Broadcast-Optimal Two Round MPC with Asynchronous Peer-to-Peer Channels

Ivan Damgård[1], *Divya Ravi*[1,2], *Luisa Siniscalchi*[3], *Sophia Yakoubov*[1]

eprint.iacr.org/2023/1187

[1]Aarhus University, [2]University of Amsterdam, [3]DTU

Broadcast-Optimal Two Round MPC

Broadcast-Optimal Two Round MPC

Broadcast-Optimal Two Round MPC

Grace

x_G

Bruce

x_B

Alan

x_A

Broadcast-Optimal Two Round MPC

$y = f(x_A, x_B, x_G)$

Grace

x_G

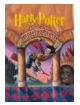
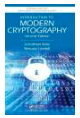
Bruce

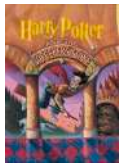
x_B

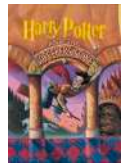
Alan

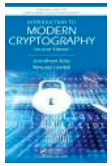
x_A

Broadcast-Optimal Two Round MPC

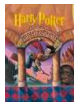
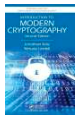
y = should we read  or  for book club?

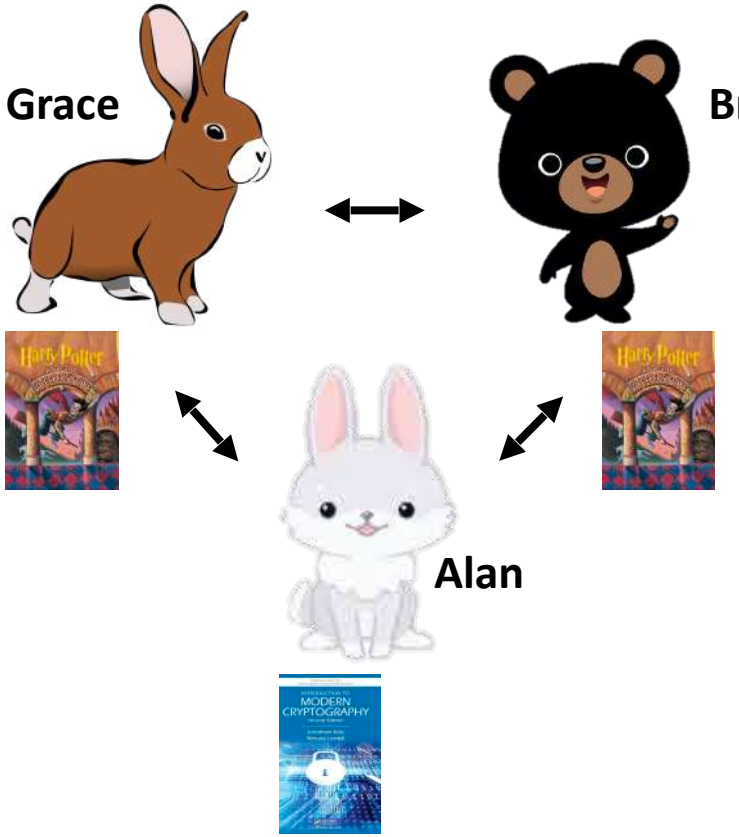




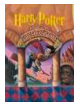
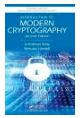


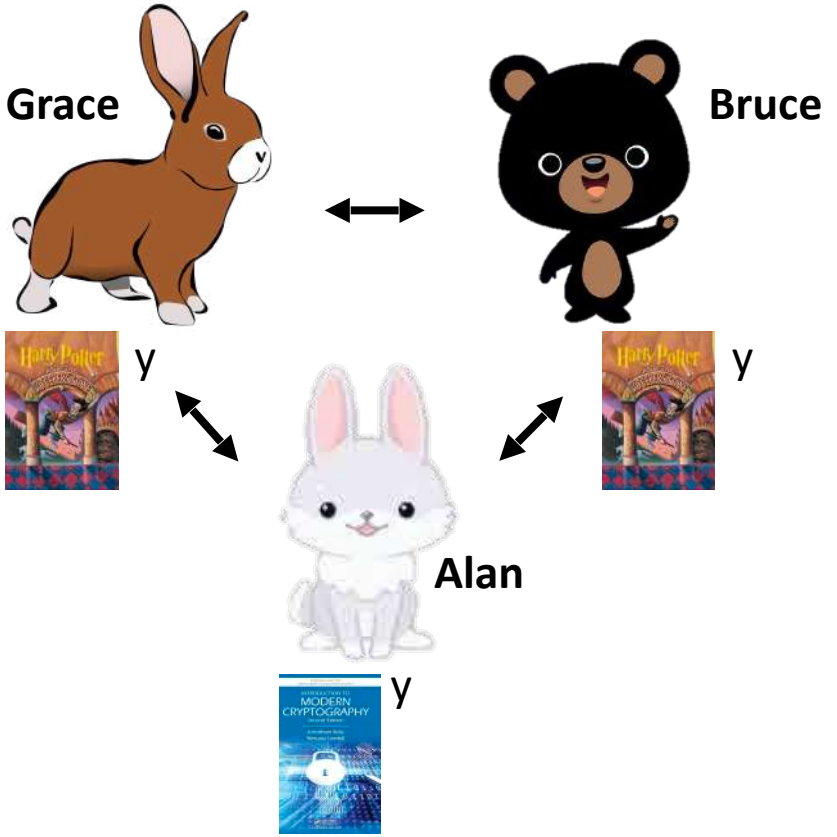
Broadcast-Optimal Two Round MPC

y = should we read  or  for book club?

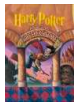
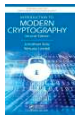


Broadcast-Optimal Two Round MPC

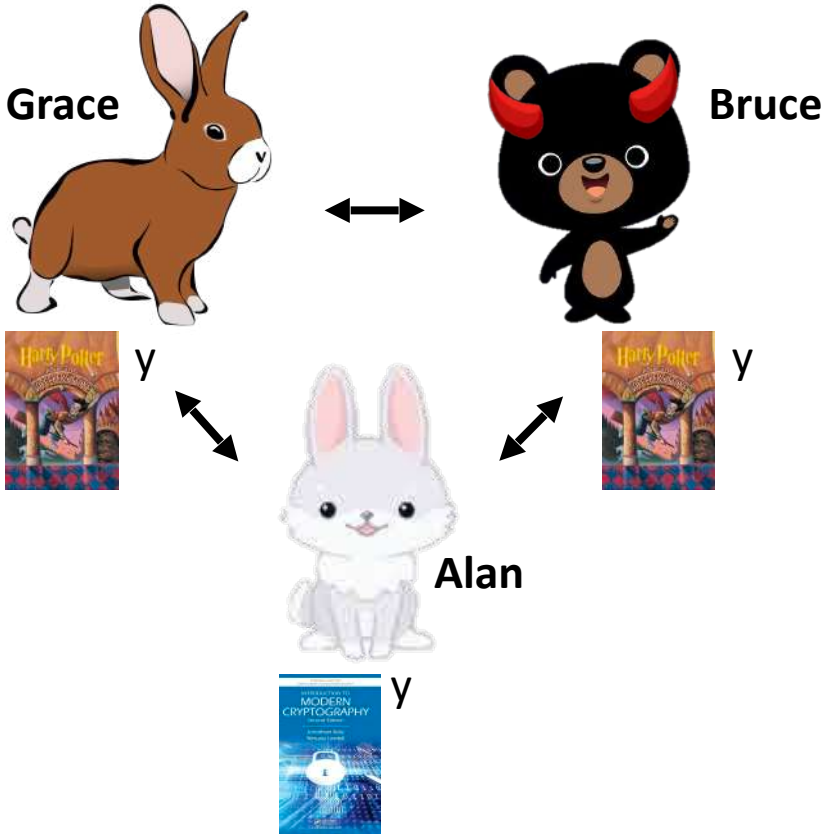
y = should we read  or  for book club?



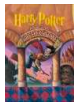
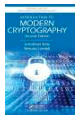
Broadcast-Optimal Two Round MPC

y = should we read  or  for book club?

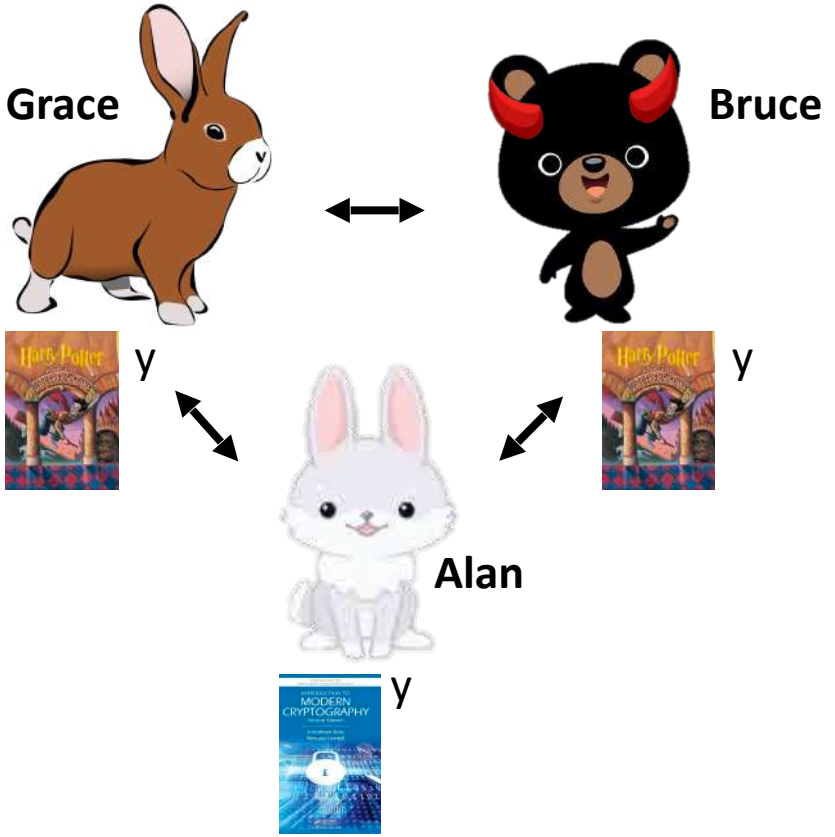
- Privacy: t corrupt parties learn no additional information about honest parties' inputs



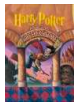
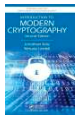
Broadcast-Optimal Two Round MPC

y = should we read  or  for book club?

- Privacy: t corrupt parties learn no additional information about honest parties' inputs
- Correctness

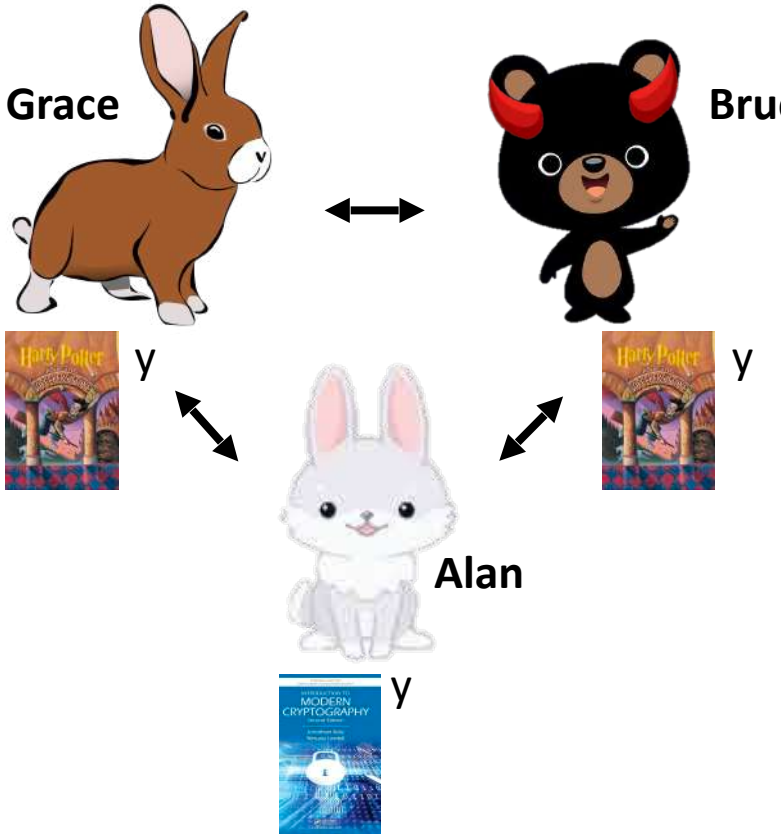


Broadcast-Optimal Two Round MPC

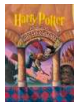
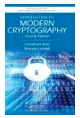
y = should we read  or  for book club?

- Privacy: t corrupt parties learn no additional information about honest parties' inputs
- Correctness

Stronger

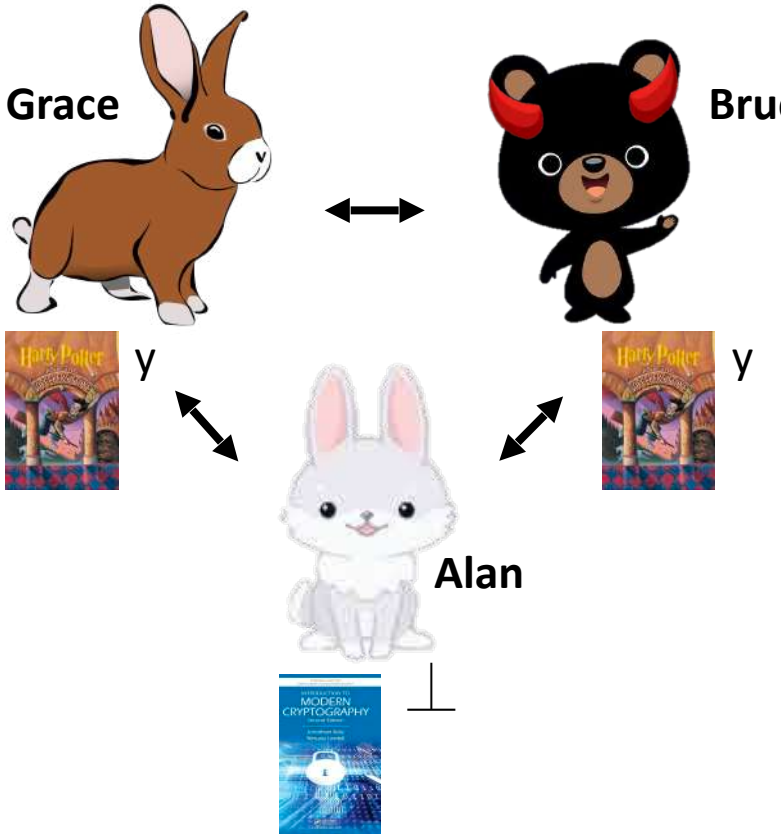


Broadcast-Optimal Two Round MPC

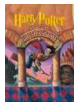
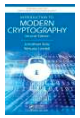
y = should we read  or  for book club?

- Privacy: t corrupt parties learn no additional information about honest parties' inputs
- Correctness
  - **Selective Abort**

Stronger

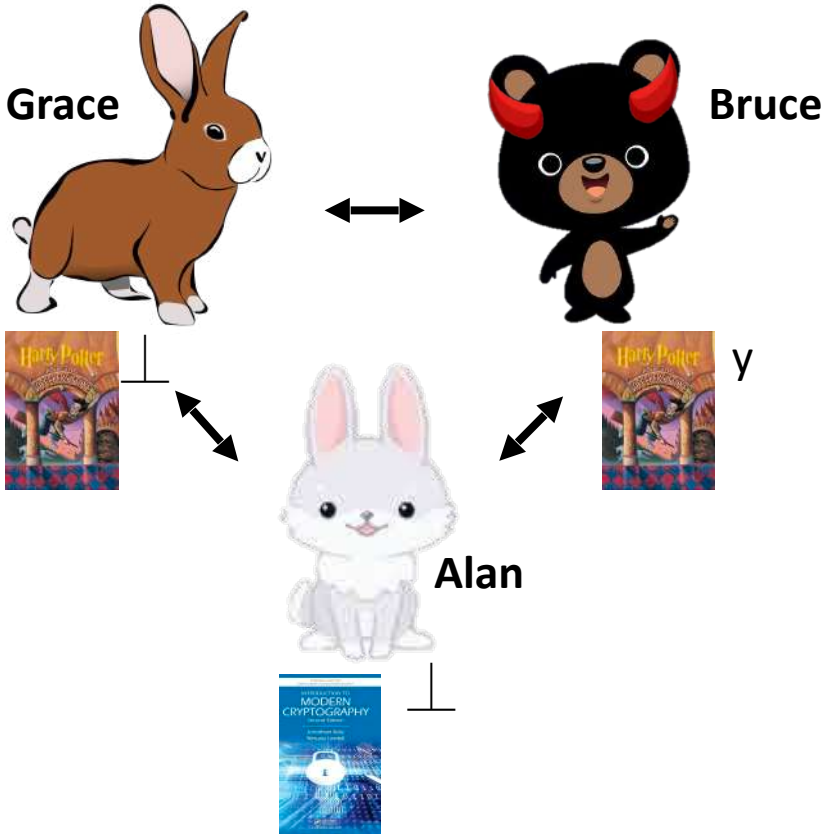


Broadcast-Optimal Two Round MPC

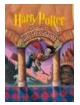
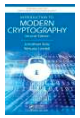
y = should we read  or  for book club?

- Privacy: t corrupt parties learn no additional information about honest parties' inputs
- Correctness
  - Selective Abort
  - **Unanimous Abort**

Stronger

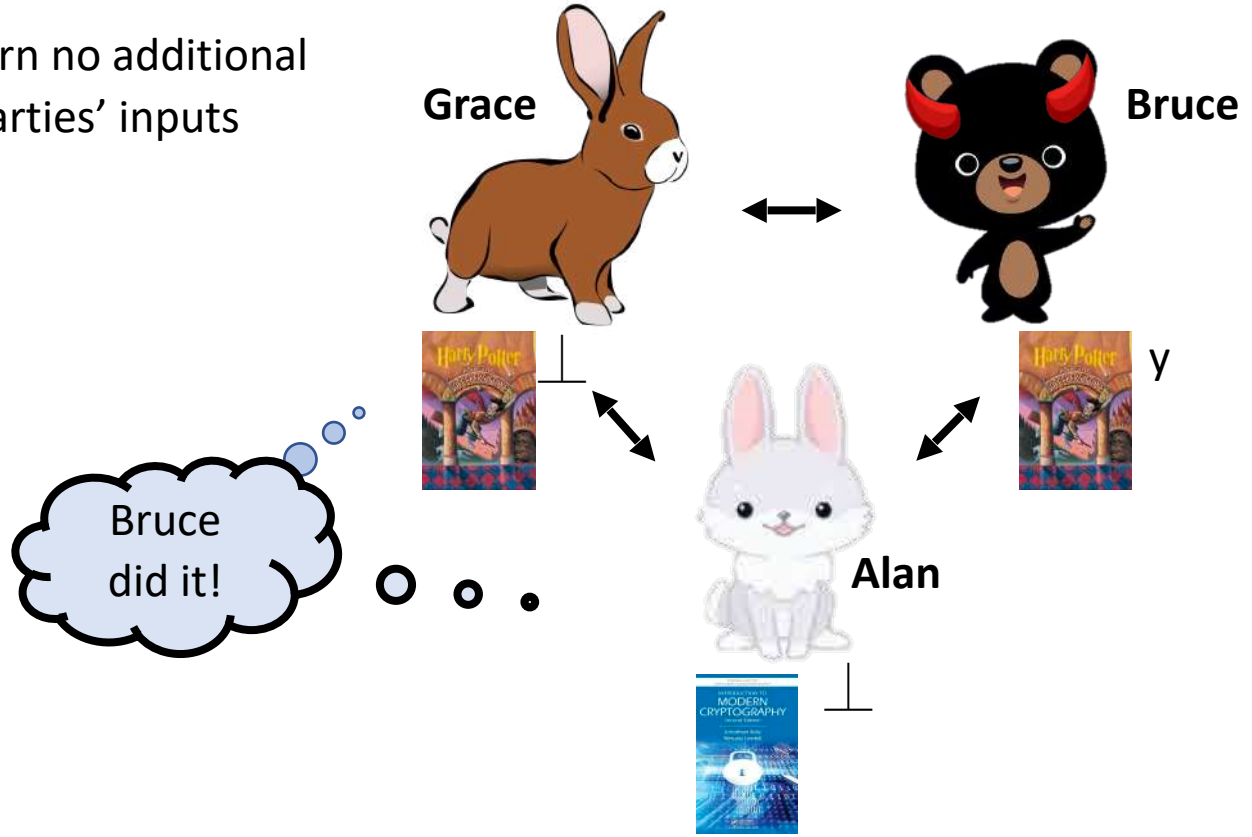


Broadcast-Optimal Two Round MPC

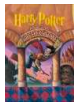
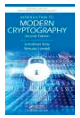
y = should we read  or  for book club?

- Privacy: t corrupt parties learn no additional information about honest parties' inputs
- Correctness:
  - Selective Abort
  - Unanimous Abort
  - **Identifiable Abort**

Stronger

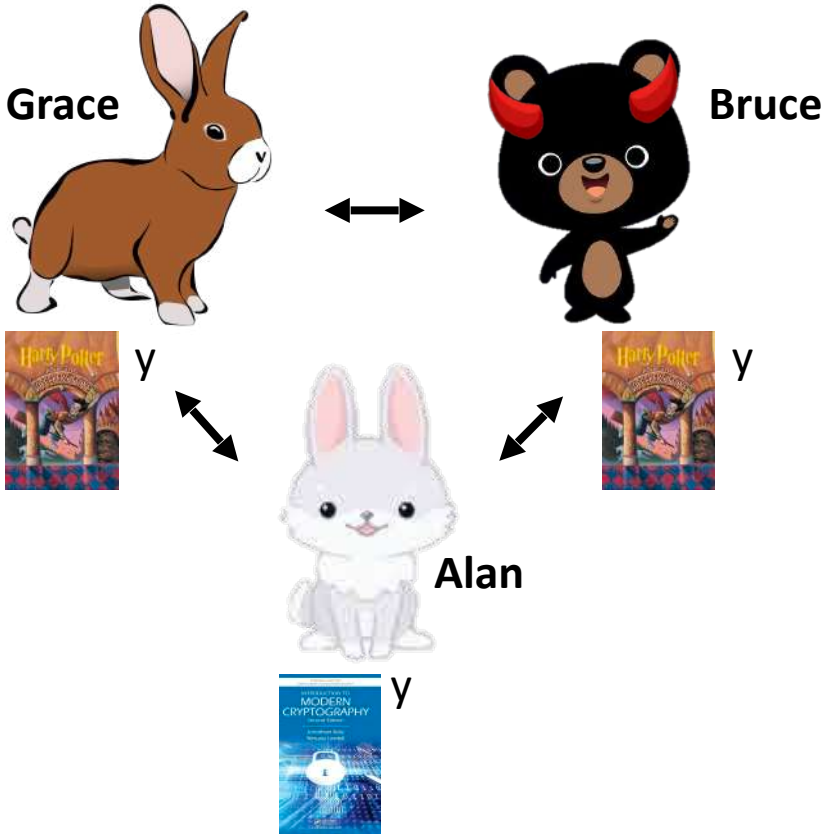


Broadcast-Optimal Two Round MPC

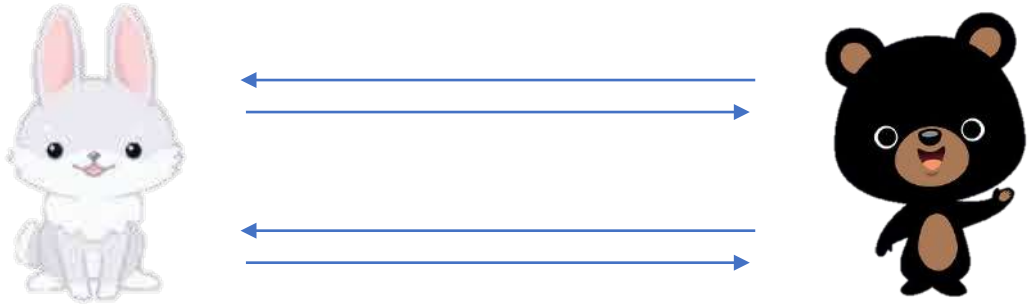
y = should we read  or  for book club?

- Privacy: t corrupt parties learn no additional information about honest parties' inputs
- Correctness:
  - Selective Abort
  - Unanimous Abort
  - Identifiable Abort
  - **Guaranteed Output Delivery**

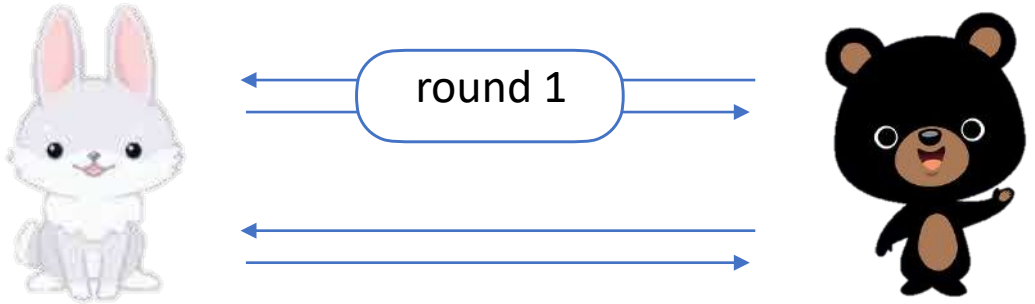
Stronger



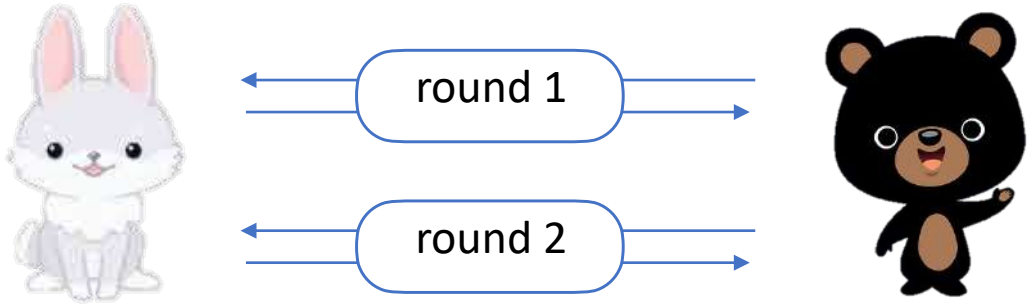
Broadcast-Optimal Two Round MPC



Broadcast-Optimal Two Round MPC

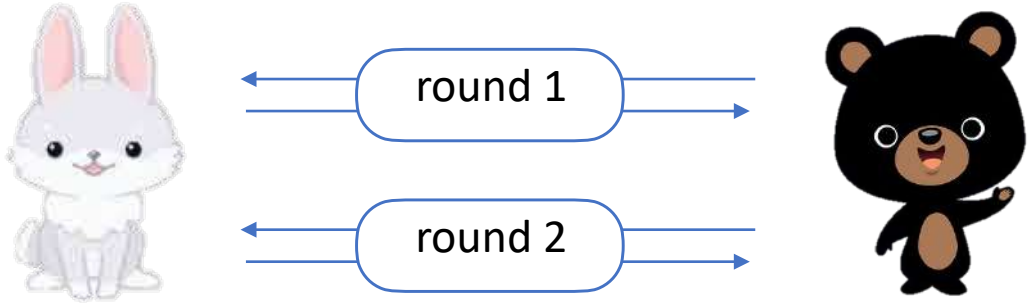


Broadcast-Optimal Two Round MPC



Broadcast-Optimal Two Round MPC

- Rounds are expensive!
  - At least two rounds needed for MPC



Broadcast-Optimal Two Round MPC

- Rounds are expensive!
  - At least two rounds needed for MPC
- Broadcast is expensive!
  - Takes many rounds, or
  - Uses expensive resources

Broadcast-Optimal Two Round MPC

- Rounds are expensive!
  - At least two rounds needed for MPC
- Broadcast is expensive!
  - Takes many rounds, or
  - Uses expensive resources
- Most two-round MPC:
  - Does not use broadcast (gets weaker guarantees - e.g. selective abort)

Broadcast-Optimal Two Round MPC

- Rounds are expensive!
  - At least two rounds needed for MPC
- Broadcast is expensive!
  - Takes many rounds, or
  - Uses expensive resources
- Most two-round MPC:
  - Does not use broadcast (gets weaker guarantees - e.g. selective abort)
  - Uses broadcast in both rounds (expensive)

Broadcast-Optimal Two Round MPC

which of the two rounds do we *really* need broadcast in?

Broadcast-Optimal Two Round MPC

which of the two rounds do we *really* need broadcast in?

	Dishonest majority	Honest majority
PKI	[CGZ20]	[DMRS**Y**21]
No PKI		[DRS**Y**23]

PKI: public key infrastructure

Broadcast-Optimal Two Round MPC

which of the two rounds do we *really* need broadcast in?

	Dishonest majority	Honest majority
PKI	[CGZ20]	[DRSY23]
No PKI		

Assumes Synchronous Channels

PKI: public key infrastructure

Synchronous communication

Synchronous communication

Guaranteed to be delivered within one round

Synchronous communication

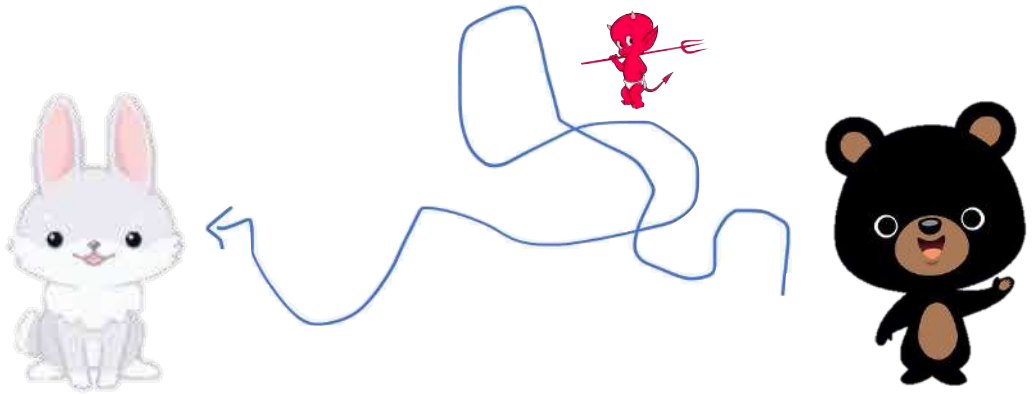
Guaranteed to be delivered within one round

Asynchronous communication

Synchronous communication

Guaranteed to be delivered within one round

Asynchronous communication

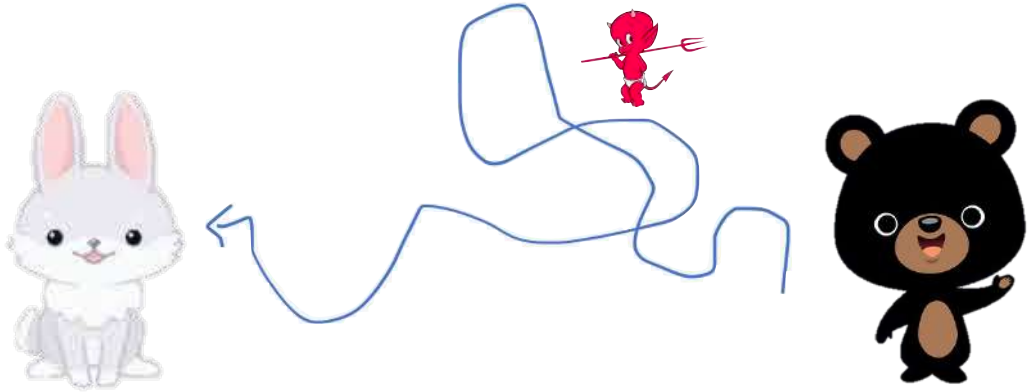


Arbitrarily delayed by adversary

Synchronous communication

Guaranteed to be delivered within one round

Asynchronous communication



Arbitrarily delayed by adversary

Honest parties never know whether…

- message was never sent, or
- It was delayed

Broadcast-Optimal Two Round MPC
with Asynchronous Peer-to-Peer Rounds

first round \ Second round	asynchronous P2P	BC
asynchronous P2P	impossible with standard definitions of security	
BC		well-studied

Broadcast-Optimal Two Round MPC with Asynchronous Peer-to-Peer Rounds

Second round

first round	asynchronous P2P	BC
asynchronous P2P	impossible with standard definitions of security	
BC	Impossible for n <= 2t Possible otherwise (under some conditions)	well-studied

Broadcast-Optimal Two Round MPC with Asynchronous Peer-to-Peer Rounds

Second round

first round	asynchronous P2P	BC
asynchronous P2P	impossible with standard definitions of security	Impossible with classical notion of asynchrony We introduce a new variant!
BC	Impossible for n <= 2t Possible otherwise (under some conditions)	well-studied

Broadcast-Optimal Two Round MPC
with Asynchronous Peer-to-Peer Rounds

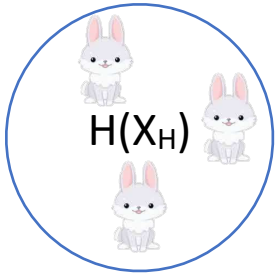
Second round

first round	asynchronous P2P	BC
asynchronous P2P	impossible with standard definitions of security	Impossible with classical notion of asynchrony We introduce a new variant!
BC	Impossible for n <= 2t Possible otherwise (under some conditions)	well-studied

Impossibility of asyncP2P, BC

Impossibility of asyncP2P, BC

Impossibility of asyncP2P, BC

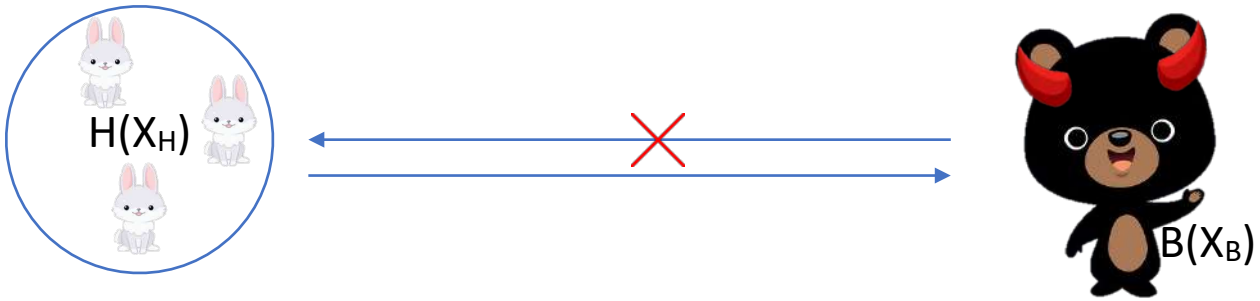


Impossibility of asyncP2P, BC

round 1: asyncP2P

round 2: BC

Impossibility of asyncP2P, BC

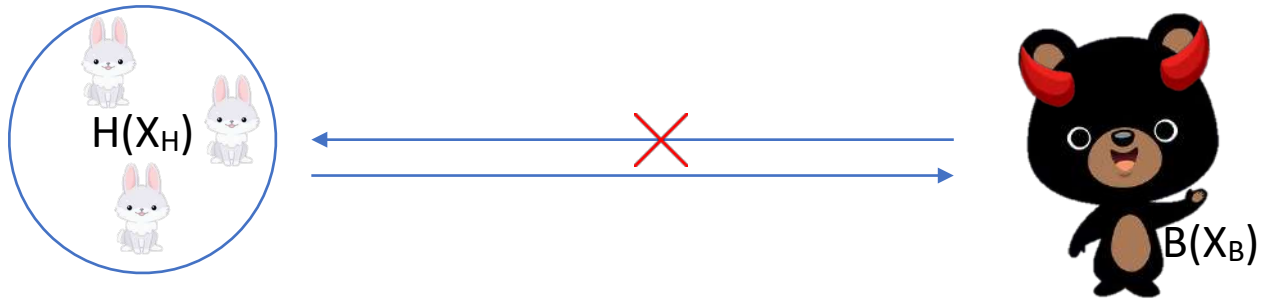


round 1: asyncP2P

round 2: BC

- Nothing H says depends on X_B

Impossibility of asyncP2P, BC

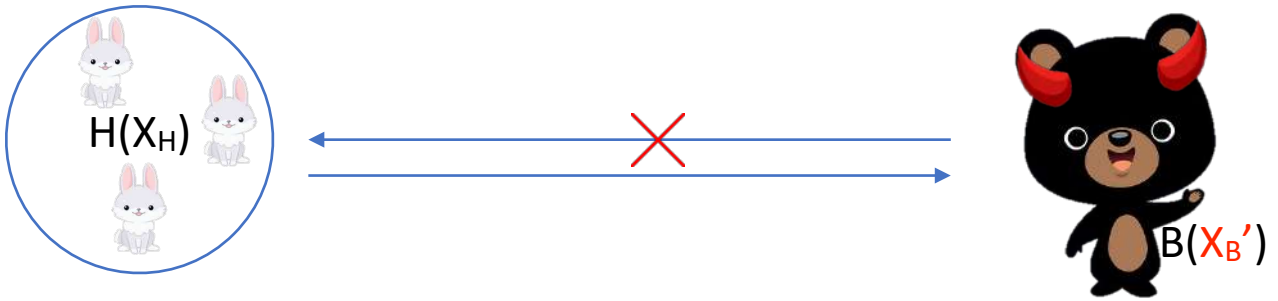


round 1: asyncP2P

round 2: BC

Impossibility of asyncP2P, BC

- Nothing H says depends on X_B
- … so B can swap out X_B *after the computation*!

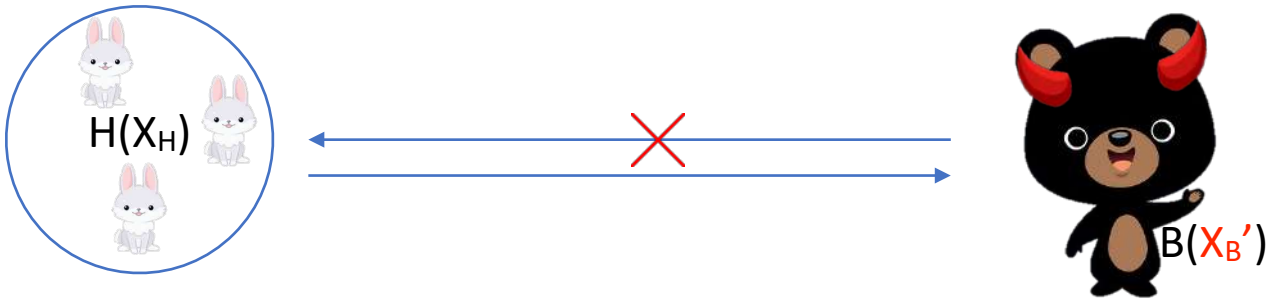


round 1: asyncP2P

round 2: BC

Impossibility of asyncP2P, BC

- Nothing H says depends on X_B
- … so B can swap out X_B *after the computation*!



round 1: asyncP2P

round 2: BC

(t_d,t_m)-asynchrony

(t_d,t_m)-asynchrony

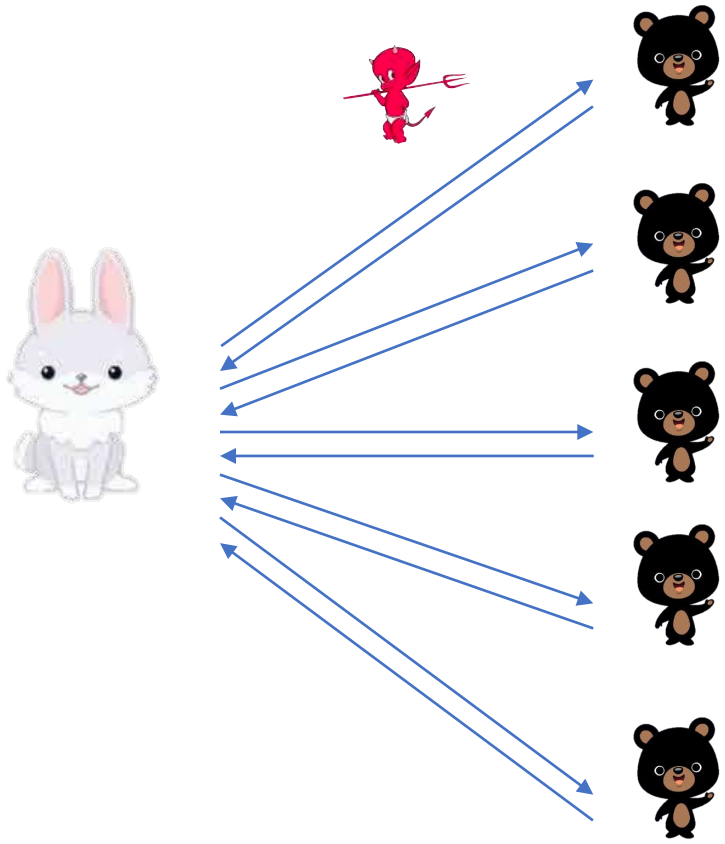
deafness threshold

muteness threshold

(t_d,t_m)-asynchrony

deafness threshold

muteness threshold

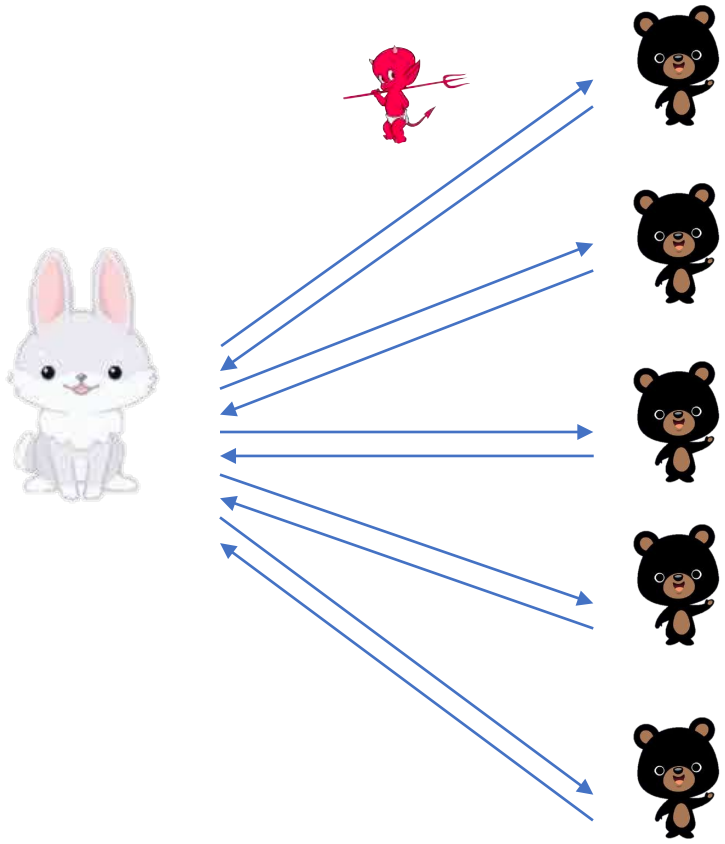


(t_d,t_m)-asynchrony

deafness threshold

muteness threshold

- $t_d = 2$

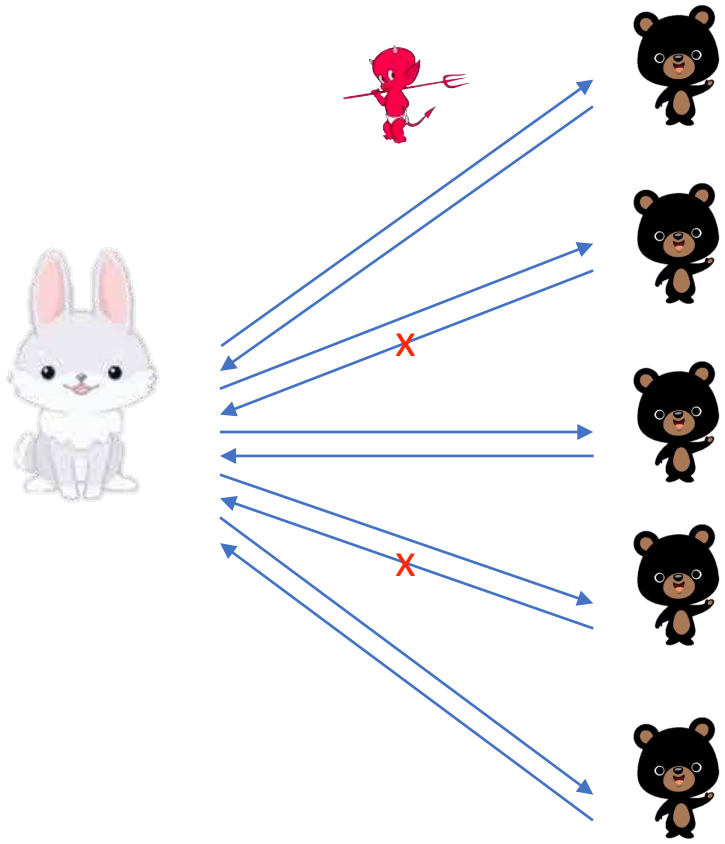


(t_d,t_m)-asynchrony

deafness threshold

muteness threshold

- $t_d = 2$

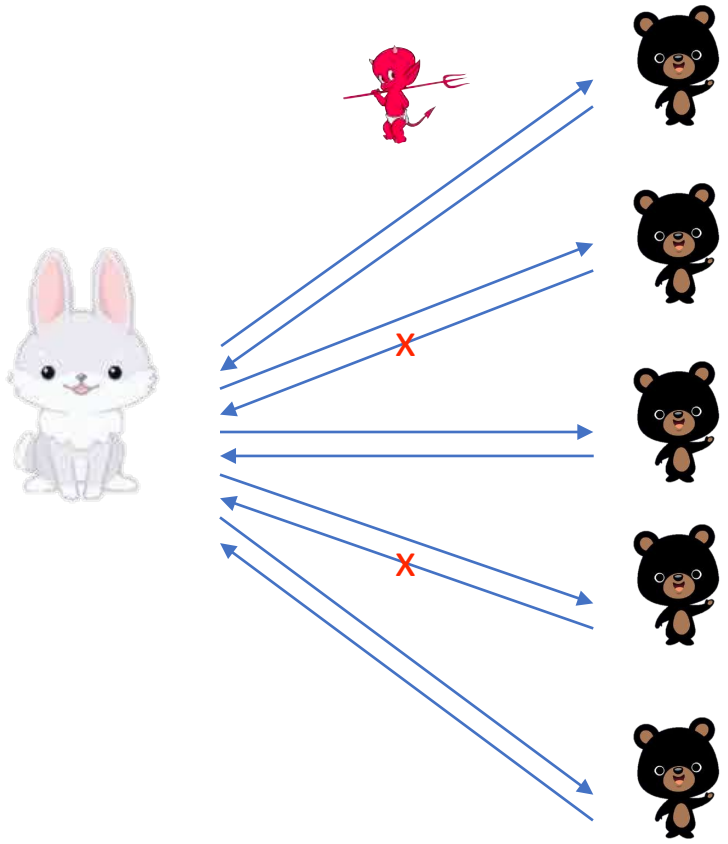


(t_d,t_m)-asynchrony

deafness threshold

muteness threshold

- $t_d = 2$
- $t_m = 1$

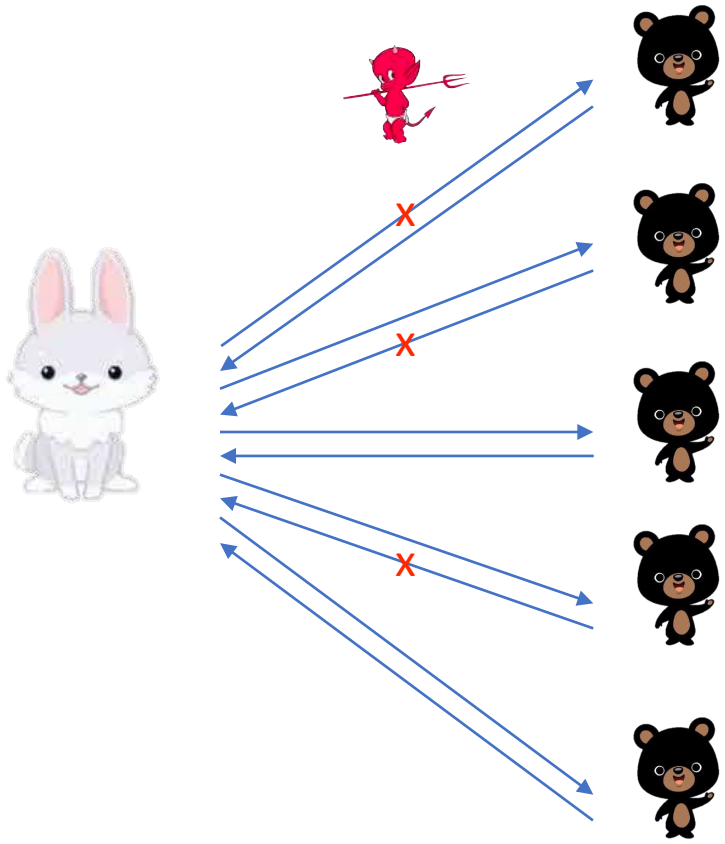


(t_d,t_m)-asynchrony

deafness threshold

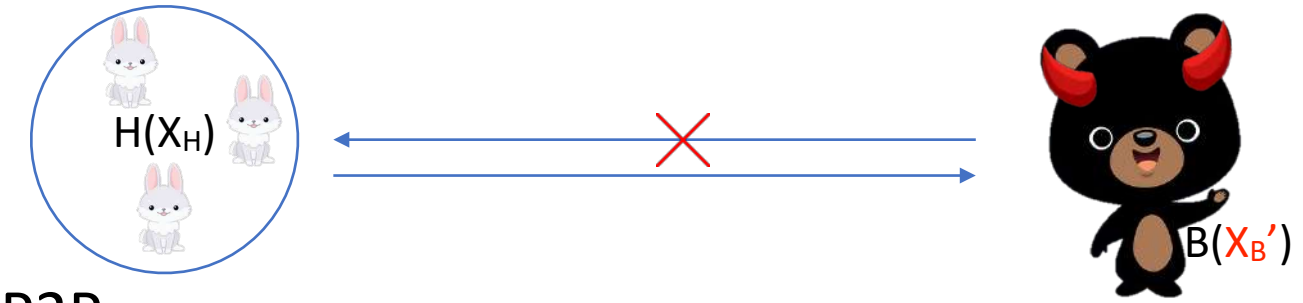
muteness threshold

- $t_d = 2$
- $t_m = 1$



(t_d,t_m)-asyncP2P, BC

with PKI

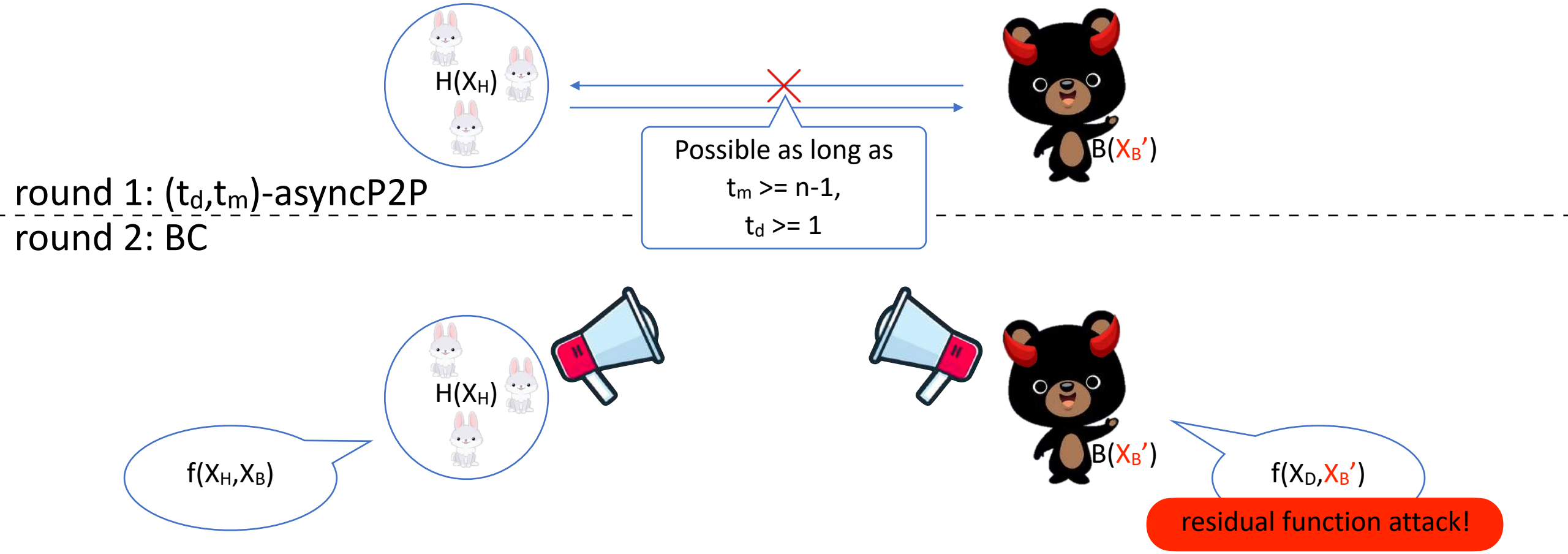


round 1: (t_d,t_m)-asyncP2P

round 2: BC

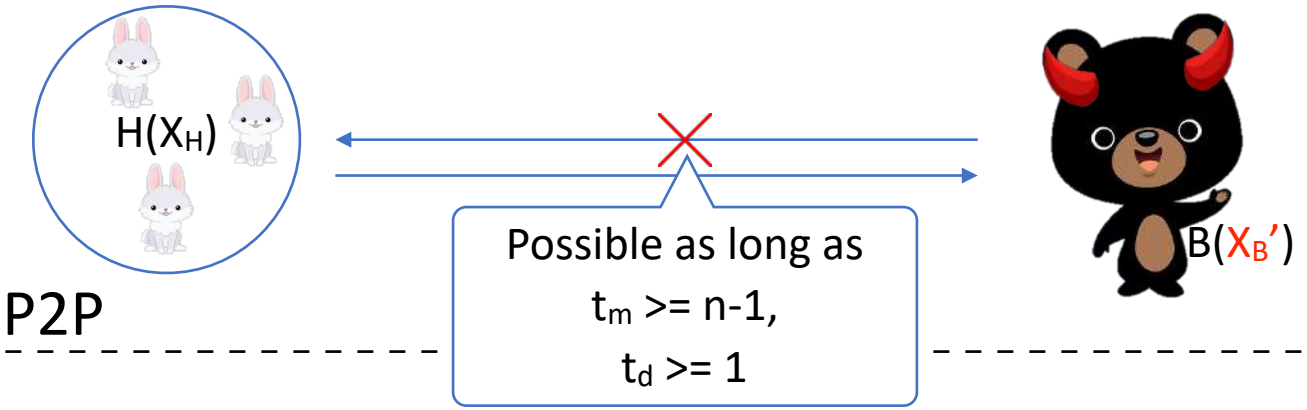
(t_d,t_m)-asyncP2P, BC

with PKI



(t_d,t_m)-asyncP2P, BC

with PKI

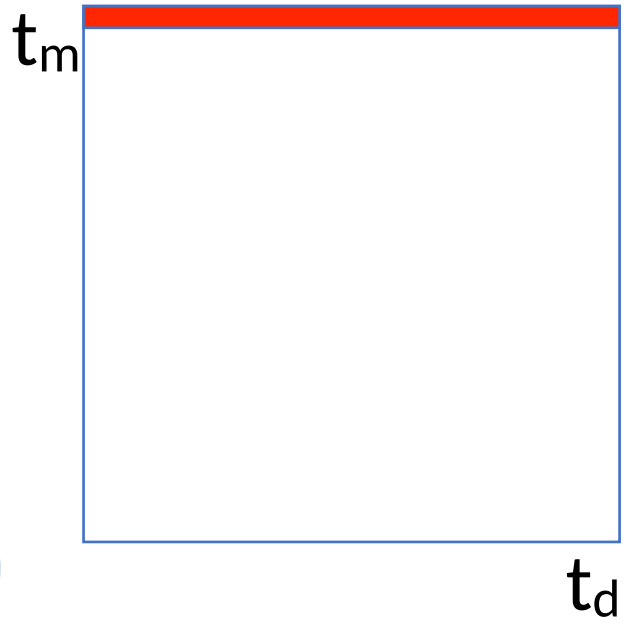


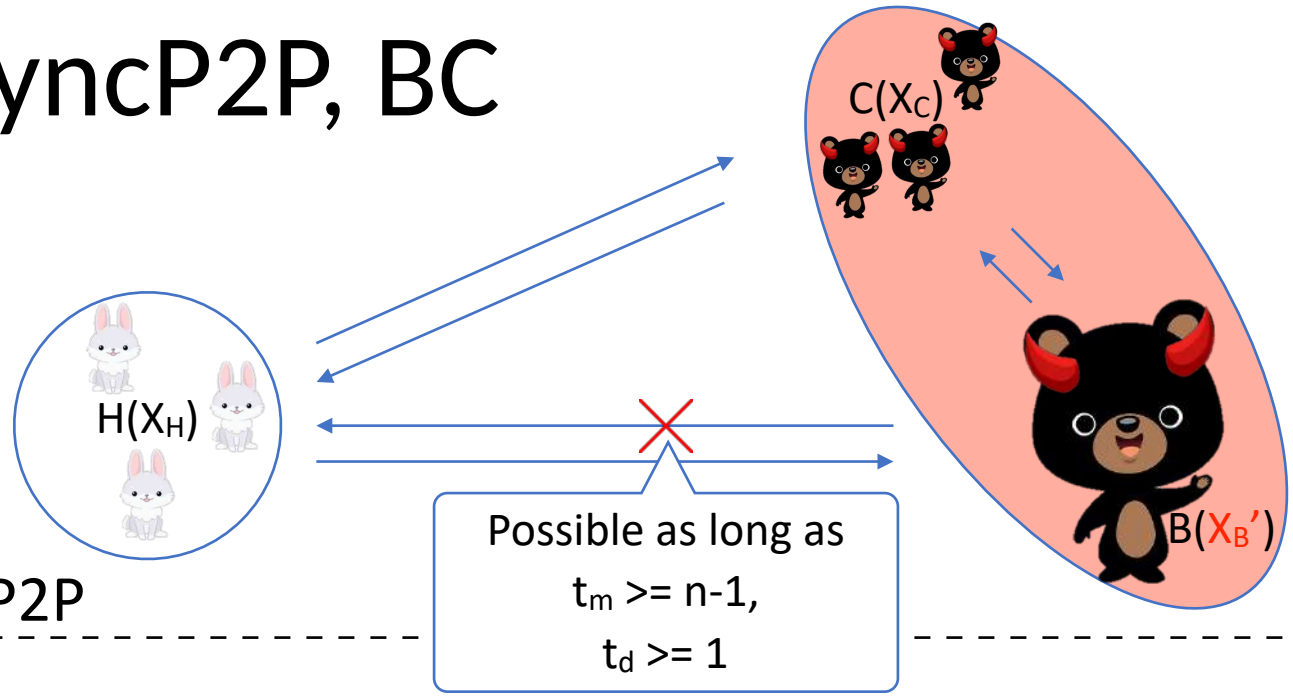
round 1: (t_d,t_m)-asyncP2P

round 2: BC

(t_d,t_m)-asyncP2P, BC

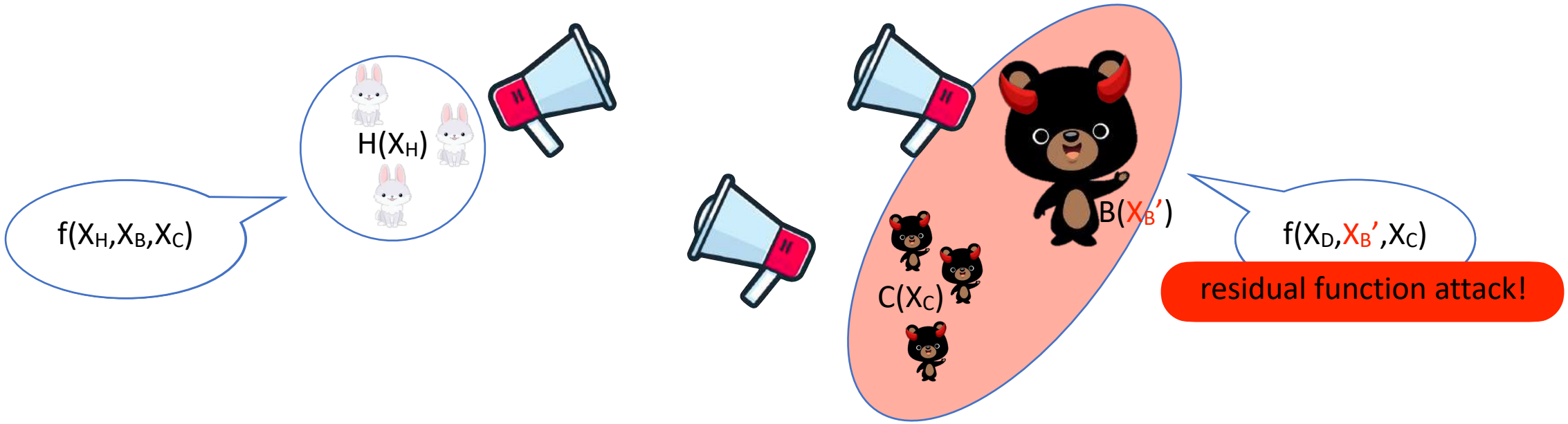
with PKI





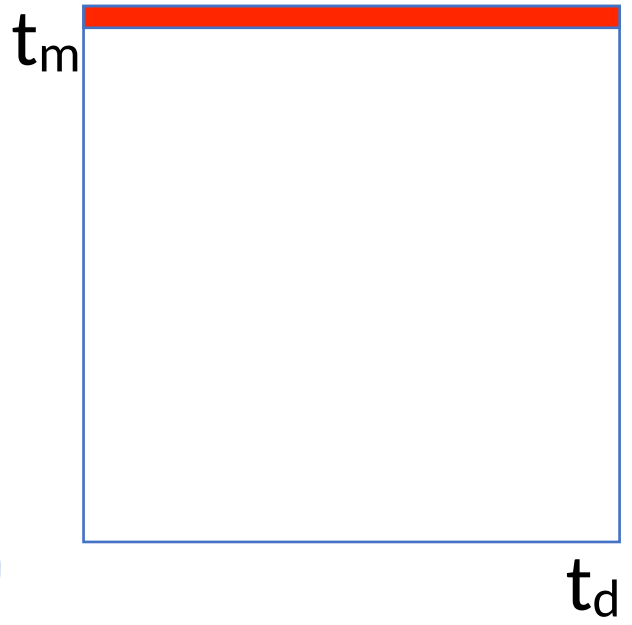
round 1: (t_d,t_m)-asyncP2P

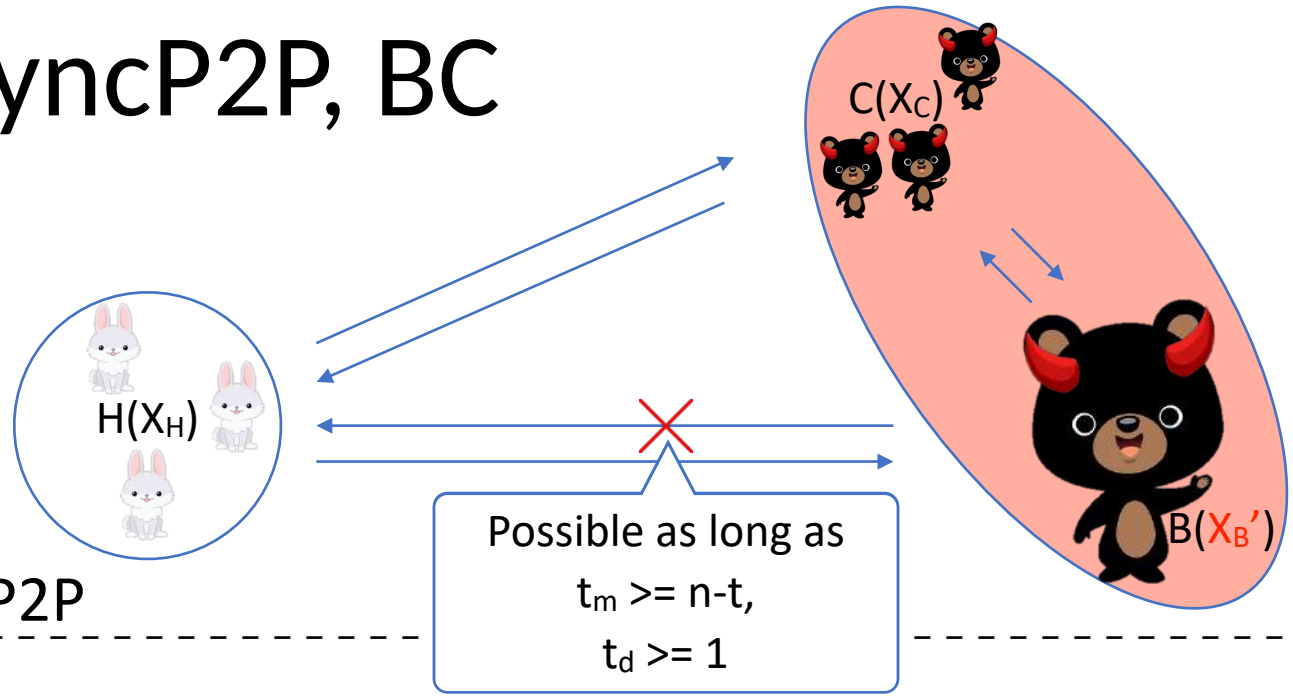
round 2: BC



(t_d,t_m)-asyncP2P, BC

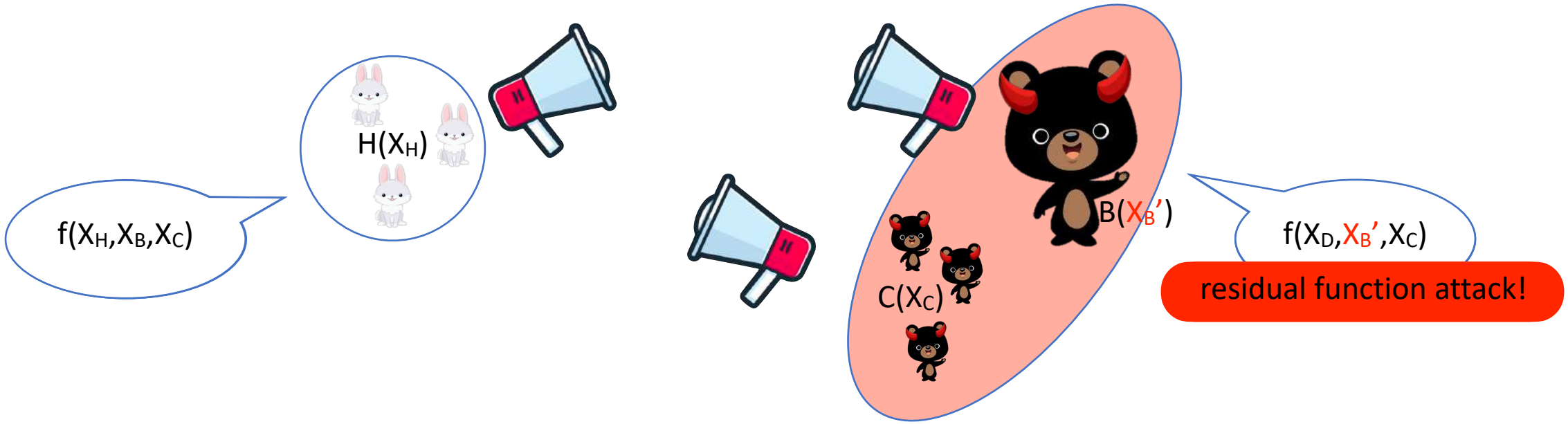
with PKI





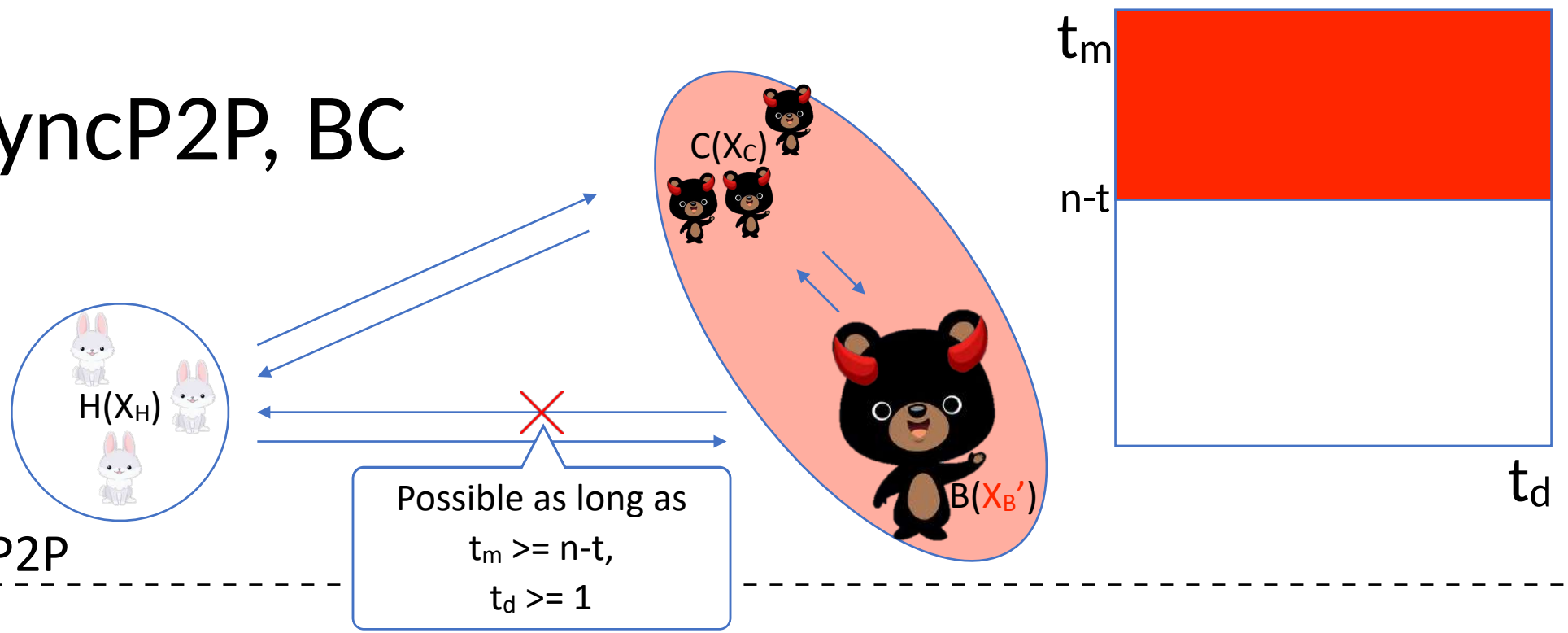
round 1: (t_d,t_m)-asyncP2P

round 2: BC



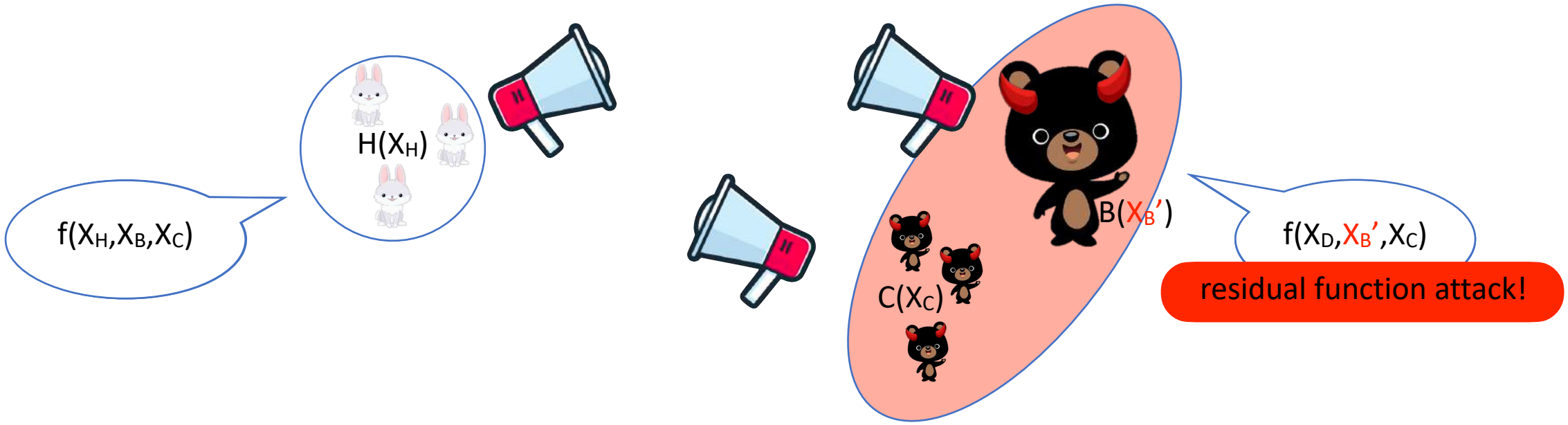
(t_d,t_m)-asyncP2P, BC

with PKI



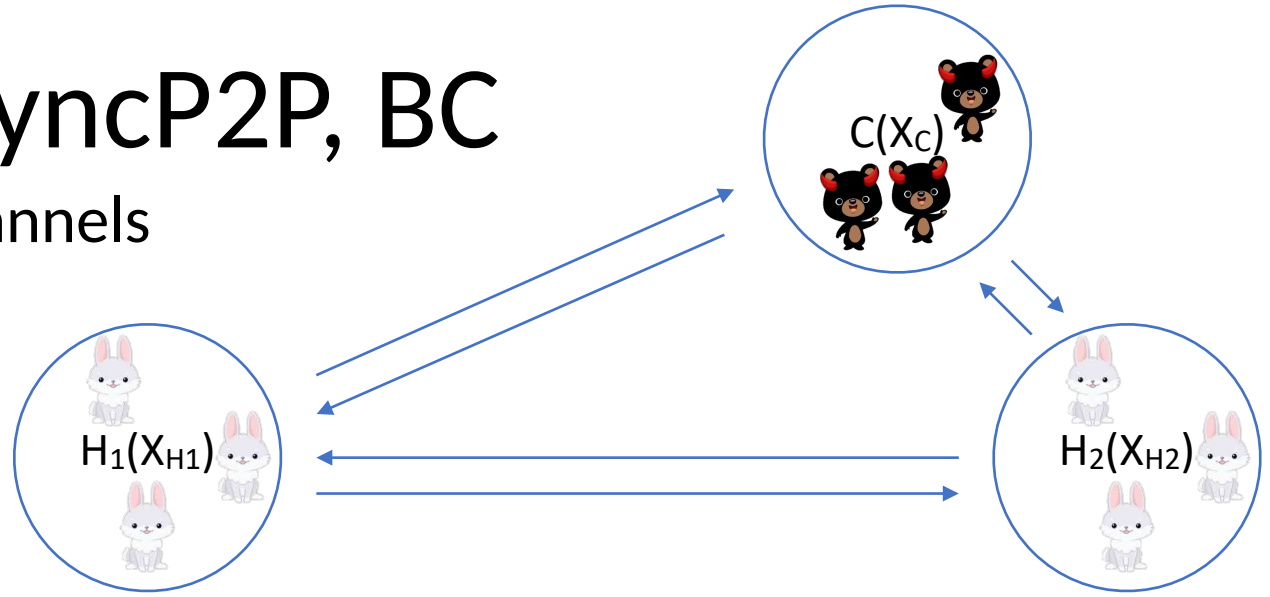
round 1: (t_d,t_m)-asyncP2P

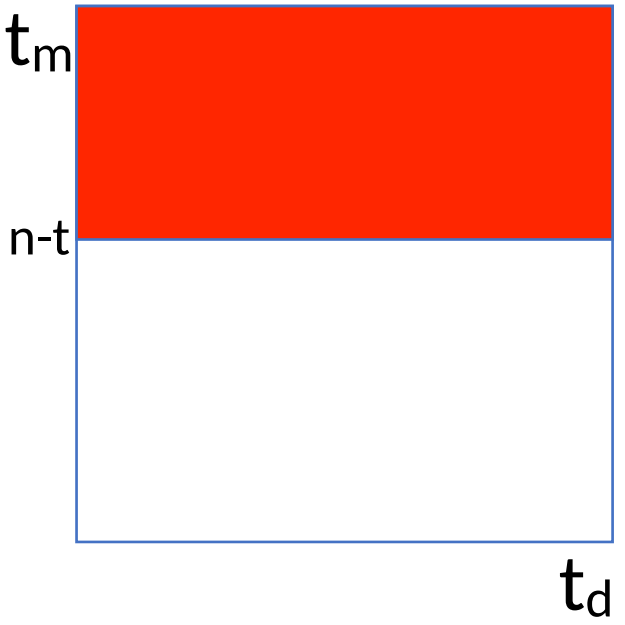
round 2: BC



(t_d,t_m)-asyncP2P, BC

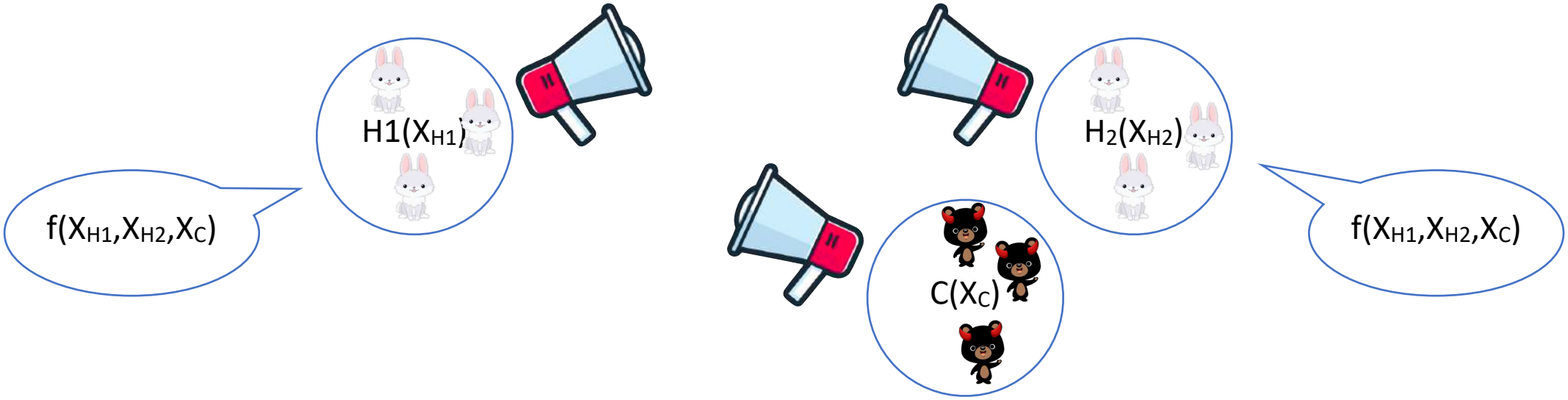
with private channels





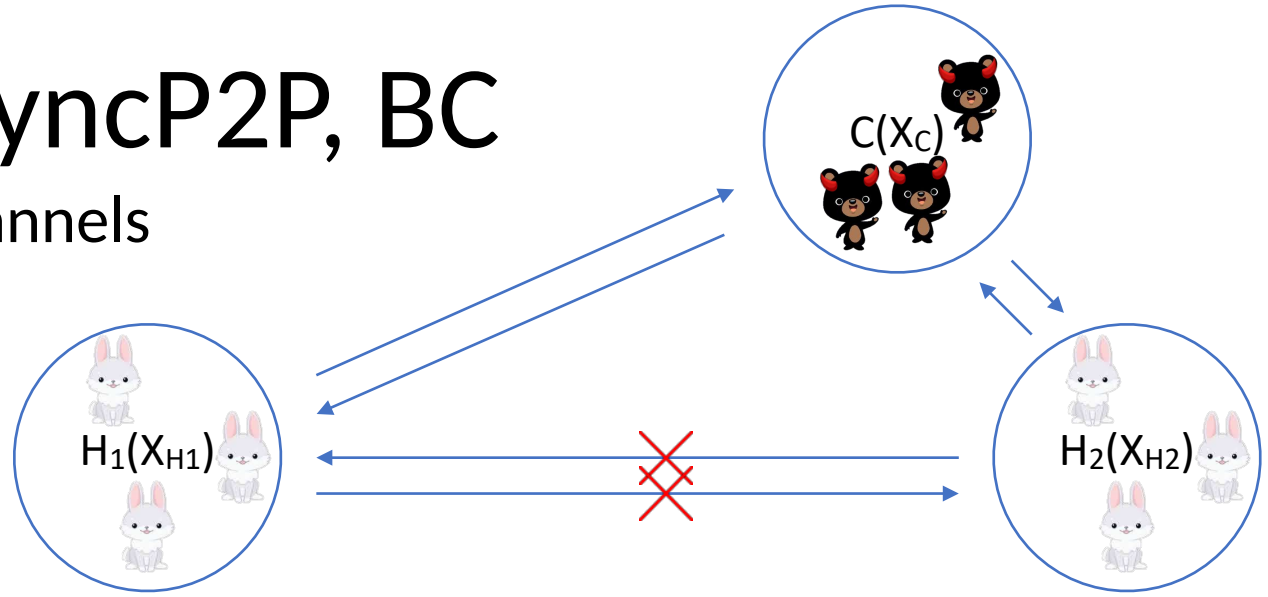
round 1: (t_d,t_m)-asyncP2P

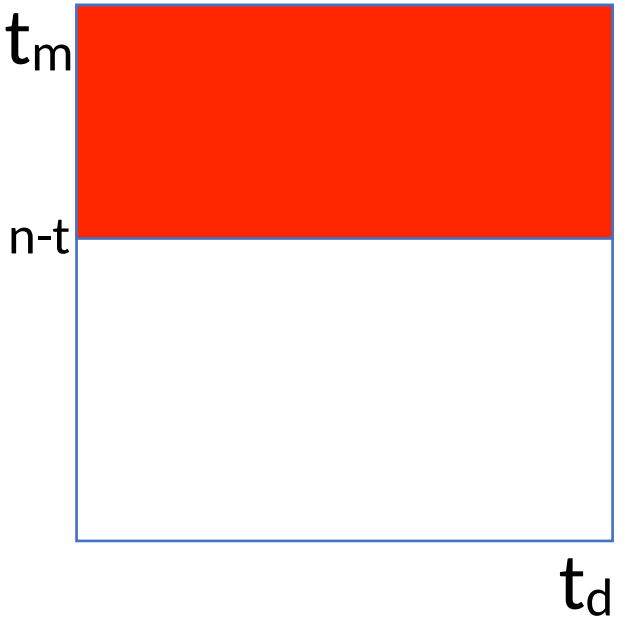
round 2: BC



(t_d,t_m)-asyncP2P, BC

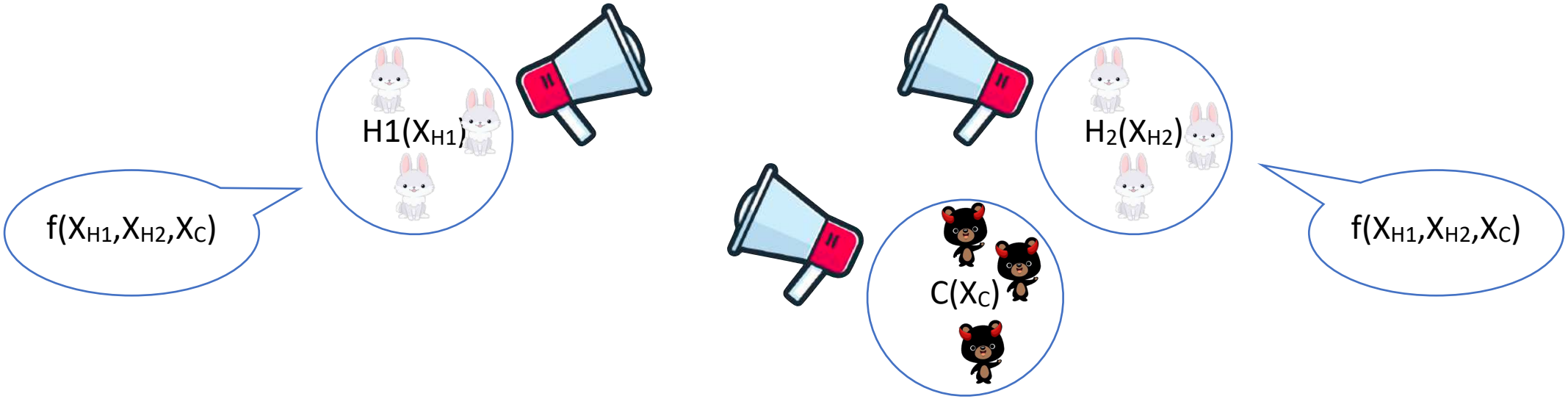
with private channels





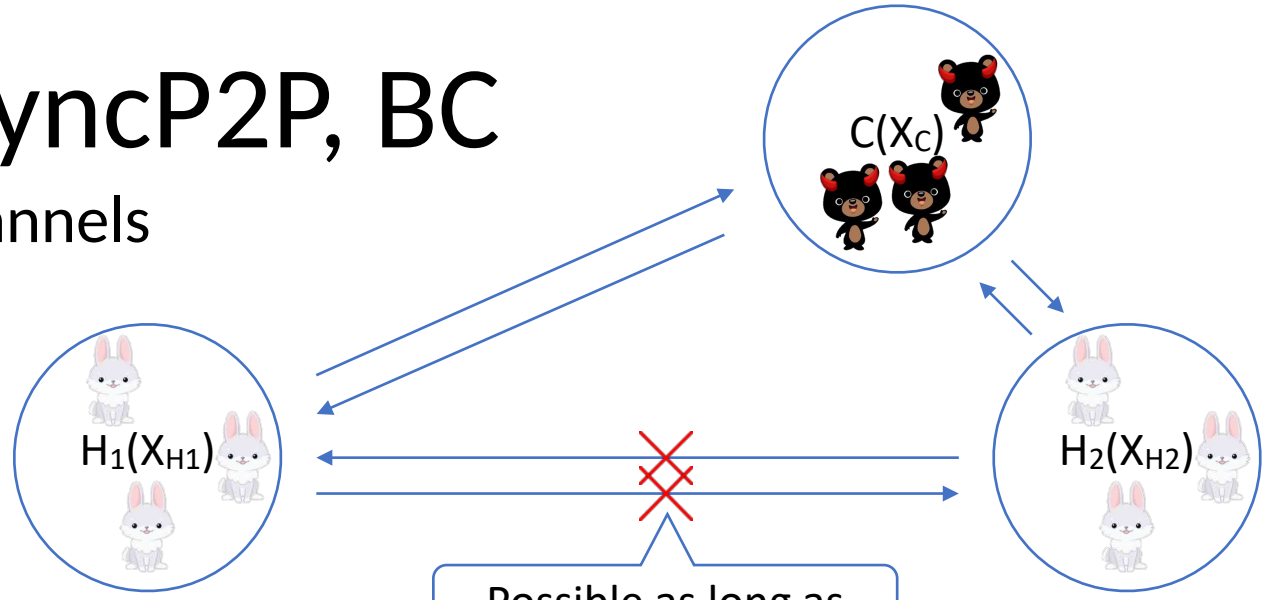
round 1: (t_d,t_m)-asyncP2P

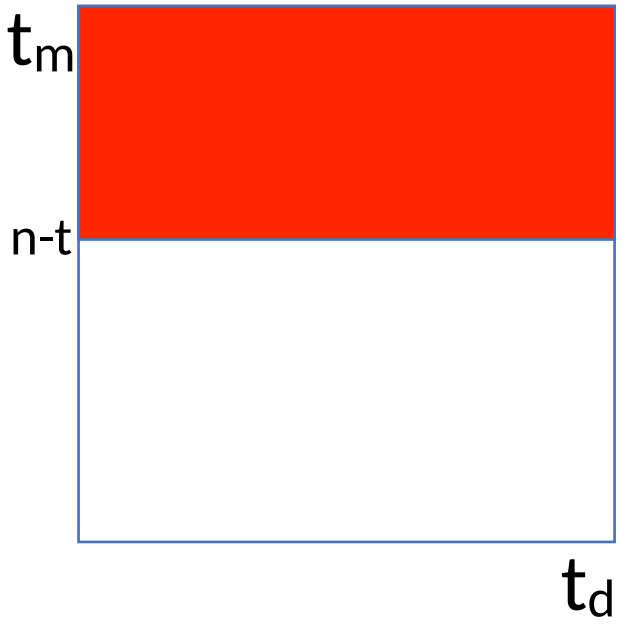
round 2: BC



(t_d,t_m)-asyncP2P, BC

with private channels

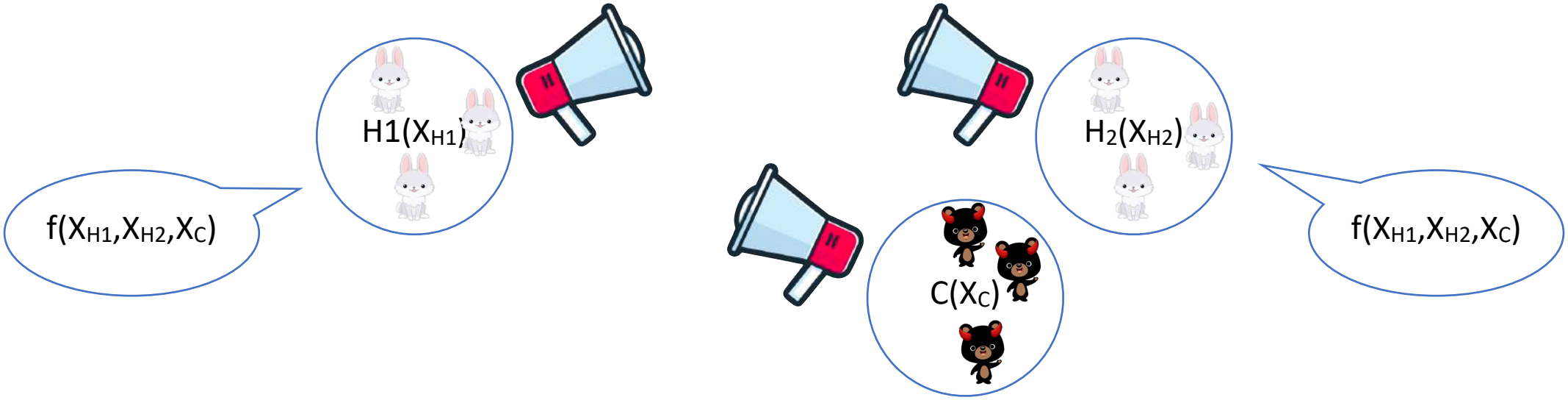




Possible as long as
$t_m >= (n-t)/2$,
$t_d >= (n-t)/2$

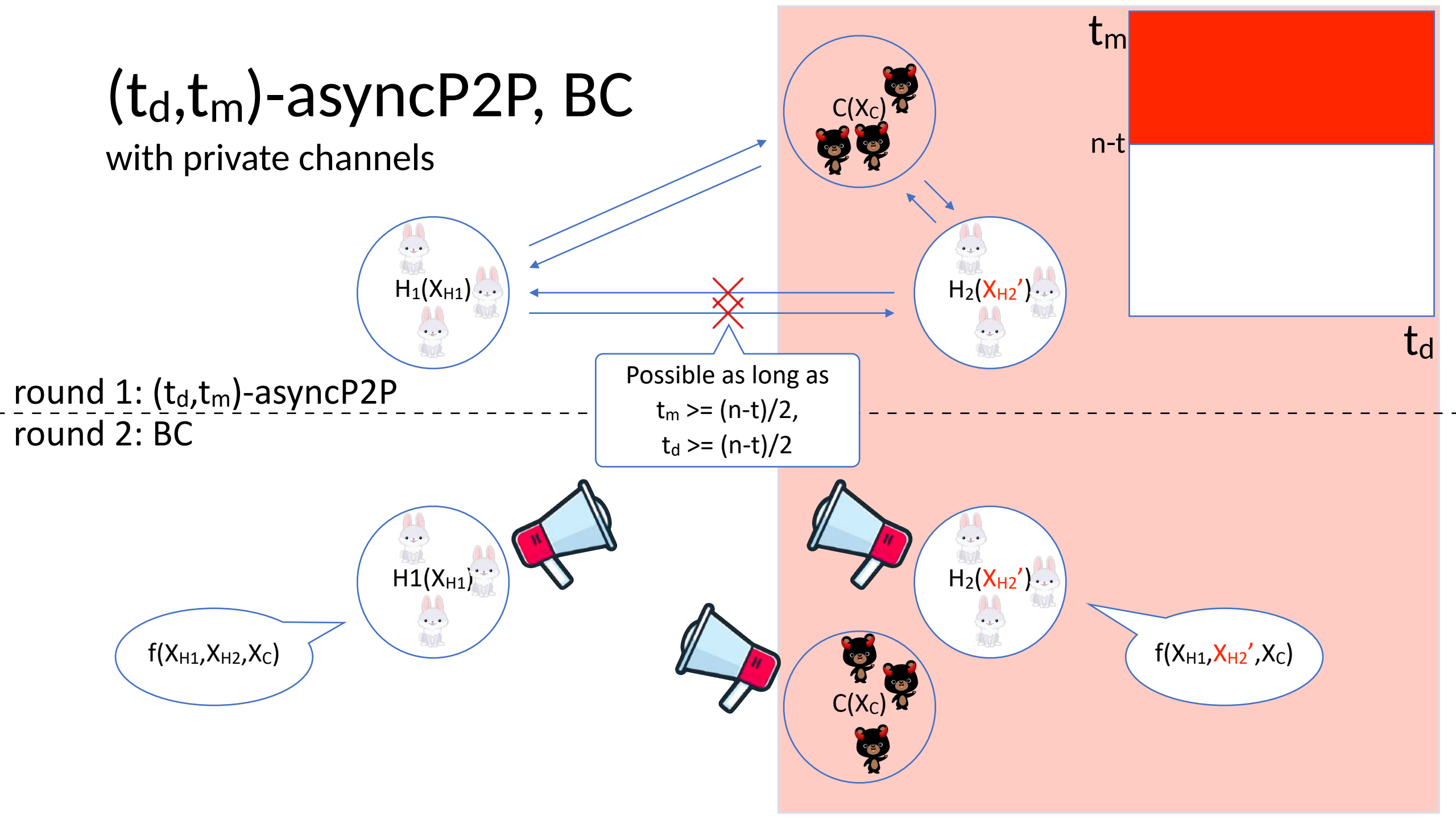
round 1: (t_d,t_m)-asyncP2P

round 2: BC



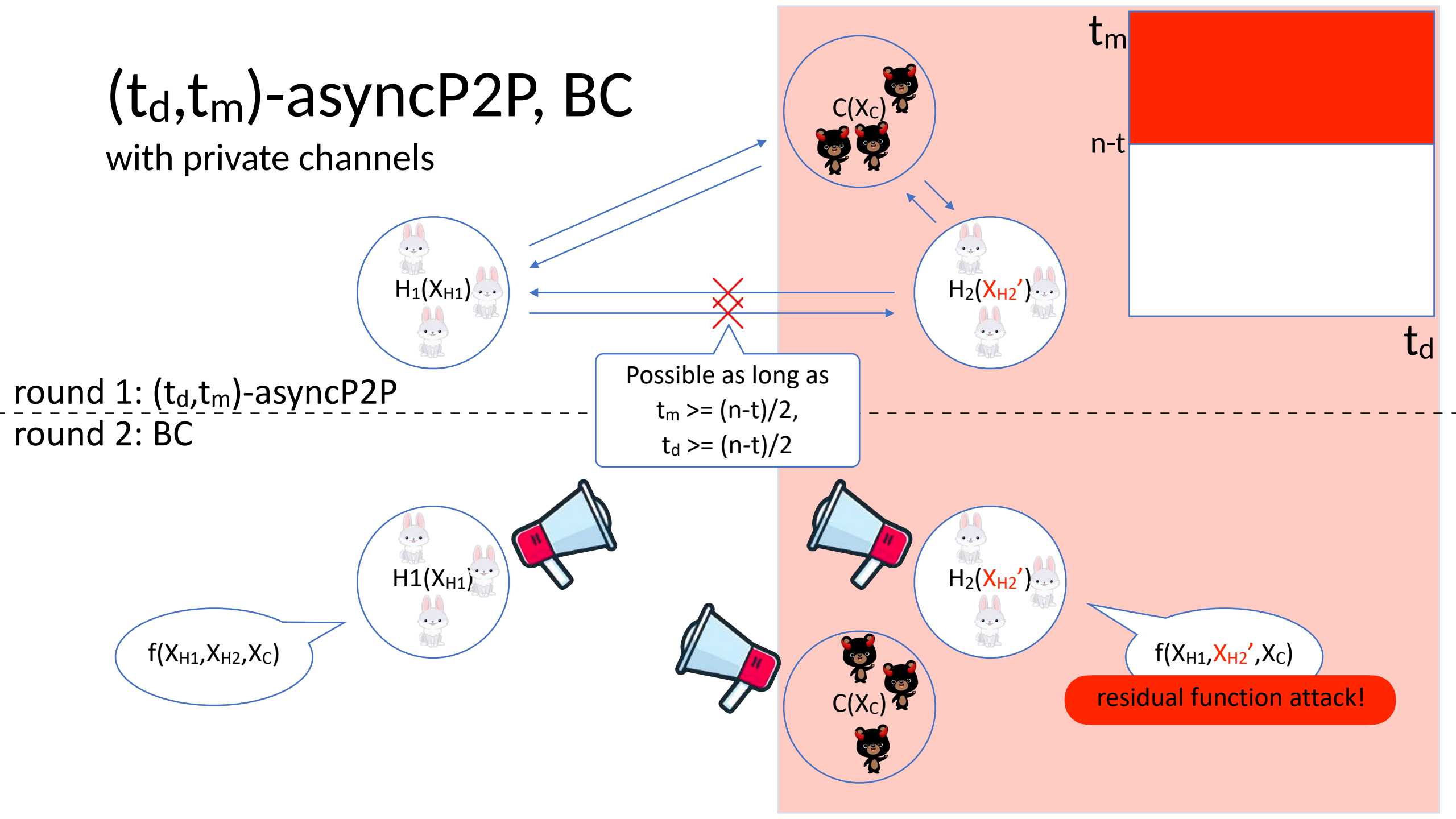
(t_d,t_m)-asyncP2P, BC

with private channels



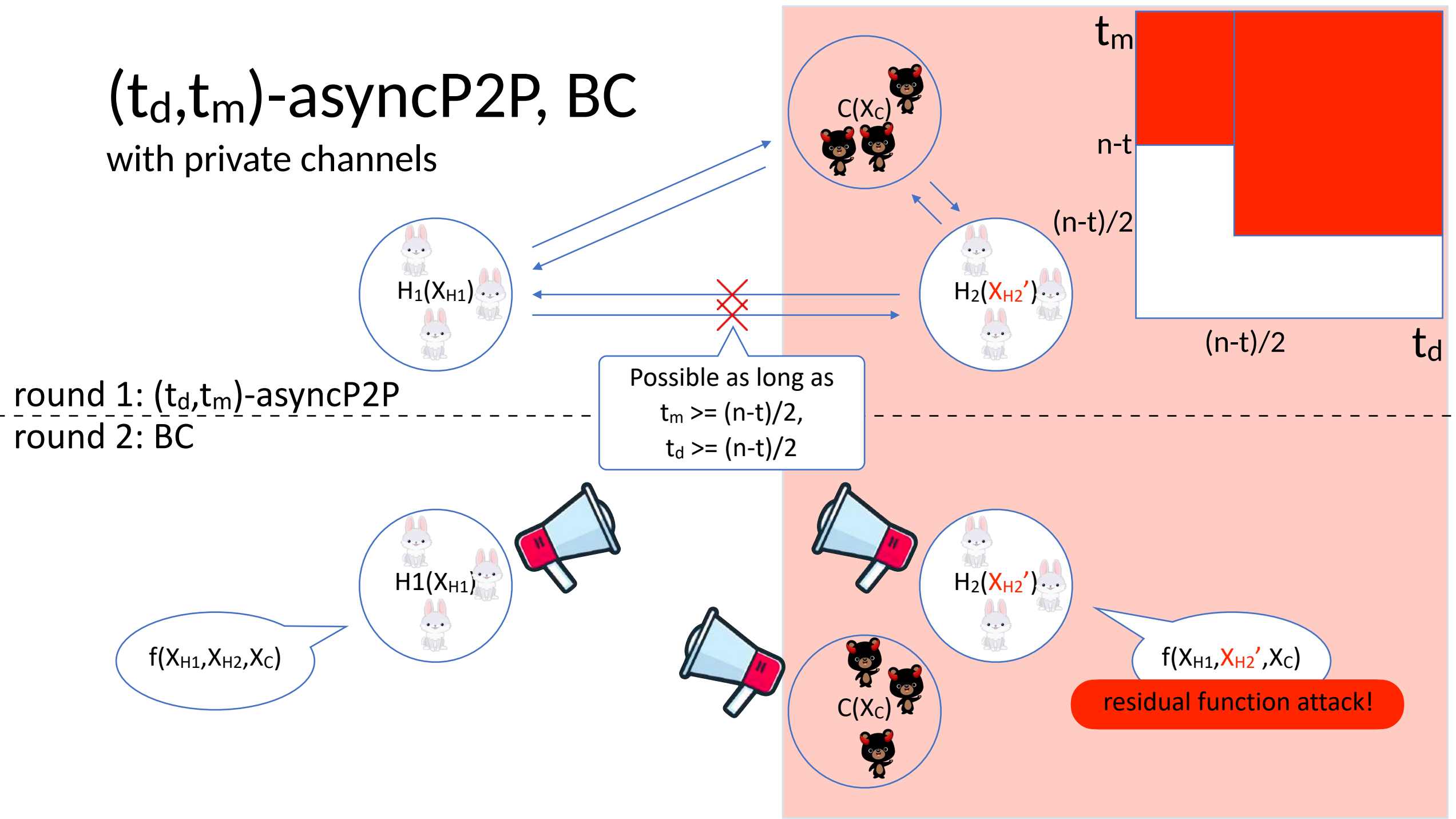
(t_d,t_m)-asyncP2P, BC

with private channels

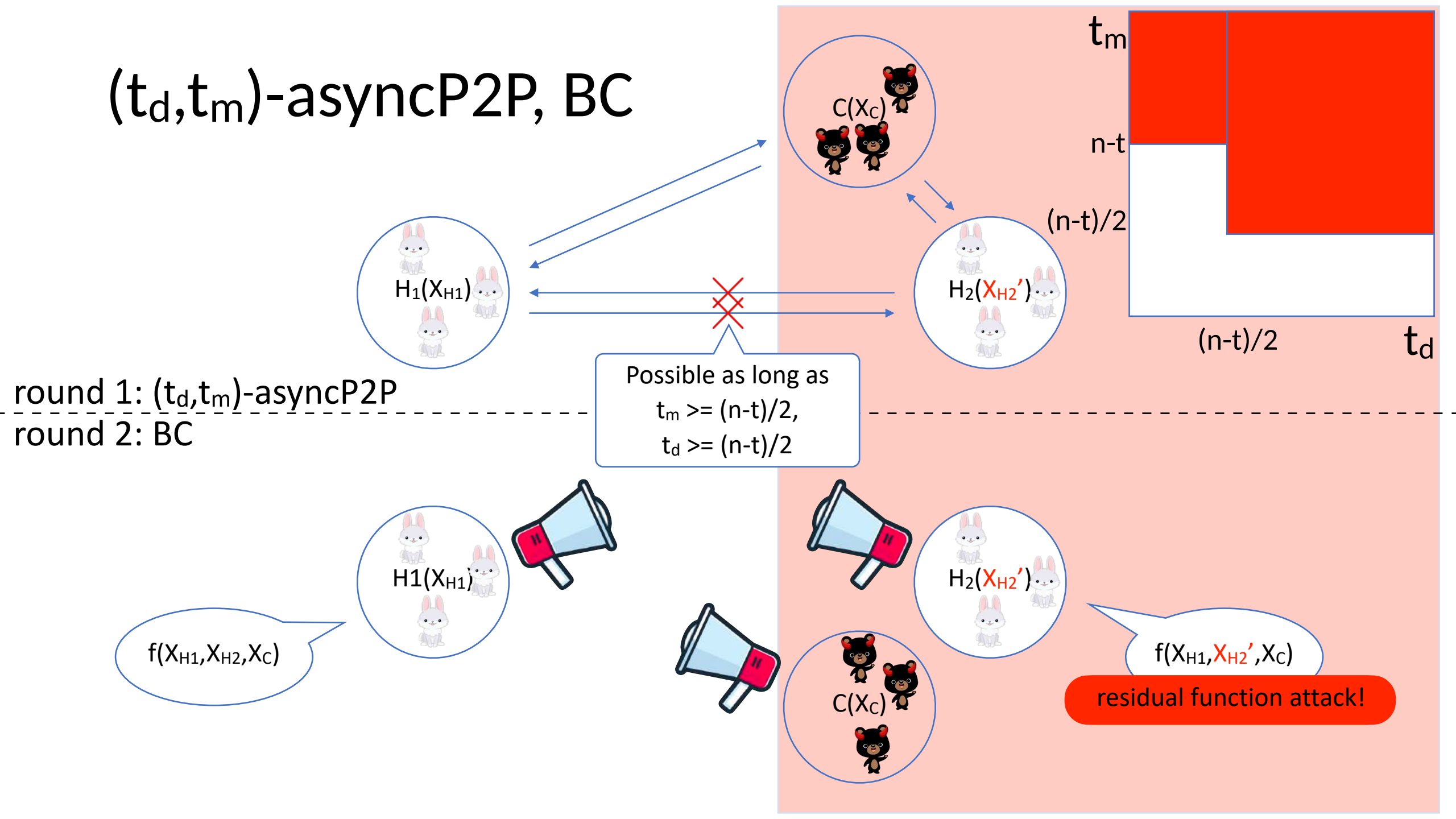


(t_d,t_m)-asyncP2P, BC

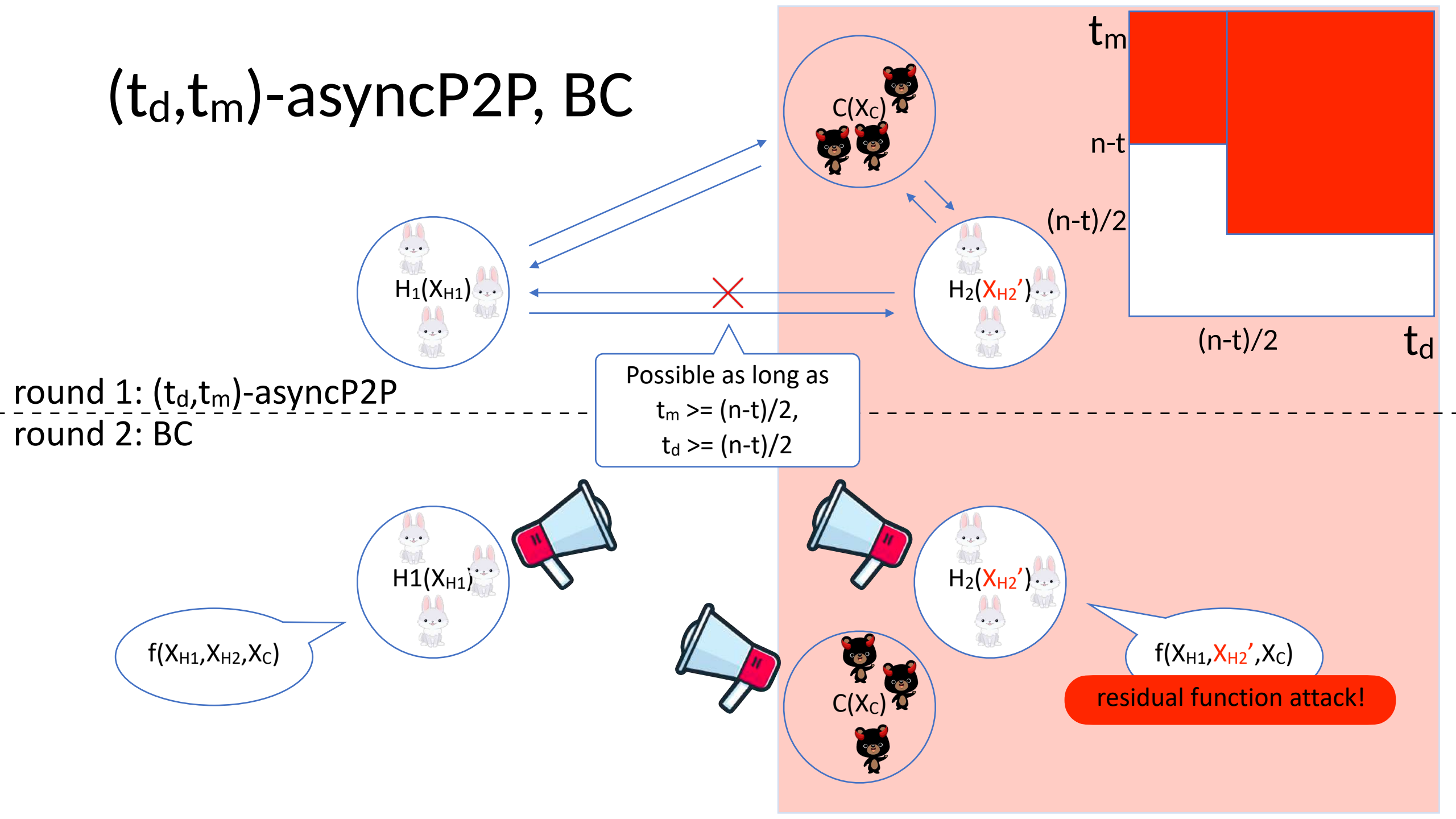
with private channels



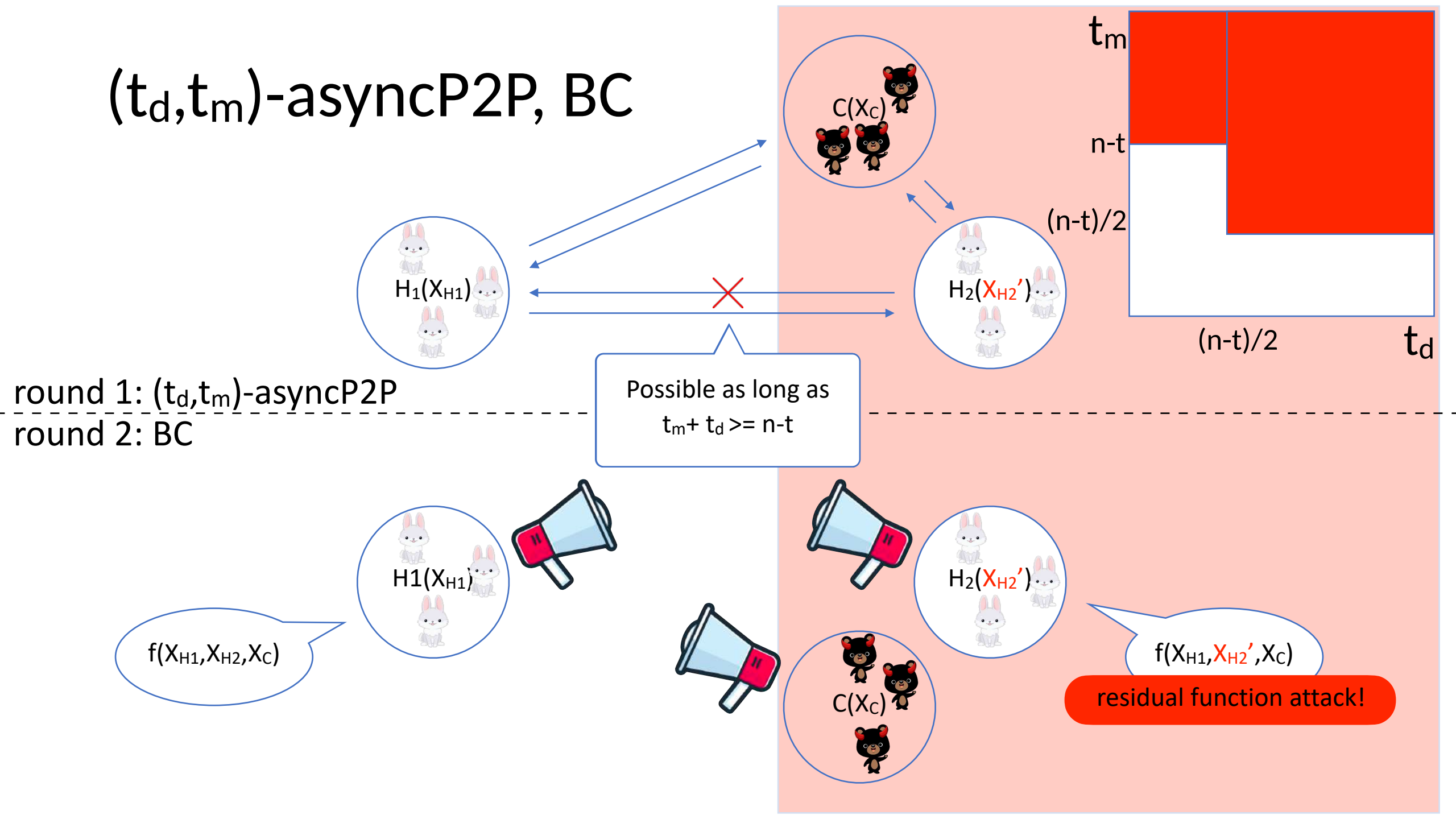
(t_d,t_m)-asyncP2P, BC



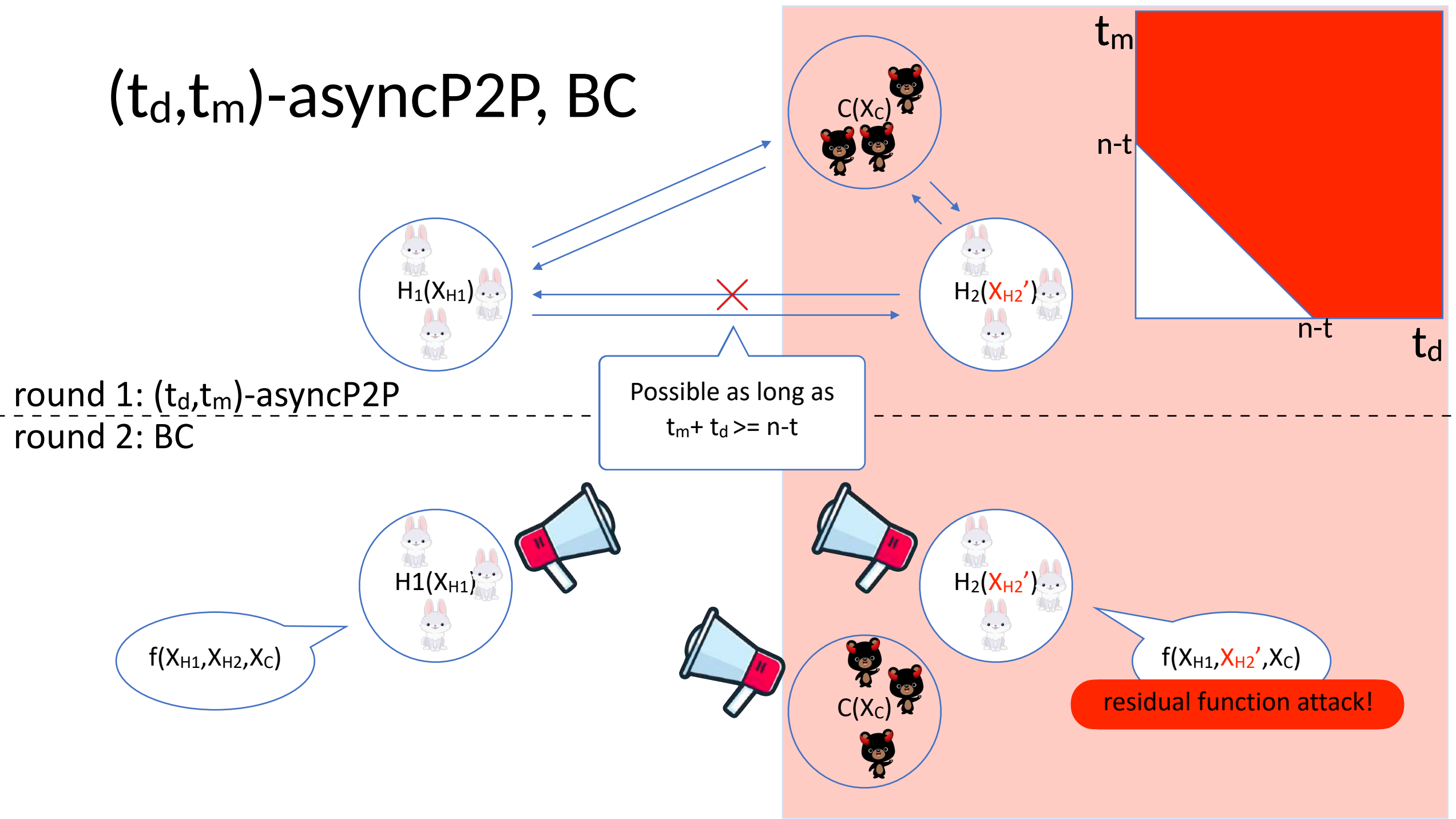
(t_d,t_m)-asyncP2P, BC



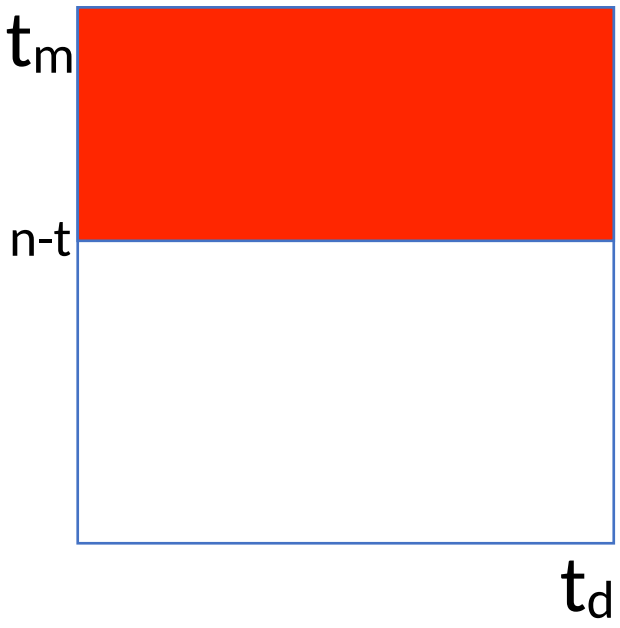
(t_d,t_m)-asyncP2P, BC



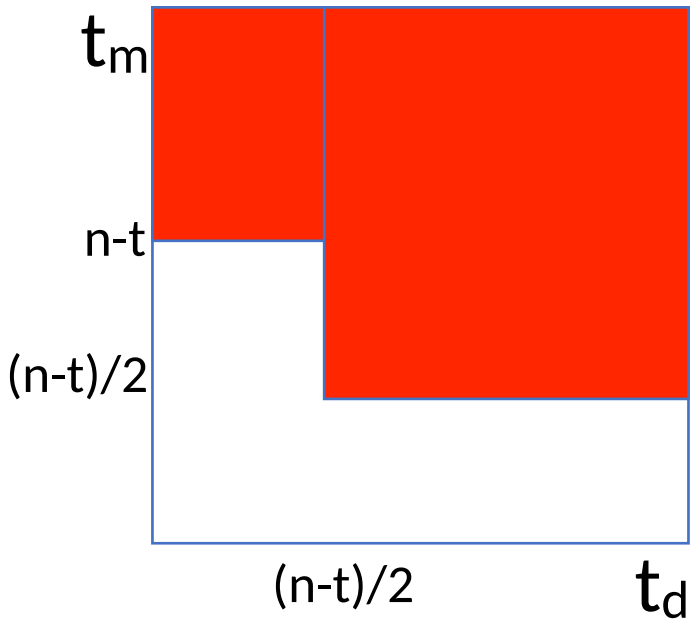
(t_d,t_m)-asyncP2P, BC



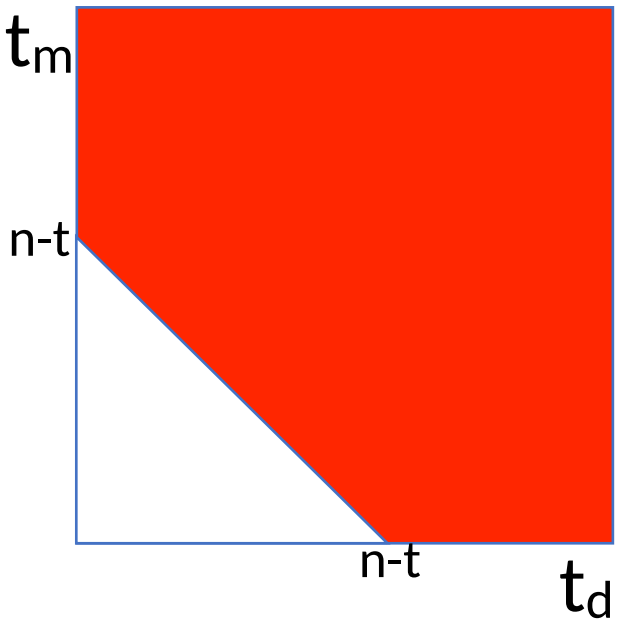
(t_d,t_m)-asyncP2P, BC



with PKI

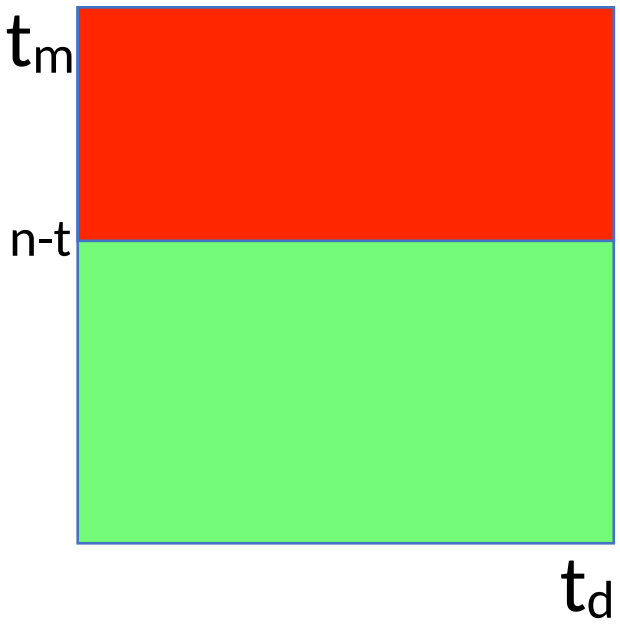


with private channels

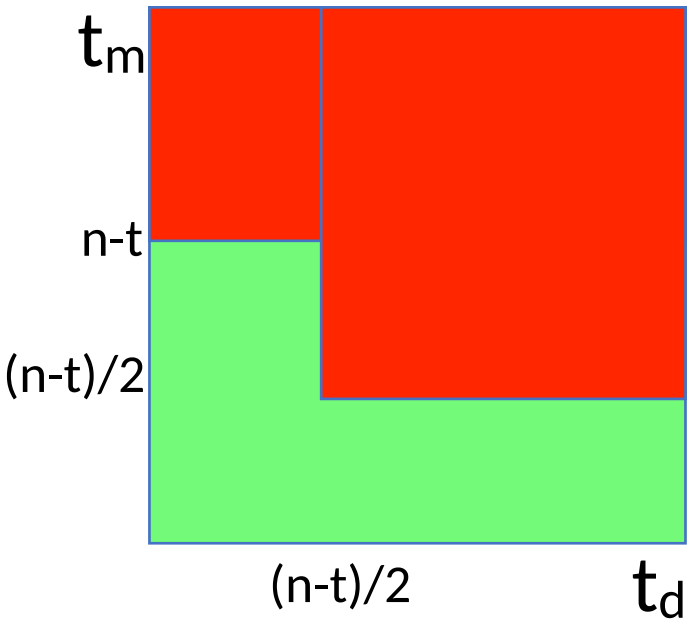


no PKI or private channels

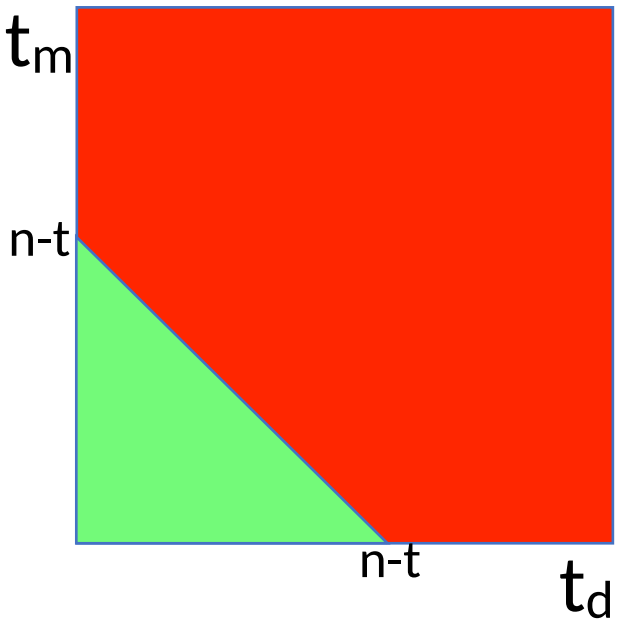
(t_d,t_m)-asyncP2P, BC



with PKI

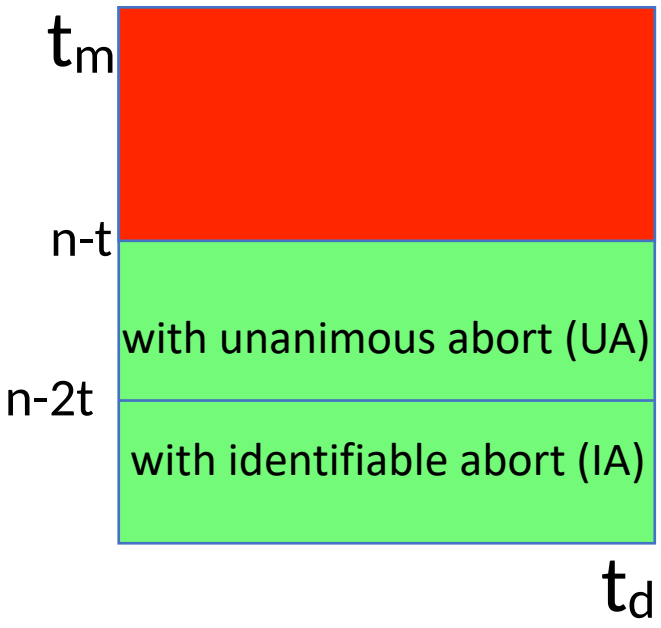


with private channels

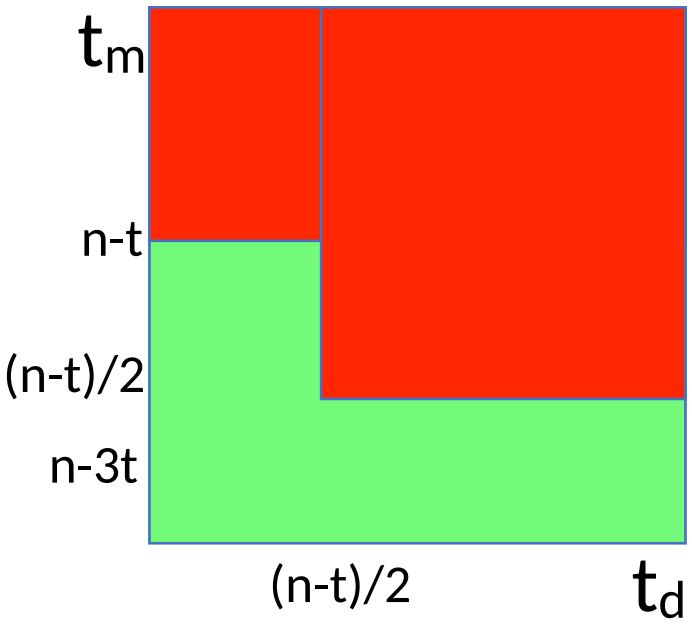


no PKI or private channels

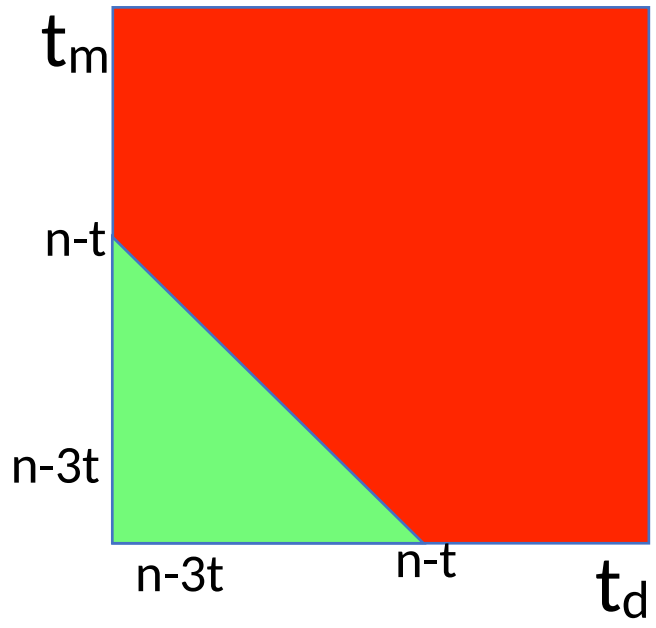
(t_d,t_m)-asyncP2P, BC



with PKI

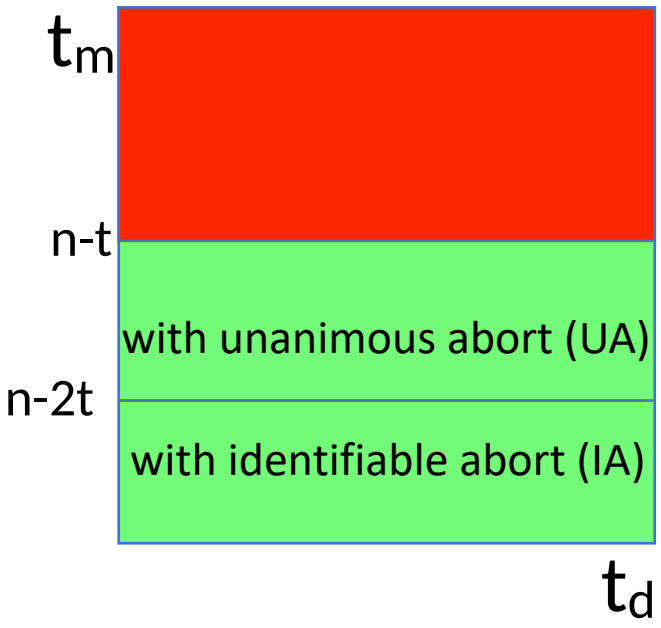


with private channels

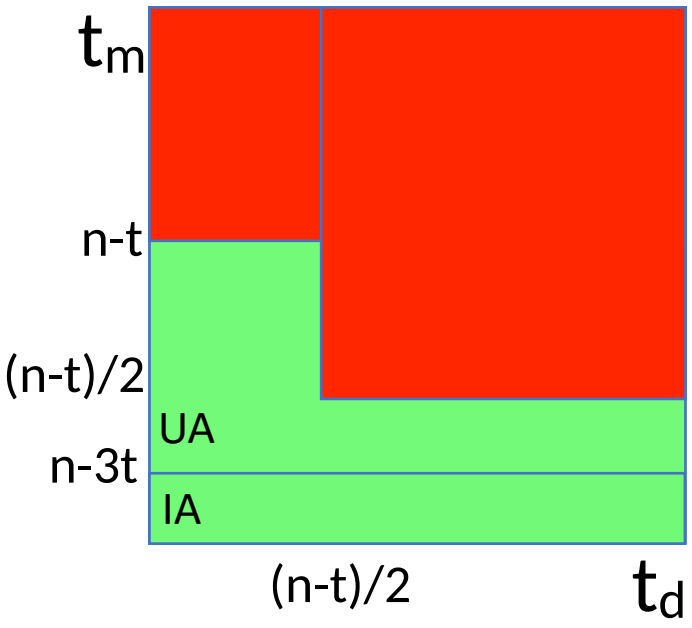


no PKI or private channels

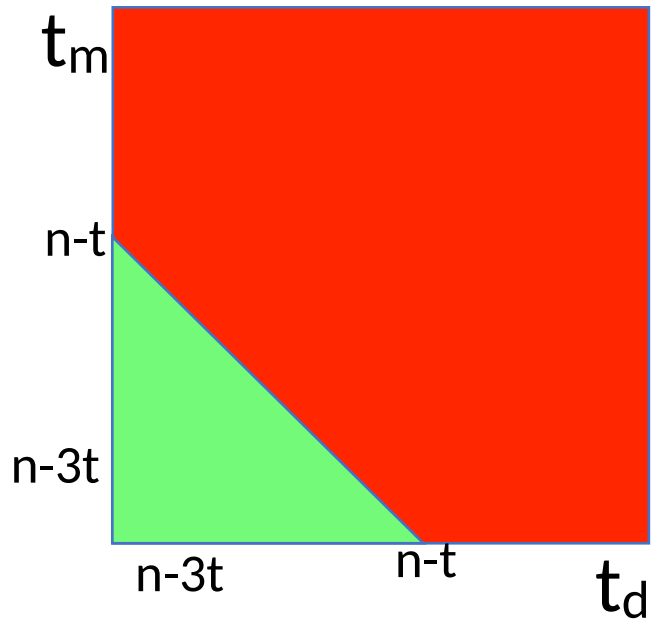
(t_d,t_m)-asyncP2P, BC



with PKI

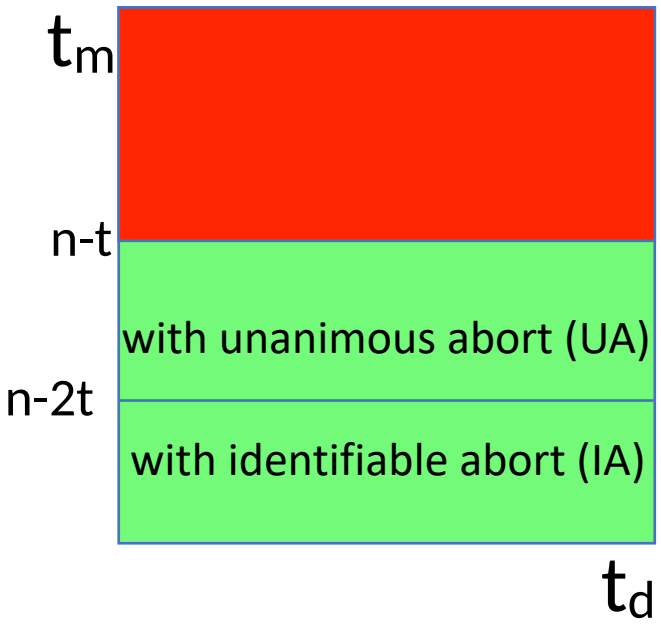


with private channels

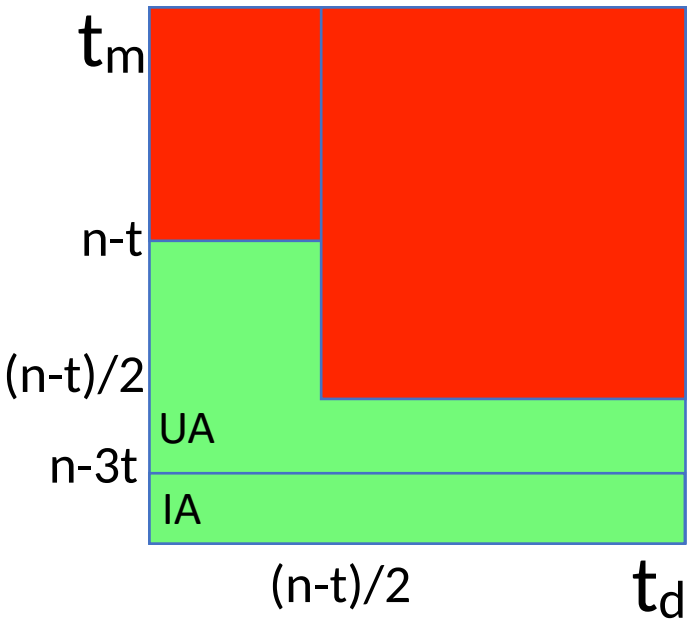


no PKI or private channels

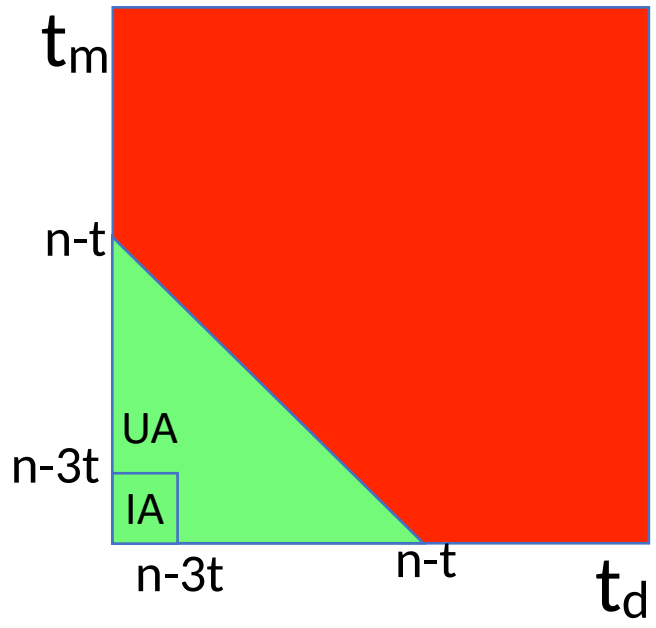
(t_d,t_m)-asyncP2P, BC



with PKI



with private channels



no PKI or private channels

(t_d,t_m)-asyncP2P, BC: Constructions

- Using tools from previous papers
  - Variants of one-or-nothing secret sharing
  - Do not support all values of t_d,t_m
- New constructions from indistinguishability obfuscation
  - New primitive: puncturable sender-public key encryption
  - Inefficient / unrealistic building blocks

Summary

- Our contributions:
  - New notion of (t_d,t_m)-asynchrony
  - Impossibility results
  - Constructions