1 current sec model to transcribe ADEM + AMAC to a more symmetric style

1.1 used primitives

- ADEM: input tag, key and message lead to a cythertext. It should be improbable distinguish the cythertexts of two messages. (adversary may choose two cythertexts and has to guess which one of the two is encrypted)

- AMAC: input tag, key and message lead to a cythertext. It should be improbable to make a forgery (a pair (key, tag, message, cythertext) that verifies without begin generated by calling Omac(key, tag, message) first)

1.2 goal

Each user is provided with two keys, a message and a tag that is bound to the user and does not repeat between users. The message is encrypted using the tag and two keys to generate a cythertext consisting of two parts. First part is Cdem which is the message encrypted with the nonce and the first key while the second part is Cmac that is the mac computed over Cdem, the tag and the second key. Given only one queries to Oenc per user and multiple queries to Odec which always occurs after the Oenc queries, the message should be protected against active adversaries as long as ADEM and AMAC are secure.

1.3 Sec model

the security is purely based on the games for the AMAC and ADEM that are visible below. All variables are elaborated in the paper

Game N-MIOT-UF$_{A,N}$	**Oracle Omac(j,t,m)**	**Oracle Ovrf(j,m,c)**
00 forged $\leftarrow 0$	07 if $C_j \neq \emptyset$: return $\perp$	13 if $C_j = \emptyset$: return $\perp$
01 $T \leftarrow \emptyset$	08 if $t \in T$: return $\perp$	14 if $(m,c) \in C_j$: return $\perp$
02 for all $j \in [1..N]$:	09 $T \leftarrow T \cup \{t\}$; $t_j \leftarrow t$	15 if M.vrf(K_j, t_j, m, c):
03 $\quad K_j \xleftarrow{\$} \mathcal{K}$	10 $c \leftarrow$ M.mac(K_j, t_j, m)	16 $\quad$ forged $\leftarrow 1$
04 $\quad C_j \leftarrow \emptyset$	11 $C_j \leftarrow C_j \cup \{(m,c)\}$	17 $\quad$ return $true$
05 run A	12 return c	18 return $false$
06 return forged		

Game N-MIOT-IND$^b_{A,N}$	**Oracle Oenc(j,t,m_0,m_1)**	**Oracle Odec(j,c)**
00 $T \leftarrow \emptyset$	06 if $C_j \neq \emptyset$: return $\perp$	12 if $C_j = \emptyset$: return $\perp$
01 for all $j \in [1..N]$:	07 if $t \in T$: return $\perp$	13 if $c \in C_j$: return $\perp$
02 $\quad K_j \xleftarrow{\$} \mathcal{K}$	08 $T \leftarrow T \cup \{t\}$; $t_j \leftarrow t$	14 $m \leftarrow$ A.dec(K_j, t_j, c)
03 $\quad C_j \leftarrow \emptyset$	09 $c \leftarrow$ A.enc(K_j, t_j, m_b)	15 return m
04 $b' \xleftarrow{\$} A$	10 $C_j \leftarrow C_j \cup \{c\}$	
05 return b'	11 return c	

with

Proc A.enc$'(K,t,m)$	**Proc A.dec$'(K,t,c)$**
00 $(K_{dem}, K_{mac}) \leftarrow K$	05 $(K_{dem}, K_{mac}) \leftarrow K$
01 $c_{dem} \leftarrow$ A.enc(K_{dem}, t, m)	06 $(c_{dem}, c_{mac}) \leftarrow c$
02 $c_{mac} \leftarrow$ M.mac(K_{mac}, t, c_{dem})	07 if M.vrf$(K_{mac}, t, c_{dem}, c_{mac})$:
03 $c \leftarrow (c_{dem}, c_{mac})$	08 $\quad m \leftarrow$ A.dec(K_{dem}, t, c_{dem})
04 return c	09 $\quad$ return m
	10 return $\perp$

2   needed sec model to transcribe ADEM + AMAC to a more symmetric style

for now we only look at the nonce based options as the pkc paper does that too.

2.1   used primitives

- ADEM: input nonce, key en message lead to a cythertext which should be improbable to distinguish from RO (adversary has to guess if he is talking to RO or ADEM)

- AMAC: input nonce, key en message lead to a tag that should be improbable to distinguishable from random oracle (adversary has to guess if he is talking to RO or AMAC)

2.2   goal

Each user is provided with two keys, a message and a lock that does not repeat between users. The message is encrypted using the lock and two keys. Given only one queries to Oenc per user and multiple queries to Odec which always occurs after the Oenc queries, the message should be protected against active adversaries as long as ADEM and AMAC are secure.

2.3   Sec model

We define the following sec games for the AMAC, the ADEM and the ADEM+AMAC (names will prob be improved later):

Game $\mathrm{AMAC}_{A,N}^{M}$	**Oracle** Omac(j,l,m)
$0:\quad L \leftarrow \emptyset$	$5:\quad$ **if** $T_j \neq \emptyset :$ **return** $\perp$
$1:\quad$ **for** $j \in [1..N] :$	$6:\quad$ **if** $l \in L :$ **return** $\perp$
$2:\qquad K_j \leftarrow^{\$} K$	$7:\quad L \leftarrow L \cup \{l\}$
$3:\quad b' \leftarrow A$	$8:\quad l_j = l$
$4:\quad$ **return** b'	$9:\quad t \leftarrow M.mac(K_j, l_j, m)$
	$10:\quad$ **return** t

Figure 1: AMAC game, M is either the MAC or Random Oracle

Game $\mathrm{AMAC}_{A,N}^{E}$	**Oracle** Omac(j,l,m)
$0:\quad L \leftarrow \emptyset$	$5:\quad$ **if** $T_j \neq \emptyset :$ **return** $\perp$
$1:\quad$ **for** $j \in [1..N] :$	$6:\quad$ **if** $l \in L :$ **return** $\perp$
$2:\qquad K_j \leftarrow^{\$} K$	$7:\quad L \leftarrow L \cup \{l\}$
$3:\quad b' \leftarrow A$	$8:\quad l_j = l$
$4:\quad$ **return** b'	$9:\quad c \leftarrow E.enc(K_j, l_j, m)$
	$10:\quad$ **return** c

Figure 2: ADEM game, E is either the DEM or Random Oracle

Game $\mathrm{AE}_{A,N}^{AE,D}$	**Oracle** Oenc(j,l,m)	**Oracle** Odec(j,m)
0 : $L \leftarrow \emptyset$	6 : **if** $T_j \neq \emptyset :$ **return** $\perp$	13 : **if** $c_j \neq \emptyset :$ **return** $\perp$
1 : **for** $j \in [1..N] :$	7 : **if** $l \in L :$ **return** $\perp$	14 : **if** $c \in C_j :$ **return** $\perp$
2 : $\quad K_j \leftarrow^{\$} K$	8 : $L \leftarrow L \cup \{l\}$	15 : $m \leftarrow D.dec(K_j, L_j, c)$
3 : $\quad C_j \leftarrow \emptyset$	9 : $l_j = l$	16 : **return** m
4 : $b' \leftarrow A$	10 : $c \leftarrow EA.enc(K_j, l_j, m)$	
5 : **return** b'	11 : $C_j \leftarrow C_j \cup c$	
	12 : **return** t	

Figure 3: AE game, where AE is either the encryption scheme having to the MAC and DEM or RO and D is either the description scheme or a function that always returns false

Where EA.enc and D.dec should be constructed from M.mac, E.enc and E.dec. Following General Composition reconsidered, three ways to construct this EA should be considered following from the N1, N2 and N3 scheme. One thing to keep in mind with this that these schemes would originally use associated data. For now we can discard this but it is not proven that the same security results would also follow form this case without associated data

3 burning questions

- Q1: Is het oke om de games gebazeerd te hebben op RO
  Q2:(klopt het dat RO stickt sterker is dan left-right)

- in GCrec, waarom zijn er bij de n-schemes geen N4 en N5 schemas?
  A: die voegen niets toe Q2: klopt dat?

4 current todo's

- in meer detail opschrijven wat de variables zijn van de sec games en wat de aannamens zijn
- vertaling van 3 N schemas opschrijven
- crypto.bib kijken
- mayhabs beginnen met schrijven in main

5   main idea

The PKC paper ends with a ADEM + AMAC construction as "solution". The original paper from ENC -¿ MAC has been revised, so this should prob be revised as well. In general its nice to write down thing in a more "sym crypto" style as we use symmetric primitives. It would probably also be nice to revise it more in general and see what other ways there are to reach the end-goal expected in the PKC paper.