NESYA LABORATORY

DIET Dipartimento di Ingegneria dell'Informazione, Elettronica e Telecomunicazioni

Trade-off in Cryptosystems by Boolean and Quantum Circuits

Leonardo Lavagna, Francesca De Falco, Andrea Ceschini, Antonello Rosato, Massimo Panella

Sapienza University of Rome

Department of Information Engineering, Electronics and Telecommunications (DIET)

Finanziato dall'Unione europea NextGenerationEU | Ministero dell'Università e della Ricerca | Italiadomani Piano Nazionale di Ripresa e Resilienza | Sapienza Università di Roma

NESYA
LABORATORY

DIET
Dipartimento di Ingegneria
dell'Informazione,
Elettronica e Telecomunicazioni

Finanziato
dall'Unione europea
NextGenerationEU

Ministero
dell'Università
e della Ricerca

Italiadomani
PIANO NAZIONALE
DI RIPRESA E RESILIENZA

SAPIENZA
UNIVERSITÀ DI ROMA

Motivation & Context

- Classical cryptography aims to construct “high-level” tools, such as encryption schemes, from “low-level” primitives, such as one-way functions

Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA
SAPIENZA UNIVERSITÀ DI ROMA

Motivation & Context

- Classical cryptography aims to construct “high-level” tools, such as encryption schemes, from “low-level” primitives, such as one-way functions
- The main focus is on feasibility and efficiency tradeoffs.

Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA
SAPIENZA UNIVERSITÀ DI ROMA

Motivation & Context

- Classical cryptography aims to construct “high-level” tools, such as encryption schemes, from “low-level” primitives, such as one-way functions
- The main focus is on feasibility and efficiency tradeoffs.
- Quantum cryptography offers remarkable advances

Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA
SAPIENZA UNIVERSITÀ DI ROMA

Motivation & Context

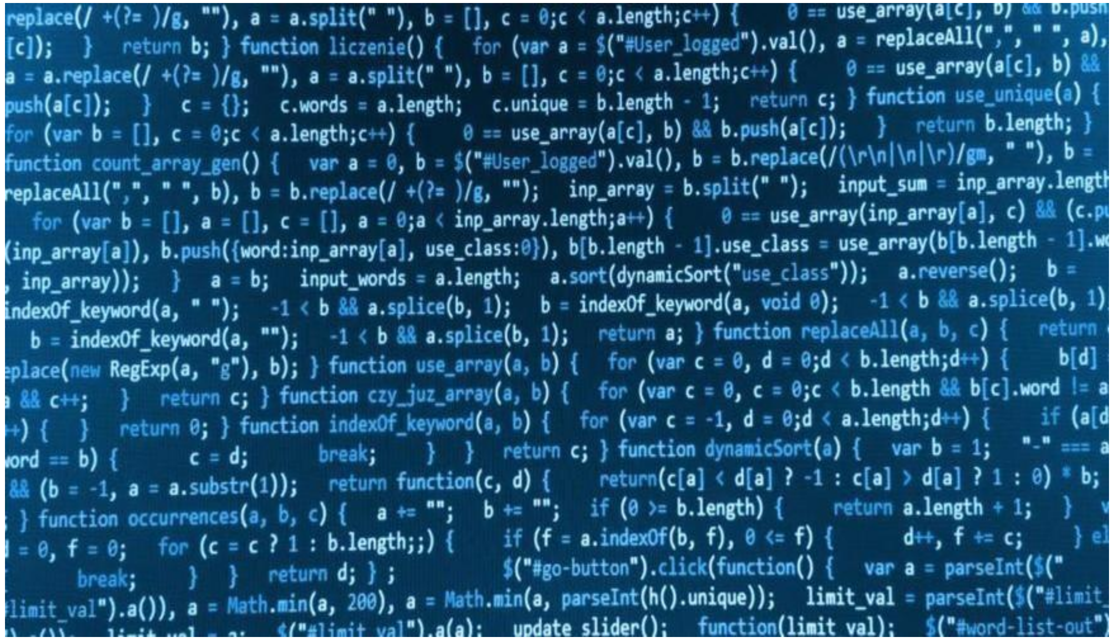
- Classical cryptography aims to construct “high-level” tools, such as encryption schemes, from “low-level” primitives, such as one-way functions
- The main focus is on feasibility and efficiency tradeoffs.
- Quantum cryptography offers remarkable advances
- Feasibility-efficiency trade-offs when transitioning from classical to quantum systems remains underexplored

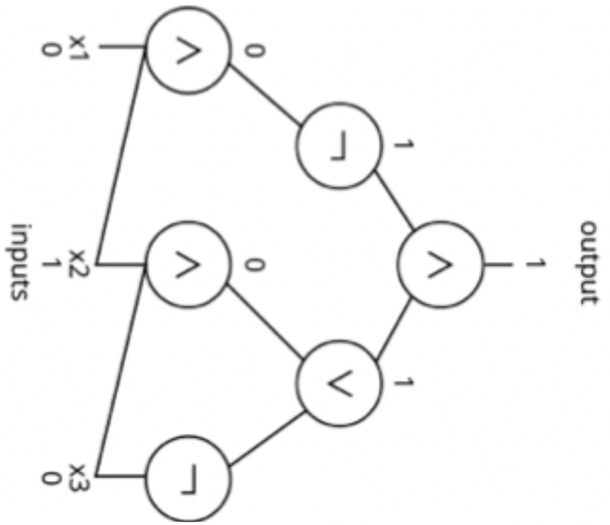
Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA
SAPIENZA UNIVERSITÀ DI ROMA

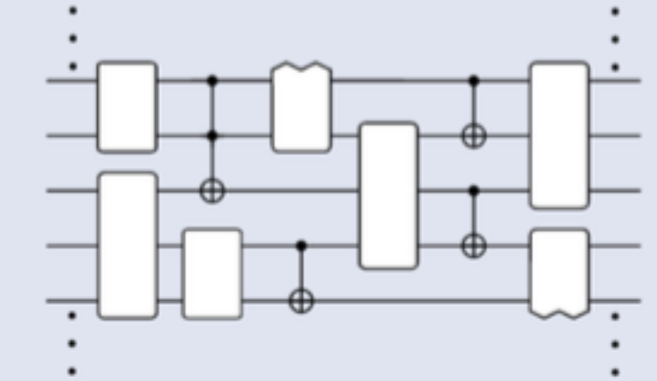
Motivation & Context

- Classical cryptography aims to construct "high-level" tools, such as encryption schemes, from "low-level" primitives, such as one-way functions
- The main focus is on feasibility and efficiency tradeoffs.
- Quantum cryptography offers remarkable advances
- Feasibility-efficiency trade-offs when transitioning from classical to quantum systems remains underexplored
- We explore this topic using a "bijection" between (quantum) cryptosystems and circuit theory

Classical trade-offs







Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA
SAPIENZA UNIVERSITÀ DI ROMA

Theoretical Framework

- Here we focus on trapdoor permutations (low-level) and symmetric encryption schemes (high-level)

Theoretical Framework

- Here we focus on trapdoor permutations (low-level) and symmetric encryption schemes (high-level)
- An attacker has chosen-ciphertext capabilities and oracle access to some parts of the system

Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA
SAPIENZA UNIVERSITÀ DI ROMA

Theoretical Framework

- Here we focus on trapdoor permutations (low-level) and symmetric encryption schemes (high-level)
- An attacker has chosen-ciphertext capabilities and oracle access to some parts of the system
- The systems can be either fully classical, fully quantum, or hybrid

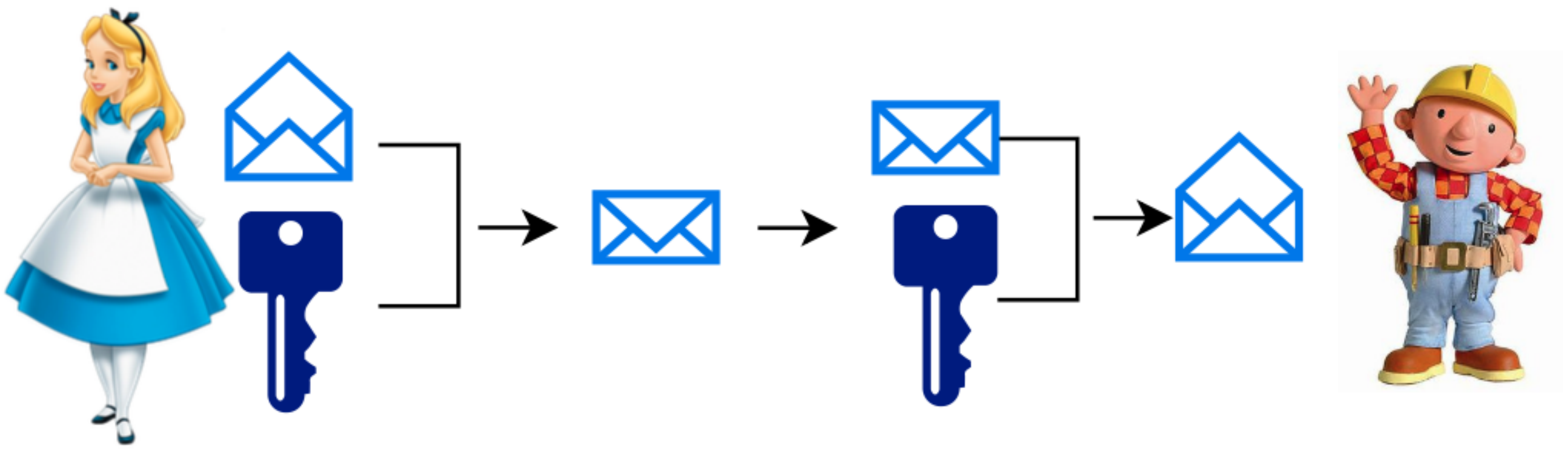
Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA
SAPIENZA UNIVERSITÀ DI ROMA

Theoretical Framework

- Here we focus on trapdoor permutations (low-level) and symmetric encryption schemes (high-level)
- An attacker has chosen-ciphertext capabilities and oracle access to some parts of the system
- The systems can be either fully classical, fully quantum, or hybrid
- Quantum processing will be considered always within NISQ devices

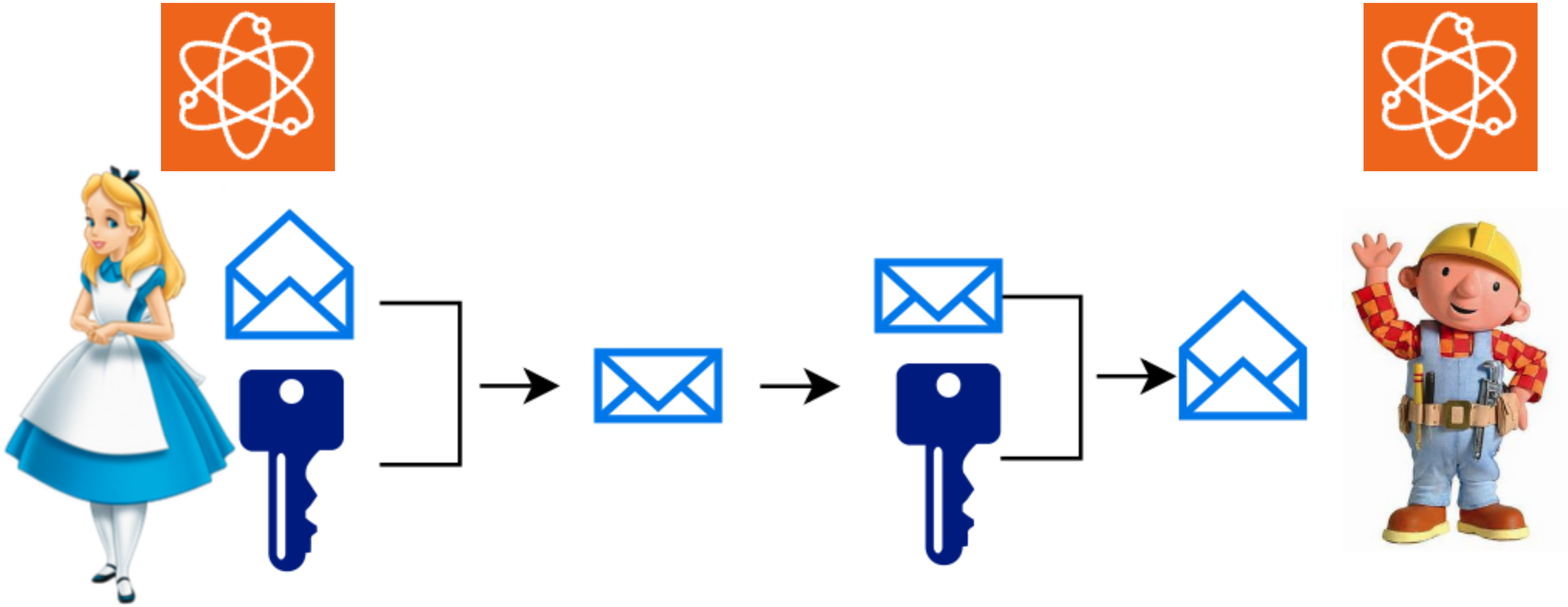
Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA
SAPIENZA UNIVERSITÀ DI ROMA

Theoretical Framework

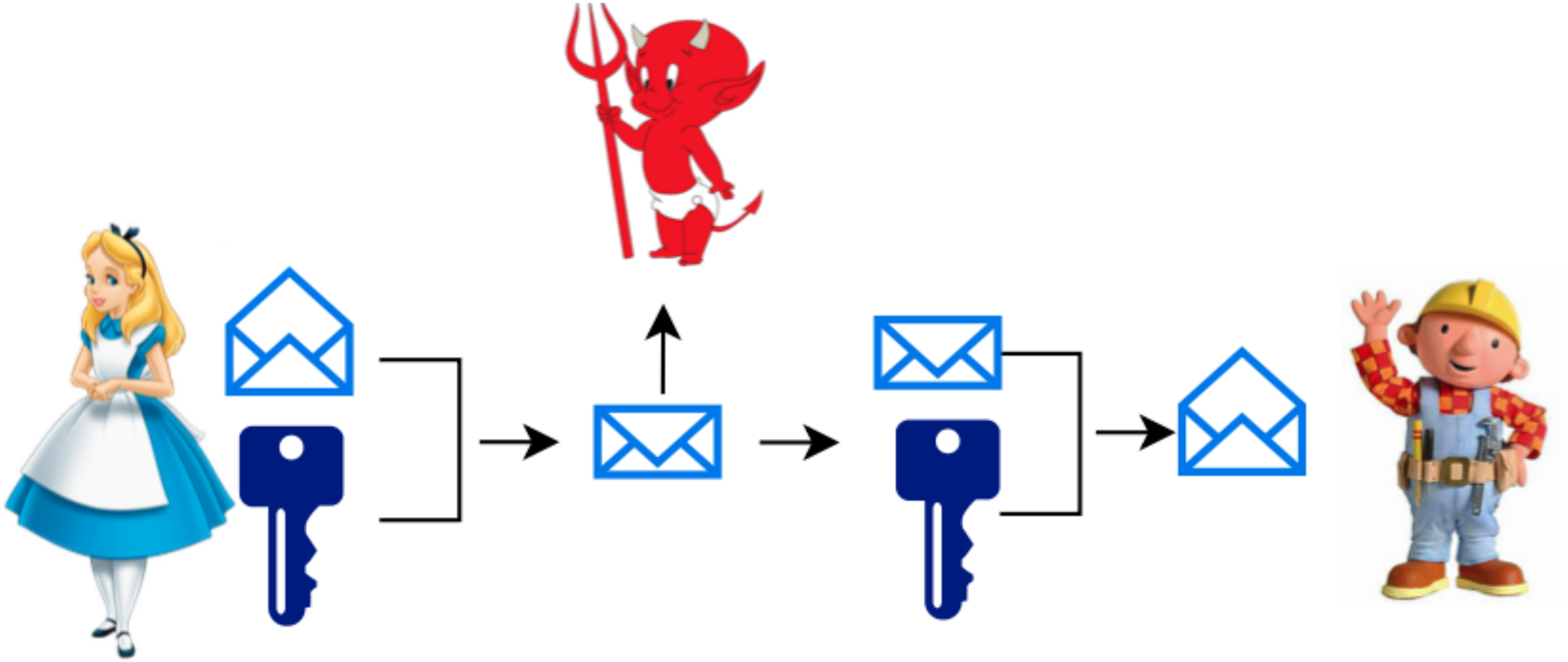


Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA
SAPIENZA UNIVERSITÀ DI ROMA

Theoretical Framework

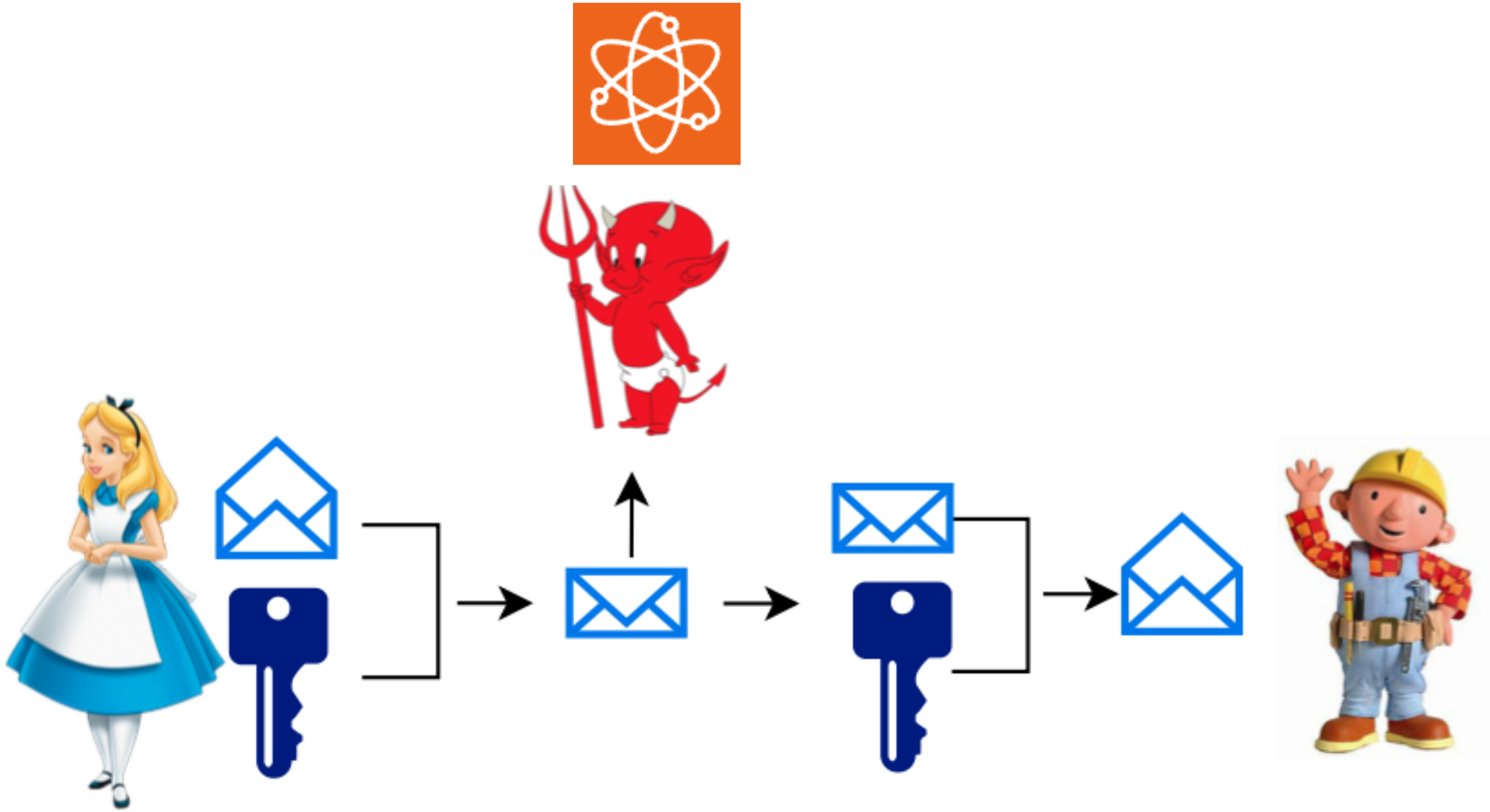


Theoretical Framework

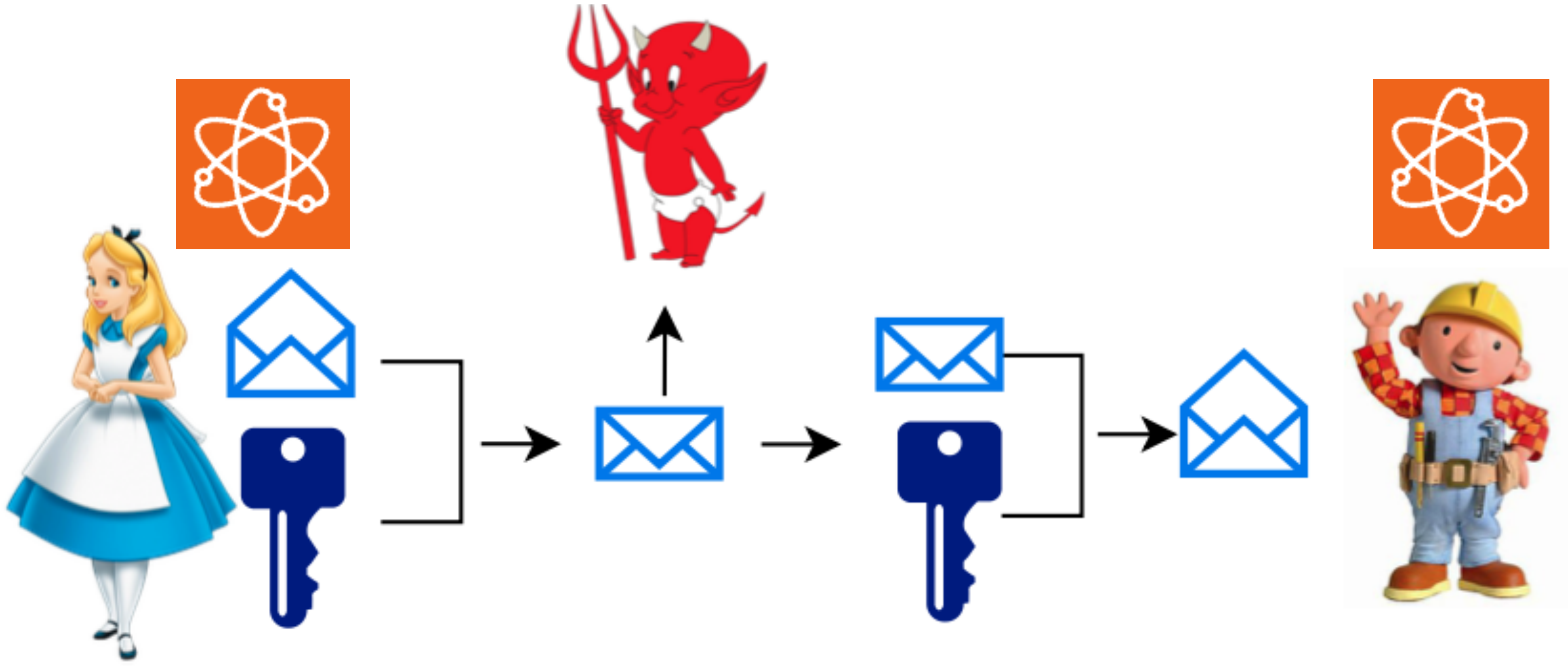


Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA
SAPIENZA UNIVERSITÀ DI ROMA

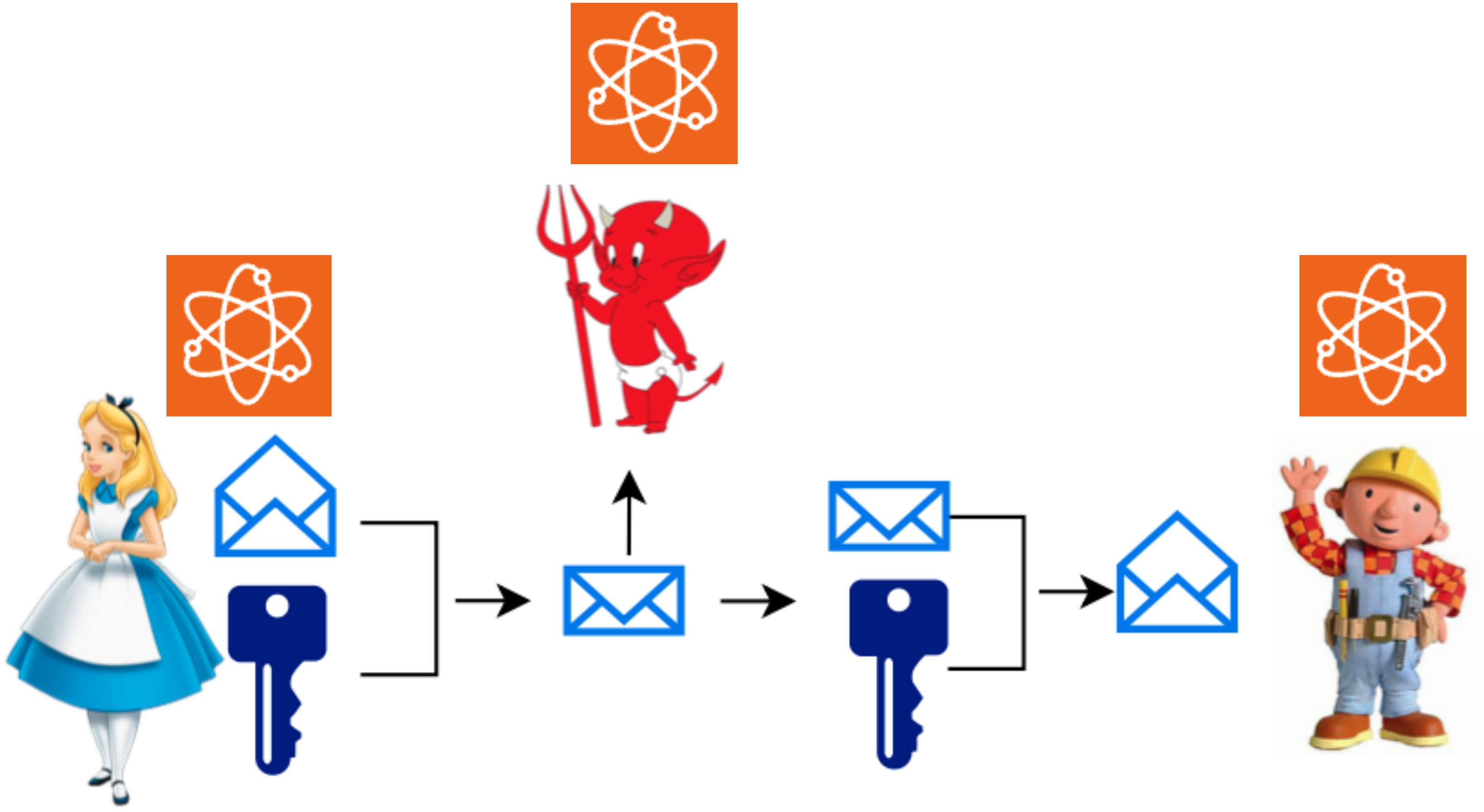
Theoretical Framework



Theoretical Framework



Theoretical Framework



Finanziato
dall'Unione europea
NextGenerationEU

Ministero
dell'Università
e della Ricerca

Italiadomani
PIANO NAZIONALE
DI RIPRESA E RESILIENZA

SAPIENZA
UNIVERSITÀ DI ROMA

Classical trade-offs

- Let $f: \{0,1\}^n \rightarrow \{0,1\}^n$ be a trapdoor permutation computable in the forward direction in $n^{O(1)}$ time. A classical result by Hellman provides key security guarantees.

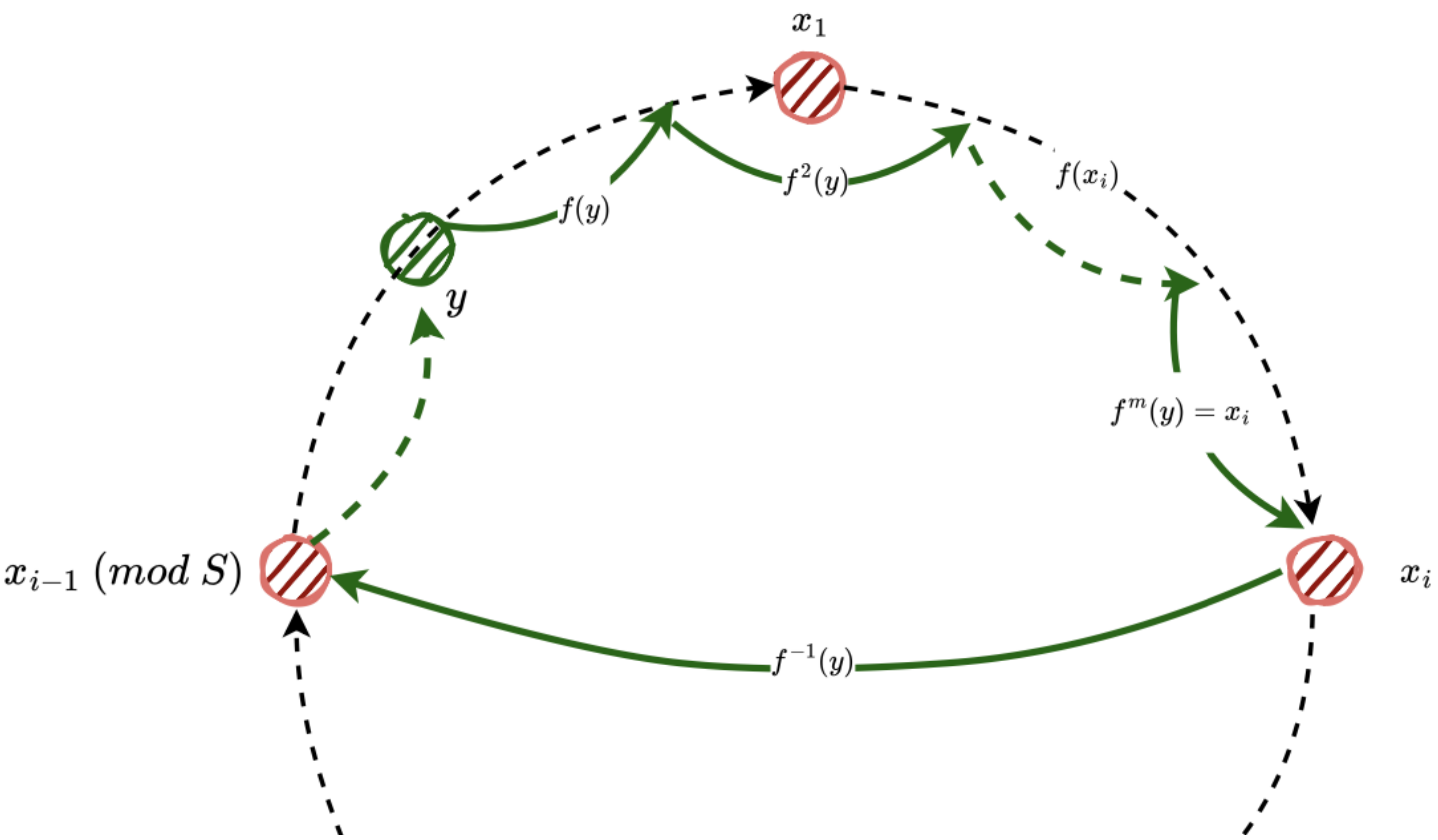
Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA
SAPIENZA UNIVERSITÀ DI ROMA

Classical trade-offs

- Let $f: \{0,1\}^n \to \{0,1\}^n$ be a trapdoor permutation computable in the forward direction in $n^{O(1)}$ time. A classical result by Hellman provides key security guarantees.
- Theorem: There exists a data structure D that occupies $O(nS)$ bits of memory, allowing f to be inverted with a speedup of the order $(n^{O(1)}\, 2^n)/S$.

Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA
SAPIENZA UNIVERSITÀ DI ROMA

Classical trade-offs



Classical trade-offs

- For fixed-size cryptosystems, security can’t rely on efficiency since an algorithm could store the entire lookup table of input-output pairs.

Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA
SAPIENZA UNIVERSITÀ DI ROMA

Classical trade-offs

- For fixed-size cryptosystems, security can’t rely on efficiency since an algorithm could store the entire lookup table of input output pairs.
- Boolean circuit complexity or code length versus running time should be considered

Classical trade-offs

- For fixed-size cryptosystems, security can't rely on efficiency since an algorithm could store the entire lookup table of input output pairs.
- Boolean circuit complexity or code length versus running time should be considered
- The tight bound is $mt = \Theta(\epsilon 2^n)$.

Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA
SAPIENZA UNIVERSITÀ DI ROMA

Classical trade-offs

- The relationship between one-way functions and encryption schemes follows by mapping messages M of length $|\mathrm{M}|$ and keys a of length $|\mathrm{a}|$ to ciphertexts via $(\mathrm{M}, \mathrm{a}) \longrightarrow \mathrm{Enc}(\mathrm{M}, \mathrm{a})$

Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA
SAPIENZA UNIVERSITÀ DI ROMA

Classical trade-offs

- The relationship between one-way functions and encryption schemes follows by mapping messages M of length $|M|$ and keys a of length $|a|$ to ciphertexts via $(M, a) \longrightarrow \mathrm{Enc}(M, a)$
- The security bounds for f generalize to encryption schemes.

Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani Piano Nazionale di Ripresa e Resilienza
SAPIENZA Università di Roma

Classical trade-offs

- The relationship between one-way functions and encryption schemes follows by mapping messages M of length $|M|$ and keys a of length $|a|$ to ciphertexts via $(M, a) \longrightarrow \mathrm{Enc}(M, a)$
- Security bounds for f generalize to encryption schemes.
- On the other hand, if an encryption scheme is based on f and an adversary is an oracle algorithm, looking at the hardness of f can yield useful information on the overall security.

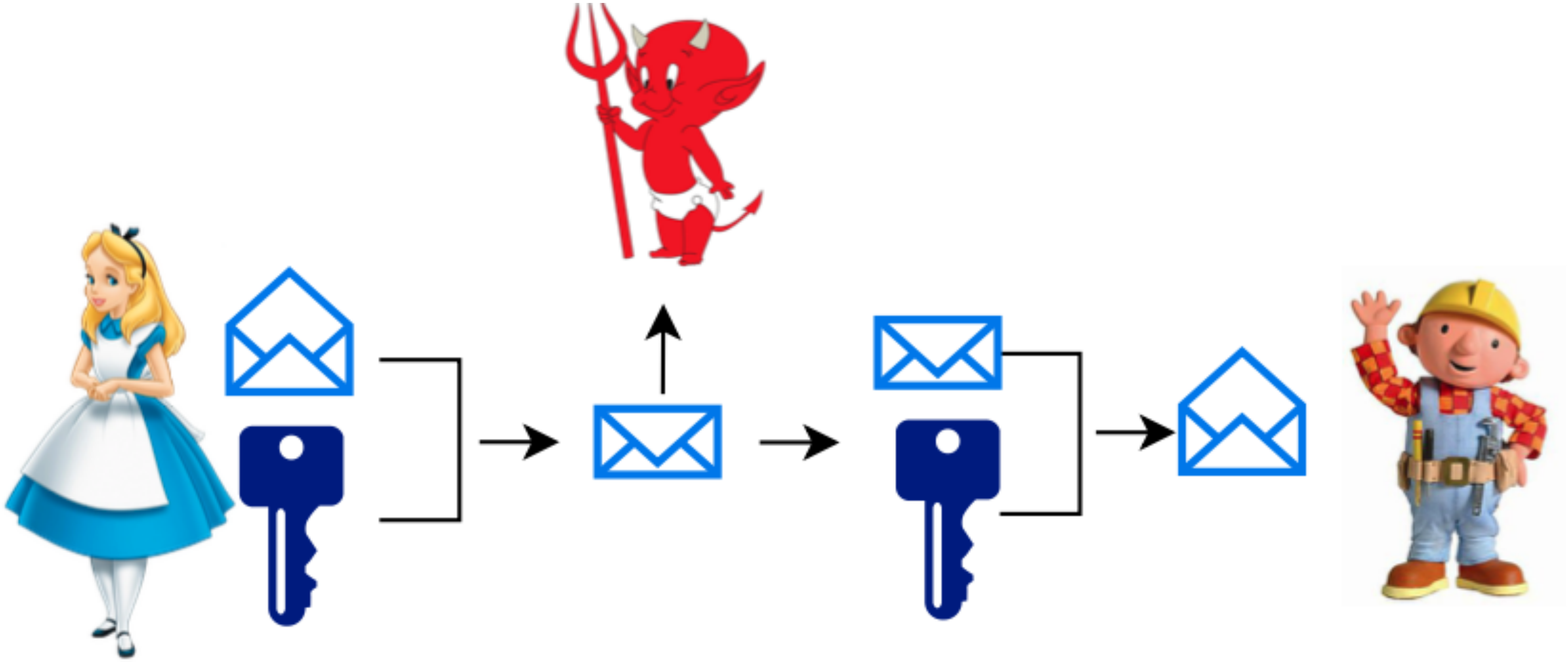
Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA
SAPIENZA UNIVERSITÀ DI ROMA

From classical to quantum trade-offs

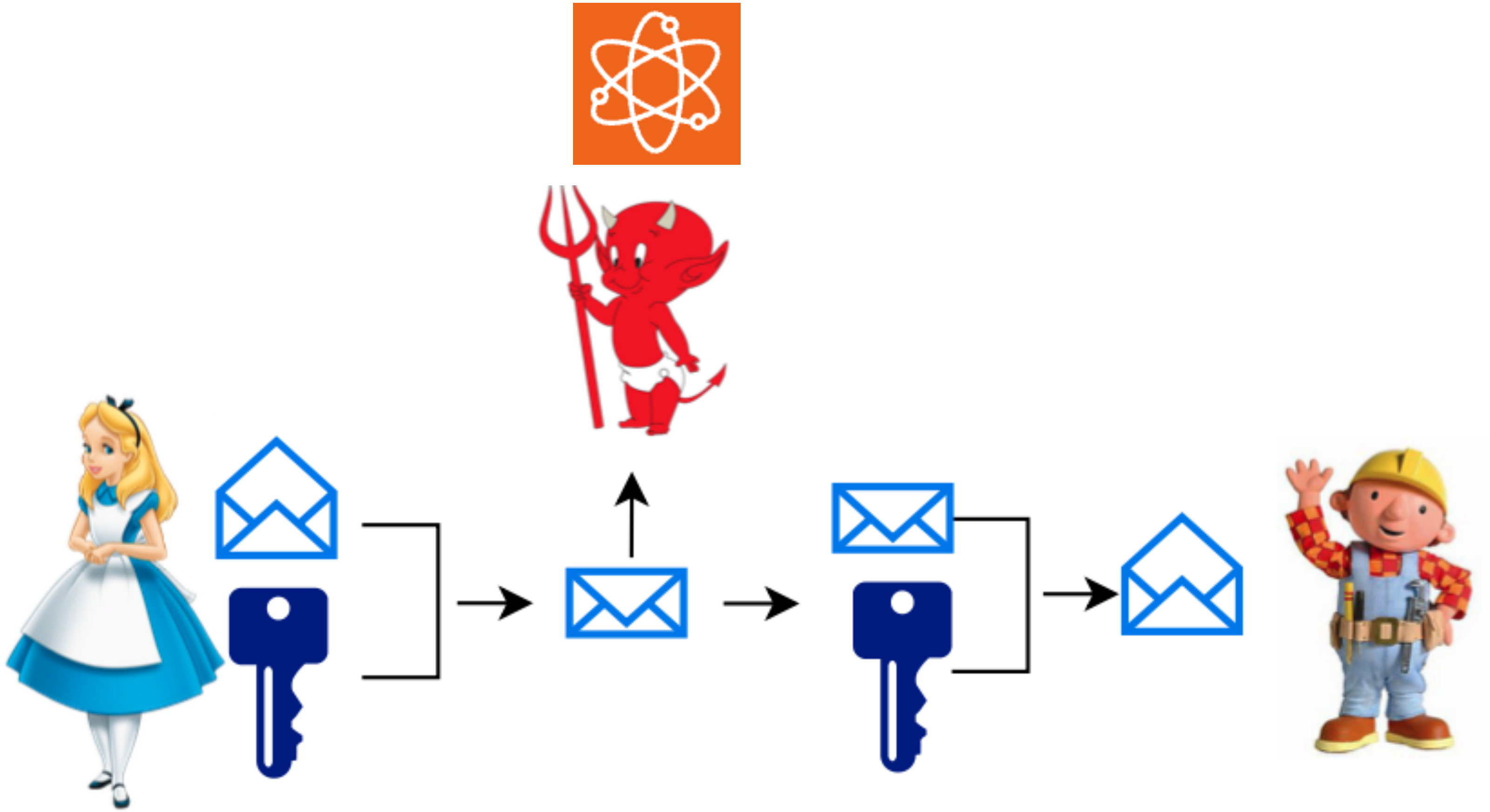
- Theorem: Unless Enc queries f at least a number of times $T = \Omega((|M|\text{-}c)/\log S)$, where for a public-key encryption scheme $c=0$ and for a a private-key encryption $c=|a|$, an unconditional one-way function exists

Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA
SAPIENZA UNIVERSITÀ DI ROMA

Theoretical Framework



The NISQ case



From classical to quantum trade-offs

- Theorem: Unless Enc queries f at least a number of times $T = \Omega((|M| - c)/\log S)$, where for a public-key encryption scheme $c=0$ and for a a private-key encryption $c=|a|$, an unconditional one-way function exists
- What happens in a fault-tolerant quantum setting?

Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA
SAPIENZA UNIVERSITÀ DI ROMA

From classical to quantum trade-offs

- Theorem: Unless Enc queries f at least a number of times $T = \Omega((|M|-c)/\log S)$, where for a public-key encryption scheme $c=0$ and for a a private-key encryption $c=|a|$, an unconditional one-way function exists
- What happens in a fault-tolerant quantum setting?
- From Grover's algorithm we gain a quadratic speedup!

Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA
SAPIENZA UNIVERSITÀ DI ROMA

From classical to quantum trade-offs

- Theorem: With advice of size S and a fault-tolerant quantum computation, inverting f is possible with time
$$\Omega(\sqrt{2^n}/S) \leq T \leq \min\{O(\sqrt{2^n}), O(2^n/S)\}$$

Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA
SAPIENZA UNIVERSITÀ DI ROMA

From classical to quantum trade-offs

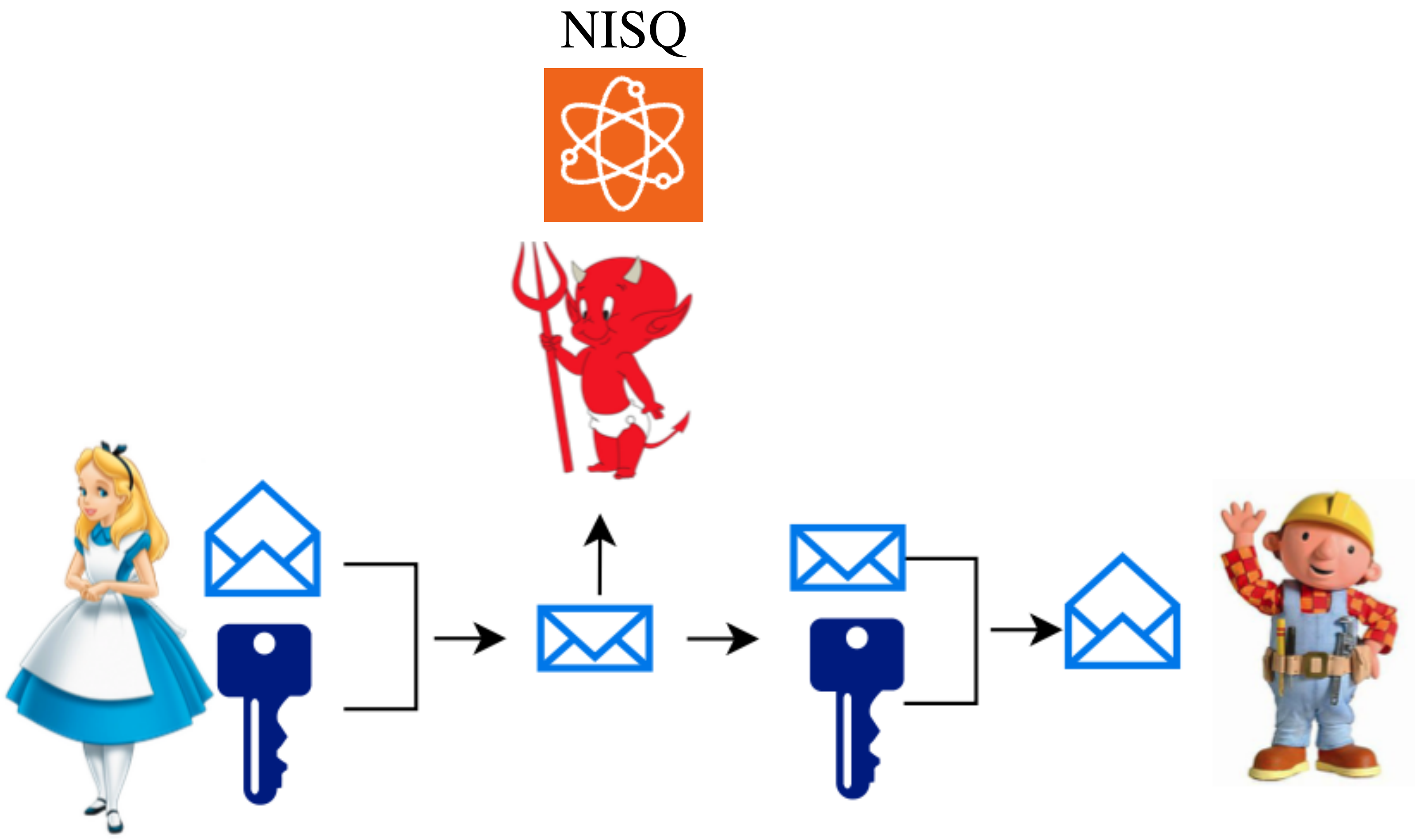
- Theorem: With advice of size S and a fault-tolerant quantum computation, inverting f is possible with time
$$\Omega(\sqrt{2^n}/S) \leq T \leq \min\{O(\sqrt{2^n}), O(2^n/S)\}$$
- If $S \leq \sqrt{2^n}$, there is no quantum advantage, while for $S \geq \sqrt{2^n}$, the quantum algorithm inverts f in time $t = O(\epsilon\, 2^n)$ and advice plays no role.

The NISQ case

- But fault-tolerance is far ahead...

Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA
SAPIENZA UNIVERSITÀ DI ROMA

The NISQ case

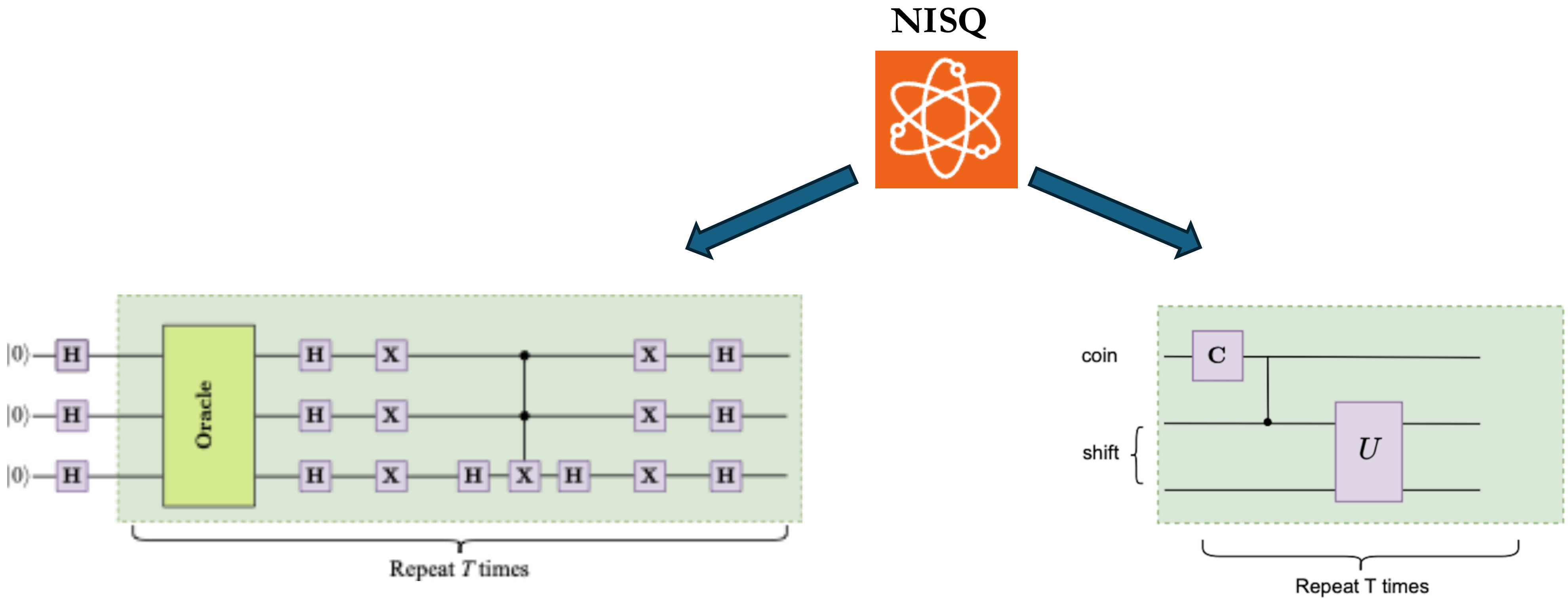


The NISQ case

- But fault-tolerance is far ahead…
- We can consider Variational Quantum Algoritms (VQAs, or parameterized quantum circuits) and Quantum Walks

Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA
SAPIENZA UNIVERSITÀ DI ROMA

The NISQ case



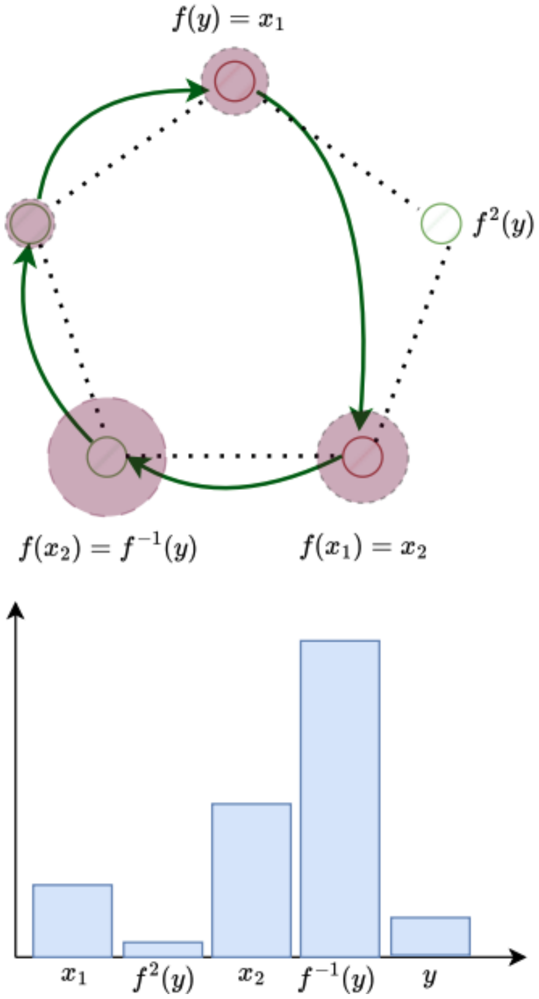
Finanziato dall'Unione europea
NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani
PIANO NAZIONALE DI RIPRESA E RESILIENZA
SAPIENZA
UNIVERSITÀ DI ROMA

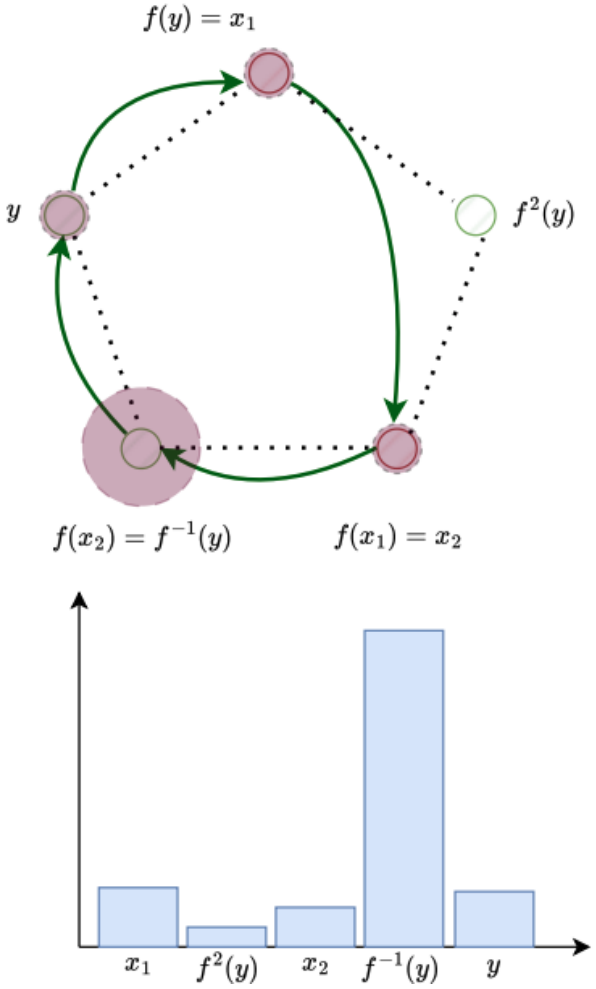
The NISQ case

- But fault-tolerance is far ahead…
- We can consider Variational Quantum Algoritms (VQAs, or parameterized quantum circuits) and Quantum Walks
- Theorem: Having access to advice of size S and a NISQ device to invert f with error δ, if E is classical encryption scheme based on a at least S-hard primitive, if A_{NISQ} is a NISQ adversary, then A_{NISQ} breaks E with probability $> \epsilon$ when $T = \Omega(\epsilon^{-2}\delta\sqrt{(|M| - c)/S})$ with $c = |a|$ in the symmetric case and $c = 0$ in the asymmetric case.

Finanziato dall'Unione europea
NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani
PIANO NAZIONALE DI RIPRESA E RESILIENZA
SAPIENZA
UNIVERSITÀ DI ROMA

The NISQ case





The NISQ case

- We report a comparison between chosen-ciphertext attacks on Caesar's cipher and a quantum walk attack using 100 random strings of length 5

The NISQ case

- We report a comparison between chosen-ciphertext attacks on Caesar’s cipher and a quantum walk attack using 100 random strings of length 5
- A classical frequency-based attack yields a success probability of $0.01 < \epsilon < 0.1$

The NISQ case

- We report a comparison between chosen-ciphertext attacks on Caesar's cipher and a quantum walk attack using 100 random strings of length 5
- A classical frequency-based attack yields a success probability of $0.01 < \epsilon < 0.1$
- A quantum walk achieves $0.3\epsilon < \epsilon' < 1.6\epsilon$

The NISQ case

- We report a comparison between chosen-ciphertext attacks on Caesar's cipher and a quantum walk attack using 100 random strings of length 5
- A classical frequency-based attack yields a success probability of $0.01 < \epsilon < 0.1$
- A quantum walk achieves $0.3\epsilon < \epsilon' < 1.6\epsilon$
- Similar, but worse, results occur with noisy Grover's algorithm, indicating that NISQ advice is unreliable, and classical methods are likely more advantageous

Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA
SAPIENZA UNIVERSITÀ DI ROMA

Conclusions & Future work

- We examined the intersection of classical cryptography and NISQ quantum circuits

Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA
SAPIENZA UNIVERSITÀ DI ROMA

Conclusions & Future work

- We examined the intersection of classical cryptography and NISQ quantum circuits
- We analyzed feasibility-efficiency trade-offs and security implications

Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA
SAPIENZA UNIVERSITÀ DI ROMA

Conclusions & Future work

- We examined the intersection of classical cryptography and NISQ quantum circuits
- We analyzed feasibility-efficiency trade-offs and security implications
- Our findings suggest that the inclusion of noisy quantum tools may compromise the security of cryptographic systems that rely on trapdoor permutations as a primitive or model for encryption, but this scenario is unlikely with current devices, as shown also by the experiments

Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA
SAPIENZA UNIVERSITÀ DI ROMA

Conclusions & Future work

- We are expanding the application domain to PRGs, signature schemes, etc…

Conclusions & Future work

- We are expanding the application domain to PRGs, signature schemes, etc…
- We have to analyze the case of quantum attackers against quantum cryptosystems

Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA
SAPIENZA UNIVERSITÀ DI ROMA

Conclusions & Future work

- We are expanding the application domain to PRGs, signature schemes, etc...
- We have to analyze the case of quantum attackers against quantum cryptosystems
- We have to understand the tightness of the results

Finanziato dall'Unione europea
NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani
PIANO NAZIONALE DI RIPRESA E RESILIENZA
SAPIENZA
UNIVERSITÀ DI ROMA

References

- M. Hellman, “A cryptanalytic time-memory trade-off,” IEEE Transactions on Information Theory, vol. 26, no. 4, pp. 401–406, 1980.
- R. Gennaro, Y. Gertner, J. Katz, and L. Trevisan, “Bounds on the efficiency of generic cryptographic constructions,” SIAM Journal on Computing, vol. 35, no. 1, pp. 217–246, 2005.
- Nayebi, S. Aaronson, A. Belovs, and L. Trevisan, “Quantum lower bound for inverting a permutation with advice,” 2015.

Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA
SAPIENZA UNIVERSITÀ DI ROMA

NESYA LABORATORY

DIET
Dipartimento di Ingegneria dell'Informazione, Elettronica e Telecomunicazioni

Thank you!

Contacts

- https://sites.google.com/view/nesya
- leonardo.lavagna@uniroma1.it
- https://github.com/leonardoLavagna/Iscas2025

Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA
SAPIENZA UNIVERSITÀ DI ROMA