

POST-QUANTUM CRYPTOGRAPHY FOR SMALL DEVICES

Christine Cloostermans¹
NOVEMBER 2022



SECURE CONNECTIONS
FOR A SMARTER WORLD

PUBLIC

NXP, THE NXP LOGO AND NXP SECURE CONNECTIONS FOR A SMARTER WORLD ARE TRADEMARKS OF NXP B.V.
ALL OTHER PRODUCT OR SERVICE NAMES ARE THE PROPERTY OF THEIR RESPECTIVE OWNERS. © 2021 NXP B.V.

¹Mostly publishing as Christine van Vredendaal





HOW TO PREPARE FOR HURRICANE SEASON Quantum



MAKE A PLAN

Airmen should create an emergency plan and/or checklist

- obtain supplies
- update personal documents
- secure household
- research evacuation options/routes
- update prescriptions



CREATE A GO-BAG

Prepare supplies ahead of a hurricane. These can include

- Food/water
- Additional clothes
- Personal documents
- Travel supplies
- Prescriptions



KNOW YOUR WING GUIDANCE

Whether preparing for a hurricane or evacuating know your wing or installation's guidance. Routinely check for updates from leadership and maintain communication with your chain of command.



RECOGNIZE WARNINGS & ALERTS

Have several ways to receive alerts. Download real-time alert apps. Sign up for community alerts in your area and be aware of the Emergency Alert System (EAS) and Wireless Emergency Alert (WEA)- which requires no-sign up.



STAY SAFE

Practice good hygiene and safety measures during any part of a hurricane evacuation or impact. Keep family considerations in mind and don't be afraid to contact leadership for guidance.

OUTLINE

- What is a smartcard?
- Why is resource constrained PQC hard?
 - Migration is hard
 - PQC is big
 - Protected PQC is bigger
 - There is not just 1 PQC
- Final thoughts



HOW TO PREPARE FOR HURRICANE SEASON Quantum



MAKE A PLAN

Airmen should create an emergency plan and/or checklist

- obtain supplies
- update personal documents
- secure household
- research evacuation options/routes
- update prescriptions



CREATE A GO-BAG

Prepare supplies ahead of a hurricane. These can include

- Food/water
- Additional clothes
- Personal documents
- Travel supplies
- Prescriptions



KNOW YOUR WING GUIDANCE

Whether preparing for a hurricane or evacuating know your wing or installation's guidance. Routinely check for updates from leadership and maintain communication with your chain of command.



RECOGNIZE WARNINGS & ALERTS

Have several ways to receive alerts. Download real-time alert apps. Sign up for community alerts in your area and be aware of the Emergency Alert System (EAS) and Wireless Emergency Alert (WEA)- which requires no-sign up.



STAY SAFE

Practice good hygiene and safety measures during any part of a hurricane evacuation or impact. Keep family considerations in mind and don't be afraid to contact leadership for guidance.

OUTLINE

- **What is a smartcard?**
- **Why is resource constrained PQC hard?**
 - Migration is hard
 - PQC is big
 - Protected PQC is bigger
 - There is not just 1 PQC
- **Final thoughts**

SECURE MICROPROCESSORS – WHY DO THEY EXIST?

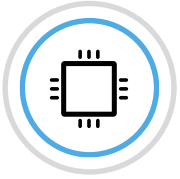
*“For some applications, national law, corporate agreements or international standards require **secure computing functions** to be **highly portable**”*

General-purpose microprocessors generally

- Do not perform modern cryptographic algorithms very well
- Are terrible at keeping their secrets to themselves during computation
- Are **unable to effectively protect stored secret data**



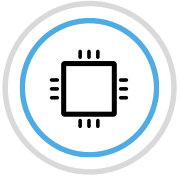
WHAT IS A SECURE MICROPROCESSOR ANYWAY?



General chip design constraints

- Functional correctness
- Power supply
- Environmental conditions
- (not a complete list, but *nearly*)

WHAT IS A SECURE MICROPROCESSOR ANYWAY?



General chip design constraints

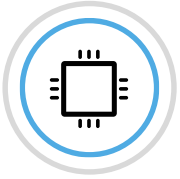
- Functional correctness
- Power supply
- Environmental conditions
- (not a complete list, but *nearly*)



Design constraints of a security μ C

- **Everything from 'general...', plus**

WHAT IS A SECURE MICROPROCESSOR ANYWAY?



General chip design constraints

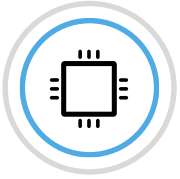
- Functional correctness
- Power supply
- Environmental conditions
- (not a complete list, but *nearly*)



Design constraints of a security μ C

- **Everything from 'general...', plus**
- Passive security

WHAT IS A SECURE MICROPROCESSOR ANYWAY?



General chip design constraints

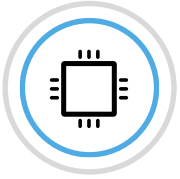
- Functional correctness
- Power supply
- Environmental conditions
- (not a complete list, but *nearly*)



Design constraints of a security μ C

- **Everything from 'general...', plus**
- Passive security
- Security against environmental attacks

WHAT IS A SECURE MICROPROCESSOR ANYWAY?



General chip design constraints

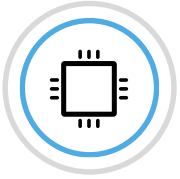
- Functional correctness
- Power supply
- Environmental conditions
- (not a complete list, but *nearly*)



Design constraints of a security μ C

- **Everything from 'general...', plus**
- Passive security
- Security against environmental attacks
- Security against intrusion

WHAT IS A SECURE MICROPROCESSOR ANYWAY?



General chip design constraints

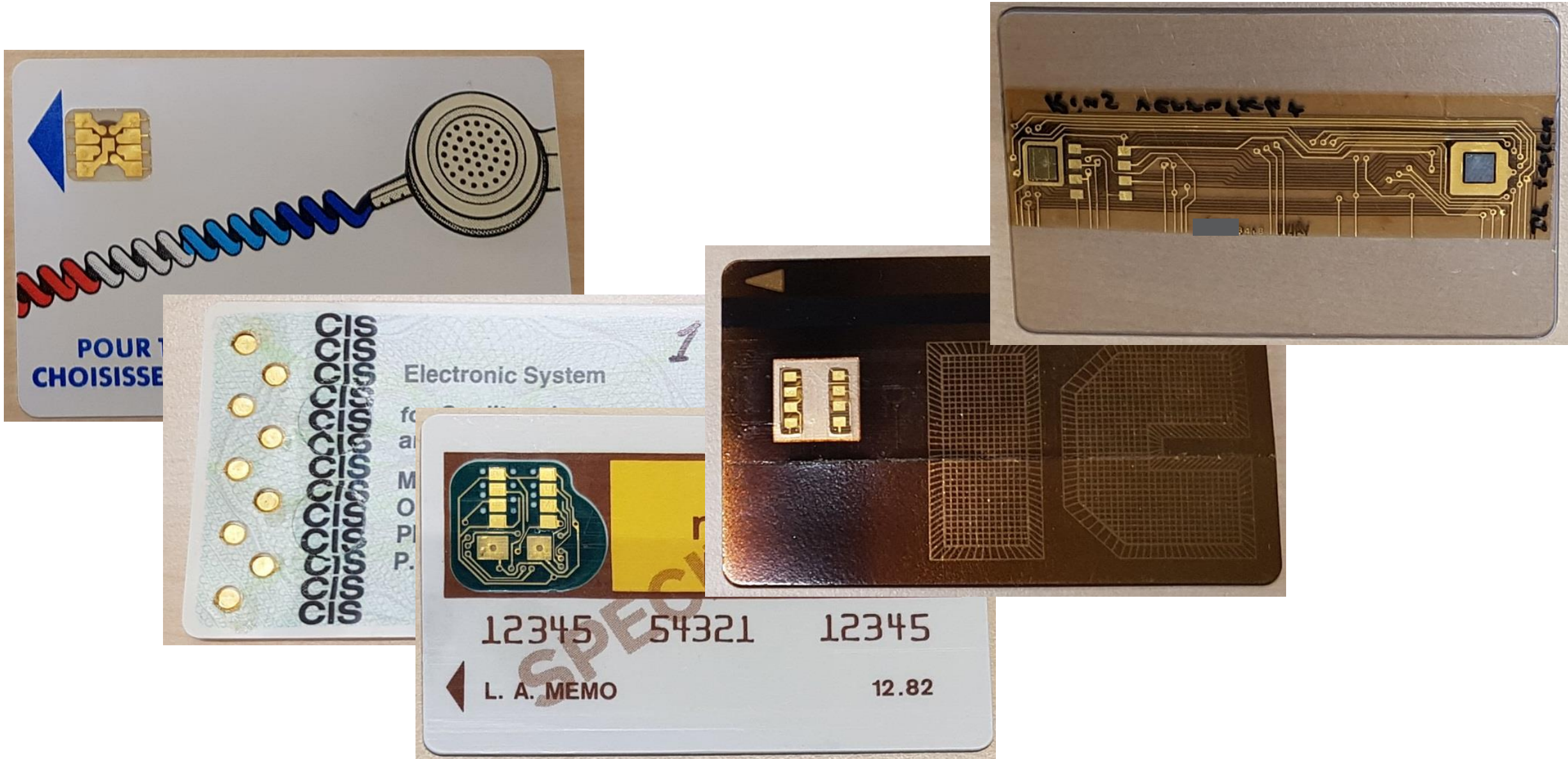
- Functional correctness
- Power supply
- Environmental conditions
- (not a complete list, but *nearly*)



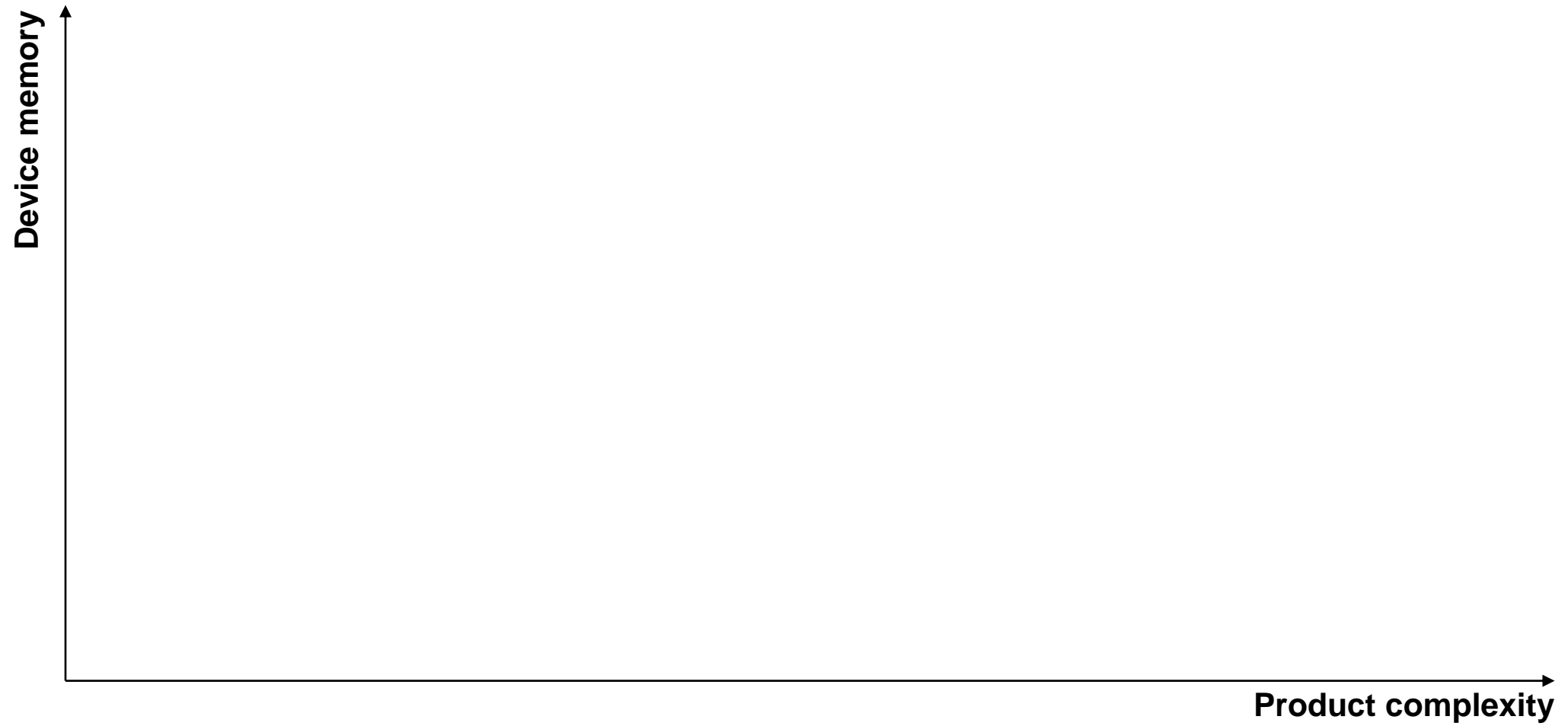
Design constraints of a security μ C

- **Everything from 'general...', plus**
- Passive security
- Security against environmental attacks
- Security against intrusion
- (not a complete list *at all*)

HISTORICAL EXAMPLES: EARLY 80s



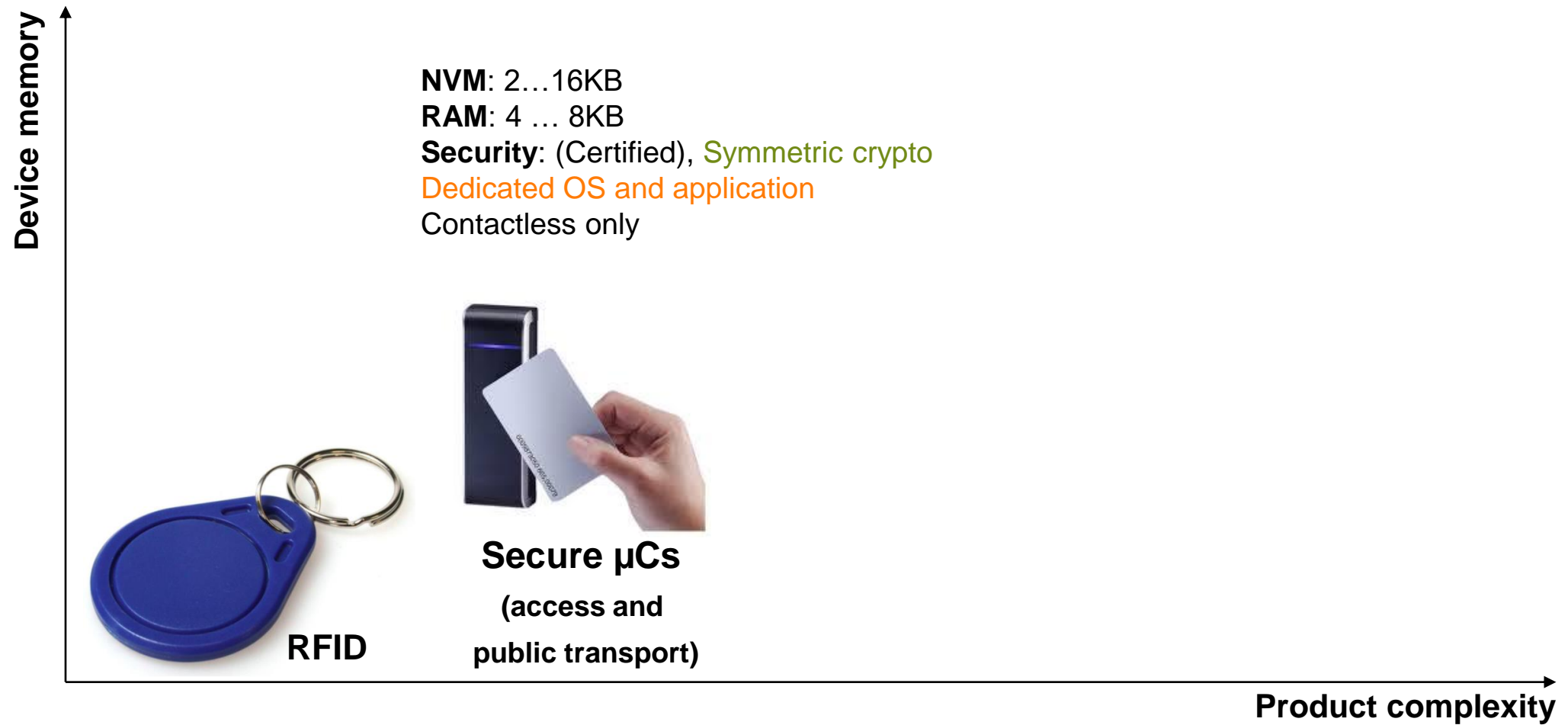
NOWADAYS



NOWADAYS



NOWADAYS



NOWADAYS

NVM: 40...256KB

RAM: 4 ... 16KB

Security: Certified, All crypto
Complex OS and applications
Contact, contactless

Device memory



RFID



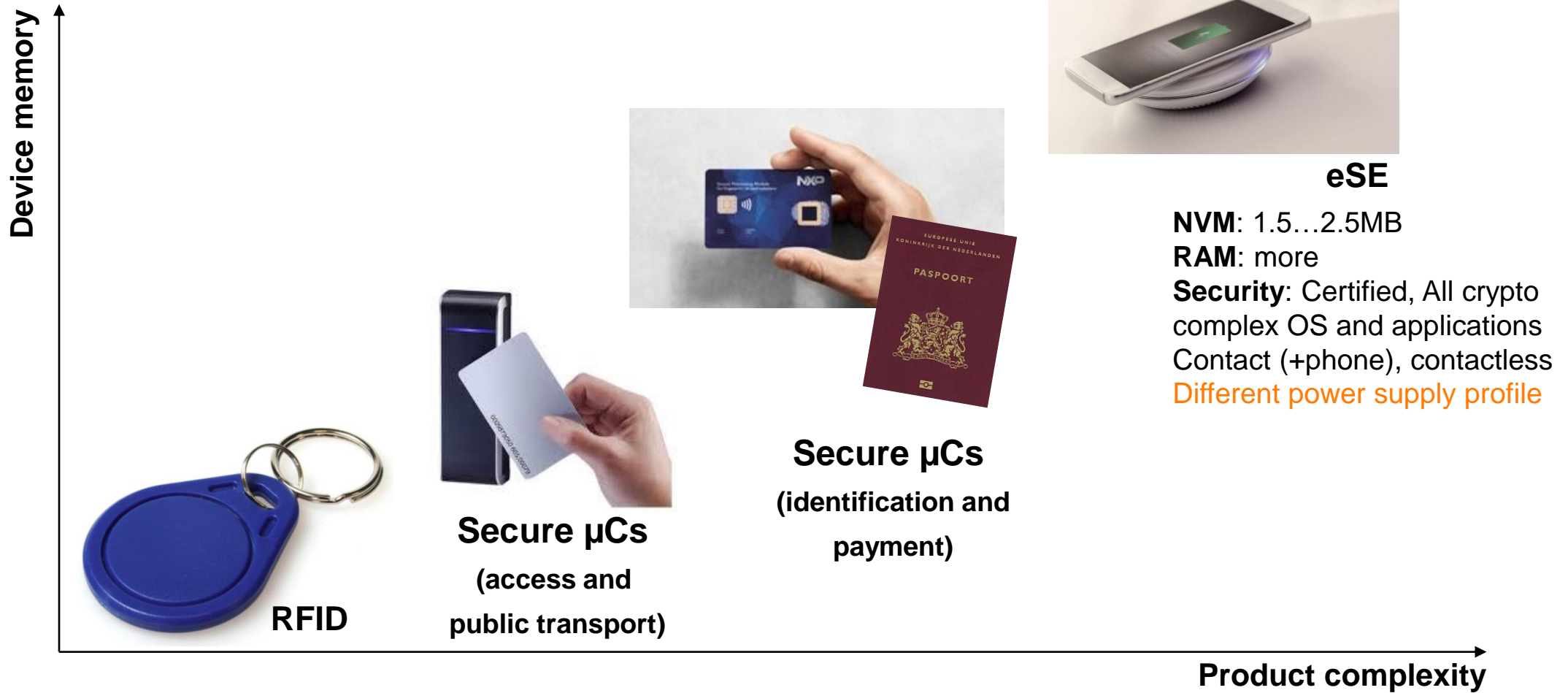
Secure μ Cs
(access and
public transport)



Secure μ Cs
(identification and
payment)

Product complexity

NOWADAYS





HOW TO PREPARE FOR HURRICANE SEASON Quantum



MAKE A PLAN

Airmen should create an emergency plan and/or checklist

- obtain supplies
- update personal documents
- secure household
- research evacuation options/routes
- update prescriptions



CREATE A GO-BAG

Prepare supplies ahead of a hurricane. These can include

- Food/water
- Additional clothes
- Personal documents
- Travel supplies
- Prescriptions



KNOW YOUR WING GUIDANCE

Whether preparing for a hurricane or evacuating know your wing or installation's guidance. Routinely check for updates from leadership and maintain communication with your chain of command.



RECOGNIZE WARNINGS & ALERTS

Have several ways to receive alerts. Download real-time alert apps. Sign up for community alerts in your area and be aware of the Emergency Alert System (EAS) and Wireless Emergency Alert (WEA)- which requires no-sign up.



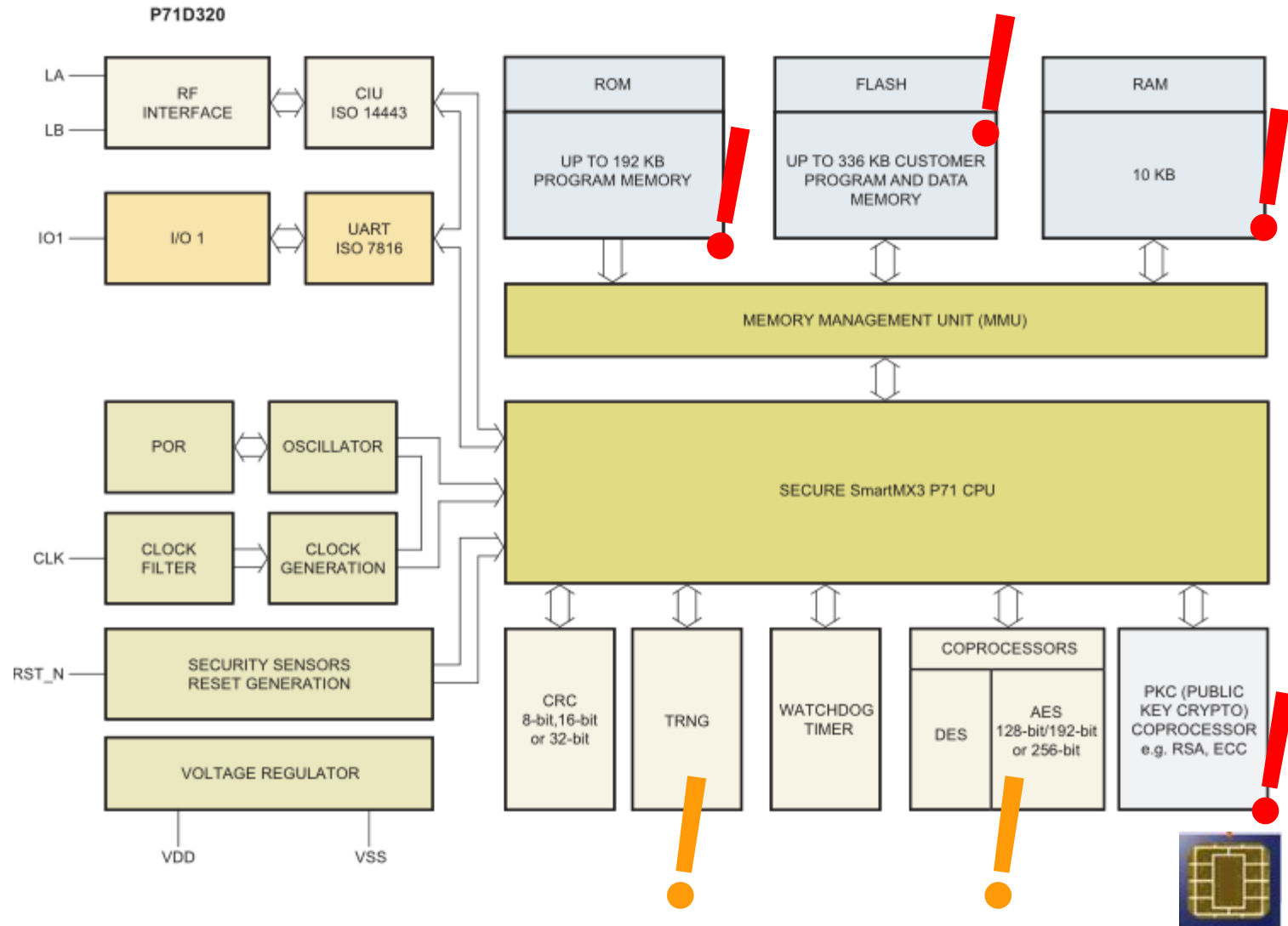
STAY SAFE

Practice good hygiene and safety measures during any part of a hurricane evacuation or impact. Keep family considerations in mind and don't be afraid to contact leadership for guidance.

OUTLINE

- What is a smartcard?
- **Why is resource constrained PQC hard?**
 - Migration is hard
 - PQC is big
 - Protected PQC is bigger
 - There is not just 1 PQC
- Final thoughts

SECURE MICROPROCESSOR, EXAMPLE BLOCK DIAGRAMS





HOW TO PREPARE FOR HURRICANE SEASON Quantum



MAKE A PLAN

Airmen should create an emergency plan and/or checklist

- obtain supplies
- update personal documents
- secure household
- research evacuation options/routes
- update prescriptions



CREATE A GO-BAG

Prepare supplies ahead of a hurricane. These can include

- Food/water
- Additional clothes
- Personal documents
- Travel supplies
- Prescriptions



KNOW YOUR WING GUIDANCE

Whether preparing for a hurricane or evacuating know your wing or installation's guidance. Routinely check for updates from leadership and maintain communication with your chain of command.



RECOGNIZE WARNINGS & ALERTS

Have several ways to receive alerts. Download real-time alert apps. Sign up for community alerts in your area and be aware of the Emergency Alert System (EAS) and Wireless Emergency Alert (WEA)- which requires no-sign up.



STAY SAFE

Practice good hygiene and safety measures during any part of a hurricane evacuation or impact. Keep family considerations in mind and don't be afraid to contact leadership for guidance.

OUTLINE

- What is a smartcard?
- **Why is resource constrained PQC hard?**
 - **Migration is hard**
 - PQC is big
 - Protected PQC is bigger
 - There is not just 1 PQC
- Final thoughts



MIGRATION OF HARDWARE

Same product different lifetimes

One product might never migrate → does not want to pay (money, performance) for extra functionality



MIGRATION OF HARDWARE

Same product different lifetimes

One product might never migrate → does not want to pay (money, performance) for extra functionality

Secure HW design can take a long time

Replacing the PKC block → many years of research

Adding the PKC block → extra space

Hybrid modes are not that clear



MIGRATION OF HARDWARE

Same product different lifetimes

One product might never migrate → does not want to pay (money, performance) for extra functionality

Secure HW design can take a long time

Replacing the PKC block → many years of research

Adding the PKC block → extra space

Hybrid modes are not that clear

HW has to be replaced physically

Maintaining interoperability is often vital



HOW TO PREPARE FOR HURRICANE SEASON Quantum



MAKE A PLAN

Airmen should create an emergency plan and/or checklist

- obtain supplies
- update personal documents
- secure household
- research evacuation options/routes
- update prescriptions



CREATE A GO-BAG

Prepare supplies ahead of a hurricane. These can include

- Food/water
- Additional clothes
- Personal documents
- Travel supplies
- Prescriptions



KNOW YOUR WING GUIDANCE

Whether preparing for a hurricane or evacuating know your wing or installation's guidance. Routinely check for updates from leadership and maintain communication with your chain of command.



RECOGNIZE WARNINGS & ALERTS

Have several ways to receive alerts. Download real-time alert apps. Sign up for community alerts in your area and be aware of the Emergency Alert System (EAS) and Wireless Emergency Alert (WEA)- which requires no-sign up.



STAY SAFE

Practice good hygiene and safety measures during any part of a hurricane evacuation or impact. Keep family considerations in mind and don't be afraid to contact leadership for guidance.

OUTLINE

- What is a smartcard?
- **Why is resource constrained PQC hard?**
 - Migration is hard
 - **PQC is big**
 - Protected PQC is bigger
 - There is not just 1 PQC
- Final thoughts

(SOME) CHALLENGES OF PQC ON EMBEDDED DEVICES

Key Sizes

- Many current embedded devices struggle with pre-quantum key sizes, e.g., RSA-3072 keys

(SOME) CHALLENGES OF PQC ON EMBEDDED DEVICES

Key Sizes

- Many current embedded devices struggle with pre-quantum key sizes, e.g., RSA-3072 keys
- **PQC is order of magnitude larger**

PQC Signature Scheme:

Crystals-
Dilithium

Compared to current solution based on ECC:

Size (bytes)	Ed25519	Dilithium-3
Private key	64	4000
Public key	32	1952
Signature	64	3293

(SOME) CHALLENGES OF PQC ON EMBEDDED DEVICES

Key Sizes

- Many current embedded devices struggle with pre-quantum key sizes, e.g., RSA-3072 keys
- PQC is order of magnitude larger

PQC Signature Scheme:

Crystals-
Dilithium

Compared to current solution based on ECC:

Size (bytes)	Ed25519	Dilithium-3
Private key	64	4000
Public key	32	1952
Signature	64	3293

ROM/Flash; **small issues** like storing many keys or McEliece keys with public key sizes of **255 KiB – 1,326 KiB**.

(SOME) CHALLENGES OF PQC ON EMBEDDED DEVICES

Key Sizes

- Many current embedded devices struggle with pre-quantum key sizes, e.g., RSA-3072 keys
- PQC is order of magnitude larger

PQC Signature Scheme:

Crystals-
Dilithium

Compared to current solution based on ECC:

Size (bytes)	Ed25519	Dilithium-3
Private key	64	4000
Public key	32	1952
Signature	64	3293

ROM/Flash; **small issues** like storing many keys or McEliece keys with public key sizes of **255 KiB – 1,326 KiB**.

RAM; **bigger issue**. Many schemes use a lot of stack by default (**50 – 100 KiB** in pqm4).

Most secure microcontrollers are closer to 8~16 KB.

Lots of optimization necessary, impacts performance

SIGNATURE VERIFICATION – ECC VERSUS PQC

PQC Signature Scheme:

Crystals-
Dilithium

Case Study: Signature Verification

- Secure Boot
- Secure (over-the-air) Update

SIGNATURE VERIFICATION – ECC VERSUS PQC

PQC Signature Scheme:

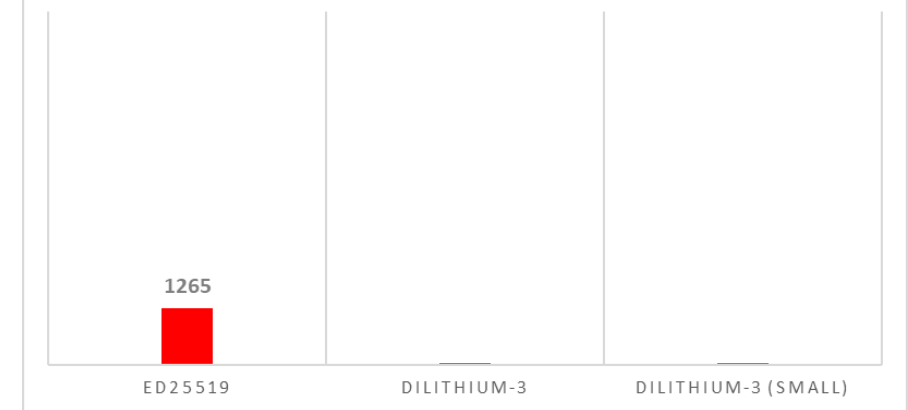
Crystals-
Dilithium

Case Study: Signature Verification

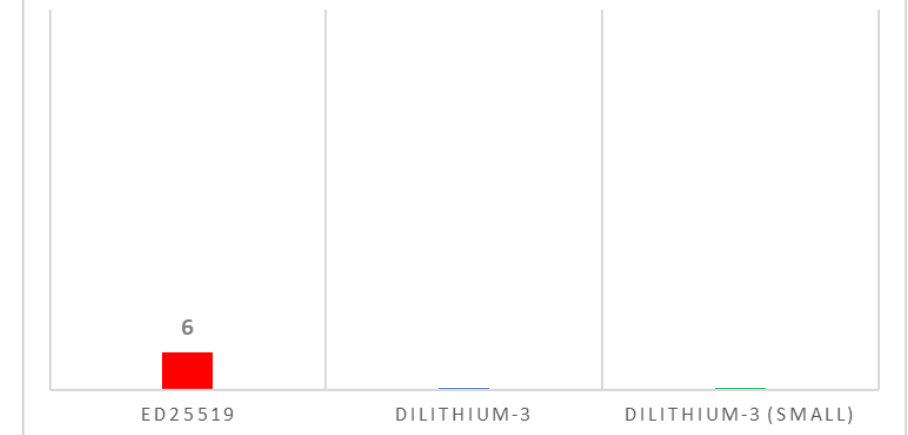
- Secure Boot
- Secure (over-the-air) Update

Academic figures on ARM Cortex-M4

VERIFY - PERFORMANCE (10³ CYCLES)



VERIFY - MEMORY (KIB)



Ed25519 from Fujii, Aranha. Curve25519 for the Cortex-M4 and beyond. In LatinCrypt 2017

SIGNATURE VERIFICATION – ECC VERSUS PQC

PQC Signature Scheme:

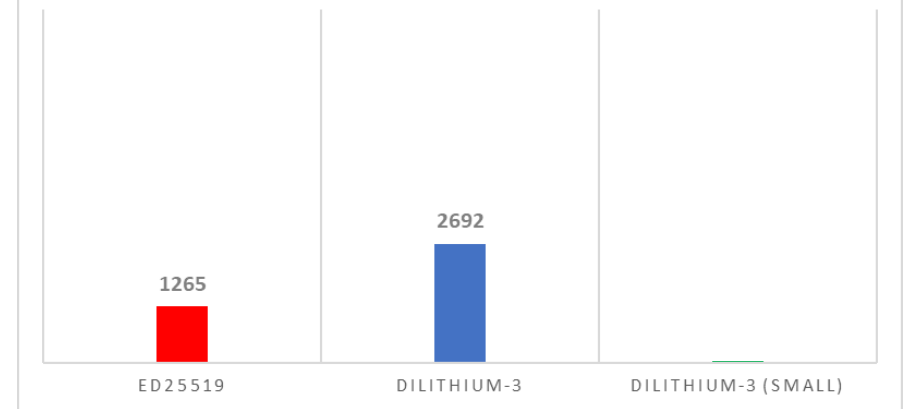
Crystals-
Dilithium

Case Study: Signature Verification

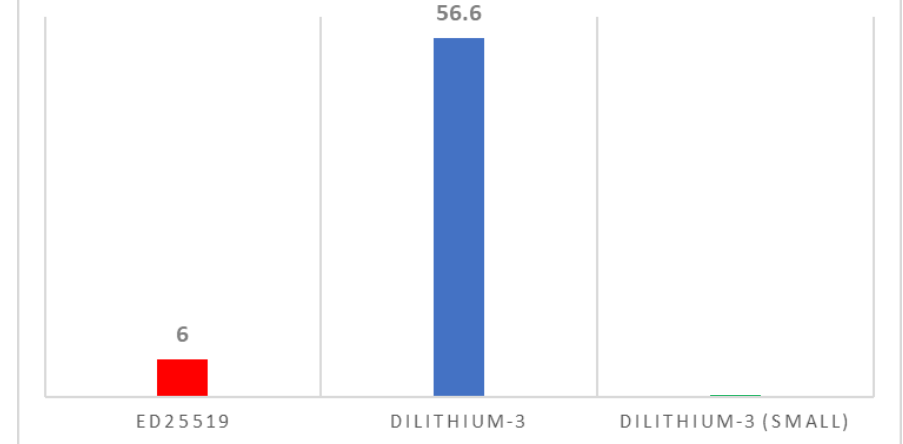
- Secure Boot
- Secure (over-the-air) Update

Academic figures on ARM Cortex-M4

VERIFY - PERFORMANCE (10³ CYCLES)



VERIFY - MEMORY (KIB)



Ed25519 from Fujii, Aranha. Curve25519 for the Cortex-M4 and beyond. In LatinCrypt 2017
Dilithium-3 from: Faster Kyber and Dilithium on the Cortex-M4. Cryptology ePrint Archive, Report 2022/112

SIGNATURE VERIFICATION – ECC VERSUS PQC

PQC Signature Scheme:

Crystals-
Dilithium

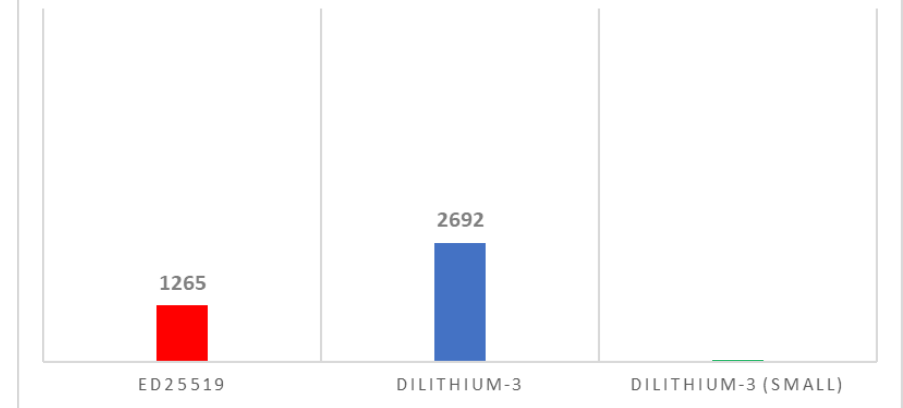
Case Study: Signature Verification

- Secure Boot
- Secure (over-the-air) Update

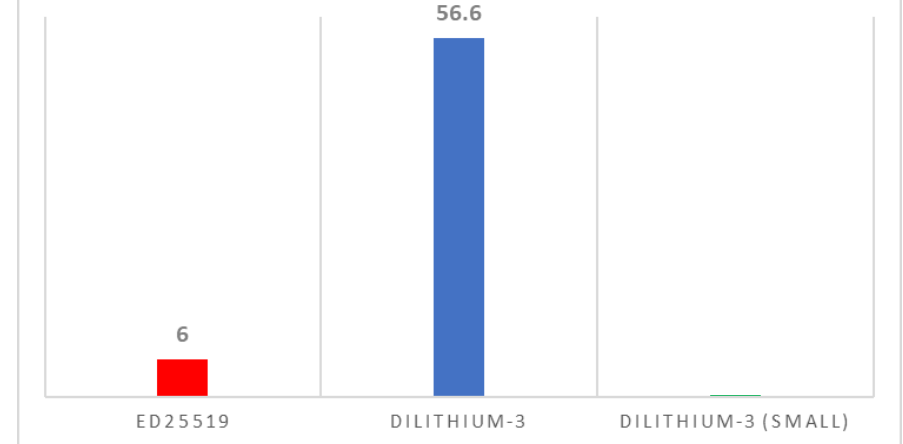
Academic figures on ARM Cortex-M4

Small Dilithium: Dilithium for Memory Constrained Devices.
Bos, Renes, Sprenkels, Cryptology ePrint Archive, Report 2022/323

VERIFY - PERFORMANCE (10³ CYCLES)



VERIFY - MEMORY (KIB)



Ed25519 from Fujii, Aranha. Curve25519 for the Cortex-M4 and beyond. In LatinCrypt 2017
Dilithium-3 from: Faster Kyber and Dilithium on the Cortex-M4. Cryptology ePrint Archive, Report 2022/112

SIGNATURE VERIFICATION – ECC VERSUS PQC

PQC Signature Scheme:

Crystals-
Dilithium

Case Study: Signature Verification

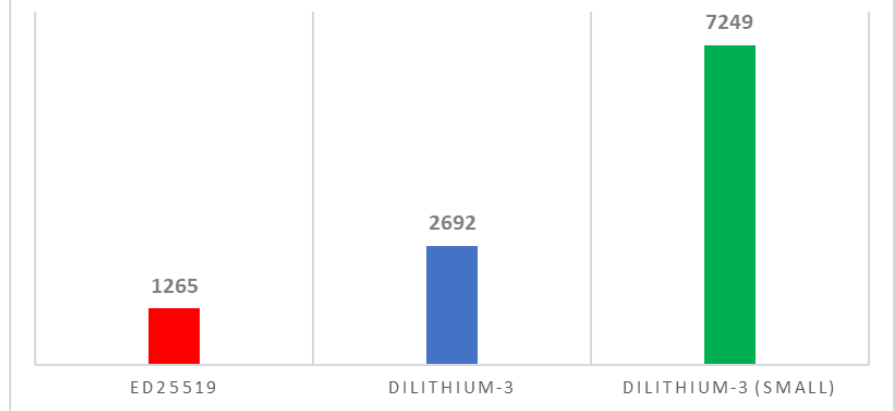
- Secure Boot
- Secure (over-the-air) Update

Academic figures on ARM Cortex-M4

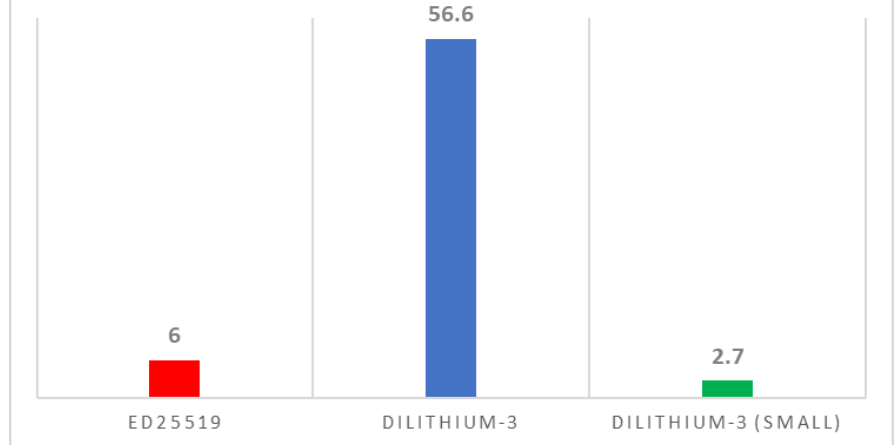
Small Dilithium: Dilithium for Memory Constrained Devices.
Bos, Renes, Sprenkels, Cryptology ePrint Archive, Report 2022/323

- Significant speed-up potential: SHA-3 HW acceleration

VERIFY - PERFORMANCE (10³ CYCLES)



VERIFY - MEMORY (KIB)



Ed25519 from Fujii, Aranha. Curve25519 for the Cortex-M4 and beyond. In LatinCrypt 2017
Dilithium-3 from: Faster Kyber and Dilithium on the Cortex-M4. Cryptology ePrint Archive, Report 2022/112

BACK TO THE SMARTCARDS

- Smartcard CPU cores are generally less efficient than an ARM Cortex M4
 - Let's say a factor c slowdown
- Need hardening against fault attacks
 - Let's say a factor f slowdown
- Back-of-the-envelope: at least 1-second for verification
 - (optimistically guess-timating @24MHz $c \geq 2, f \geq 2$, no public estimates available)



BACK TO THE SMARTCARDS

- Smartcard CPU cores are generally less efficient than an ARM Cortex M4
 - Let's say a factor c slowdown
- Need hardening against fault attacks
 - Let's say a factor f slowdown
- Back-of-the-envelope: at least 1-second for verification
 - (optimistically guess-timating @24MHz $c \geq 2, f \geq 2$, no public estimates available)
- This does not take **protocol operations** into account
- Industry standard (access control, payment) ~200ms
- Hardened signing will be worse





HOW TO PREPARE FOR HURRICANE SEASON Quantum



MAKE A PLAN

Airmen should create an emergency plan and/or checklist

- obtain supplies
- update personal documents
- secure household
- research evacuation options/routes
- update prescriptions



CREATE A GO-BAG

Prepare supplies ahead of a hurricane. These can include

- Food/water
- Additional clothes
- Personal documents
- Travel supplies
- Prescriptions



KNOW YOUR WING GUIDANCE

Whether preparing for a hurricane or evacuating know your wing or installation's guidance. Routinely check for updates from leadership and maintain communication with your chain of command.



RECOGNIZE WARNINGS & ALERTS

Have several ways to receive alerts. Download real-time alert apps. Sign up for community alerts in your area and be aware of the Emergency Alert System (EAS) and Wireless Emergency Alert (WEA)- which requires no-sign up.



STAY SAFE

Practice good hygiene and safety measures during any part of a hurricane evacuation or impact. Keep family considerations in mind and don't be afraid to contact leadership for guidance.

OUTLINE

- What is a smartcard?
- **Why is resource constrained PQC hard?**
 - Migration is hard
 - PQC is big
 - **Protected PQC is bigger**
 - There is not just 1 PQC
- Final thoughts



SIDE-CHANNEL ATTACKS

For ECC/RSA, SCA are quite mature and well-understood

For PQC work has started ~5 years ago

There are many more types of schemes




SIDE-CHANNEL ATTACKS

For ECC/RSA, SCA are quite mature and well-understood

For PQC work has started ~5 years ago

There are many more types of schemes
and it was not taken into account for algorithm design

Performance overhead compared to **unprotected** (d=1) Kyber on Cortex-M4 for high noise (SW) / low noise settings (HW + SW) [BGR+21]:

SCA security level					
					
d=2	d=3	d=4	d=5	d=6	d=7
3.5x	64x	110x	197x	293x	397x



SIDE-CHANNEL ATTACKS

For ECC/RSA, SCA are quite mature and well-understood

For PQC work has started ~5 years ago

There are many more types of schemes
and it was not taken into account for algorithm design

Performance overhead compared to **unprotected** (d=1) Kyber on Cortex-M4 for high noise (SW) / low noise settings (HW + SW) [BGR+21]:

SCA security level					
d=2	d=3	d=4	d=5	d=6	d=7
3.5x	64x	110x	197x	293x	397x
18x		High(er)			



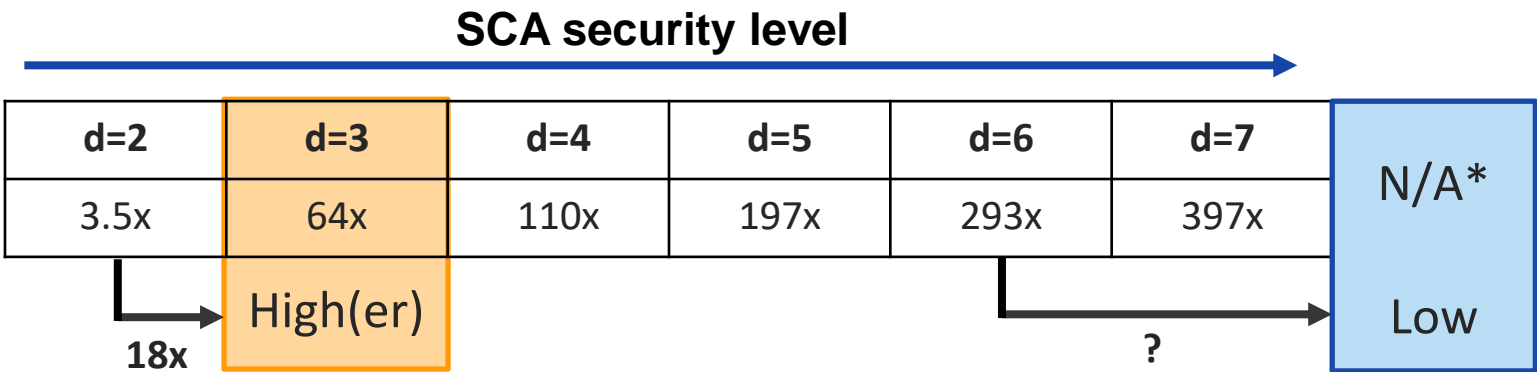
SIDE-CHANNEL ATTACKS

For ECC/RSA, SCA are quite mature and well-understood

For PQC work has started ~5 years ago

There are many more types of schemes
and it was not taken into account for algorithm design

Performance overhead compared to **unprotected** (d=1) Kyber on Cortex-M4 for high noise (SW) / low noise settings (HW + SW) [BGR+21]:



* For this specific implementation + board.

Requires further stack usage optimization.





HOW TO PREPARE FOR HURRICANE SEASON Quantum



MAKE A PLAN

Airmen should create an emergency plan and/or checklist

- obtain supplies
- update personal documents
- secure household
- research evacuation options/routes
- update prescriptions



CREATE A GO-BAG

Prepare supplies ahead of a hurricane. These can include

- Food/water
- Additional clothes
- Personal documents
- Travel supplies
- Prescriptions



KNOW YOUR WING GUIDANCE

Whether preparing for a hurricane or evacuating know your wing or installation's guidance. Routinely check for updates from leadership and maintain communication with your chain of command.



RECOGNIZE WARNINGS & ALERTS

Have several ways to receive alerts. Download real-time alert apps. Sign up for community alerts in your area and be aware of the Emergency Alert System (EAS) and Wireless Emergency Alert (WEA)- which requires no-sign up.



STAY SAFE

Practice good hygiene and safety measures during any part of a hurricane evacuation or impact. Keep family considerations in mind and don't be afraid to contact leadership for guidance.

OUTLINE

- What is a smartcard?
- **Why is resource constrained PQC hard?**
 - Migration is hard
 - PQC is big
 - Protected PQC is bigger
 - **There is not just 1 PQC**
- Final thoughts



NO ONE STANDARD TO RULE THEM ALL

Secure microcontrollers are used in varied **markets** in varied **countries**

→ For the same chip different support might be needed



NO ONE STANDARD TO RULE THEM ALL

Secure microcontrollers are used in varied **markets** in varied **countries**

→ For the same chip different support might be needed

So, what to support?

- Stateful hash-based DS

Scheme	Number of schemes
Signature	1
KEM	0



NO ONE STANDARD TO RULE THEM ALL

Secure microcontrollers are used in varied **markets** in varied **countries**

→ For the same chip different support might be needed

So, what to support?

- Stateful hash-based DS
- NIST competition winners

Scheme	
Signature	1 4
KEM	0 1



NO ONE STANDARD TO RULE THEM ALL

Secure microcontrollers are used in varied **markets** in varied **countries**
→ For the same chip different support might be needed

So, what to support?

- Stateful hash-based DS
- NIST competition winners
- ~2025 and beyond: Round 4 winners

Scheme	
Signature	1-4 5
KEM	0-1 2



NO ONE STANDARD TO RULE THEM ALL

Secure microcontrollers are used in varied **markets** in varied **countries**

→ For the same chip different support might be needed

So, what to support?

- Stateful hash-based DS
- NIST competition winners
- ~2025 and beyond: Round 4 winners
- EU: Frodo/McEliece advised by *BSI/ANSSI/AIVD/NCSA* (**passports**)

Scheme	
Signature	1-4 5
KEM	0-1-2 4

NO ONE STANDARD TO RULE THEM ALL

Secure microcontrollers are used in varied **markets** in varied **countries**

→ For the same chip different support might be needed

So, what to support?

- Stateful hash-based DS
- NIST competition winners
- ~2025 and beyond: Round 4 winners
- EU: Frodo/McEliece advised by *BSI/ANSSI/AIVD/NCSA* (**passports**)
- China: LAC
- Others?

Scheme		
Signature	1 4 5	???
KEM	0 1 2 4 5	

HIGHER-LEVEL STANDARDS

With standardization for core DS/KEM algorithms a good first step is made, but...



HIGHER-LEVEL STANDARDS

With standardization for core DS/KEM algorithms a good first step is made, but...

A lot of (secure microcontroller) applications follow standards

- Global Platform for trusted digital services
- Trusted Computing Group for trusted computing platforms
- IETF for Internet things
- ISO/IEC for all kinds of application domains
- Cloud Security Alliance for Cloud things

The logo for the National Institute of Standards and Technology (NIST), consisting of the letters "NIST" in a bold, black, sans-serif font.The logo for the Global Platform, featuring the word "GLOBAL" in black and "PLATFORM" in black, with a small orange and blue icon to the left of "PLATFORM".The logo for the Trusted Computing Group, featuring the words "TRUSTED", "COMPUTING", and "GROUP" in blue, stacked vertically, with a small registered trademark symbol to the right of "TRUSTED".The text logo for the Internet Engineering Task Force (IETF), consisting of the letters "I E T F" in a bold, black, sans-serif font, with a small registered trademark symbol to the right of "F".The logo for the Cloud Security Alliance (CSA), featuring the letters "CSA" in blue, bold, sans-serif font, followed by the words "cloud", "security", and "alliance" in orange, stacked vertically, with a small "SM" trademark symbol to the right of "alliance".

HIGHER-LEVEL STANDARDS

With standardization for core DS/KEM algorithms a good first step is made, but...

A lot of (secure microcontroller) applications follow standards

- Global Platform for trusted digital services
- Trusted Computing Group for trusted computing platforms
- IETF for Internet things
- ISO/IEC for all kinds of application domains
- Cloud Security Alliance for Cloud things

What if some lag behind in setting post-quantum standards?

What if these do not agree?

What if a secure microcontroller has to support multiple?



GLOBALPLATFORM

TRUSTED[®]
COMPUTING
GROUP



I E T F[®]



cloud
CSA security
allianceSM



HOW TO PREPARE FOR HURRICANE SEASON Quantum



MAKE A PLAN

Airmen should create an emergency plan and/or checklist

- obtain supplies
- update personal documents
- secure household
- research evacuation options/routes
- update prescriptions



CREATE A GO-BAG

Prepare supplies ahead of a hurricane. These can include

- Food/water
- Additional clothes
- Personal documents
- Travel supplies
- Prescriptions



KNOW YOUR WING GUIDANCE

Whether preparing for a hurricane or evacuating know your wing or installation's guidance. Routinely check for updates from leadership and maintain communication with your chain of command.



RECOGNIZE WARNINGS & ALERTS

Have several ways to receive alerts. Download real-time alert apps. Sign up for community alerts in your area and be aware of the Emergency Alert System (EAS) and Wireless Emergency Alert (WEA)- which requires no-sign up.



STAY SAFE

Practice good hygiene and safety measures during any part of a hurricane evacuation or impact. Keep family considerations in mind and don't be afraid to contact leadership for guidance.

OUTLINE

- What is a smartcard?
- Why is resource constrained PQC hard?
 - Migration is hard
 - PQC is big
 - Protected PQC is bigger
 - There is not just 1 PQC
- Final thoughts



HOW TO PREPARE FOR HURRICANE SEASON Quantum



MAKE A PLAN

Airmen should create an emergency plan and/or checklist

- obtain supplies
- update personal documents
- secure household
- research evacuation options/routes
- update prescriptions



CREATE A GO-BAG

Prepare supplies ahead of a hurricane. These can include

- Food/water
- Additional clothes
- Personal documents
- Travel supplies
- Prescriptions



KNOW YOUR WING GUIDANCE

Whether preparing for a hurricane or evacuating know your wing or installation's guidance. Routinely check for updates from leadership and maintain communication with your chain of command.



RECOGNIZE WARNINGS & ALERTS

Have several ways to receive alerts. Download real-time alert apps. Sign up for community alerts in your area and be aware of the Emergency Alert System (EAS) and Wireless Emergency Alert (WEA)- which requires no-sign up.



STAY SAFE

Practice good hygiene and safety measures during any part of a hurricane evacuation or impact. Keep family considerations in mind and don't be afraid to contact leadership for guidance.

FINAL THOUGHTS



HOW TO PREPARE FOR HURRICANE SEASON Quantum



MAKE A PLAN

Airmen should create an emergency plan and/or checklist

- obtain supplies
- update personal documents
- secure household
- research evacuation options/routes
- update prescriptions



CREATE A GO-BAG

Prepare supplies ahead of a hurricane. These can include

- Food/water
- Additional clothes
- Personal documents
- Travel supplies
- Prescriptions



KNOW YOUR WING GUIDANCE

Whether preparing for a hurricane or evacuating know your wing or installation's guidance. Routinely check for updates from leadership and maintain communication with your chain of command.



RECOGNIZE WARNINGS & ALERTS

Have several ways to receive alerts. Download real-time alert apps. Sign up for community alerts in your area and be aware of the Emergency Alert System (EAS) and Wireless Emergency Alert (WEA)- which requires no-sign up.



STAY SAFE

Practice good hygiene and safety measures during any part of a hurricane evacuation or impact. Keep family considerations in mind and don't be afraid to contact leadership for guidance.

FINAL THOUGHTS

PQC is coming.

Irrelevant if the quantum threat is real or not.

Customers already request support for the future standard.



HOW TO PREPARE FOR HURRICANE SEASON Quantum



MAKE A PLAN

Airmen should create an emergency plan and/or checklist

- obtain supplies
- update personal documents
- secure household
- research evacuation options/routes
- update prescriptions



CREATE A GO-BAG

Prepare supplies ahead of a hurricane. These can include

- Food/water
- Additional clothes
- Personal documents
- Travel supplies
- Prescriptions



KNOW YOUR WING GUIDANCE

Whether preparing for a hurricane or evacuating know your wing or installation's guidance. Routinely check for updates from leadership and maintain communication with your chain of command.



RECOGNIZE WARNINGS & ALERTS

Have several ways to receive alerts. Download real-time alert apps. Sign up for community alerts in your area and be aware of the Emergency Alert System (EAS) and Wireless Emergency Alert (WEA)- which requires no-sign up.



STAY SAFE

Practice good hygiene and safety measures during any part of a hurricane evacuation or impact. Keep family considerations in mind and don't be afraid to contact leadership for guidance.

FINAL THOUGHTS

PQC is coming.

Irrelevant if the quantum threat is real or not.

Customers already request support for the future standard.

PQC will be a challenge.

Performance, memory, key size, hardening, migration and agility.

What will be the main challenge for your industry?



HOW TO PREPARE FOR HURRICANE SEASON Quantum



MAKE A PLAN

Airmen should create an emergency plan and/or checklist

- obtain supplies
- update personal documents
- secure household
- research evacuation options/routes
- update prescriptions



CREATE A GO-BAG

Prepare supplies ahead of a hurricane. These can include

- Food/water
- Additional clothes
- Personal documents
- Travel supplies
- Prescriptions



KNOW YOUR WING GUIDANCE

Whether preparing for a hurricane or evacuating know your wing or installation's guidance. Routinely check for updates from leadership and maintain communication with your chain of command.



RECOGNIZE WARNINGS & ALERTS

Have several ways to receive alerts. Download real-time alert apps. Sign up for community alerts in your area and be aware of the Emergency Alert System (EAS) and Wireless Emergency Alert (WEA)- which requires no-sign up.



STAY SAFE

Practice good hygiene and safety measures during any part of a hurricane evacuation or impact. Keep family considerations in mind and don't be afraid to contact leadership for guidance.

FINAL THOUGHTS

PQC is coming.

Irrelevant if the quantum threat is real or not.

Customers already request support for the future standard.

PQC will be a challenge.

Performance, memory, key size, hardening, migration and agility.

What will be the main challenge for your industry?

Start now.

Identify issues now, so bottlenecks can be solved.

Can serve as input for standardization.

THANK YOU.

QUESTIONS?



SECURE CONNECTIONS
FOR A SMARTER WORLD

CONTACT: PQC@NXP.COM | NXP.COM/PQC