Research on anonymous communication in German(y) 1983-1990

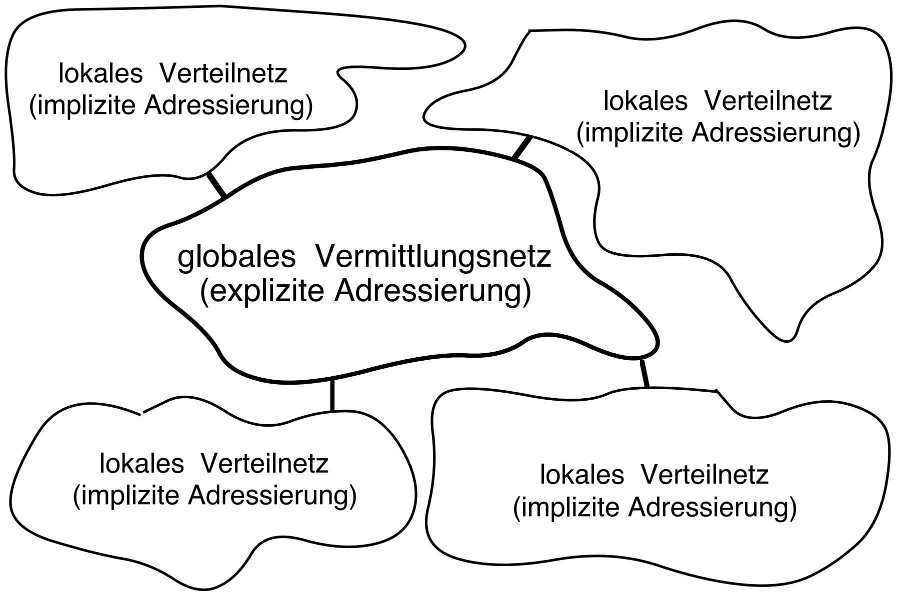
Andreas Pfitzmann
TU Dresden, Fakultät Informatik, D-01062 Dresden
Phone +49 351 463-38277, e-mail: pfitza@inf.tu-dresden.de, http://dud.inf.tu-dresden.de/

Site to download the original papers and reports:
http://dud.inf.tu-dresden.de/sireneLit.shtml

Aims of my talk

- Make historic knowledge (pre WWW, originally written mostly in German) available
- Give a tutorial on basic techniques mostly forgotten, but – in my opinion – terribly useful and terribly needed in designing today's and tomorrow's (IP v6) communication systems
- Learn from 20+ years history to re-focus PET research and development

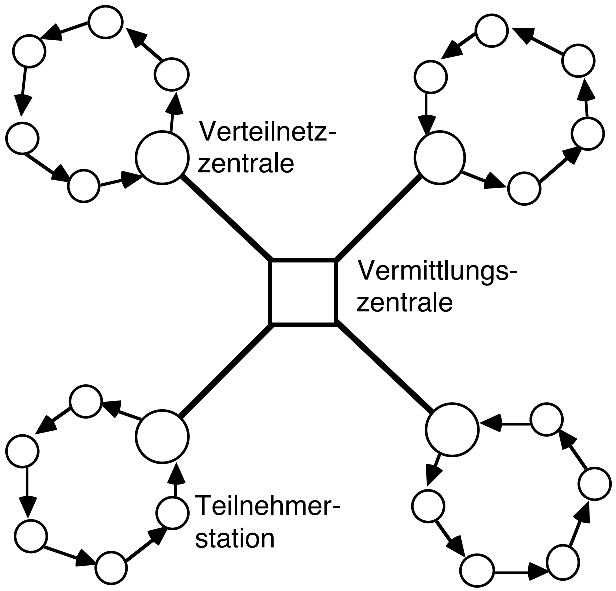
Switched/broadcast network (1983 - 1985)



Switched WAN
(possibly including MIXes)

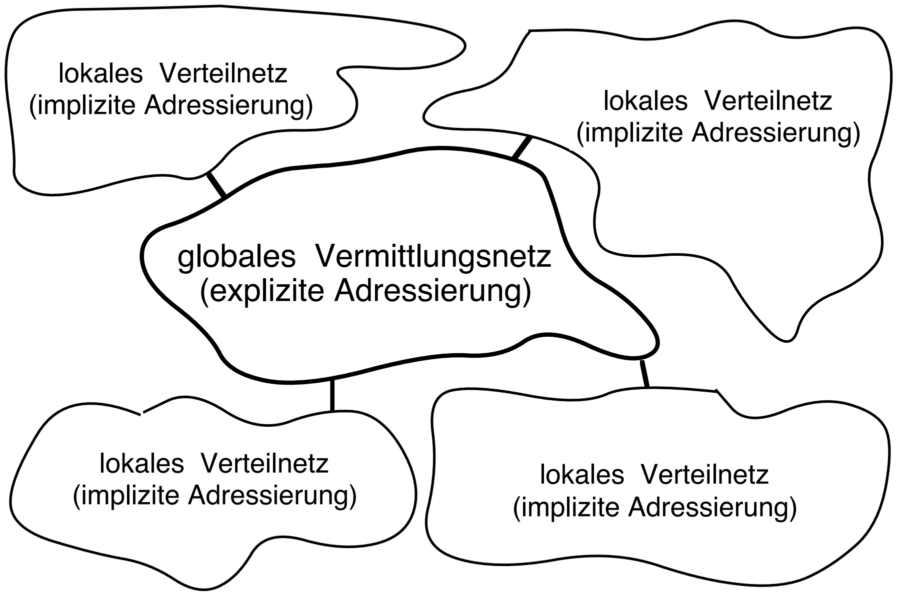
connecting

broadcast LANs
(RING-net, DC-net)



- i.e. taking anonymity and unobservability into account when building networks physically
- statically fixed structure (or dynamically adaptable subset/superset construction) is well suited to counter intersection attacks

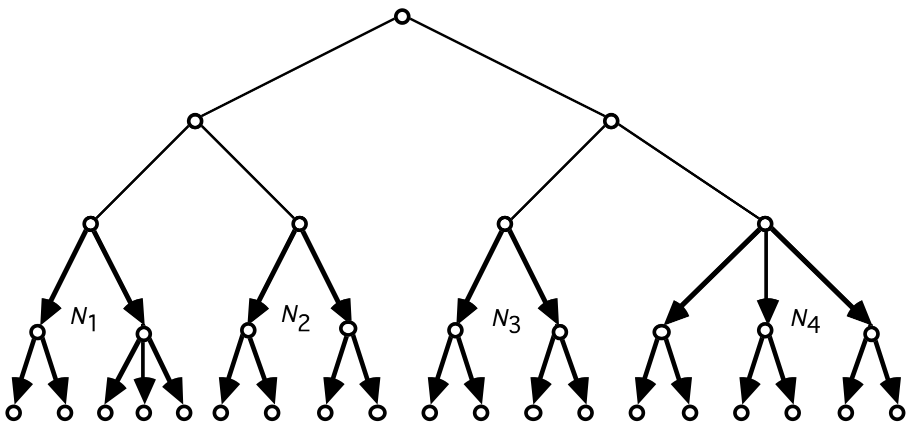
Switched/broadcast network (1983 - 1985)



Switched WAN
(possibly including MIXes)

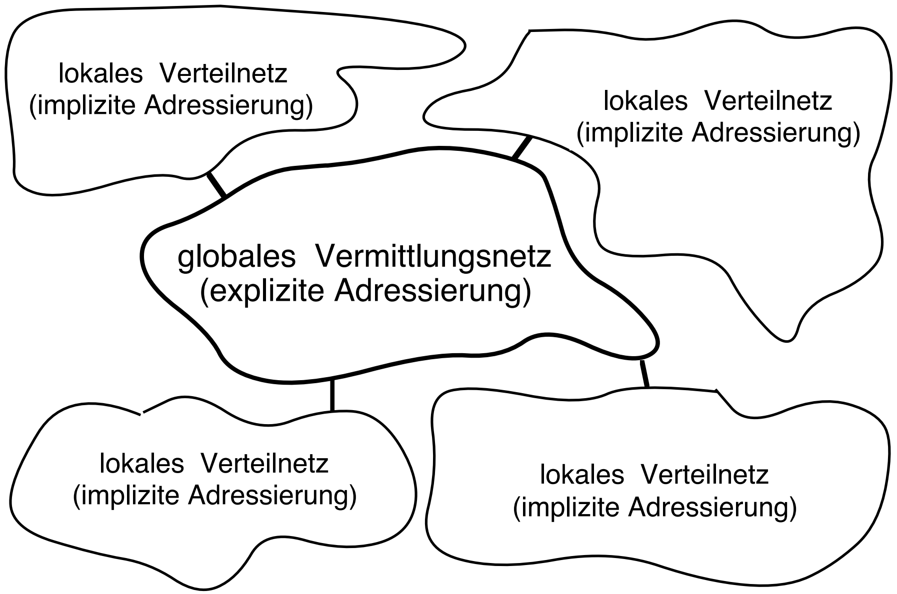
connecting

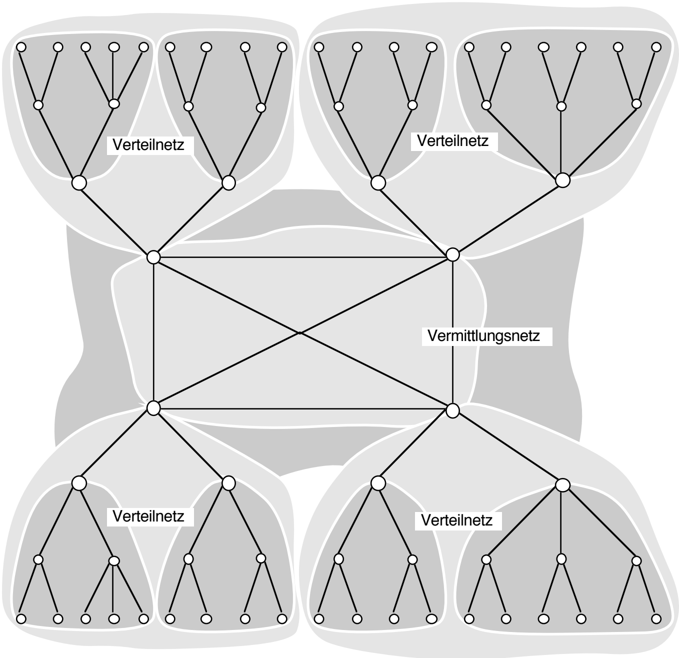
broadcast LANs
(RING-net, DC-net)



- i.e. taking anonymity and unobservability into account when building networks physically
- statically fixed structure (or dynamically adaptable subset/superset construction) is well suited to counter intersection attacks

Switched/broadcast network (1983 - 1985)





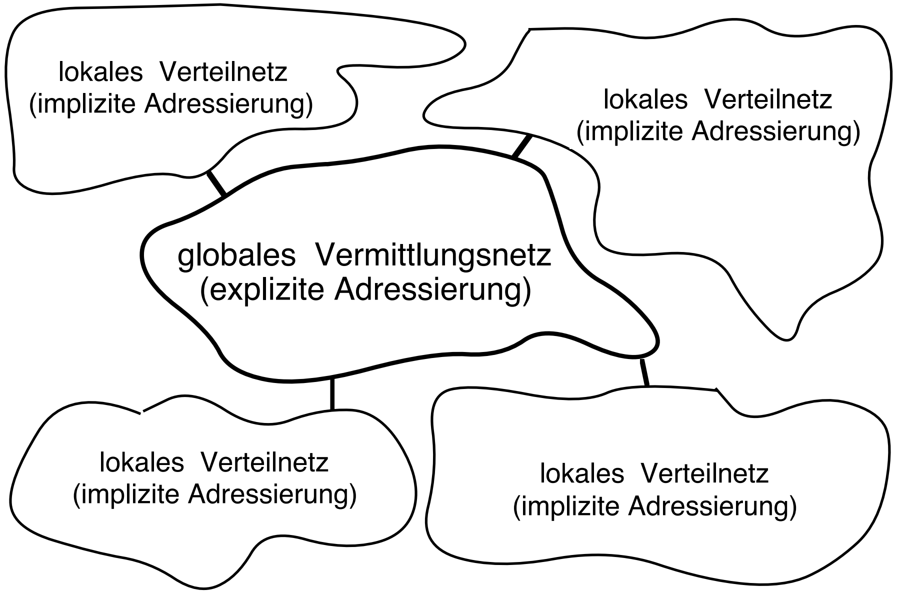
Switched WAN
(possibly including MIXes)

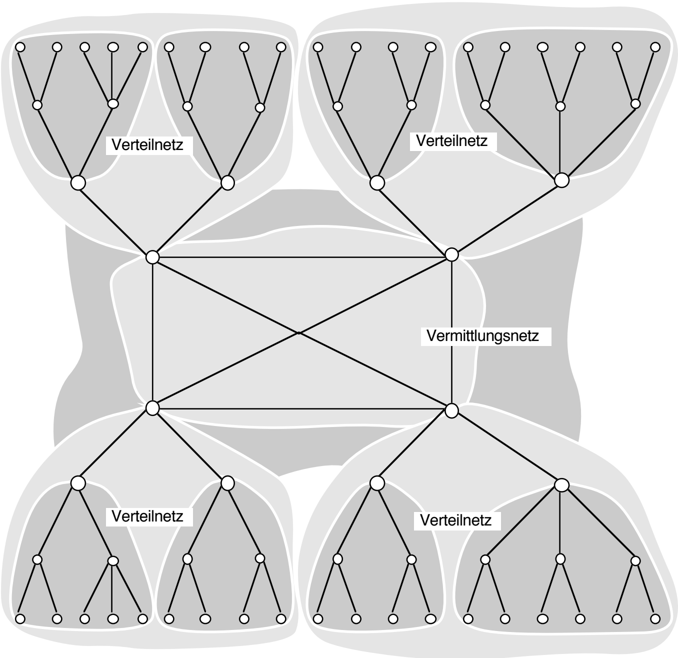
connecting

broadcast LANs
(RING-net, DC-net)

- i.e. taking anonymity and unobservability into account when building networks physically
- statically fixed structure (or dynamically adaptable subset/superset construction) is well suited to counter intersection attacks

Switched/broadcast network (1983 - 1985)



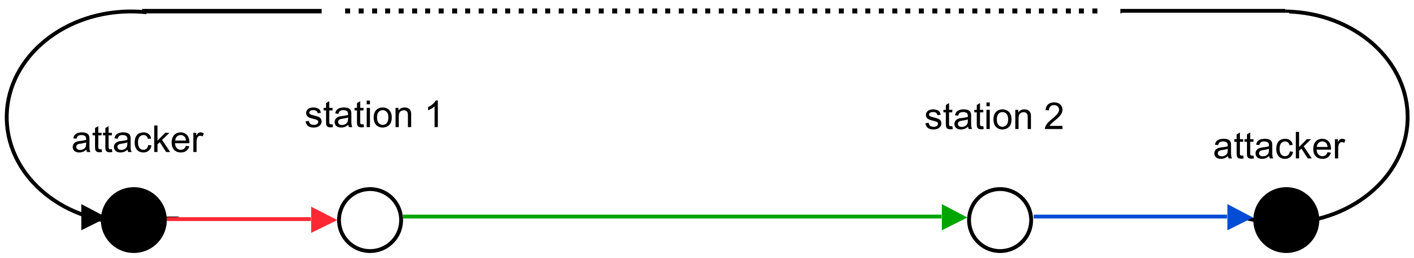


Switched WAN
(possibly including MIXes)
for services tolerating longer delays
connecting

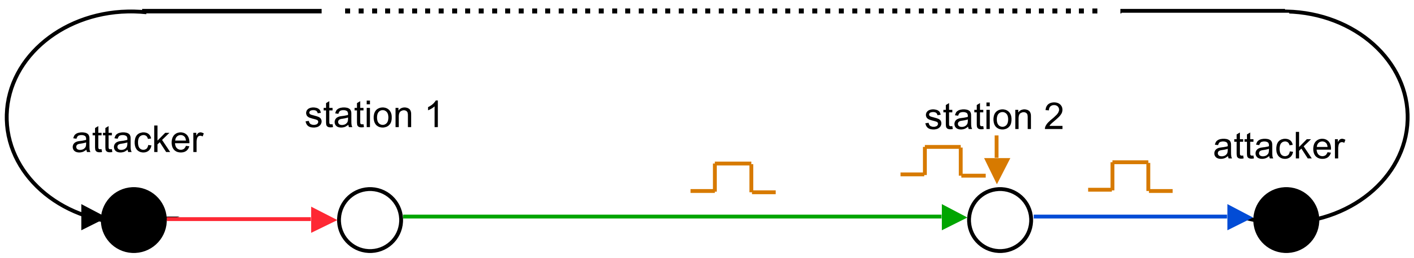
broadcast LANs
(RING-net, DC-net)

- i.e. taking anonymity and unobservability into account when building networks physically
- statically fixed structure (or dynamically adaptable subset/superset construction) is well suited to counter intersection attacks

RING-net (1983-1985)



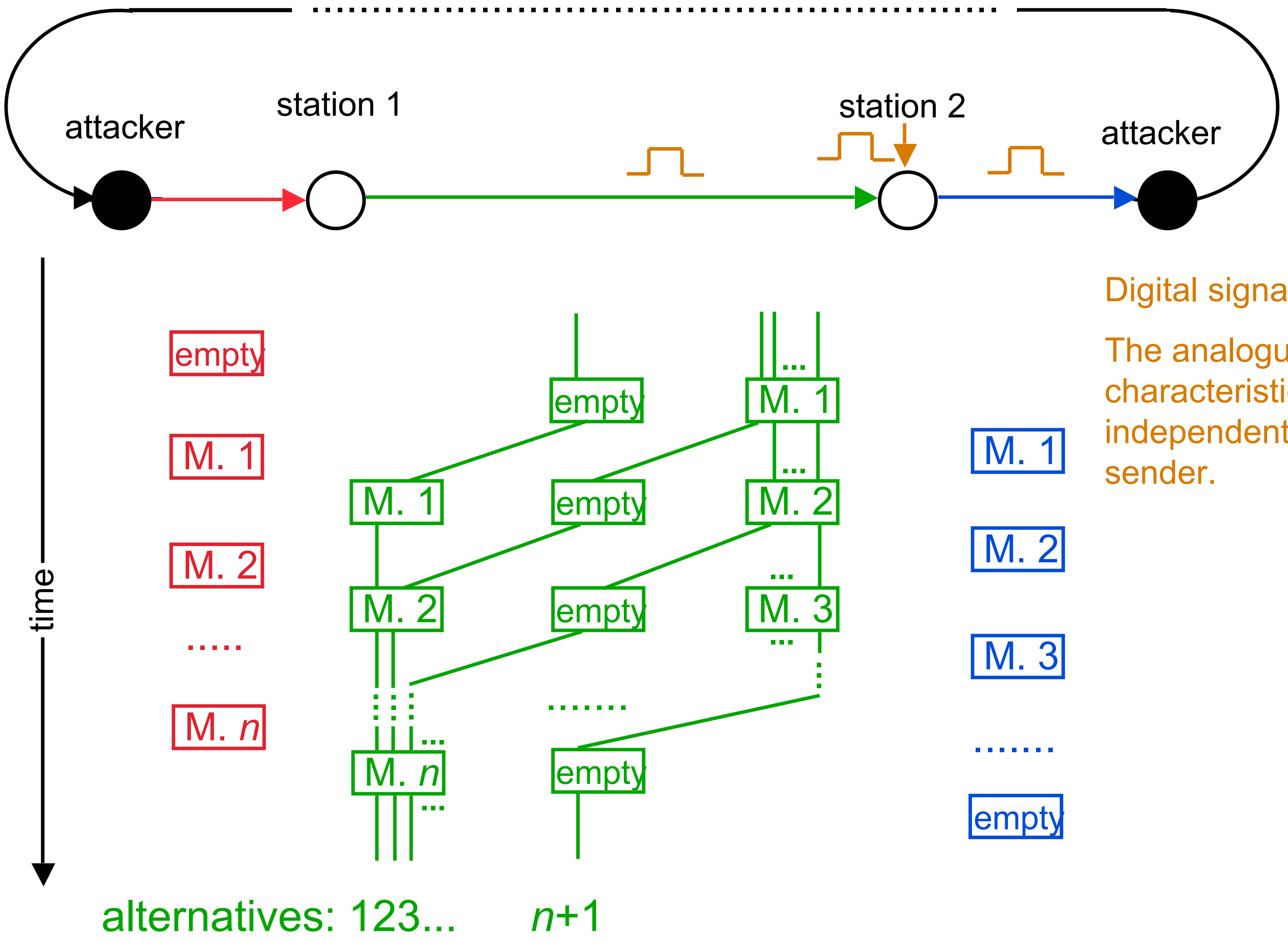
RING-net (1983-1985)



Digital signal regeneration:

The analogue characteristics of bits are independent of their true sender.

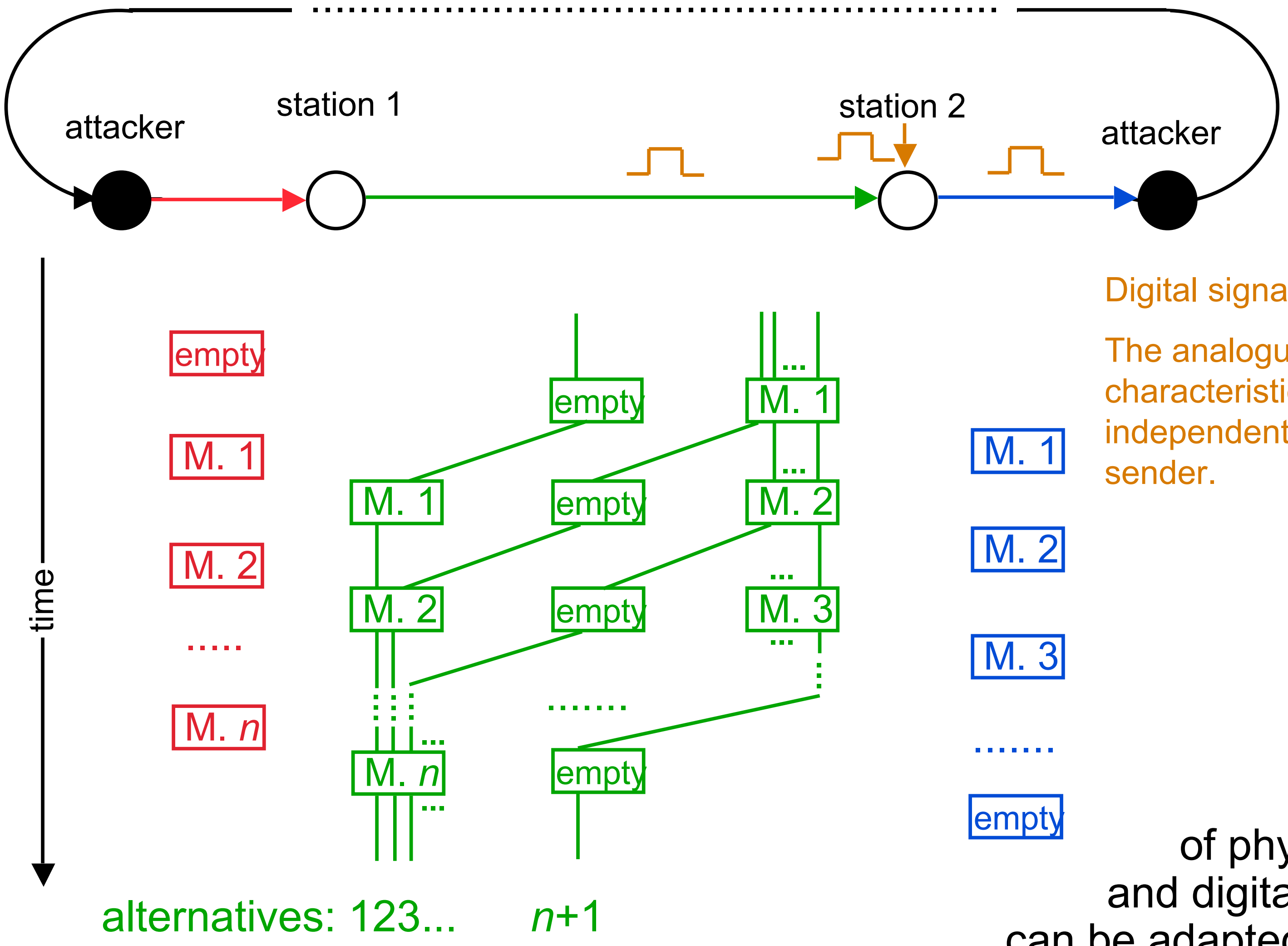
RING-net (1983-1985)



Digital signal regeneration:

The analogue characteristics of bits are independent of their true sender.

RING-net (1983-1985)

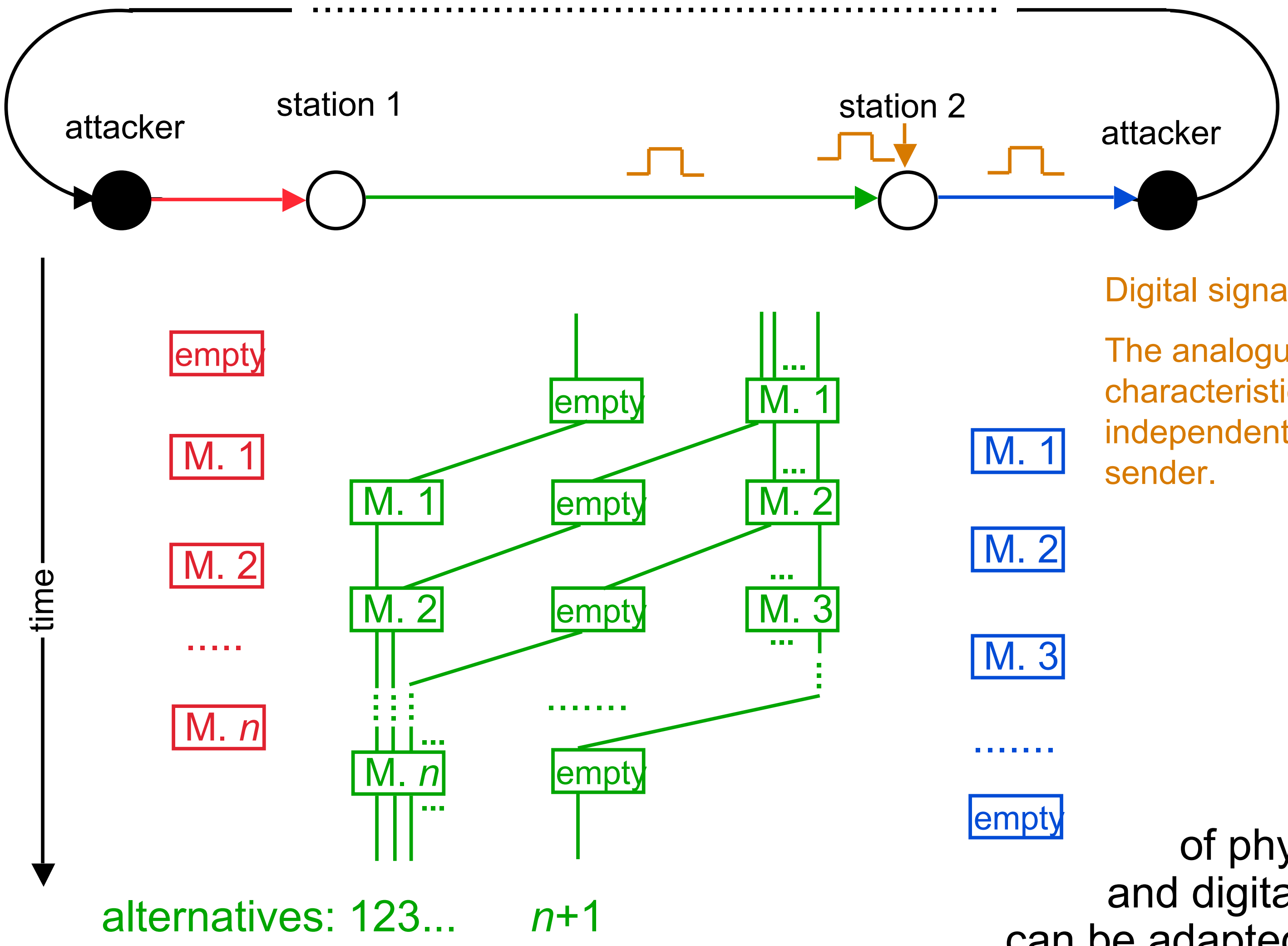


Digital signal regeneration:

The analogue characteristics of bits are independent of their true sender.

The idea of physical unobservability and digital signal regeneration can be adapted to other topologies, i.e. tree-shaped CATV networks;

RING-net (1983-1985)



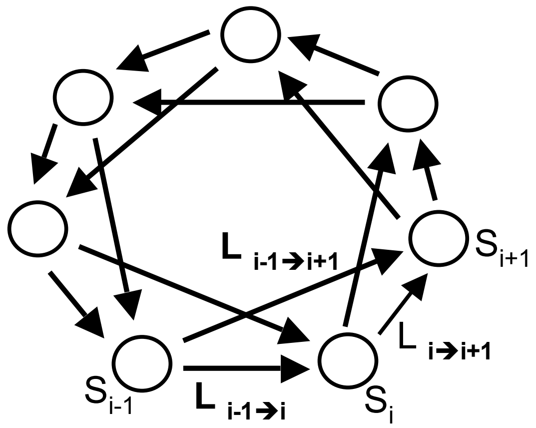
Digital signal regeneration:

The analogue characteristics of bits are independent of their true sender.

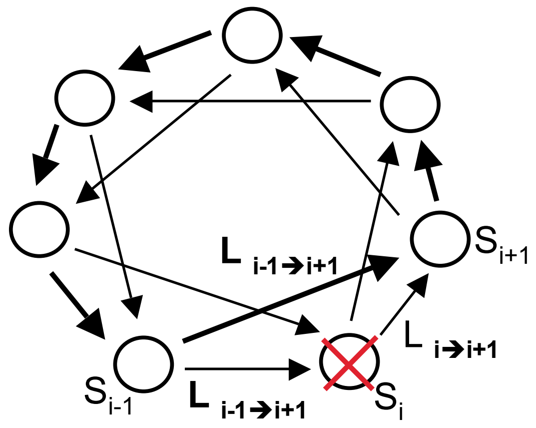
The idea of physical unobservability and digital signal regeneration can be adapted to other topologies, i.e. tree-shaped CATV networks;

It reappears in another context in Crowds

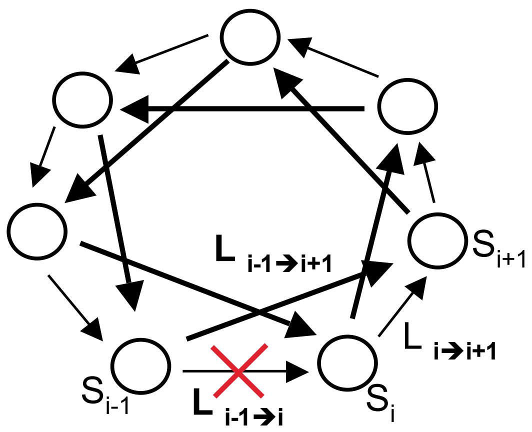
Braided RING (1985-1987)



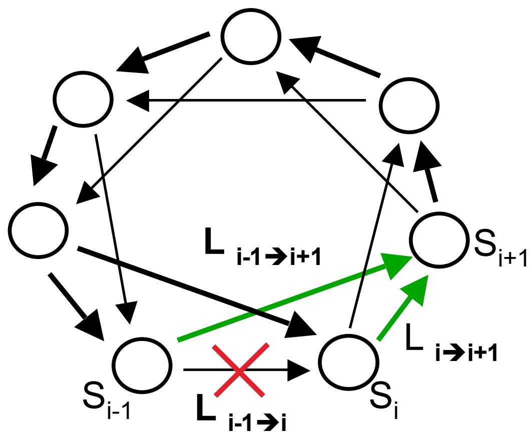
Two RINGs operating
if no faults



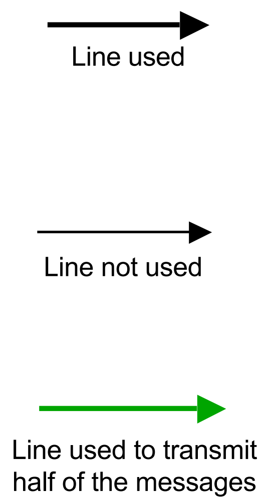
Reconfiguration of the outer
RING if a station fails



Reconfiguration of the inner
RING if an outer line fails



Reconfiguration of the outer
RING if an outer line fails



Addressing in broadcast networks (1985)

Addressing
explicit addresses: routing
implicit addresses: attribute recognizable by the station of the recipient

invisible <==> encryption system
visible pseudo random number, associative memory to detect

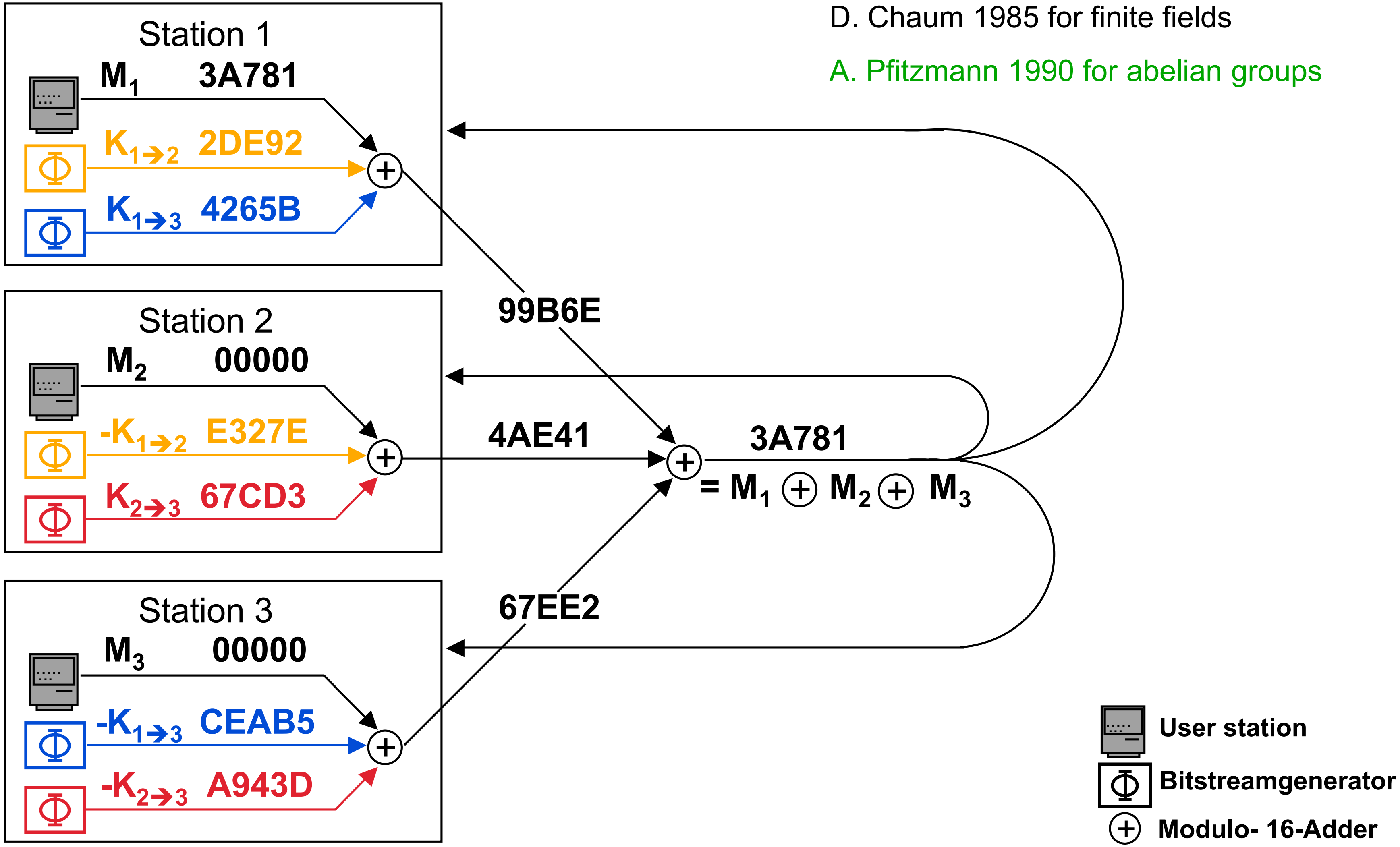
		address distribution	
		public address	private address
implicit address	invisible	very costly, but necessary to establish contact	costly
	visible	should not be used	change after use

invisible public address <==> asymmetric cryptosystem
invisible private address <==> symmetric cryptosystem

DC-net

D. Chaum 1985 for finite fields

A. Pfitzmann 1990 for abelian groups



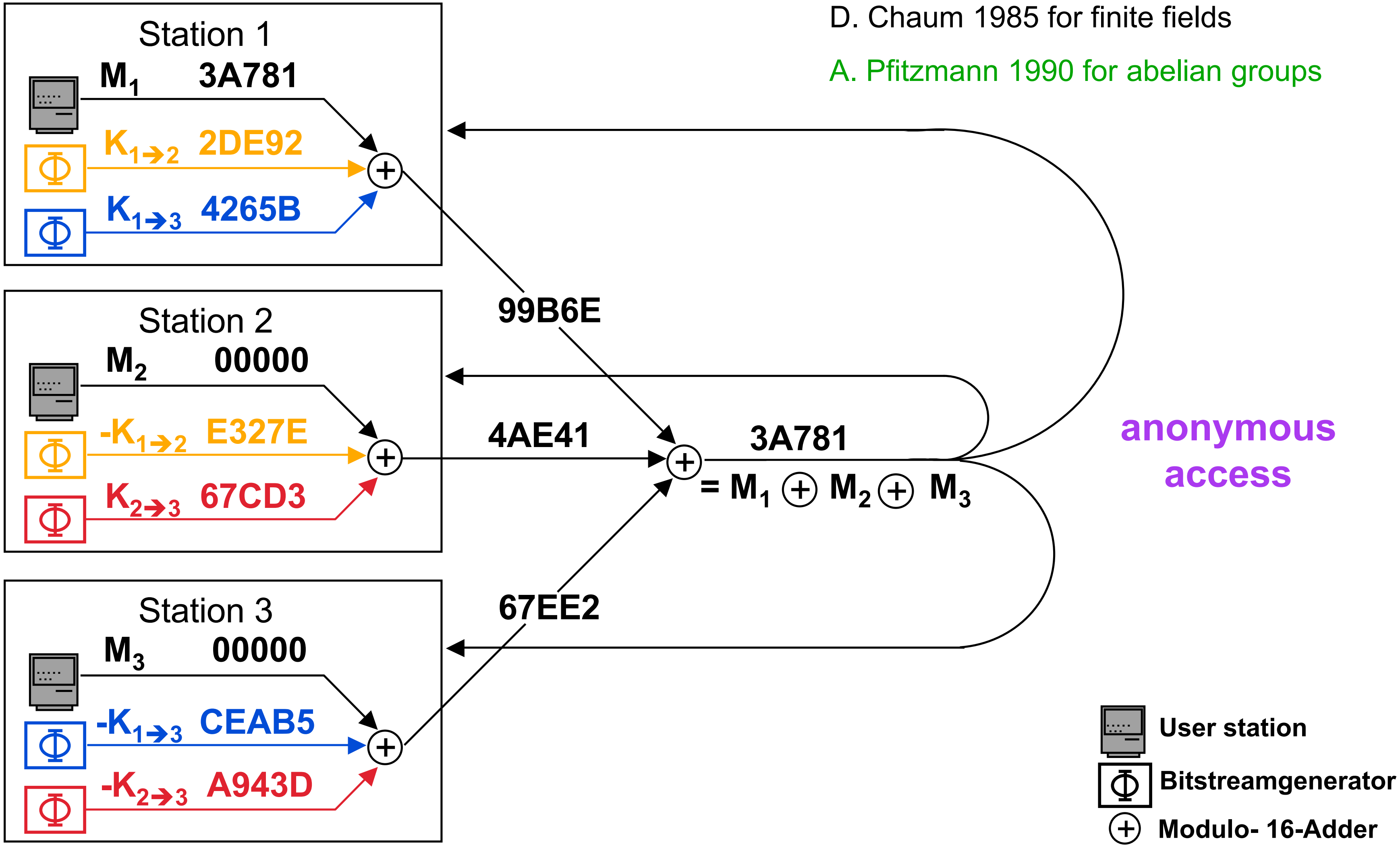
Anonymity of the sender

If stations are connected by keys the value of which is completely unknown to the attacker, tapping all lines does not give him any information about the sender.

DC-net

D. Chaum 1985 for finite fields

A. Pfitzmann 1990 for abelian groups



Anonymity of the sender

If stations are connected by keys the value of which is completely unknown to the attacker, tapping all lines does not give him any information about the sender.

Anonymity of the recipient: Fail-stop key generation (1989-91)

- DC-net provides recipient anonymity only against a passive attacker – an active attacker might manipulate the consistency of the broadcast.
- Fail-stop key generation (use the locally received result of round *r* as one input to calculate the keys for all rounds to come) guarantees consistency unconditionally, which yields unconditional recipient anonymity even against computationally unrestricted active attackers.

Michael Waidner, Birgit Pfitzmann: Unconditional Sender and Recipient Untraceability in spite of Active Attacks - Some Remarks; Fakultät für Informatik, Universität Karlsruhe, Interner Bericht 5/89, March 1989.

Michael Waidner: Unconditional Sender and Recipient Untraceability in spite of Active Attacks; Eurocrypt '89, LNCS 434, Springer-Verlag, Berlin 1990, 302-319.

Jörg Lukat, Andreas Pfitzmann, Michael Waidner: Effizientere fail-stop Schlüsselerzeugung für das DC-Netz; Datenschutz und Datensicherung DuD 15/2 (1991) 71-75.

Superposed receiving (1988-1990)

Whoever knows the sum of *n* characters and *n*-1 of these *n* characters, can calculate the *n*-th character.

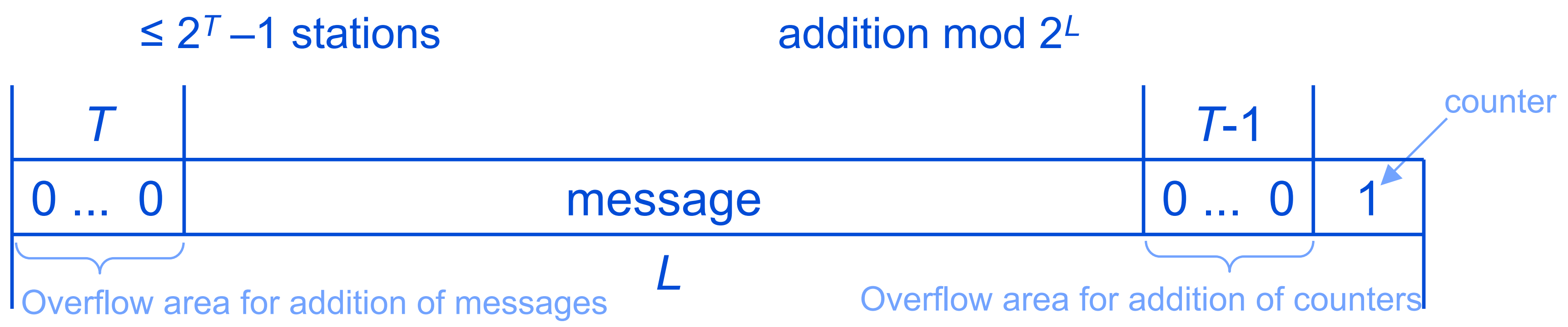
pairwise superposed receiving (reservation scheme: n=2)

Two stations send simultaneously.
Each subtracts their character from the sum to receive the character sent by the other station.
==> Duplex channel in the bandwidth of a simplex channel

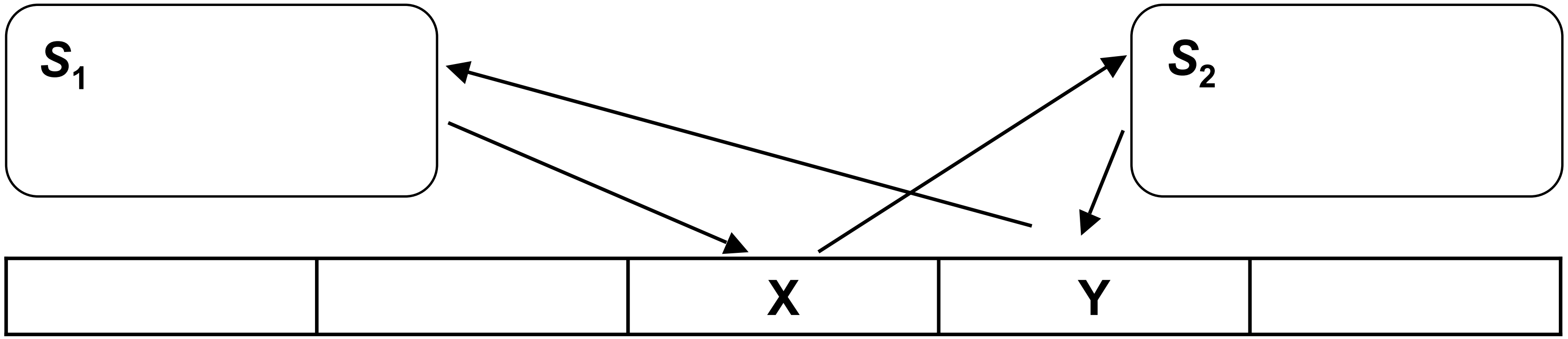
global superposed receiving (direct transmission: $n \geq 2$)

Result of a collision is stored, so that if *n* messages collide, only *n*-1 of them have to be sent again.

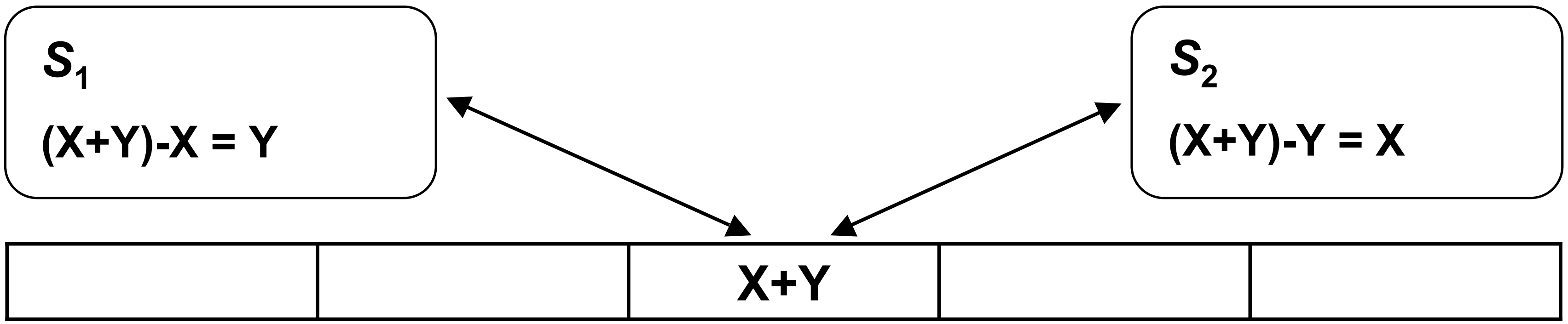
Collision resolution algorithm using the mean of messages:



Pairwise superposed receiving (1988-1990)



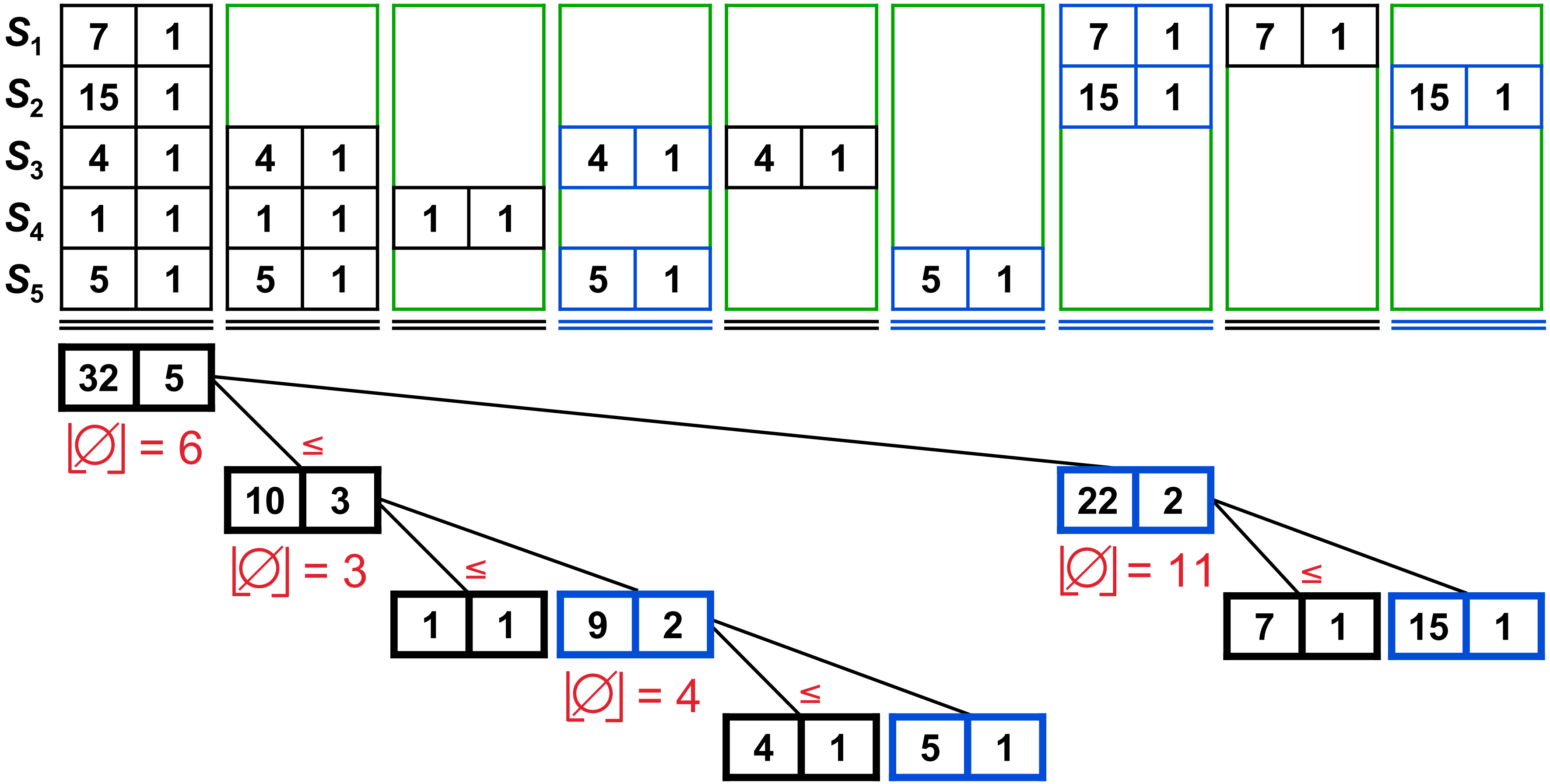
Without superposed receiving



With pairwise superposed receiving

Andreas Pfitzmann: Diensteintegrierende Kommunikationsnetze mit teilnehmerüberprüfbarem Datenschutz; IFB 234, Springer-Verlag, Heidelberg 1990. ISBN 3-540-52327-8, p. 99

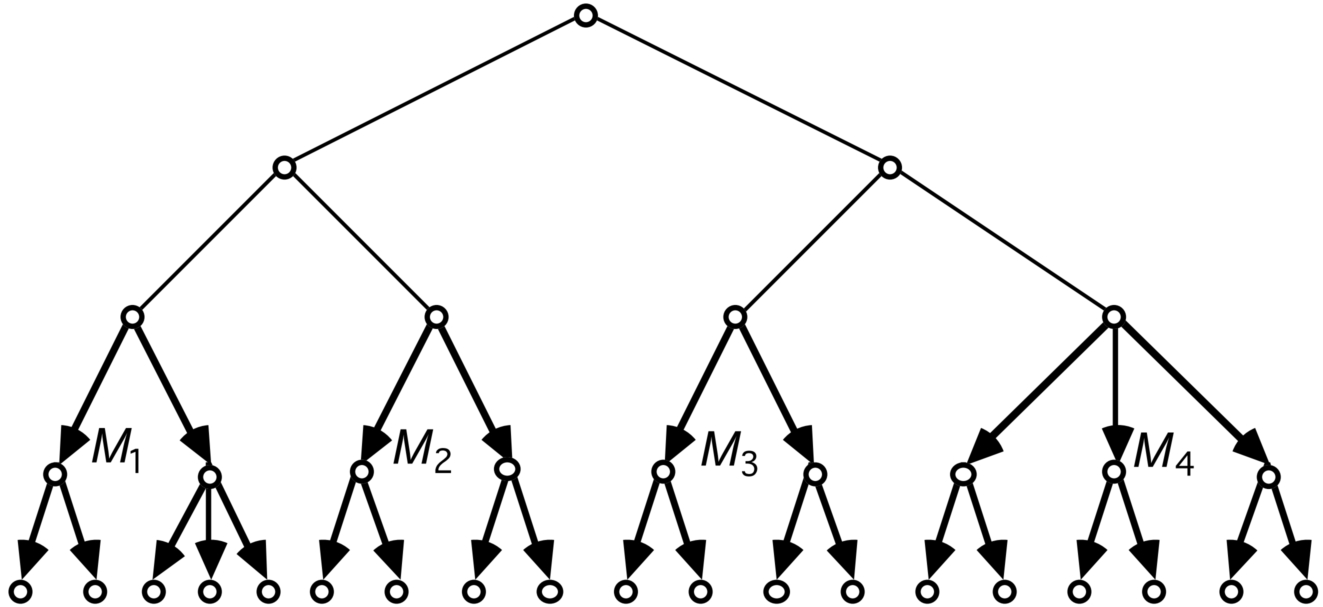
Global superposed receiving (1988-1990)



Collision resolution algorithm with mean calculation and superposed receiving

Andreas Pfitzmann: Diensteintegrierende Kommunikationsnetze mit teilnehmerüberprüfbarem Datenschutz; IFB 234, Springer-Verlag, Heidelberg 1990. ISBN 3-540-52327-8, p. 134

DC-net with dynamically partitioned broadcast (1985)



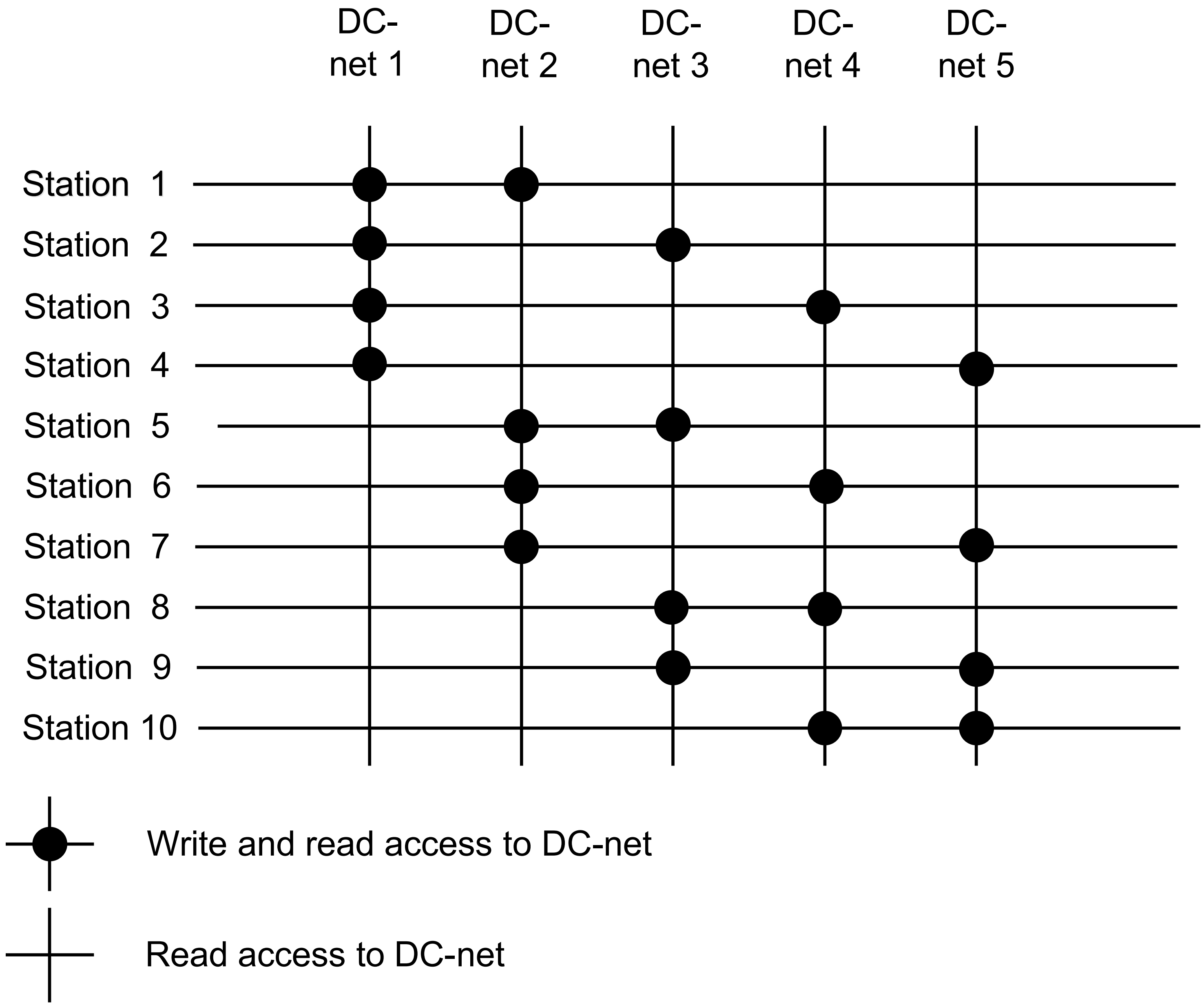
Time division partitioning of the tree and appropriately chosen dynamic key graphs:

In the first time partition (potentially) global (e.g. international) traffic takes place: all messages travel to the root and are broadcast world-wide. Keys for this time partition can (and should be) shared with other user stations all over the world.

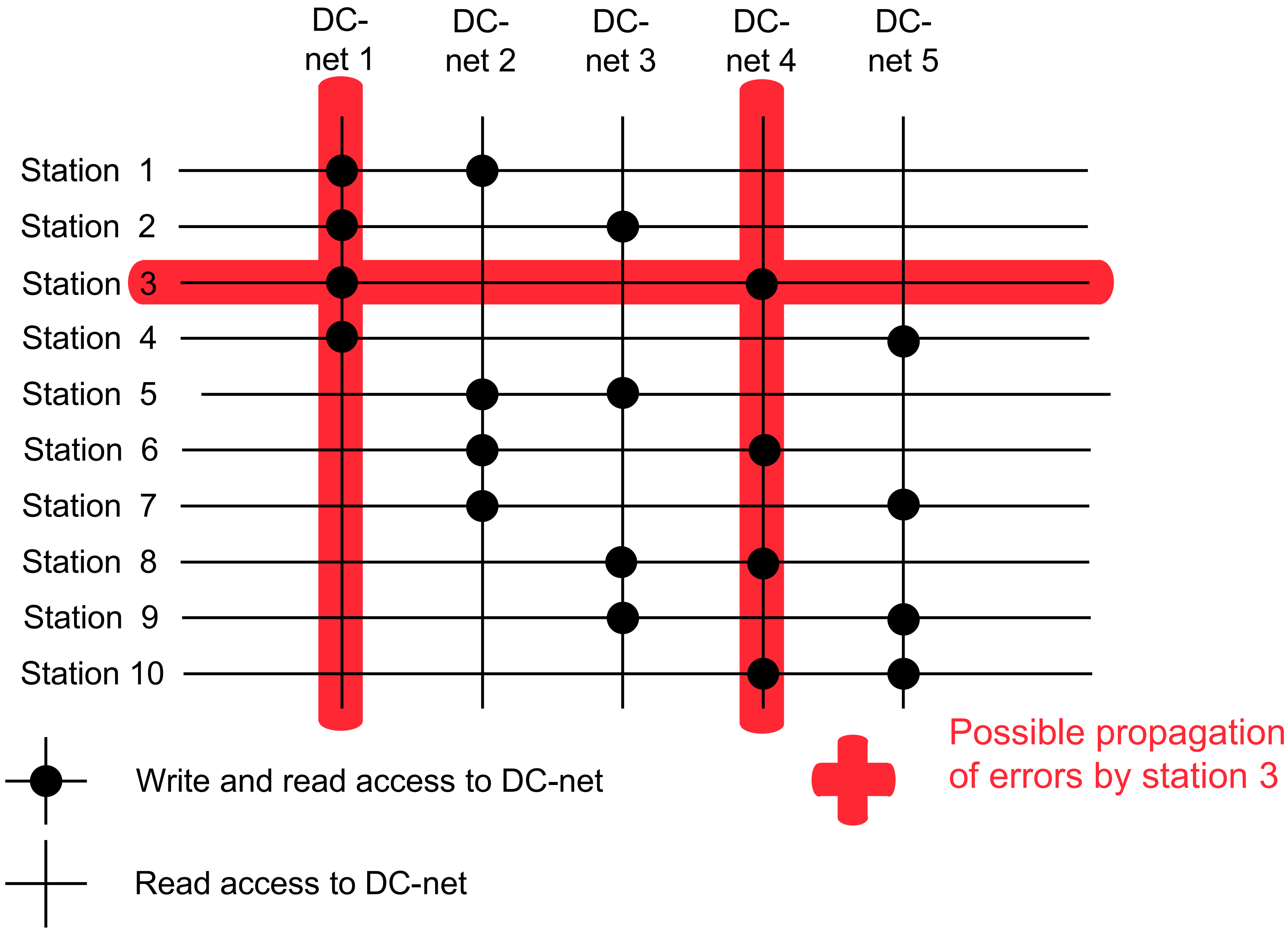
In the n+1[st] time partition, all messages travel only to the n^{th} sons of the root (representing e.g. continentals, states, districts, ...). Keys for these time partitions are only shared between user stations which are sons of the same n^{th} son of the root.

A. Pfitzmann: How to implement ISDNs without user observability - Some remarks; Interner Bericht 14/85, Univ. Karlsruhe, Fak. Informatik, p. 67

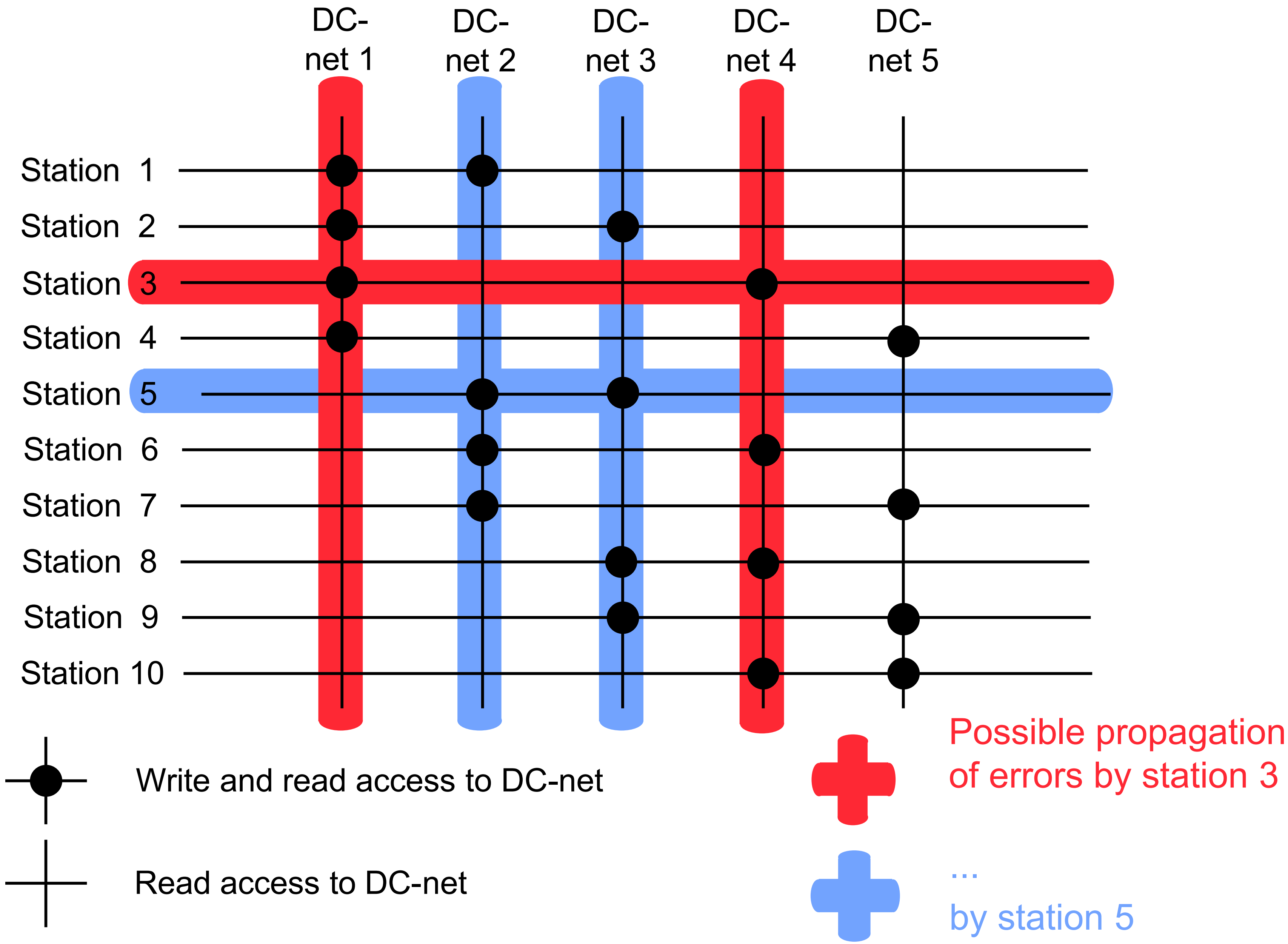
Fault tolerance: sender-partitioned DC-net (1990)



Fault tolerance: sender-partitioned DC-net (1990)



Fault tolerance: sender-partitioned DC-net (1990)



Enhancements of MIXes (1985-1990)

Symmetric crypto for first and last MIX

Channels: reduce delay (and storage),

but must start and end at the same time

--> time-slice channels

Constant rate dummy traffic end-to-end having 3 advantages:

1. real-time behavior of batch MIXes
2. unobservable sending and receiving of messages
3. when combined with cascade,
   - MIXes may substitute traffic for users to hide their presence/absence or failures of their machines or counter active attacks
   - linkability of some messages does not change the anonymity more than absolutely unavoidable

Design optimized for ISDN: Real-Time MIXes (1989-1991)

Requirements: ISDN services using the ISDN transmission system

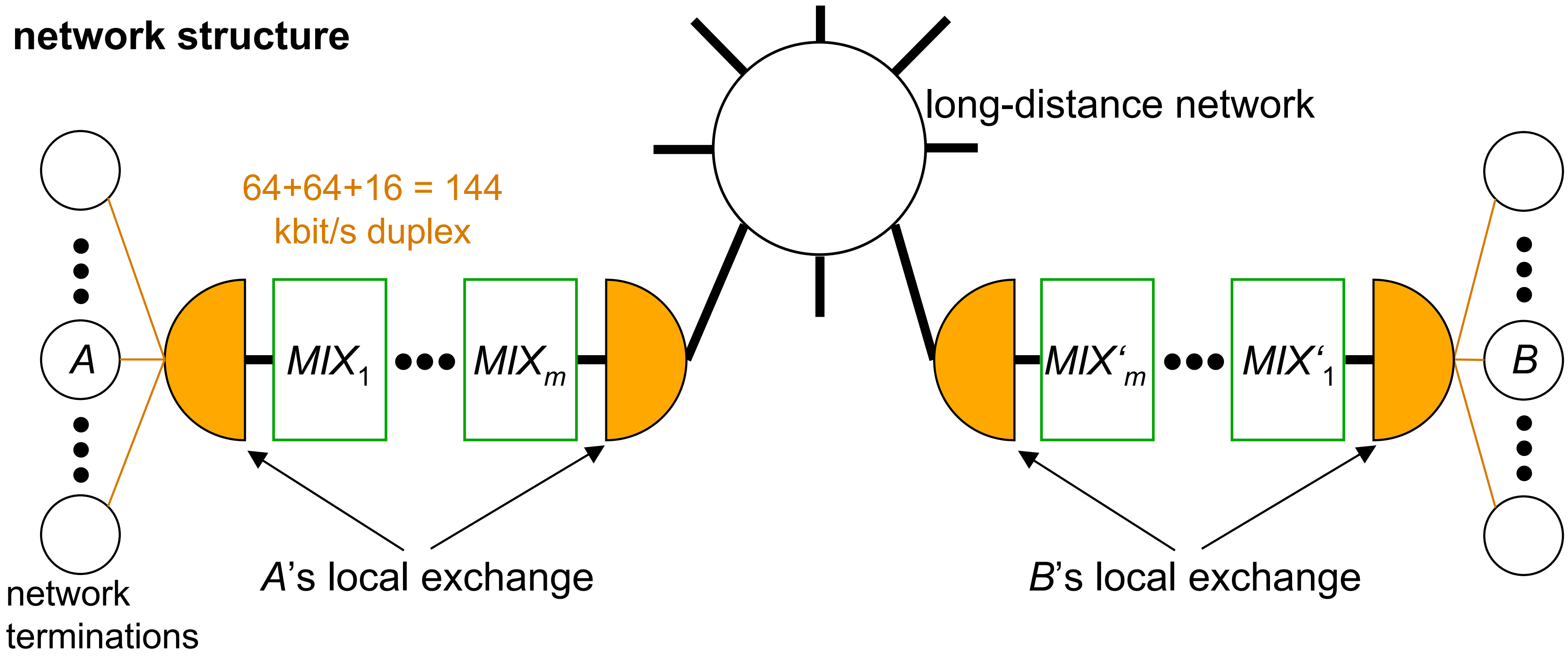
2 independent 64-kbit/s duplex channels using 144-kbit/s subscriber lines

nearly no delay on established channels

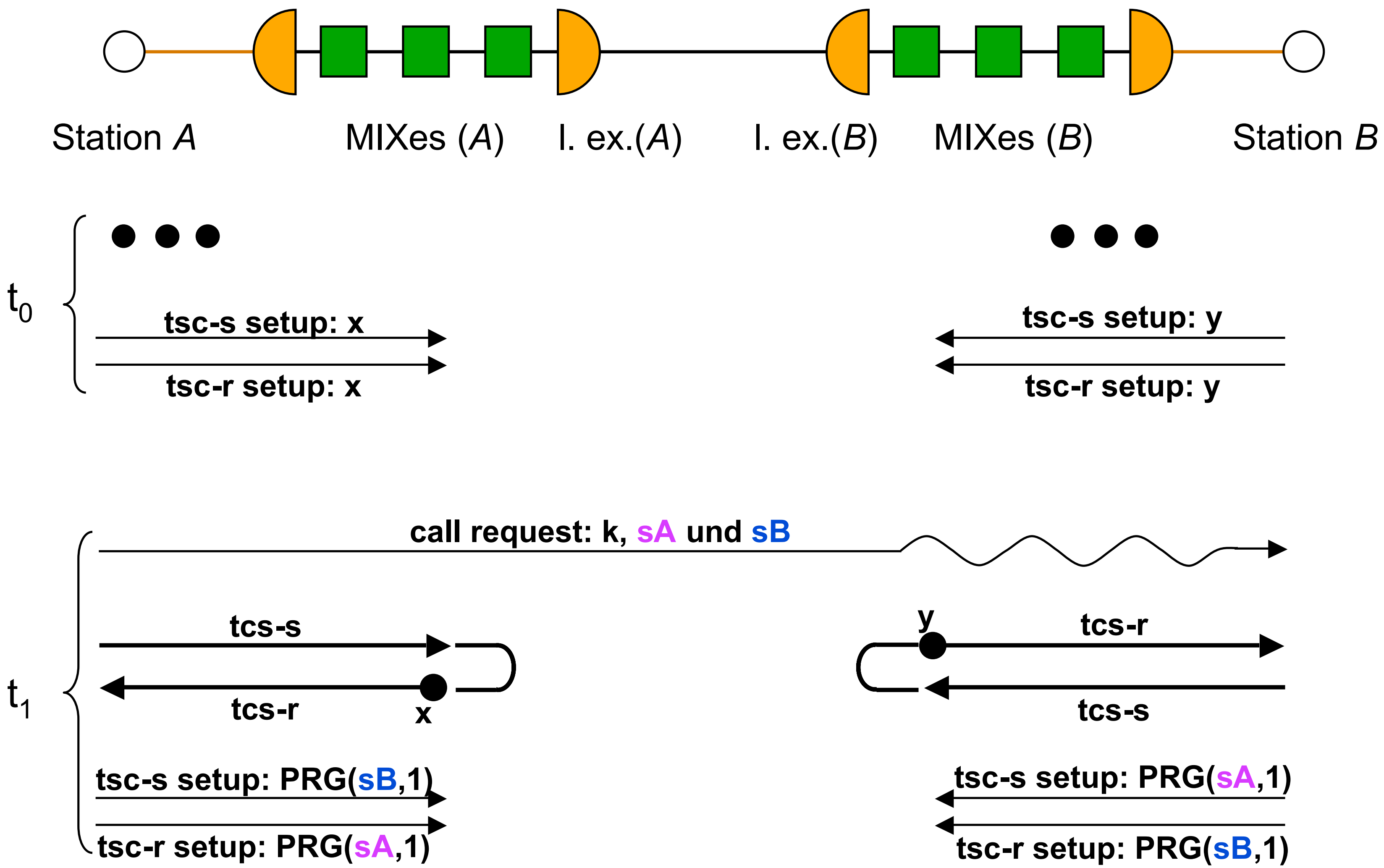
establishment of channels within 3 seconds

no additional load to the long-distance network

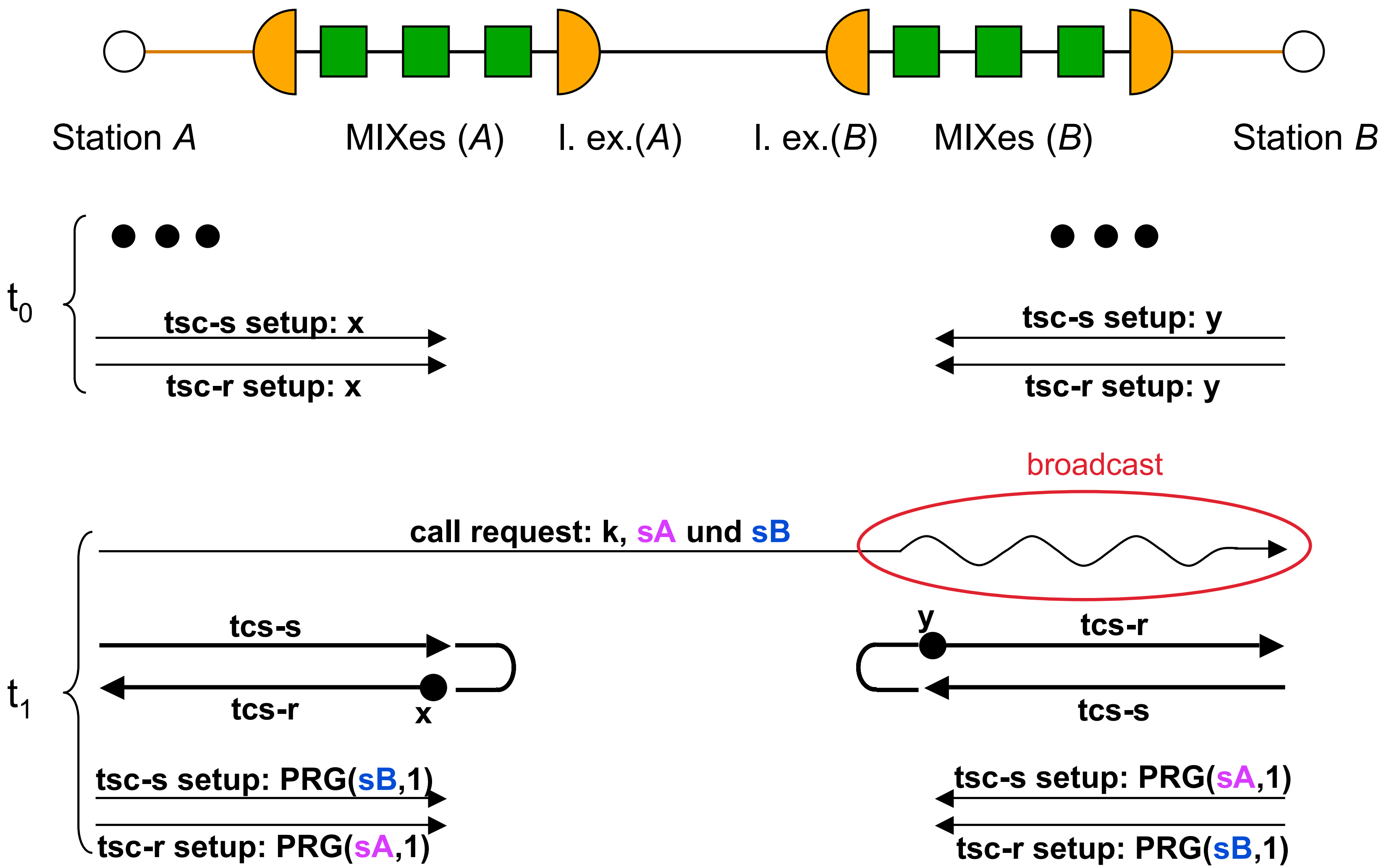
network structure



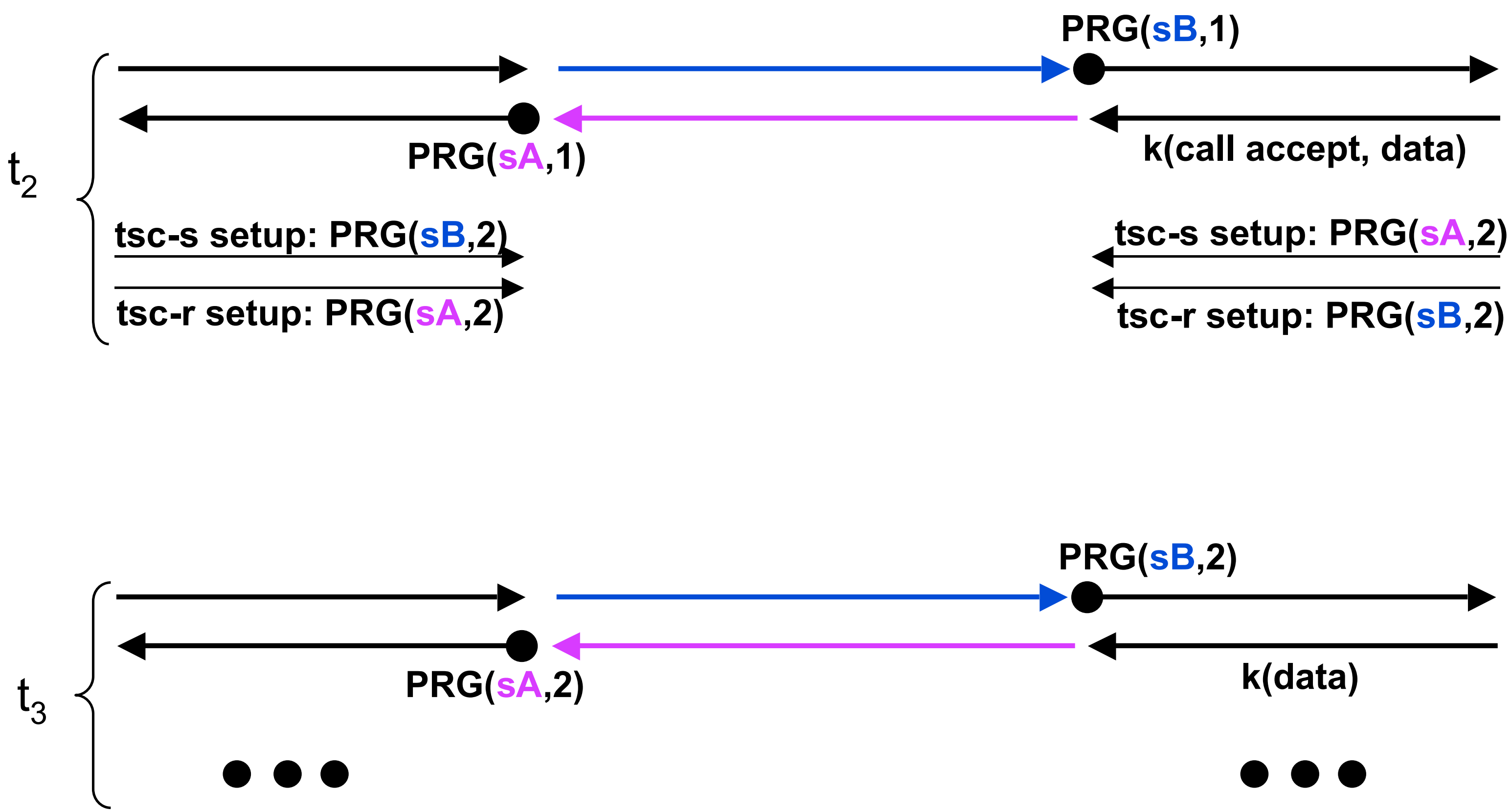
Time-Slice Channels (1989)



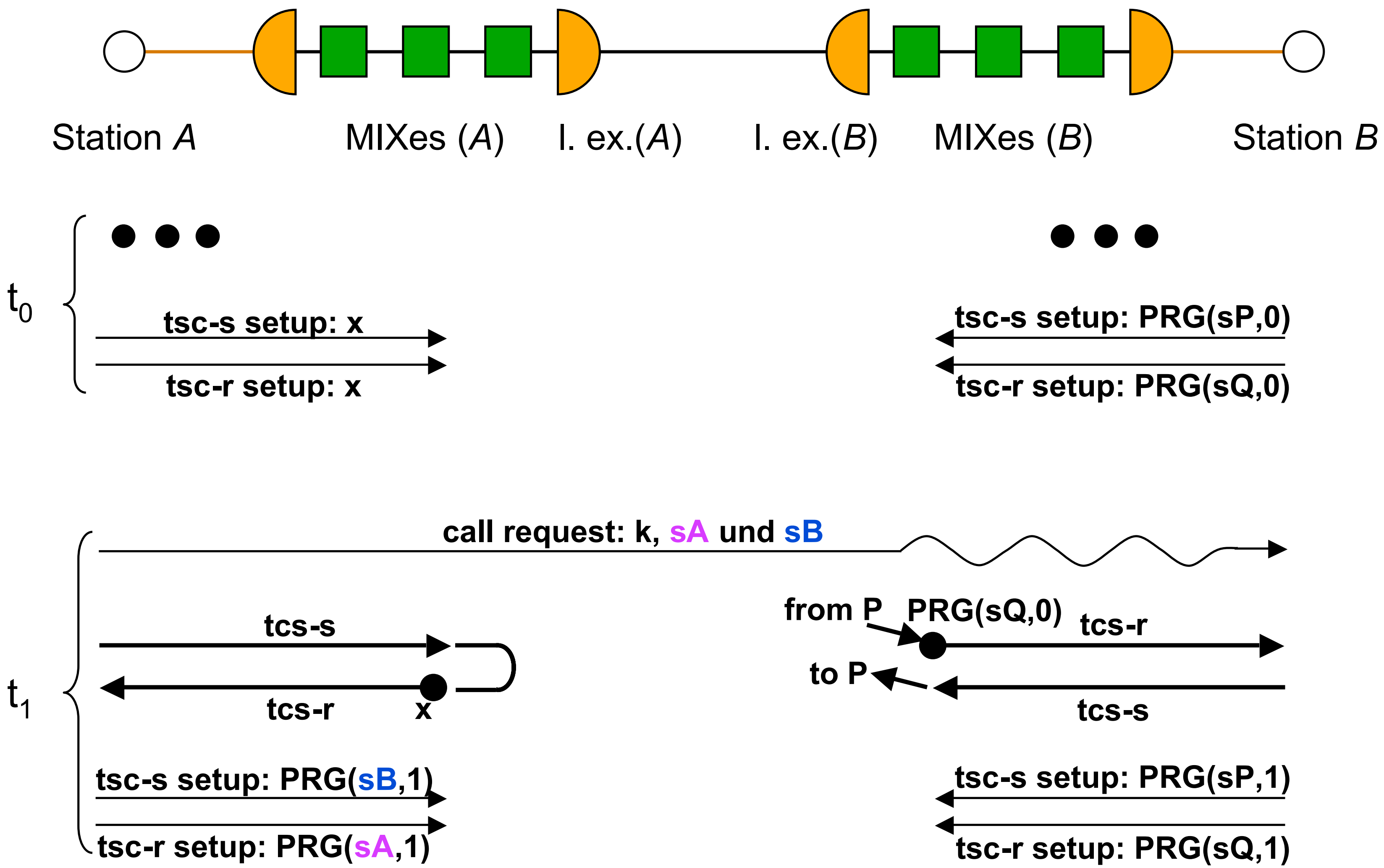
Time-Slice Channels (1989)



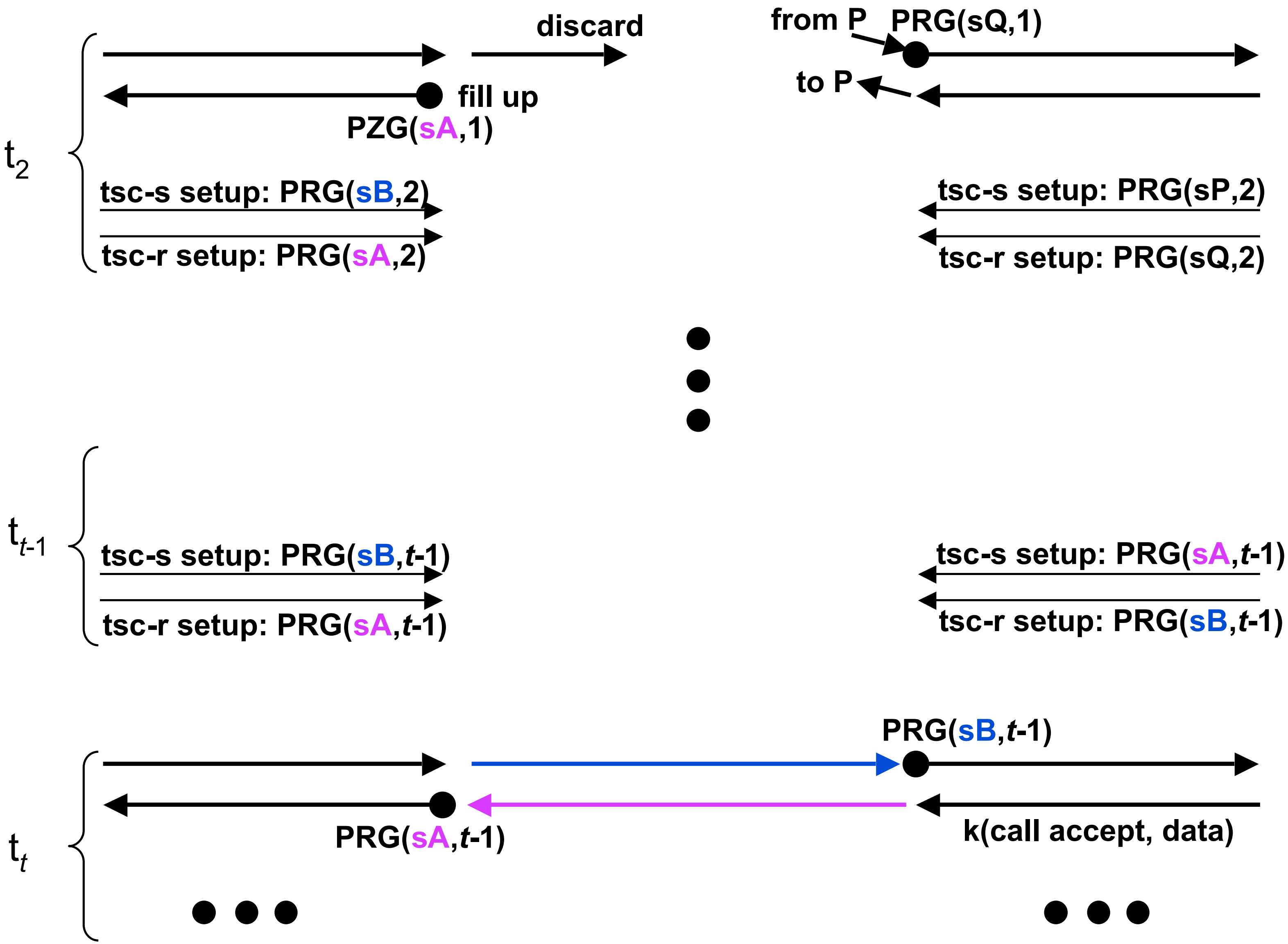
Time-Slice Channels (cont.)



Delayed acceptance of call



Delayed acceptance of call (cont.)



Advantages of Real-Time MIXes

- recipient anonymity without untraceable return addresses with long validity (good for fault tolerance)
- cascade: pipelining -> even distribution of processing of traffic without any stochastic assumptions
- together: avoiding any need of long term storage of (hashes of) messages

Andreas Pfitzmann, Birgit Pfitzmann, Michael Waidner: Telefon-MIXe: Schutz der Vermittlungsdaten für zwei 64-kbit/s-Duplexkanäle über den (2*64 + 16)-kbit/s-Teilnehmeranschluß; Datenschutz und Datensicherung DuD /12 (1989) 605-622.

Andreas Pfitzmann, Birgit Pfitzmann, Michael Waidner: ISDN-MIXes - Untraceable Communication with very small Bandwidth Overhead; Information Security, Proc. IFIP/Sec'91, May 1991, Brighton, D. T. Lindsay, W. L. Price (eds.), North-Holland, Amsterdam 1991, 245-258.

Anja Jerichow, Jan Müller, Andreas Pfitzmann, Birgit Pfitzmann, Michael Waidner: Real-Time Mixes: A Bandwidth-Efficient Anonymity Protocol; IEEE Journal on Selected Areas in Communications 16/4 (1998) 495-509.

"Proof" of MIX cascade (1990)

Maximum anonymity means (possibilistic setting):

- all other senders or recipients of the messages of a particular time interval or
- all MIXes

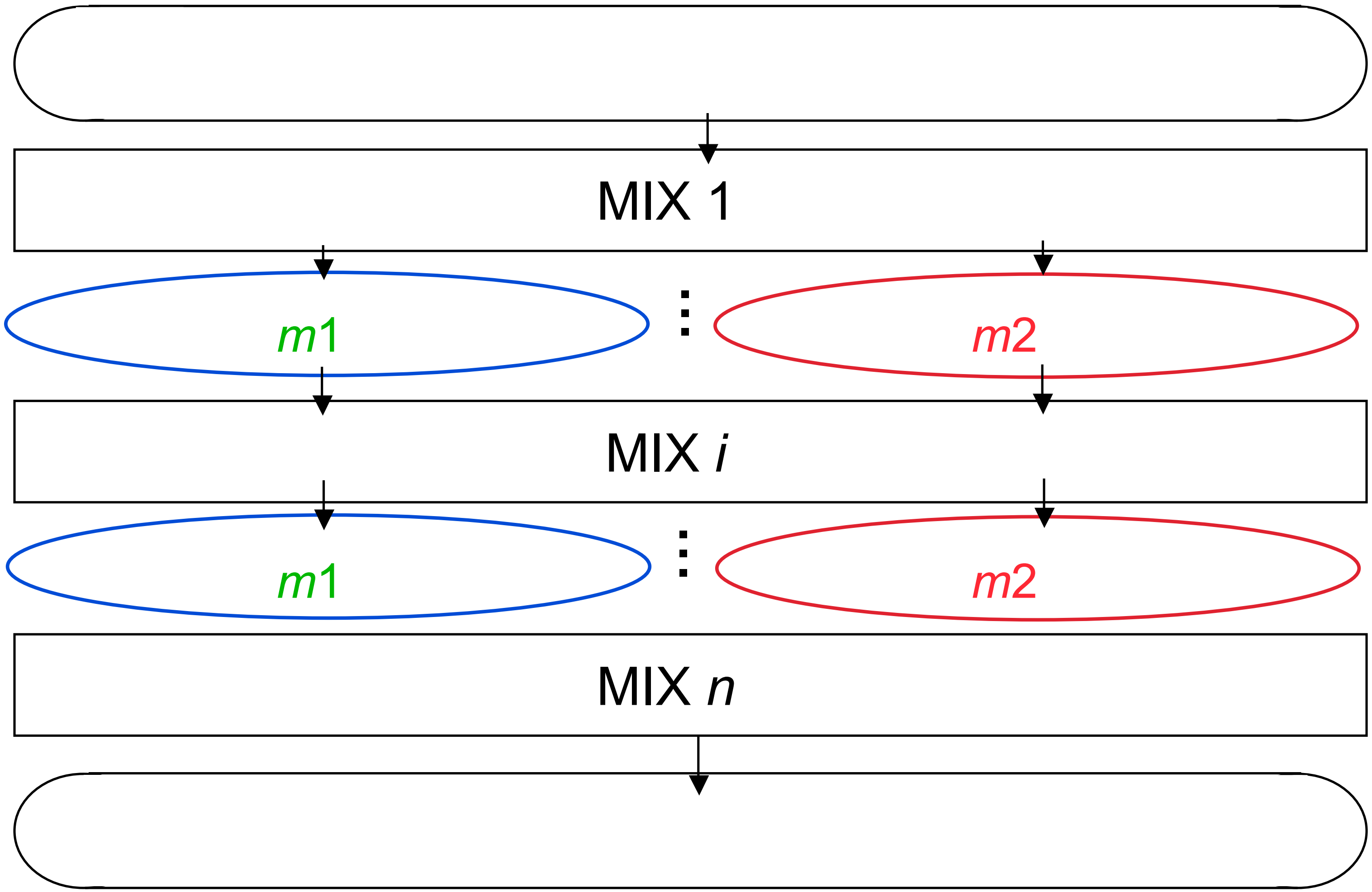
have to cooperate to trace a message against the wish of its sender or recipient.

Assuming that each message is mixed by each MIX only once, to achieve maximum anonymity, all these messages have to pass each MIX simultaneously and therefore all the MIXes in the same order (-> MIX cascade). (Remark: In a probabilistic setting, this would hold as well.)

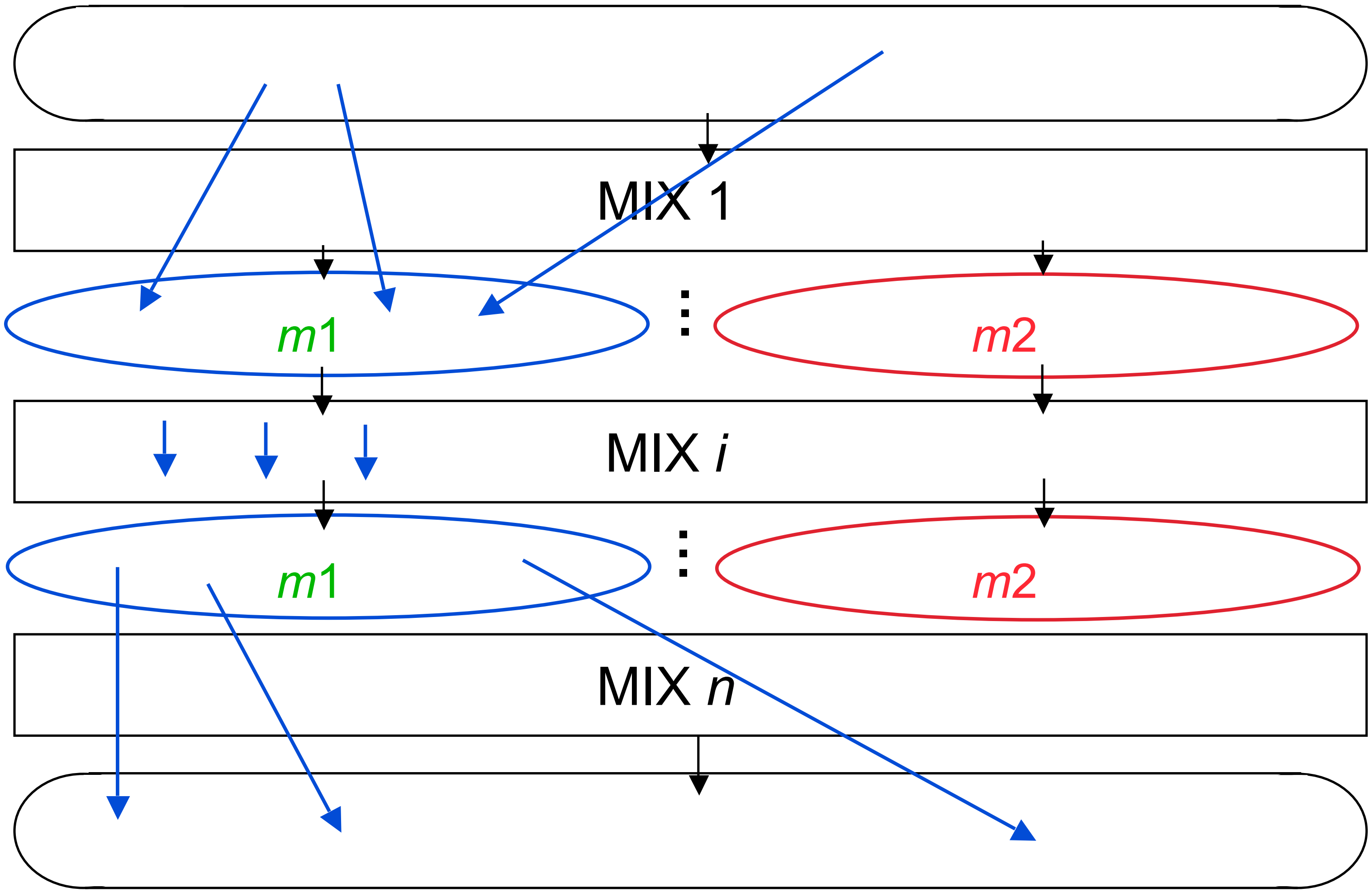
Proof (ind.): Assume not all these messages pass each MIX simultaneously, then there exist a MIX *i* and two messages *m*1 and *m*2 which do not pass MIX *i* simultaneously. If all other MIXes except *i* cooperate, they can trace *m*1 and *m*2 before and after MIX *i*. If all other senders and recipients than those of *m*1 and *m*2 cooperate, this means that both *m*1 and *m*2 are completely traceable, if no other senders or recipients cooperate, it means that the anonymity set of both *m*1 and *m*2 is decreased.

Andreas Pfitzmann: Diensteintegrierende Kommunikationsnetze mit teilnehmerüberprüfbarem Datenschutz; IFB 234, Springer-Verlag, Heidelberg 1990. ISBN 3-540-52327-8, p. 69

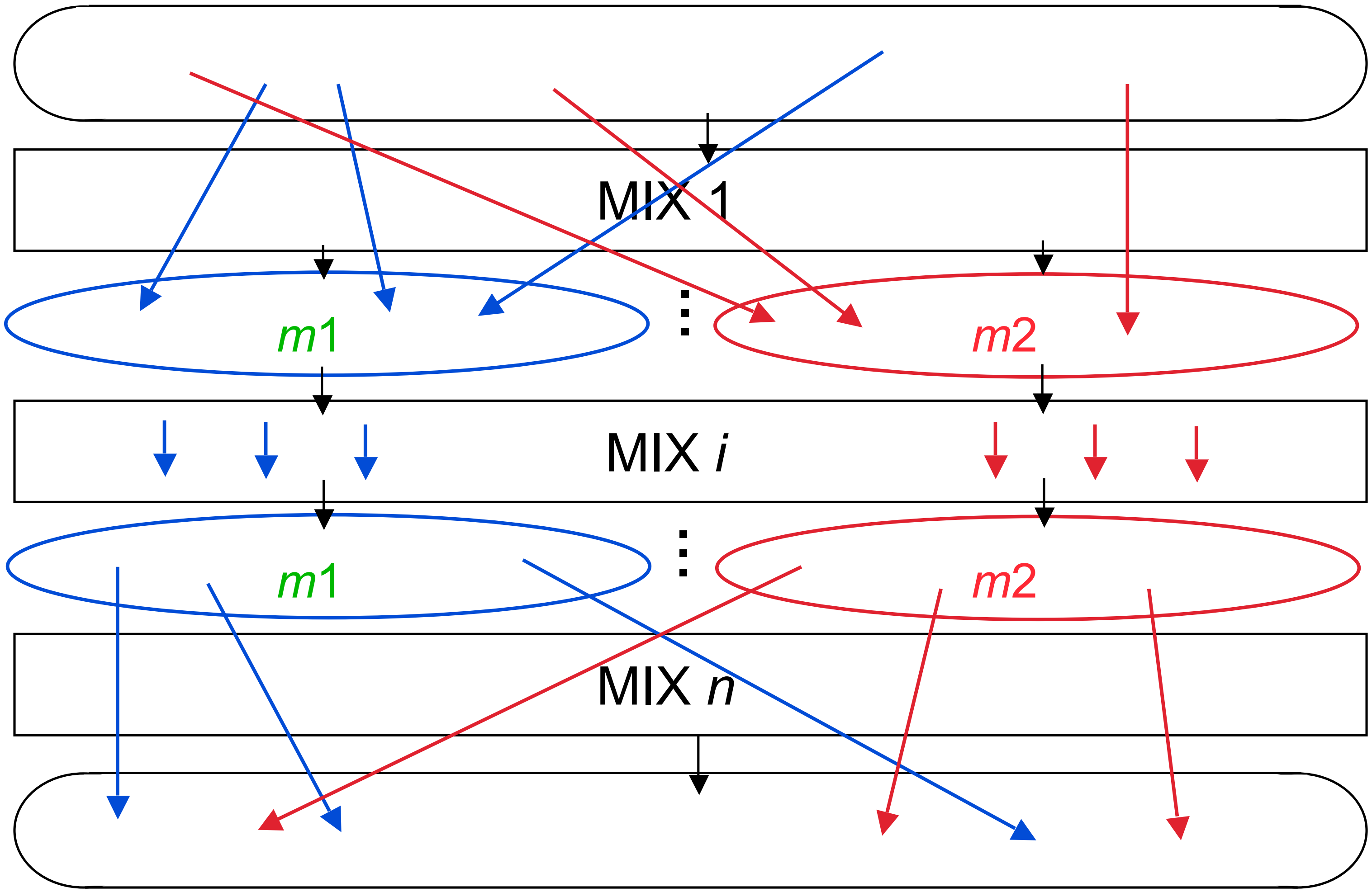
"Proof" of MIX cascade (cont.)



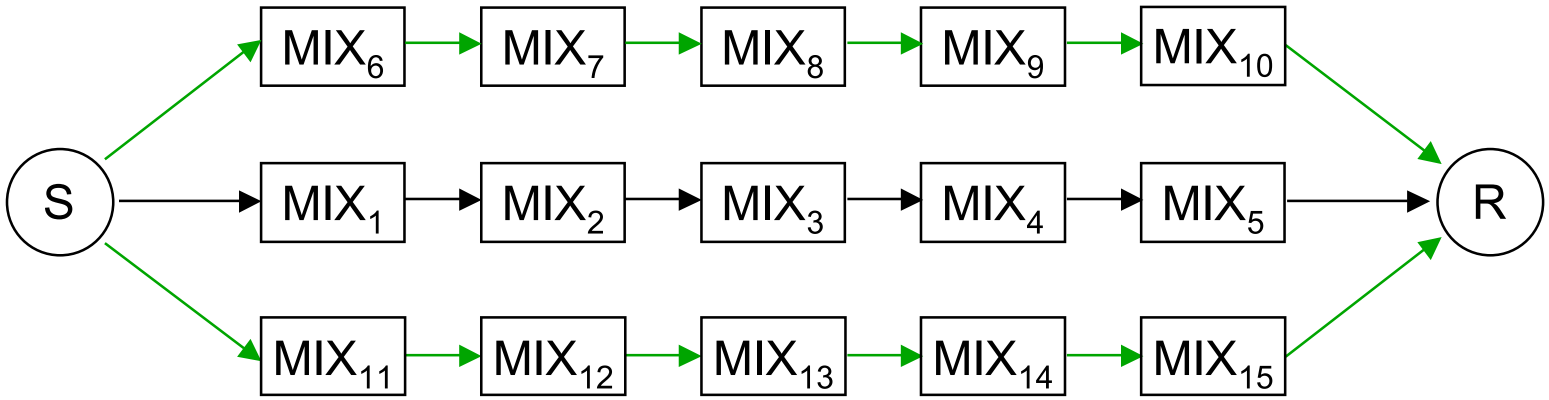
"Proof" of MIX cascade (cont.)



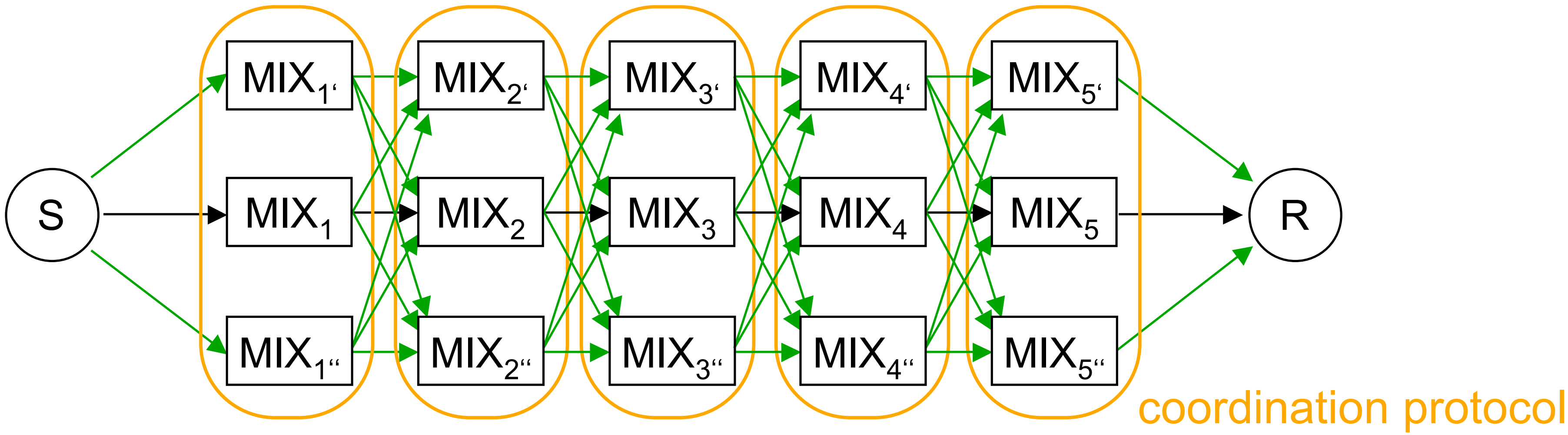
"Proof" of MIX cascade (cont.)



Fault-tolerance within the MIX-net (1985-1990)

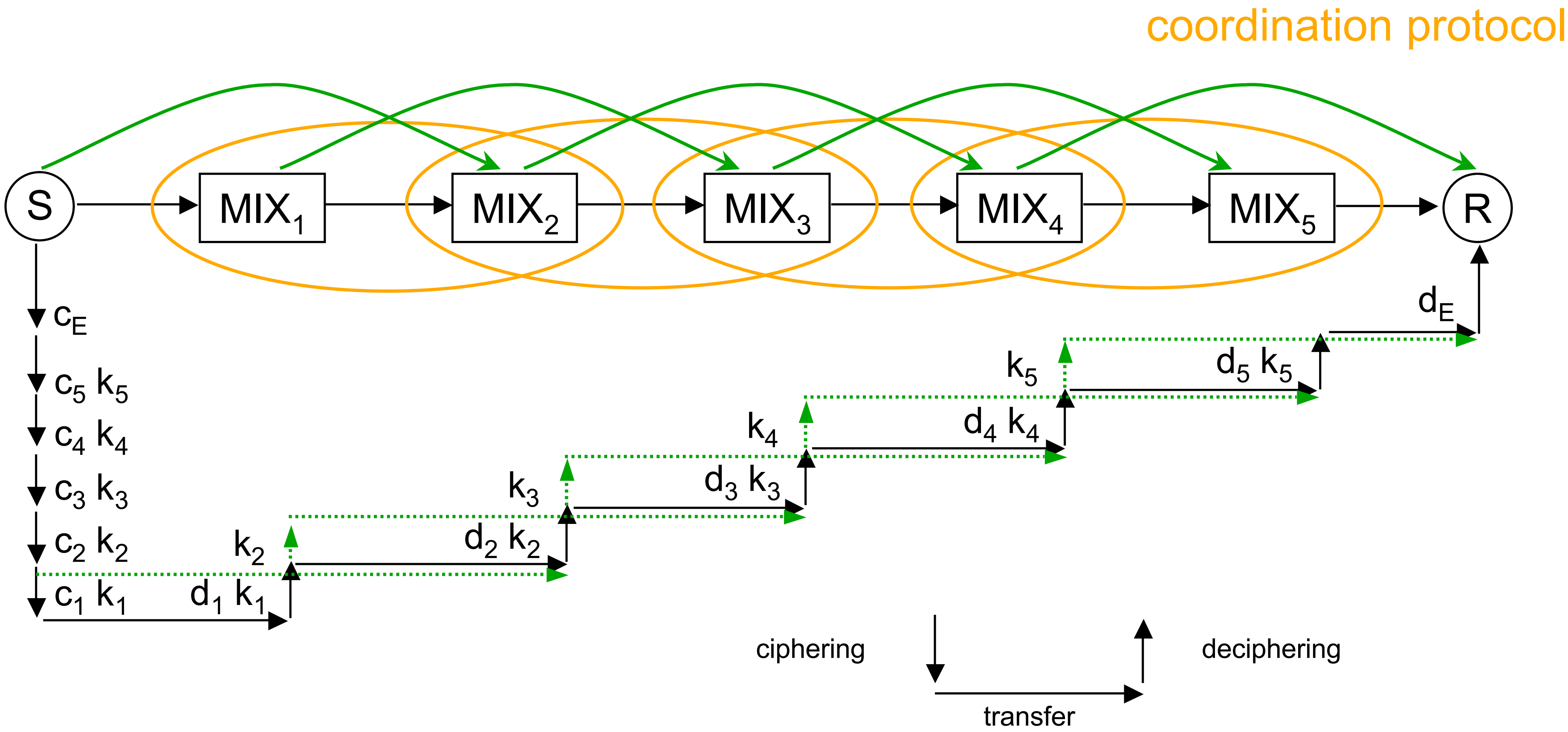


2 alternate paths through disjunct MIXes



$MIX_{i'}$ or $MIX_{i''}$ can replace MIX_i

Fault-tolerance within the MIX-net (cont.)



Single MIXes can be skipped

At which layer? (1985-1990)

OSI layers	Broadcast	MIX-net	DC-net	RING-net
7 application				
6 presentation				
5 session				
4 transport	implicit addressing			
3 network	broadcast	batch and change encoding		
2 data link			anonymous access	anonymous access
1 physical	channel selection		superpose messages and keys	digital signal regeneration
0 medium				ring

has to preserve anonymity against the communication partner

end-to-end encryption

has to preserve anonymity

can be built without regard to anonymity

Lessons I learned

1. strong (but completely hypothetical in 1985) **attacker models** got reality in the meantime, cf. interfaces for law enforcement in all communication networks; nevertheless, the research community mainly addresses weaker attacker models in the last 10 years than David Chaum and my group did 1983-1990
2. **Quality of Service** (QoS): delay very low + throughput high, otherwise anonymity and unobservability will never get a service to the masses, but the PET research community considers mainly P2P, i.e. ignores QoS, when the Internet community finally starts to get QoS aware (e.g. IP v6)
3. anonymity and unobservability work well with **isochronous traffic** (common in channel switched networks)
4. 2. and 3. suggest that the PET community will finally rediscover **isochronous (dummy) traffic** in future
5. the **interface** between anonymous communication and applications has to have **as less assumptions as possible**, cf. dummy traffic, static networks ...