A quantum-resistant unlinkable and strongly-unsplittable multi-coupon system

#ProyectosCiber

Sergi Simón Balcells

2025/04/01

Financiado por la Unión Europea
NextGenerationEU

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES

Plan de Recuperación, Transformación y Resiliencia

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

Acknowledgements

Esta investigación resulta del Proyecto Estratégico 'Avances en criptografía post-cuántica aplicados al desarrollo de un sistema de cupones' (C039/24), fruto del convenio de colaboración suscrito entre el Instituto Nacional de Ciberseguridad (INCIBE) y la Universidad de Lleida. Esta iniciativa se realiza en el marco de los fondos del Plan de Recuperación, Transformación y Resiliencia, financiados por la Unión Europea (Next Generation).

Outline

Multi-coupon system

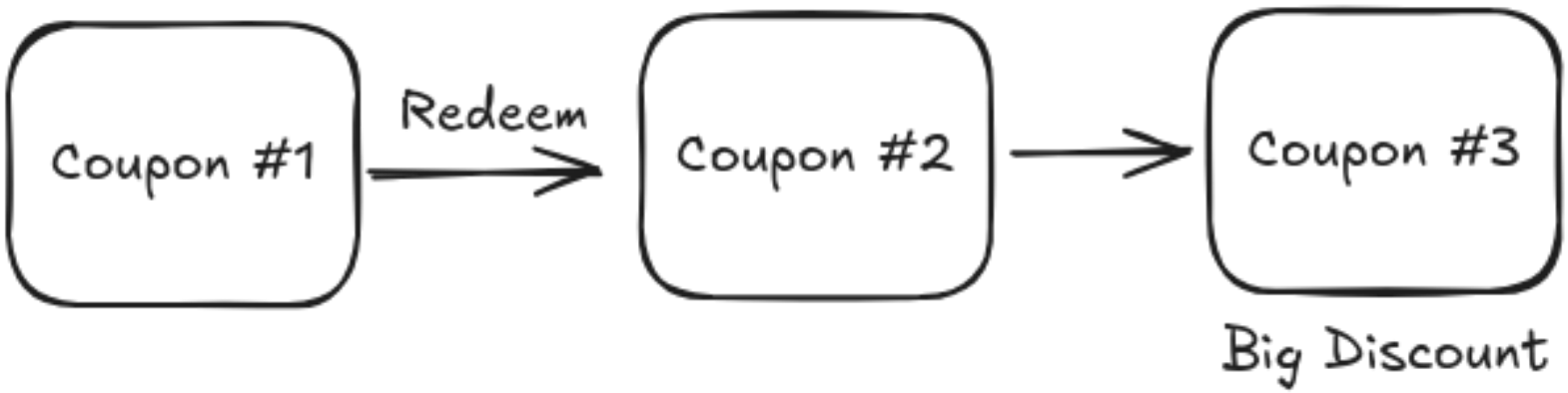

Figure: Schematic of a multi-coupon system

Multi-coupon redeem

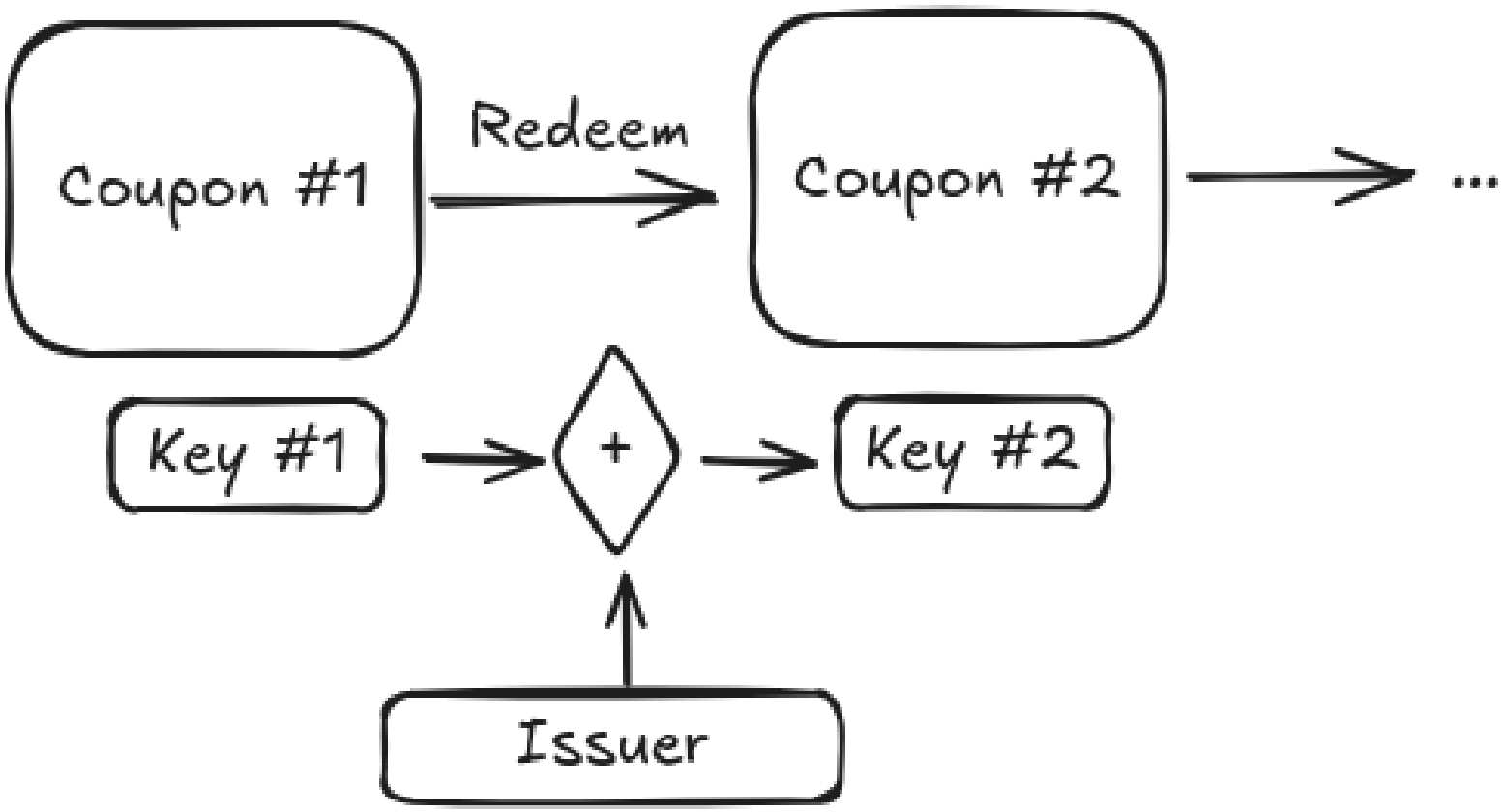

Figure: Redeem token with the issuer.

Privacy Requirements

1. The tokens redeemed are unlinkable.

Privacy Requirements

1. The tokens redeemed are unlinkable.
2. The tokens are unforgeable.

Privacy Requirements

1. The tokens redeemed are unlinkable.
2. The tokens are unforgeable.
3. The multi-coupon system is strongly unsplittable.

Privacy Requirements

1. The tokens redeemed are unlinkable.
2. The tokens are unforgeable.
3. The multi-coupon system is strongly unsplittable.
4. The employed cryptography is quantum-resistant.

A Post-Quantum Approach: Results

Table: Running times in milliseconds (ms) of the procedures composing the multi-coupon system.

Processor	Set up	Token creation	Token redemption
i7-6700HQ	13059.45	127.07	150.46
Ryzen 5 3600	9258.17	103.41	125.29
i7-9700K	9249.97	93.80	111.69
i7-12700H	4949.05	60.89	79.41

- Python and SageMath implementation.
- Network cost is 0.

Thanks for your attention