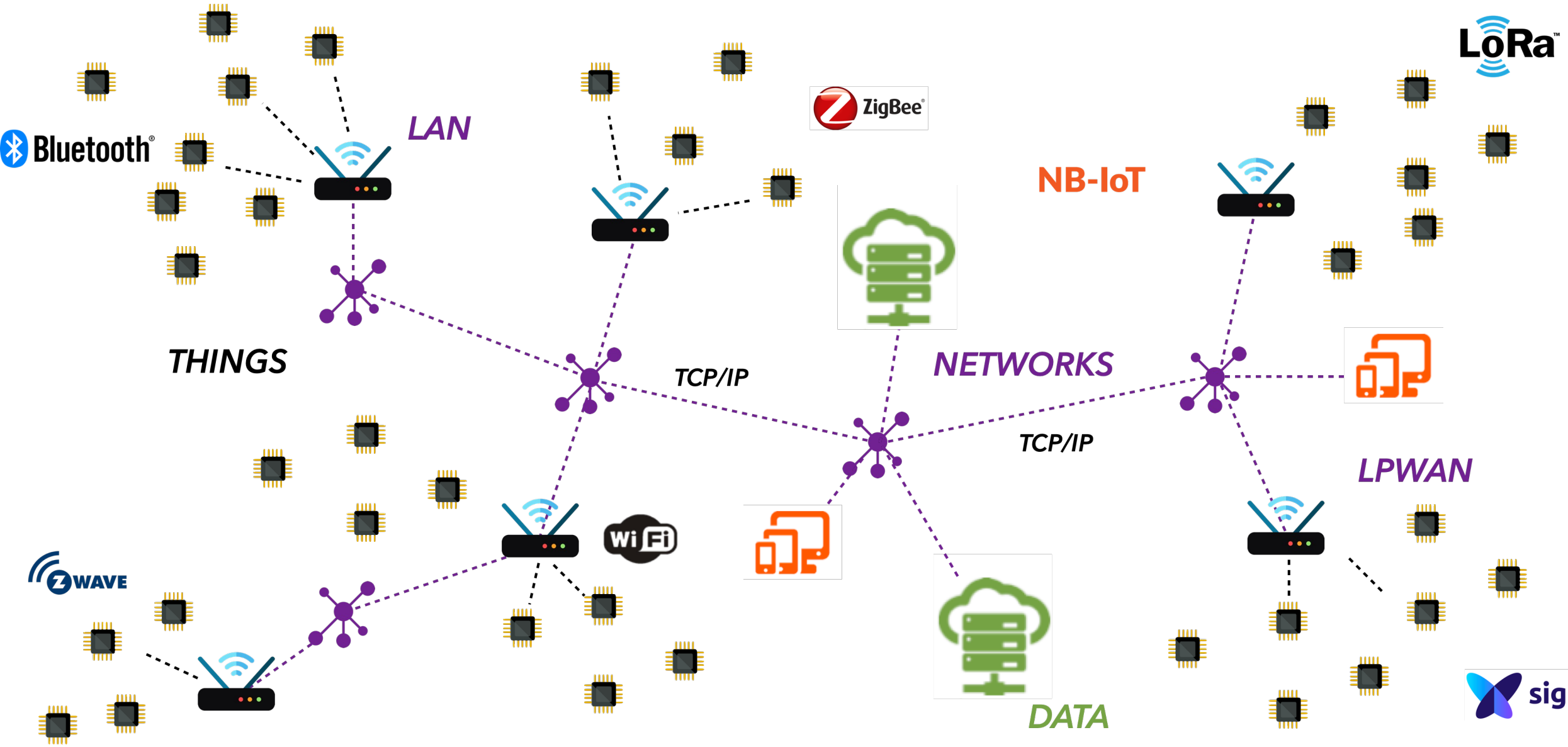
De la vulnérabilité des nœuds capteurs à la certification des transactions sur le réseau, une approche de la sécurisation de l'Internet des Objets

Présentée par Loïc Dalmasso

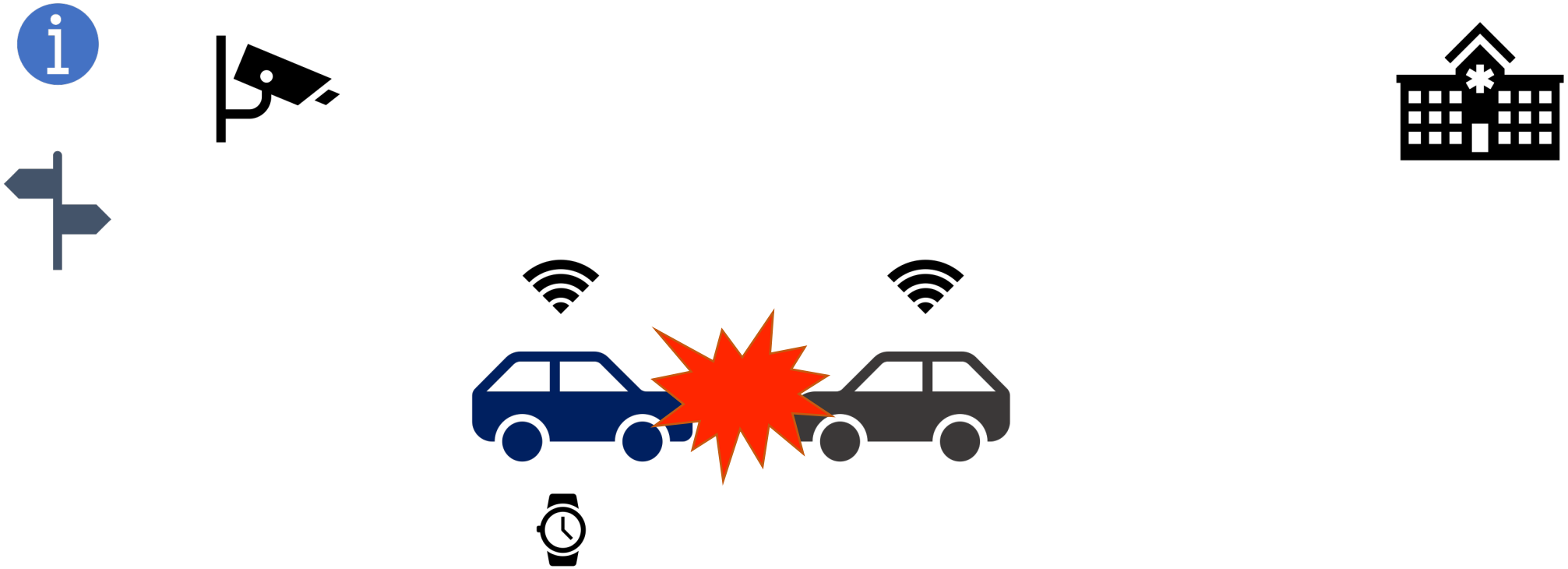
Devant le jury composé de

Pascal Benoit	Maître de Conférences, Université de Montpellier	Directeur de thèse
Florent Bruguier	Maître de Conférences, Université de Montpellier	Examinateur
Loïc Lagadec	Professeur, ENSTA-Bretagne	Rapporteur
Lionel Torres	Professeur, Université de Montpellier	Examinateur
Assia Tria	Directrice Scientifique, CEA-Leti	Examinatrice
François Verdier	Professeur, Université de Nice	Rapporteur

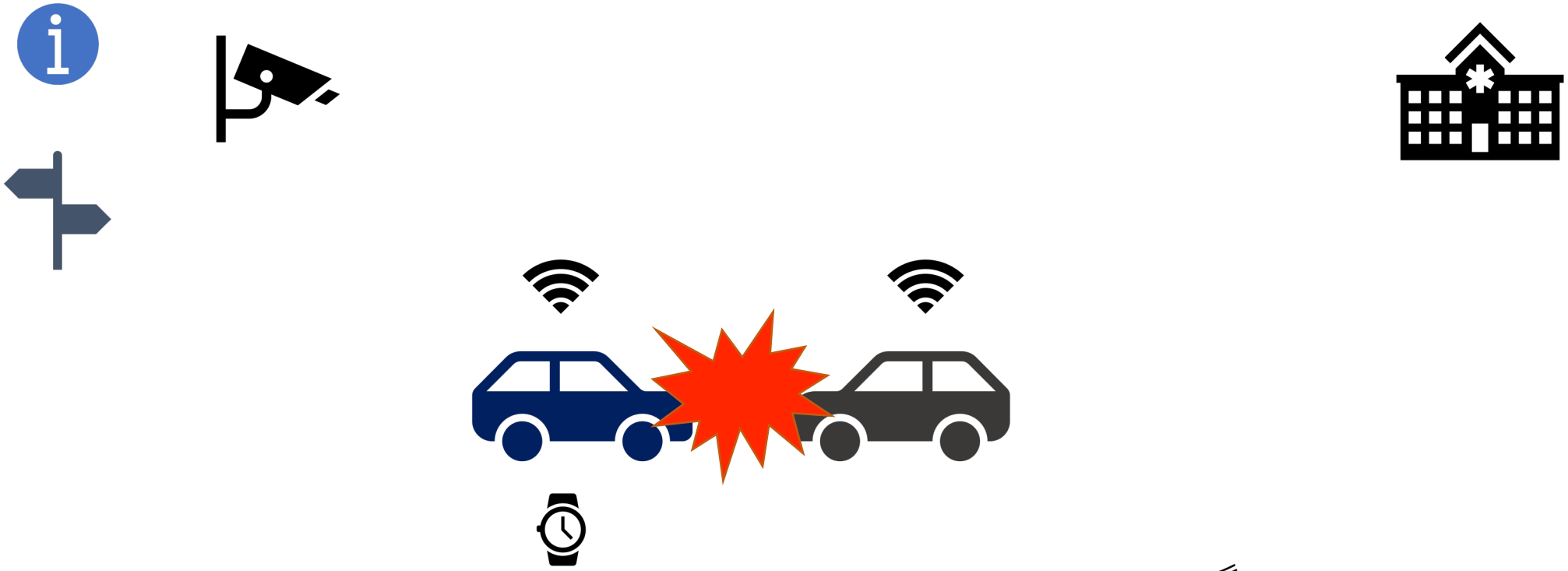
Internet of Things, an Hyperconnected and Heterogeneous Environment



Internet of Things, an Hyperconnected and Heterogeneous Environment



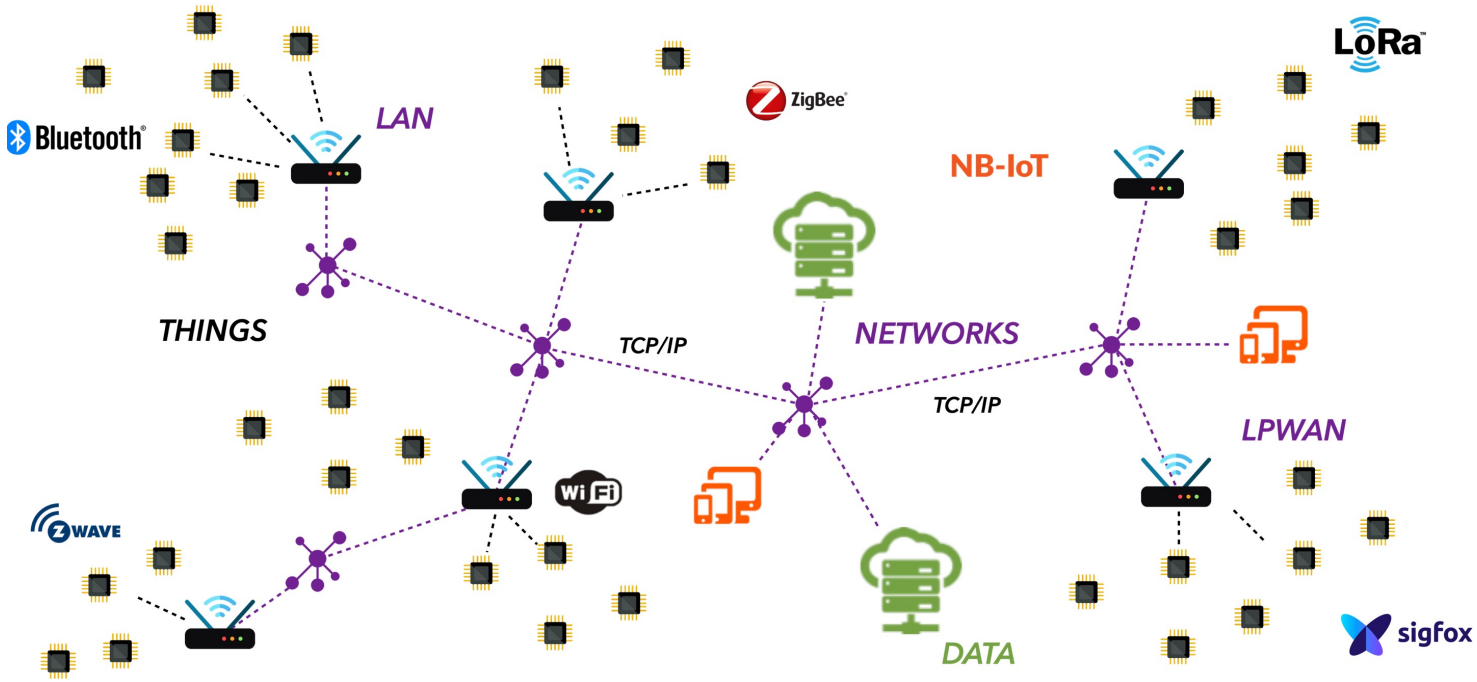
Internet of Things, an Hyperconnected and Heterogeneous Environment



COSIC

Source: https://www.wired.com/story/tesla-model-x-hack-bluetooth/

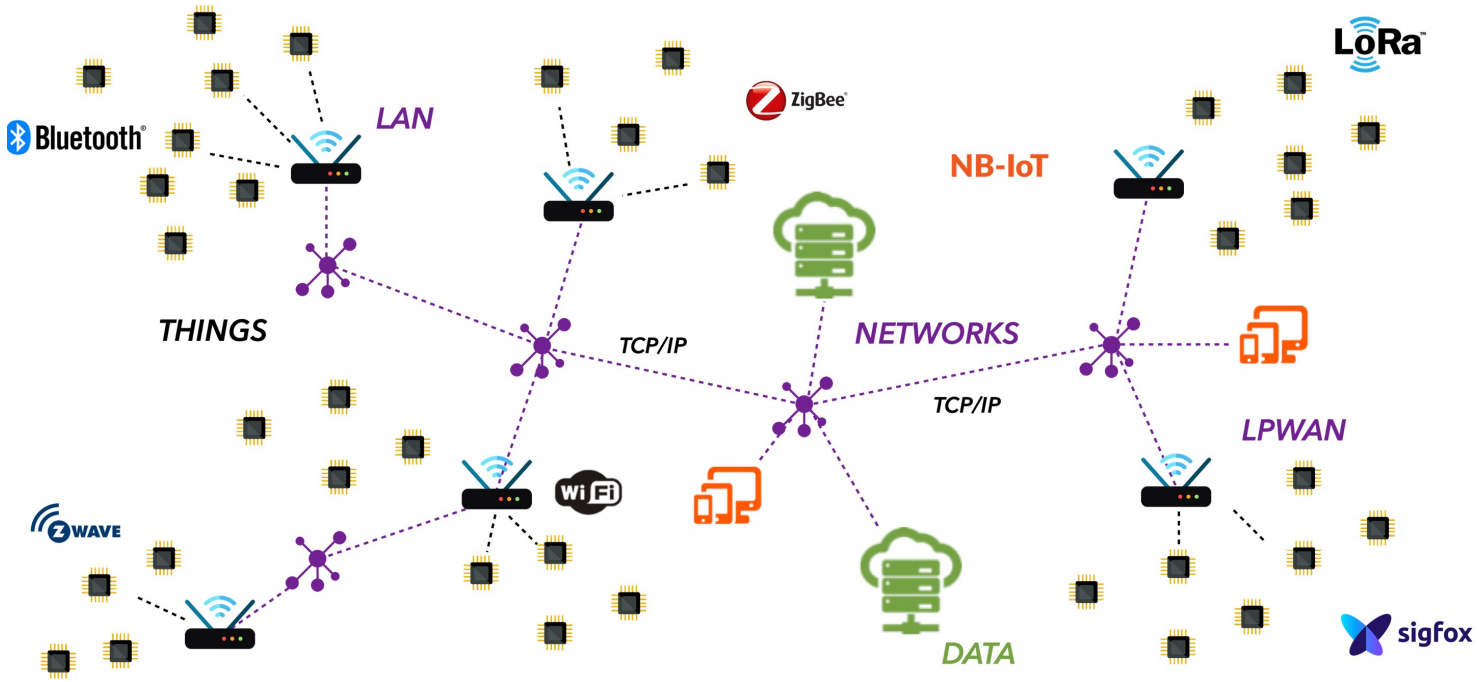
Security for Internet of Things



Ensure the confidentiality on very constrained devices

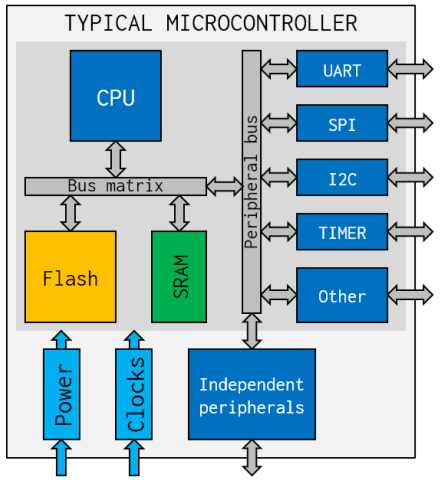
Ensure the trust in a decentralized network

Ensure the Confidentiality on Very Constrained Devices



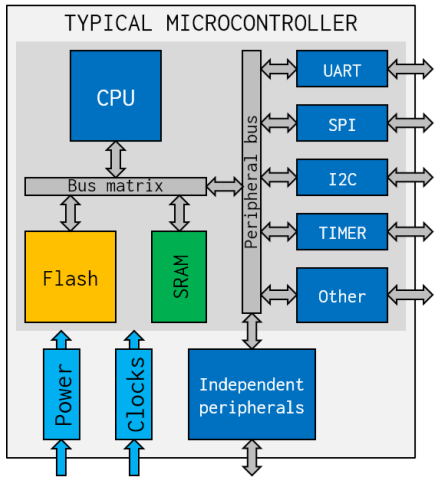
Ensure the confidentiality on very constrained devices

Ensure the Confidentiality on Very Constrained Devices



Size **Computing Power** **Memory** **Energy**

Ensure the Confidentiality on Very Constrained Devices



Size **Computing Power** **Memory** **Energy**

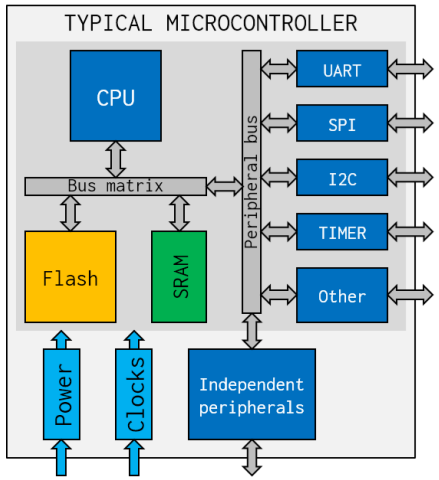
AES-128 (Software)		
Paper	Architecture	Cycles
D.Dinu et al. (*FELICS*)	ARM 32-bit	20 265

CSMA/CA Algorithm		
Paper	SoC	Cycles
C. Del-Valle-Soto *et al.*	TI CC2530	~30 000

AES-128 (Hardware)		
Paper	Platform	# LUT-6 Input
N.Hanley *et al.*	Virtex-5	1 266

ARM Cortex-M0		
Paper	Platform	# LUT-6 Input
G.Patrigeon *et al.*	Artix-7	3 224

Ensure the Confidentiality on Very Constrained Devices



Size **Computing Power** **Memory** **Energy**

Which algorithm achieves the most efficient hardware implementation ?

$$Area$$

$$Throughput = \frac{Data_{size}}{NB_{Rounds}} \times Freq$$

$$Efficiency = \frac{Throughput}{Area}$$

$$Success\ Rate$$

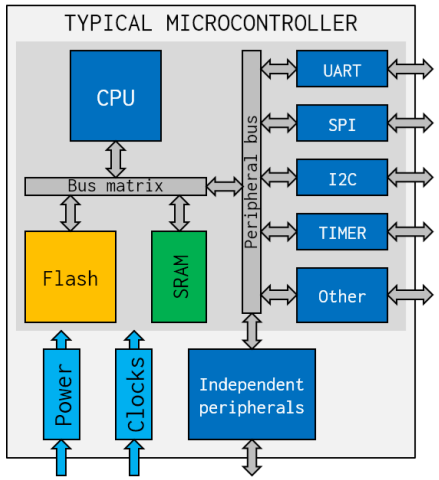
AES-128 (Software)		
Paper	Architecture	Cycles
D.Dinu et al. (*FELICS*)	ARM 32-bit	20 265

CSMA/CA Algorithm		
Paper	SoC	Cycles
C. Del-Valle-Soto *et al.*	TI CC2530	~30 000

AES-128 (Hardware)		
Paper	Platform	# LUT-6 Input
N.Hanley *et al.*	Virtex-5	1 266

ARM Cortex-M0		
Paper	Platform	# LUT-6 Input
G.Patrigeon *et al.*	Artix-7	3 224

Ensure the Confidentiality on Very Constrained Devices



Size **Computing Power** **Memory** **Energy**

Which algorithm achieves the most efficient hardware implementation ?

$$Area$$

$$Throughput = \frac{Data_{size}}{NB_{Rounds}} \times Freq$$

$$Efficiency = \frac{Throughput}{Area}$$

$$Success\ Rate$$

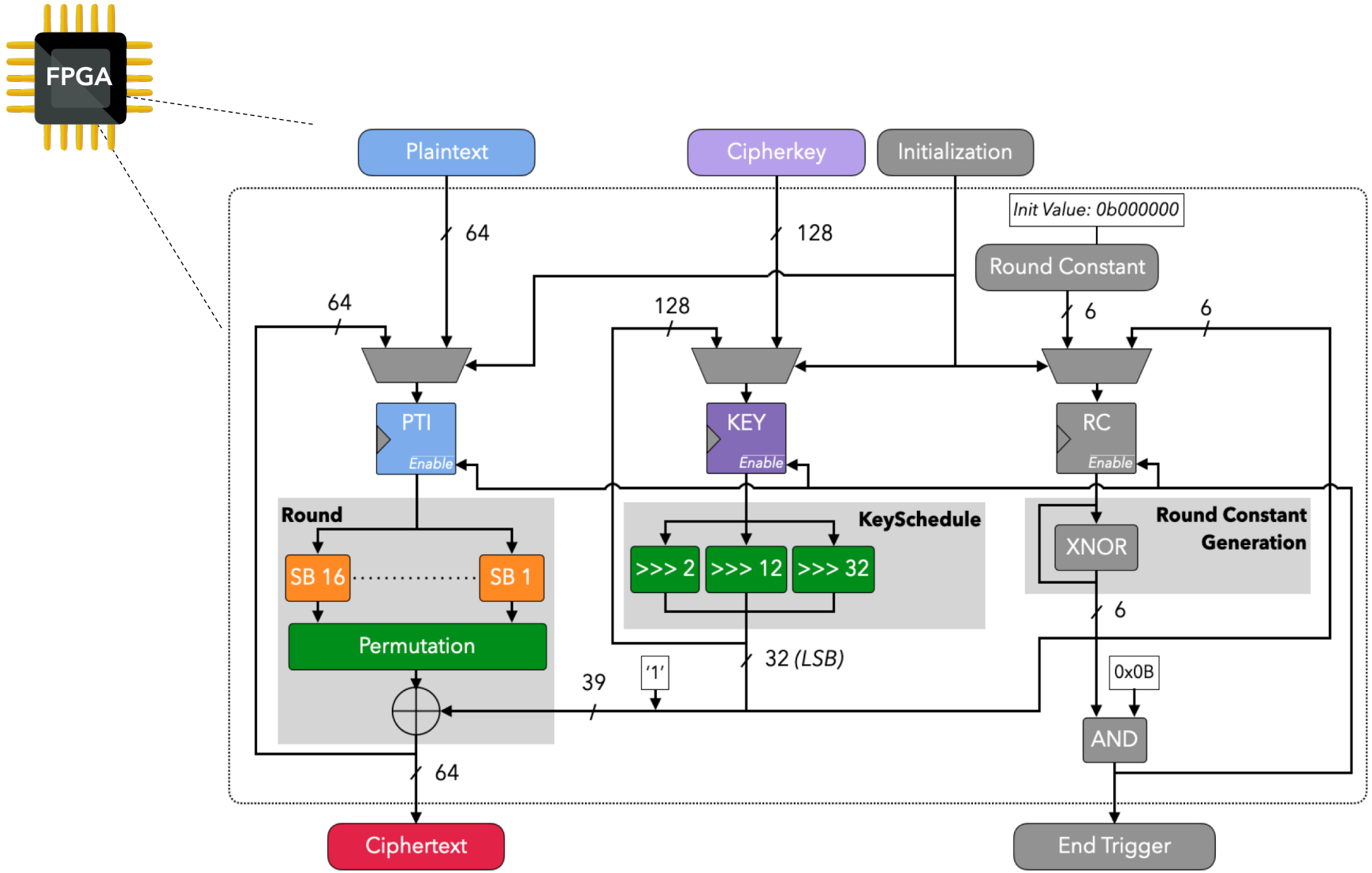
AES-128 (Software)		
Paper	Architecture	Cycles
D.Dinu et al. (*FELICS*)	ARM 32-bit	20 265

CSMA/CA Algorithm		
Paper	SoC	Cycles
C. Del-Valle-Soto *et al.*	TI CC2530	~30 000

AES-128 (Hardware)		
Paper	Platform	# LUT-6 Input
N.Hanley *et al.*	Virtex-5	1 266

ARM Cortex-M0		
Paper	Platform	# LUT-6 Input
G.Patrigeon *et al.*	Artix-7	3 224

FPGA Prototyping



State of the Art Comparisons

AES-128			
Papers	Platform	Freq (MHz)	Area (Slices)
N.Hanley *et al.*	Virtex-5	96	359
A.Aghaie *et al.*	Artix-7	141	530
This Work		**166**	**412**

PRESENT-128			
Papers	Platform	Freq (MHz)	Area (Slices)
C. A. Lara-Nino *et al.*	Artix-7	145	66
This Work		**285**	**73**

GIFT-64-128			
Papers	Platform	Freq (MHz)	Area (Slices)
C. A. Lara-Nino *et al.*	Artix-7	218	52
This Work		**319**	**59**

State of the Art Comparisons

AES-128				
Papers	Platform	Freq (MHz)	Area (Slices)	Efficiency @ 13.56MHz (Mbps/Slices)
N.Hanley *et al.*	Virtex-5	96	359	0.5
A.Aghaie *et al.*	Artix-7	141	530	0.3
This Work		**166**	**412**	**0.4**

PRESENT-128			
Papers	Platform	Freq (MHz)	Area (Slices)
C. A. Lara-Nino *et al.*	Artix-7	145	66
This Work		**285**	**73**

GIFT-64-128			
Papers	Platform	Freq (MHz)	Area (Slices)
C. A. Lara-Nino *et al.*	Artix-7	218	52
This Work		**319**	**59**

State of the Art Comparisons

AES-128				
Papers	Platform	Freq (MHz)	Area (Slices)	Efficiency @ 13.56MHz (Mbps/Slices)
N.Hanley *et al.*	Virtex-5	96	359	0.5
A.Aghaie *et al.*	Artix-7	141	530	0.3
This Work		**166**	**412**	**0.4**

PRESENT-128				
Papers	Platform	Freq (MHz)	Area (Slices)	Efficiency @ 13.56MHz (Mbps/Slices)
C. A. Lara-Nino *et al.*	Artix-7	145	66	0.4
This Work		**285**	**73**	**0.4**

GIFT-64-128			
Papers	Platform	Freq (MHz)	Area (Slices)
C. A. Lara-Nino *et al.*	Artix-7	218	52
This Work		**319**	**59**

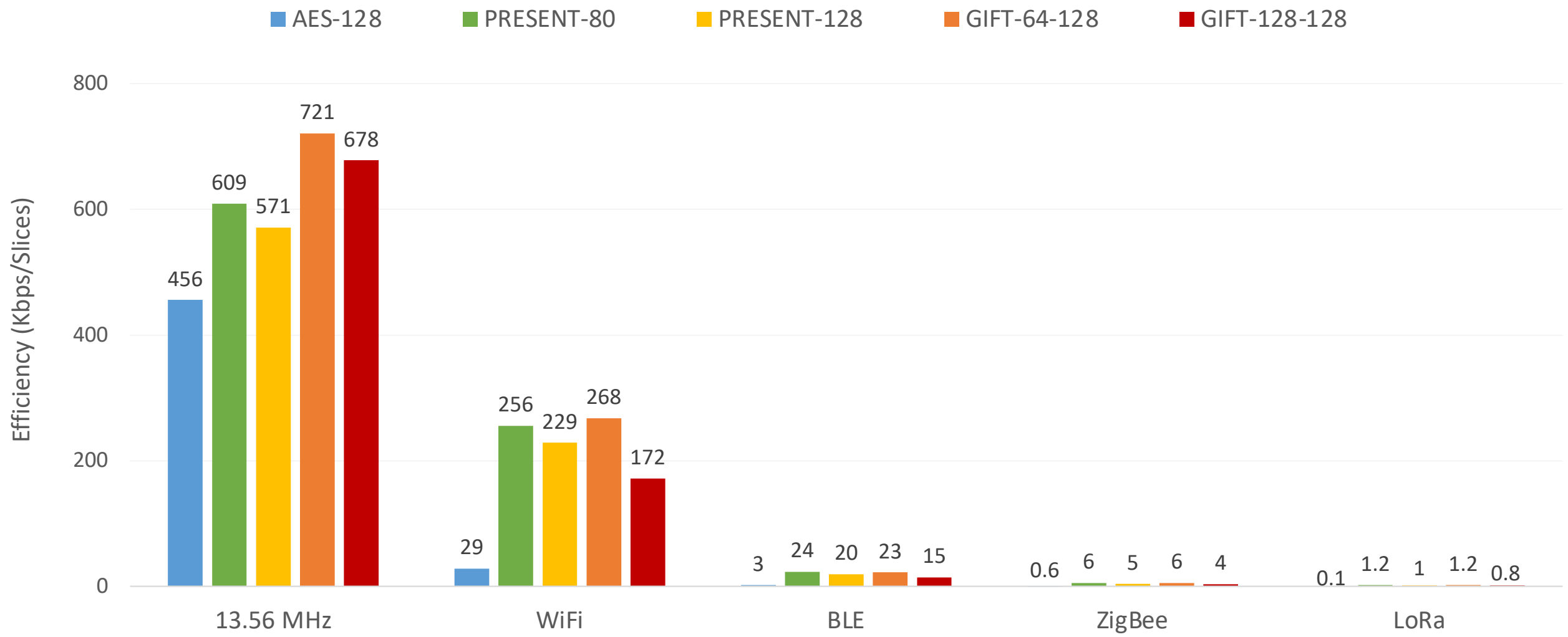
State of the Art Comparisons

AES-128				
Papers	Platform	Freq (MHz)	Area (Slices)	Efficiency @ 13.56MHz (Mbps/Slices)
N.Hanley *et al.*	Virtex-5	96	359	0.5
A.Aghaie *et al.*	Artix-7	141	530	0.3
This Work		**166**	**412**	**0.4**

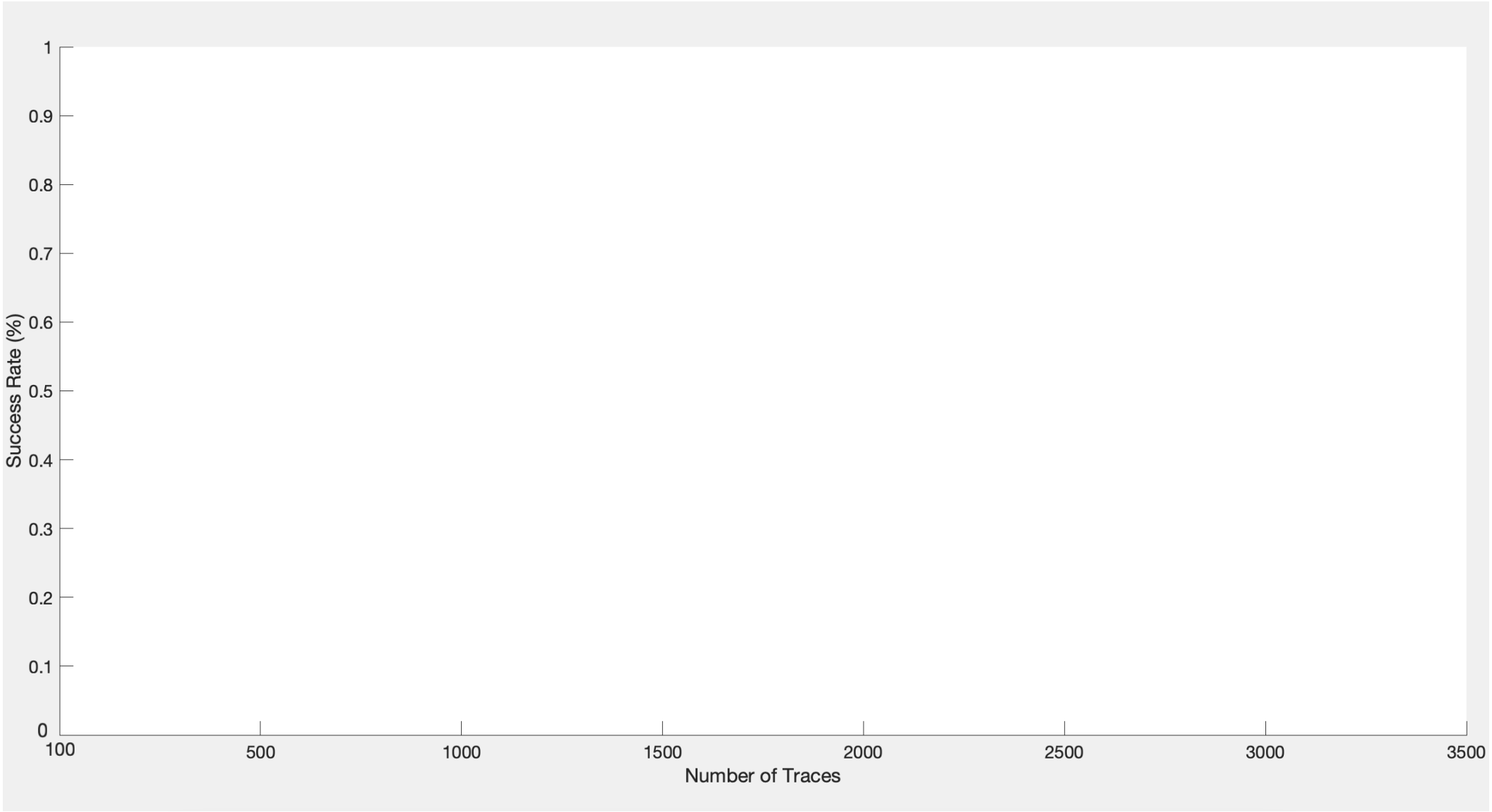
PRESENT-128				
Papers	Platform	Freq (MHz)	Area (Slices)	Efficiency @ 13.56MHz (Mbps/Slices)
C. A. Lara-Nino *et al.*	Artix-7	145	66	0.4
This Work		**285**	**73**	**0.4**

GIFT-64-128				
Papers	Platform	Freq (MHz)	Area (Slices)	Efficiency @ 13.56MHz (Mbps/Slices)
C. A. Lara-Nino *et al.*	Artix-7	218	52	0.6
This Work		**319**	**59**	**0.5**

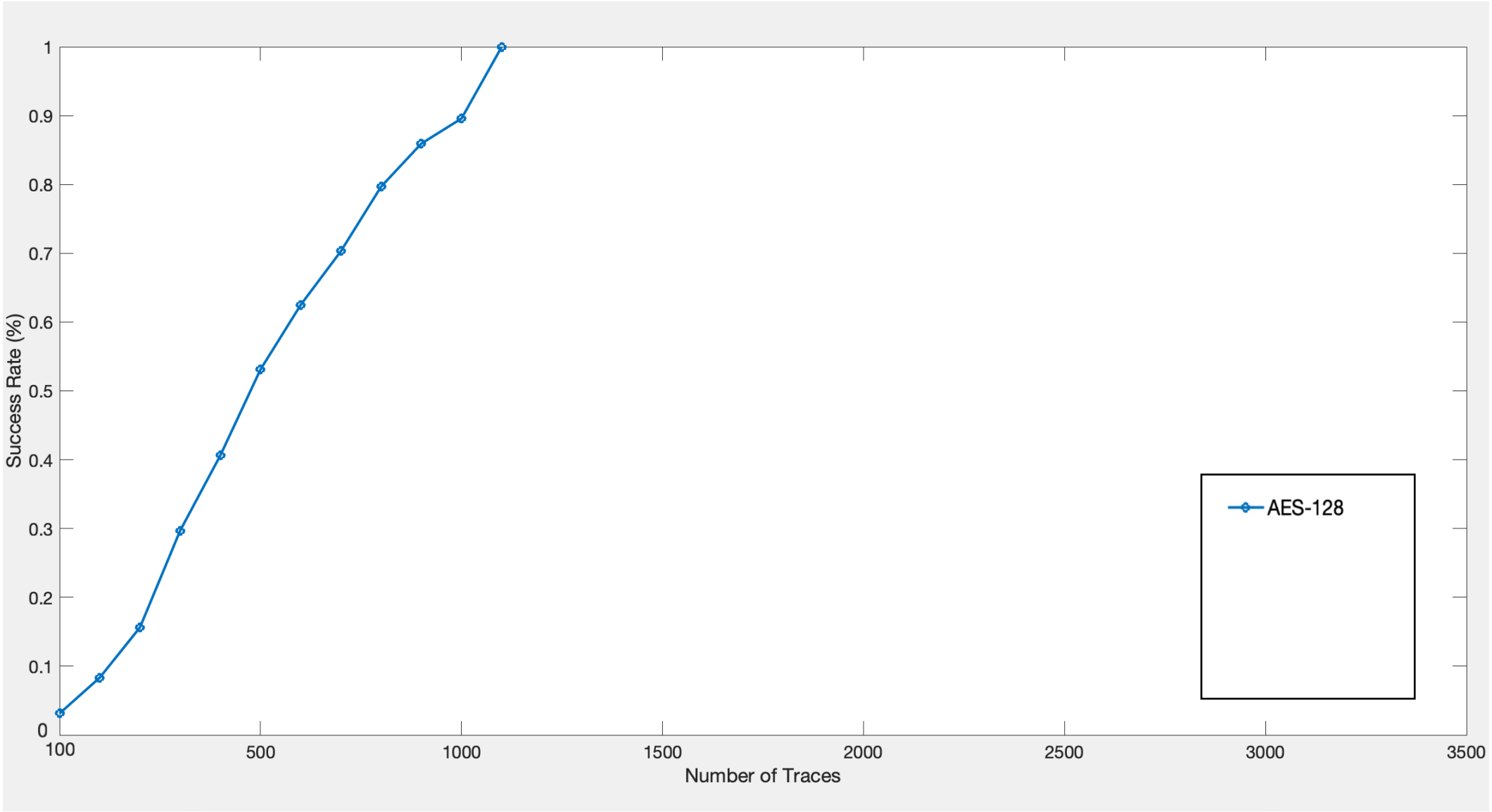
Crypto-Ciphers Performances Evaluations



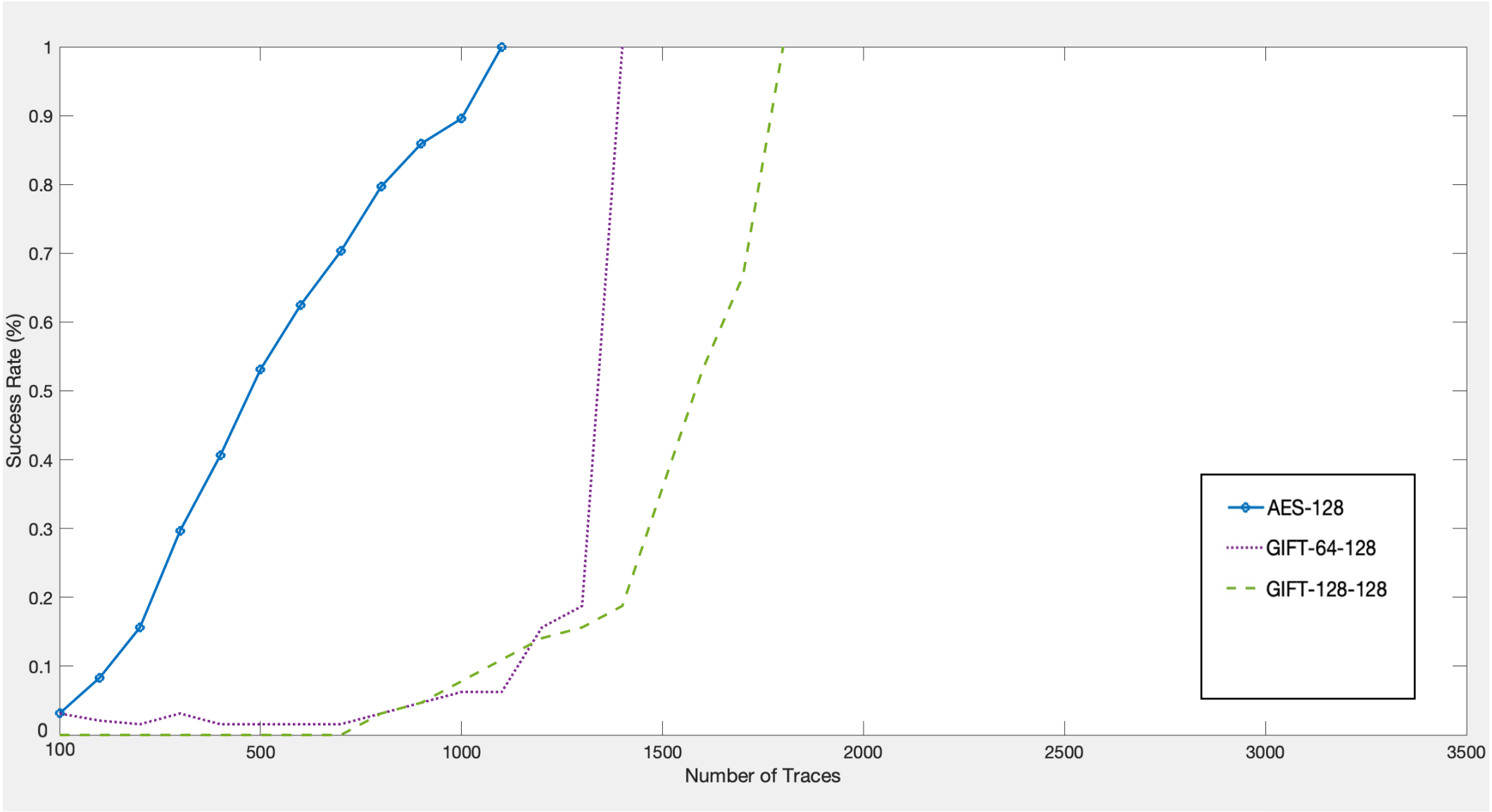
Crypto-Ciphers Robustness Evaluations



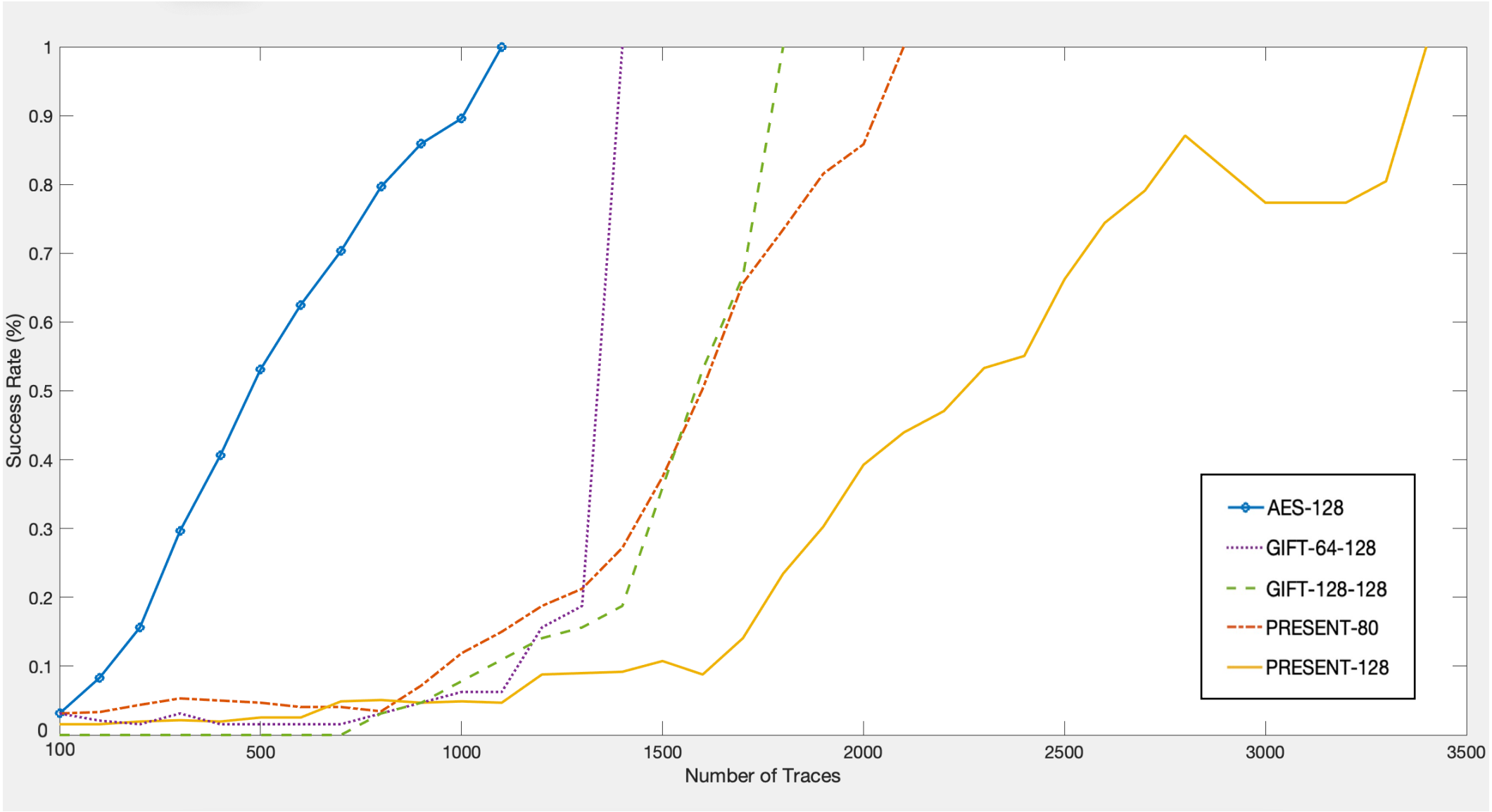
Crypto-Ciphers Robustness Evaluations



Crypto-Ciphers Robustness Evaluations



Crypto-Ciphers Robustness Evaluations



Crypto-Ciphers Evaluations Summary

Which algorithm achieves the most efficient hardware implementation ?

AES-128: **the least efficient (58%)**
the least resistant (÷ 3)

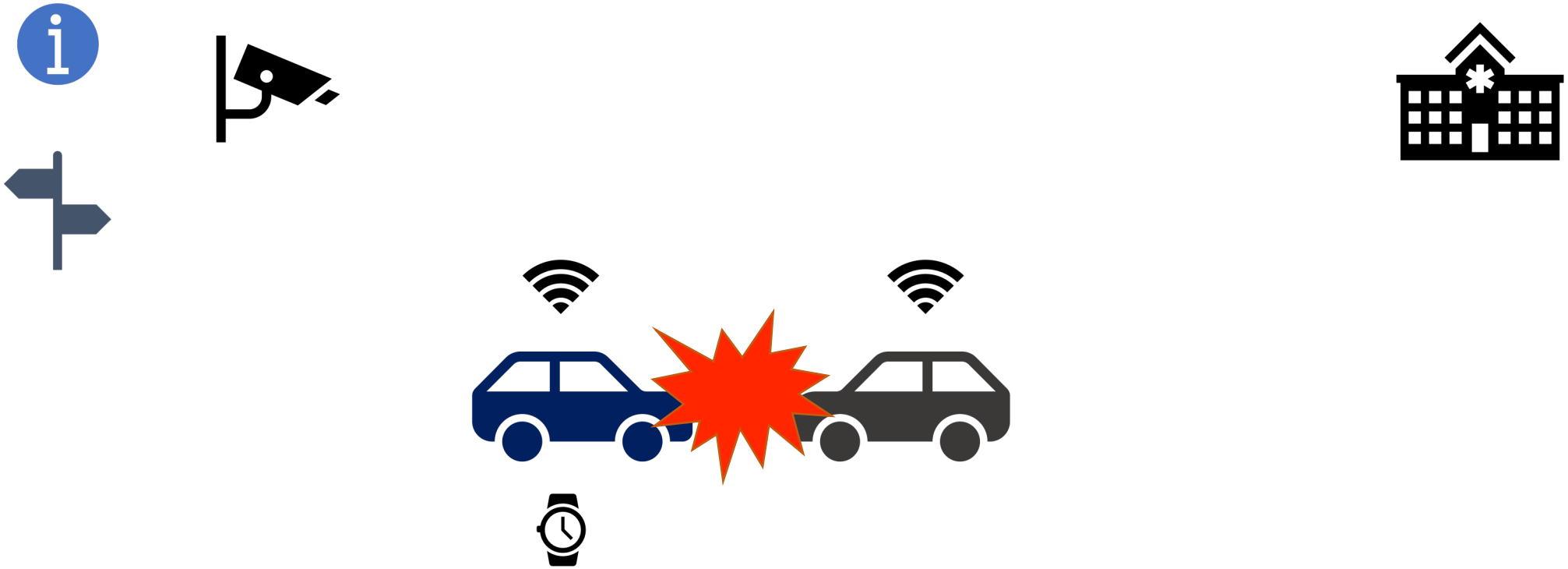
GIFT-64-128: **the best efficient (26% PRESENT-128)**

PRESENT-128: **the most resistant (x3 AES, x2 GIFT)**

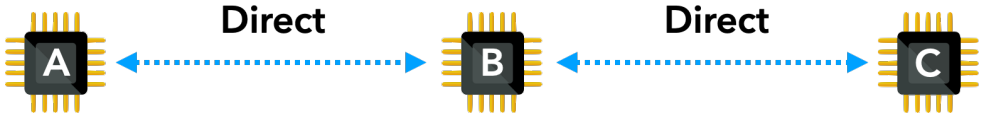
GIFT-128-128: **+19% on efficiency (PRESENT-128)**
-47% on robustness (PRESENT-128)
+63% on robustness (AES-128)

L. Dalmasso, F. Bruguier, P. Benoit, and L. Torres "Evaluation of SPN-Based Lightweight Crypto-Ciphers," IEEE Access, vol. 7, pp. 10559–10567, 2019.

Ensure the Trust in a Decentralized Network



Ensure the Trust in a Decentralized Network



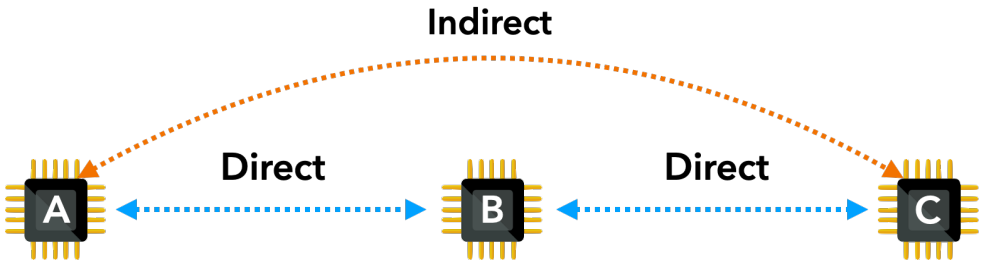
Honesty [1]

Latency [2]

Signal Quality, Energy [3]

[1] F. Bao and I.-R. Chen, “Dynamic trust management for internet of things applications”
[2] J. Liang, M. Zhang, and V. C. M. Leung, “A Reliable Trust Computing Mechanism Based on Multisource Feedback and Fog Computing in Social Sensor Cloud”
[3] N. Djedjig, D. Tandjaoui, F. Medjek, and I. Romdhani, “Trust-aware and cooperative routing protocol for IoT security”

Ensure the Trust in a Decentralized Network



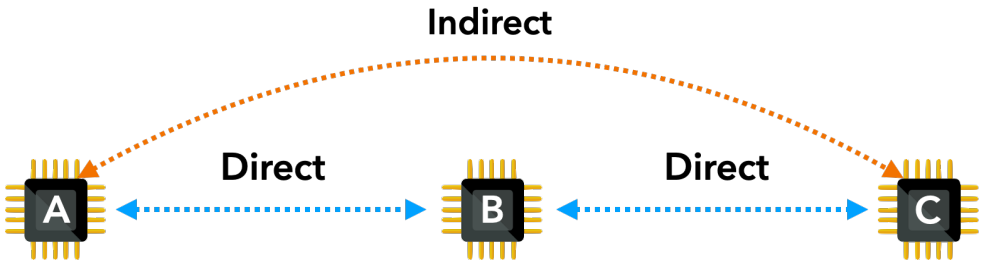
Honesty [1]

Latency [2]

Signal Quality, Energy [3]

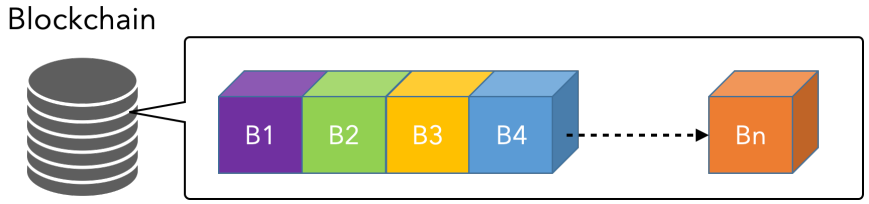
[1] F. Bao and I.-R. Chen, “Dynamic trust management for internet of things applications”
[2] J. Liang, M. Zhang, and V. C. M. Leung, “A Reliable Trust Computing Mechanism Based on Multisource Feedback and Fog Computing in Social Sensor Cloud”
[3] N. Djedjig, D. Tandjaoui, F. Medjek, and I. Romdhani, “Trust-aware and cooperative routing protocol for IoT security”

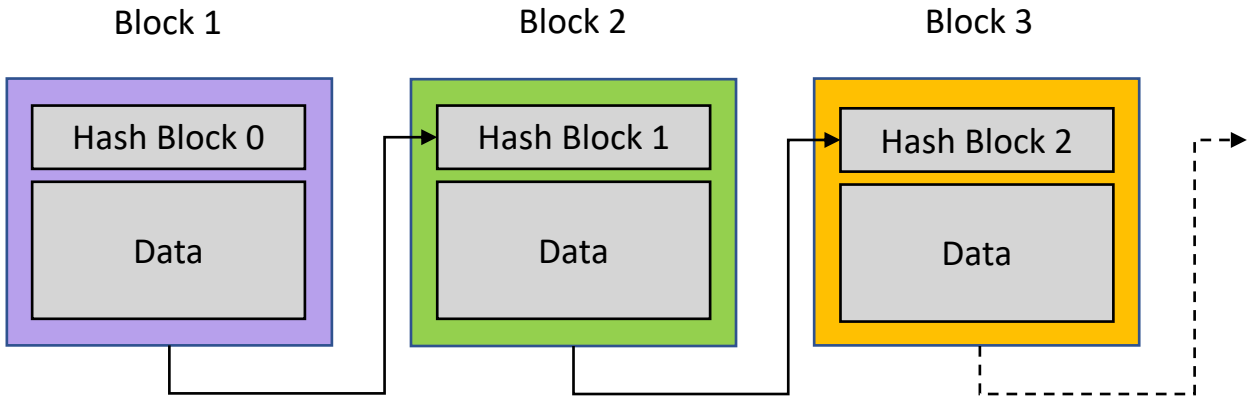
Ensure the Trust in a Decentralized Network



Honesty [1] Latency [2]

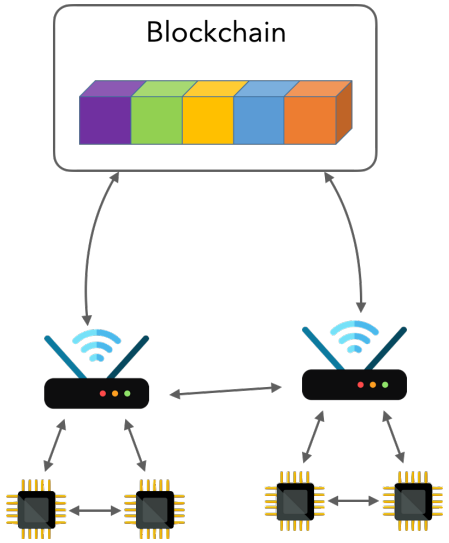
Signal Quality, Energy [3]





[1] F. Bao and I.-R. Chen, “Dynamic trust management for internet of things applications”
[2] J. Liang, M. Zhang, and V. C. M. Leung, “A Reliable Trust Computing Mechanism Based on Multisource Feedback and Fog Computing in Social Sensor Cloud”
[3] N. Djedjig, D. Tandjaoui, F. Medjek, and I. Romdhani, “Trust-aware and cooperative routing protocol for IoT security”

Internet of Things and Blockchain

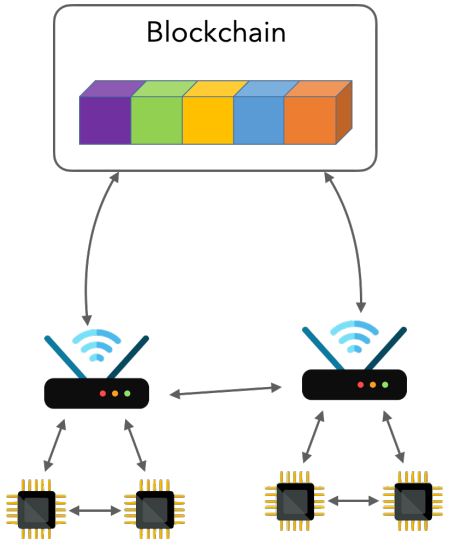


[1], [2]

Papers	Approaches	Blockchains
[3]	Token Access Control	Bitcoin
[4]	IoT Data Marketplace	Ethereum
[5]	Data Sharing Reward	IOTA

[1] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, “On blockchain and its integration with IoT. Challenges and opportunities”
[2] M.S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, M.H. Rehmani, “Applications of Blockchains in the Internet of Things: A Comprehensive Survey”
[3] H. Shafagh, L. Burkhalter, A. Hithnawi, and S. Duquennoy, “Towards blockchain-based auditable storage and sharing of IoT data”
[4] P. Missier, S. Bajoudah, A. Capossele, A. Gaglione, and M. Nati, “Mind my value: A decentralized infrastructure for fair and trusted IoT data trading”
[5] O. Lamtzidis and J. Gialelis, “An IOTA Based Distributed Sensor Node System”

Internet of Things and Blockchain

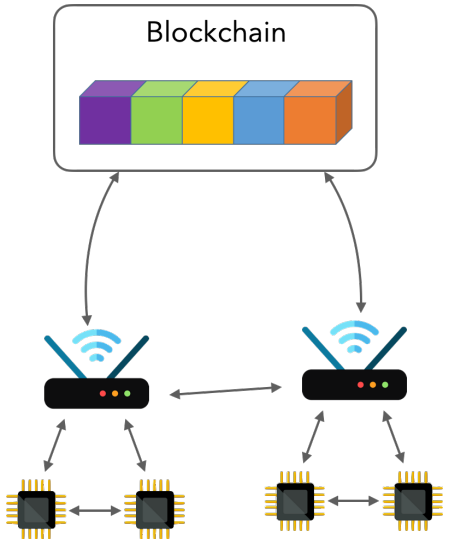


[1], [2]

Papers	Approaches	Blockchains
[3]	Token Access Control	Bitcoin
[4]	IoT Data Marketplace	Ethereum
[5]	Data Sharing Reward	IOTA

[1] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, “On blockchain and its integration with IoT. Challenges and opportunities”
[2] M.S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, M.H. Rehmani, “Applications of Blockchains in the Internet of Things: A Comprehensive Survey”
[3] H. Shafagh, L. Burkhalter, A. Hithnawi, and S. Duquennoy, “Towards blockchain-based auditable storage and sharing of IoT data”
[4] P. Missier, S. Bajoudah, A. Capossele, A. Gaglione, and M. Nati, “Mind my value: A decentralized infrastructure for fair and trusted IoT data trading”
[5] O. Lamtzidis and J. Gialelis, “An IOTA Based Distributed Sensor Node System”

Internet of Things and Blockchain



[1], [2]

IOTA

1 500 TPS

1.6 KB / Block

Nano

7 000 TPS

500 B / Block

Papers	Approaches	Blockchains
[3]	Token Access Control	Bitcoin
[4]	IoT Data Marketplace	Ethereum
[5]	Data Sharing Reward	IOTA

Blockchains	Benchmark on Raspberry Pi 3B+	RAM Requirements
Nano	> 4h	4 GB
IOTA	> 1min [6]	2 GB

[1] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, “On blockchain and its integration with IoT. Challenges and opportunities”

[2] M.S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, M.H. Rehmani, “Applications of Blockchains in the Internet of Things: A Comprehensive Survey”

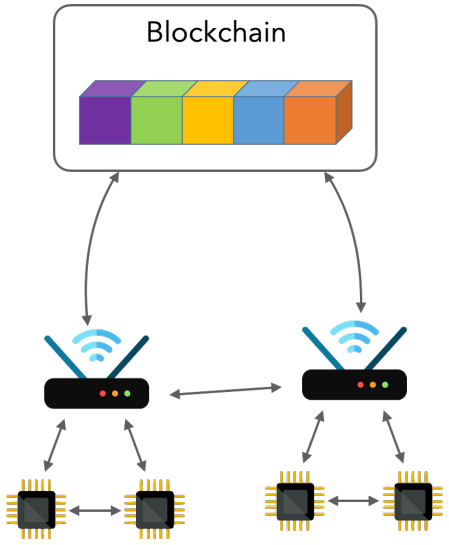
[3] H. Shafagh, L. Burkhalter, A. Hithnawi, and S. Duquennoy, “Towards blockchain-based auditable storage and sharing of IoT data”

[4] P. Missier, S. Bajoudah, A. Capossele, A. Gaglione, and M. Nati, “Mind my value: A decentralized infrastructure for fair and trusted IoT data trading”

[5] O. Lamtzidis and J. Gialelis, “An IOTA Based Distributed Sensor Node System”

[6] A. Elsts, E. Mitskas, and G. Oikonomou, “Distributed Ledger Technology and the Internet of Things: A Feasibility Study”

Internet of Things and Blockchain



[1], [2]

Papers	Approaches	Blockchains
[3]	Token Access Control	Bitcoin
[4]	IoT Data Marketplace	Ethereum
[5]	Data Sharing Reward	IOTA

IOTA

1 500 TPS

1.6 KB / Block

Nano

7 000 TPS

500 B / Block

Blockchains	Benchmark on Raspberry Pi 3B+	RAM Requirements
Nano	> 4h	4 GB
IOTA	> 1min [6]	2 GB

Wallance, an Alternative to Blockchain for IoT

[1] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, “On blockchain and its integration with IoT. Challenges and opportunities”

[2] M.S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, M.H. Rehmani, “Applications of Blockchains in the Internet of Things: A Comprehensive Survey”

[3] H. Shafagh, L. Burkhalter, A. Hithnawi, and S. Duquennoy, “Towards blockchain-based auditable storage and sharing of IoT data”

[4] P. Missier, S. Bajoudah, A. Capossele, A. Gaglione, and M. Nati, “Mind my value: A decentralized infrastructure for fair and trusted IoT data trading”

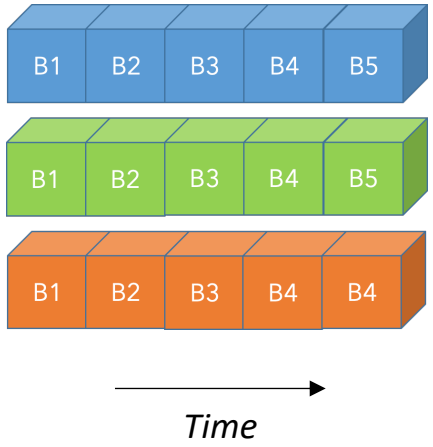
[5] O. Lamtzidis and J. Gialelis, “An IOTA Based Distributed Sensor Node System”

[6] A. Elsts, E. Mitskas, and G. Oikonomou, “Distributed Ledger Technology and the Internet of Things: A Feasibility Study”

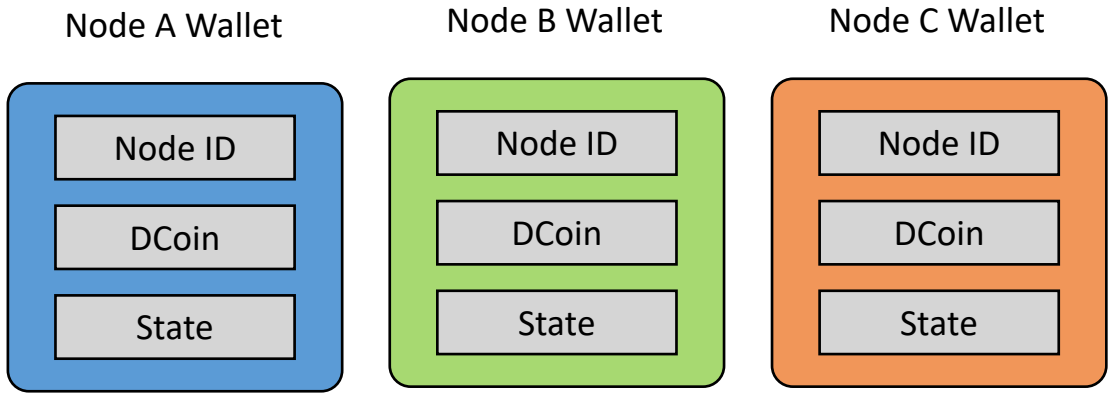
Wallance Design

Nano

Block Lattice Structure



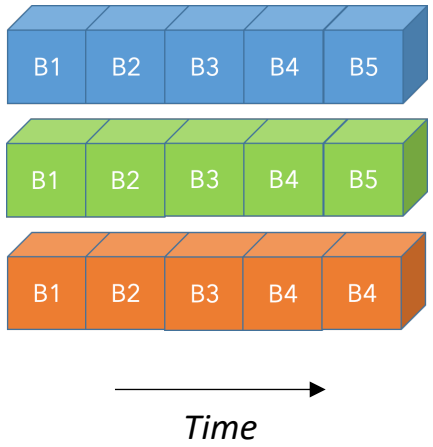
Wallance



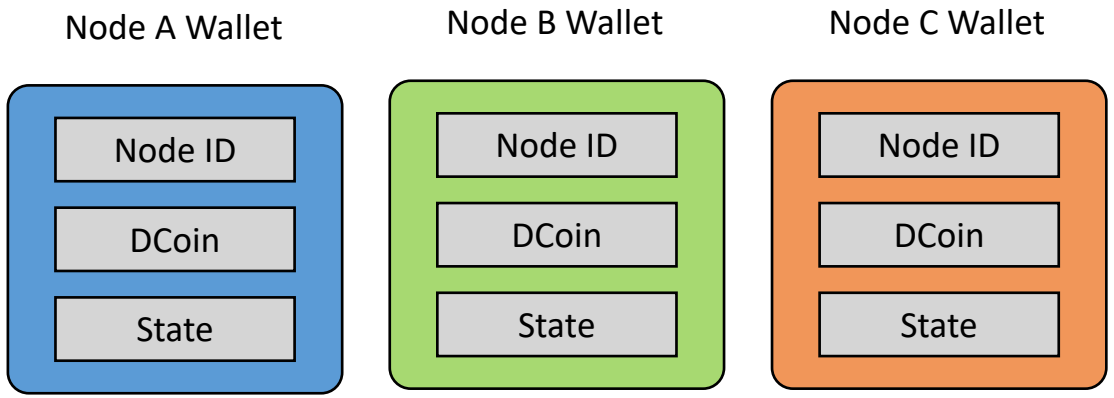
Wallance Design

Nano

Block Lattice Structure



Wallance

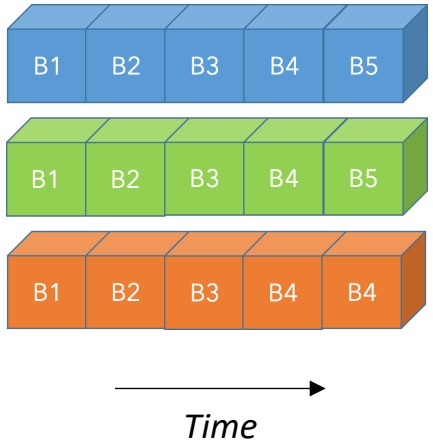


Properties	Nano	Wallance
Consensus Model	Voting System	Voting System

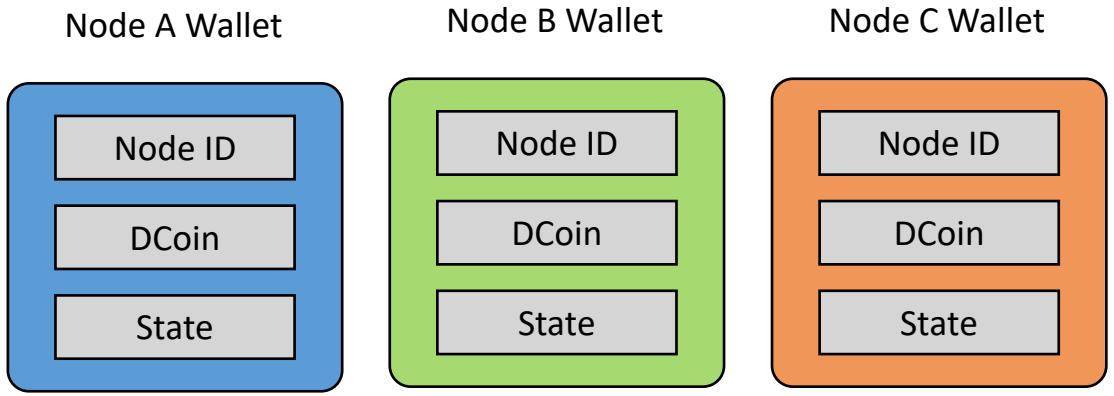
Wallance Design

Nano

Block Lattice Structure



Wallance

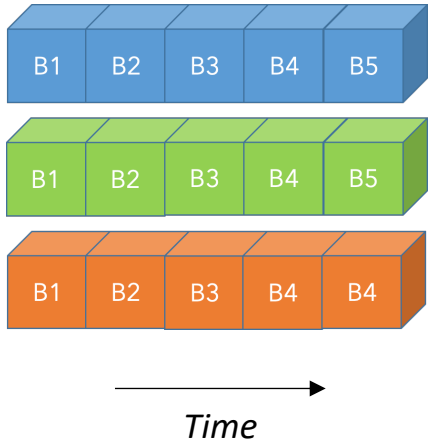


Properties	Nano	Wallance
Consensus Model	Voting System	Voting System
Decentralization	Richest Nodes	All Nodes

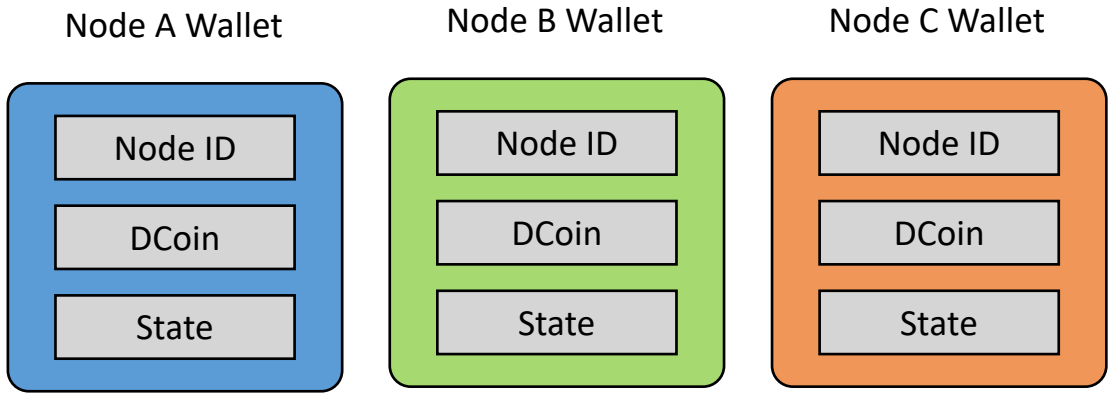
Wallance Design

Nano

Block Lattice Structure



Wallance

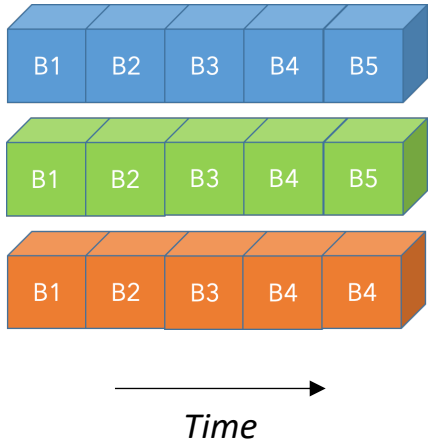


Properties	Nano	Wallance
Consensus Model	Voting System	Voting System
Decentralization	Richest Nodes	All Nodes
Incentive Mechanism	None	Reward

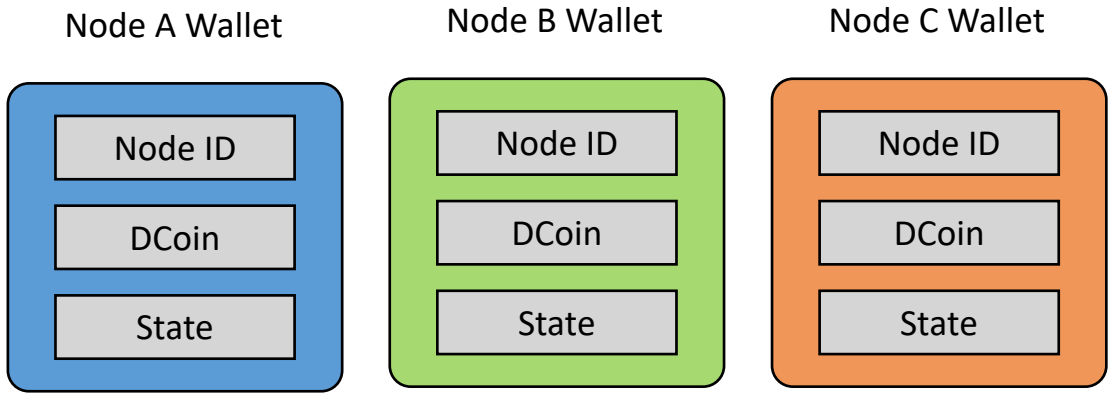
Wallance Design

Nano

Block Lattice Structure



Wallance

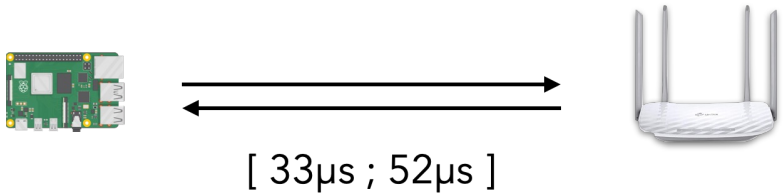


Properties	Nano	Wallance
Consensus Model	Voting System	Voting System
Decentralization	Richest Nodes	All Nodes
Incentive Mechanism	None	Reward

Wallance Evaluations : Anti-Spam Lightweight Proof-of-Work (LWPoW)

Computation Time (Raspberry Pi 3B+)

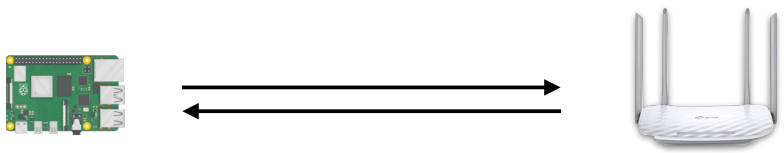
Difficulty (nibbles to '0')	Average Tentatives	Computation Time (Average)
0	1	40 µs
1	16	652 µs
2	263	11 ms
3	4 258	183 ms



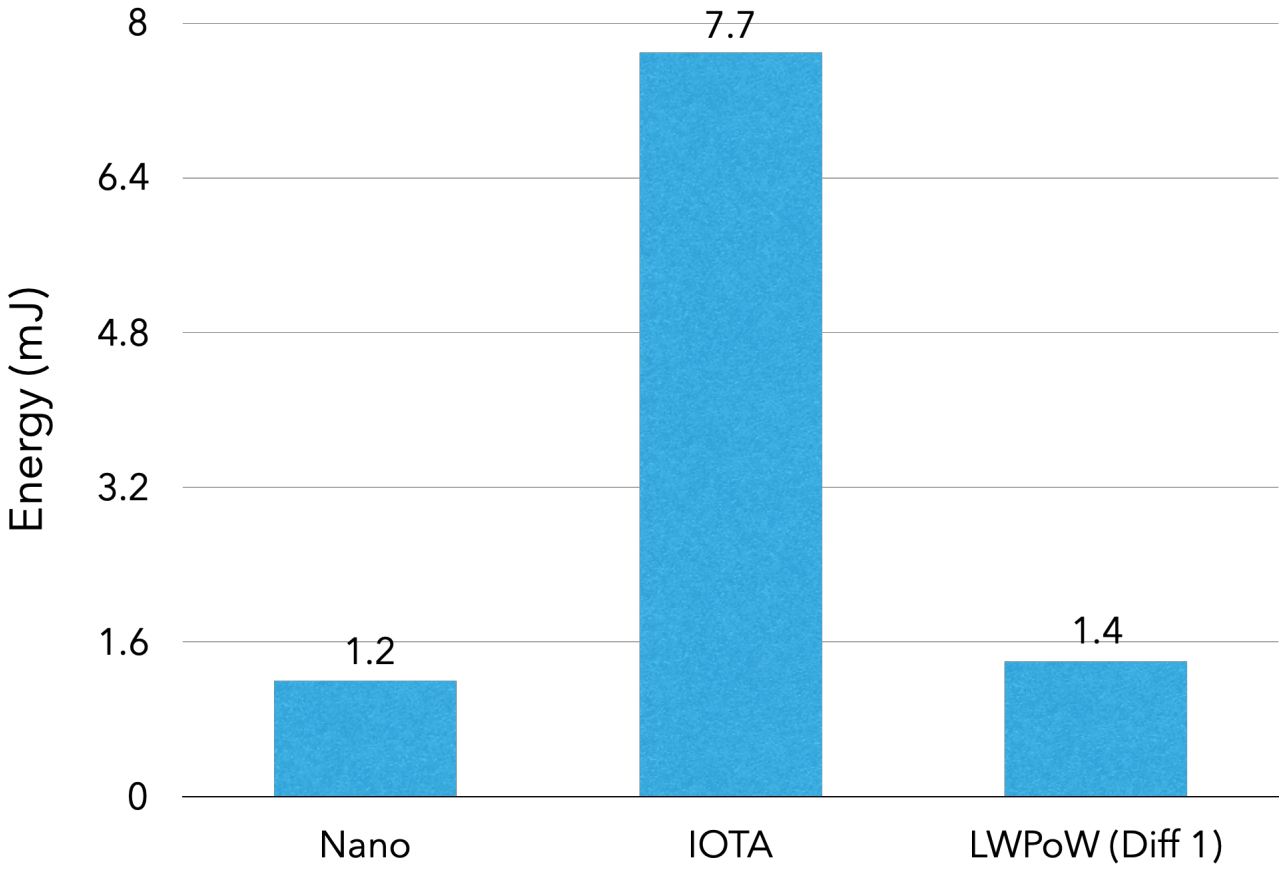
Wallance Evaluations : Anti-Spam Lightweight Proof-of-Work (LWPoW)

Computation Time (Raspberry Pi 3B+)

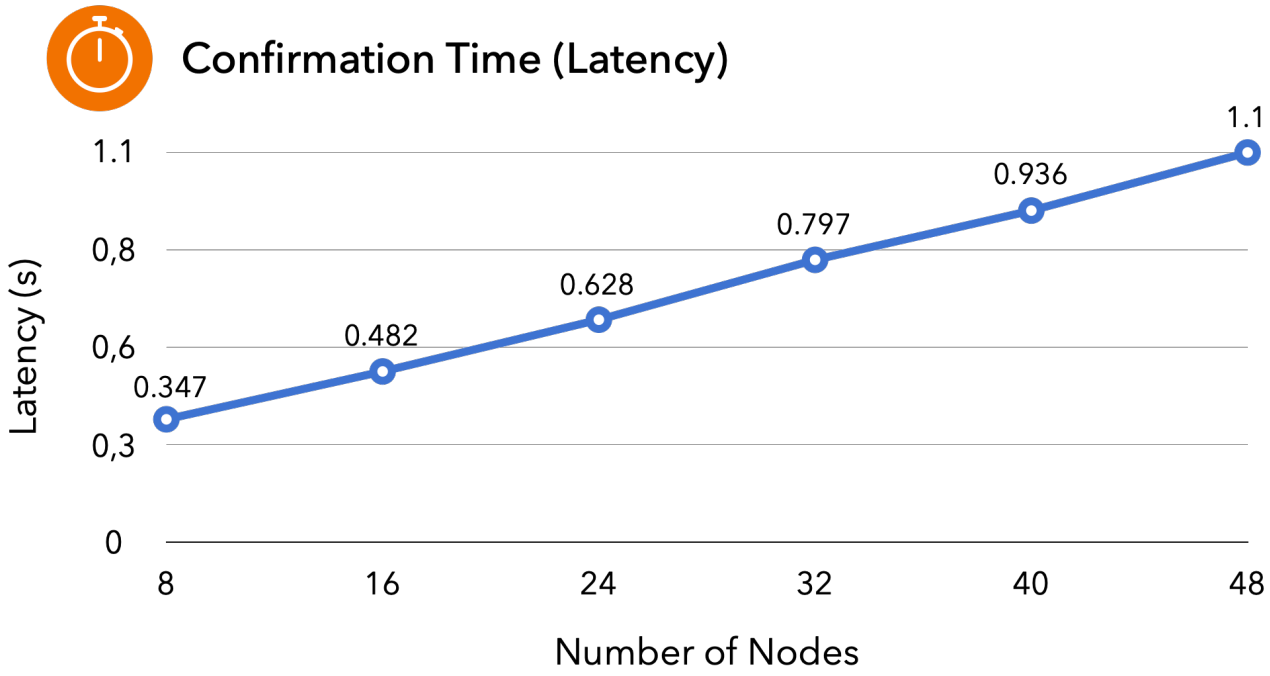
Difficulty (nibbles to '0')	Average Tentatives	Computation Time (Average)
0	1	40 µs
1	16	652 µs
2	263	11 ms
3	4 258	183 ms



Energy Comparison with Equivalent Difficulty

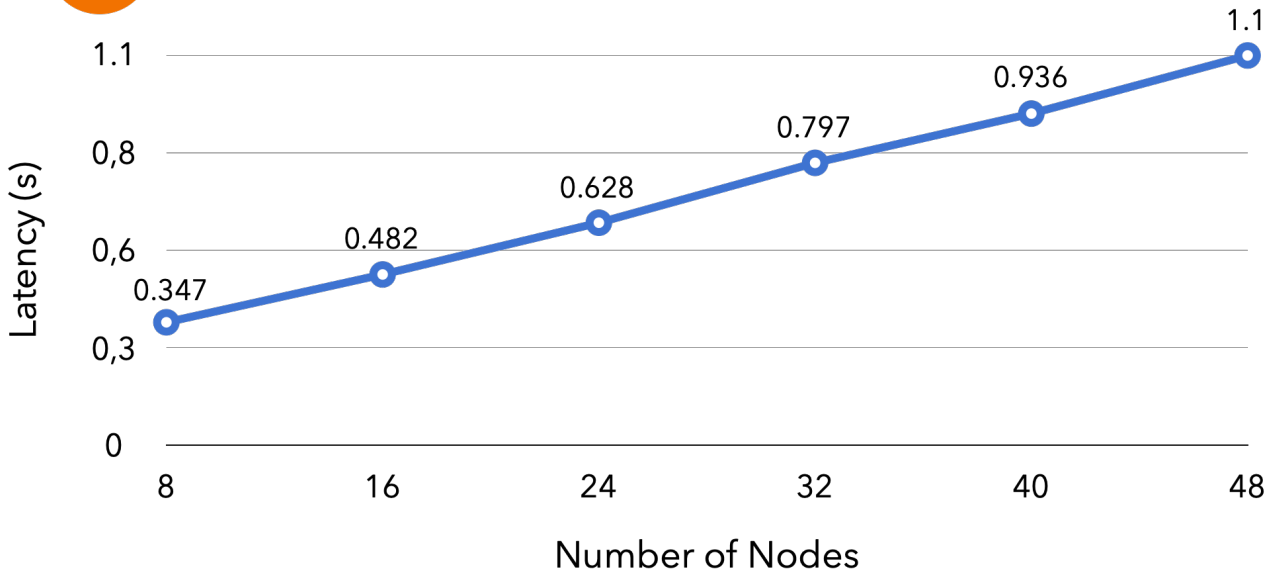


Wallance Evaluations : Consensus



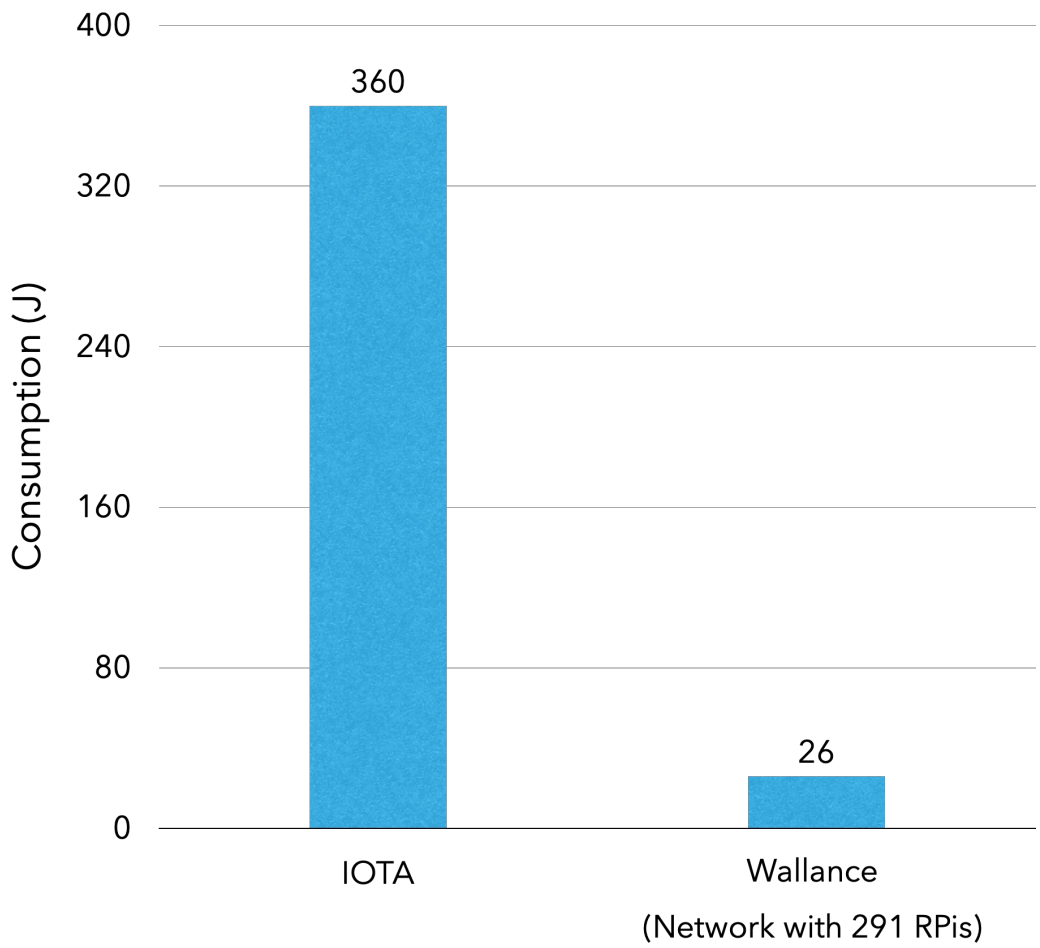
Wallance Evaluations : Consensus

Confirmation Time (Latency)

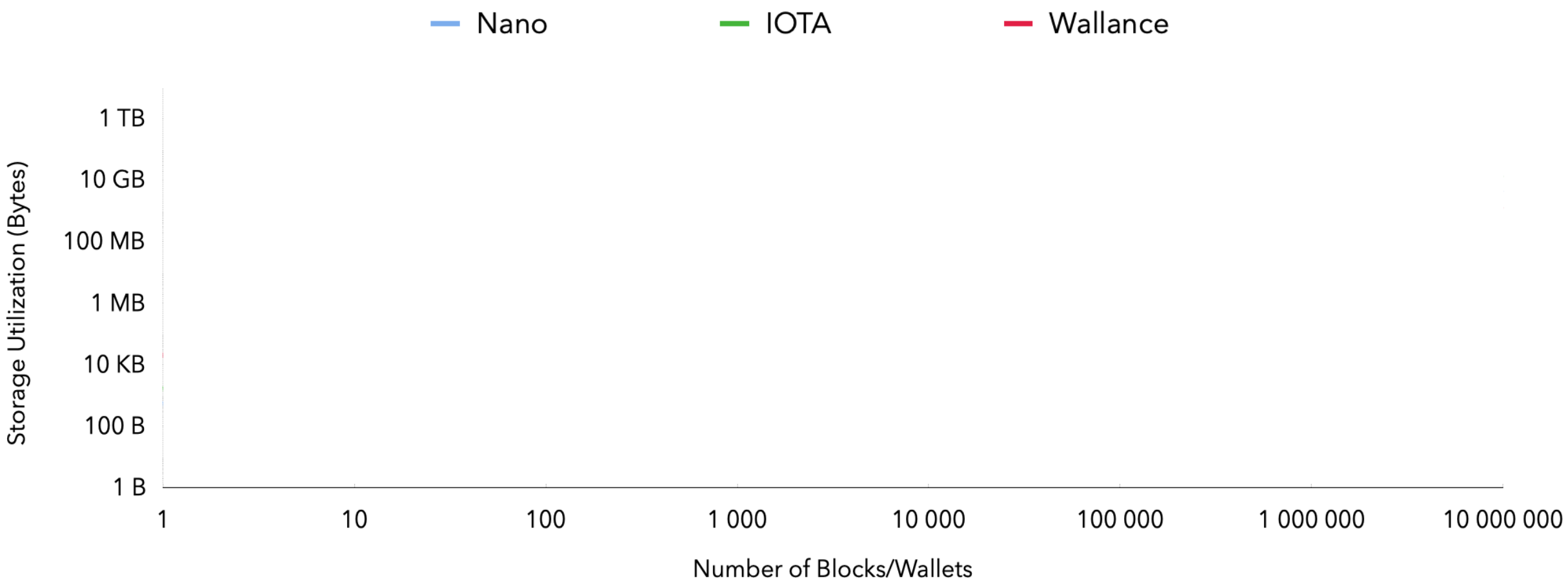


Blockchains	Number of Nodes	Confirmation Time	Wallance Confirmation Time
Nano	90	< 2 s	1.9 s
IOTA	291	10 s	5.7 s

Energy Comparison for 1 TX Validation



Wallance Evaluations : Storage Utilization



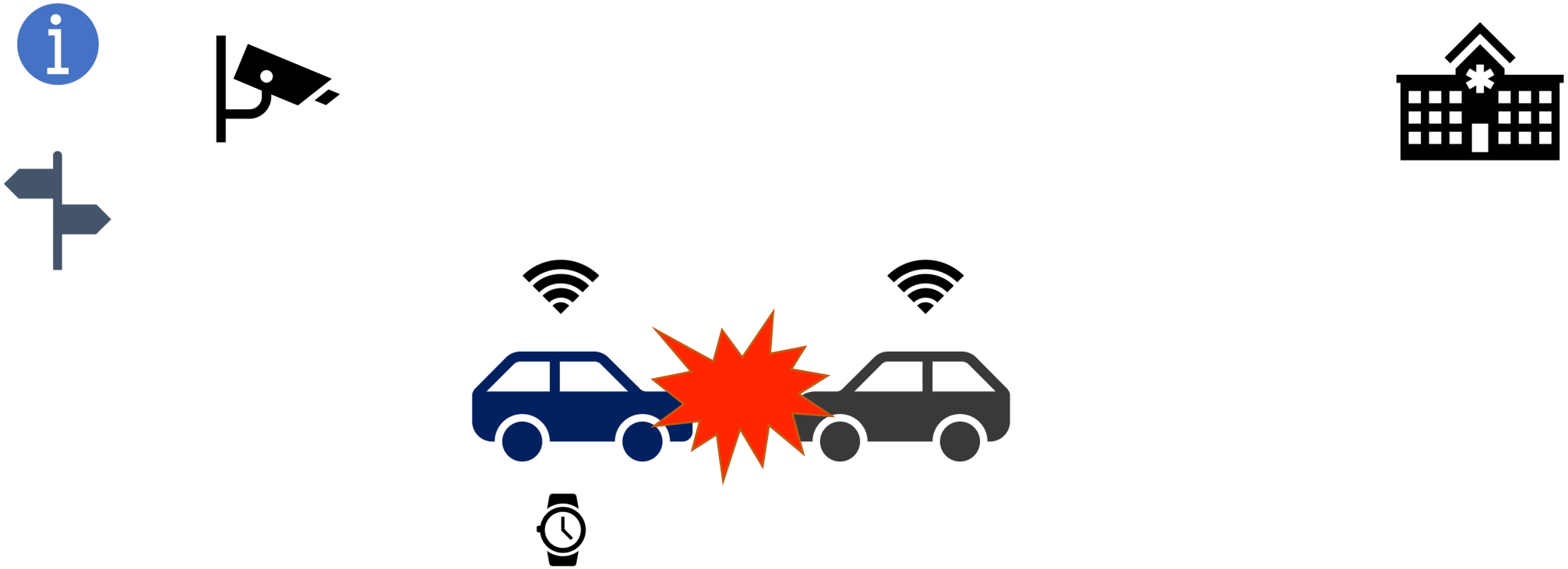
Wallance, an Alternative to Blockchain for IoT : Summary

Ensure the trust in a decentralized network

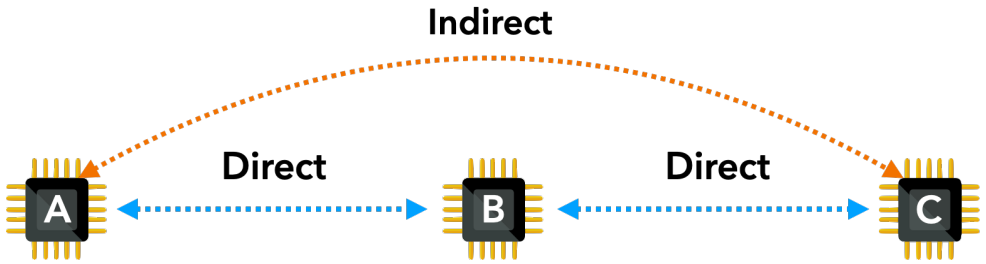
Computing Power :	**Designed for embedded systems (e.g. Rasperry Pi)** **IOTA (2 GB RAM)** **Nano (4 GB RAM)**
Storage Utilization:	**146 MB for 1M Wallets** **IOTA (÷10)** **Nano (÷3)**
Low Latency:	**IOTA (÷2), ≈ Nano**
Low Energy Consumption:	**IOTA (÷10)**

Loïc Dalmasso, Florent Bruguier, Achraf Lamlih, Pascal Benoit : « Wallance, an Alternative to Blockchain for IoT », dans IEEE World Forum on Internet of Things 2020 (WF-IOT), Jun 2020, New Orleans, United States.

Ensure the Trust in a Decentralized Network, at Device Level

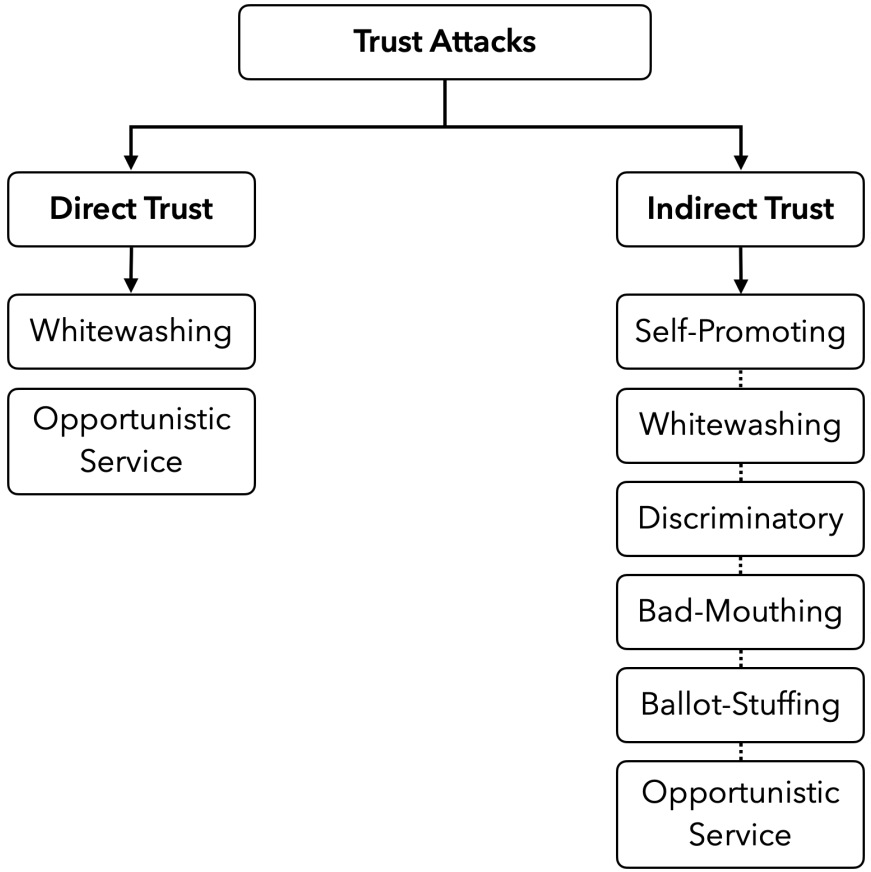


Ensure the Trust in a Decentralized Network, at Device Level



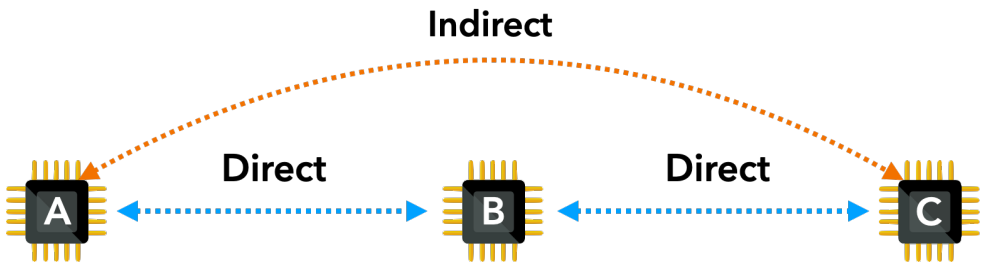
Trust = Direct + Indirect [1]

[2][3]



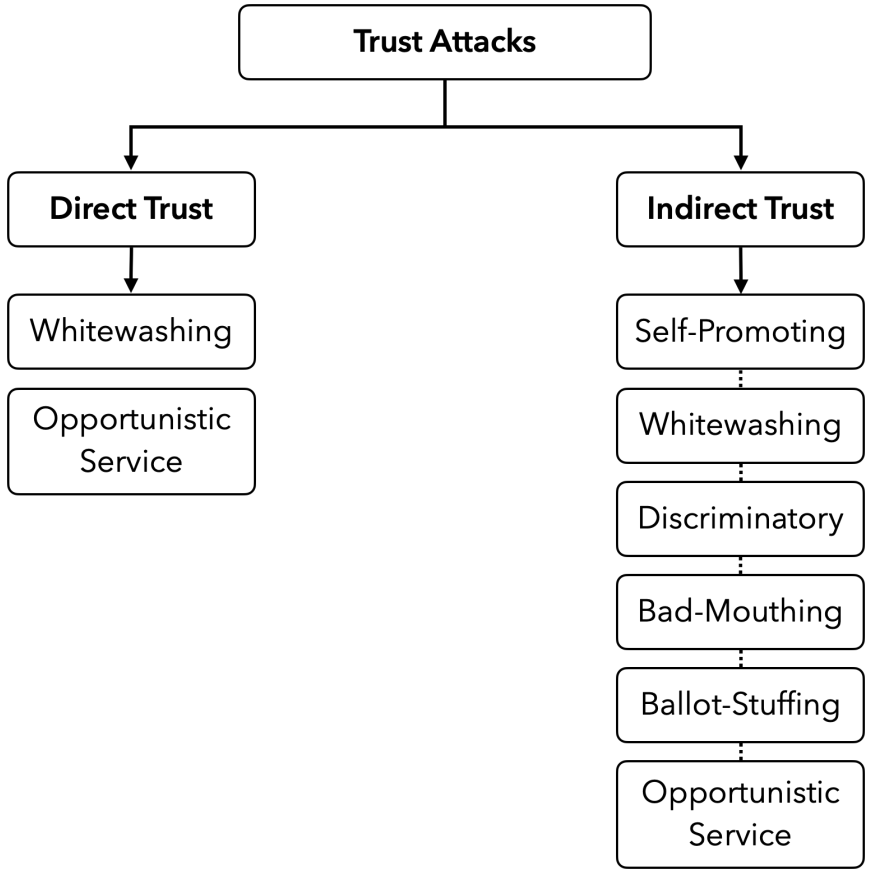
[1] B. Wang, M. Li, X. Jin, and C. Guo, “A Reliable IoT Edge Computing Trust Management Mechanism for Smart Cities”
[2] F. Bao, I. Chen and J. Guo, “Scalable, adaptive and survivable trust management for community of interest based Internet of Things systems”
[3] D. E. Kouicem, A. Bouabdallah, and H. Lakhlef, “An Efficient Architecture for Trust Management in IoE Based Systems of Systems”

Ensure the Trust in a Decentralized Network, at Device Level



Trust = Direct + Indirect [1]

[2][3]



[1] B. Wang, M. Li, X. Jin, and C. Guo, “A Reliable IoT Edge Computing Trust Management Mechanism for Smart Cities”
[2] F. Bao, I. Chen and J. Guo, “Scalable, adaptive and survivable trust management for community of interest based Internet of Things systems”
[3] D. E. Kouicem, A. Bouabdallah, and H. Lakhlef, “An Efficient Architecture for Trust Management in IoE Based Systems of Systems”

TrustLib : Metrics for Sensors and Actuators

Operation Success : $O_{S_{ij}} = \begin{cases} -1 \; when \; operation \; fails \\ 1 \; when \; operation \; succeeds \end{cases}$

Latency : $L_{ij} \in [0 ; 1]$

1 = High Latency (worst case)
0 = Low Latency (best case)

Signal Strength : $S_{Q_{ij}} \in [0 ; 1]$

1 = Strong Signal (best case)
0 = Weak Signal (worst case)

Battery : $Bat_i \in [0.1 ; 1]$

1 = Full (best case)
0.1 = Empty (worst case)

TrustLib : Metrics for Sensors and Actuators

$Device_i$ $Device_j$

It is harder to gain trust than to lose it

Operation Success : $O_{S_{ij}} = \begin{cases} -1 \text{ when operation fails} \\ 1 \text{ when operation succeeds} \end{cases}$

Latency : $L_{ij} \in [0\,;1]$

1 = High Latency (worst case)
0 = Low Latency (best case)

Signal Strength : $S_{Q_{ij}} \in [0\,;1]$

1 = Strong Signal (best case)
0 = Weak Signal (worst case)

Battery : $Bat_i \in [0.1\,;1]$

1 = Full (best case)
0.1 = Empty (worst case)

$$AG_{ij} = O_{S_{ij}} \times \left(\qquad \right)$$

TrustLib : Metrics for Sensors and Actuators

It is harder to gain trust than to lose it

Operation Success : $O_{S_{ij}} = \begin{cases} -1 \; when \; operation \; fails \\ 1 \; when \; operation \; succeeds \end{cases}$

Latency : $L_{ij} \in [0 ; 1]$

1 = High Latency (worst case)
0 = Low Latency (best case)

Signal Strength : $S_{Q_{ij}} \in [0 ; 1]$

1 = Strong Signal (best case)
0 = Weak Signal (worst case)

Battery : $Bat_i \in [0.1 ; 1]$

1 = Full (best case)
0.1 = Empty (worst case)

$$AG_{ij} = O_{S_{ij}} \times \left(\frac{1}{(\quad)^{O_{S_{ij}}}} \right)$$

TrustLib : Metrics for Sensors and Actuators

It is harder to gain trust than to lose it

Operation Success : $O_{S_{ij}} = \begin{cases} -1 \text{ when operation fails} \\ 1 \text{ when operation succeeds} \end{cases}$

Latency : $L_{ij} \in [0\,;1]$

1 = High Latency (worst case)
0 = Low Latency (best case)

Signal Strength : $S_{Q_{ij}} \in [0\,;1]$

1 = Strong Signal (best case)
0 = Weak Signal (worst case)

Battery : $Bat_i \in [0.1\,;1]$

1 = Full (best case)
0.1 = Empty (worst case)

$$AG_{ij} = O_{S_{ij}} \times \left(\frac{1}{\left(\quad + \quad \right)^{O_{S_{ij}}}} \right)$$

TrustLib : Metrics for Sensors and Actuators

It is harder to gain trust than to lose it

Operation Success : $O_{S_{ij}} = \begin{cases} -1 \text{ when operation fails} \\ 1 \text{ when operation succeeds} \end{cases}$

Latency : $L_{ij} \in [0\,;1]$

1 = High Latency (worst case)
0 = Low Latency (best case)

Signal Strength : $S_{Q_{ij}} \in [0\,;1]$

1 = Strong Signal (best case)
0 = Weak Signal (worst case)

Battery : $Bat_i \in [0.1\,;1]$

1 = Full (best case)
0.1 = Empty (worst case)

$$AG_{ij} = O_{S_{ij}} \times \left(\frac{1}{\left((1 + L_{ij}) + (2 - S_{Q_{ij}}) \right)^{O_{S_{ij}}}} \right)$$

TrustLib : Metrics for Sensors and Actuators

It is harder to gain trust than to lose it

Operation Success : $O_{S_{ij}} = \begin{cases} -1 \text{ when operation fails} \\ 1 \text{ when operation succeeds} \end{cases}$

Latency : $L_{ij} \in [0\,;1]$

1 = High Latency (worst case)
0 = Low Latency (best case)

Signal Strength : $S_{Q_{ij}} \in [0\,;1]$

1 = Strong Signal (best case)
0 = Weak Signal (worst case)

Battery : $Bat_i \in [0.1\,;1]$

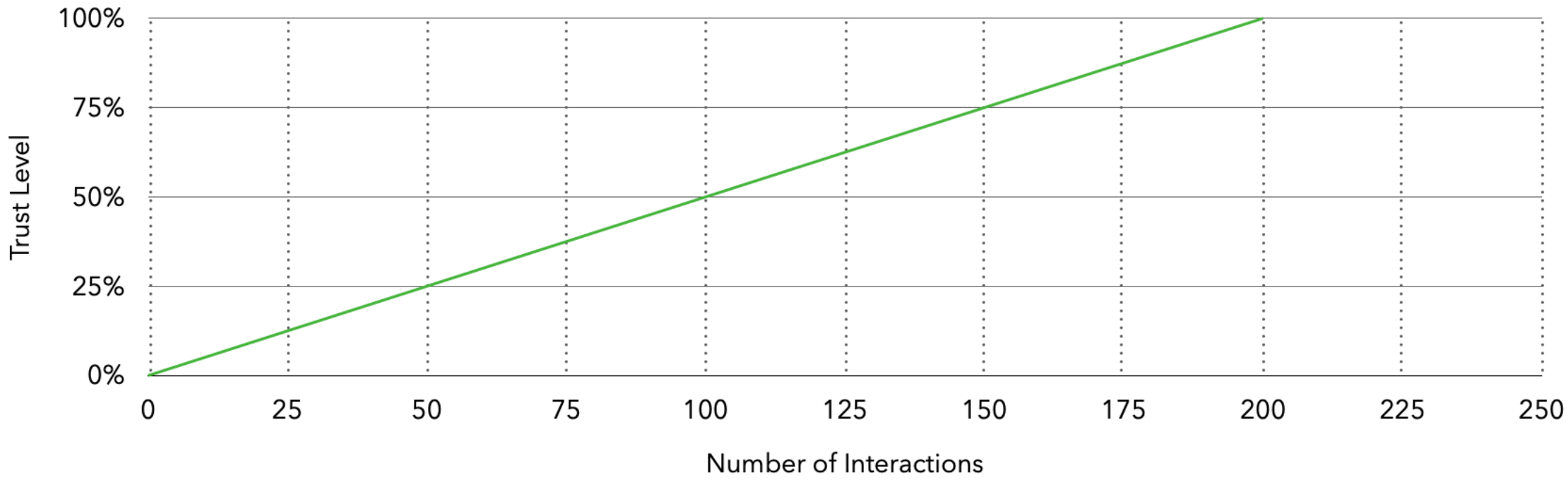
1 = Full (best case)
0.1 = Empty (worst case)

$$AG_{ij} = O_{S_{ij}} \times \left(\frac{1}{\left((1 + L_{ij}) + (2 - S_{Q_{ij}}) \right)^{O_{S_{ij}}}} \right) \times \frac{1}{Bat_i}$$

$$TrustLevel_{ij_n} = TrustLevel_{ij_{n-1}} + AG_{ij}$$

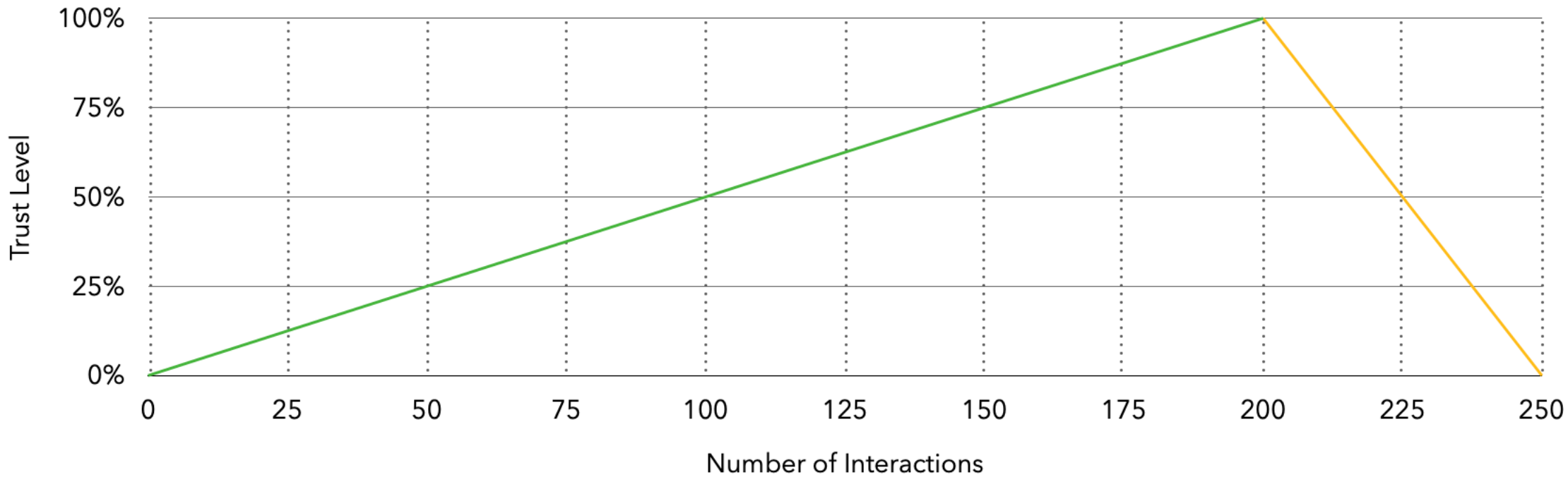
TrustLib : Metrics for Sensors and Actuators

Curves	Metric Configurations
	$O_{S_{ij}} = 1$; $L_{ij} = 0$; $S_{Q_{ij}} = 1$; $Bat_i = 1$



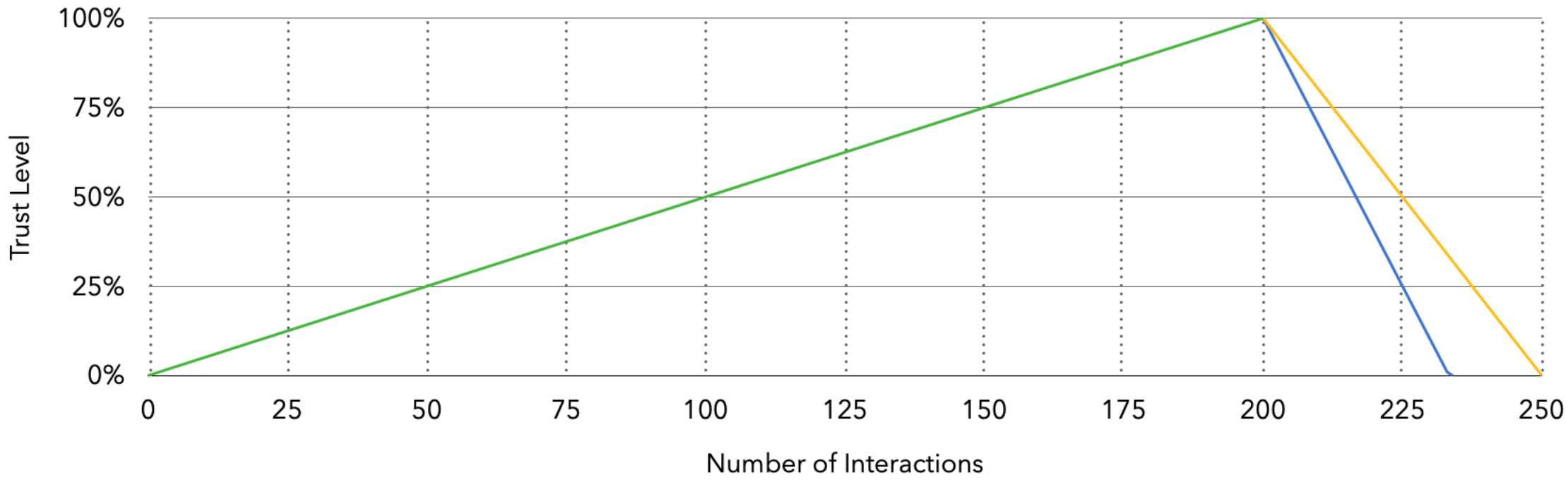
TrustLib : Metrics for Sensors and Actuators

Curves	Metric Configurations
	$O_{S_{ij}} = 1 \ ; \ L_{ij} = 0 \ ; \ S_{Q_{ij}} = 1 \ ; \ Bat_i = 1$
	$O_{S_{ij}} = -1 \ ; \ L_{ij} = 0 \ ; \ S_{Q_{ij}} = 1 \ ; \ Bat_i = 1$



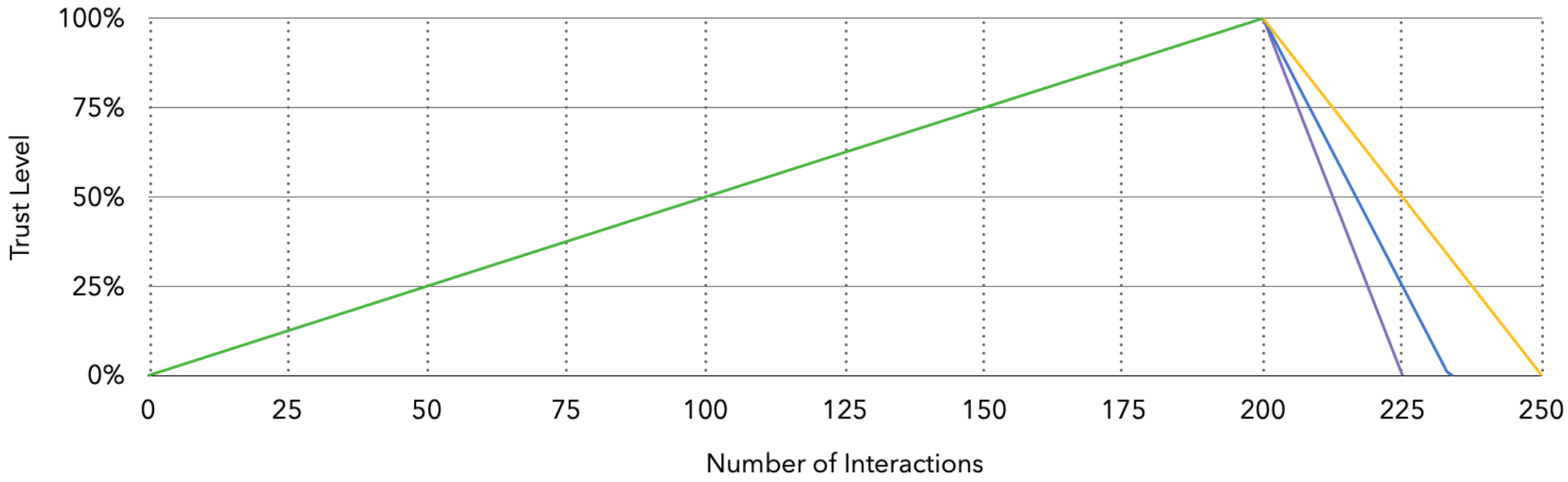
TrustLib : Metrics for Sensors and Actuators

Curves	Metric Configurations
	$O_{S_{ij}} = 1 \ ; \ L_{ij} = 0 \ ; \ S_{Q_{ij}} = 1 \ ; \ Bat_i = 1$
	$O_{S_{ij}} = -1 \ ; \ L_{ij} = 0 \ ; \ S_{Q_{ij}} = 1 \ ; \ Bat_i = 1$
	$O_{S_{ij}} = -1 \ ; \ L_{ij} = 1 \ ; \ S_{Q_{ij}} = 1 \ ; \ Bat_i = 1$



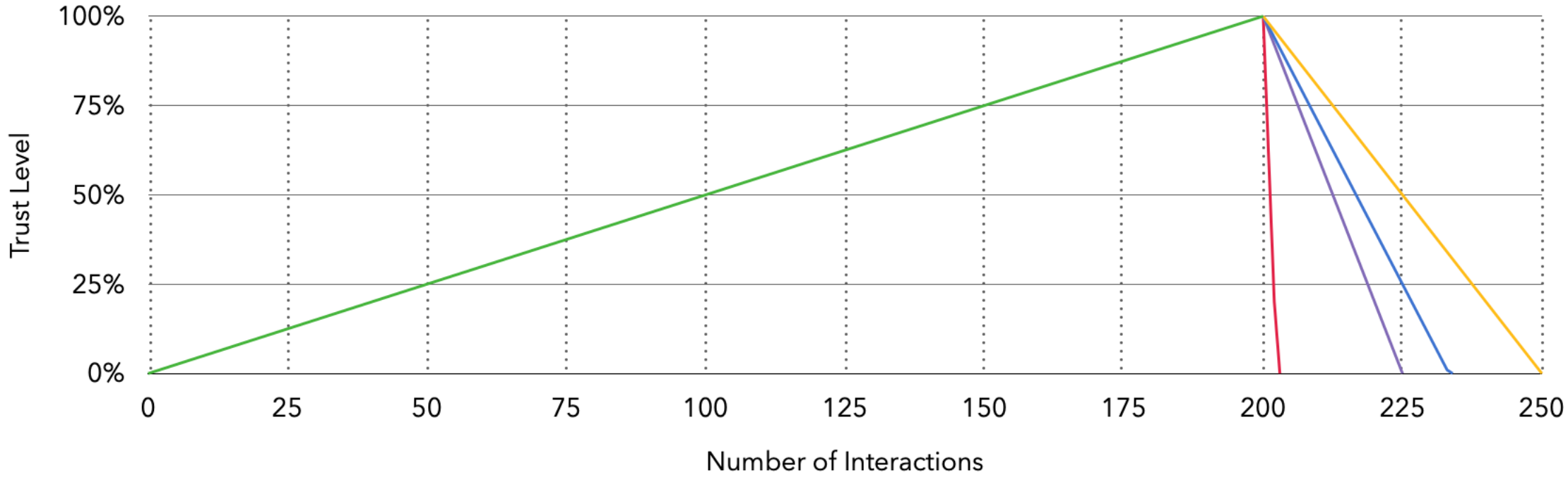
TrustLib : Metrics for Sensors and Actuators

Curves	Metric Configurations
	$O_{S_{ij}} = 1 \ ; \ L_{ij} = 0 \ ; \ S_{Q_{ij}} = 1 \ ; \ Bat_i = 1$
	$O_{S_{ij}} = -1 \ ; \ L_{ij} = 0 \ ; \ S_{Q_{ij}} = 1 \ ; \ Bat_i = 1$
	$O_{S_{ij}} = -1 \ ; \ L_{ij} = 1 \ ; \ S_{Q_{ij}} = 1 \ ; \ Bat_i = 1$
	$O_{S_{ij}} = -1 \ ; \ L_{ij} = 1 \ ; \ S_{Q_{ij}} = 0 \ ; \ Bat_i = 1$

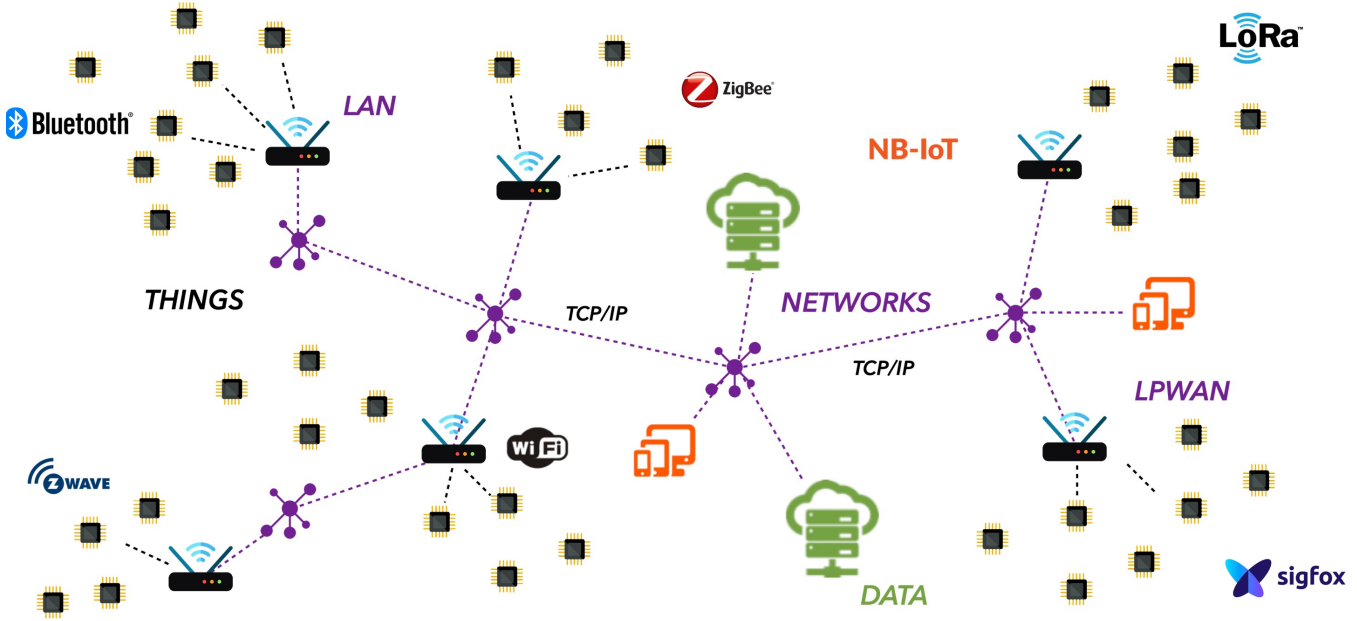


TrustLib : Metrics for Sensors and Actuators

Curves	Metric Configurations
	$O_{S_{ij}} = 1 \ ; \ L_{ij} = 0 \ ; \ S_{Q_{ij}} = 1 \ ; \ Bat_i = 1$
	$O_{S_{ij}} = -1 \ ; \ L_{ij} = 0 \ ; \ S_{Q_{ij}} = 1 \ ; \ Bat_i = 1$
	$O_{S_{ij}} = -1 \ ; \ L_{ij} = 1 \ ; \ S_{Q_{ij}} = 1 \ ; \ Bat_i = 1$
	$O_{S_{ij}} = -1 \ ; \ L_{ij} = 1 \ ; \ S_{Q_{ij}} = 0 \ ; \ Bat_i = 1$
	$O_{S_{ij}} = -1 \ ; \ L_{ij} = 1 \ ; \ S_{Q_{ij}} = 0 \ ; \ Bat_i = 0.1$



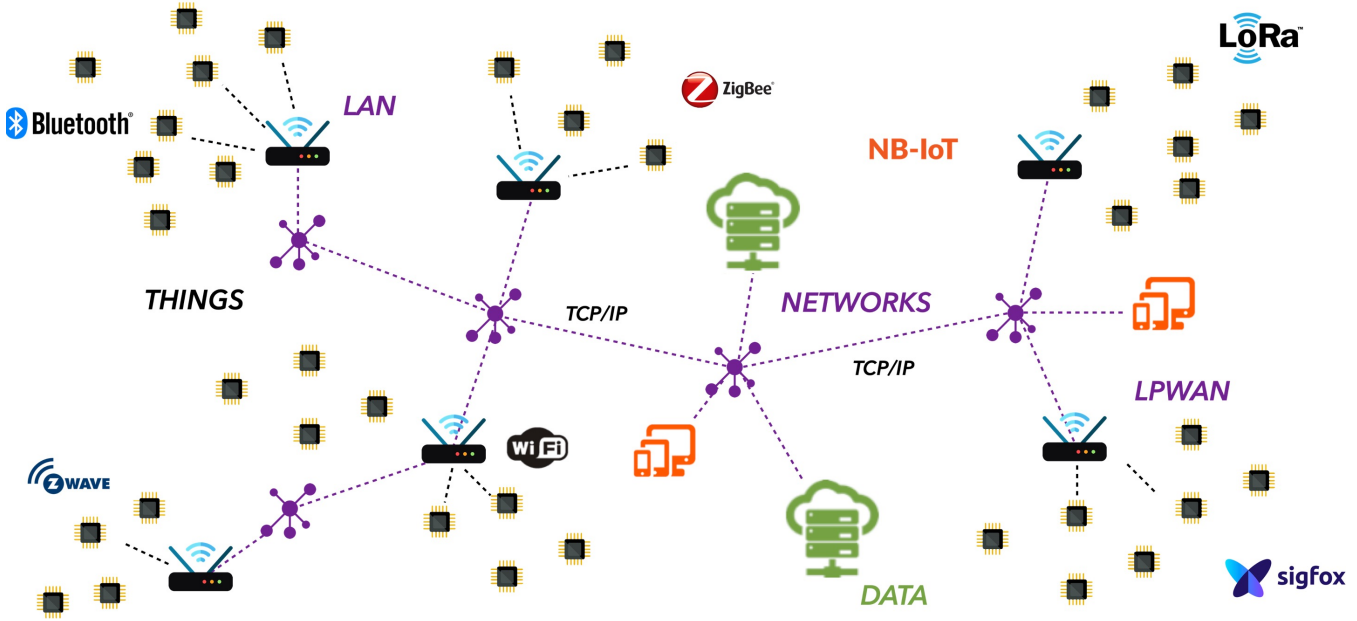
Conclusion



Which algorithm achieves the most efficient hardware implementation ?

GIFT-128-128: +19% on efficiency (PRESENT-128)
-47% on robustness (PRESENT-128)
+63% on robustness (AES-128)

Conclusion



Which algorithm achieves the most efficient hardware implementation ?

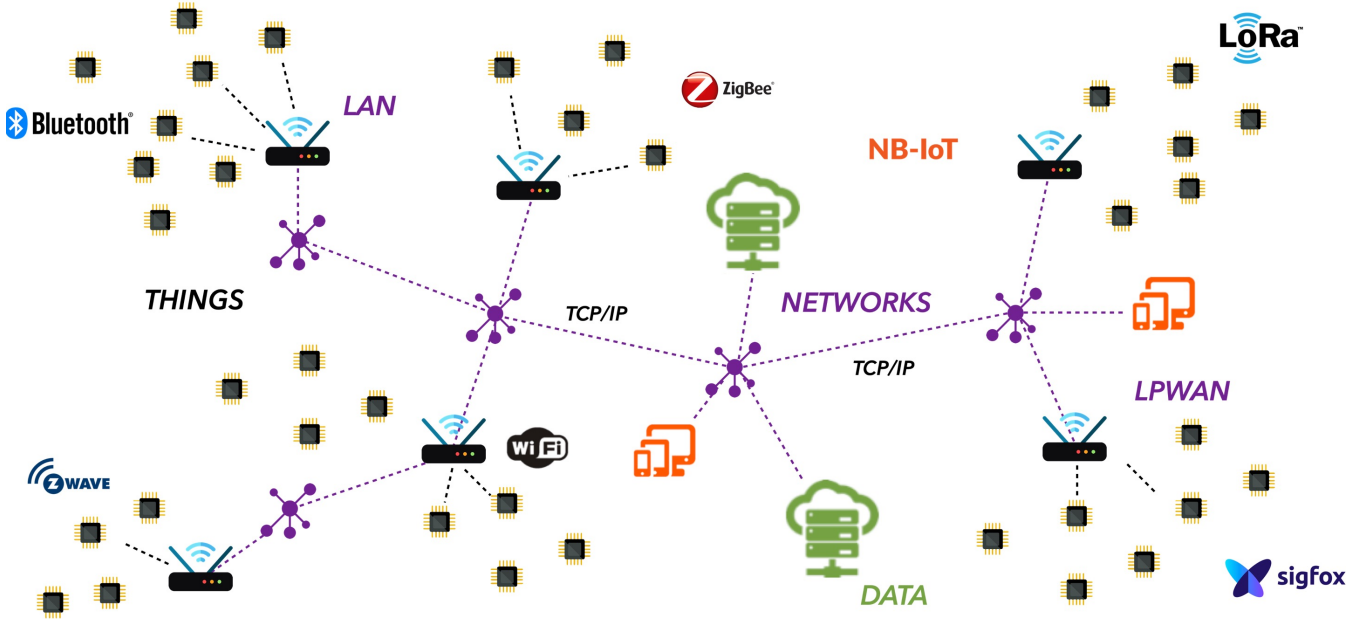
GIFT-128-128: +19% on efficiency (PRESENT-128)
-47% on robustness (PRESENT-128)
+63% on robustness (AES-128)

Ensure the trust in a decentralized network

Wallance, an Alternative to Blockchain for IoT

TrustLib, a Lightweight Trust Protocol for IoT Device

Perspectives



PRESENT-128: the most resistant (x3 AES, x2 GIFT)
But … only 3 400 Traces

Wallance : New Model based on QoS and Energy

Lightweight Countermeasures

TrustLib for Gateway …

… and the Cloud

LIRMM

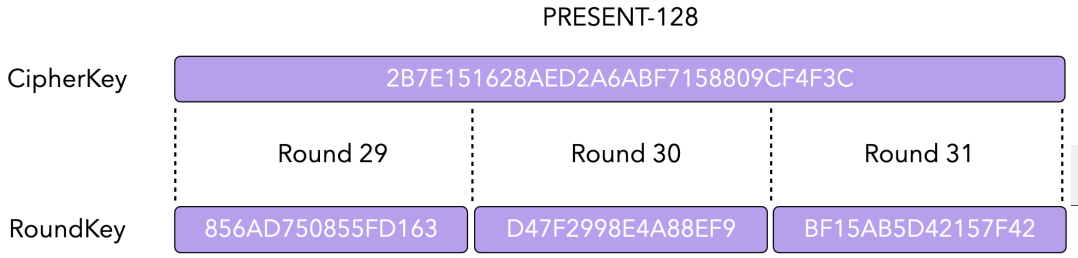
Thank You

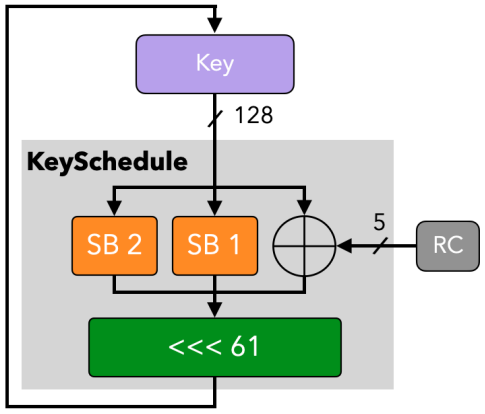
cnfm GIP IDEFI finmina

cnrs advancing the frontiers

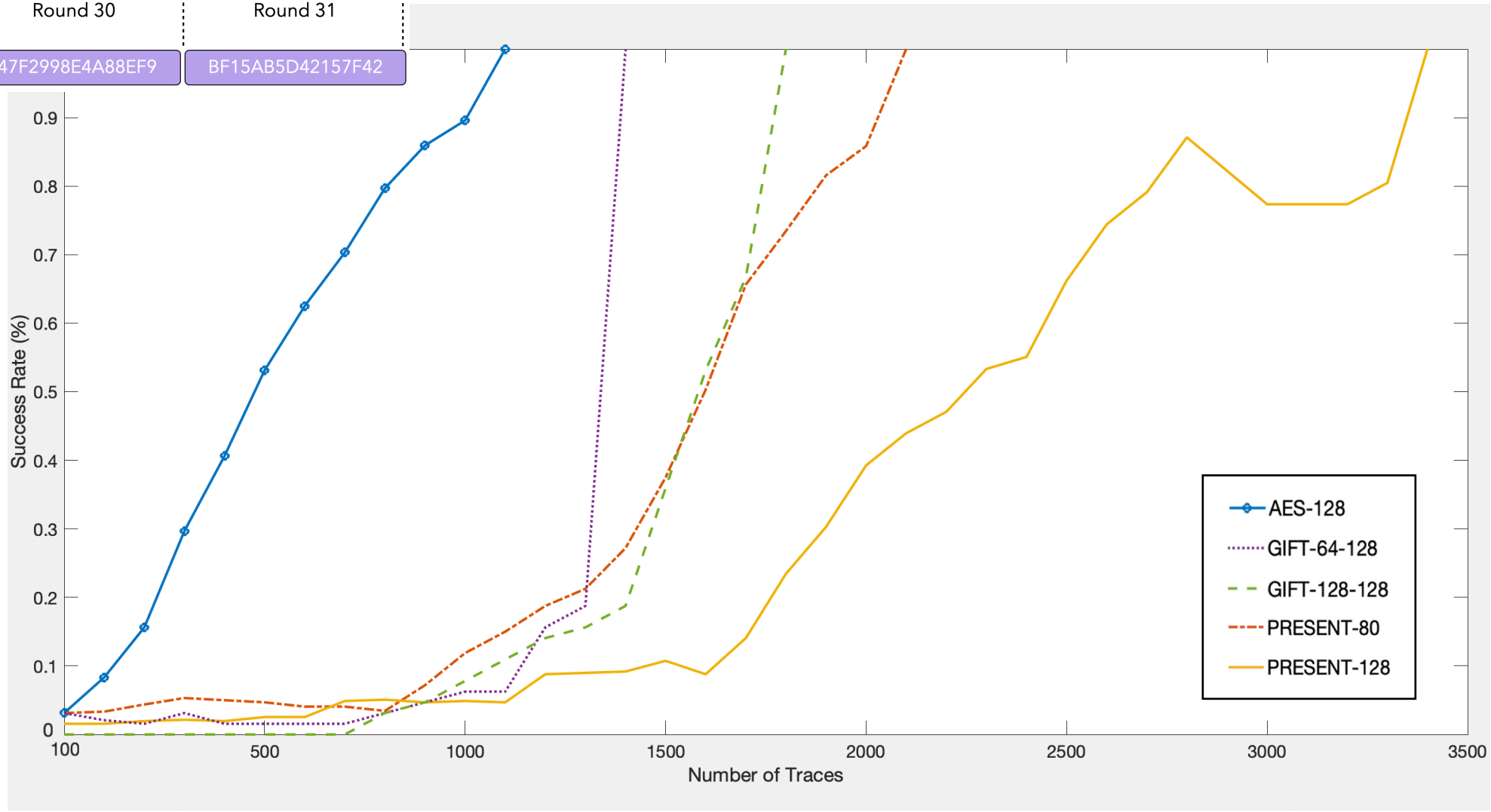
Université Montpellier

Crypto-Ciphers Robustness Evaluations

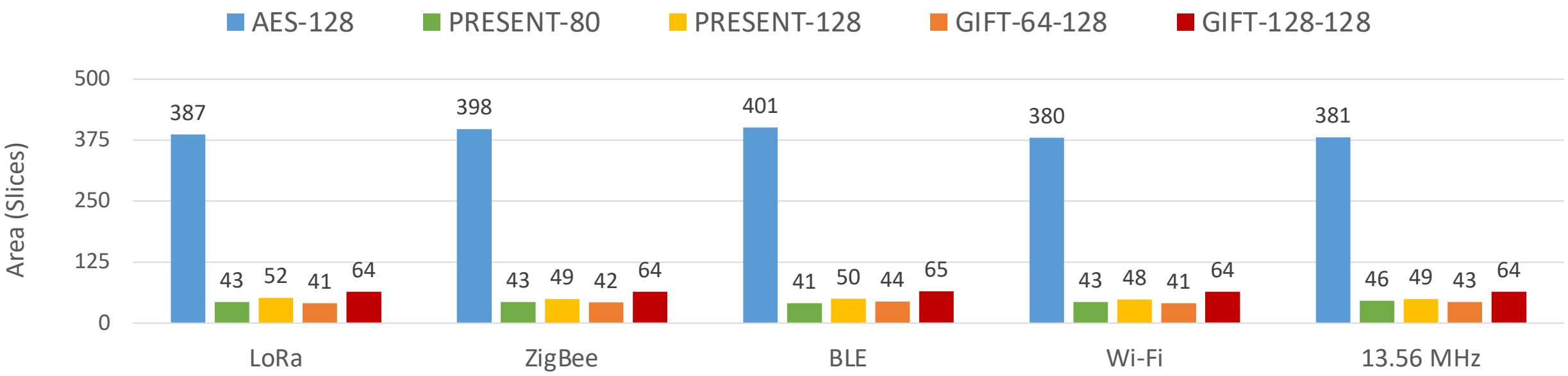


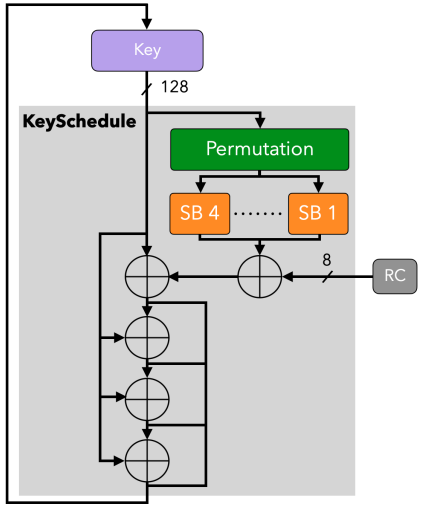


PRESENT-128

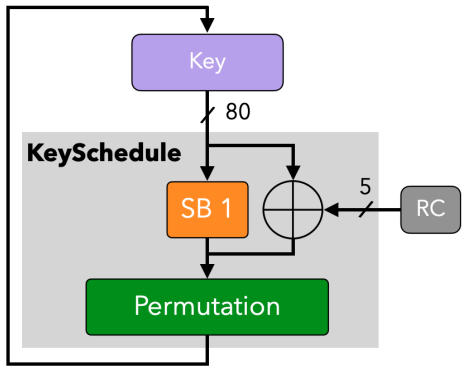


Crypto-Ciphers Performances Evaluations

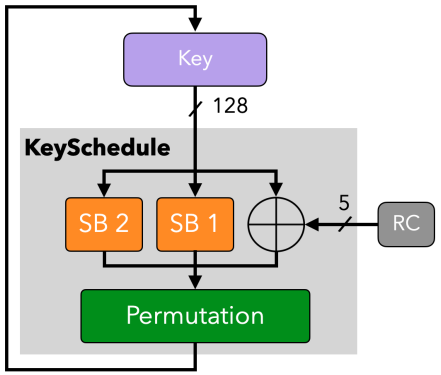




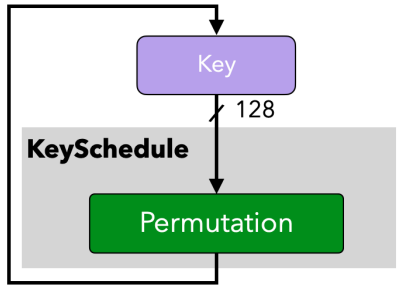
AES-128



PRESENT-80



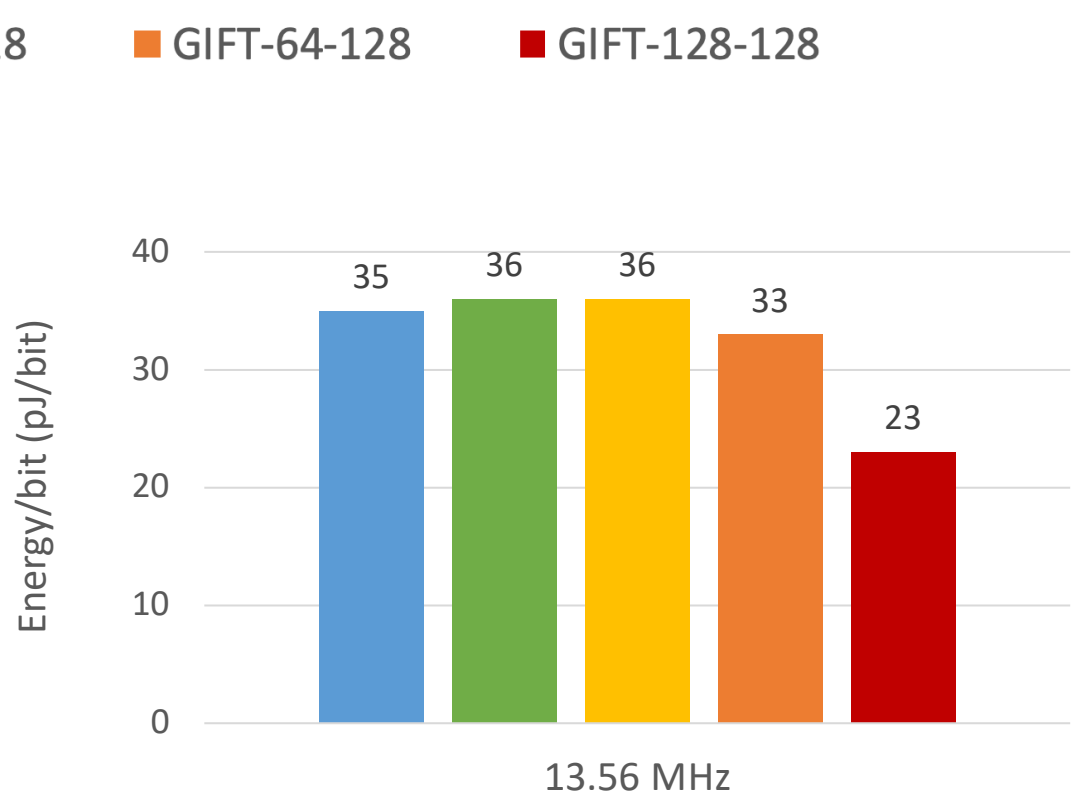
PRESENT-128



GIFT-64-128
GIFT-128-128

Crypto-Ciphers Performances Evaluations

Algorithms	Key Size (bits)	Data Size (bits)	Rounds
AES-128	128	128	10
PRESENT-80	80	64	31
PRESENT-128	128	64	31
GIFT-64-128	128	64	28
GIFT-128-128	128	128	40



$$Power_{AES} = 6\ mW$$

$$Power_{PRESENT/GIFT} = 1\ mW$$

$$Energy_{bit} = \frac{NB_{Rounds} \times Power}{Freq \times Data_{size}}$$

TrustLib Computation Time Evaluations

Computation Time Comparison

Evaluations done on Raspberry Pi 3B+, compiled with *gcc Os* flag

TrustList of 50 Entities

Operations	Computation Time (Average)
Normalization	0.3 - 0.4 µs
Aggregation	0.1 µs
Initialization of the list	1.5 µs
Recover Trust Level	1 µs
Recover Deadline	1 µs
Get most Trusted Node	1.2 µs
Trust Management	4 µs

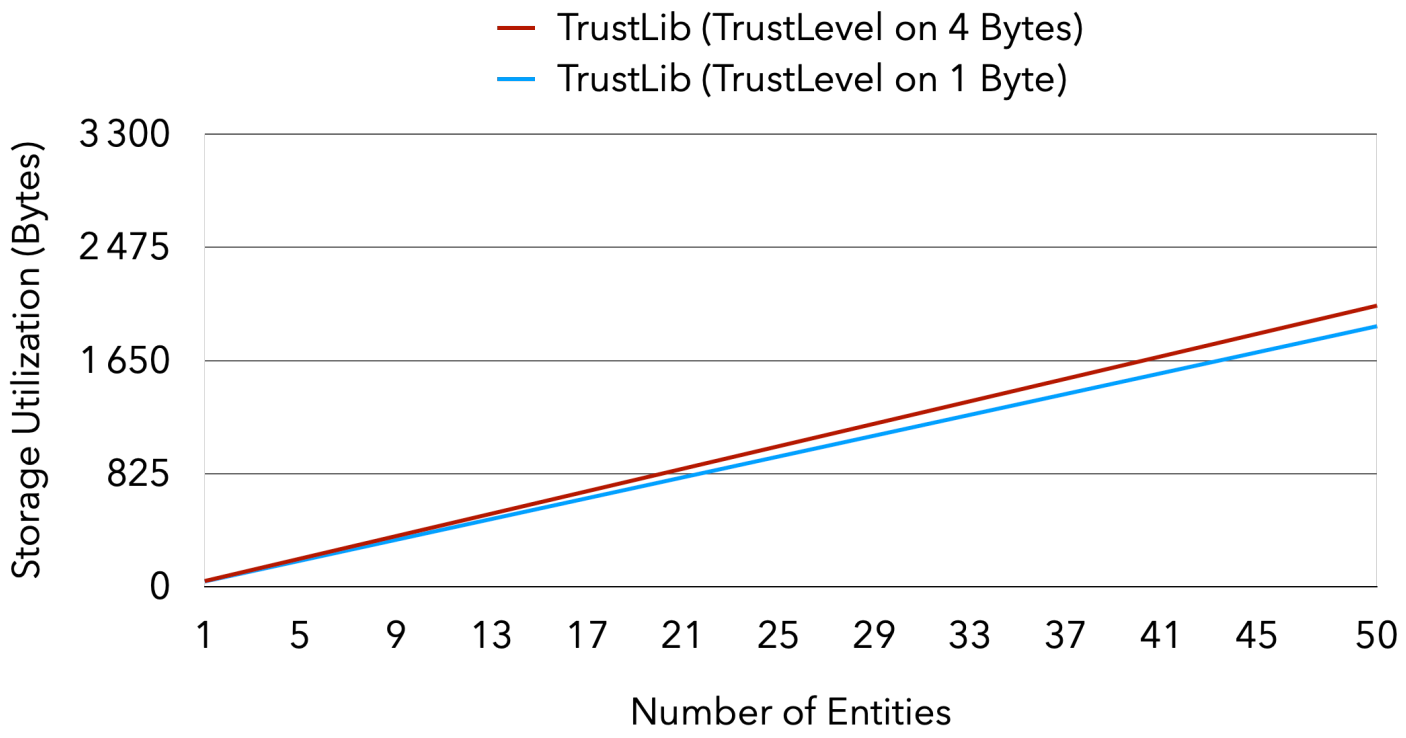
~ 2KB

TrustLib Storage Evaluation

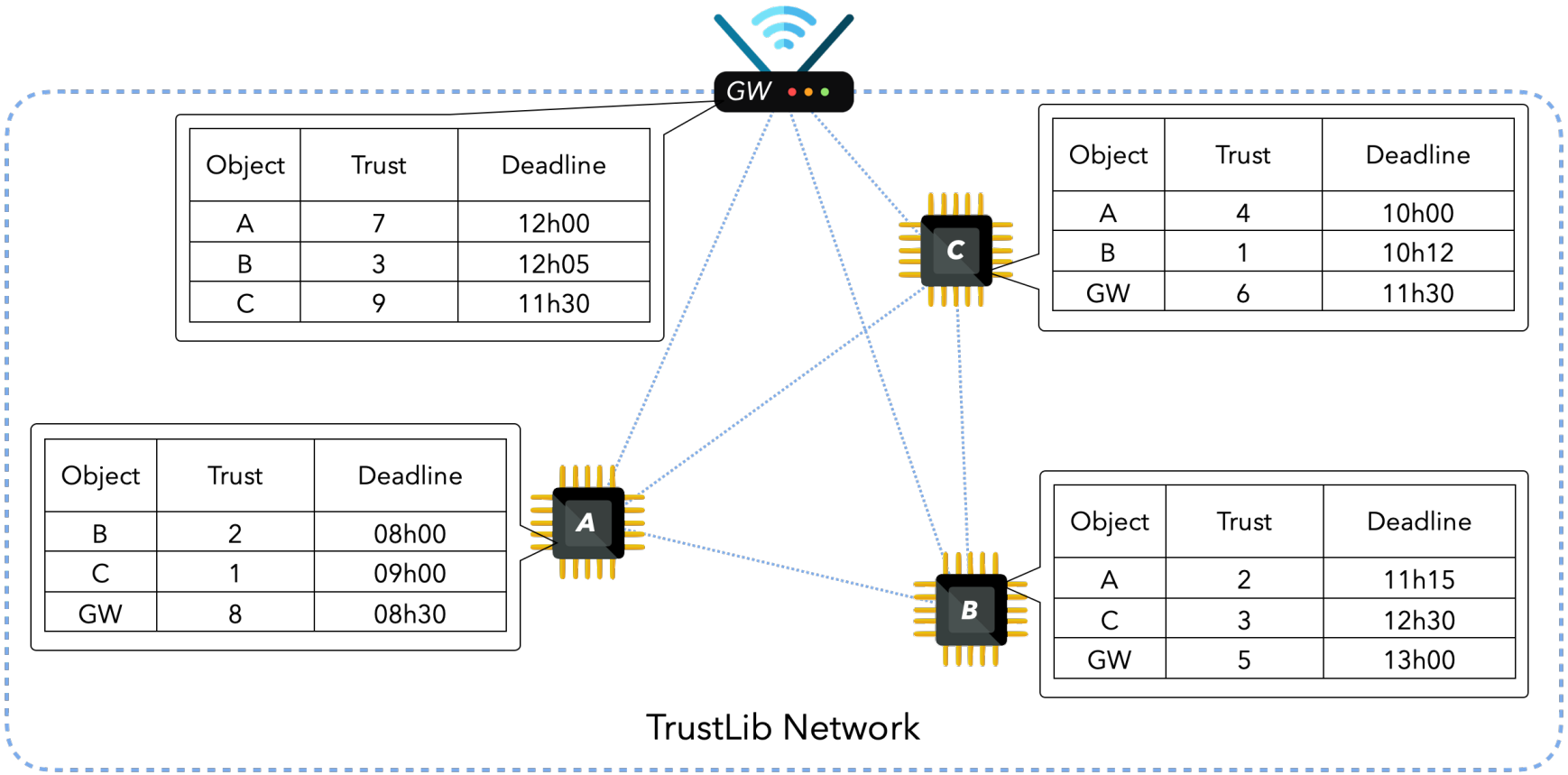
Storage Utilization

Object	Trust	Deadline
33 Bytes	1 - 4 Bytes	4 Bytes

~ 41B



TrustLib Structure



TrustLib Management