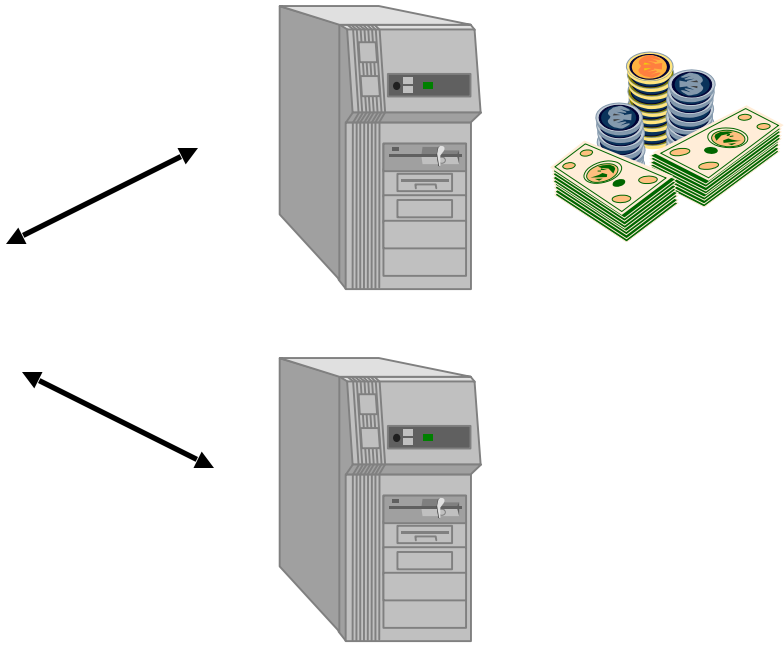
Experimenting with Electronic Commerce on the PalmPilot



Neil Daswani, Dan Boneh,

Stanford University

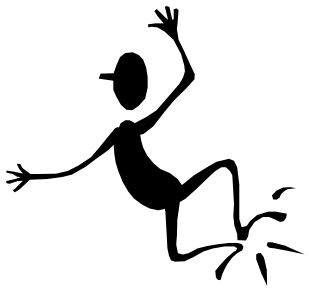
Trade-offs

- Vs. SmartCards
  - no tamper resistance
  - no cryptographic accelerators

  - direct line of communication with user
  - more processing power
  - more memory

Trade-offs

- Vs. Desktops
  - less memory
  - less processing power
  - portable



Cryptographic Primitives

Algorithm	Time
DES Encryption	4.9ms / block
SHA-1	2.7ms / block
512-bit RSA key gen.	3.4 minutes
512-bit RSA sig. gen.	7028 ms
512-bit RSA sig. verify	438 ms
163-bit ECC-DSA key gen.	597 ms
163-bit ECC-DSA sig. gen	776 ms
163-bit ECC-DSA sig. verify	2448 ms

* DES, SHA-1, RSA figures obtained with SSLeay
* ECC-DSA figures obtained with Certicom Security Builder Toolkit

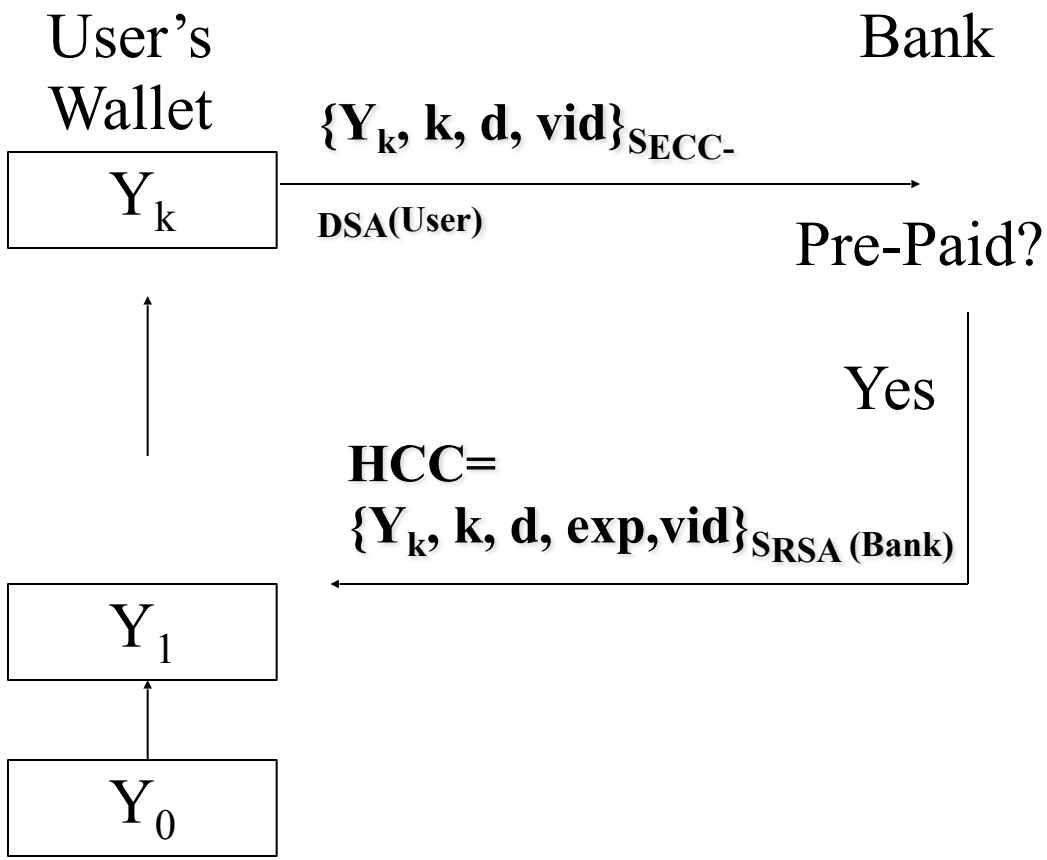
E-Commerce on a PDA

- Small payments ($5 -> $50)
- Target Application: Pony Vending Machine
  - Pre-pay
  - Vendor-specific
- Where to start?
  - PayWord (Rivest, Shamir)

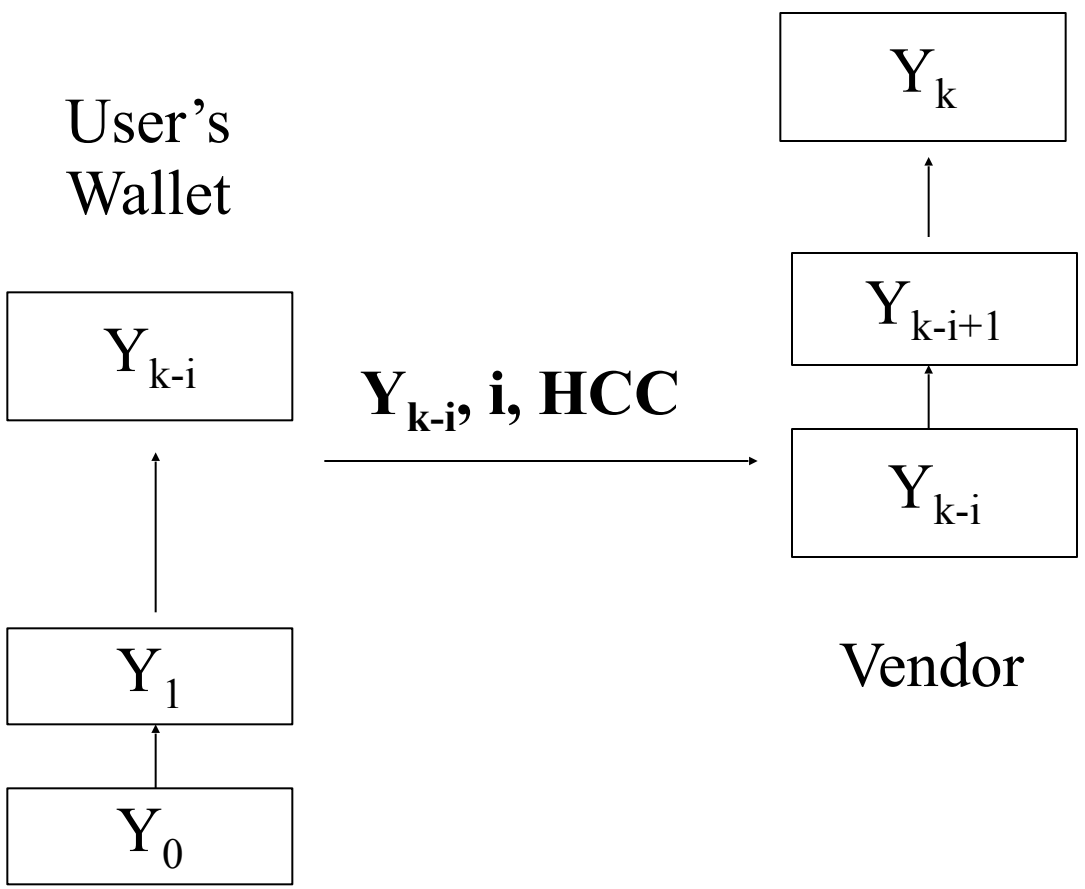
PDA-PayWord

- PalmPilot implementation of PayWord
- Minimize cryptographic operations
- Minimize storage requirements

PDA-PayWord: Withdrawal



PDA-PayWord: Purchase



PDA-PayWord: Withdrawal Timings

Amount ($)	Hash Chain Size (words)	Avg time (ms)
5	100	504
10	200	896
20	400	1667
50	1000	3970
Sign Withdrawal Request (ECC-DSA) + Receive HCC = 1874ms		
Hash Chain Certificate Verification: 1008ms		

Note: d = 5

PDA-PayWord: Purchase Timings

Instrument Amount ($)	Hashes Req'd (words)	Transaction Time (ms)
5	70	1090
10	170	1467
15	370	2267
50	970	4580

(First time $1.50 buy)

Conclusions / Summary

- PDA = portable commerce device w/o tamper resistance
- Suitable for small payments
- Commerce protocols can be adapted

- Example: PDA-PayWord
  - leverages best of ECC and RSA

Acknowledgements: Andrew Toy & Certicom