement Key (2048b)</p>	<p>RSA Key Slot 0</p> <p>● ● ●</p>
<p>Hash</p>	<p>Storage Root Key (2048b)</p>	<p>RSA Key Slot 9</p>
<p>HMAC</p>	<p>Owner Auth Secret (160b)</p>	<p>PCR-0</p> <p>● ● ●</p>
<p>RSA Key Generation</p>		<p>PCR-14</p>
<p>RSA Encrypt / Decrypt</p>		<p>Key Handles</p>
		<p>Auth Session Handles</p>