TrustED 2011

µPay: NFC-Based Micropayment System and its Android Implementation

Mauro Conti*, Hendri Appelmelk*, **Earlence Fernandes*** and Bruno Crispo**

*   Vrije Universiteit Amsterdam
** University of Trento

Introduction/NFC/Micropayment

Significant Related Research

µPay Micropayment System

- Protocol Overview
- Android Implementation

Evaluation

Introduction

A micropayment is a financial transaction involving a very small sum of money which therefore allows relaxed security.

The money involved in a micropayment transaction should have the same properties as “real” money:

- Acceptability
- Anonymity
- Speed
- Offline
- Cost
- Non-Traceability
- Invention
- Overspending

Near Field Communication

- Proximity based Communication

(13.56 MHz, 106-424 Kbits/s, ~4 cm)

- Short Distances

- Low cost link setup (comparatively, eg: Bluetooth)

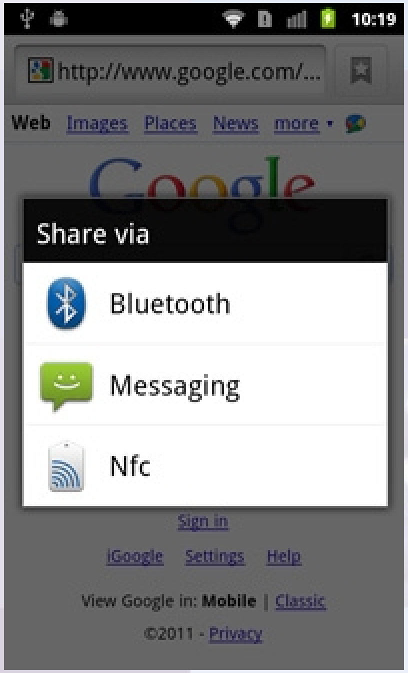
- Standardized (ISO/IEC 18092, 21481)

Really hot right now. (read: Google Android NFC)

Near Field Communication

NFC enables:

1. Electronic Ticketing
2. Payments in Public Transport
3. Electronic Boarding Passes
4. …



Share via

Bluetooth

Messaging

Nfc

Related Research (1/2)

Ron Rivest and Adi Shamir – PayWord (1997) *

- A chain of hash values
- Each element of the chain represents a “PayWord” which is “money”
- Items to be bought are worth one or a multiple of “PayWords”
- **Each hash chain can only be spent at a single vendor**

* - R. Rivest and A. Shamir, “Payword and micromint: Two simple micropayment schemes,” in Security Protocols, pp. 69–87. 1997

Related Research (2/2)

E. Blass et al. - PSP: Private and Secure Payment with RFID (2009) *

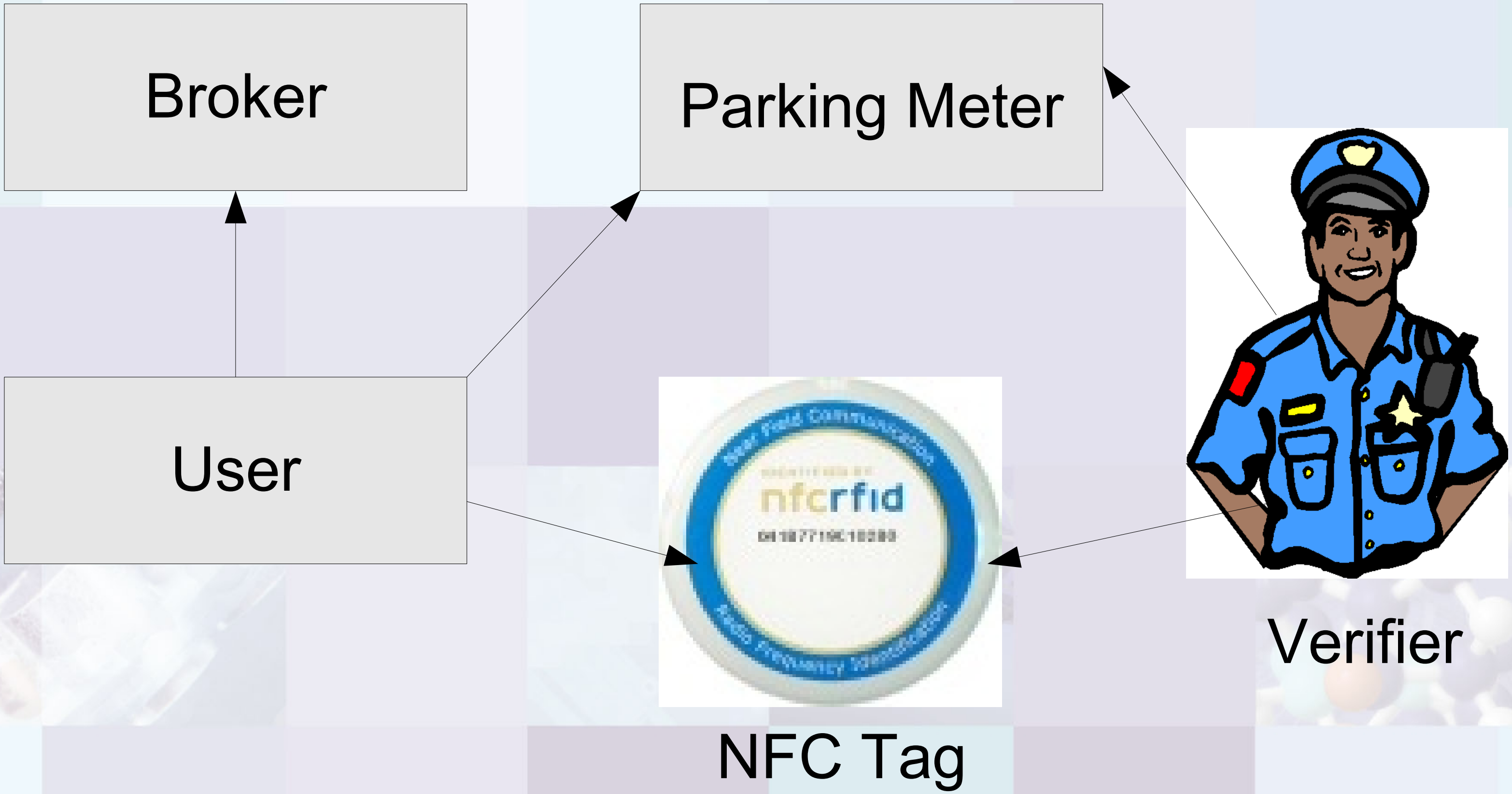
- RFID tags with info. To “create money”
- User “charges tag” from a Broker
- Readers have a bloom filter
- **Money can be generated by unauthorized parties**

* - E. Blass, A. Kurmus, R. Molva, and T. Strufe, “PSP: Private and Secure Payment with RFID,” in Proceedings of the 8th ACM workshop on Privacy in the electronic society, 2009, pp. 51–60

µPay

- ✓ Micropayment system using NFC
- ✓ Implemented on Android
- ✓ Prevents Overspending
- ✓ First of its kind in this space
- ✓ Fraud Detection

µPay



Broker

Parking Meter

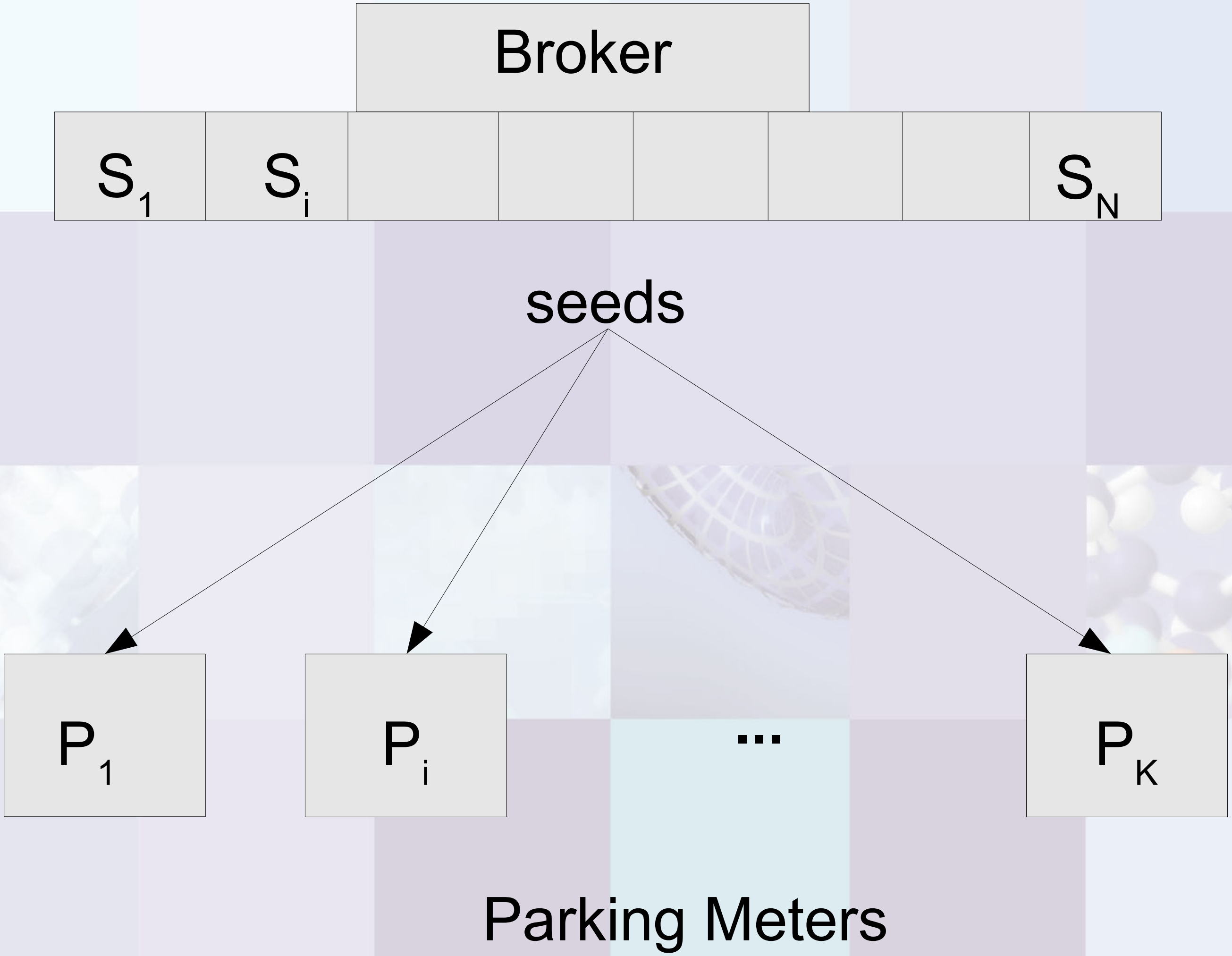
User

Verifier

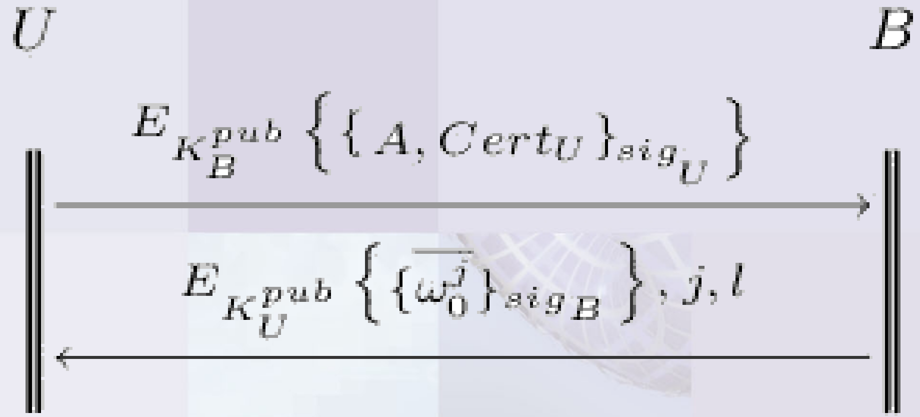
NFC Tag

Architecture

Protocol Overview (1/4) - Initialization



Protocol Overview (2/4) - Charge



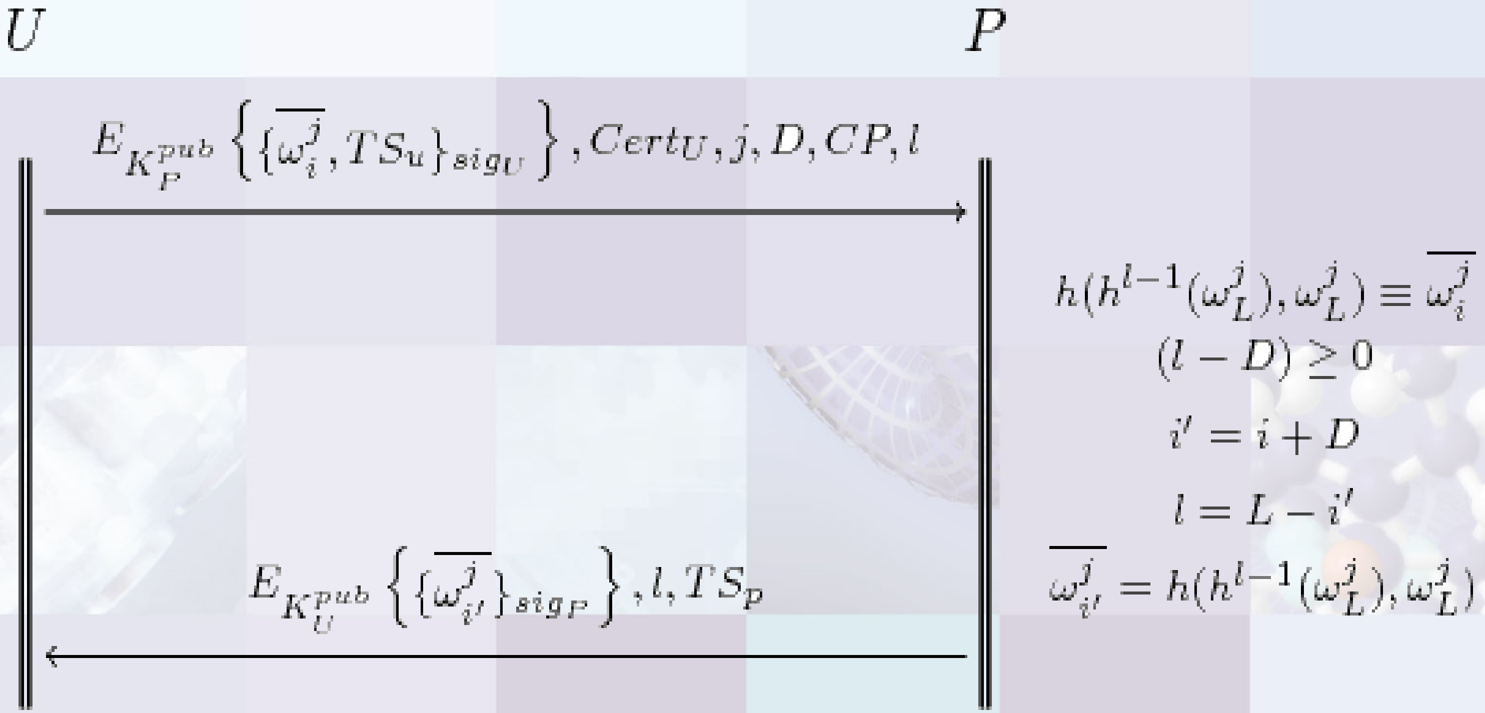
U

B

$E_{K_B^{pub}}\left\{\{A, Cert_U\}_{sig_U}\right\}$

$E_{K_U^{pub}}\left\{\{\overline{\omega_0^j}\}_{sig_B}\right\}, j, l$

Protocol Overview (3/4) – Check In



U

P

$E_{K_P^{pub}}\left\{\{\overline{\omega_i^j}, TS_u\}_{sig_U}\right\}, Cert_U, j, D, CP, l$

$$h(h^{l-1}(\omega_L^j), \omega_L^j) \equiv \overline{\omega_i^j}$$

$$(l - D) \geq 0$$

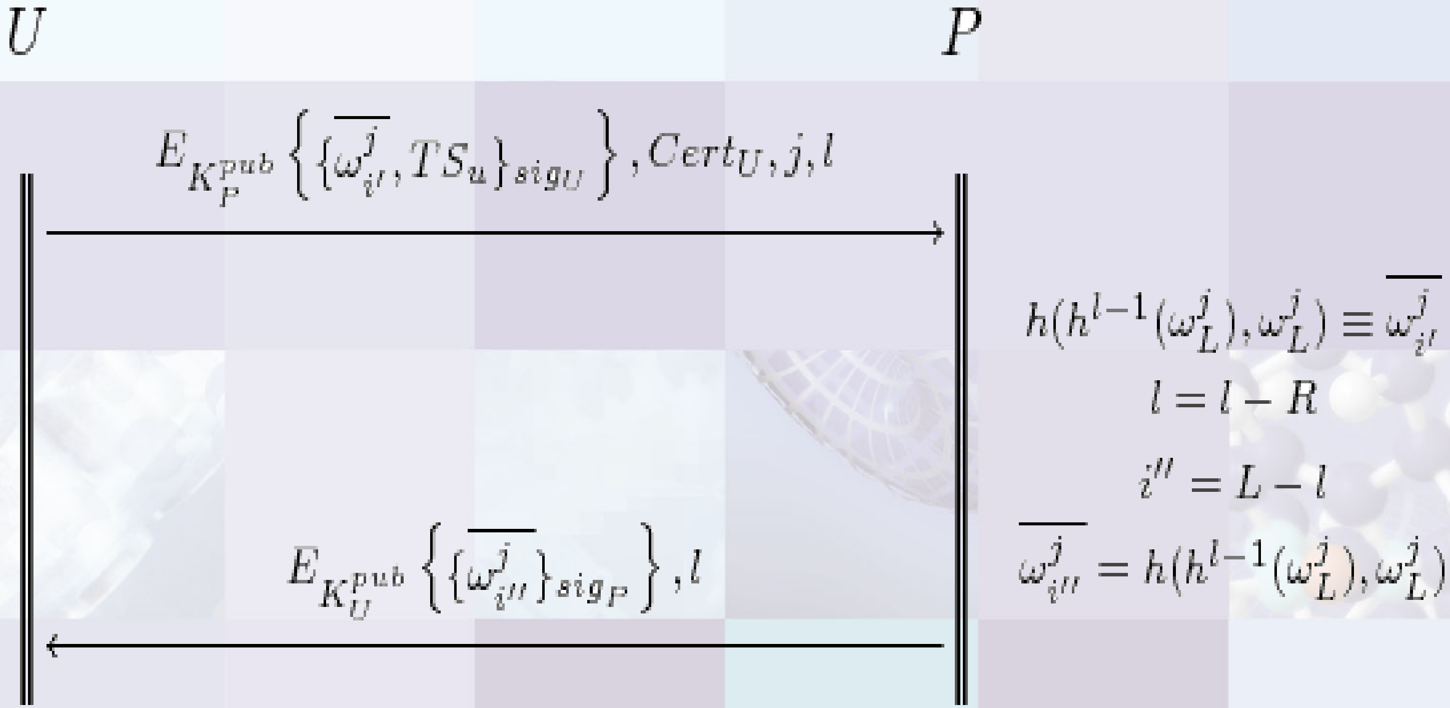
$$i' = i + D$$

$$l = L - i'$$

$$\overline{\omega_{i'}^j} = h(h^{l-1}(\omega_L^j), \omega_L^j)$$

$E_{K_U^{pub}}\left\{\{\overline{\omega_{i'}^j}\}_{sig_P}\right\}, l, TS_p$

Protocol Overview (4/4) – Check Out



U

P

$$E_{K_P^{pub}}\left\{\{\overline{\omega^j_{i'}}, TS_u\}_{sig_U}\right\}, Cert_U, j, l$$

$$h(h^{l-1}(\omega^j_L), \omega^j_L) \equiv \overline{\omega^j_{i'}}$$

$$l = l - R$$

$$i'' = L - l$$

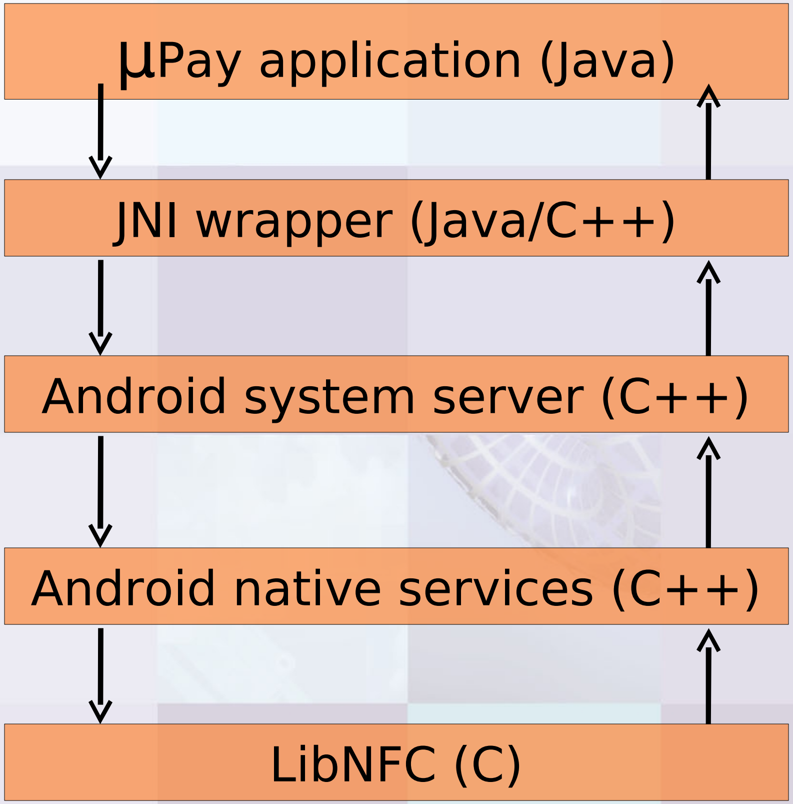
$$\overline{\omega^j_{i''}} = h(h^{l-1}(\omega^j_L), \omega^j_L)$$

$$E_{K_U^{pub}}\left\{\{\overline{\omega^j_{i''}}\}_{sig_P}\right\}, l$$

Implementation Details (1/2)

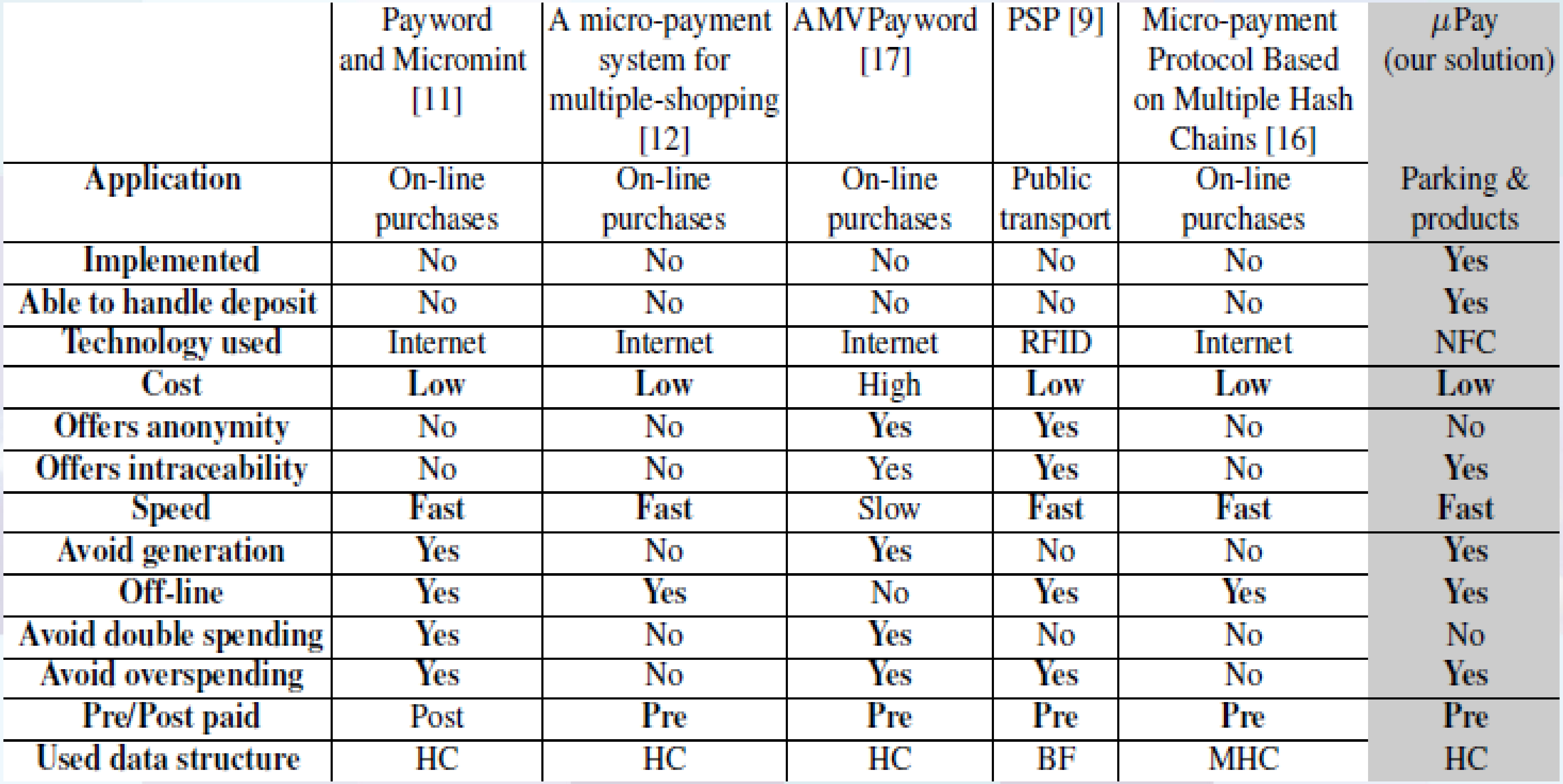
- ✓ Android 2.2 + Nexus One + Arygon NFC Reader
- ✓ USB Host Mode – Kernel Mod
- ✓ Couple of Kernel Modules – usbserial.ko, cp210x.ko
- ✓ libnfc
- ✓ Some framework hacking

Implementation Details (2/2)



System Architecture

Evaluation



	Payword and Micromint [11]	A micro-payment system for multiple-shopping [12]	AMVPayword [17]	PSP [9]	Micro-payment Protocol Based on Multiple Hash Chains [16]	μPay (our solution)
Application	On-line purchases	On-line purchases	On-line purchases	Public transport	On-line purchases	Parking & products
Implemented	No	No	No	No	No	Yes
Able to handle deposit	No	No	No	No	No	Yes
Technology used	Internet	Internet	Internet	RFID	Internet	NFC
Cost	Low	Low	High	Low	Low	Low
Offers anonymity	No	No	Yes	Yes	No	No
Offers intraceability	No	No	Yes	Yes	No	Yes
Speed	Fast	Fast	Slow	Fast	Fast	Fast
Avoid generation	Yes	No	Yes	No	No	Yes
Off-line	Yes	Yes	No	Yes	Yes	Yes
Avoid double spending	Yes	No	Yes	No	No	No
Avoid overspending	Yes	No	Yes	Yes	No	Yes
Pre/Post paid	Post	Pre	Pre	Pre	Pre	Pre
Used data structure	HC	HC	HC	BF	MHC	HC

Future/On-going Work

- ✓ Nexus S implementation
- ✓ Broker Implementation
- ✓ Formal Protocol Verification

http://www.few.vu.nl/~earlence