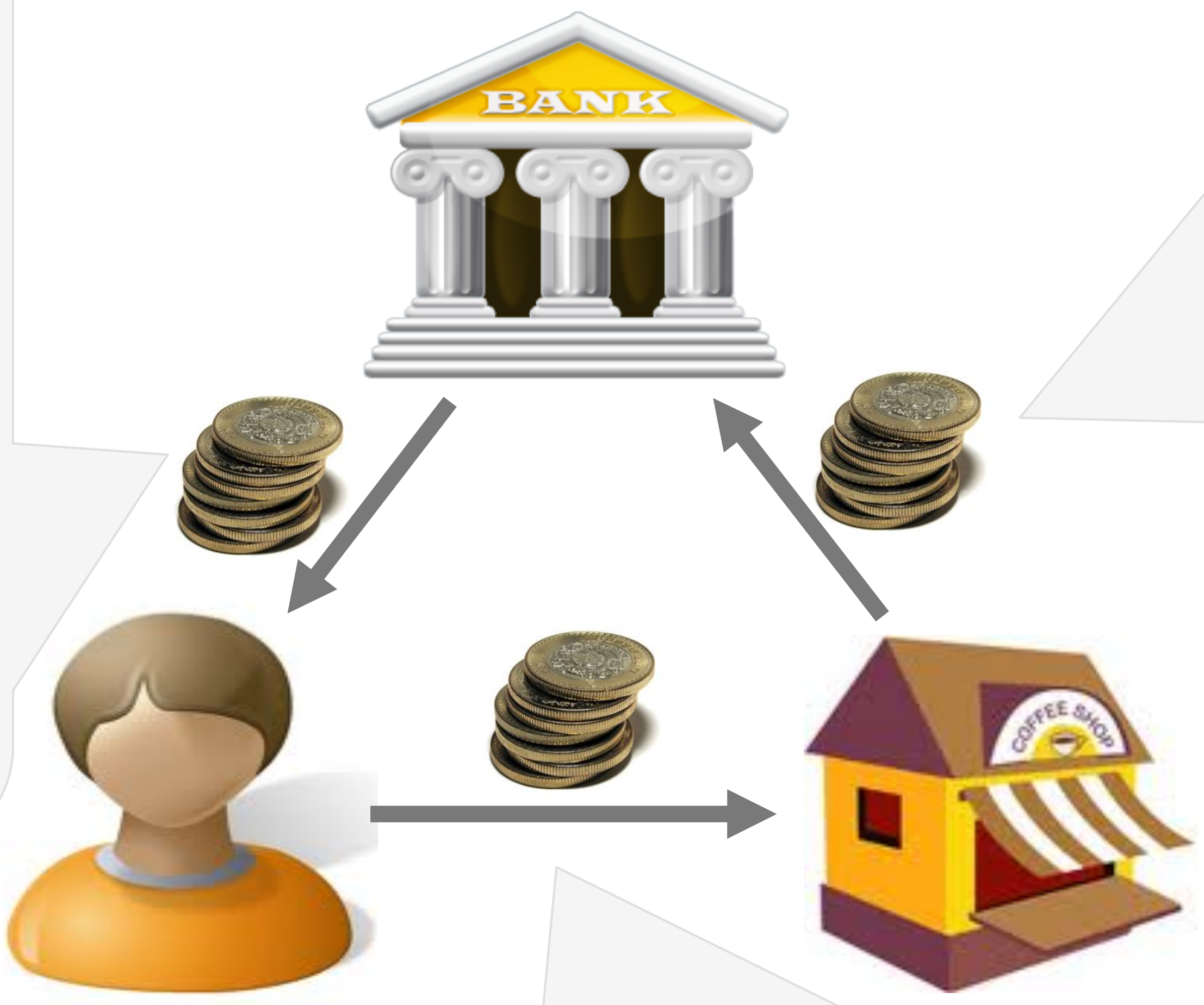
E-cash for Intelligent Public Transportation

Gesine Hinterwälder, Christian T. Zenger (Ruhr-University of Bochum),
Foteini Baldimtsi (Brown University), Wayne P. Burleson, Christof Paar

Electronic payments have many benefits, including improved throughput, new capabilities (congestion-based pricing etc.), user convenience, and they allow the easy collection of useful data about customer behavior. That makes them especially suitable for use in transportation payment systems. Yet, currently employed systems present no means to protect the user's locational privacy.

oyster
Transport for Lon
MTA MetroCard
CharlieCard
Stored Value CharlieTicket
Massachusetts Bay Transportation Authority

E-cash



Withdrawal

The bank issues coins to the user. Coins have a serial number and the user ID encoded in a blinded fashion. Some schemes additionally allow to encode user attributes (e.g. the age). This allows selective data collection and private variable pricing.

Deposit

The shop deposits its coins to its bank account. The bank checks whether the received coin had been deposited before. If a user had spent the same coin before, his identity can be revealed from the coin.

Spending

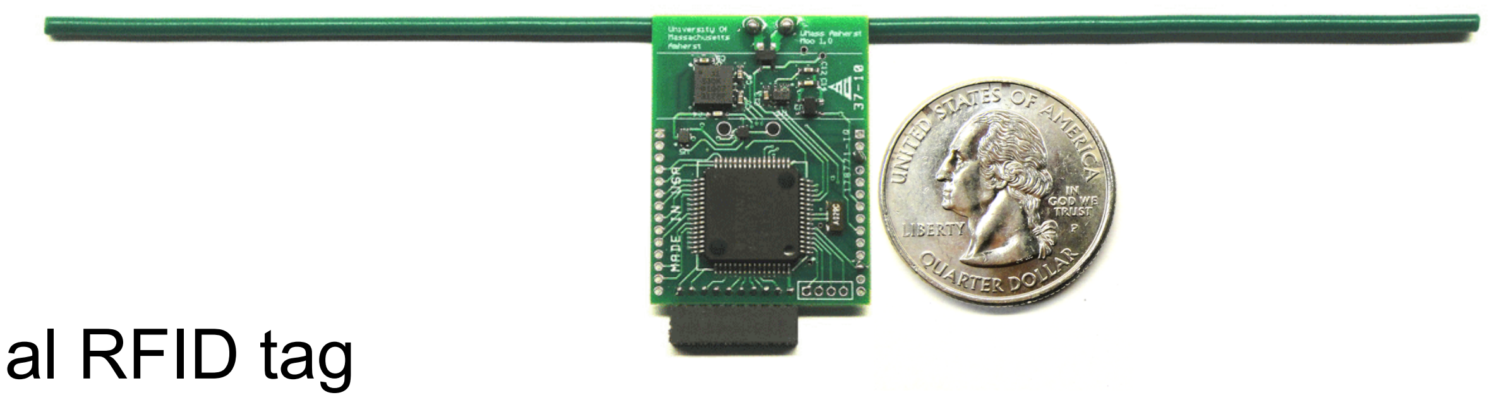
The user spends coins to the shop. He can additionally reveal attributes that are encoded into the coin. The shop can verify the validity of the coin offline, but not check, whether coin had been spent before.

Problem Statement

- E-cash based on public-key cryptography (very computationally intensive)
- Payments in public transportation systems should not exceed 400 ms
- Loading payment device should not take longer than a few seconds
- Payment devices limited in computation capabilities and power

We implement schemes that can be based on Elliptic Curve Cryptography (ECC). Though the most efficient established public-key scheme, it is still computationally intensive.

Implementation on UMass Moo



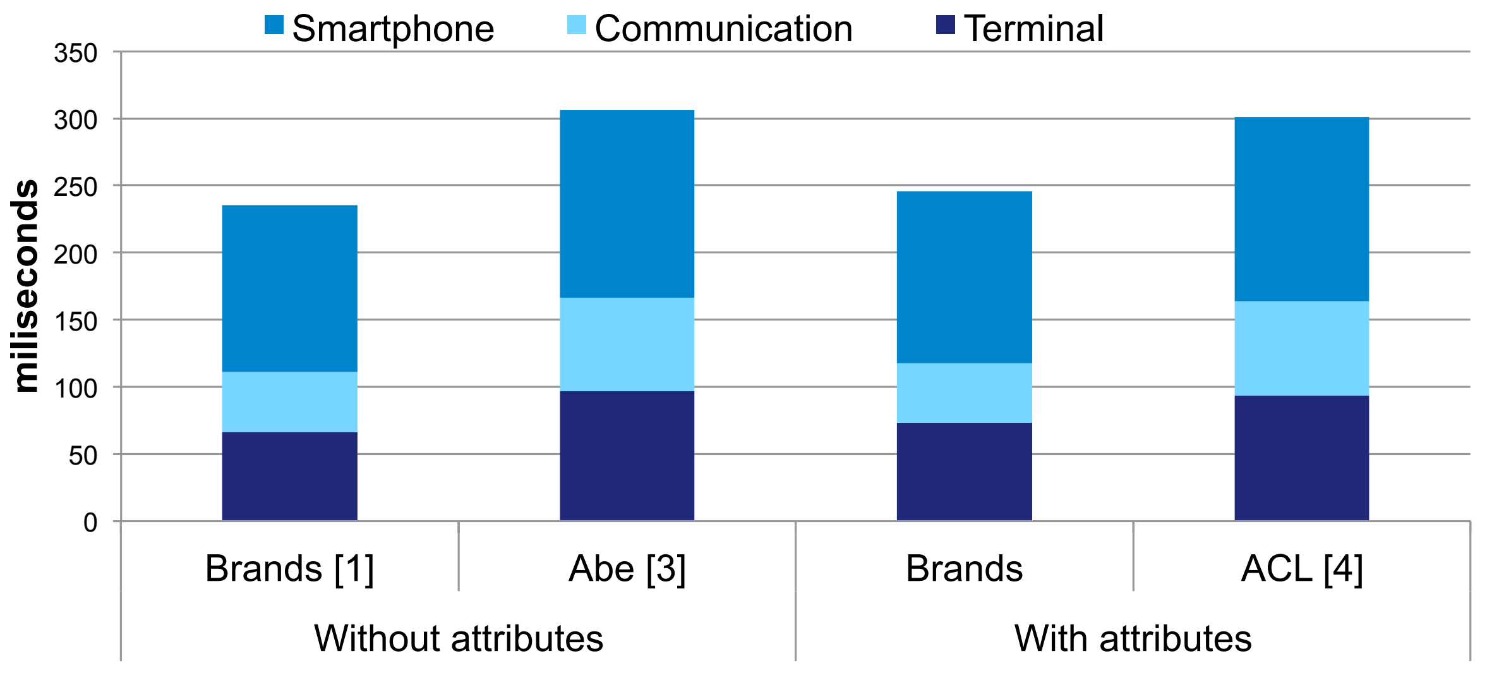
- Computational RFID tag
- Passively powered
- Can communicate over a distance of up to several meters
- Approximates future payment tokens
- Implemented Brands' Untraceable Offline Cash scheme [1]

The execution time for the spending of a coin on the UMass Moo is 13 ms, while withdrawal takes 4.5 sec.
→ Feasible to execute the spending on the RFID tag, while the withdrawal part is still problematic.

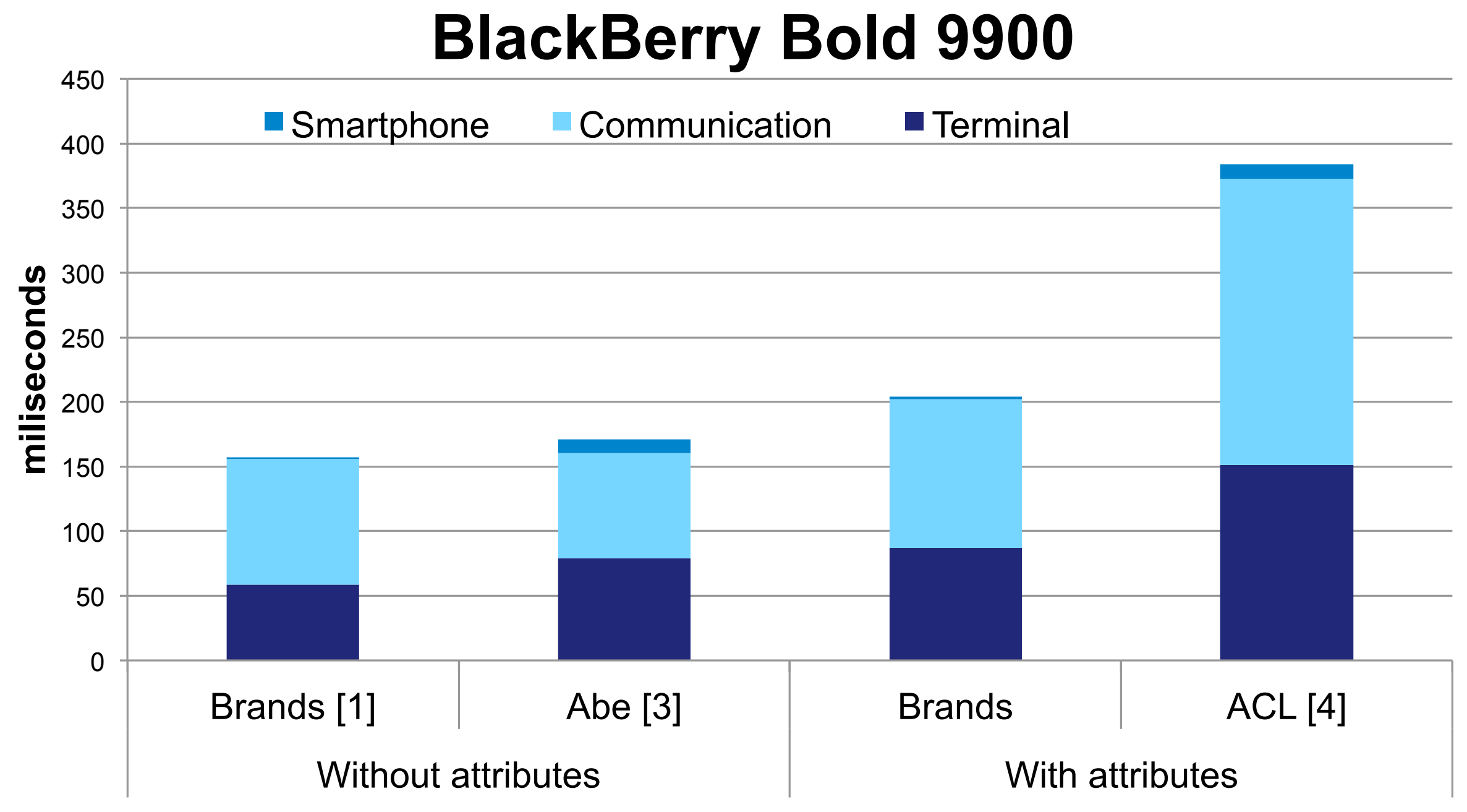
Implementation on BlackBerry Bold 9900

- NFC-enabled mobile phone
- Implementation of cryptographic framework in Java impossible => had to make use of API functionality
- Used Bouncy Castle for ECC framework on terminal side

Execution time for withdrawal of one coin on BlackBerry Bold 9900



Execution time for spending of one coin on BlackBerry Bold 9900



[1] S. Brands. Untraceable Off-line Cash in Wallets With Observers (Extended Abstract). In CRYPTO'93, pages 302-318

[2] G. Hinterwälder, C. Paar, and W. P. Burleson. Privacy Preserving Payments on Computational RFID Devices with Application in Intelligent Transportation Systems. In Workshop for RFID Security and Privacy 2012

[3] M. Abe. A Secure Three-move Blind Signature Scheme for Polynomially Many Signatures. In EUROCRYPT'01, pages 136-151

[4] F. Baldimtsi, A. Lysyanskaya. Anonymous Credentials Light. IACR Cryptology Eprint Archive, 2012/298, 2012.

Acknowledgements: This project has been funded by the National Science Foundation under CNS-0964641.