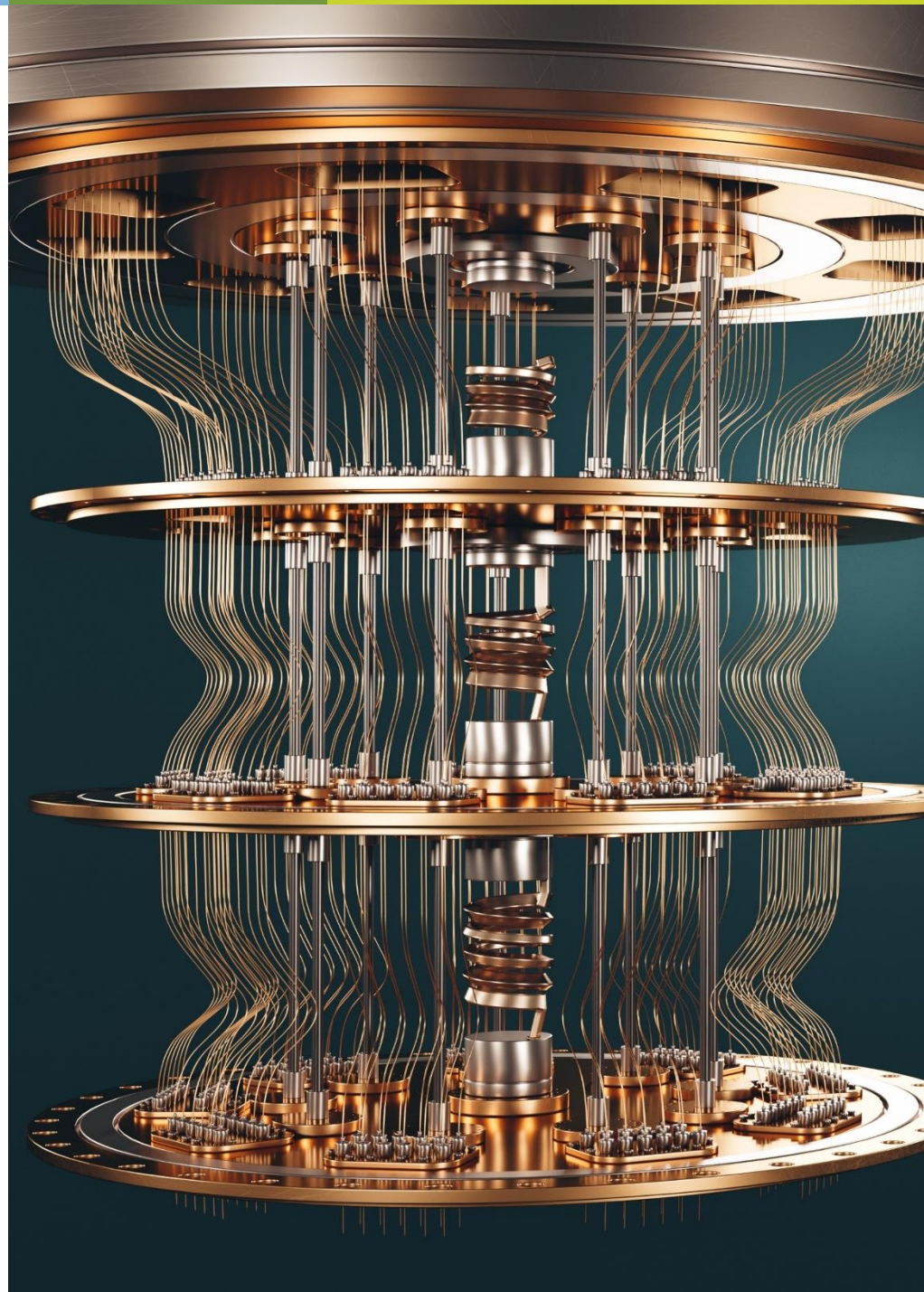
Lessons Learned from Protecting CRYSTALS-DILITHIUM

Melissa Azouaoui, Joppe Bos, Olivier Bronchain, Joost Renes, Markus Schönauer, **Tobias Schneider**, and Christine van Vredendaal

contact: pqc@nxp.com

RWC 2023
March 27, 2023



NXP | SECURE CONNECTIONS FOR A SMARTER WORLD

PUBLIC

WHY DO WE WANT TO PROTECT DILITHIUM?

NIST chooses **Dilithium** as primary digital signature algorithm.

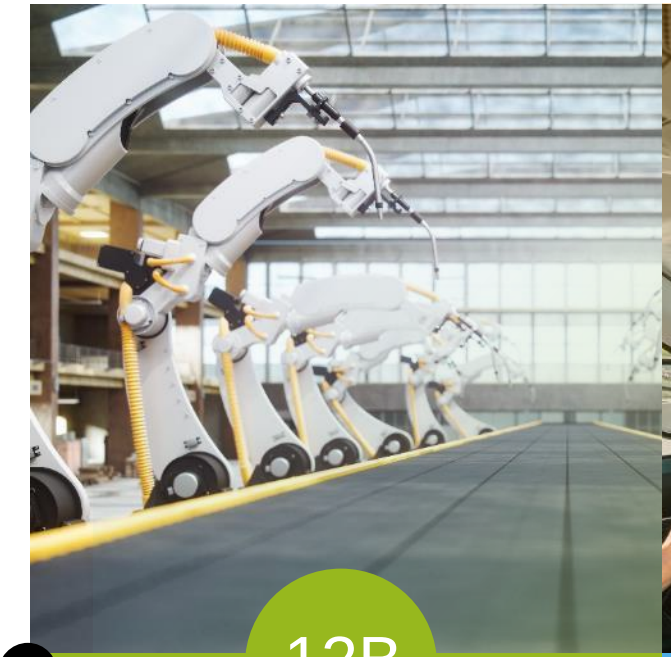
Transition

2022

2024

NIST publishes **standardization documents**.

INDUSTRIAL & IOT



12B

IoT Edge & end nodes from **6B units** in 2021 to **12B units** in **2025**

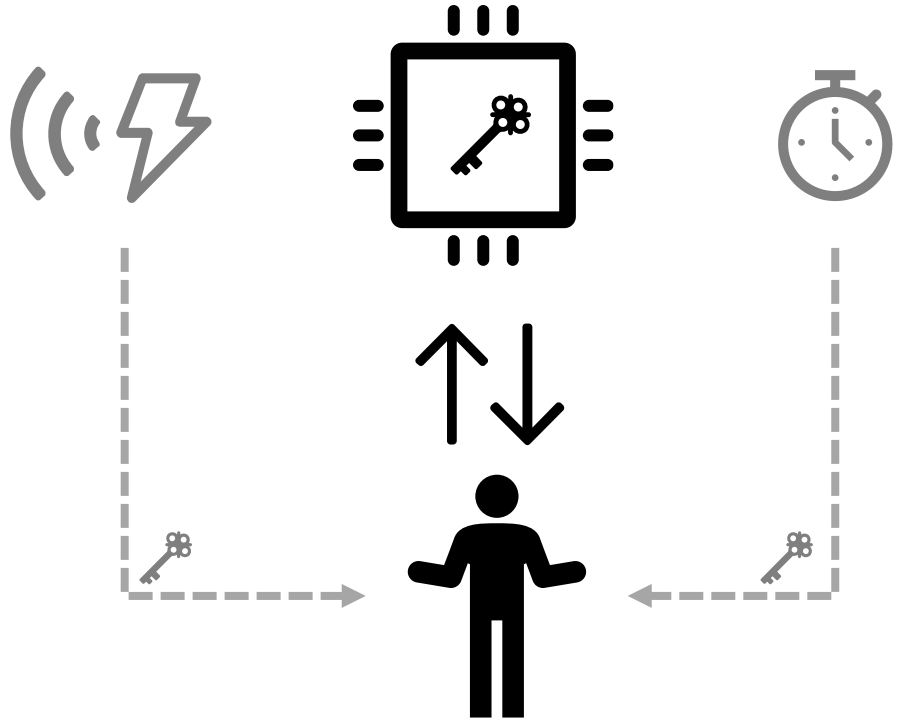
AUTOMOTIVE

70%

70% connected cars by 2025

WHY DO WE WANT TO PROTECT DILITHIUM?

Embedded devices are vulnerable to **physical attacks.**

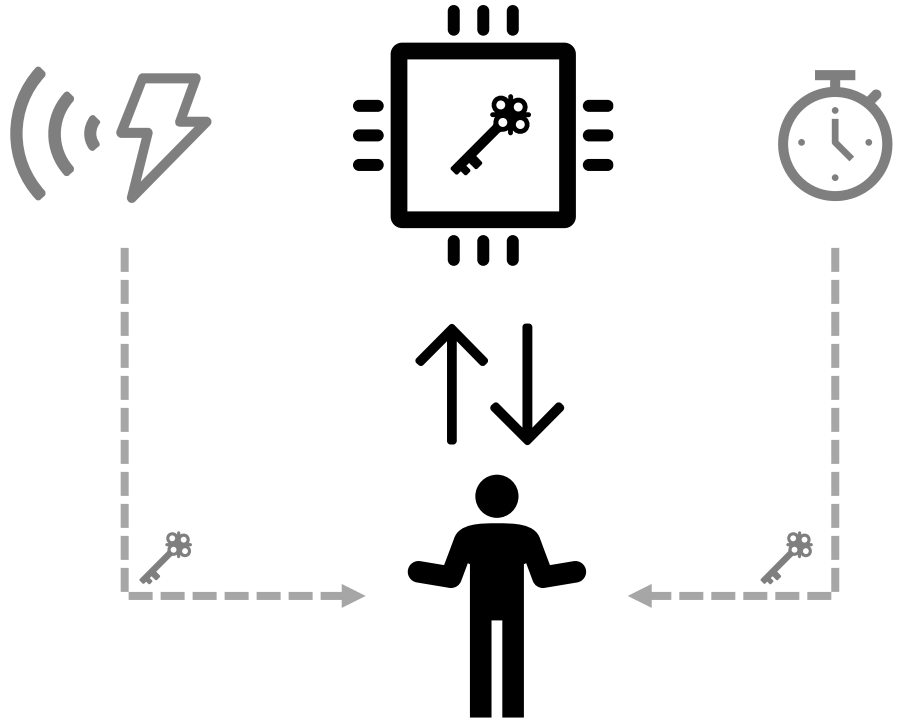


Protection could require **significant effort**.

Potential to **delay** deployment of **secure PQC**.

WHY DO WE WANT TO PROTECT DILITHIUM?

Embedded devices are vulnerable to **physical attacks.**



Protection could require **significant effort**.

Potential to **delay** deployment of **secure PQC**.

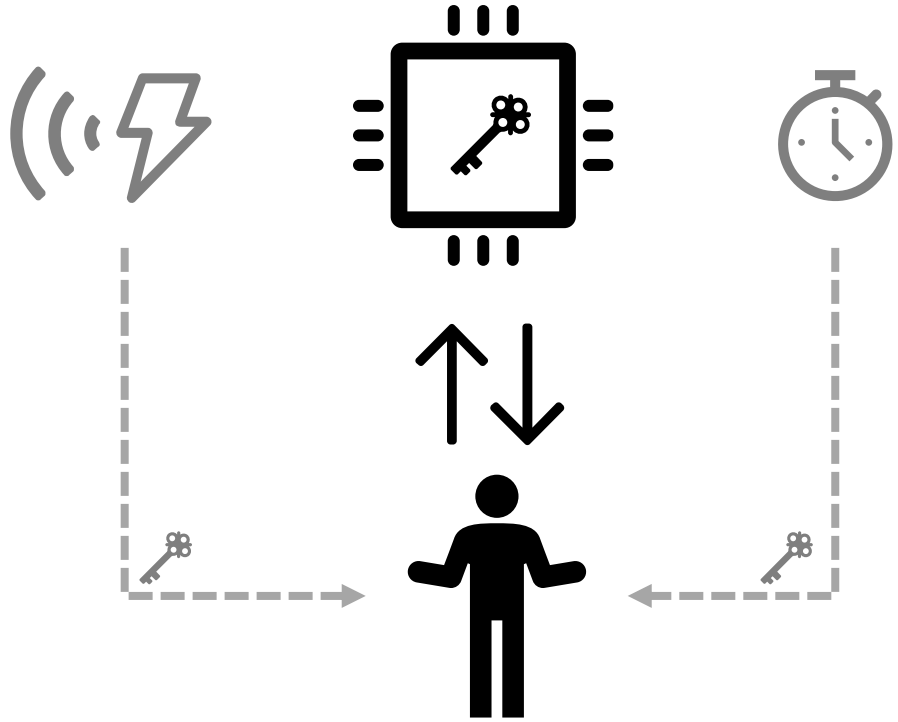
Found to be extremely vulnerable.

RWC 2022: FO-CALYPSE

RWC 2023: Breaking 5th order masking

WHY DO WE WANT TO PROTECT DILITHIUM?

Embedded devices are vulnerable to **physical attacks.**



Protection could require **significant effort**.

Potential to **delay** deployment of **secure PQC**.

Found to be extremely vulnerable.

RWC 2022: FO-CALYPSE

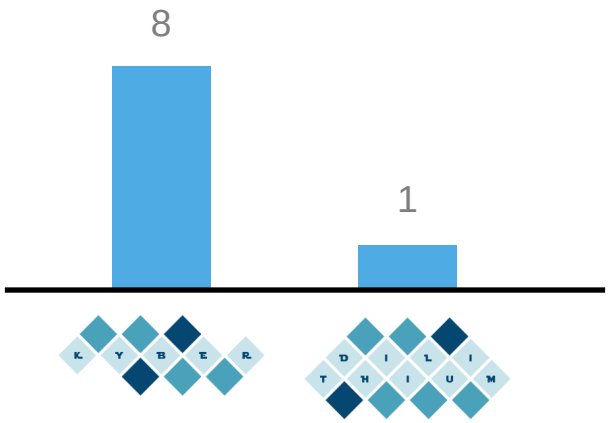
RWC 2023: Breaking 5th order masking

Less investigated**.**

RWC 2023: Lessons learned

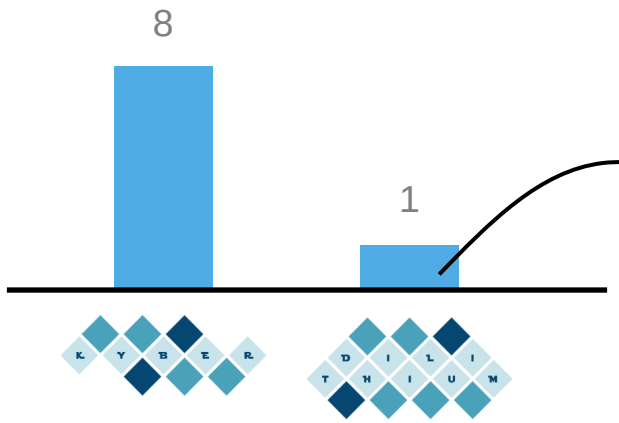
DO WE KNOW HOW TO PROTECT DILITHIUM?

Masking Publications until October'22



DO WE KNOW HOW TO PROTECT DILITHIUM?

Masking Publications until October'22



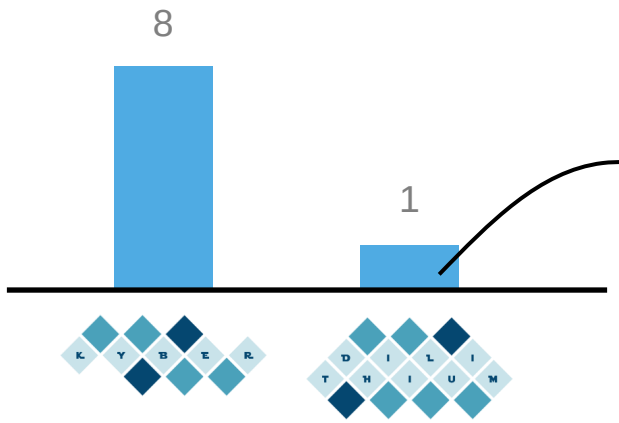
Prior Work [MGTF19]

Masking Dilithium: Efficient Implementation and Side-Channel Evaluation

Vincent Migliore[1], Benoit Gérard[23], Mehdi Tibouchi[4] and Pierre-Alain Fouque[2]

DO WE KNOW HOW TO PROTECT DILITHIUM?

Masking Publications until October'22



Prior Work [MGTF19]

Masking Dilithium: Efficient Implementation and Side-Channel Evaluation

Vincent Migliore[1], Benoit Gérard[23], Mehdi Tibouchi[4] and Pierre-Alain Fouque[2]

ePrint 2022/1406

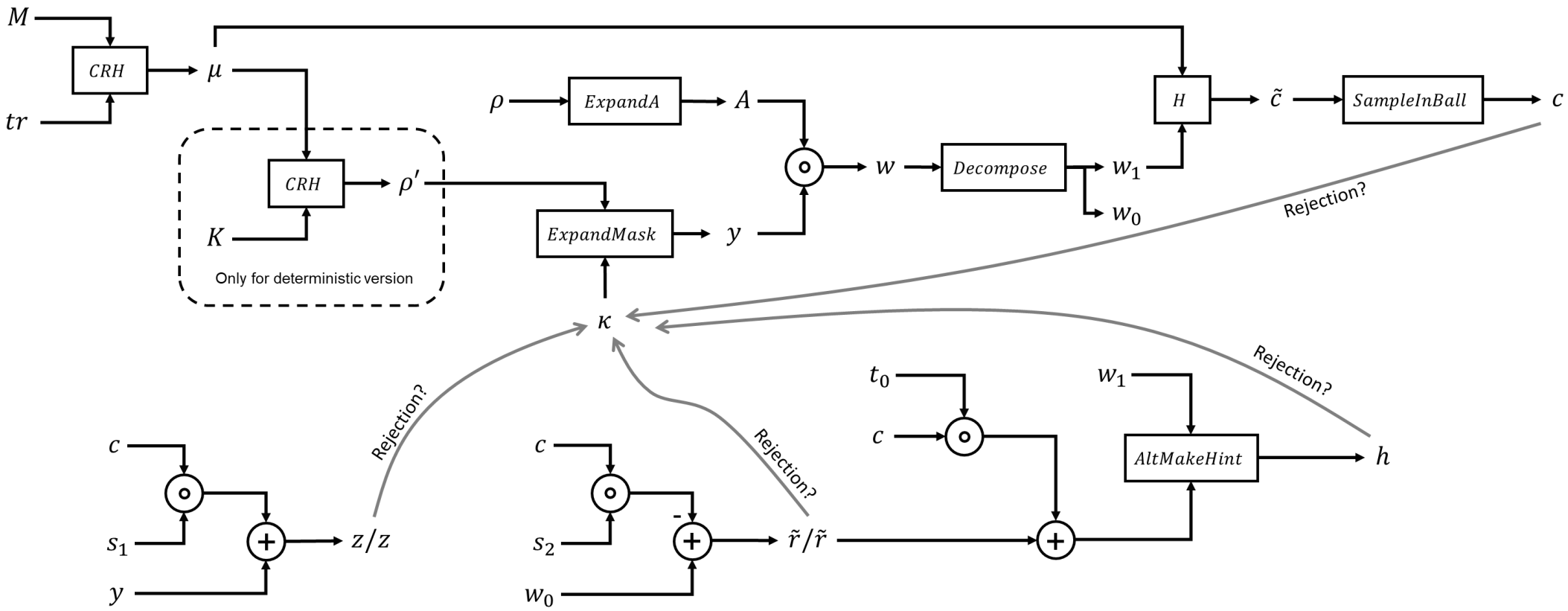
Leveling Dilithium against Leakage

Revisited Sensitivity Analysis and Improved Implementations

Melissa Azouaoui[1], Olivier Bronchain[1,2], Gaëtan Cassiers[2,3,4], Clément Hoffmann[2], Yulia Kuzovkova[1], Joost Renes[1], Tobias Schneider[1], Markus Schönauer[1], François-Xavier Standaert[2] and Christine van Vredendaal[1]

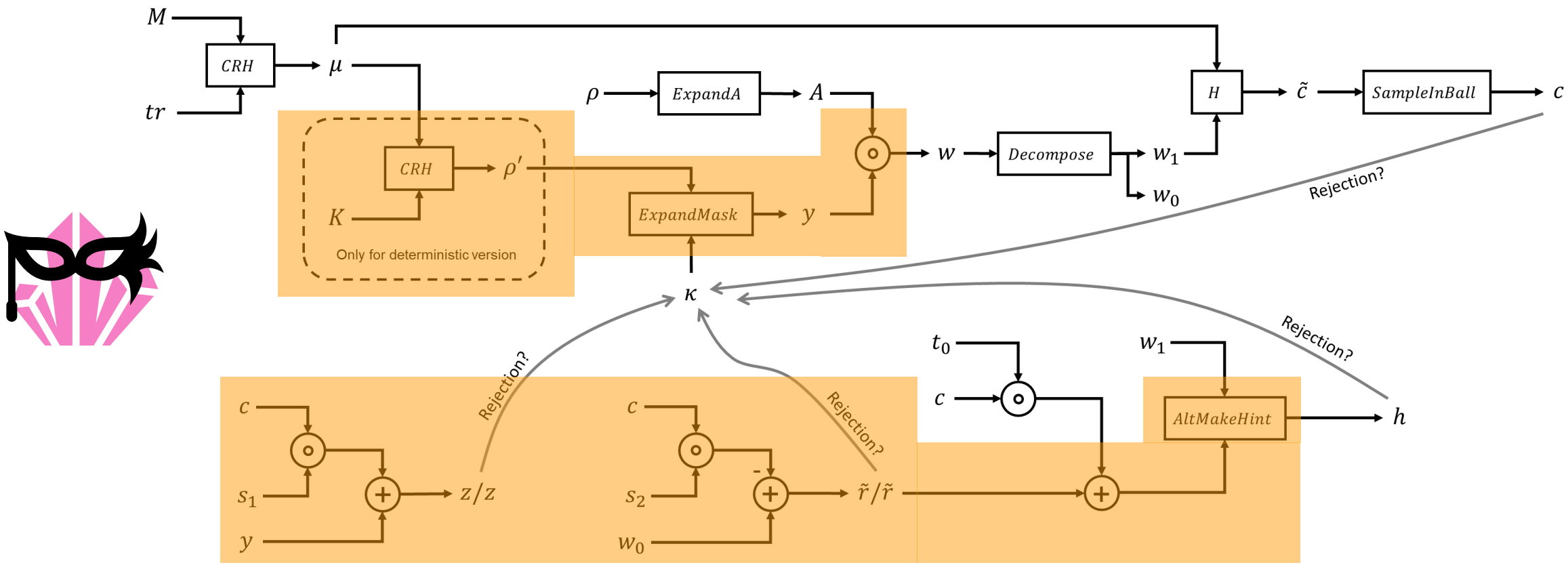
What needs to be protected?
How should it be protected?
What are the bottlenecks?
How can it be fixed?

WHAT NEEDS TO BE PROTECTED?



Signature Generation

PRIOR WORK [MGTF19]

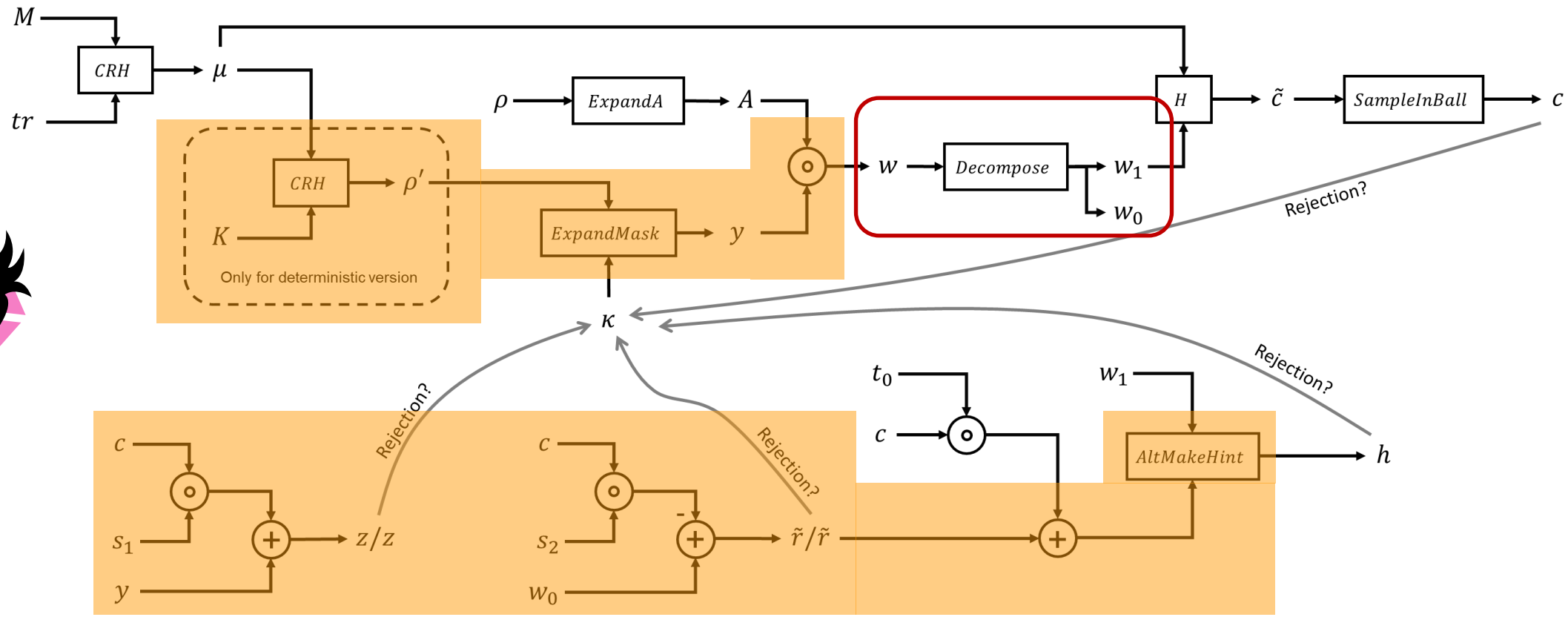


Signature Generation

PRIOR WORK [MGTF19]

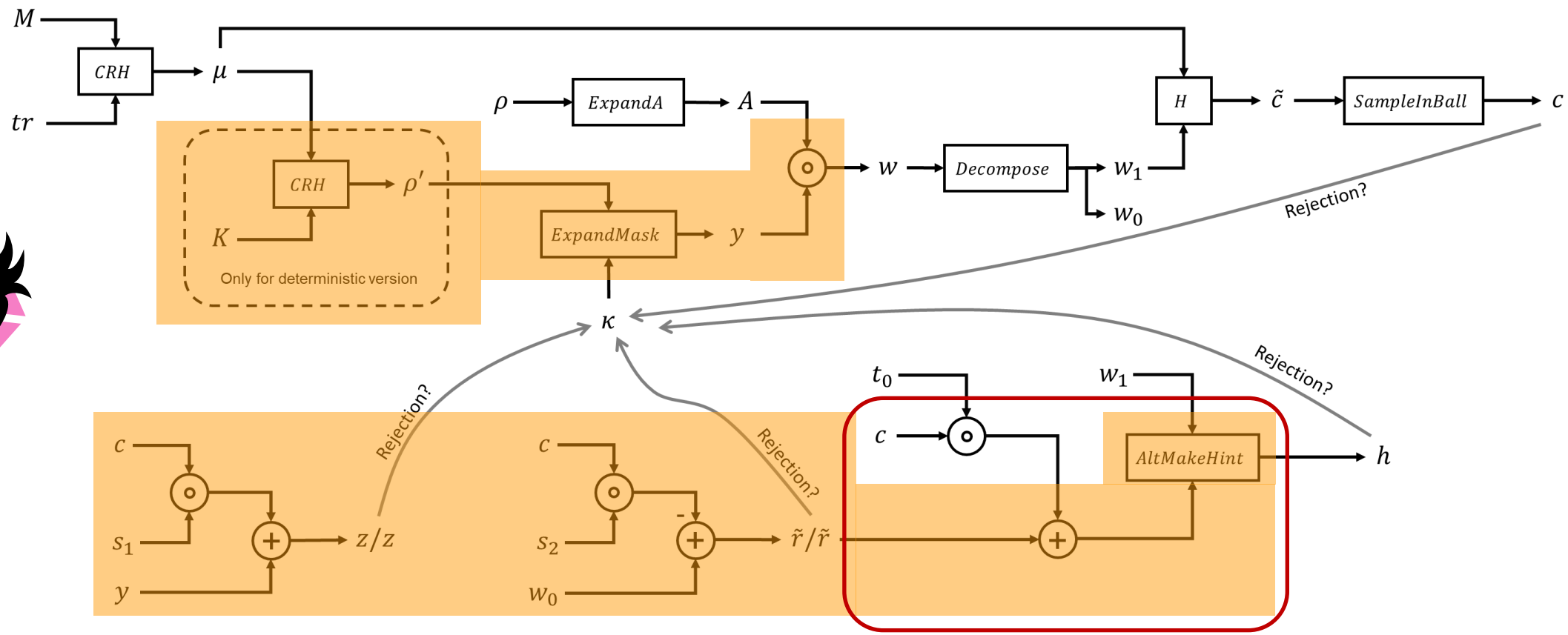
Protecting **w**

$\mathbf{w} = \mathbf{A} \cdot \mathbf{y} \Rightarrow \mathbf{y}$ can be computed from **w**



Signature Generation

PRIOR WORK [MGTF19]



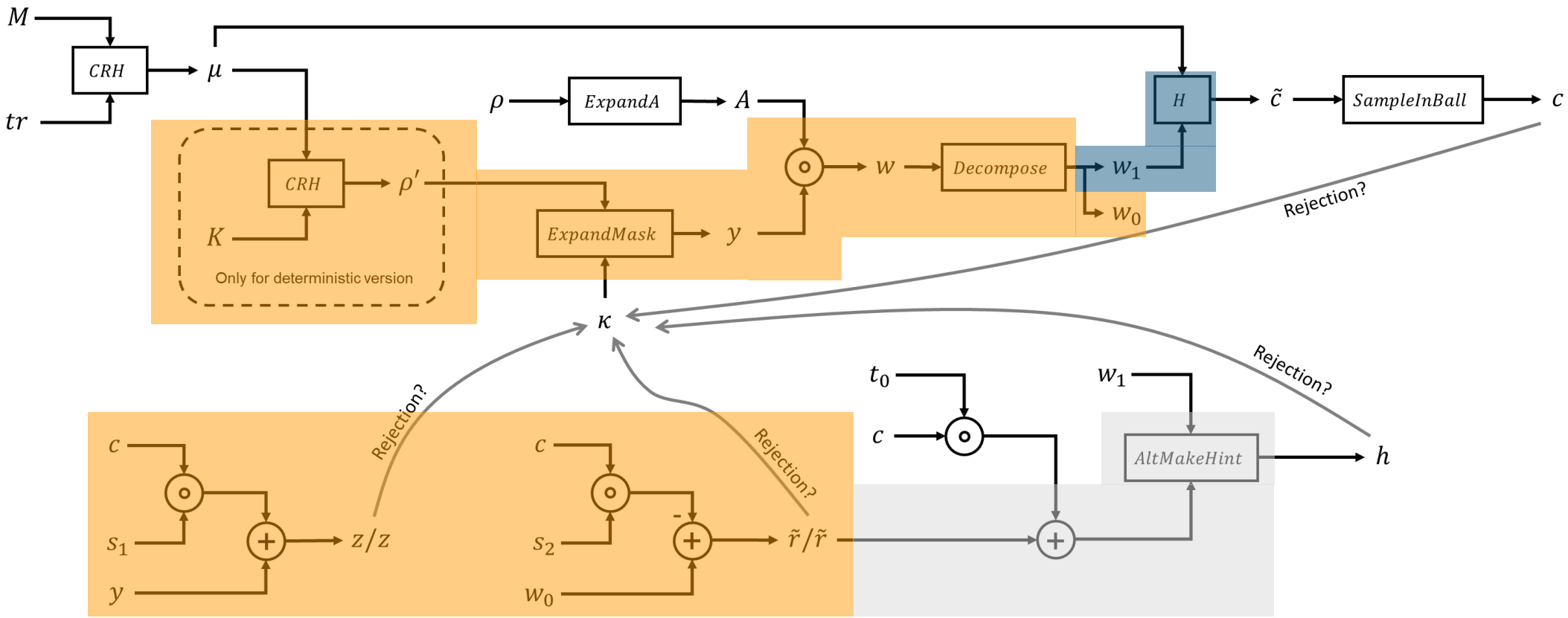
Signature Generation

Unmasking $\tilde{\mathbf{r}}$

$\mathbf{Az} - \mathbf{ct} = \alpha.\mathbf{w_1} + \tilde{\mathbf{r}} \Rightarrow \tilde{\mathbf{r}}$

can be computed from public values only

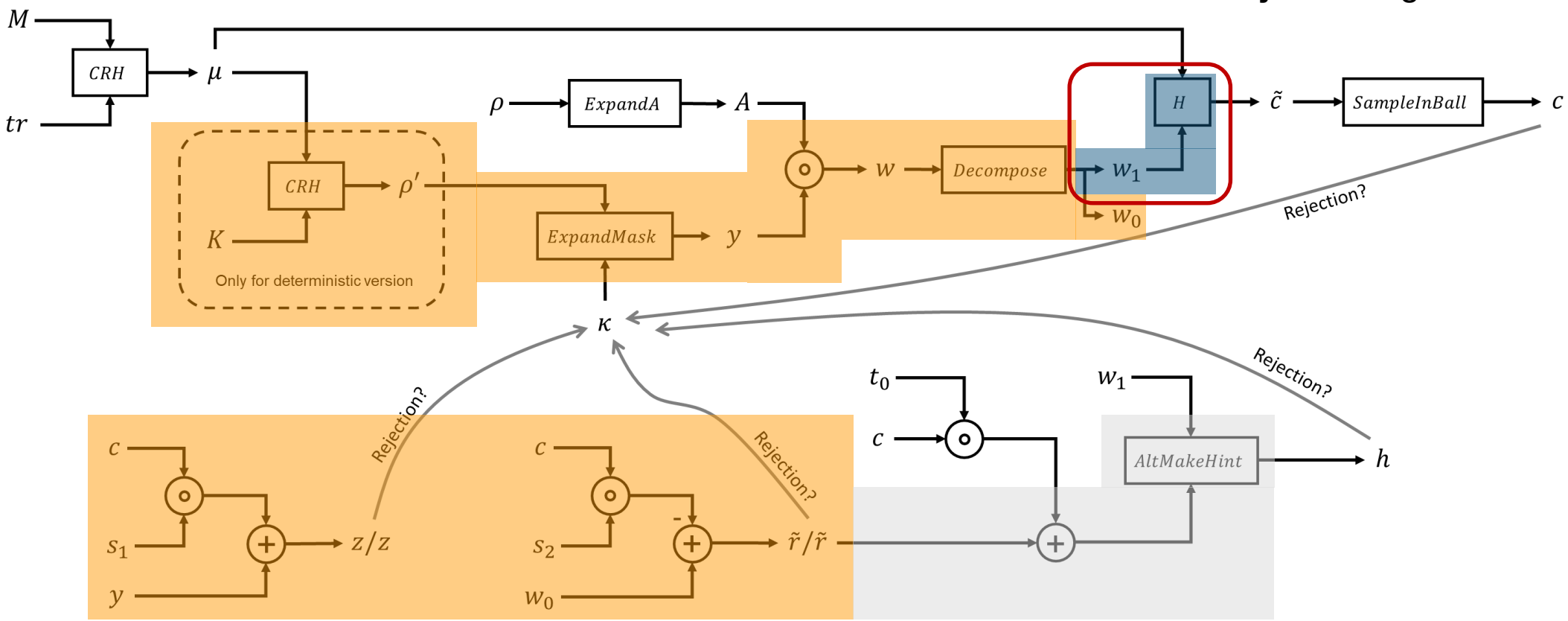
UPDATED SENSITIVITY ANALYSIS



Signature Generation

UPDATED SENSITIVITY ANALYSIS

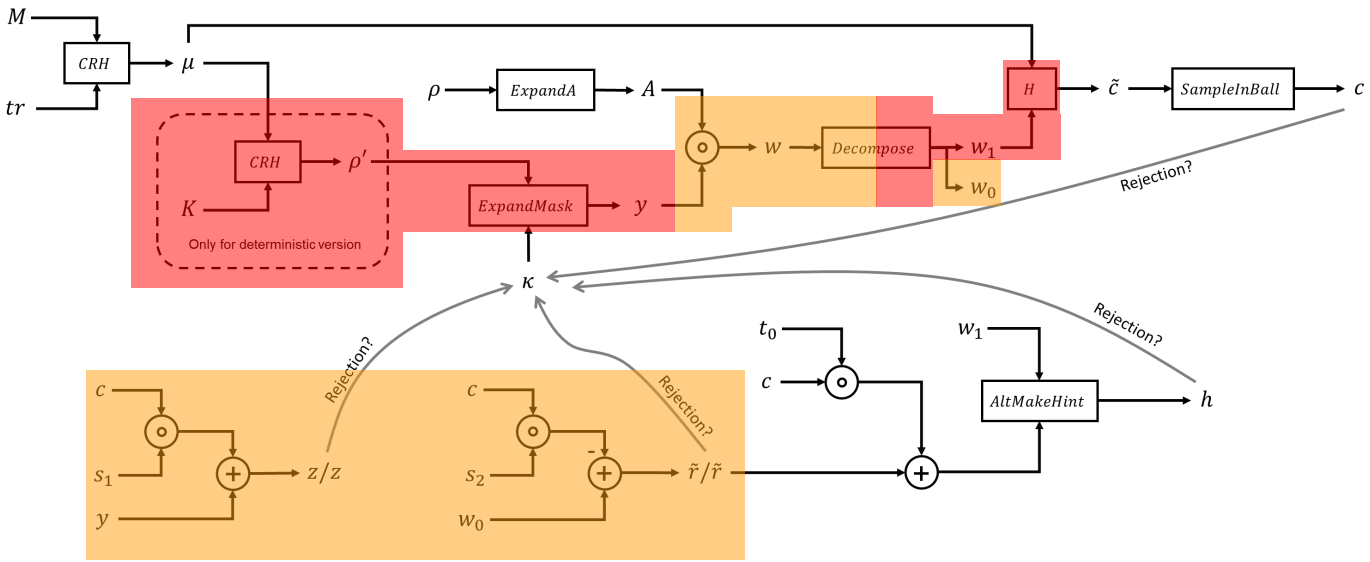
Protecting $\mathbf{w_1}$
Public for **valid** signatures,
unclear for **rejected** signatures



Signature Generation

HOW SHOULD IT BE PROTECTED?

Standard Approach: Masking

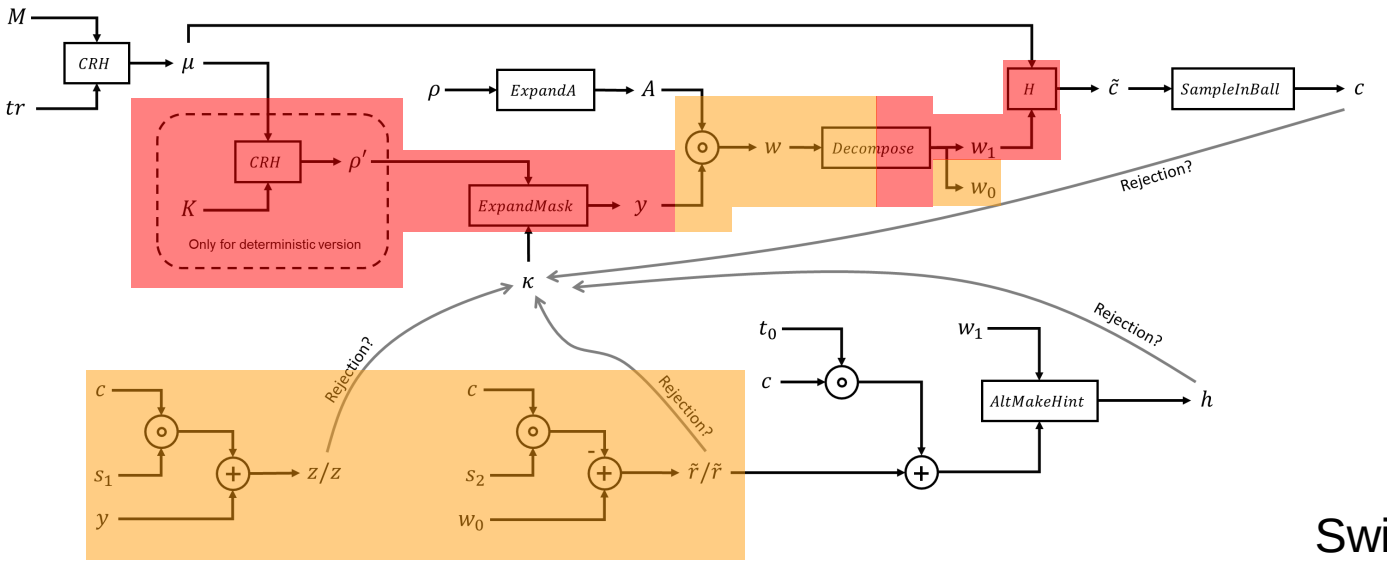


Signature Generation

Observation 1:
Requires a mixture of **Boolean** and **arithmetic** masking with a **prime modulus**

HOW SHOULD IT BE PROTECTED?

Standard Approach: Masking



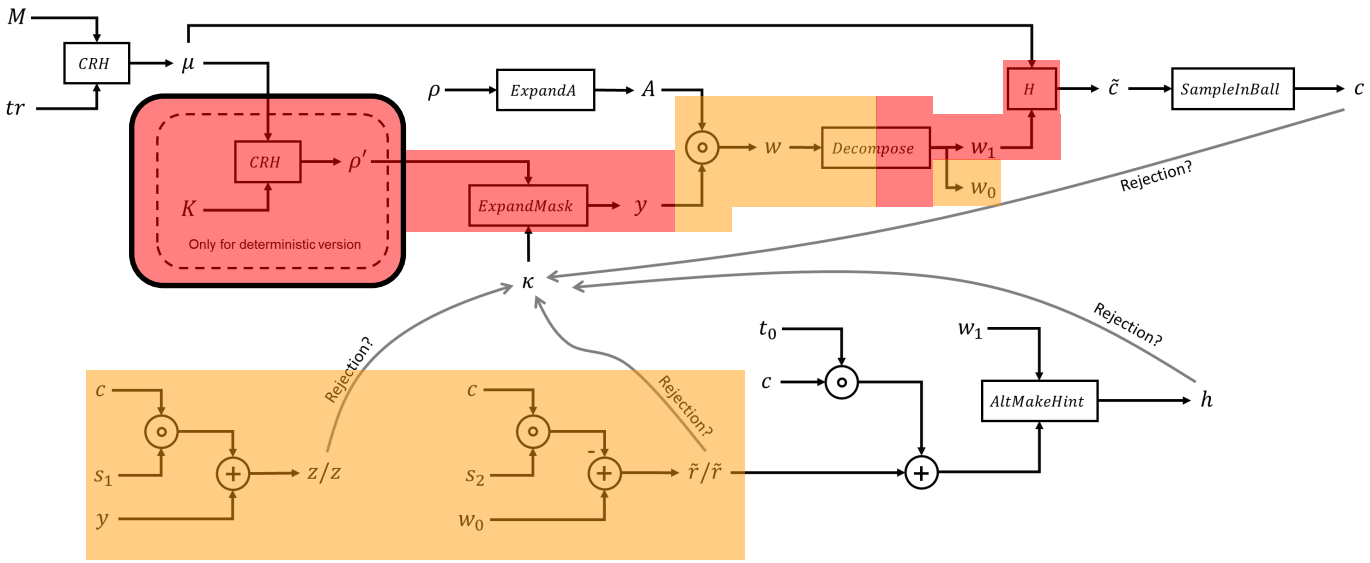
Signature Generation

Observation 1:
Requires a mixture of **Boolean** and **arithmetic** masking with a **prime modulus**

Proposal from [MGTF19]:
Switch from prime to **power-of-two modulus** results in **7x – 9x speed-up**

HOW SHOULD IT BE PROTECTED?

Standard Approach: Masking



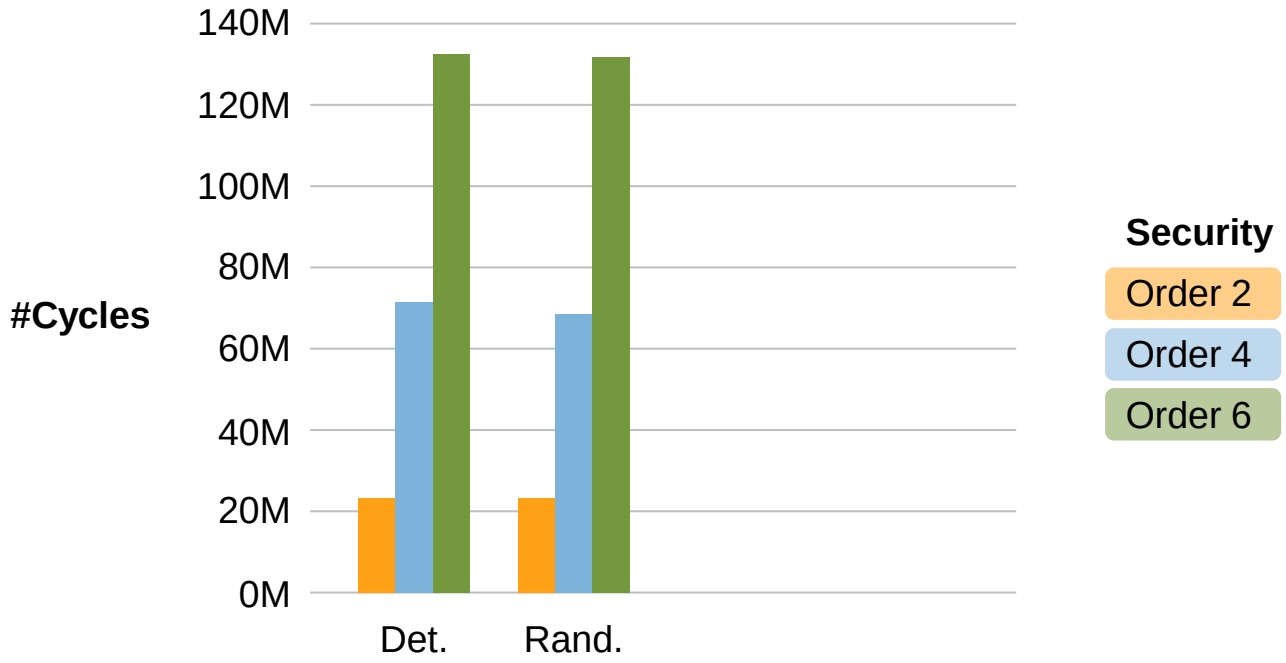
Signature Generation

Observation 2:
Deterministic is much more vulnerable than **randomized** Dilithium.

- Additional long-term secret K
- Measurements can be repeated with same inputs to reduce noise.
- More vulnerable to fault attacks as well.

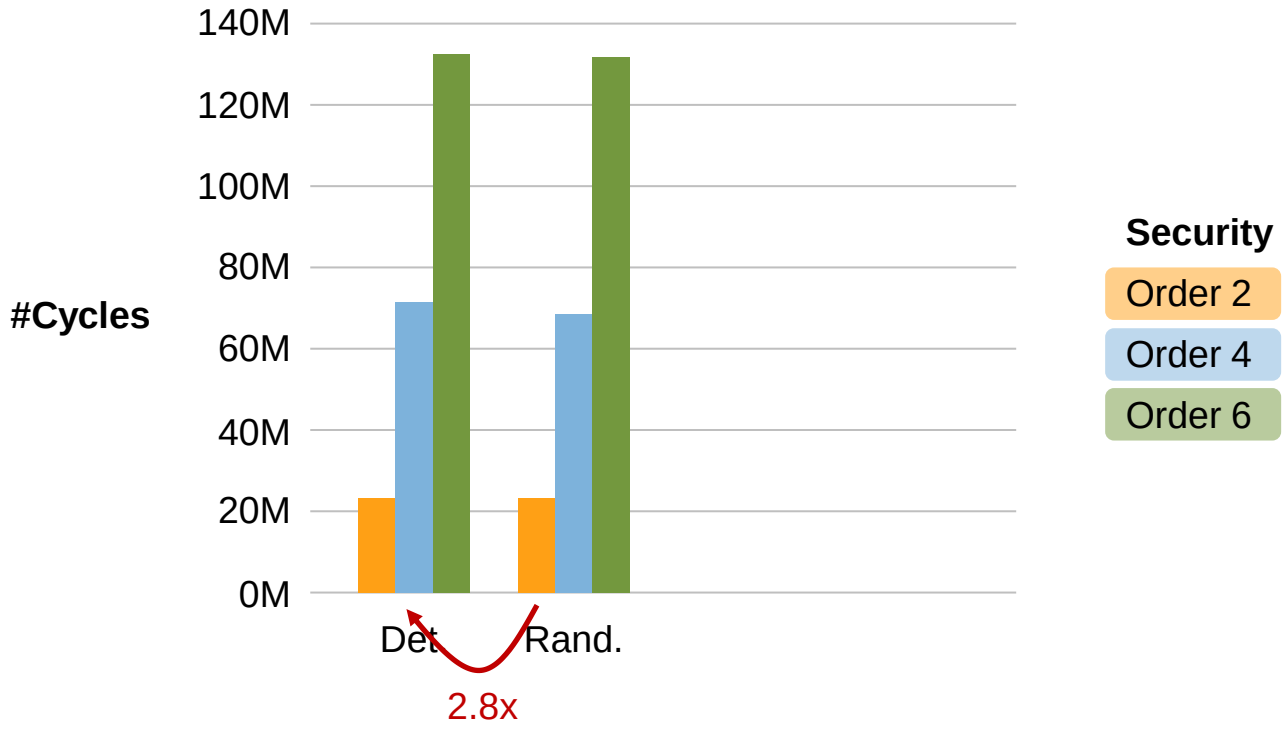
WHAT ARE THE BOTTLENECKS?

Benchmark Masked Dilithium-3 (M4):



WHAT ARE THE BOTTLENECKS?

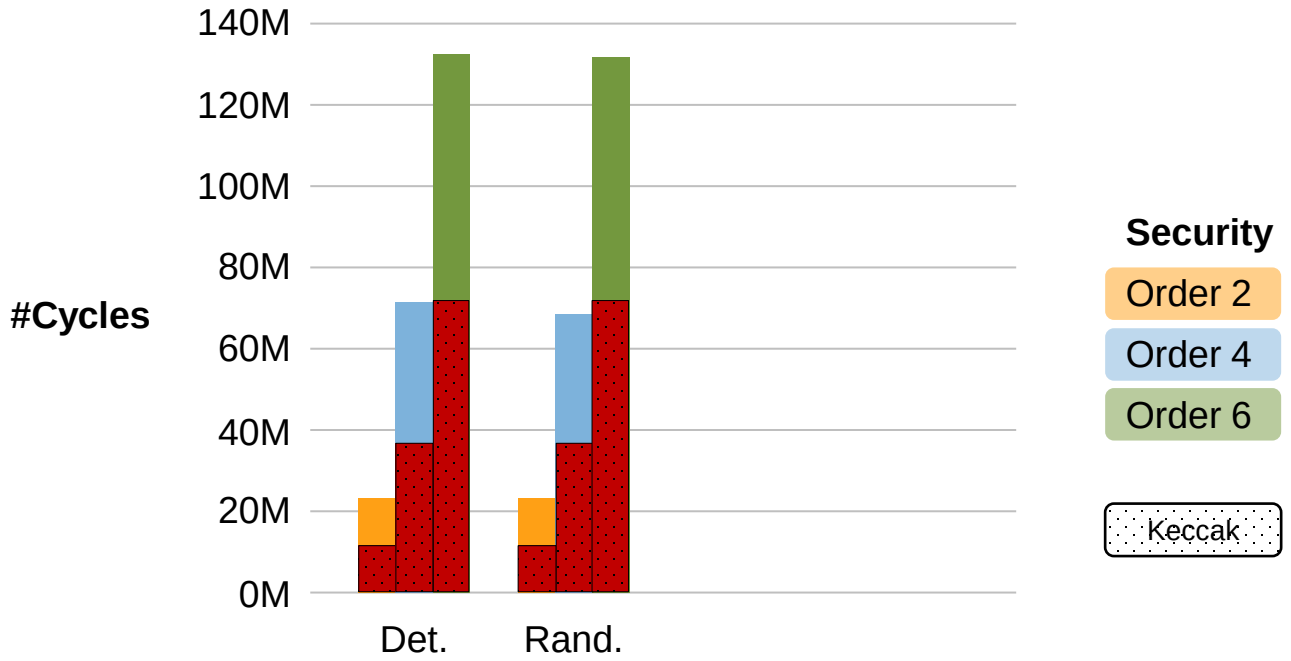
Benchmark Masked Dilithium-3 (M4):



Observation 1:
Deterministic has comparable performance to randomized for **same** security order.
Deterministic requires increased order.
Note: Impacts memory requirements as well.

WHAT ARE THE BOTTLENECKS?

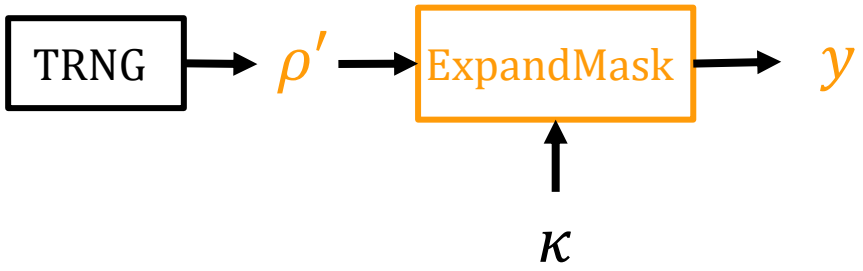
Benchmark Masked Dilithium-3 (M4):



Observation 2:
Protected Keccak for sampling y takes up **50%** of runtime.

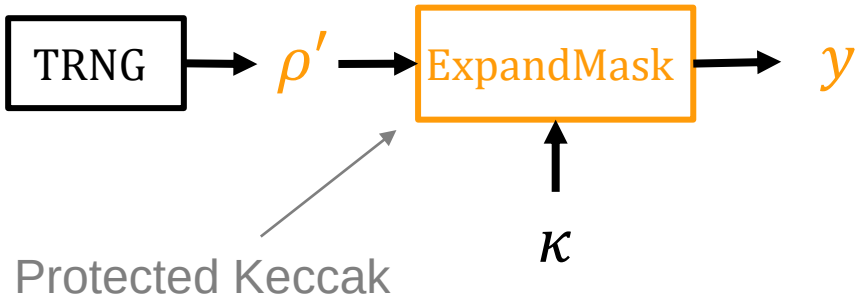
HOW COULD IT BE FIXED?

Randomized:



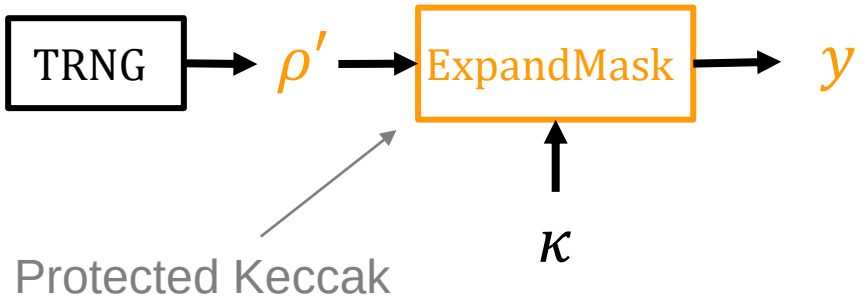
HOW COULD IT BE FIXED?

Randomized:



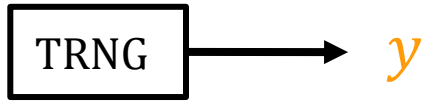
HOW COULD IT BE FIXED?

Randomized:



Flexible-Sampling:

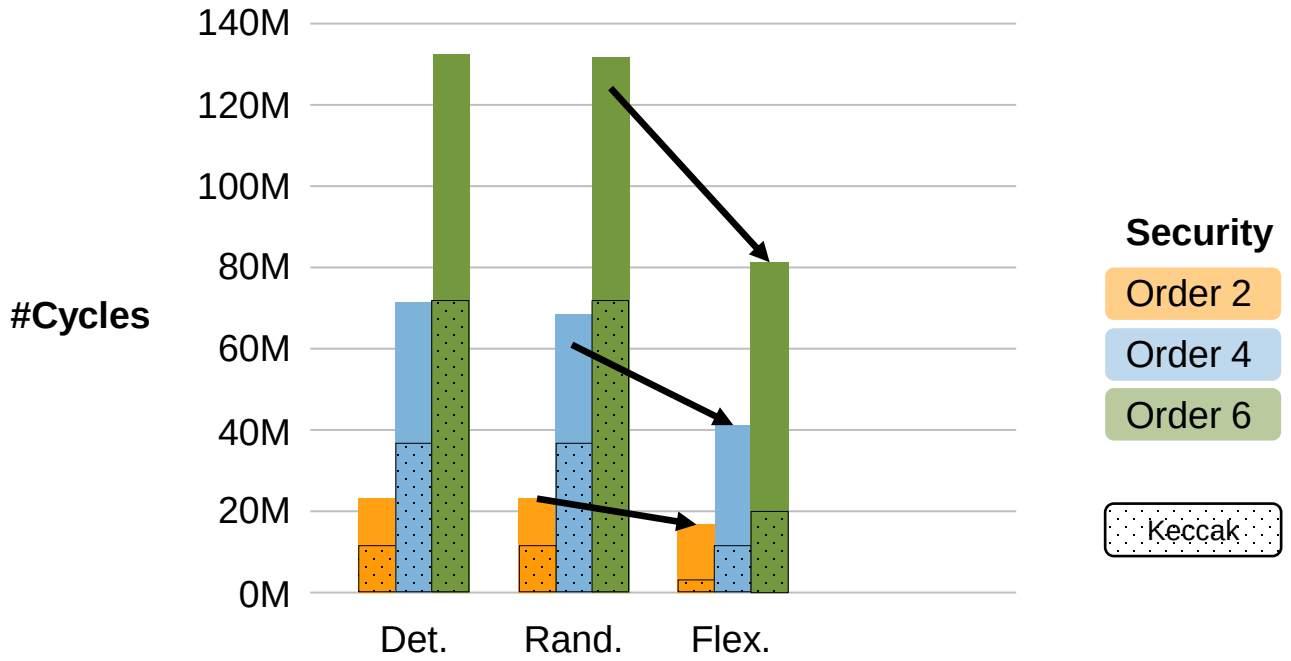
- Does not specify how y is sampled
- Option: Generate shares of y via TRNG



Note: Requires proper TRNG or post-processing

WHAT ARE THE BOTTLENECKS?

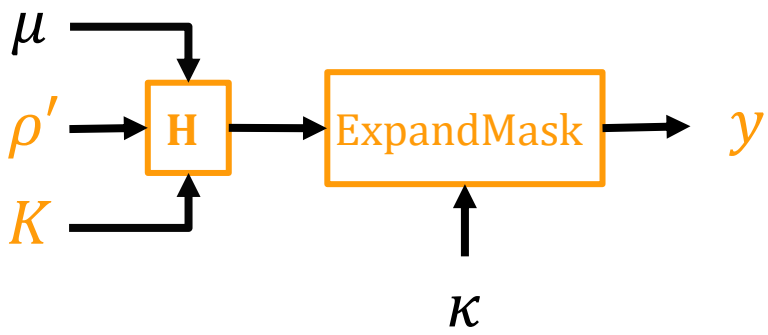
Benchmark Masked Dilithium-3 (M4):



Observation 3:
Flexible-Sampling provides significant speed-up over **randomized**.

WHAT WILL BE DONE?

Hedged:



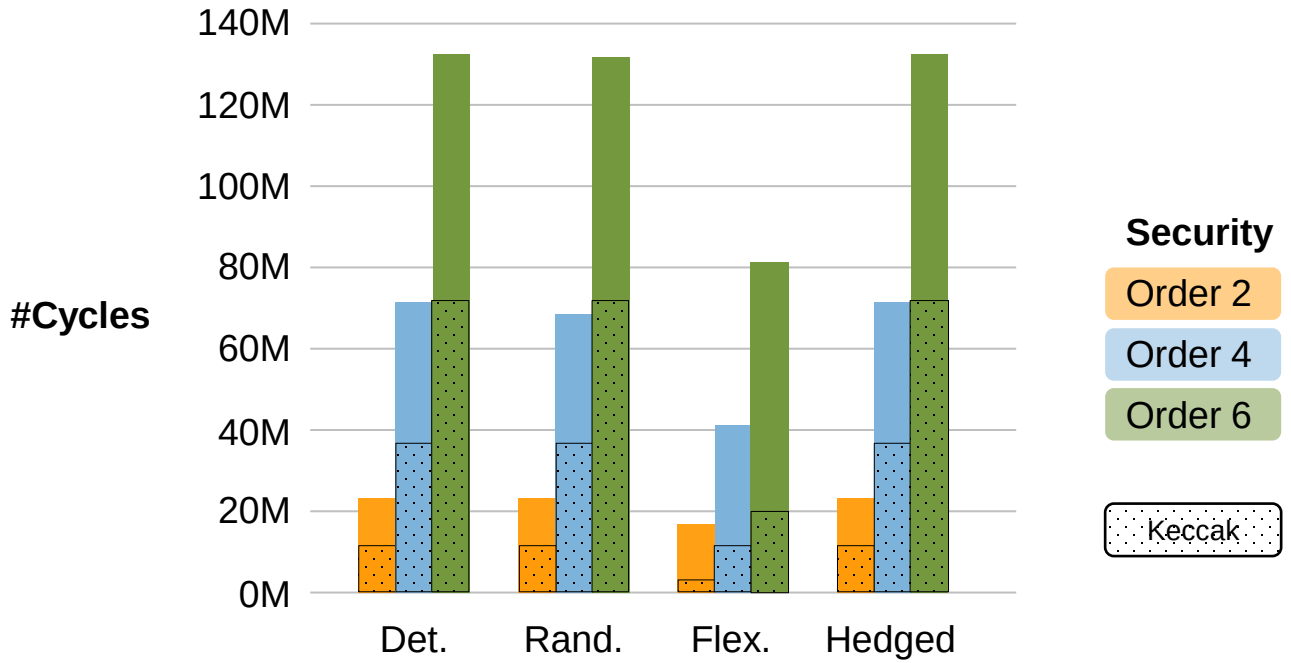
Combined deterministic and randomized Dilithium into one

$\rho' = random\ string$ if randomized Dilithium

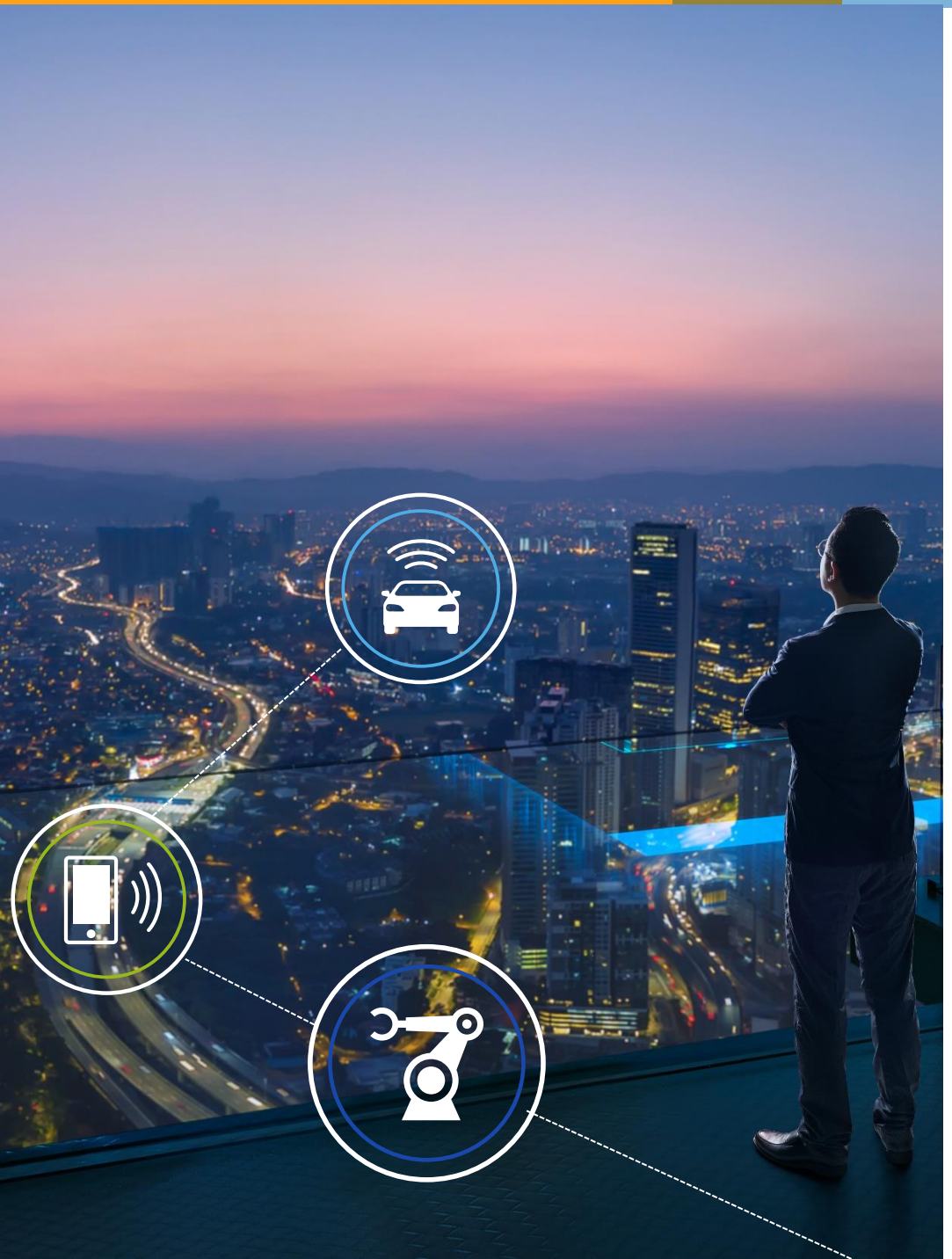
$\rho' =$ "" if deterministic Dilithium

WHAT ARE THE BOTTLENECKS?

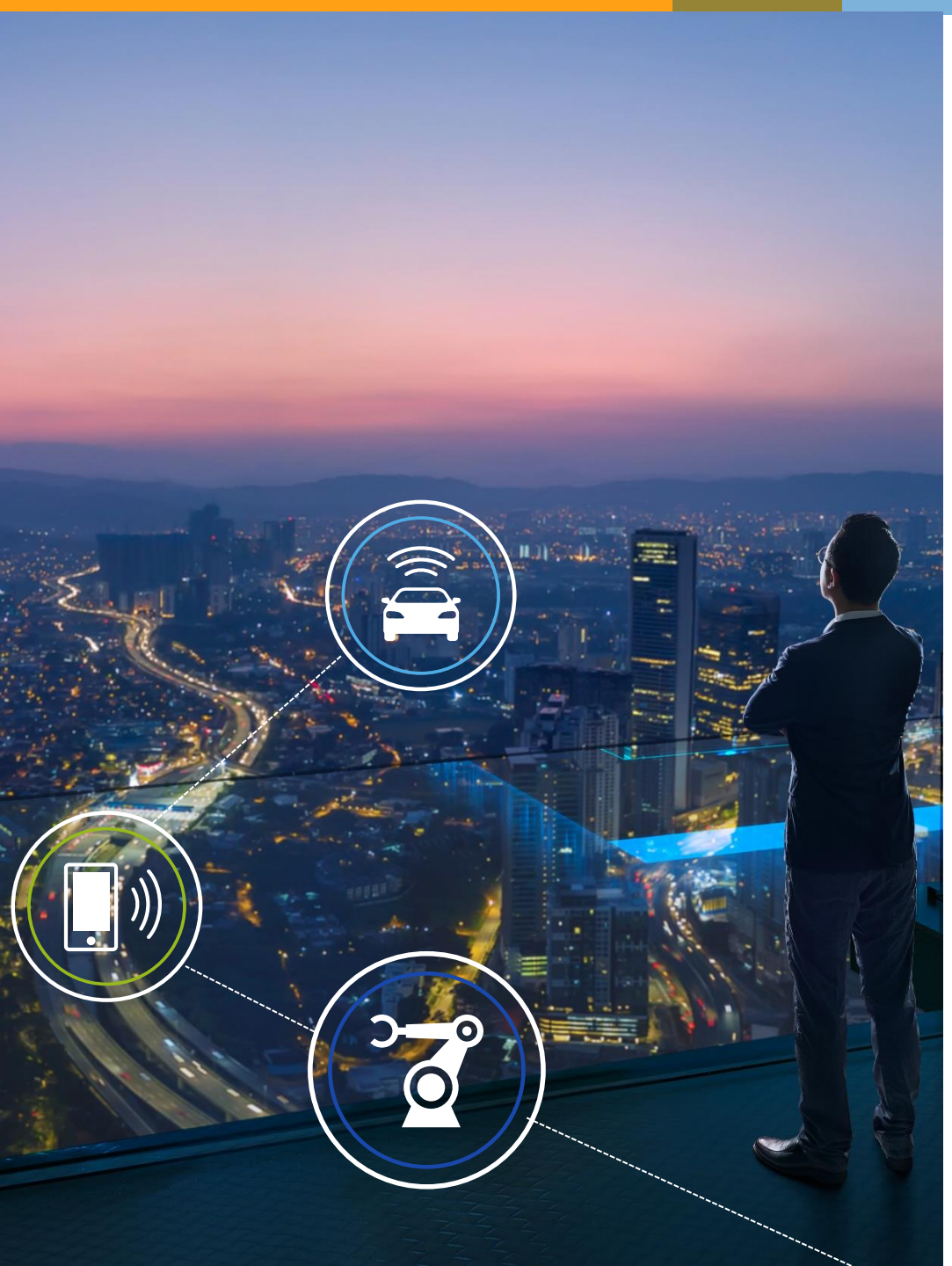
Benchmark Masked Dilithium-3 (M4):



Observation 4:
Hedged (Randomized) provides comparable performance as **randomized.**



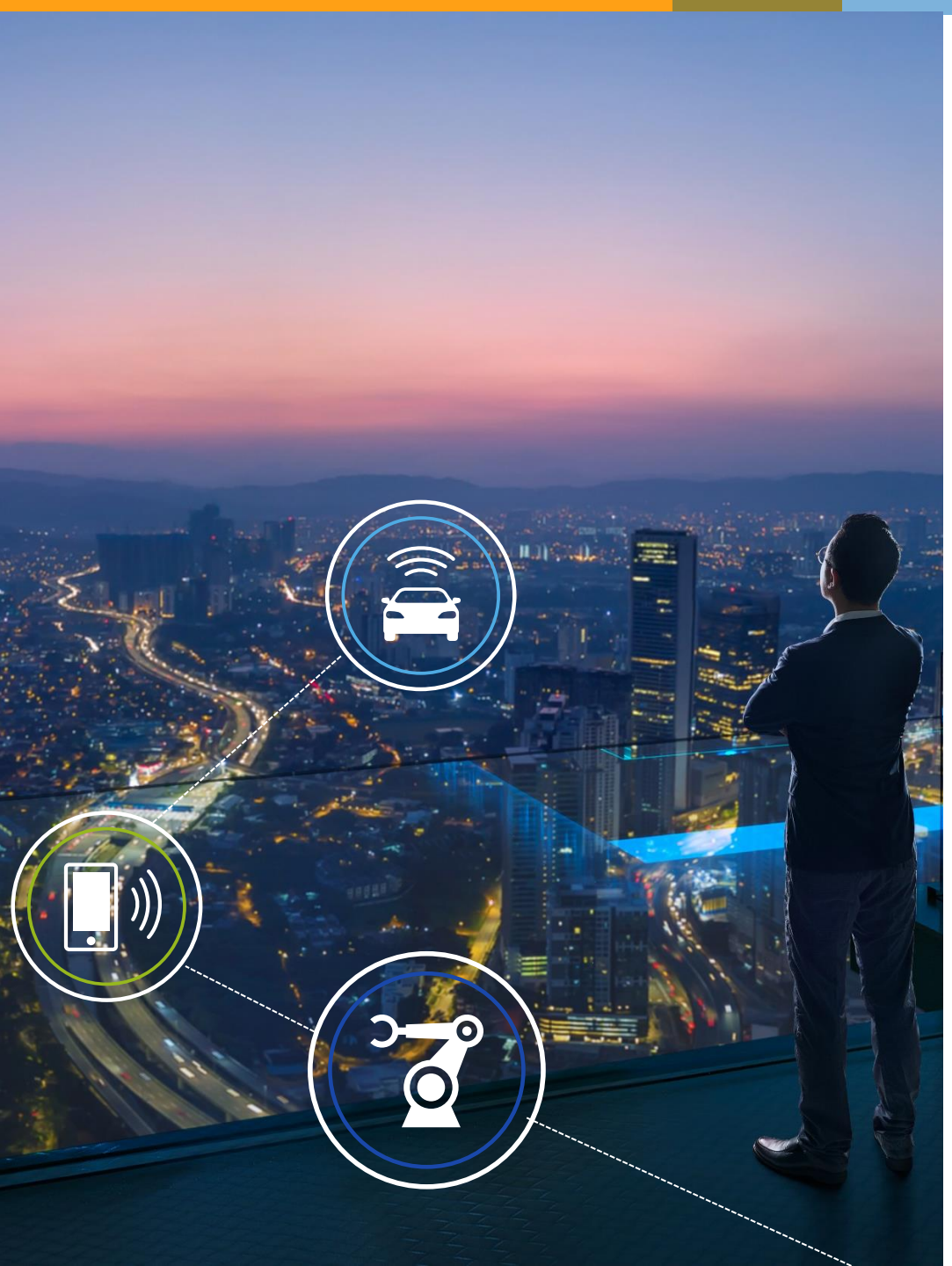
LESSONS LEARNED



LESSONS LEARNED

Randomized should be the default for embedded.

Hedged has negligible impact on runtime.

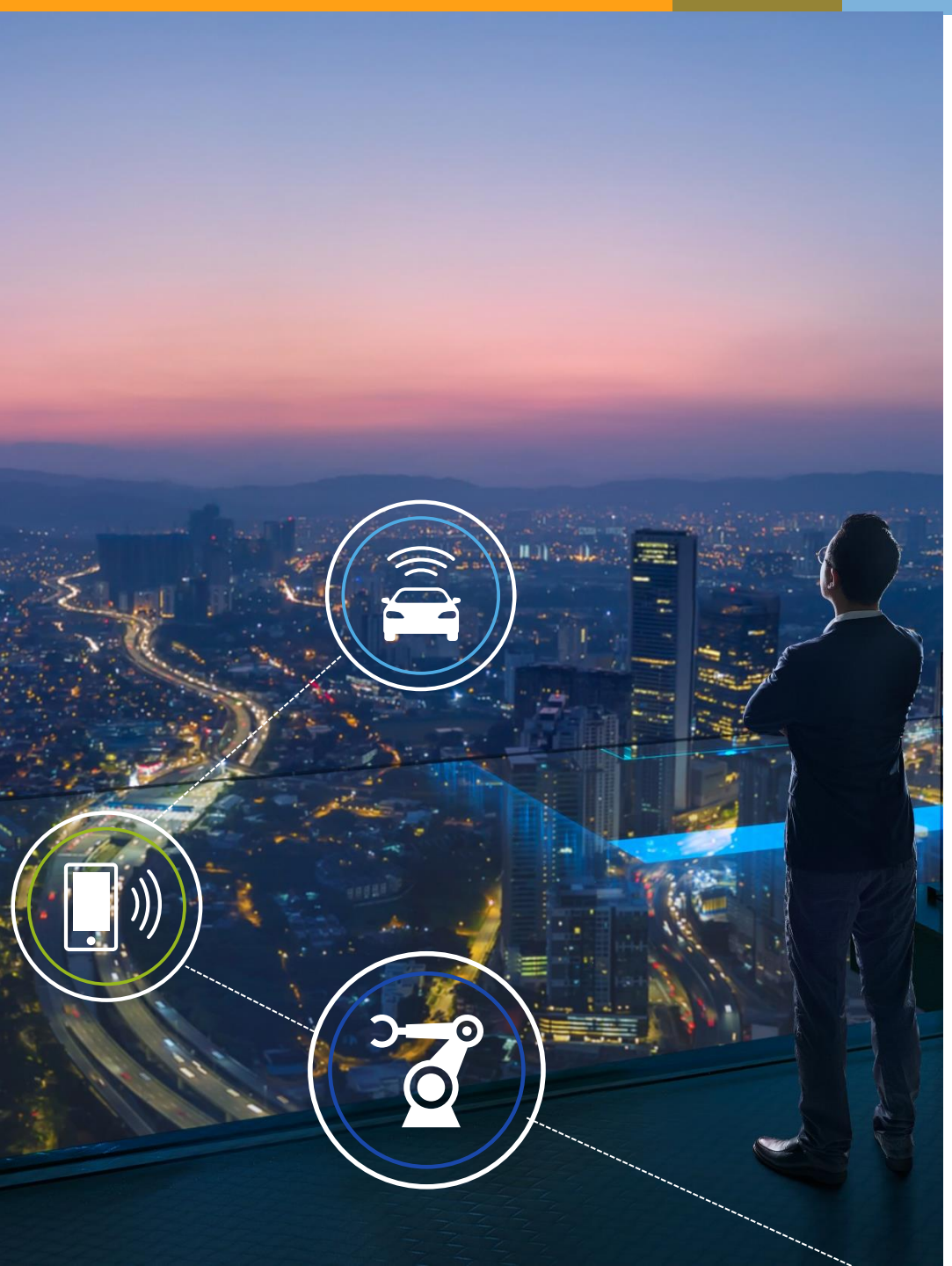


LESSONS LEARNED

Randomized should be the default for embedded.

Hedged has negligible impact on runtime.

Flexible sampling would enable significant speed-up.



LESSONS LEARNED

Randomized should be the default for embedded.

Hedged has negligible impact on runtime.

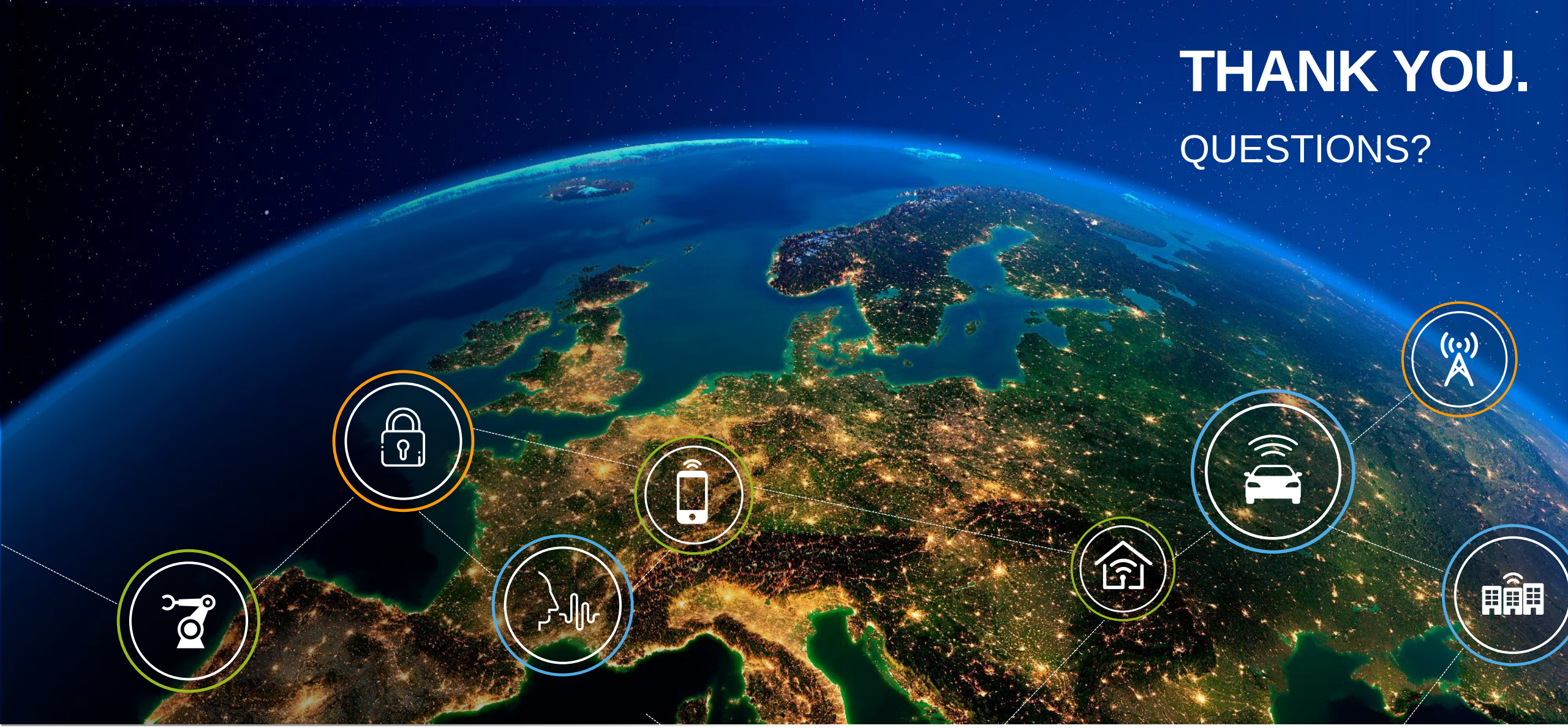
Flexible sampling would enable significant speed-up.

Hardening Dilithium still not mature.

Much less studied than Kyber.

THANK YOU.

QUESTIONS?



SECURE CONNECTIONS
FOR A SMARTER WORLD

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