A lightweight protocol for the generation and distribution of secure e-coupons

C. Blundo, S. Cimato and A. De Bonis
University of Salerno
Italy

Outline of the talk

- Motivations
- A PKI based solution
- The lightweight protocol
  - The static model
  - The dynamic model
  - The extended model

C. Blundo S. Cimato A. De Bonis
Università di Salerno

The motivations

- The web and the market
  - E-commerce
  - Advertising
- Advertising on the web
  - Web servers host ads
    - Non-active role
    - Banners, product info, etc.
  - Web servers distribute promotional material
    - Active role
    - Discounts, gifts, etc.

C. Blundo S. Cimato A. De Bonis
Università di Salerno

From coupons to e-coupons

- Paper coupons
  - traditional form of advertisement distributed by
    - mail
    - fliers
    - newspapers and magazines
    - ...
  - redemption at physical store

- Hybrid coupons
  - downloaded from the web or received by e-mail
  - printed out
  - redemption at physical store

C. Blundo S. Cimato A. De Bonis
Università di Salerno

E-coupons

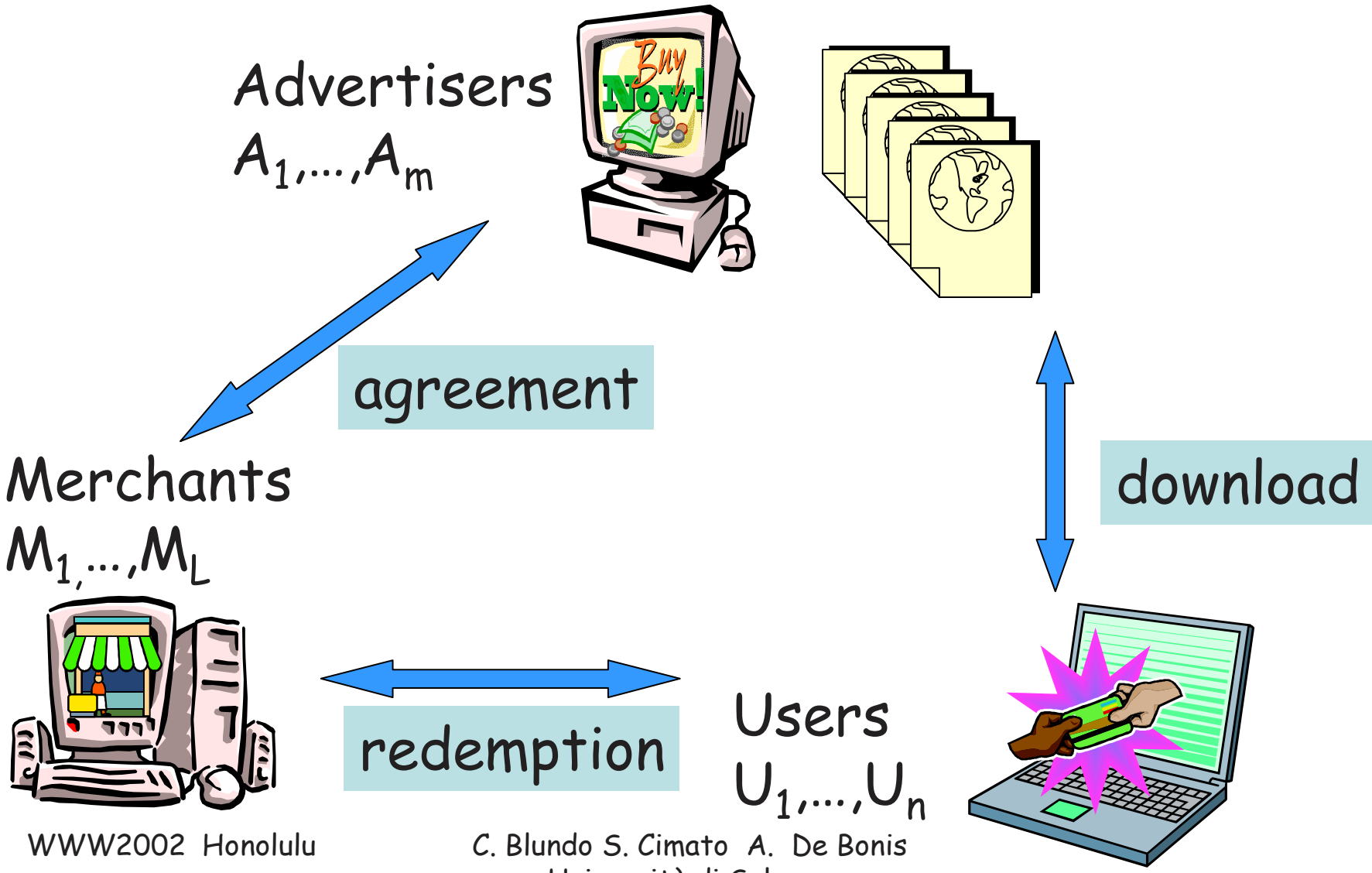
- Truly digital
  - download from advertisers' web sites
  - redemption at stores' web site

- Advantages
  - ✓ Easy to distribute, to store and to use
  - ✓ Target recipients
  - ✓ Feedback on promotional campaign

- Disadvantages
  - ✓ Duplication
  - ✓ Double spending
  - ✓ Forging
  - ✓ Manipulation

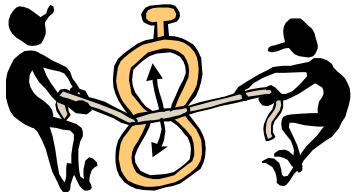
C. Blundo S. Cimato A. De Bonis
Università di Salerno

The scenario & life cycle



C. Blundo S. Cimato A. De Bonis
Università di Salerno

Requirements



Practical Requirements

- Soundness
- Efficiency
- Ease to use
- Interoperability
- Customers' anonymity

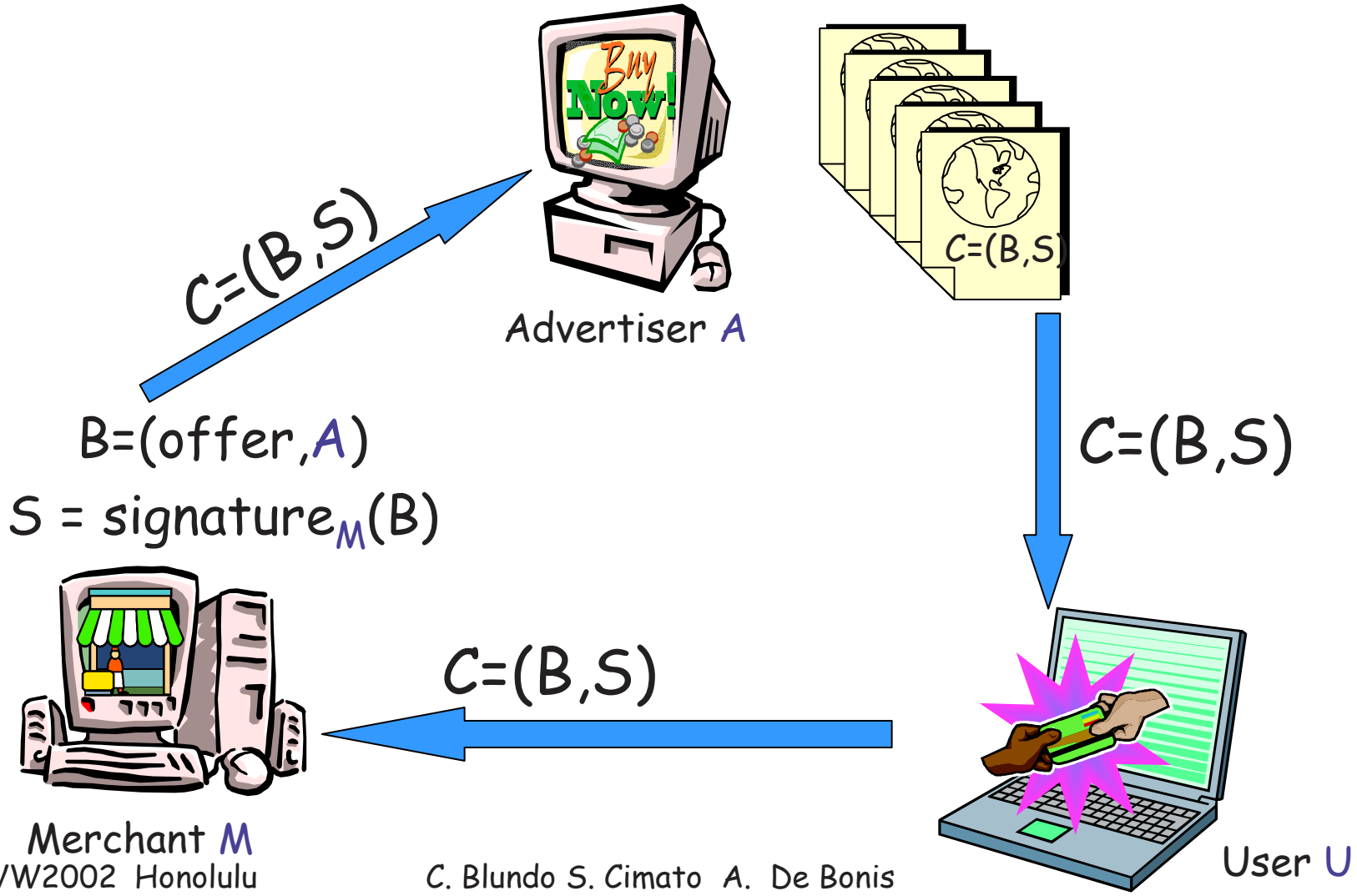
Security Requirements

- No unauthorized issuance
- No manipulation
- No double spending

C. Blundo S. Cimato A. De Bonis
Università di Salerno

A solution based on digital signature

[Jakobsson et al., WWW8]



C. Blundo S. Cimato A. De Bonis
Università di Salerno

Analysis of Jakobsson et al. solution

- Security Requirements:

Yes No unauthorized issuance
Yes No manipulation
Yes Double spending (if record of each e-coupon is mantained)

- Practical Requirements:

Yes Soundness
Yes Ease to use
Yes Interoperability
Yes Customers' anonymity
No Efficiency : Public key operations are very costly

C. Blundo S. Cimato A. De Bonis
Università di Salerno

A lightweight protocol

Idea: Use Mac Algorithms instead of digital signatures

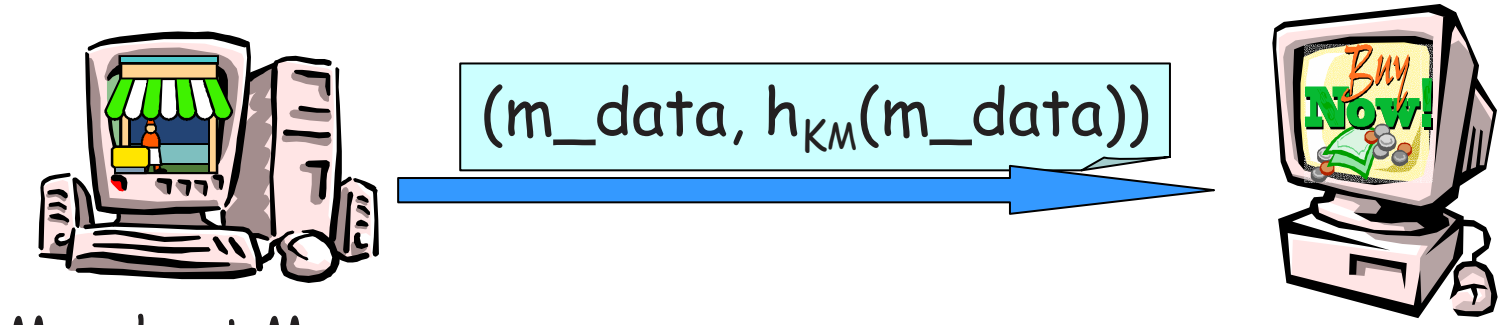
Mac Algorithm:

- encoding functions $h_k(\cdot)$ parameterized by secret key k
  - easy to compute
  - compression: finite bit length output string
  - computational resistance: if k unknown, it is computationally infeasible to compute $h_k(x)$

C. Blundo S. Cimato A. De Bonis
Università di Salerno

Initialization phase

- Merchant M sends the e-coupon framework to advertiser A

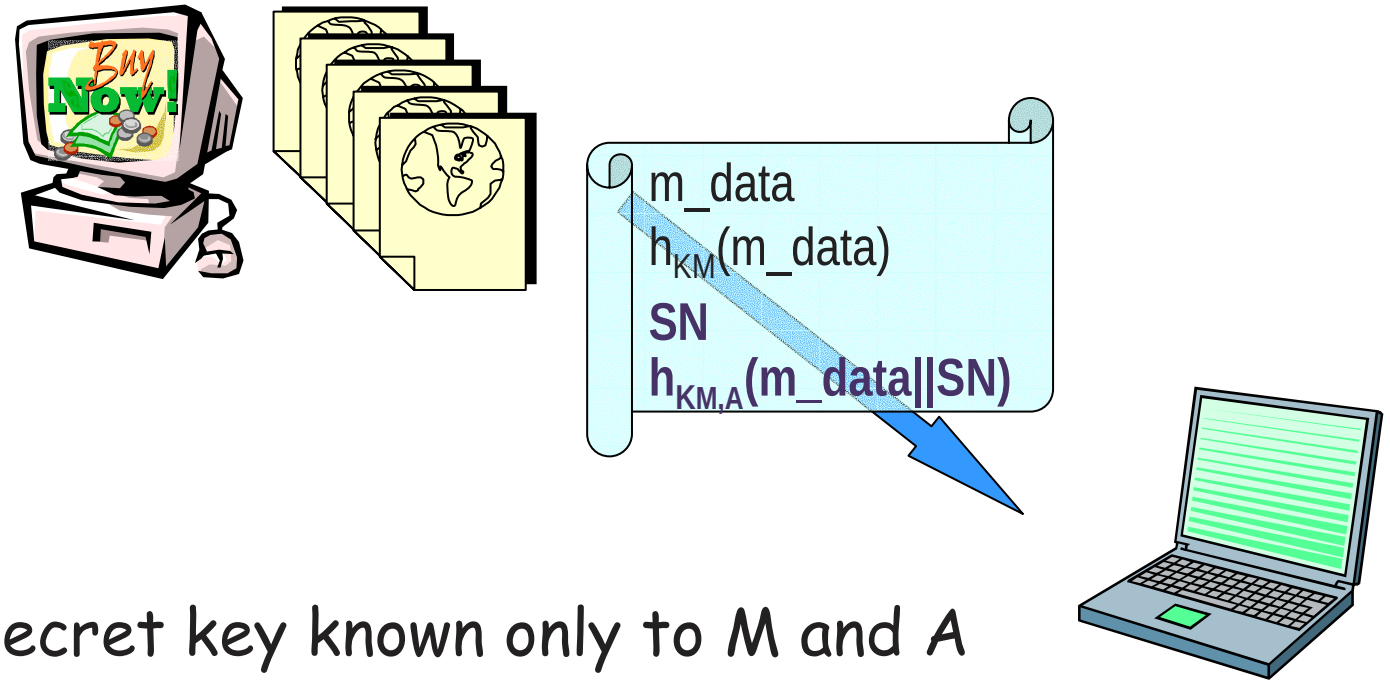


- K_M : secret key known only to M
- h_{kM} : MAC algorithm with parameter k_M
- m_data : merchant id, advertiser id, offer info,...

C. Blundo S. Cimato A. De Bonis
Università di Salerno

Generation phase

Advertiser A generates e-coupons using M's framework

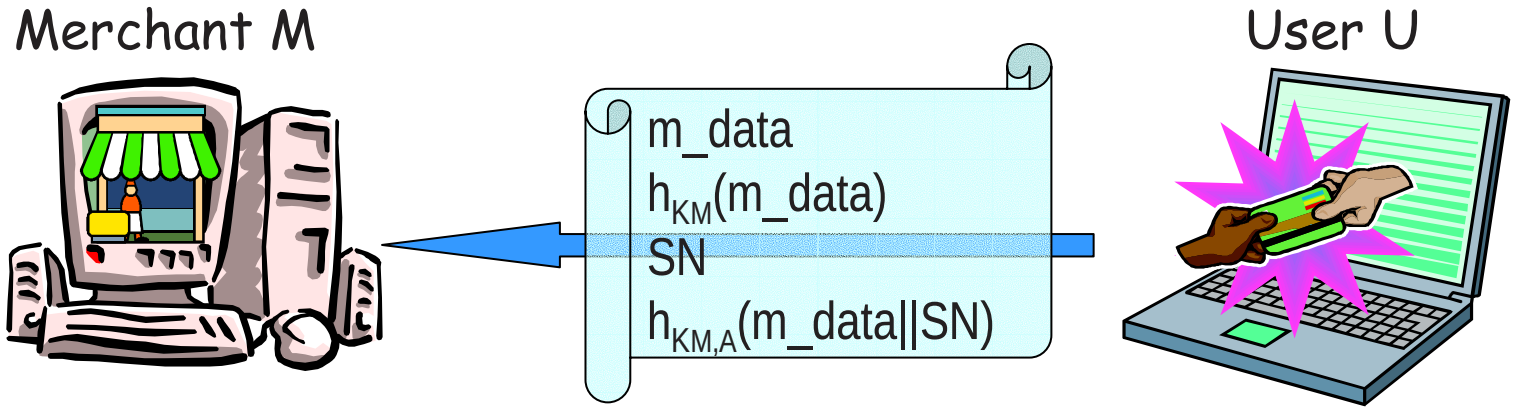


- $k_{M,A}$: secret key known only to M and A
- h_{KMA}: MAC algorithm with parameter $k_{M,A}$
- SN : e-coupon serial number

C. Blundo S. Cimato A. De Bonis
Università di Salerno

Redemption phase

User U sends the e-coupon to merchant M



M computes h_{KM}(m_data) and $h_{KM,A}$(m_data||SN) and accepts e-coupon iff

- computed values = values stored in e-coupon
- SN has not been seen before

C. Blundo S. Cimato A. De Bonis
Università di Salerno

Security

- No unauthorized issuance:
  - Users cannot compute h_{KM}(m_data) and $h_{KM,A}$(m_data||SN)
  - Advertiser cannot compute h_{KM}(m_data||SN)
- No manipulation:
  - Changing e-coupon data requires to compute new values of h_{KM}(m_data) and $h_{KM,A}$(m_data||SN)
- No double-spending:
  - No two accepted e-coupons with the same Serial Number

C. Blundo S. Cimato A. De Bonis
Università di Salerno

Dynamic e-coupons

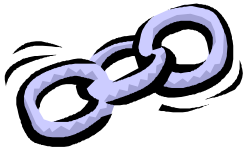
- Dynamic e-coupons contain information on the release time:
  - *Aging e-coupon:* offer decreases from the moment e-coupon is downloaded
- Dynamic e-coupons are released for marketing purposes:
  - Discourage users from shopping around for better offers
  - Give immediate feedback on advertisement campaign

C. Blundo S. Cimato A. De Bonis
Università di Salerno

Dynamic e-coupons

Idea: released e-coupons form a dependence chain

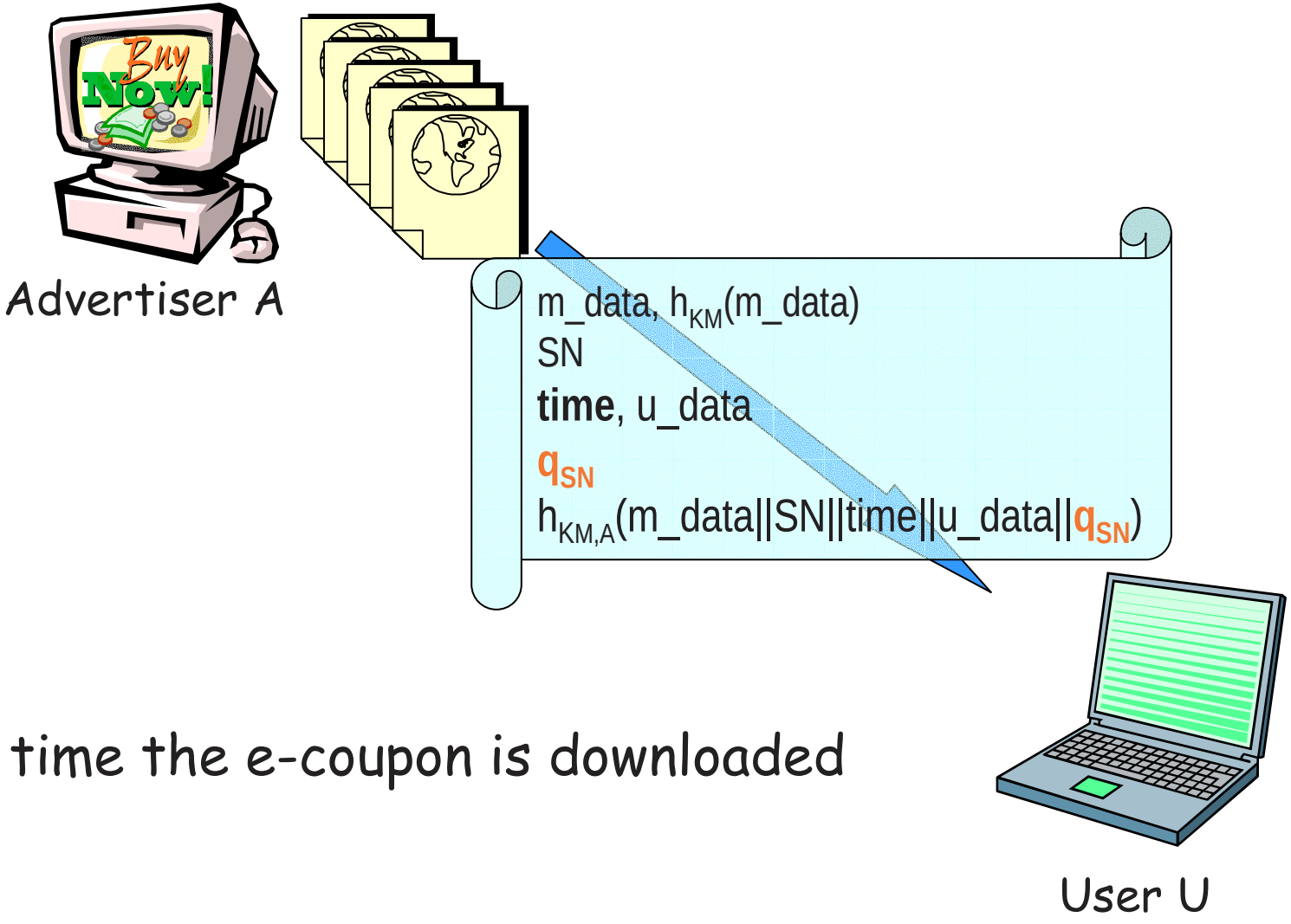
$q_1, q_2, q_3, \ldots,$



- Advertiser computes:
  - chain "ring" for released e-coupon
    - $q_{SN} = q(u\_data||q_{SN-1})$ (SN = serial number)
- Needed:
  - u_data: info released by user (e.g., IP address)
  - q: collision resistant hash function
    - It is computationally infeasible to find distinct x and y such that q(x)= q(y)

C. Blundo S. Cimato A. De Bonis
Università di Salerno

Generation of Dynamic E-coupons

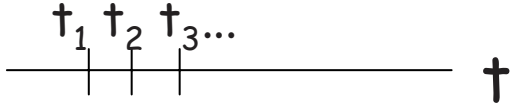


- time: time the e-coupon is downloaded

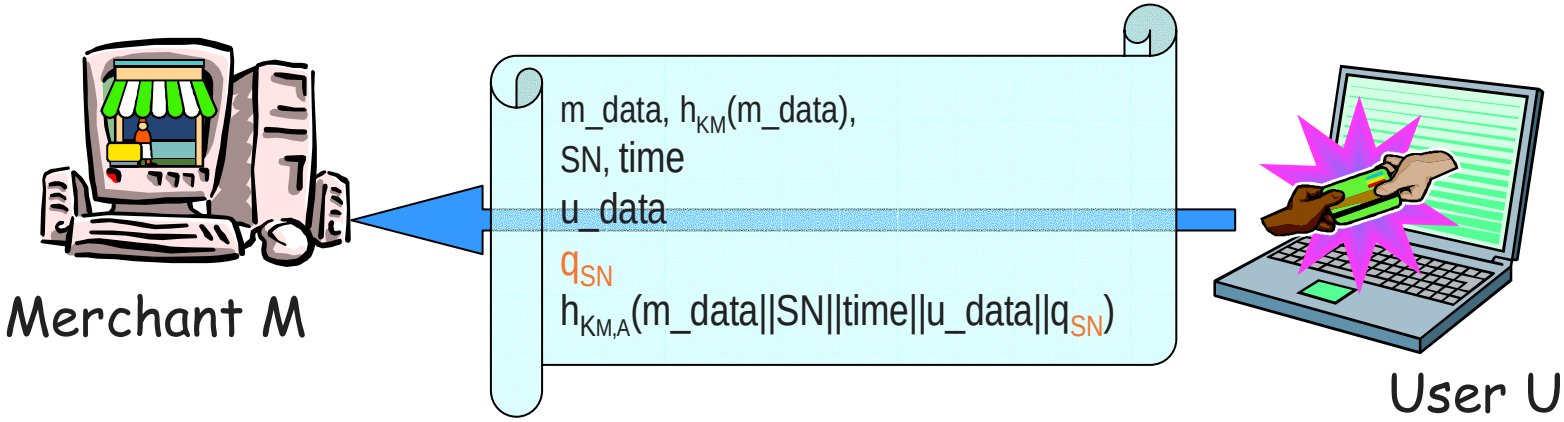
C. Blundo S. Cimato A. De Bonis
Università di Salerno

Redemption phase

- Time is divided in time frames $t_1, t_2, t_3, \ldots,$



- *A gives M the dependence chains for previous time frames*

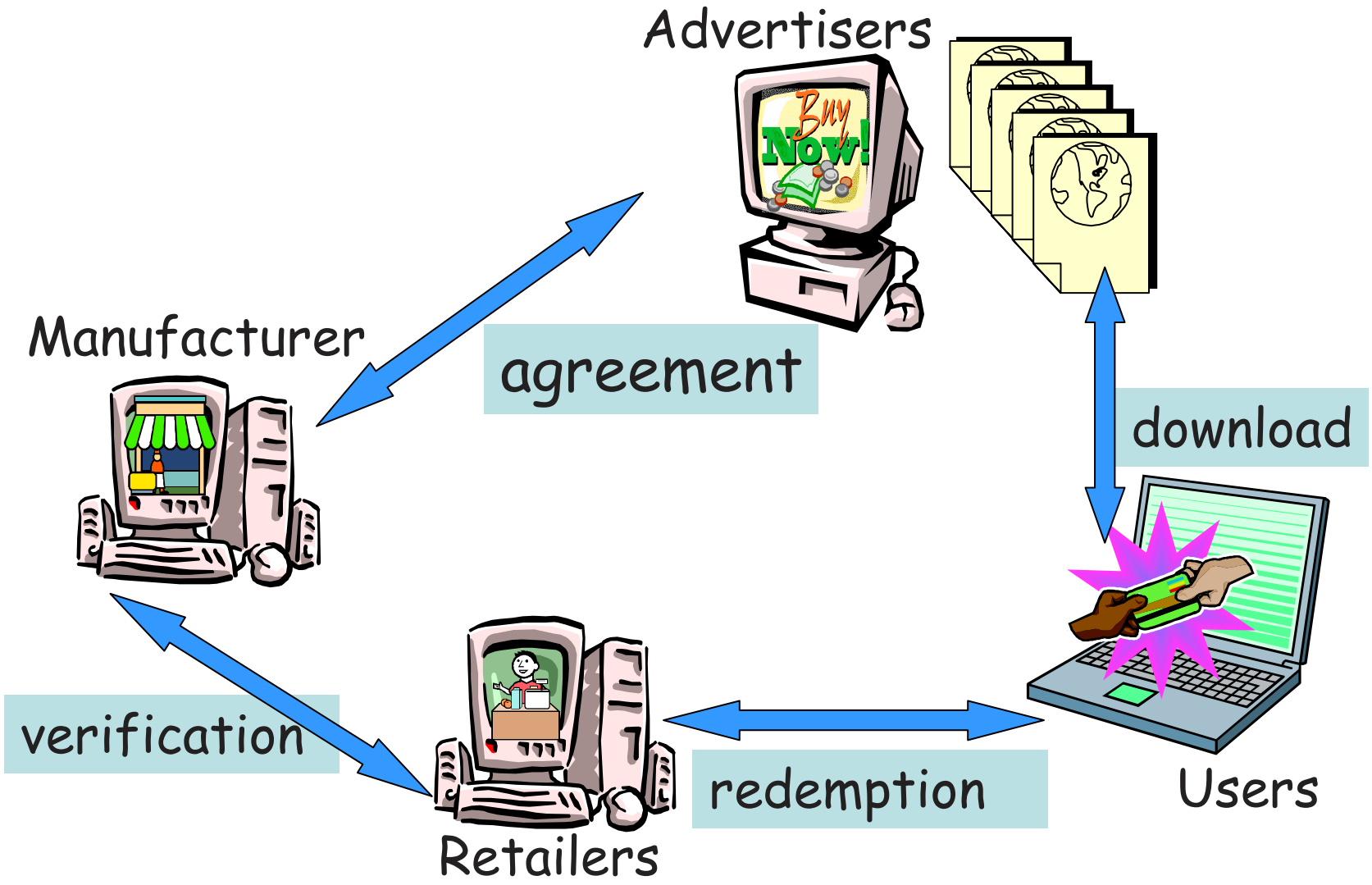


M computes $h_{KM}(m\_data||q_{SN})$ and $h_{KM,A}(m\_data||\ldots||q_{SN})$ and accepts e-coupon iff

- computed values = values stored in e-coupon
- SN has not been seen before
- q_{SN} in e-coupon = q_{SN} in dependence chain (when dependence chain is available)

C. Blundo S. Cimato A. De Bonis
Università di Salerno

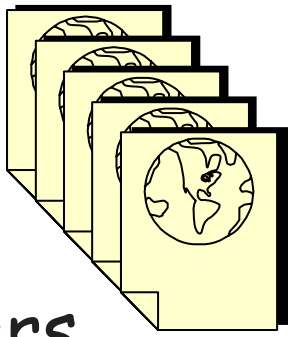
The extended model



C. Blundo S. Cimato A. De Bonis
Università di Salerno

Implementation

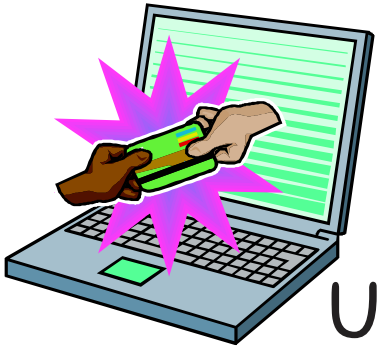
Advertisers



plugin

Coup$_1$
Coup$_2$
Coup$_3$
...
Coup$_n$

Wallet



Users

Merchants

C. Blundo S. Cimato A. De Bonis
Università di Salerno

Conclusions

- Our protocol is
  - ***secure:***
    - no unauthorized issuance
    - no manipulation
    - no double spending
  - ***lightweight:***
    - no need of public key infrastructure
  - ***practically implementable:***
    - it exploits HTTP protocol
  - ***respects user's privacy:***
    - no registration required

C. Blundo S. Cimato A. De Bonis
Università di Salerno