Gizem Akman
Valtteri Niemi
Department of Computer Science, University of Helsinki

Anonymous Location-Based Advertising with Fine-Grained Statistics

EC-APP is an application that grants to its users e-coupons for shops when they are near the shopping mall that hosts the shops.

E-coupons

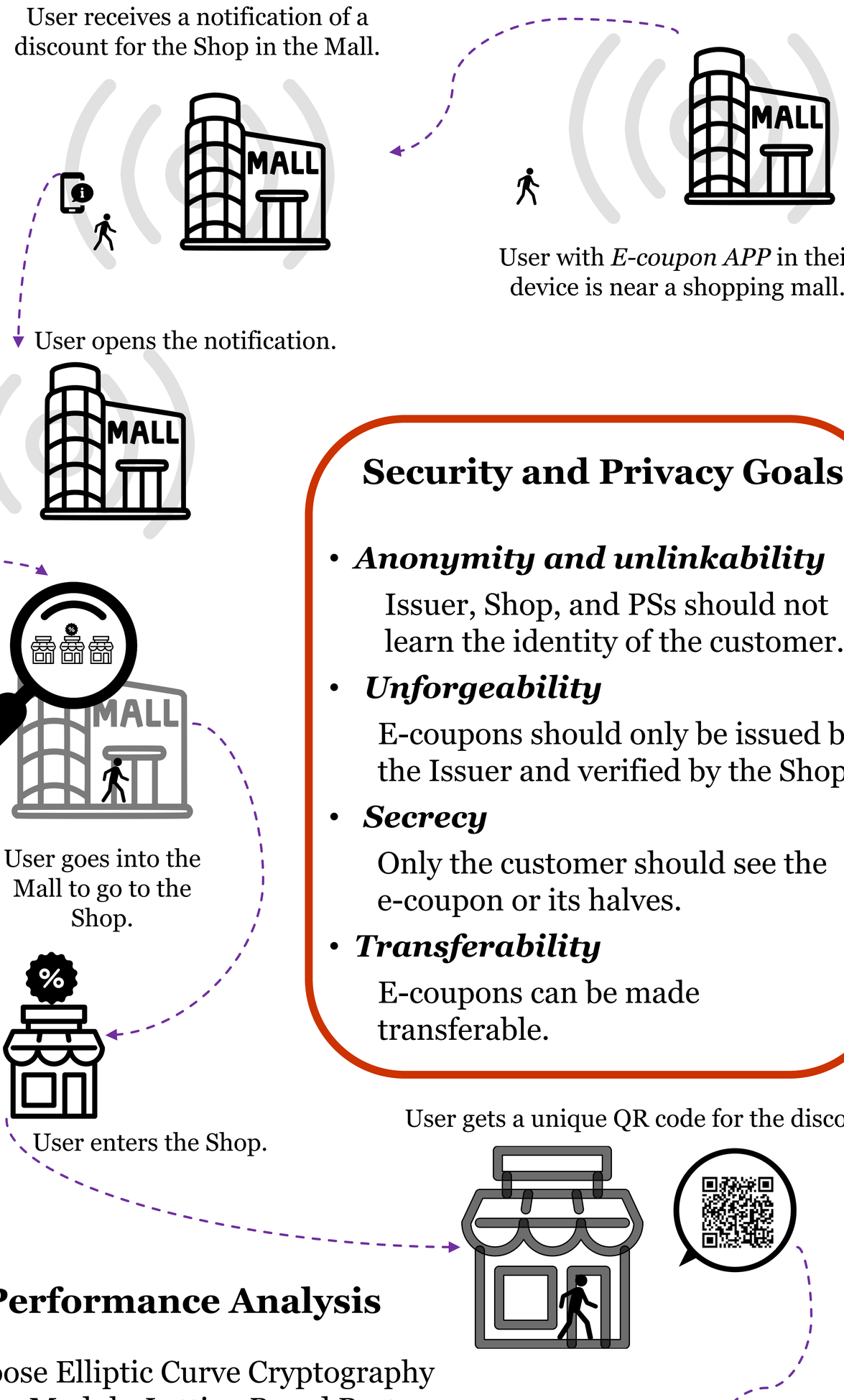
- Essential for digital marketing.
- Counterfeit coupons, phishing scams, and malware attacks pose risks to both businesses and customers.
- Proximity marketing uses location-based technologies to engage customers in real-time.
- Businesses can send personalized offers to customers in proximity, enhancing engagement and conversion rates.

Marketing Goals

Giving e-coupons as advertisements to the EC-APP users.

To improve marketing, the Issuer wants to know how many customers

1) get the e-coupon for a Shop,
2) go to the Shop with the e-coupon,
3) eventually use the e-coupon.



Security and Privacy Goals

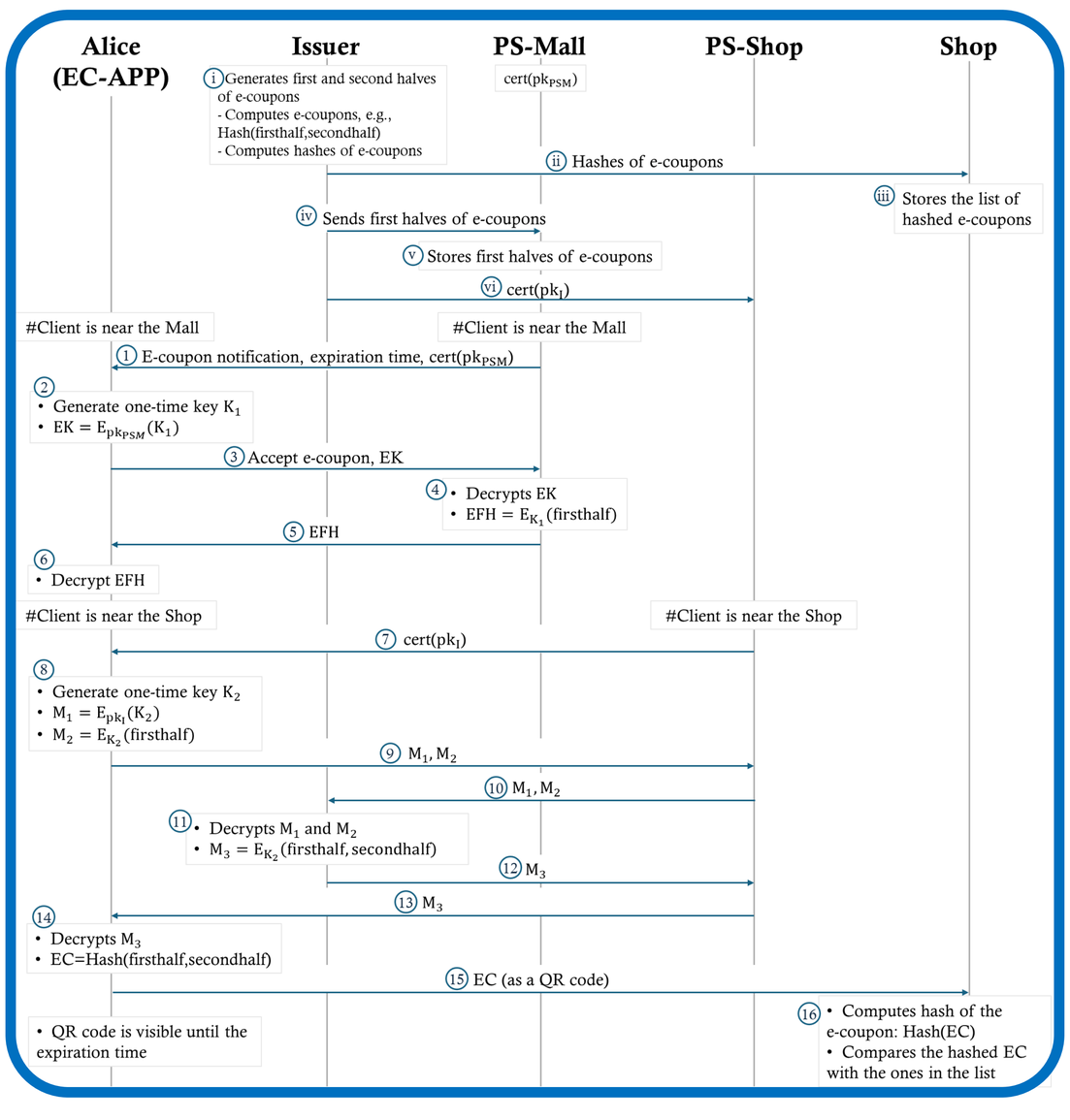
- ***Anonymity and unlinkability***
  Issuer, Shop, and PSs should not learn the identity of the customer.
- ***Unforgeability***
  E-coupons should only be issued by the Issuer and verified by the Shop.
- ***Secrecy***
  Only the customer should see the e-coupon or its halves.
- ***Transferability***
  E-coupons can be made transferable.

Variants for the Protocol

We propose two variants of the e-coupon distribution protocol: the e-coupon parts are delivered by the Issuer

(1) through EC-APP or

(2) through proximity services (PSs).



Performance Analysis

We choose Elliptic Curve Cryptography (ECC) or Module-Lattice-Based Post-Quantum Cryptography (ML) as public key primitives.

The communication cost is 64·n+1240 or 64·n+9548 bytes, considering ECC and ML, resp.

The computation time* of the protocol is 459.88 µs and 273.80 µs, considering ECC and ML, resp. for n=1000 coupons.

*Computed with OpenSSL 3.5.0 on an x86-64 machine with Linux kernel version 6.14.0-37-generic

Implementation, Performance and Security Analysis Source codes