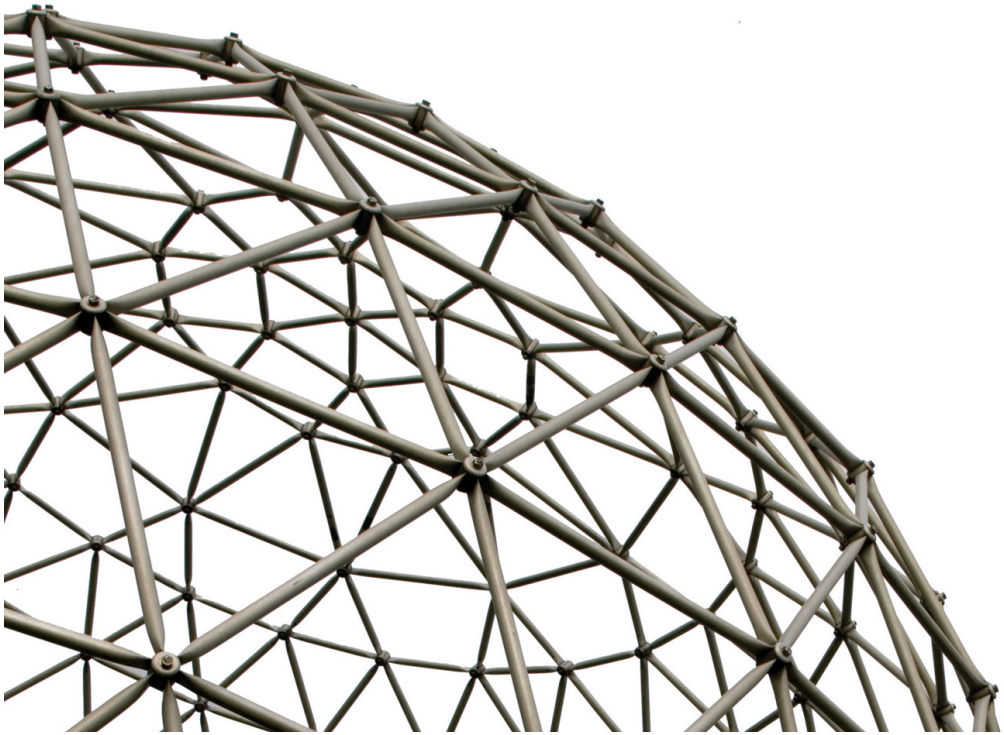
UNIVERSITY OF SURREY

Formal Security Analysis and Improvement of a hash-based NFC M-coupon Protocol

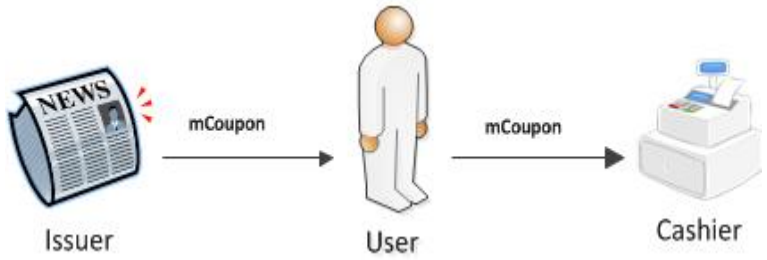


Ali Alshehri and Steve Schneider

Agenda

- Introduction. ✓
- Approach
  - CasperFDR (example)
  - More about the underline theory (CSP)
- Apply to the Hash-based NFC M-coupon protocols by Hsiang et al.
  - Capturing the requirements:
    - In CasperFDR
    - From the CSP aspect
  - Analysis (Attack & solutions)

Introduction

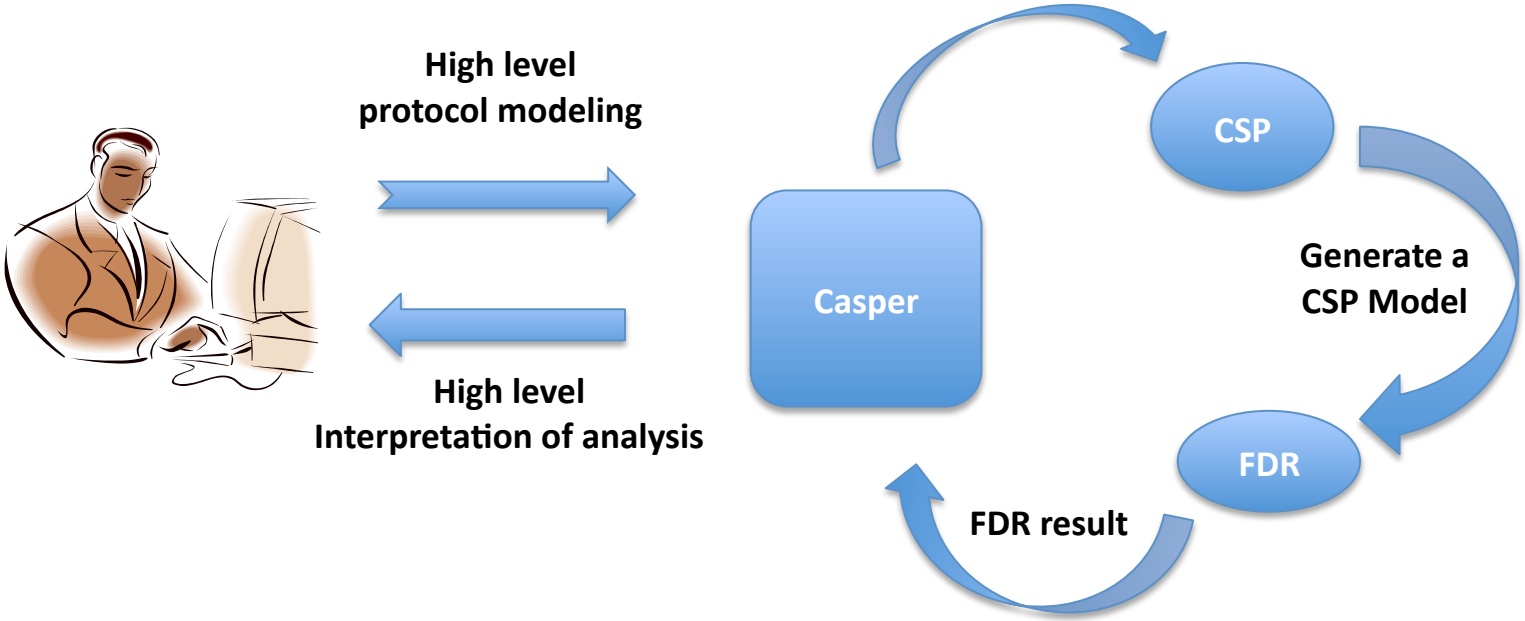


- **NFC** (Near Field Communication).
- **NFC mobile coupon protocols.**
  - The Hash-based M-coupon protocol.
- **Formal security analysis.**
  - CasperFDR

Agenda

- Introduction. ✓
- Approach ✓
  - CasperFDR (example)
  - More about the underline theory (CSP)
- Apply to a Hash-based NFC M-coupon protocols by Hsiang et al.
  - Capturing the requirements:
    - In CasperFDR
    - From the CSP aspect
  - Analysis (Attack & solutions)

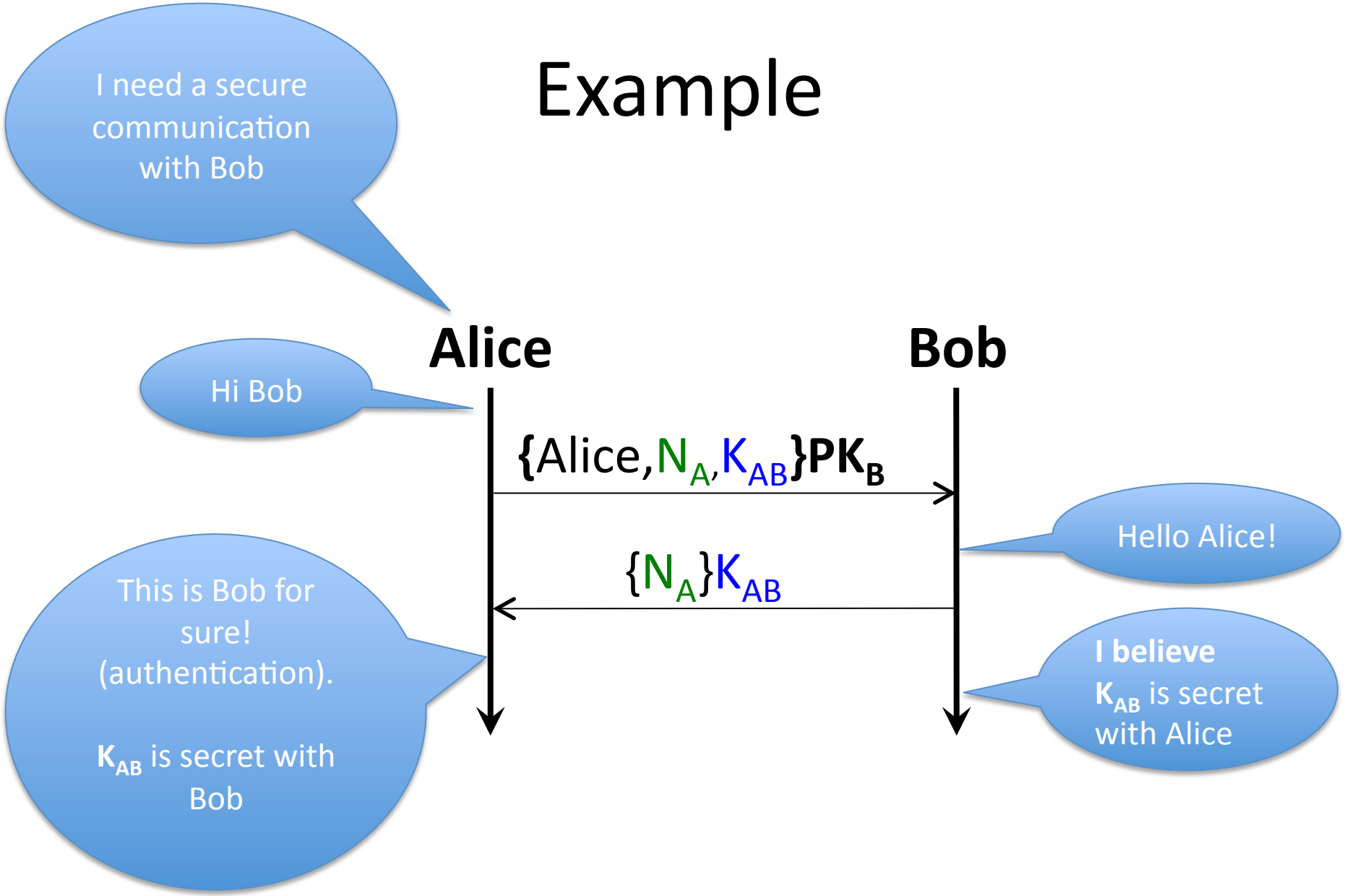
CasperFDR



-**CSP (Communicating Sequential Processes)**:
is a formal language for describing patterns of interaction in concurrent systems.

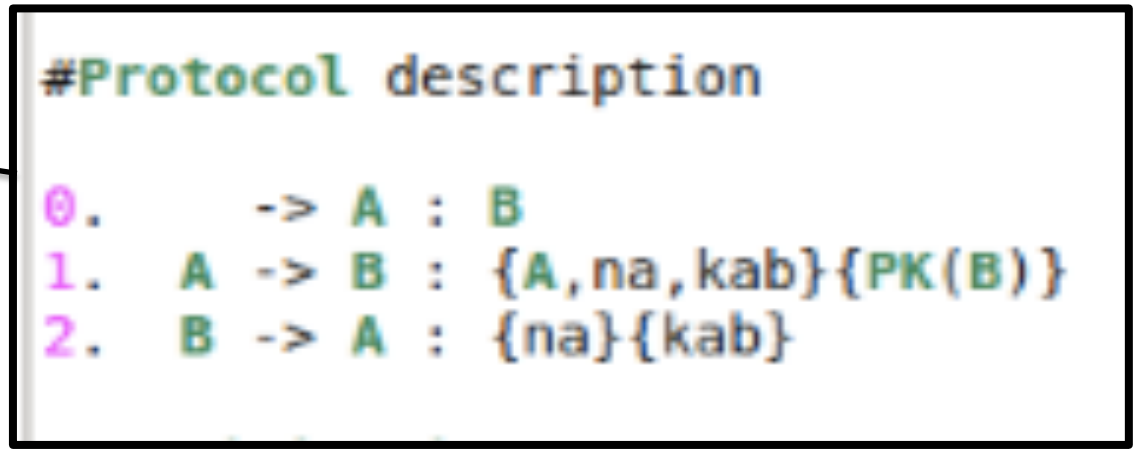
- FDR (Failures Divergences Refinement) : CSP refinement checker.

Example


I need a secure communication with Bob
Alice
Bob
Hi Bob
{Alice,N_A,K_{AB}}PK_B
Hello Alice!
{N_A}K_{AB}
This is Bob for sure! (authentication).
K_{AB} is secret with Bob
I believe K_{AB} is secret with Alice

Modeling in CasperFDR

```
#Free variables

A,B: Agent
na   : Nonce
PK :Agent -> PublicKey
SK :Agent -> SecretKey
InverseKeys =   (kab,kab), (PK, SK)
kab : SessionKey

#Processes

INITIATOR(A,B,na, kab)  knows PK
RESPONDER(B,A)          knows PK, SK(B)


#Protocol description

0.    -> A : B
1.  A -> B : {A,na,kab}{PK(B)}
2.  B -> A : {na}{kab}

#Specification

Secret(B,  kab , [A])
Agreement(B,A,[na,kab])

#Actual variables

Alice, Bob, Mallory : Agent
Na, Nm : Nonce
Kab,Km : SessionKey
InverseKeys = (Kab,Kab), (Km,Km)

#Functions
symbolic PK, SK

#System

INITIATOR(Alice,Bob,Na,Kab)
RESPONDER(Bob,Alice)

#Intruder Information
Intruder = Mallory
IntruderKnowledge = {Alice, Bob, Mallory, Nm, Km,PK, SK(Mallory)}
```



Applications Places System Thu 24 Jan, 6:52 PM

CasperFDR

File

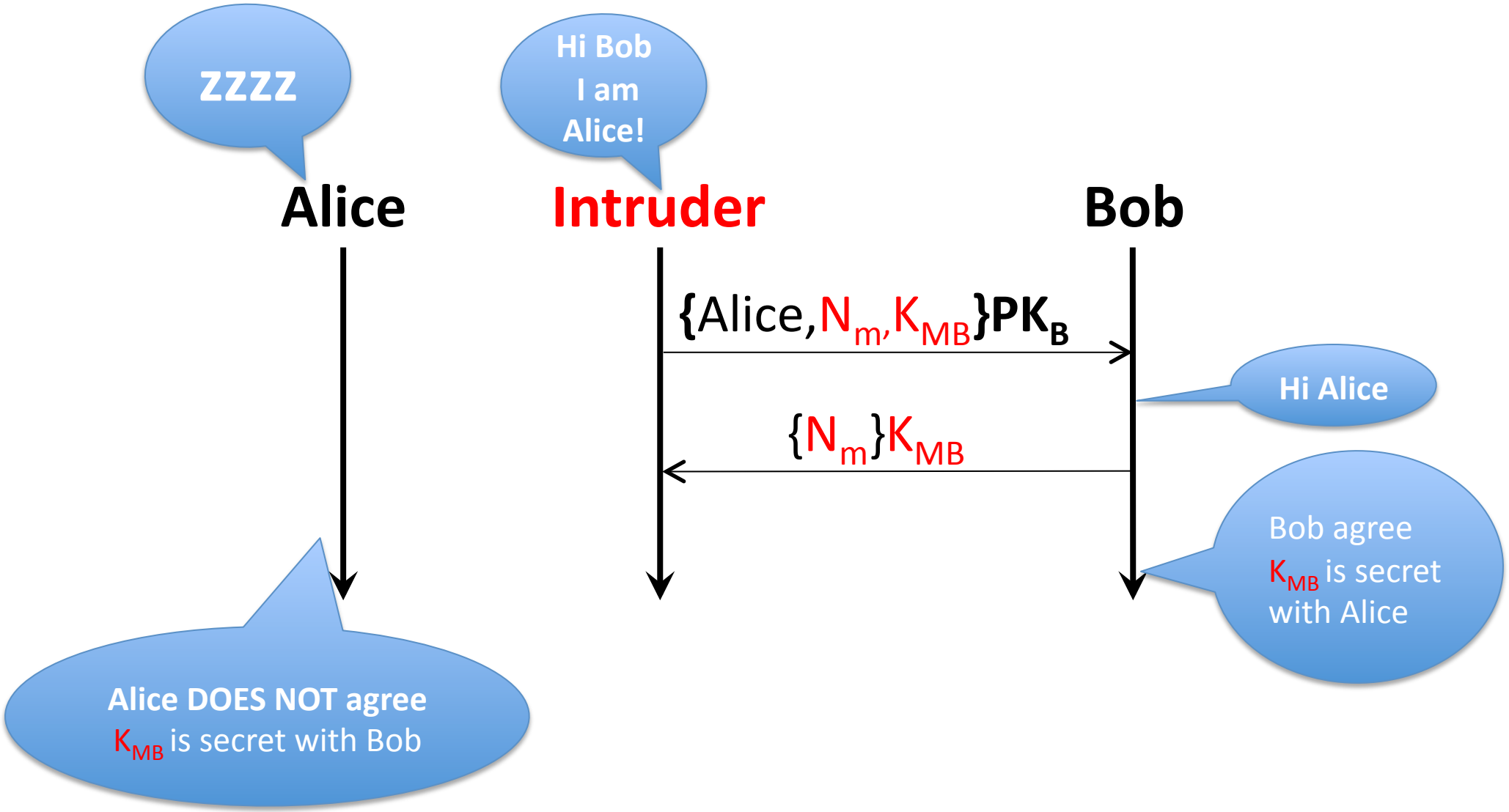
compile check compile & check

```
Initialising Casper....  Done.
Initialising FDR....  Done.
Ready.

Casper version 2.0

Parsing...
Type checking...
Consistency checking...
Compiling...
Writing output...
Output written to /home/cs/pgr/aa00538/Modelling
Done

Starting FDR
Checking /home/cs/pgr/aa00538/Modelling_Cods/Cas

Checking assertion SECRET_M::SECRET_SPEC [T= SEC
Attack found:

Top level trace:
  Bob believes Km is a secret shared with Alice
  The intruder knows Km

System level:
Casper> 1. I_Alice ->   Bob   : {Alice, Nm, Km}{
2.   Bob   -> I_Alice : {Nm}{Km}
  The intruder knows Km

**BEGIN TRACE example=1 process=1 path=0

BEGIN TRACE example=1 process=1 path=0
No attack found

**_tau

**_tau

_tau
No attack found

**signal.Claim_Secret.Bob.Km.{Alice}

**leak.Km
```

```
Top level trace:
  Bob believes Km is a secret shared with Alice
  The intruder knows Km

System level:
Casper> 1. I_Alice ->   Bob   : {Alice, Nm, Km}{PK(Bob)}
2.   Bob   -> I_Alice : {Nm}{Km}
  The intruder knows Km
```

file: NFC13_example

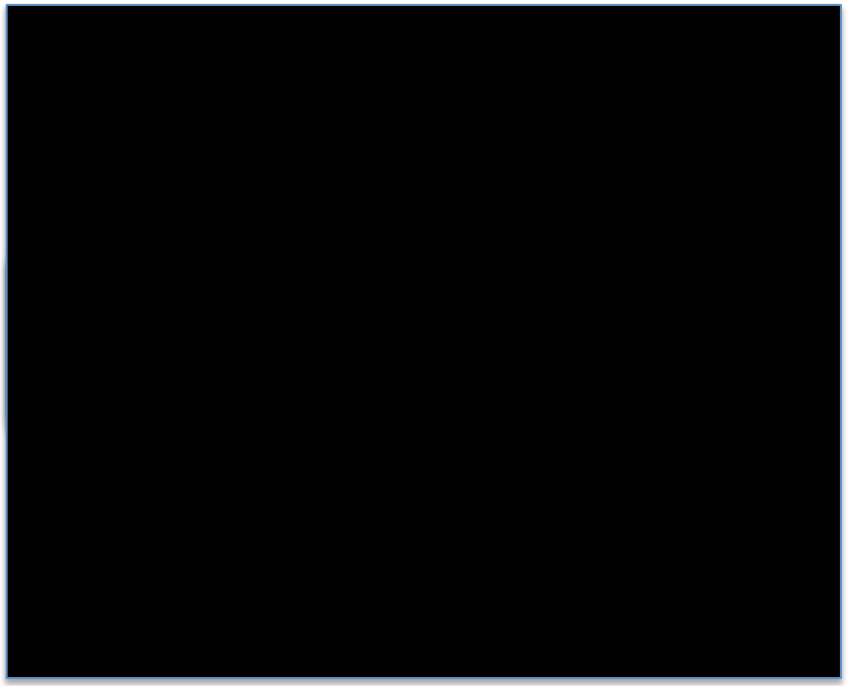
[NFC13_exampl...] [Terminal] [Terminal] [FDR 2.91 Acad...] CasperFDR [FDR Debug 3] [Screenshot-2.p...]


ZZZZ
Hi Bob
I am
Alice!
Alice
Intruder
Bob
{Alice,Nm,KMB}PKB
Hi Alice
{Nm}KMB
Bob agree
KMB is secret
with Alice
Alice DOES NOT agree
KMB is secret with Bob

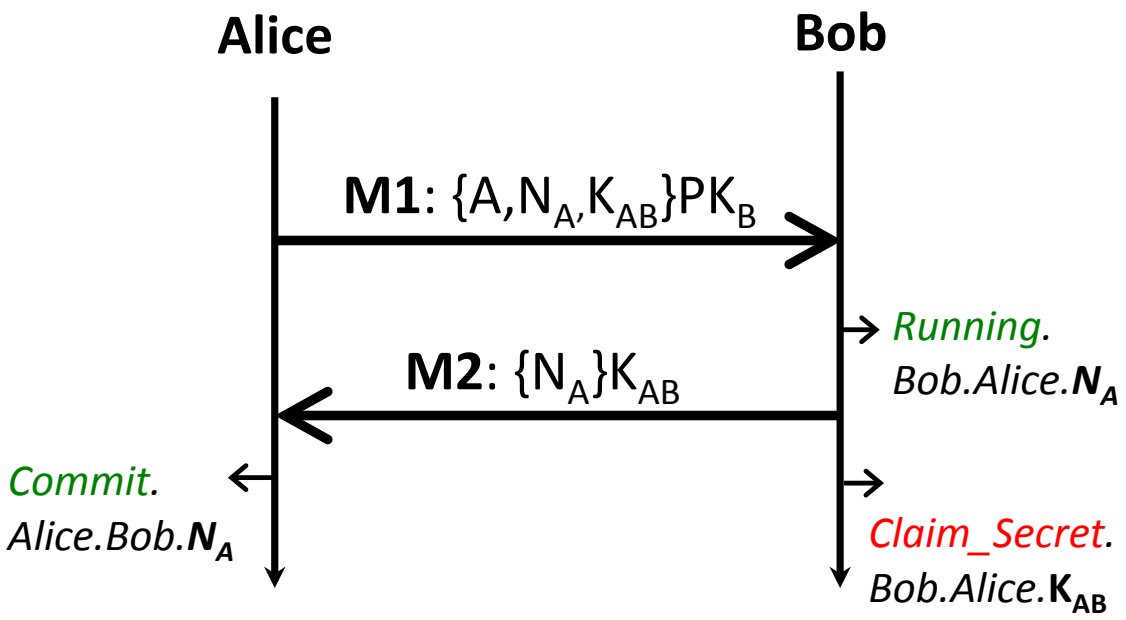
CasperFDR (black-box User)

High level protocol modeling

High level Interpretation of analysis

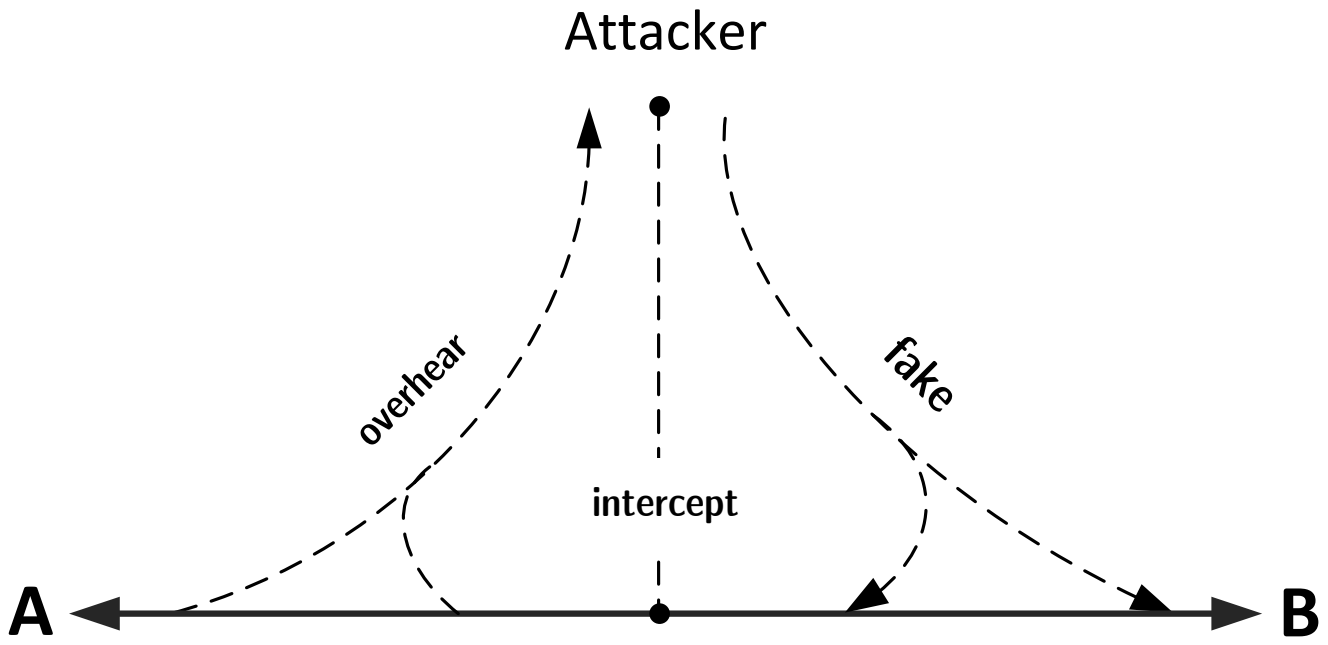


The CSP theory aspect



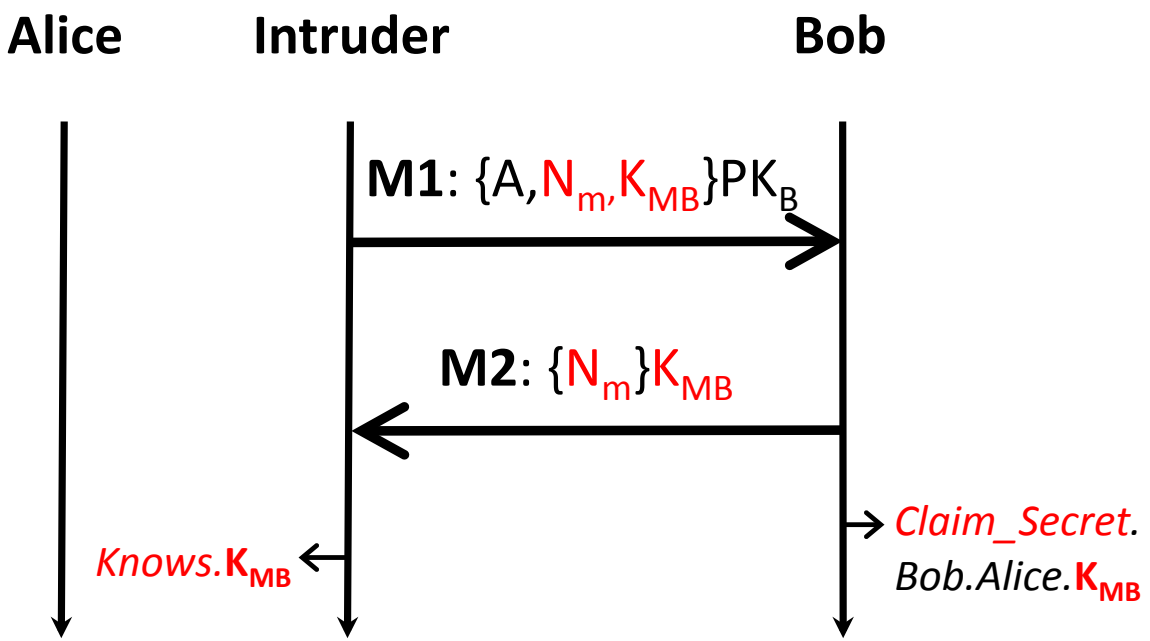
New events – Independent processes

The CSP theory aspect



Dolev-Yao model threat

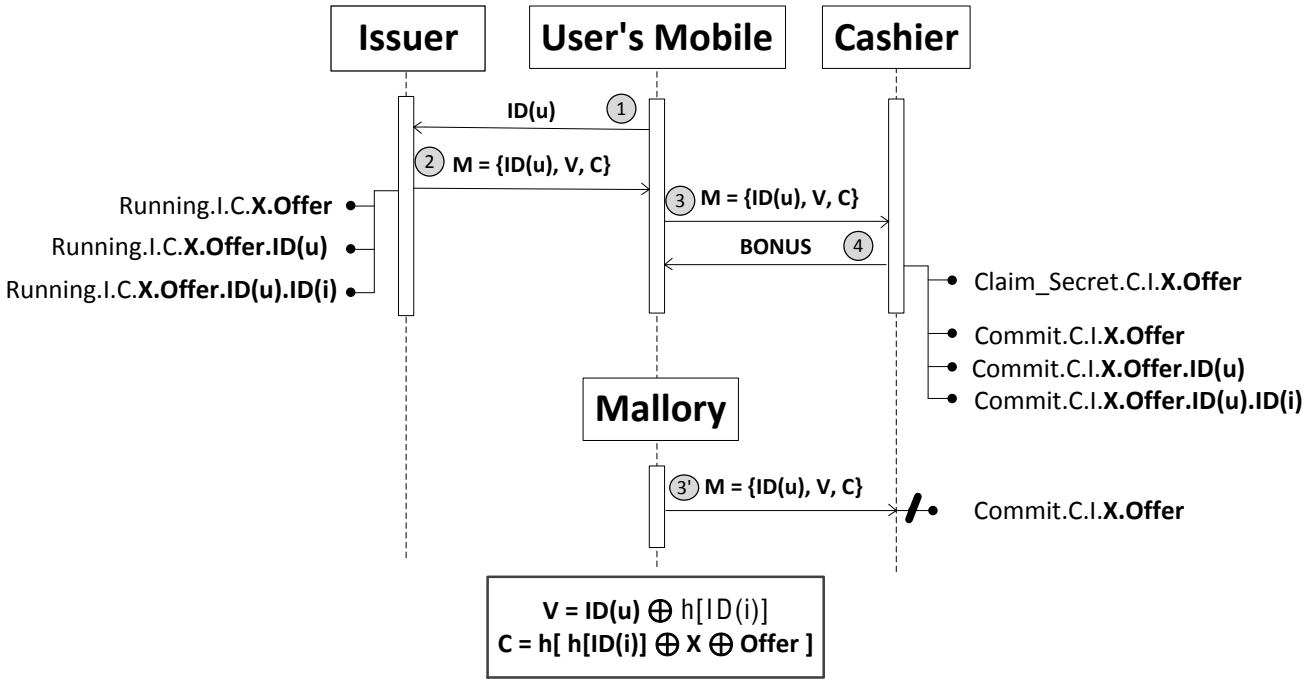
The CSP theory aspect



Agenda

- Introduction. ✓
- Approach ✓
  - CasperFDR (example)
  - More about the underline theory (CSP)
- Apply to a Hash-based NFC M-coupon protocols by Hsiang et al. ✓
  - Capturing the requirements:
    - In CasperFDR
    - From the CSP aspect
  - Analysis (Attack & solutions)

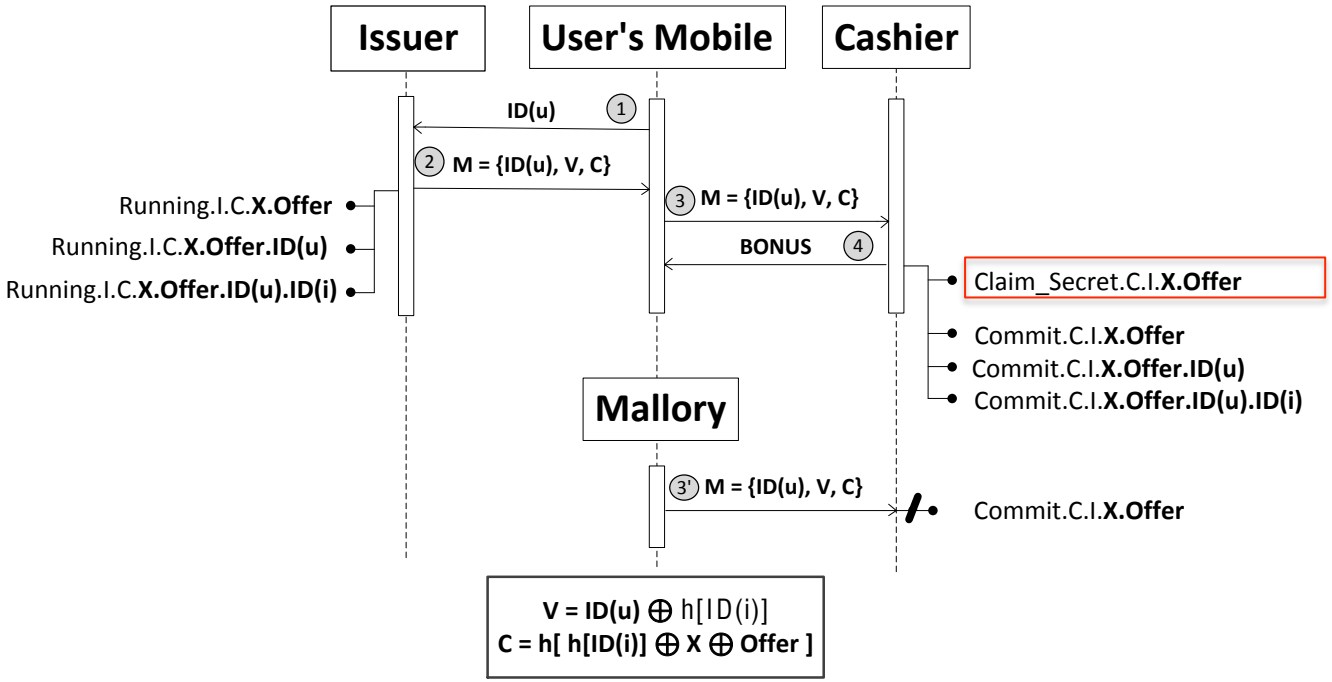
Hash-based M-coupon protocol



Security Requirements:

- Confidentiality
- Forgery Protection: (No Unauthorized Generation & No Manipulation)
- Unauthorized Copying: (Not Transferable)
- Data Integrity
- No Multiple Cash-in

Hash-based M-coupon protocol



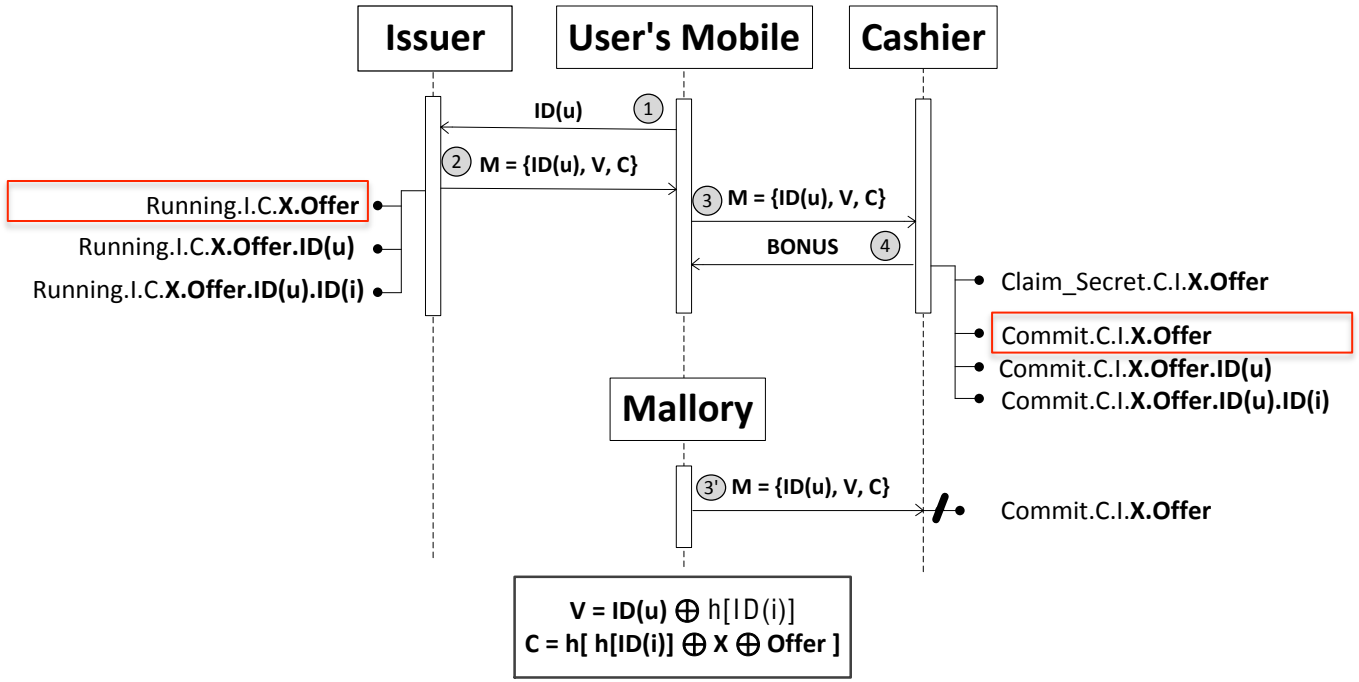
Security Requirements:

- Confidentiality
- Forgery Protection: (No Unauthorized Generation & No Manipulation)
- Unauthorized Copying: (Not Transferable)
- Data Integrity
- No Multiple Cash-in

In CasperFDR:

StrongSecret (C, X, Offer , [I])

Hash-based M-coupon protocol



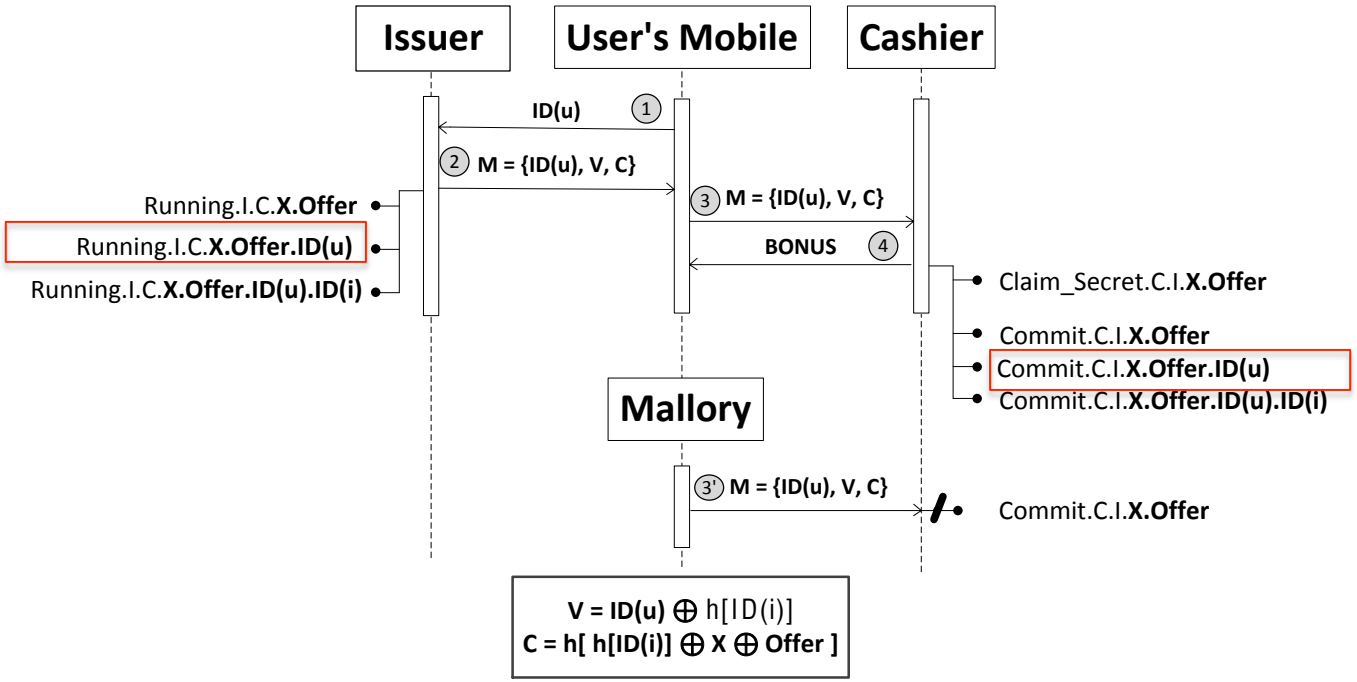
Security Requirements:

- Confidentiality
- Forgery Protection: (No Unauthorized Generation & No Manipulation)
- Unauthorized Copying: (Not Transferable)
- Data Integrity
- No Multiple Cash-in

In CasperFDR:

NonInjectiveAgreement (I,C,[X,Offer])

Hash-based M-coupon protocol



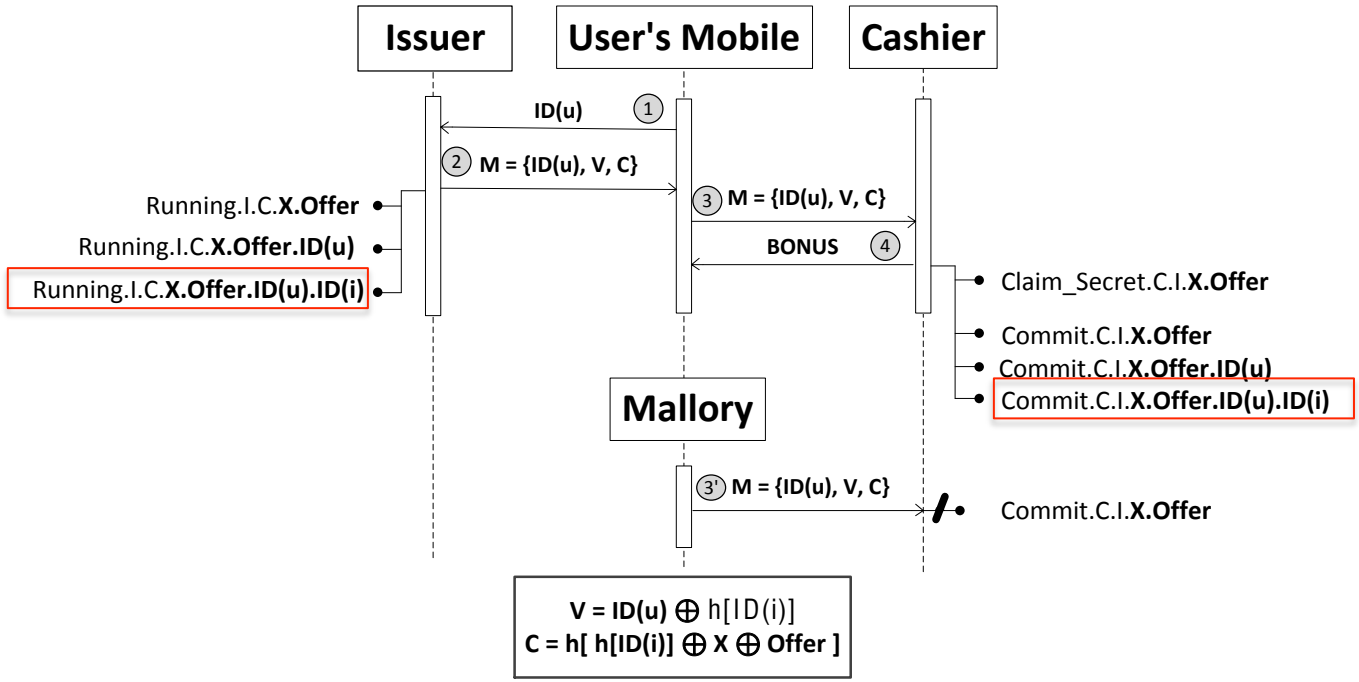
Security Requirements:

- Confidentiality
- Forgery Protection: (No Unauthorized Generation & No Manipulation)
- Unauthorized Copying: (Not Transferable)
- Data Integrity
- No Multiple Cash-in

In CasperFDR:

NonInjectiveAgreement (I,C,[X,Offer,ID(u)])

Hash-based M-coupon protocol



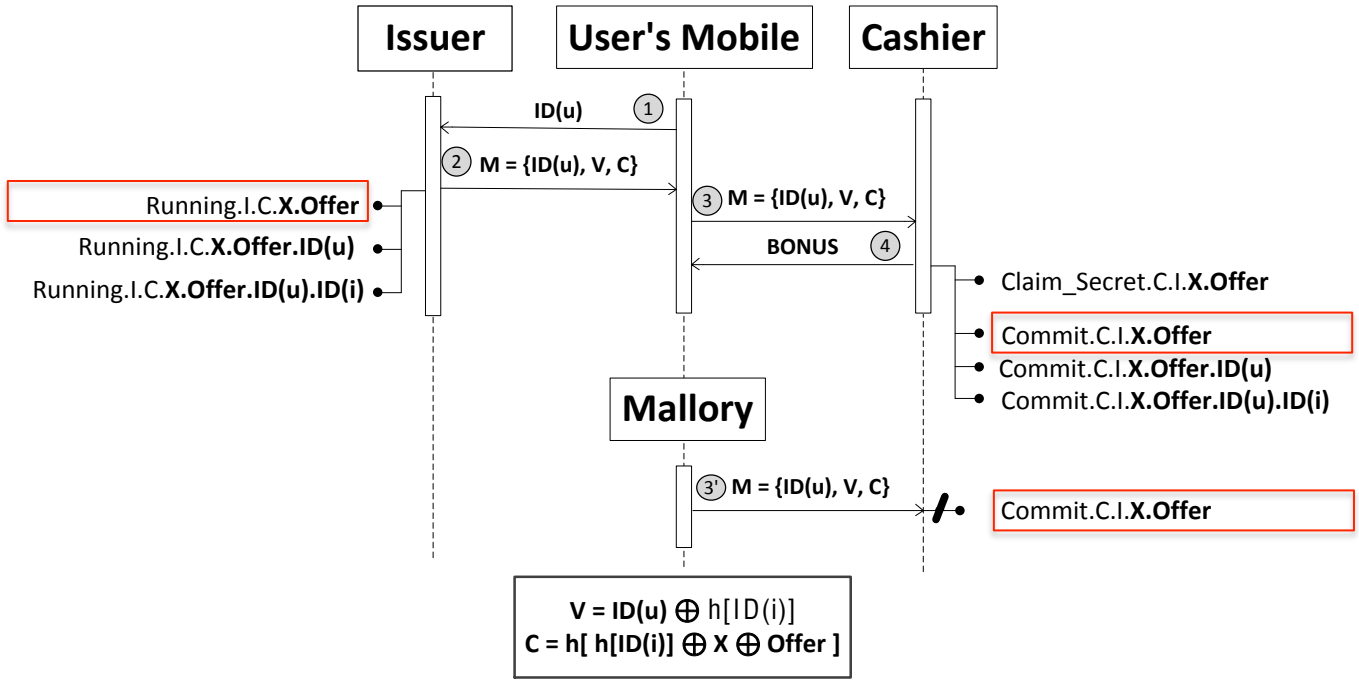
Security Requirements:

- Confidentiality
- Forgery Protection: (No Unauthorized Generation & No Manipulation)
- Unauthorized Copying: (Not Transferable)
- Data Integrity
- No Multiple Cash-in

In CasperFDR:

NonInjectiveAgreement (I,C,[X,Offer,ID(u),ID(i)])

Hash-based M-coupon protocol



Security Requirements:

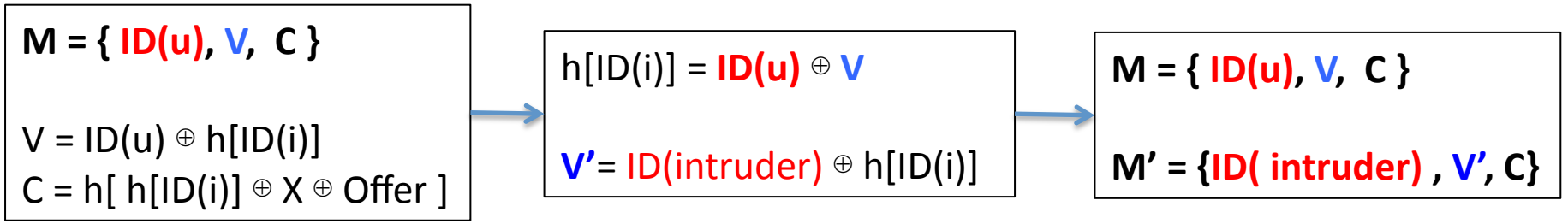
- Confidentiality
- Forgery Protection: (No Unauthorized Generation & No Manipulation)
- Unauthorized Copying: (Not Transferable)
- Data Integrity
- No Multiple Cash-in

In CasperFDR:

Agreement (I,C,[X,Offer])

Analysis

	Hash-based
Confidentiality	√
Forgery Protection	√
Data Integrity	x
No Multiple Cash in	x
Not Transferable	x



Solution

	Hash-based	Enhanced Hash-based
Confidentiality	√	√
Forgery Protection	√	√
Data Integrity	x	√
No Multiple Cash in	x	√
Not Transferable	x	√
User Authentication		

Hash-based

M = { ID(u), V, C }

$V = ID(u) \oplus h[ID(i)]$

$C = h[\, h[ID(i)] \oplus X \oplus Offer \,]$

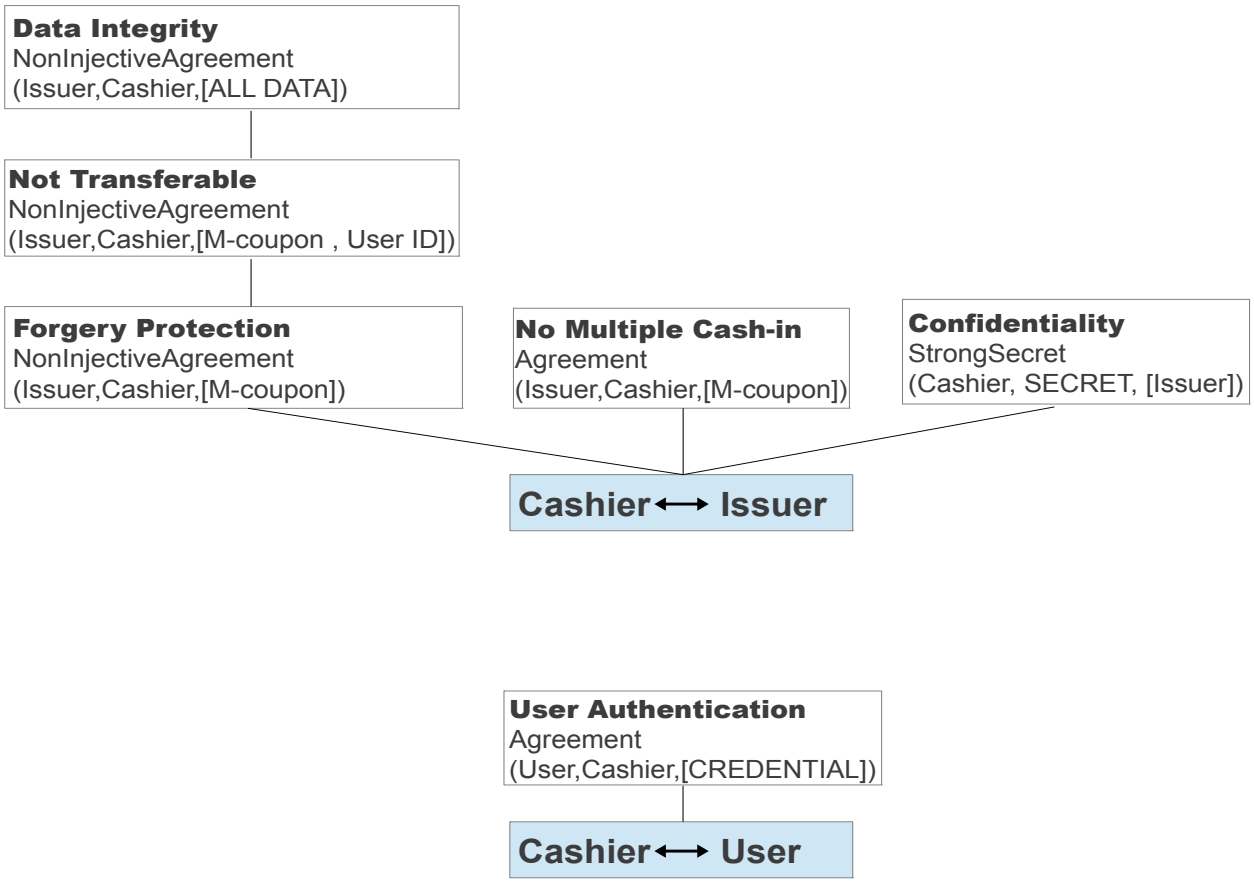
Enhanced Hash-based

M = { ID(u), V, C }

$V = ID(u) \oplus h[ID(i)]$

$C = h[\, h[ID(i)] \oplus X \oplus Offer \oplus \mathbf{ID(u)} \,]$

A general framework



Conclusion

- Hash-based M-coupon protocol.
- Deep formal analysis.
- Other solutions suggested (footfall, premium)

Thank you

- Questions?

Ali Alshehri
a.a.alshehri@surrey.ac.uk