P-19 15
GW

2002

Topics in Concurrency (2)

[Uses Ch. on Security Protocols from notes on "Topics in Concurrency

(a) Agent A:

out A . in x . out $\{x\}_{key(A,S)}$. nil

Agent B:

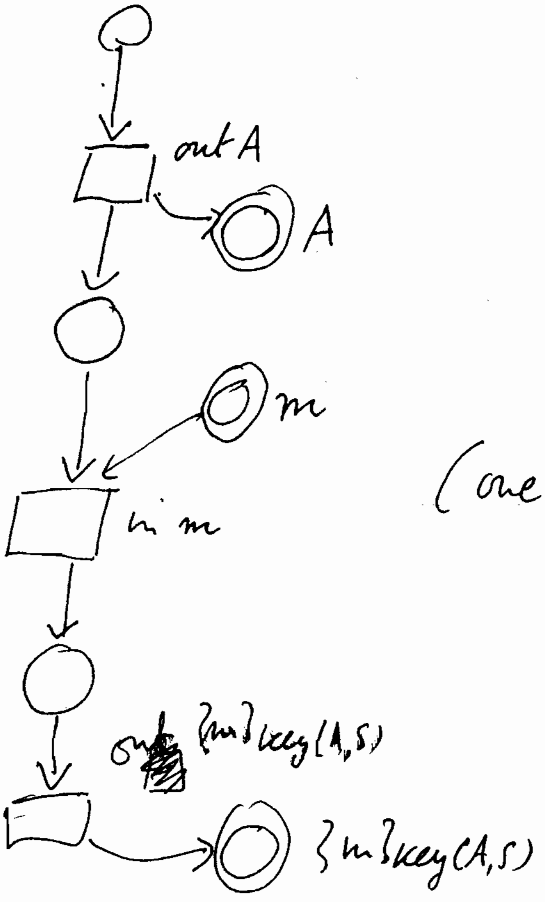
in A . out new x x . in **Z** out $\{A, z\}_{key(B,S)}$. in $\{A, x\}_{key}$. nil

Agent S:

in $\{A, \{x\}_{key(A,S)}\}_{key(B,S)}$. out $\{A, x\}_{key(B,S)}$. nil.

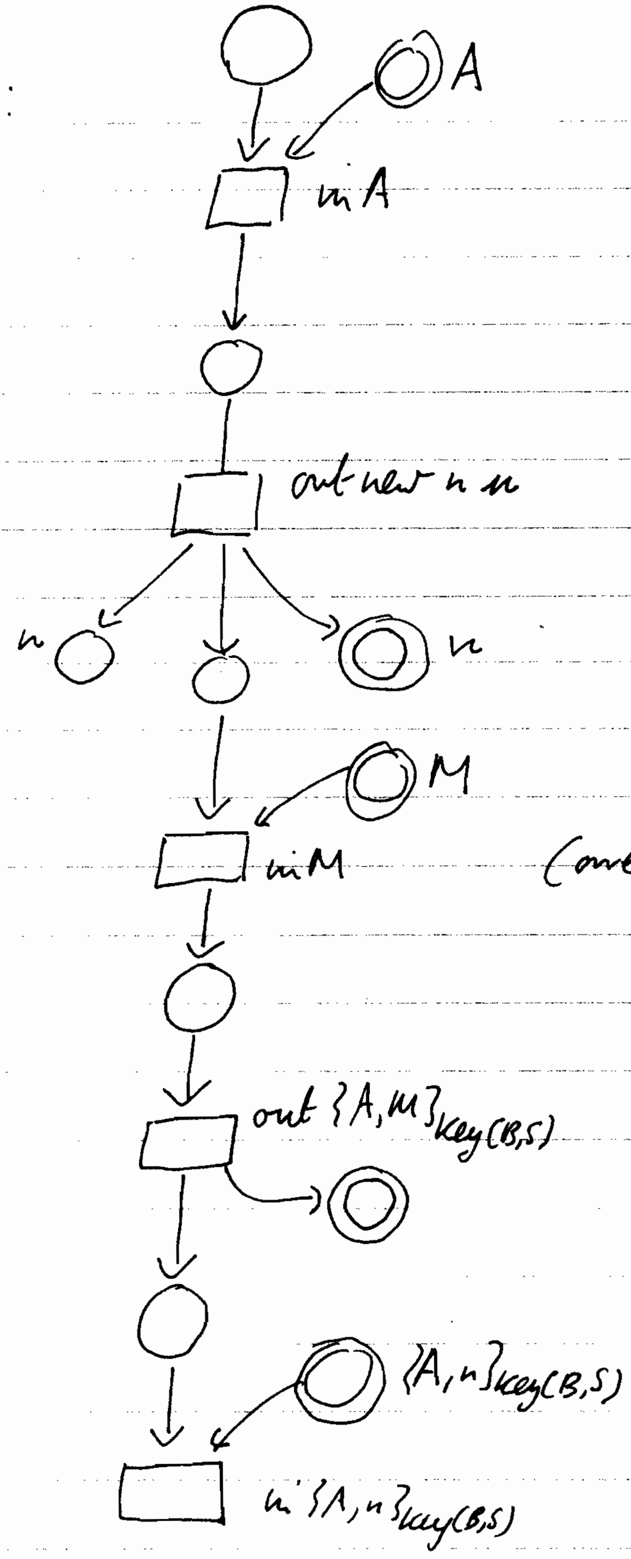
(b) Their events:

A:



(one event for ea. choice of m)

B :

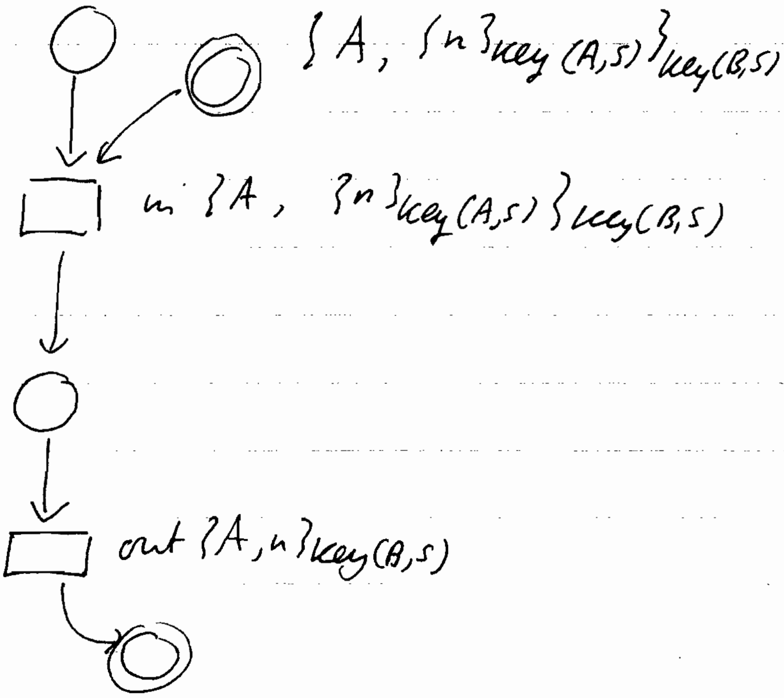


(an event for ea. choice of n)

(one event for ea. choice of M)

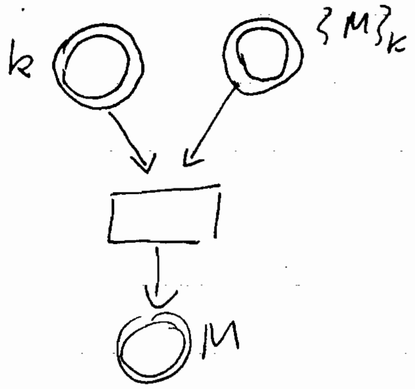
S :

(an event for ea. choice of n)

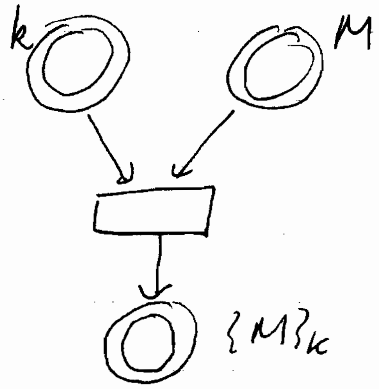

$\{A, \{n\}_{key(A,S)}\}_{key(B,S)}$
in $\{A, \{n\}_{key(A,S)}\}_{key(B,S)}$
out $\{A, n\}_{key(B,S)}$

(2) (c) Attacker events:

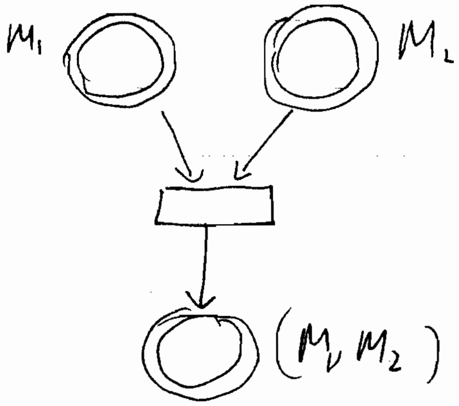
decryption :



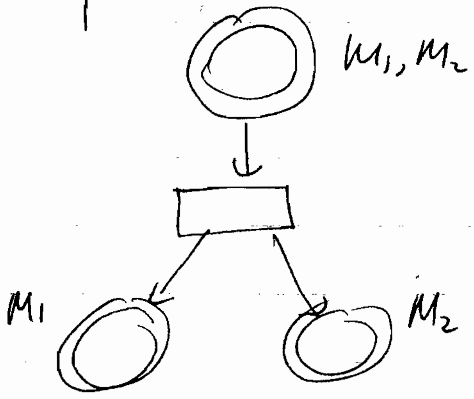
encryption :



composition :



Decomposition



(d) $Q(\mathcal{M})$ means

$$key(A,S),\ key(B,S) \not\sqsubset M$$

for all output conditions $M \in \mathcal{M}$. ($\sqsubset$ is the submessage relation)

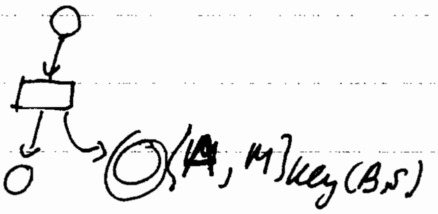
Suppose $Q(\mathcal{M})$ holds at the initial marking. There cannot be an earliest event e violating Q by the following argument, considering the possible forms of events.

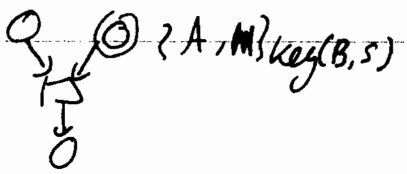
If e is an attacker event, with postcondition M s.t.

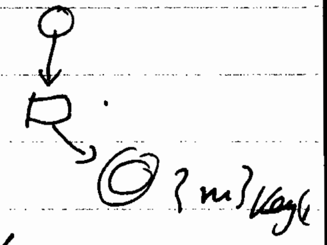
$$key(A,S) \sqsubset M \quad \text{or} \quad key(B,S) \sqsubset M \qquad (*)$$

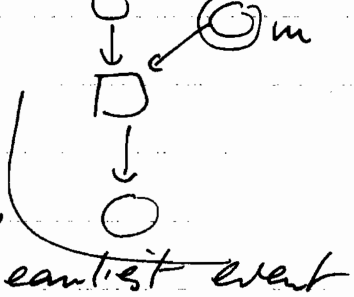
then it will have a precondition s.t. (*), so cannot be the earliest event violating Q.

If e is an output event of B, then <u>either</u> the output is a name (so does not violate Q)

<u>or</u> e =  in which

case by control precedence e depends on the previous occurrence of an event  so cannot be the earliest event violating Q.

If e is an output event of A, then *either* the output is agent name A (so does not violate Q)
or the event has the form 

By control precedence e depends on the previous occurrence of an event 

in which $key(A,S) \sqsubset m$ or $key(B,S) \sqsubset m$, and hence e cannot be the earliest event violating Q.

(e) ~~[illegible]~~ The principles ~~below~~ are ~~order~~ freshness, control precedence, ~~output input precedence~~ and well-foundedness ~~Freshness~~ are used, well-foundedness with the property

$$R(\mathcal{M}) \iff \forall m \in \mathcal{M}.\ \{A,n\}_{Key(B,S)} \not\sqsubset M$$