Privacy-Preserving Incentive Systems with Highly Efficient Point-Collection

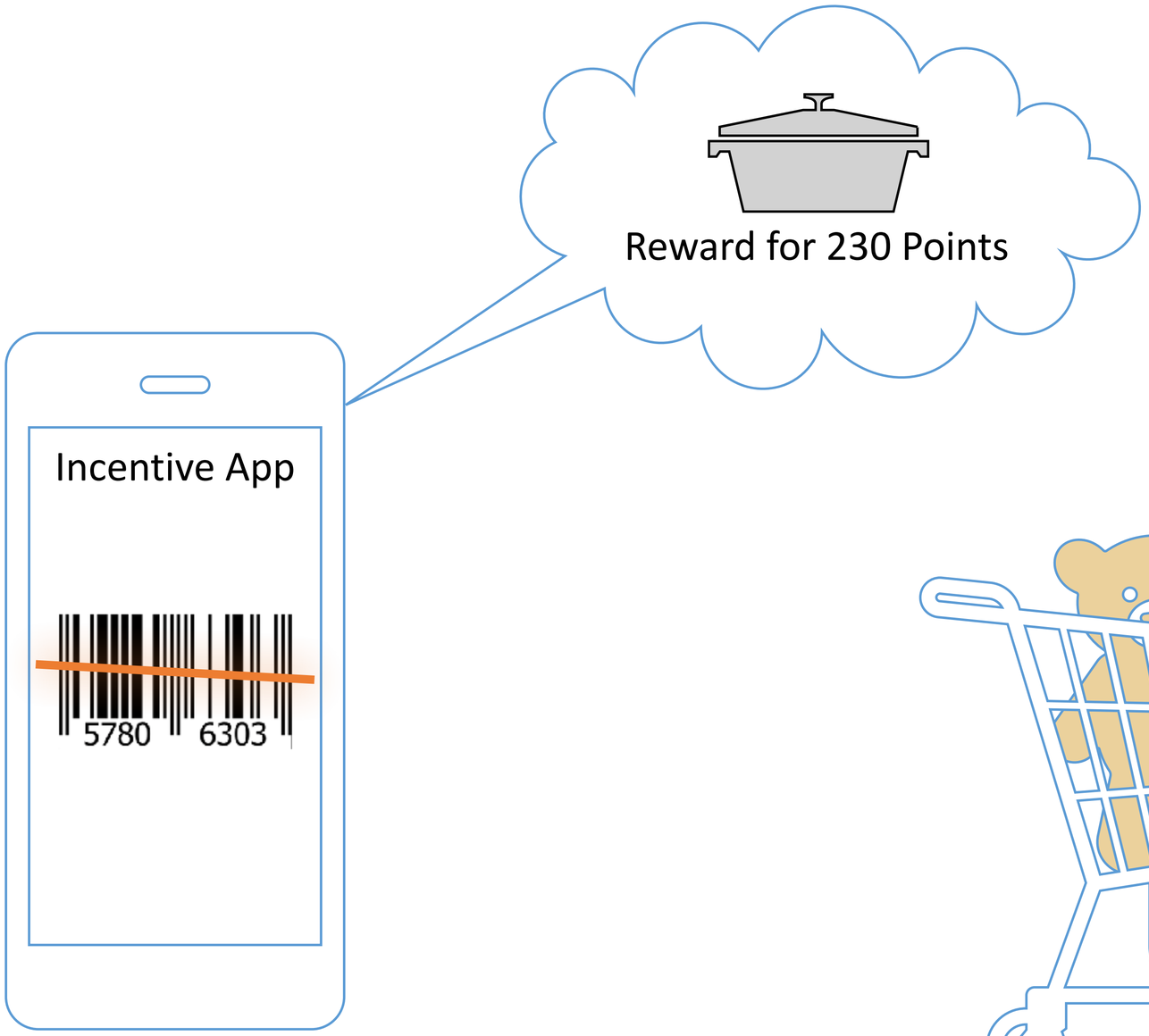
Jan Bobolz (), Fabian Eidens (),

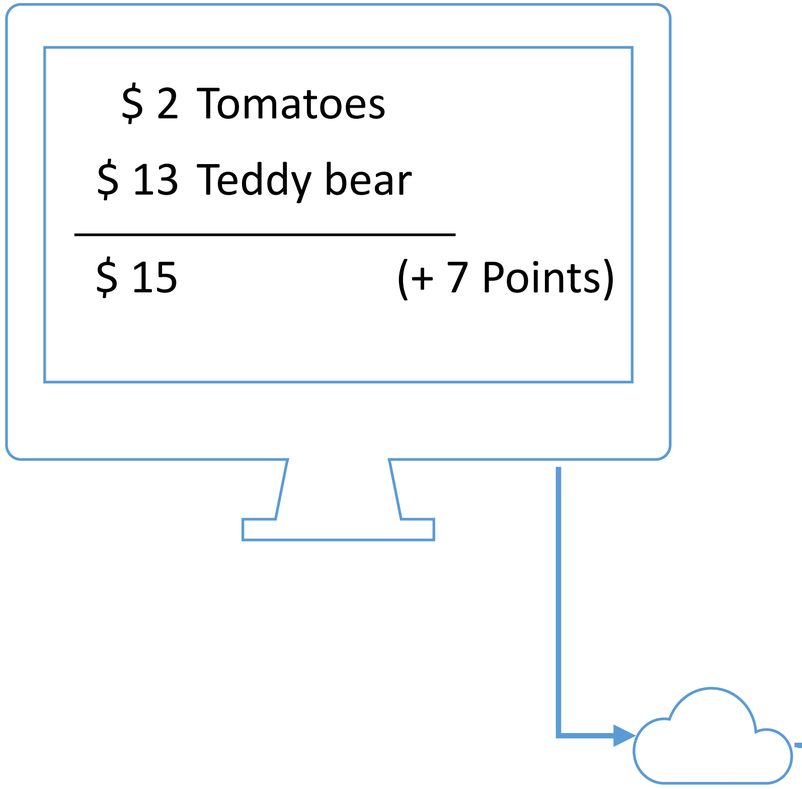
Stephan Krenn (), Daniel Slamanig (), Christoph Striecks ()

PADERBORN UNIVERSITY

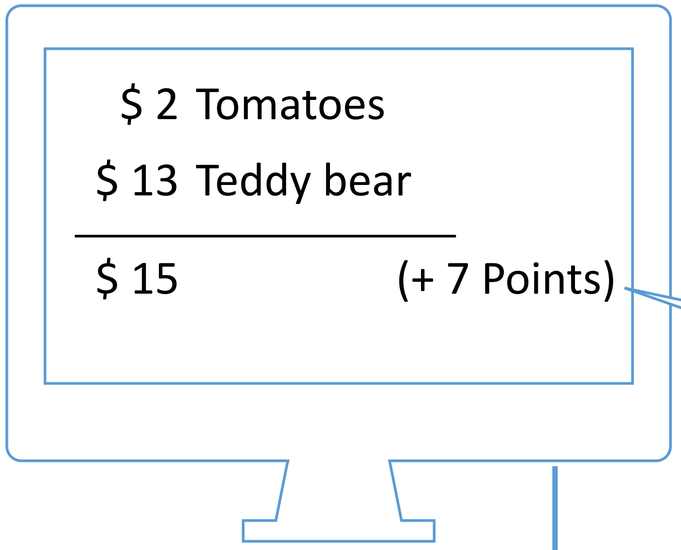
AUSTRIAN INSTITUTE OF TECHNOLOGY

Incentive Systems / Point Collection: In practice





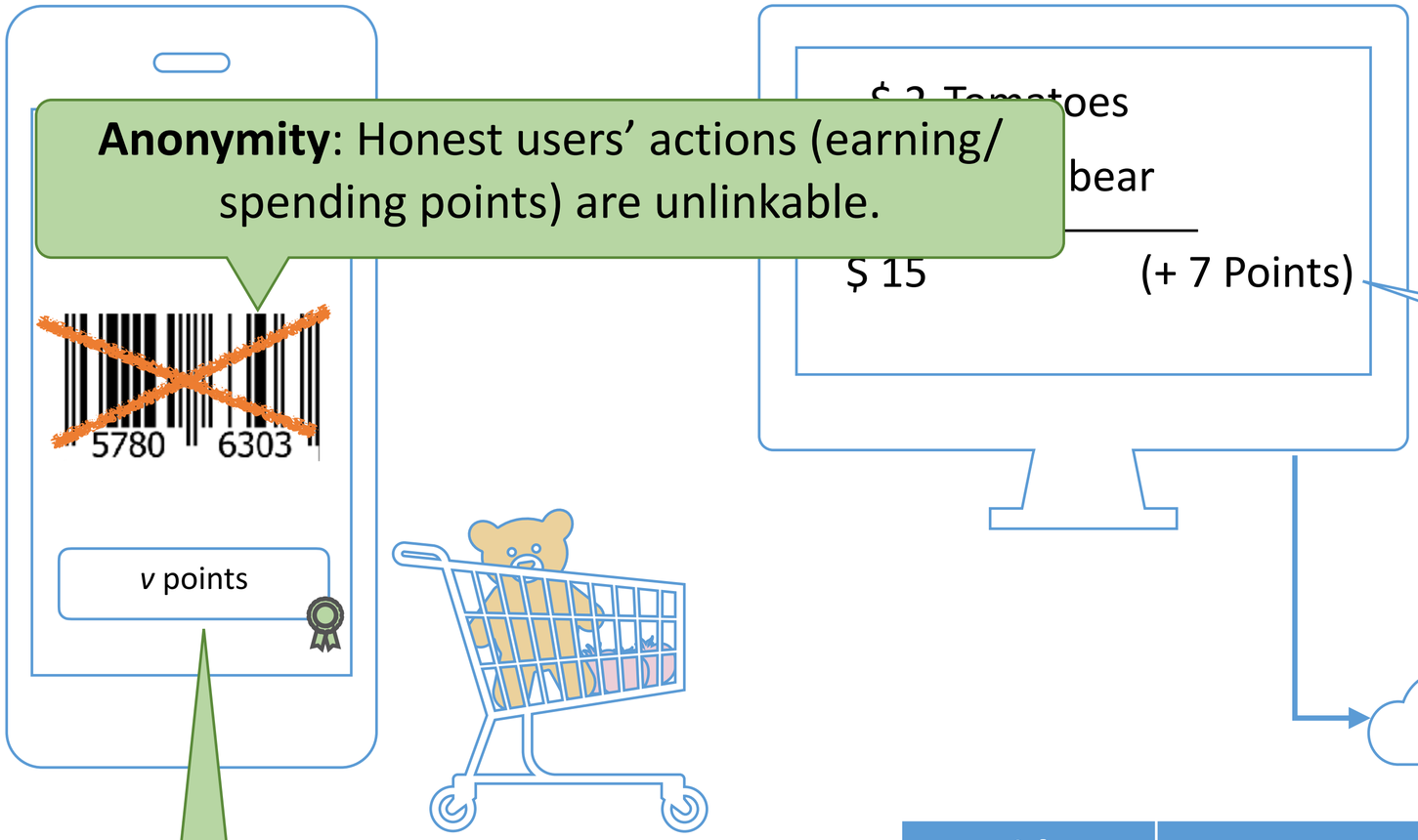
Incentive Systems / Point Collection: In practice



Goals:
- Reward customer loyalty
- Incentivize specific behavior
- Collect user data

user id	name	points	buying habits
…	…	…	…
5780 6303	Jimothy Halpert	~~200~~ 207	*Yesterday*: Pregnancy test *Today*: Tomatoes, teddy bear.
…	…	…	…

Goals for cryptographic incentive systems



Anonymity: Honest users' actions (earning/ spending points) are unlinkable.

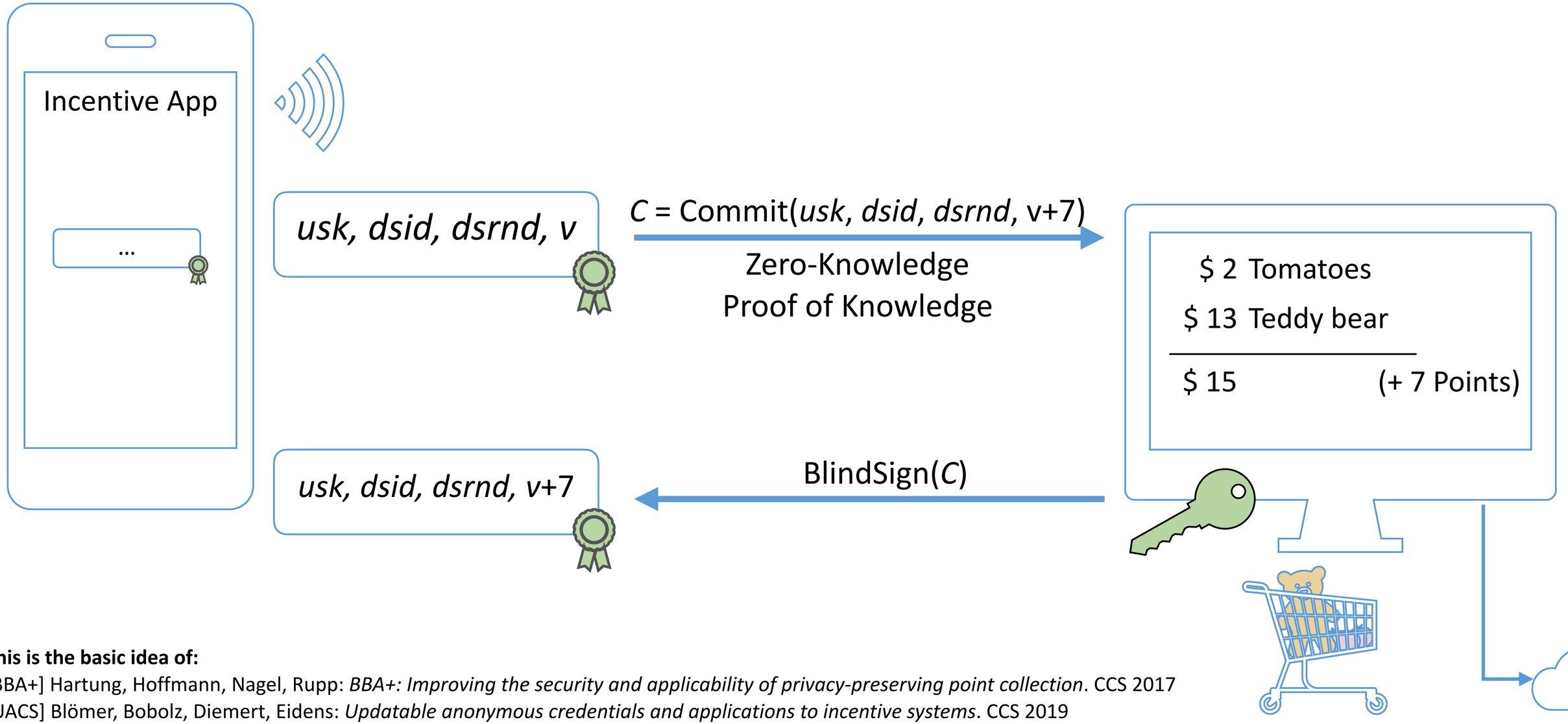
Soundness: Users cannot spend more points than they have.

Goals:
- Reward customer loyalty
- Incentivize specific behavior
- Collect user data

user id	name	points	buying habits
…	…	…	
5780 6303	Jimothy Halpert	2	
…	…	…	…

Offline double-spending protection: Stores don't need persistent database connection to deal with double-spending

Prior Work: Earning Points



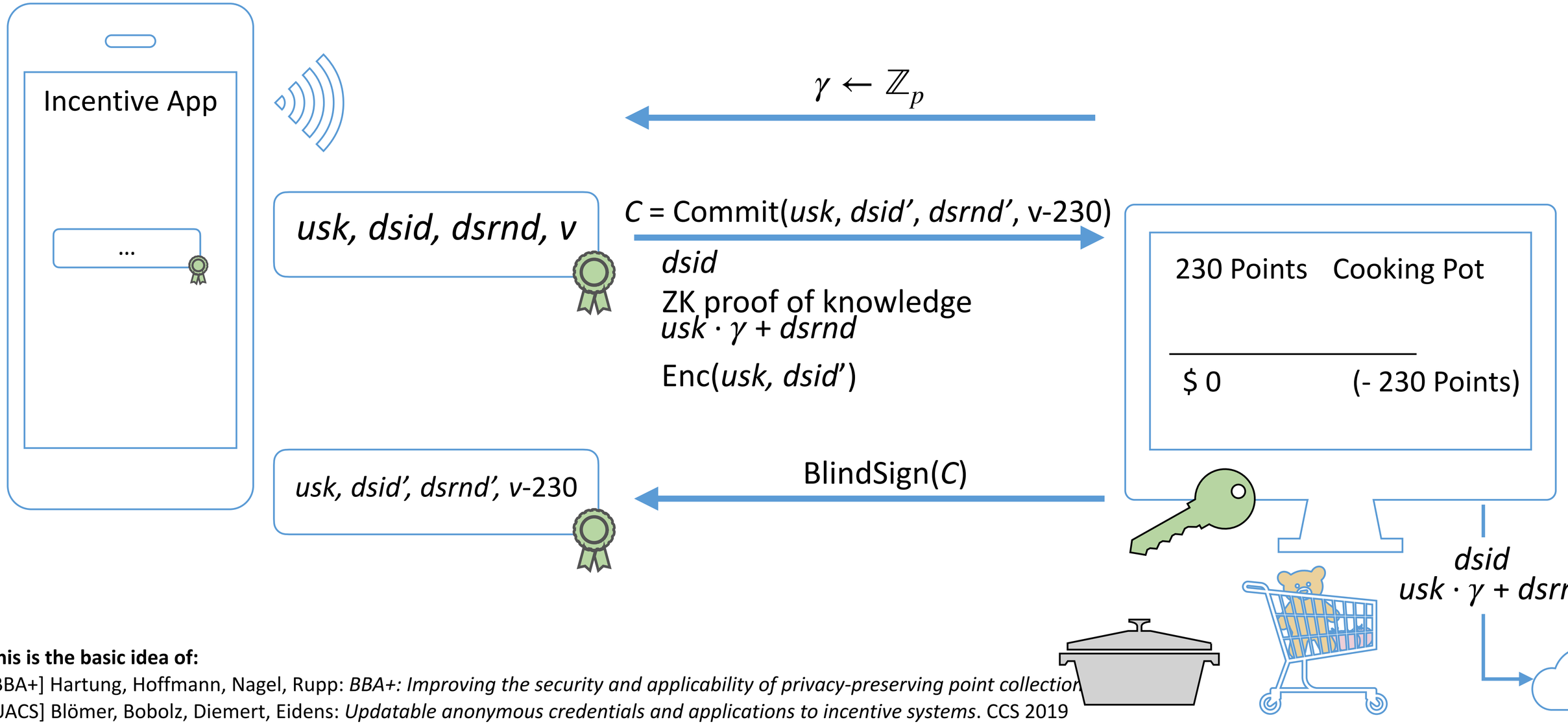
This is the basic idea of:

[BBA+] Hartung, Hoffmann, Nagel, Rupp: *BBA+: Improving the security and applicability of privacy-preserving point collection*. CCS 2017

[UACS] Blömer, Bobolz, Diemert, Eidens: *Updatable anonymous credentials and applications to incentive systems*. CCS 2019

[BBW] Hoffmann, Klooß, Raiber, Rupp: *Black-box wallets: Fast anonymous two-way payments for constrained devices*. PoPETS 2020

Prior Work: Spending Points



This is the basic idea of:

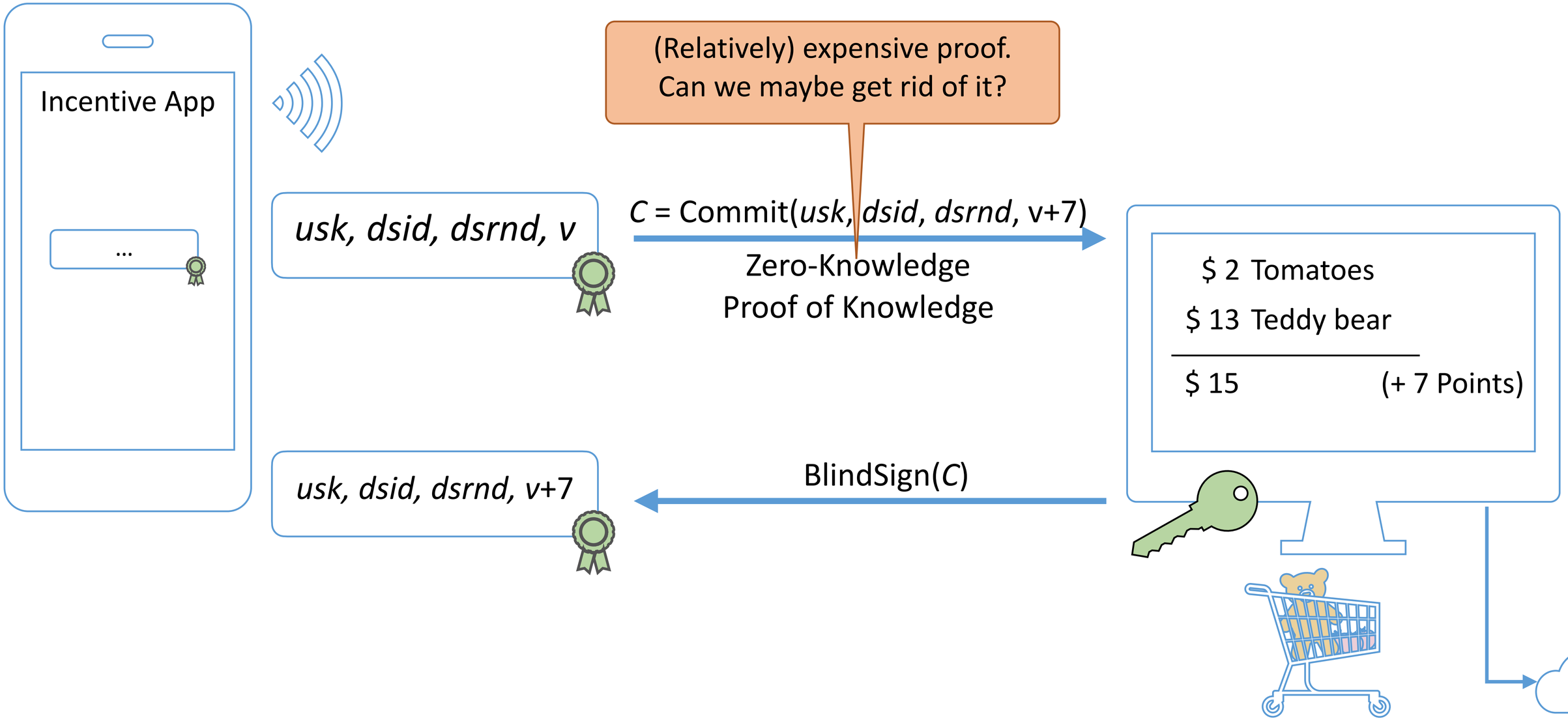
[BBA+] Hartung, Hoffmann, Nagel, Rupp: *BBA+: Improving the security and applicability of privacy-preserving point collection*

[UACS] Blömer, Bobolz, Diemert, Eidens: *Updatable anonymous credentials and applications to incentive systems*. CCS 2019

[BBW] Hoffmann, Klooß, Raiber, Rupp: *Black-box wallets: Fast anonymous two-way payments for constrained devices*. PoPETS 2020

More Efficient Point Earn Protocol

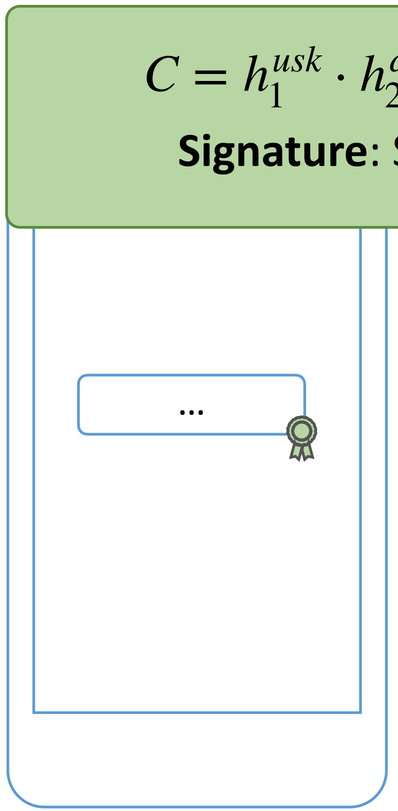
Idea: Efficiently Earning Points



Our Work: Efficiently Earning Points

$$C = h_1^{usk} \cdot h_2^{dsid} \cdot h_3^{dsrnd} \cdot h_4^{v} \cdot h_5^{t}$$

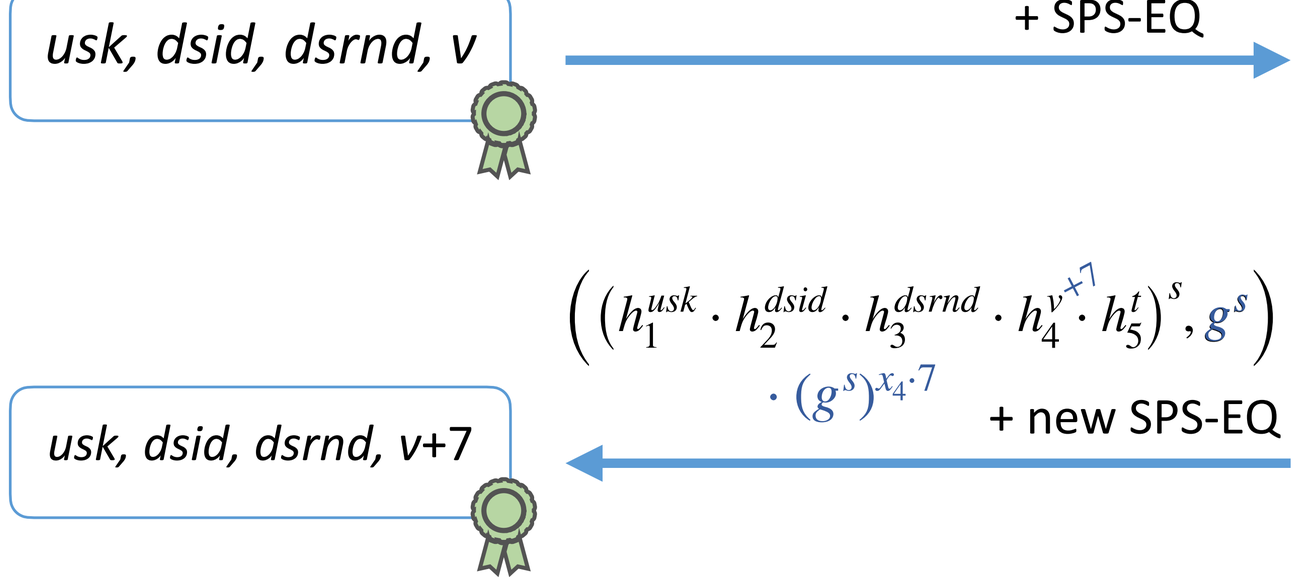
Signature: SPS-EQ on (C, g).



usk, dsid, dsrnd, v

$$\left(\left(h_1^{usk} \cdot h_2^{dsid} \cdot h_3^{dsrnd} \cdot h_4^{v} \cdot h_5^{t} \right)^s, g^s \right)$$

+ SPS-EQ



$$\left(\left(h_1^{usk} \cdot h_2^{dsid} \cdot h_3^{dsrnd} \cdot h_4^{v+7} \cdot h_5^{t} \right)^s, g^s \right) \cdot (g^s)^{x_4 \cdot 7}$$

+ new SPS-EQ

usk, dsid, dsrnd, v+7

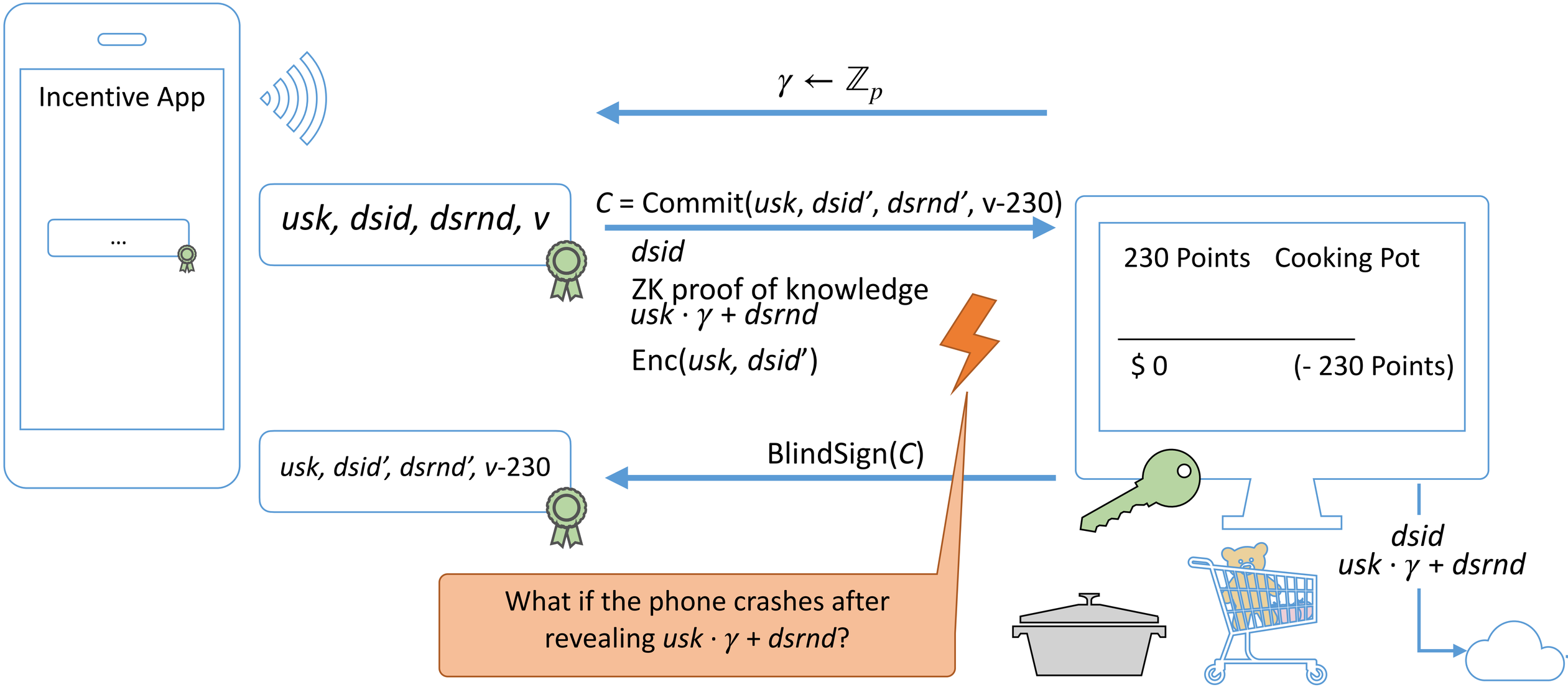
SPS-EQ: Valid signature on $(C, g) \in \mathbb{G}_1^2$

can be changed to *fresh-looking* valid signature on (C^s, g^s)

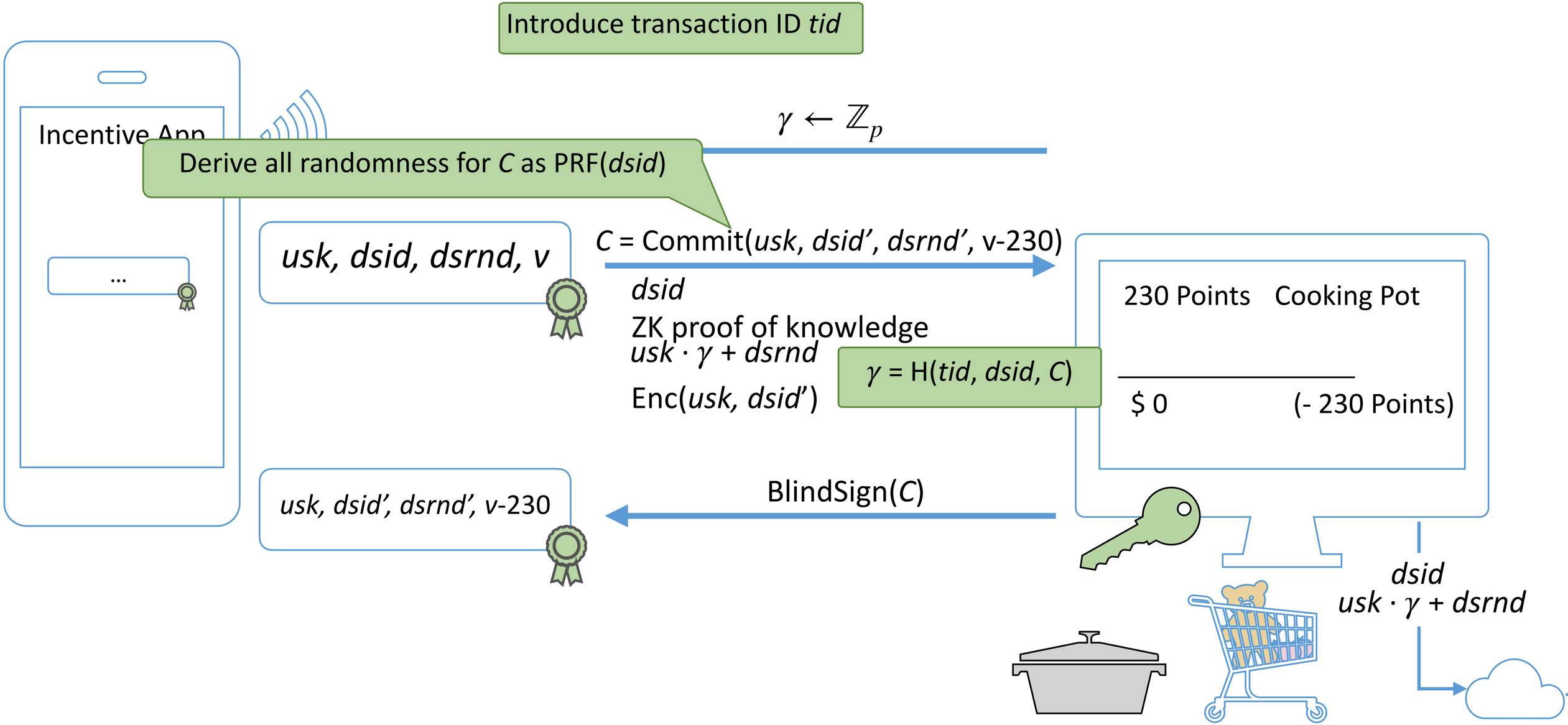
[SPSEQ] Fuchsbauer, Hanser, Slamanig: *Structure-preserving signatures on equivalence classes and constant-size anonymous credentials*. Journal of Cryptology 2019

Recovery

Idea: Recovery

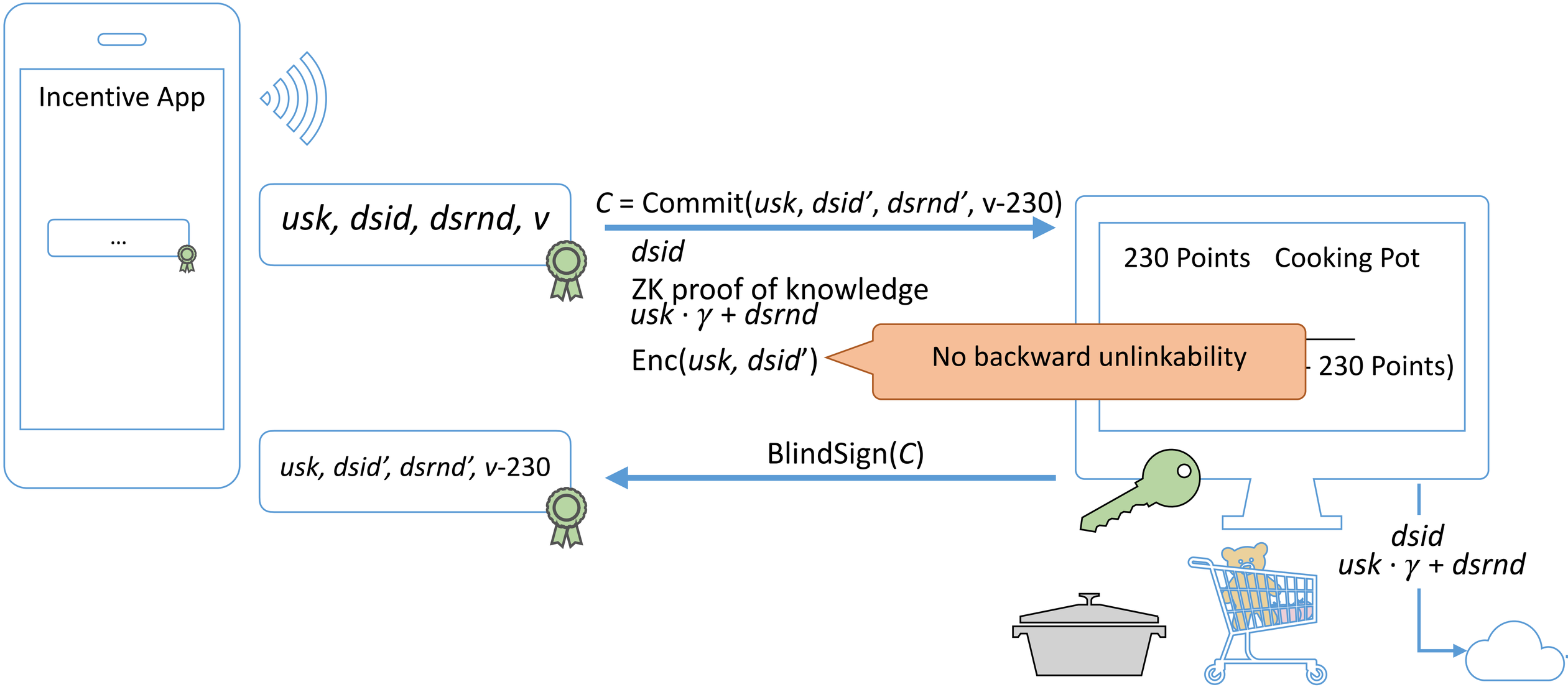


Our Work: Recovery

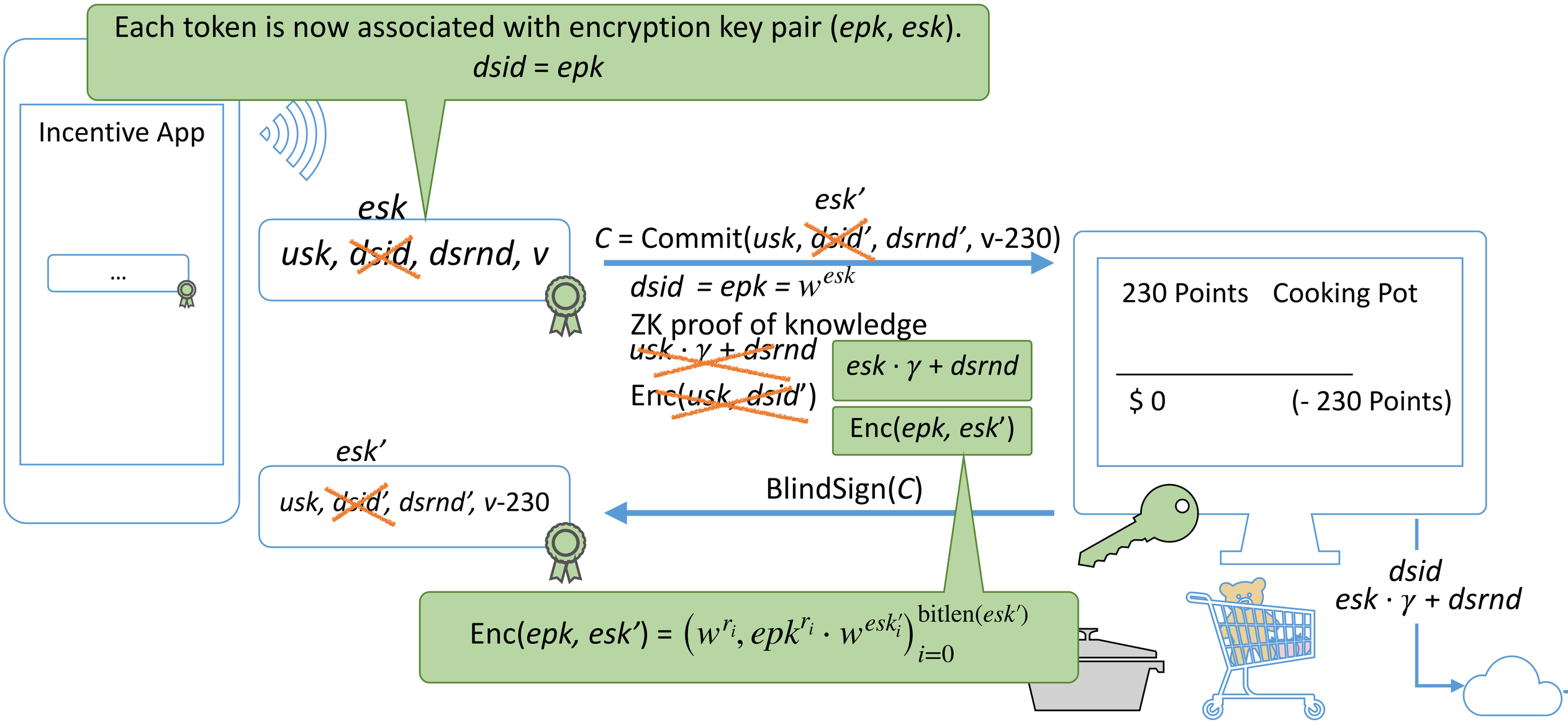


Backward Unlinkability

Idea: Backward Unlinkability



Our Work: Backward Unlinkability



Evaluation and Summary

Performance

Device	Issue	Join	Credit	Earn	Deduct	Spend
Phone (2016, Snapdragon 821)	88 ms	**116 ms**	28 ms	**60 ms**	1083 ms	**1017 ms**
Laptop (2019, i7-8650U)	**14 ms**	19 ms	**4 ms**	9 ms	**237 ms**	220 ms

Average computation time for each protocol

Implemented using upb.crypto (github.com/upbcuk) and mcl (github.com/herumi/mcl).

Summary

Lots of technical challenges

- Paper: definitions, details, proofs, …

Often the most frequent operation

- Very efficient *earning* of points through SPS-EQ

- Simple mechanism to handle *spend* retries

Tolerates interruptions of protocol execution without triggering double-spending detection

Better privacy in case of future device corruption

- *Backward-unlinkability* combined with traceability of remainder tokens
  - But: somewhat performance-hungry

Future Work: Any ideas more efficient than bitwise ElGamal?