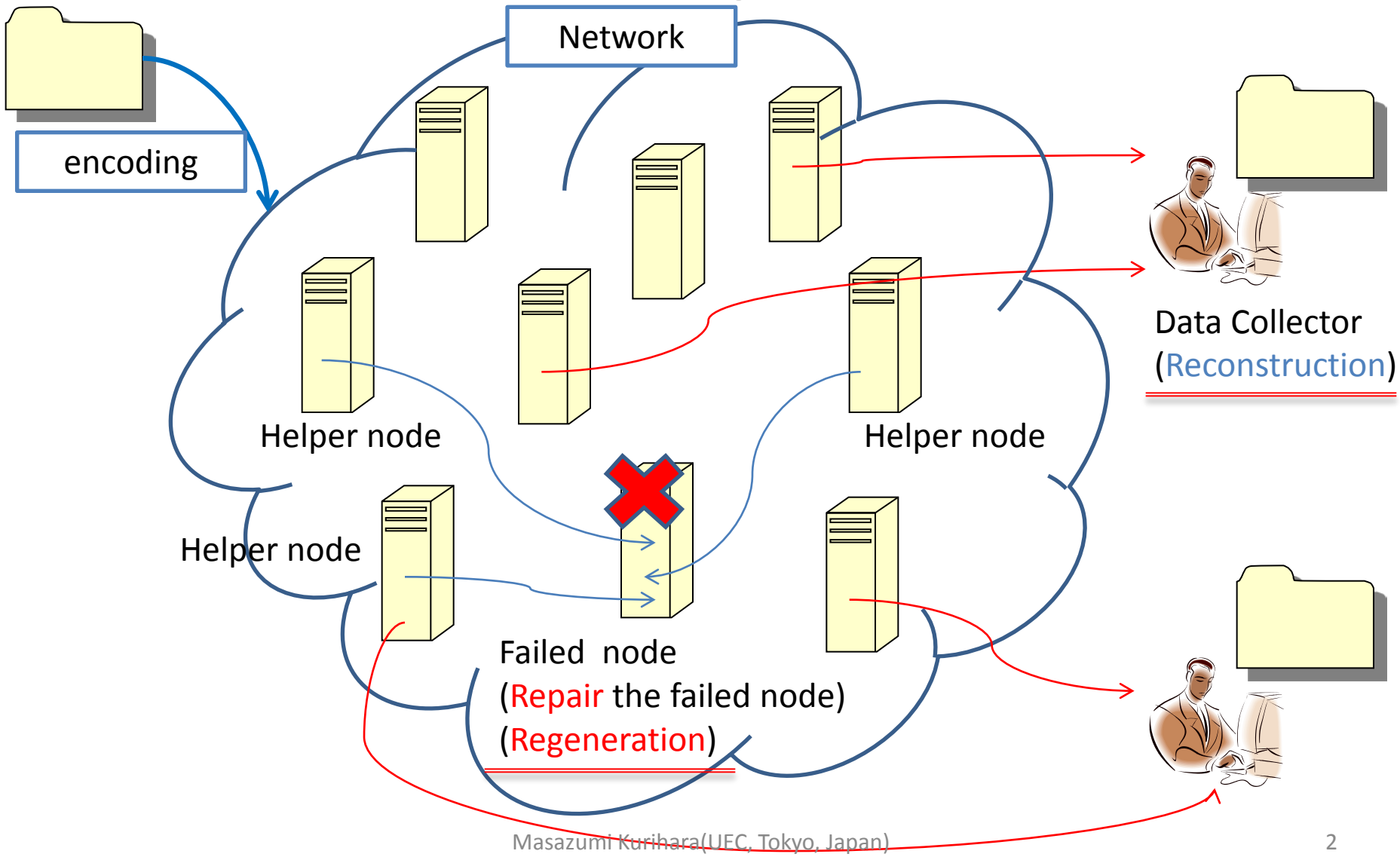
On Secret Sharing Schemes based on Regenerating Codes

Masazumi Kurihara

(University of Electro-Communications)

2012 IEICE General Conference, Okayama, Japan, 20-23, March, 2012.
(Proc. of 2012 IEICE General Conference, AS-2-1, pp.S17-S18)

Distributed Storage System (Secret Sharing Scheme ?)



Regenerating Codes

- A.G.Dimakis, P.B.Godfrey, Y.Wu, M.J.Wainwright, K.Ramchandran, "Network Coding for Distributed Storage Systems," IEEE IT Trans. Vol.56, no.9, 2010. → [Dimakis, et al.,2010]

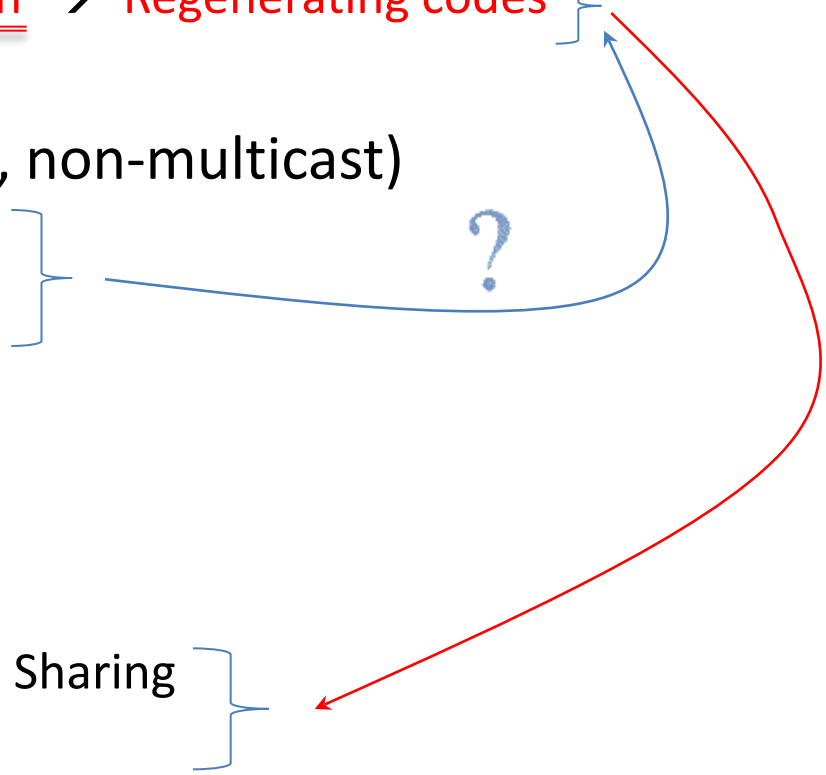
- Repair Problem (--- symmetry ---)
  -- Repairing a failed node
  -- Regenerating data that was stored in the failed node

Contents

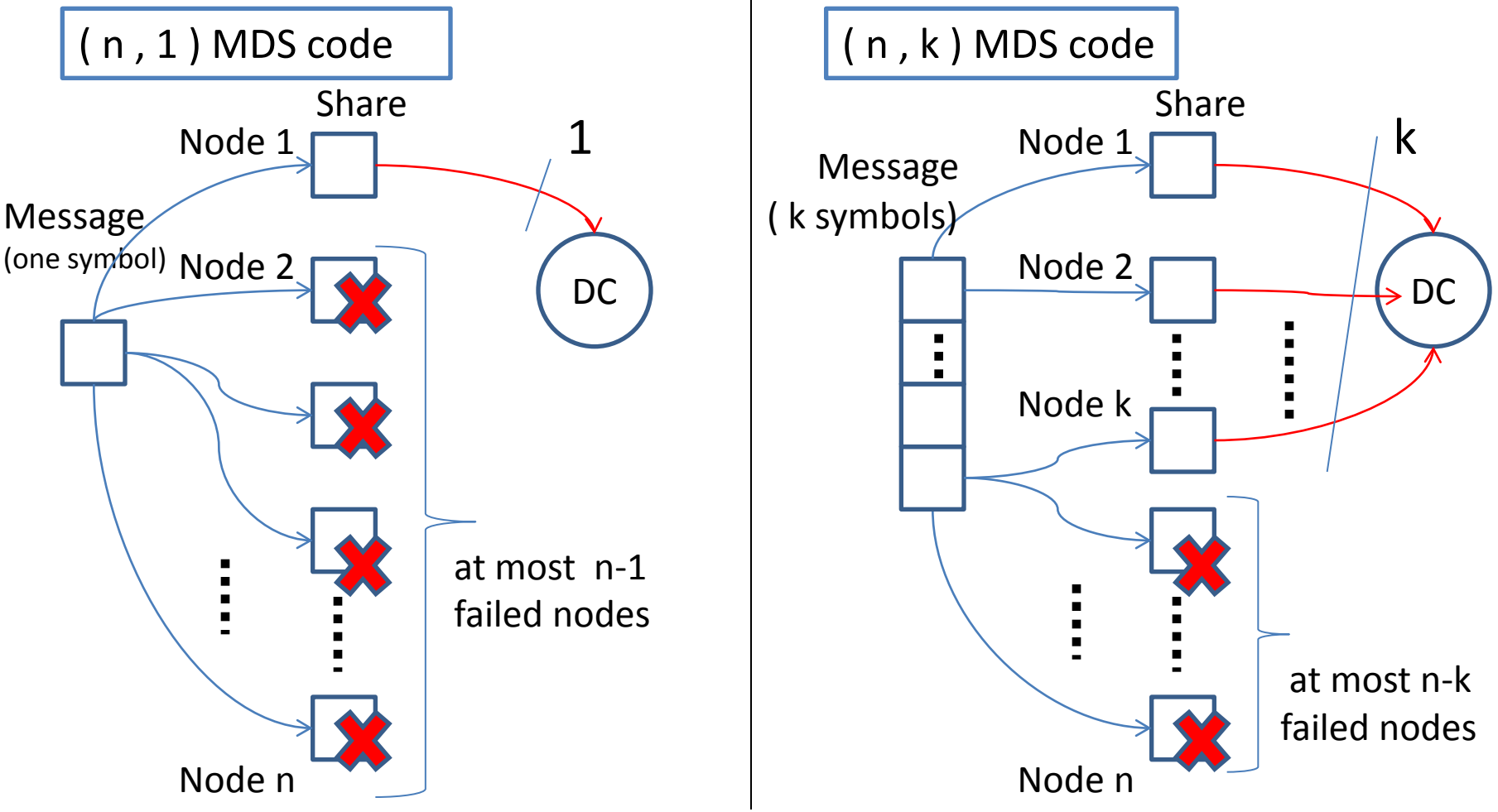
1. Concept of regenerating codes
2. Relation between network-coding and distributed-storage (The results of Dimakis, et al.)
3. Several current regenerating codes
4. Secret sharing scheme based on regenerating codes (Secure regenerating codes)

Keywords and their relation

- Codes for Distributed Storage
  - Reconstruction(Recovery) → Erasure codes (MDS codes, RS codes, etc.)
  - Reconstruction and Regeneration → Regenerating codes
- Network Coding (for multicast, non-multicast)
  - Liner network Coding
  - Random linear network Coding
- Secret Sharing
  - MDS-code-based Secret Sharing
  - Regenerating-code-based Secret Sharing (Secure Regenerating Codes)



Distributed Storage using (n , k) MDS codes

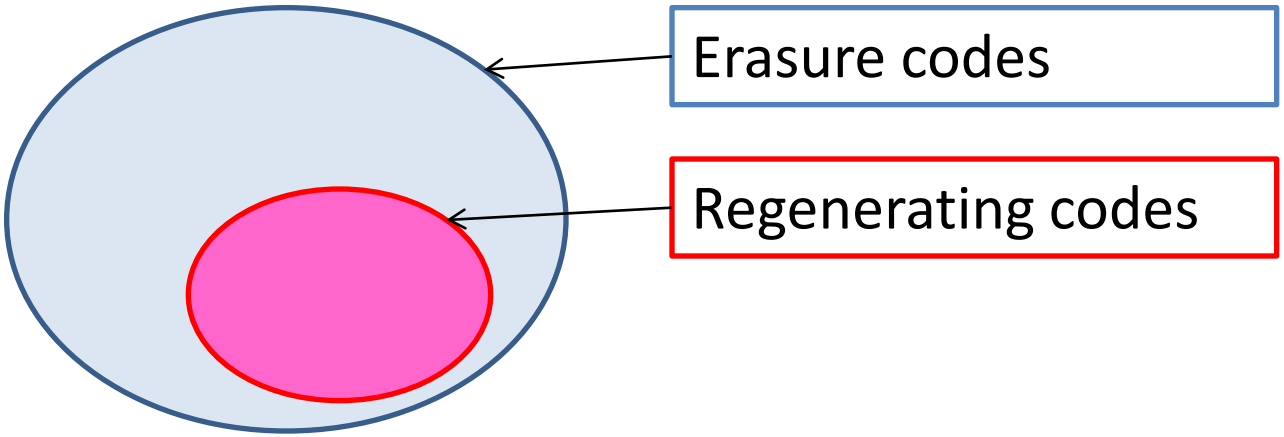


Tradeoff between Redundancy and Reliability

Performance metric

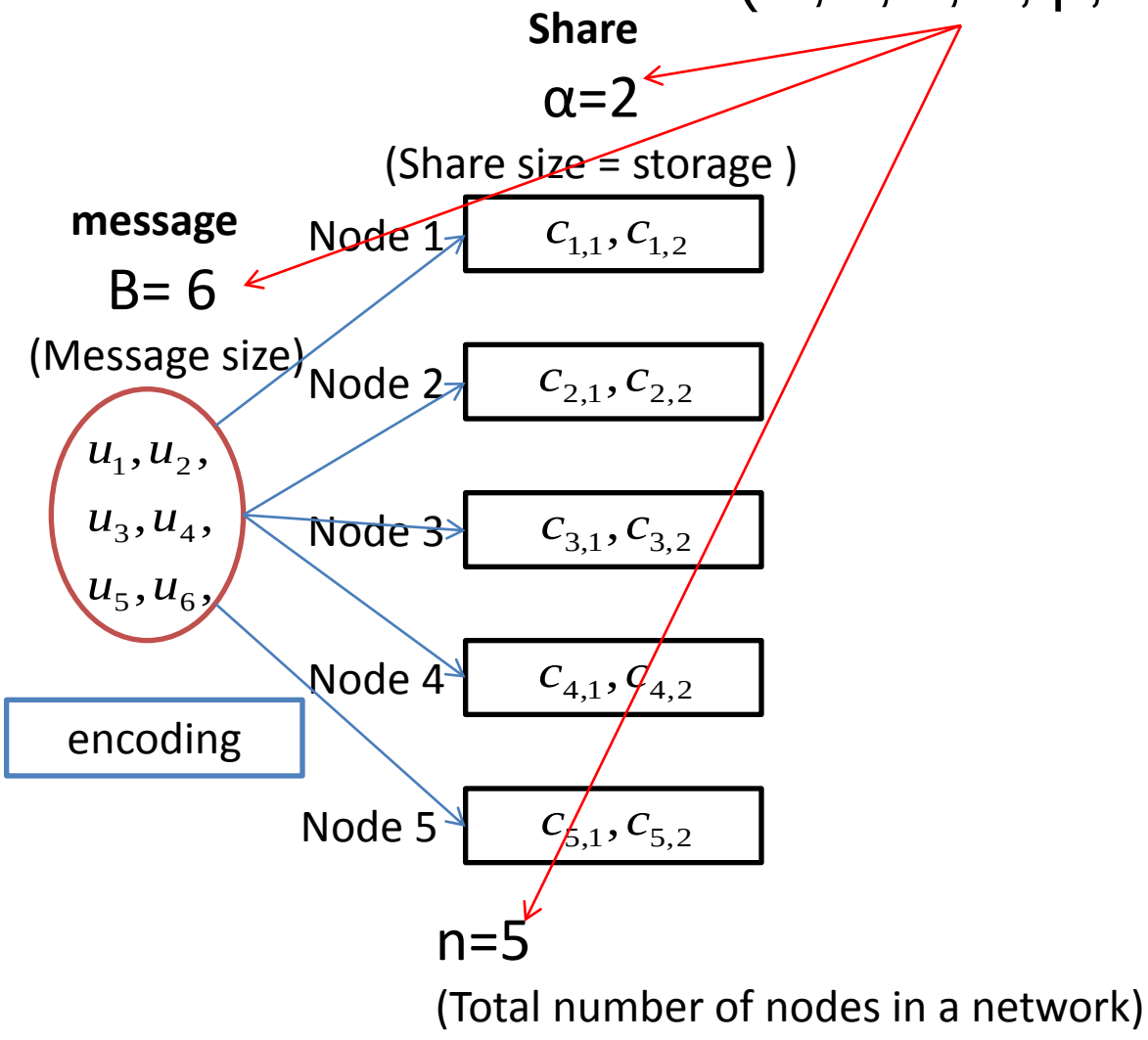
Regenerating Codes

- Collection of six parameters (n, k, d, α, β, B)
- Reconstruction property
  - A data collector can reconstruct the original data by using the data downloaded from any k active nodes.
- Regeneration property
  - A failed node can regenerate the data, which was stored in itself, by using the data downloaded from any d active nodes.



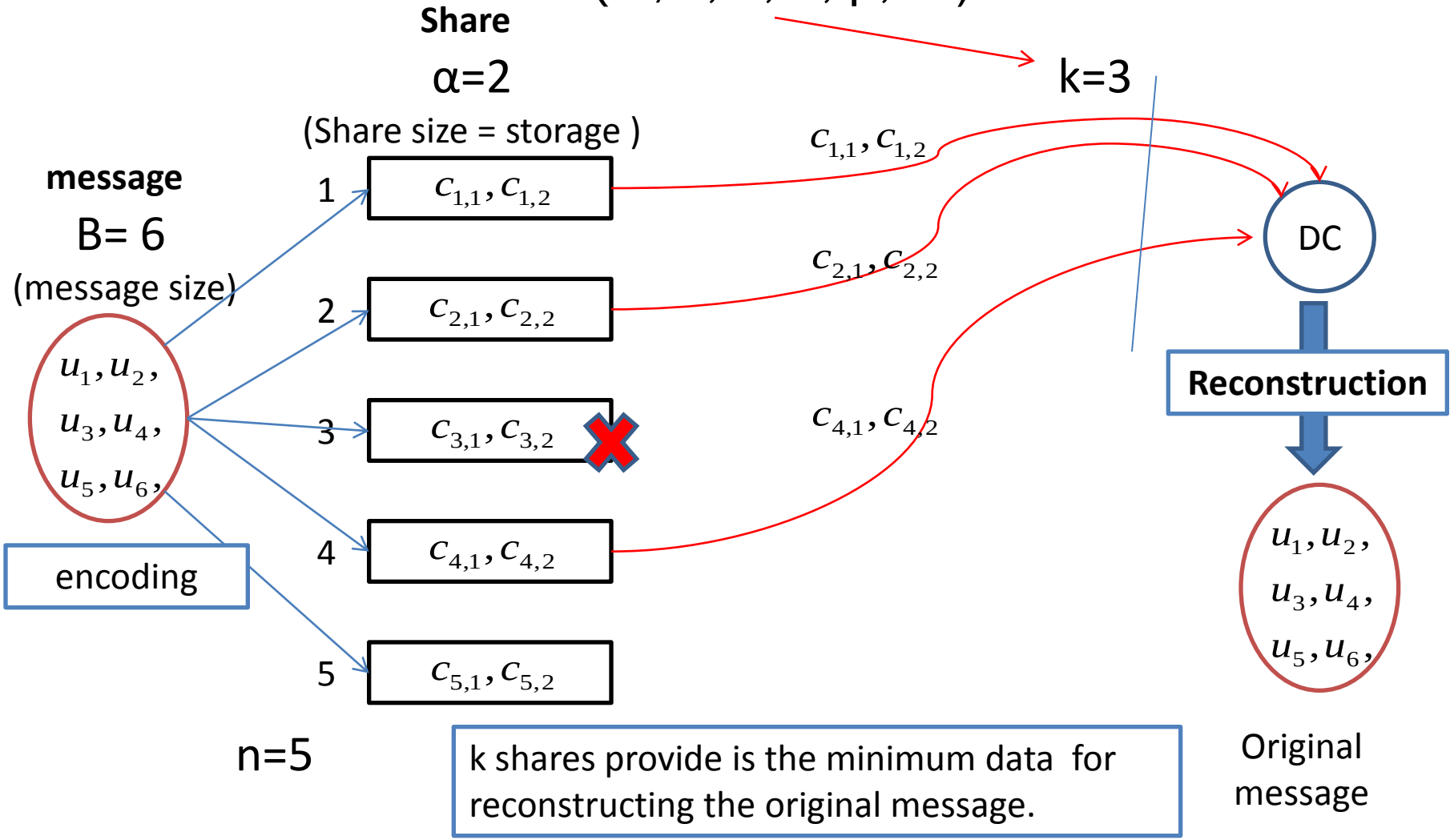
Message, Encoding , and Shares

(n, k, d, α, β, B)

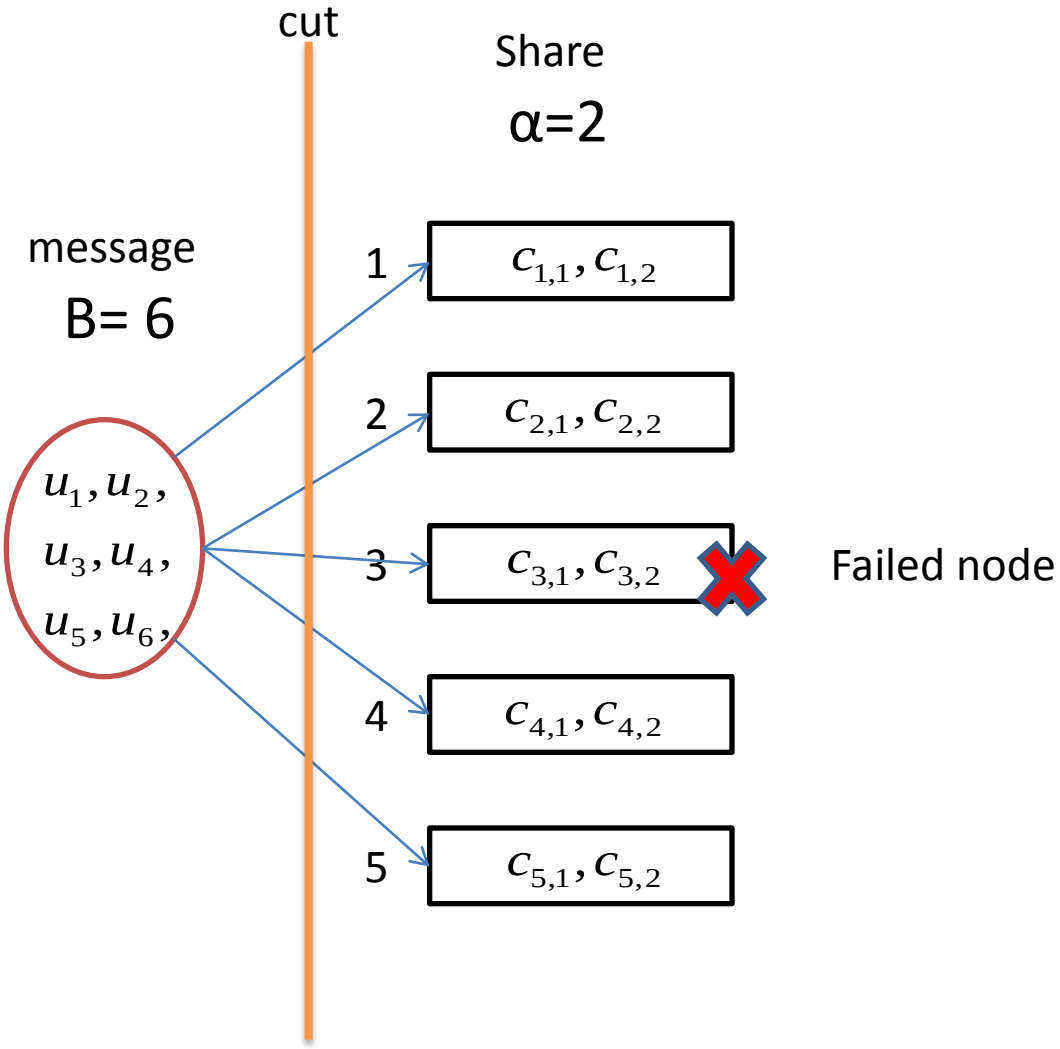


Reconstruction Property(k)

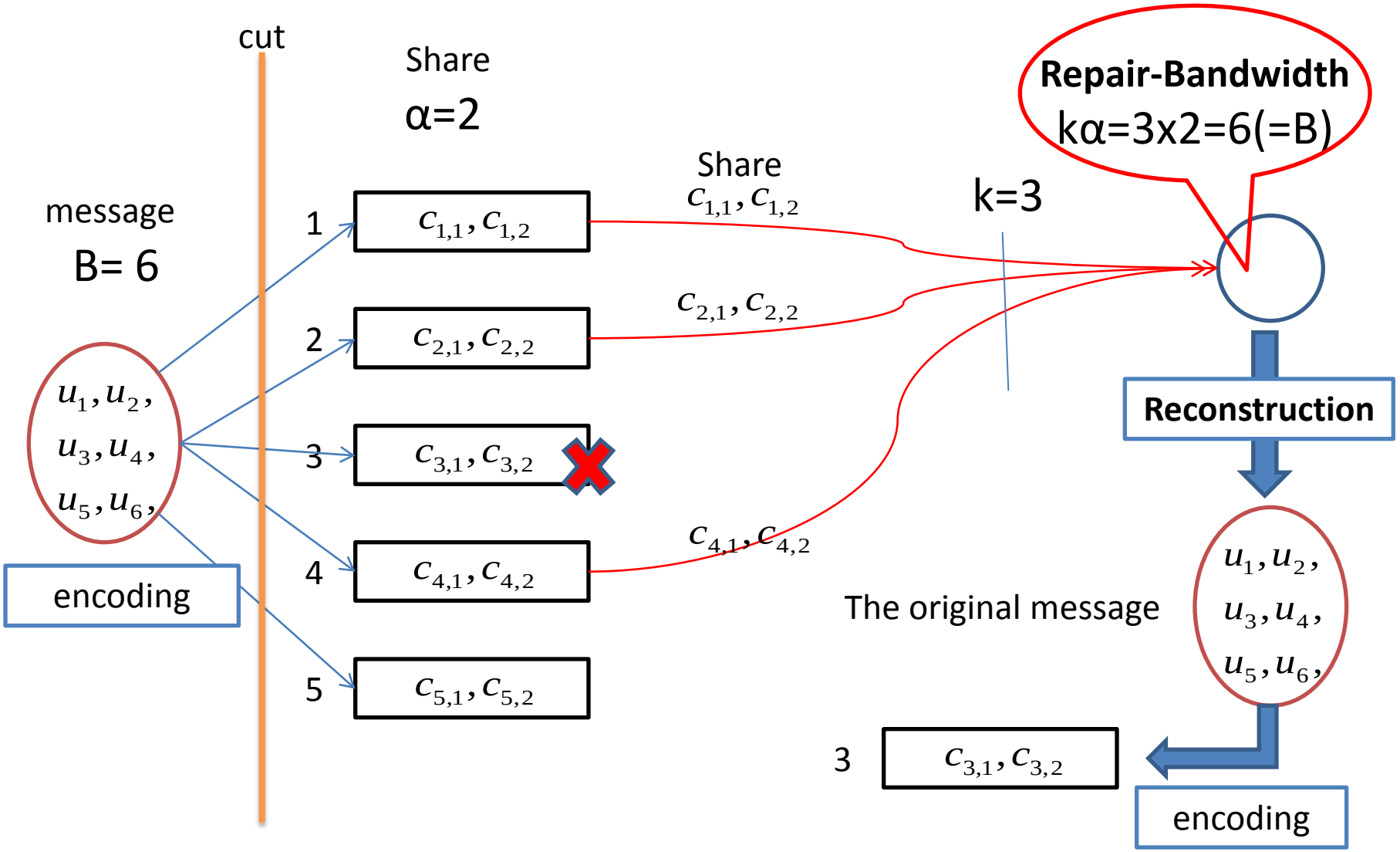
(n, k, d, α, β, B)



Maintaining the reliable distributed storage system (Repair a failed node, i.e., regenerate the share of it)



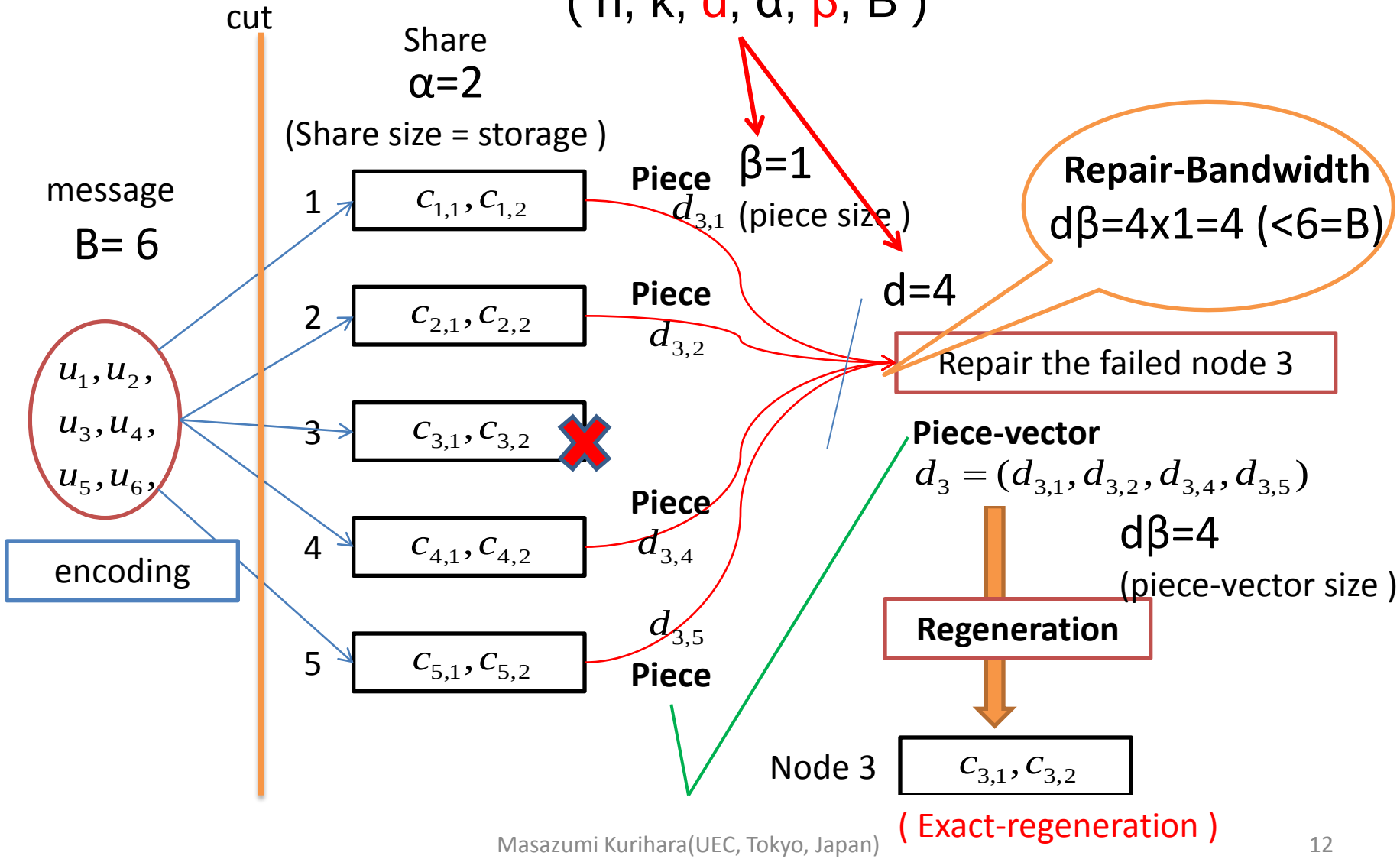
Regeneration by reconstruction



Point (d ≧ k)

Regeneration Property (d and β)

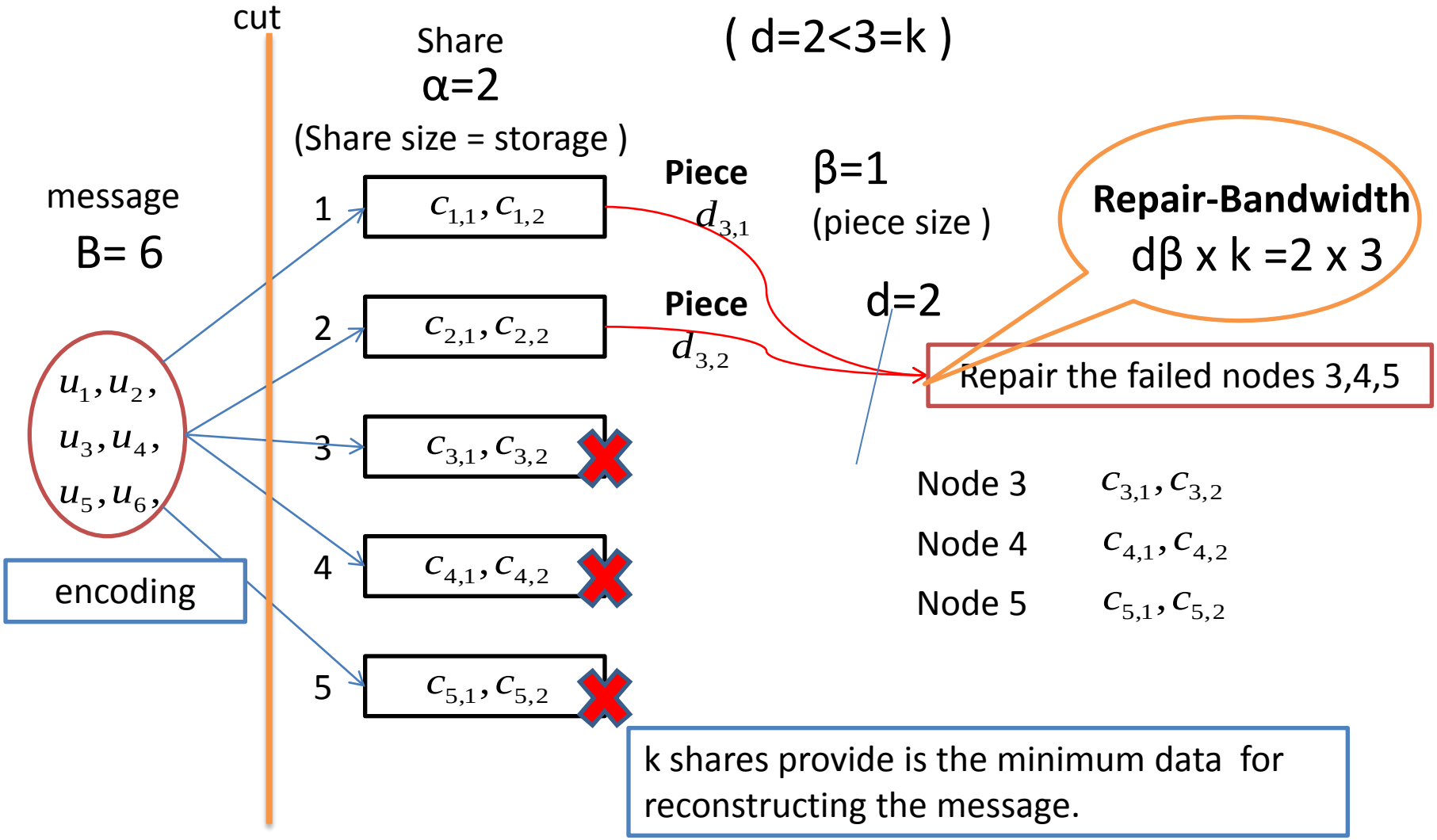
(n, k, d, α, β, B)



skip

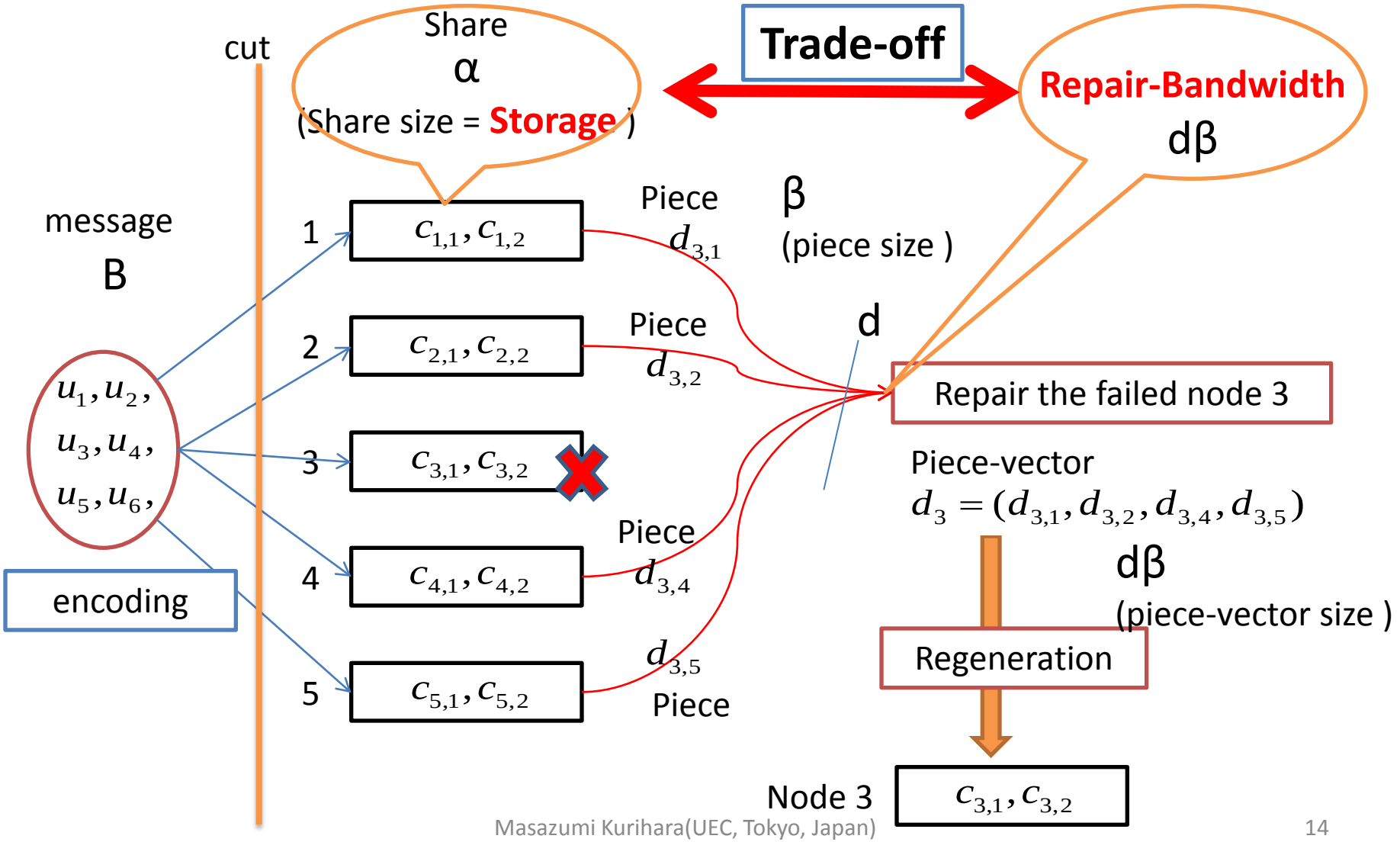
Why d ≧ k ?
If d<k, then …

(d=2<3=k)

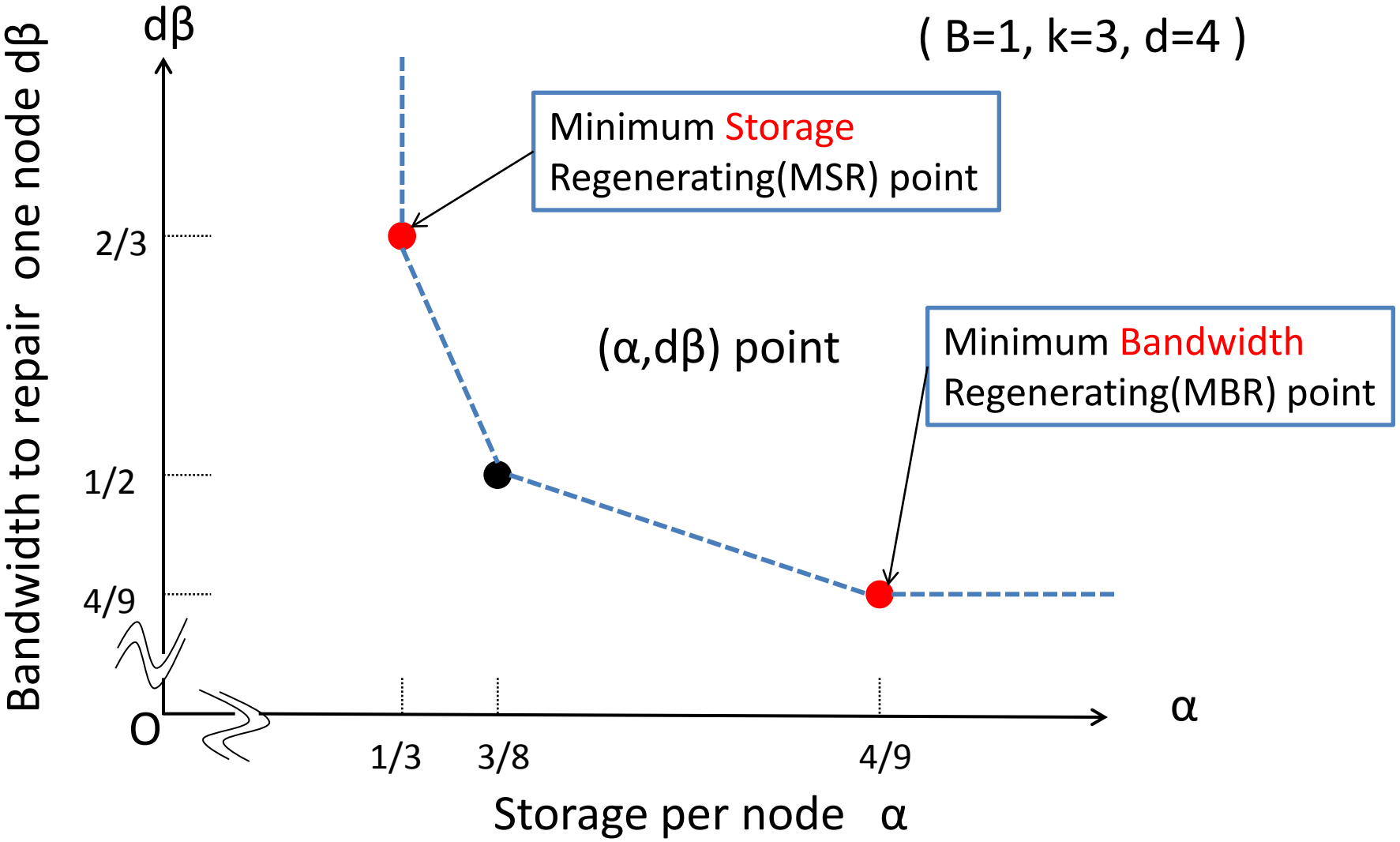


1. Reducing the repair-bandwidth
2. Tradeoff between Storage, α, and Repair-Bandwidth, dβ

(Fixed k and d)



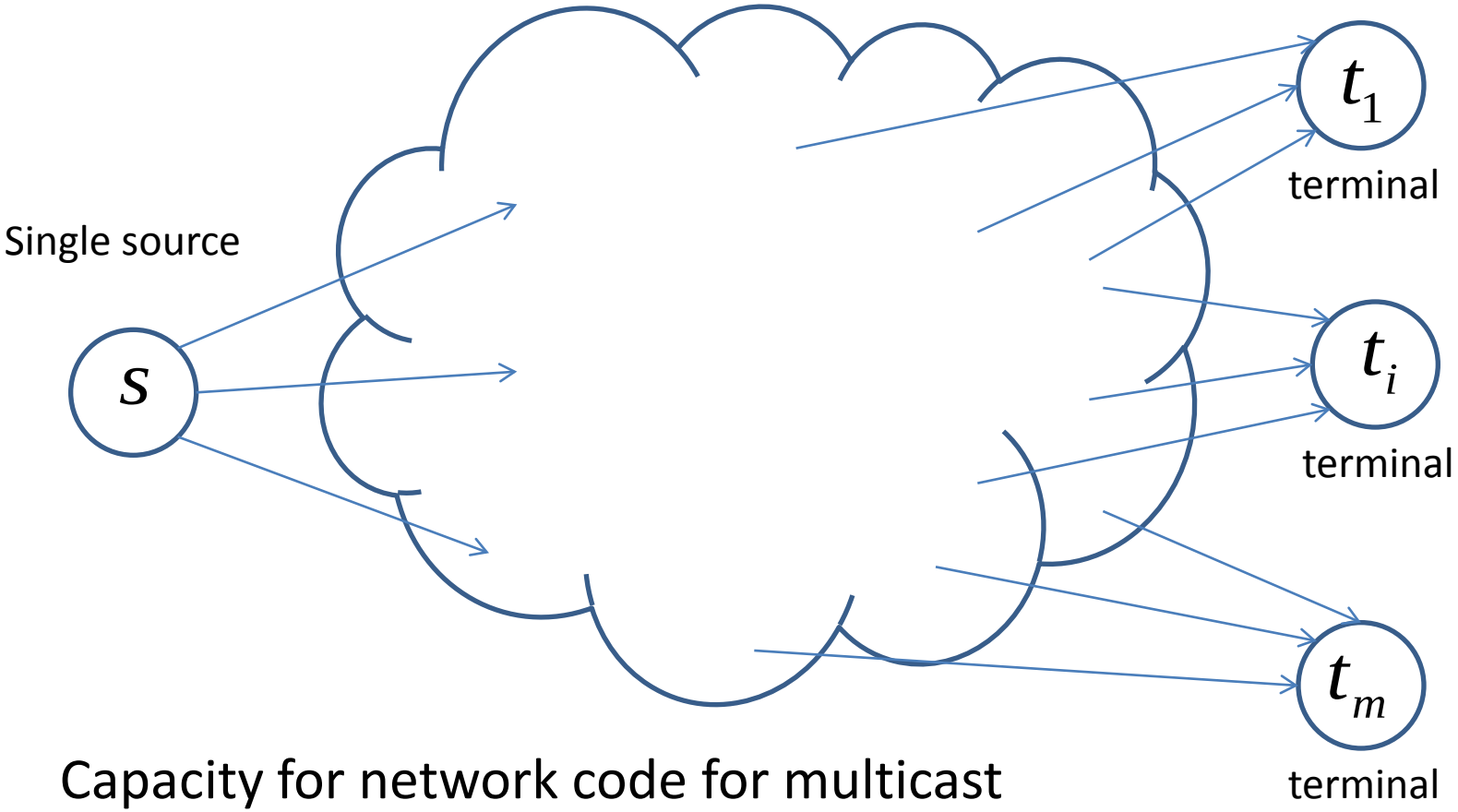
Tradeoff between Storage, α, and Repair-Bandwidth, dβ



Contents

1. Concept of regenerating codes
2. Relation between network-coding and distributed-storage
3. Several current regenerating codes
4. Secret sharing scheme based on regenerating codes
   (Secure regenerating codes)

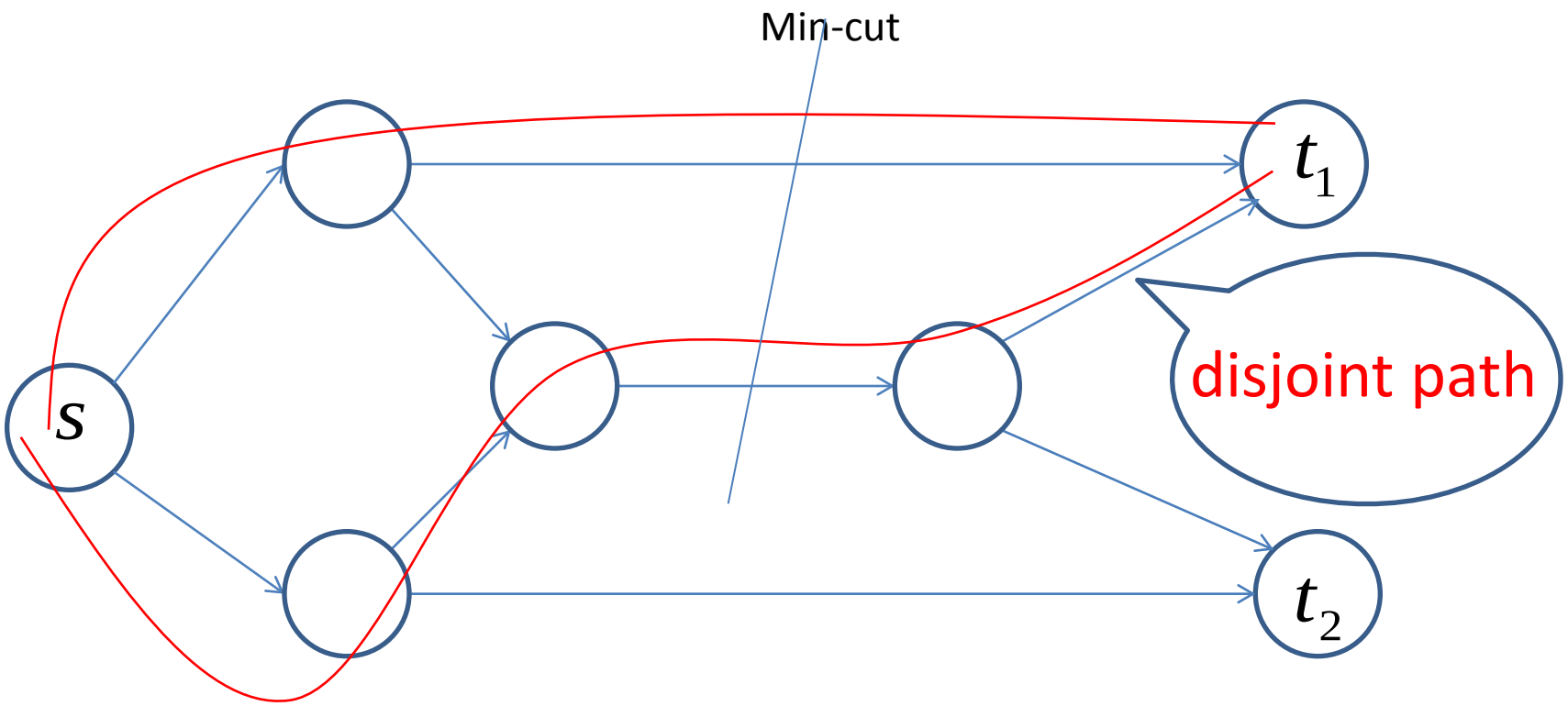
(Linear) Network Coding for multicast



Capacity for network code for multicast

$$\min\{\text{maxflow}(s,t_i), i=1,2,\ldots,m\}$$

Max-flow min-cut theorem

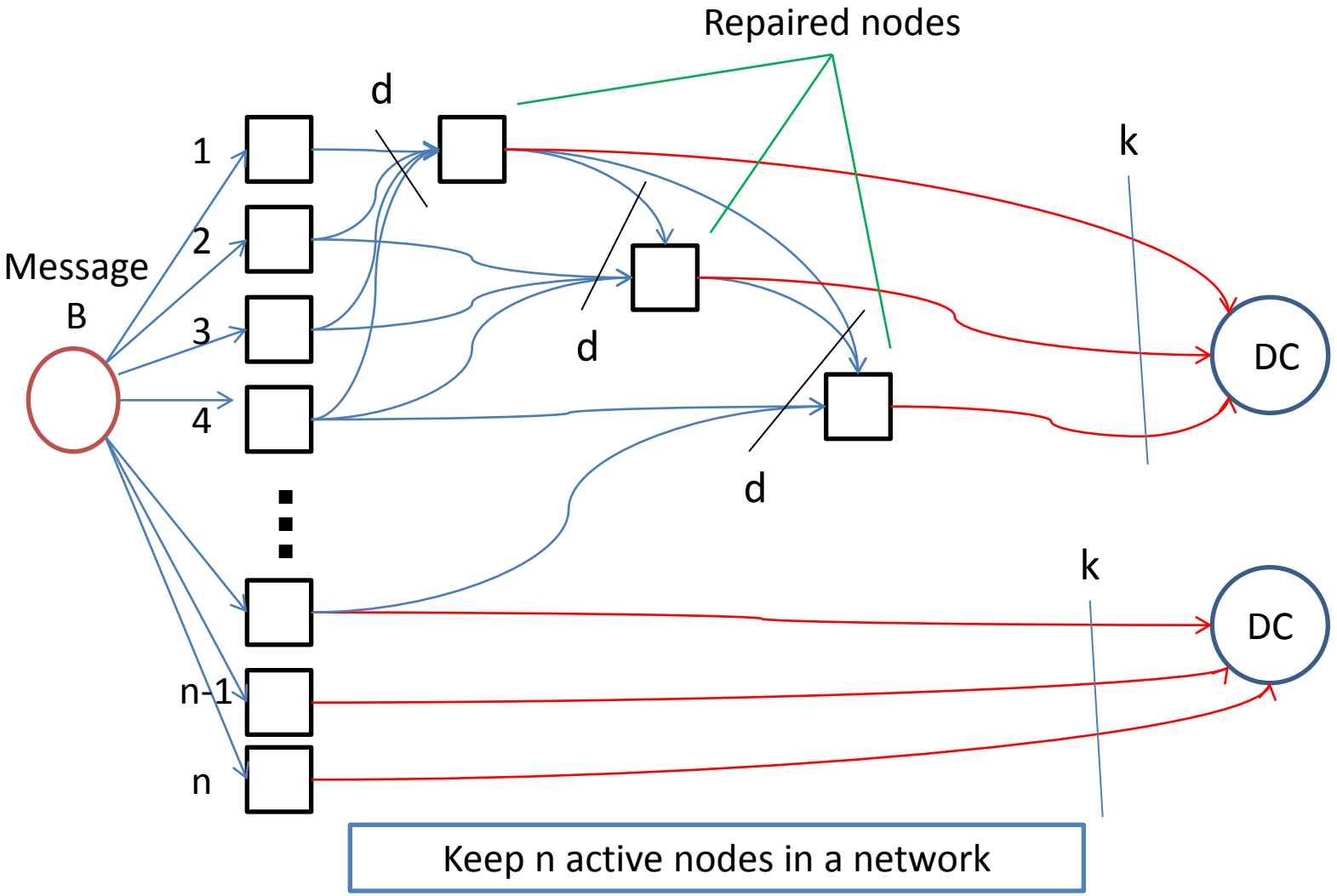


Max-flow from source s to terminal t_{1}

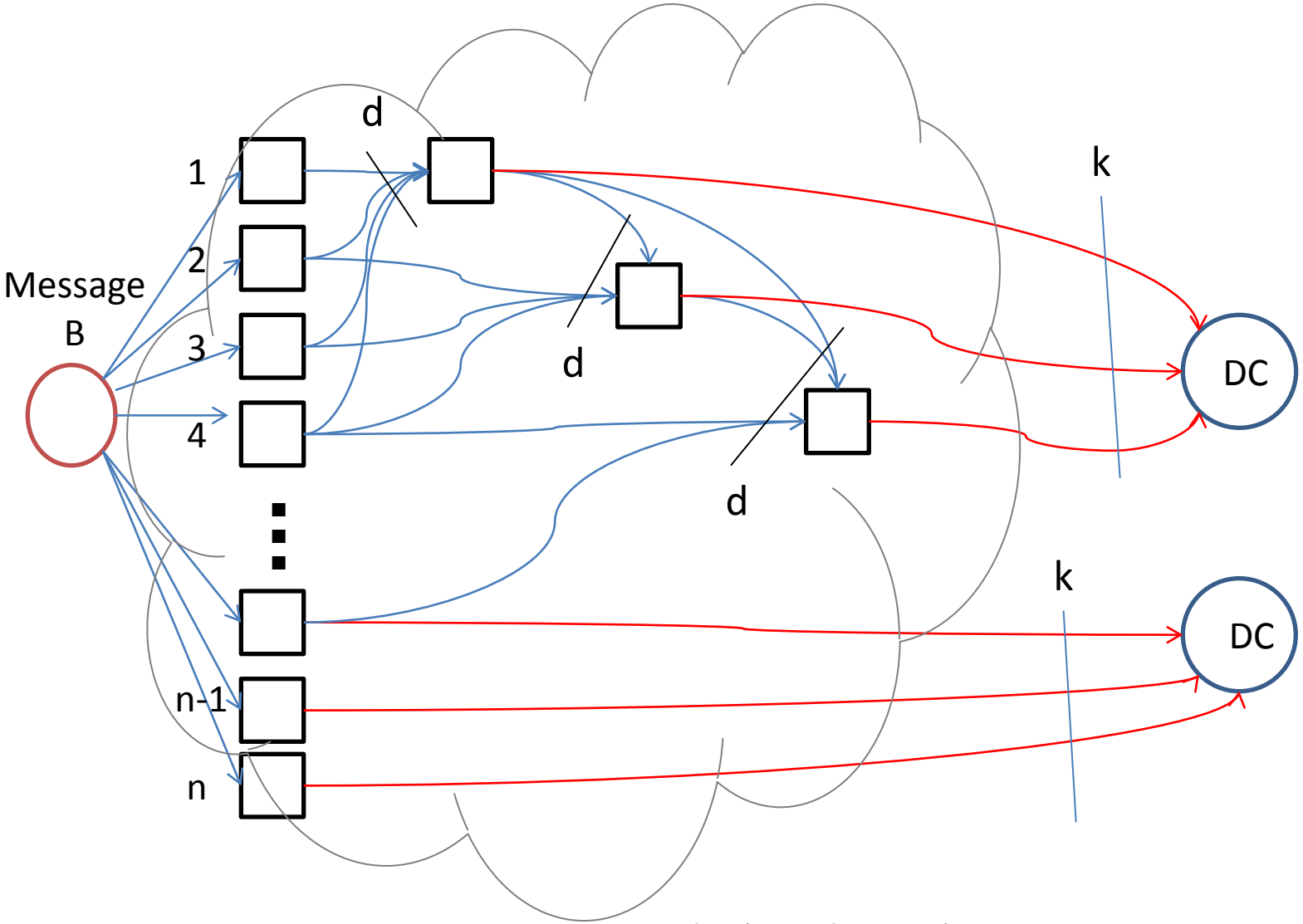
$$\mathrm{maxflow}(s, t_1) = 2$$

Information flow graph

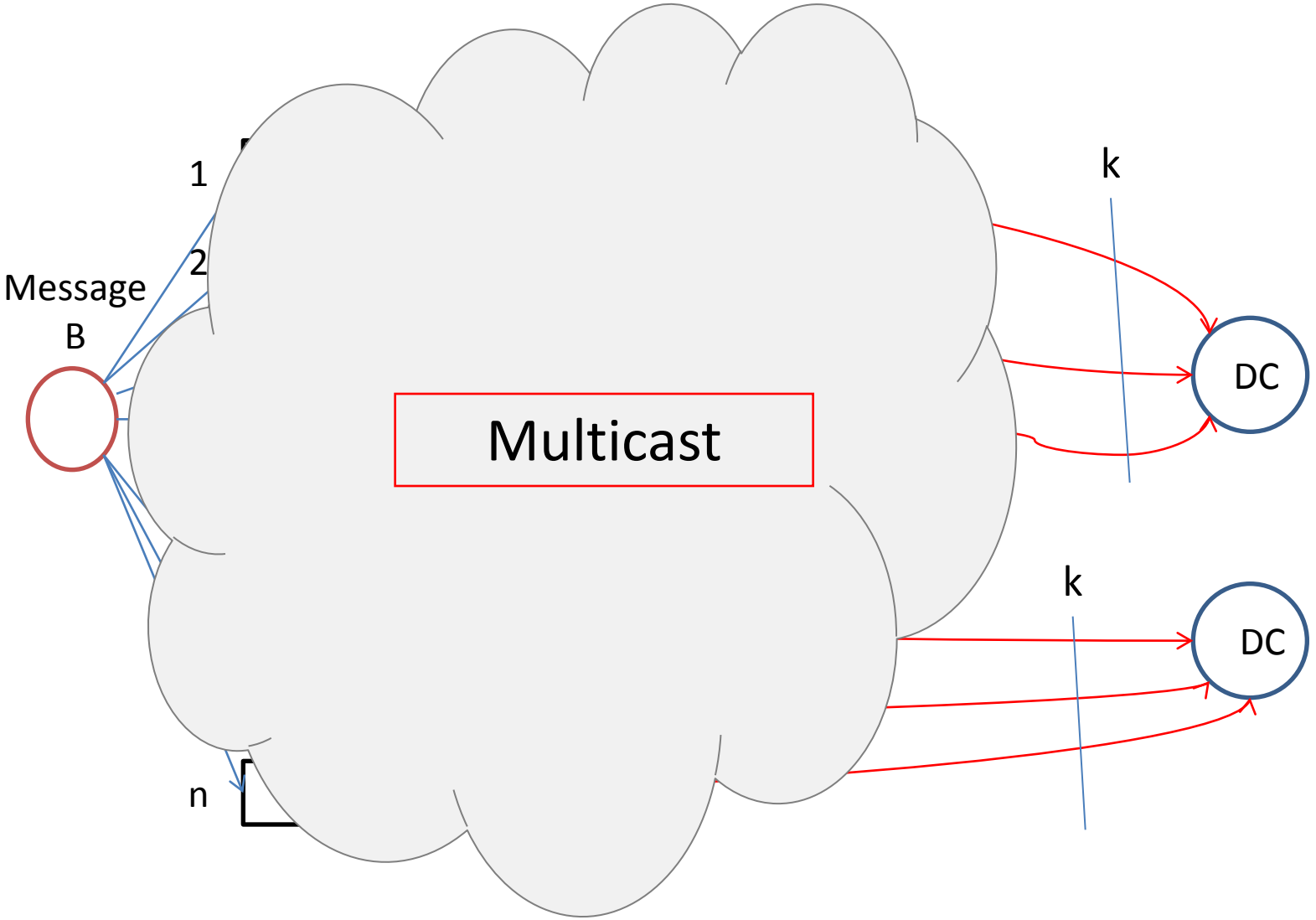
Repairable distributed storage system (Network coding for multicast)(1/3)



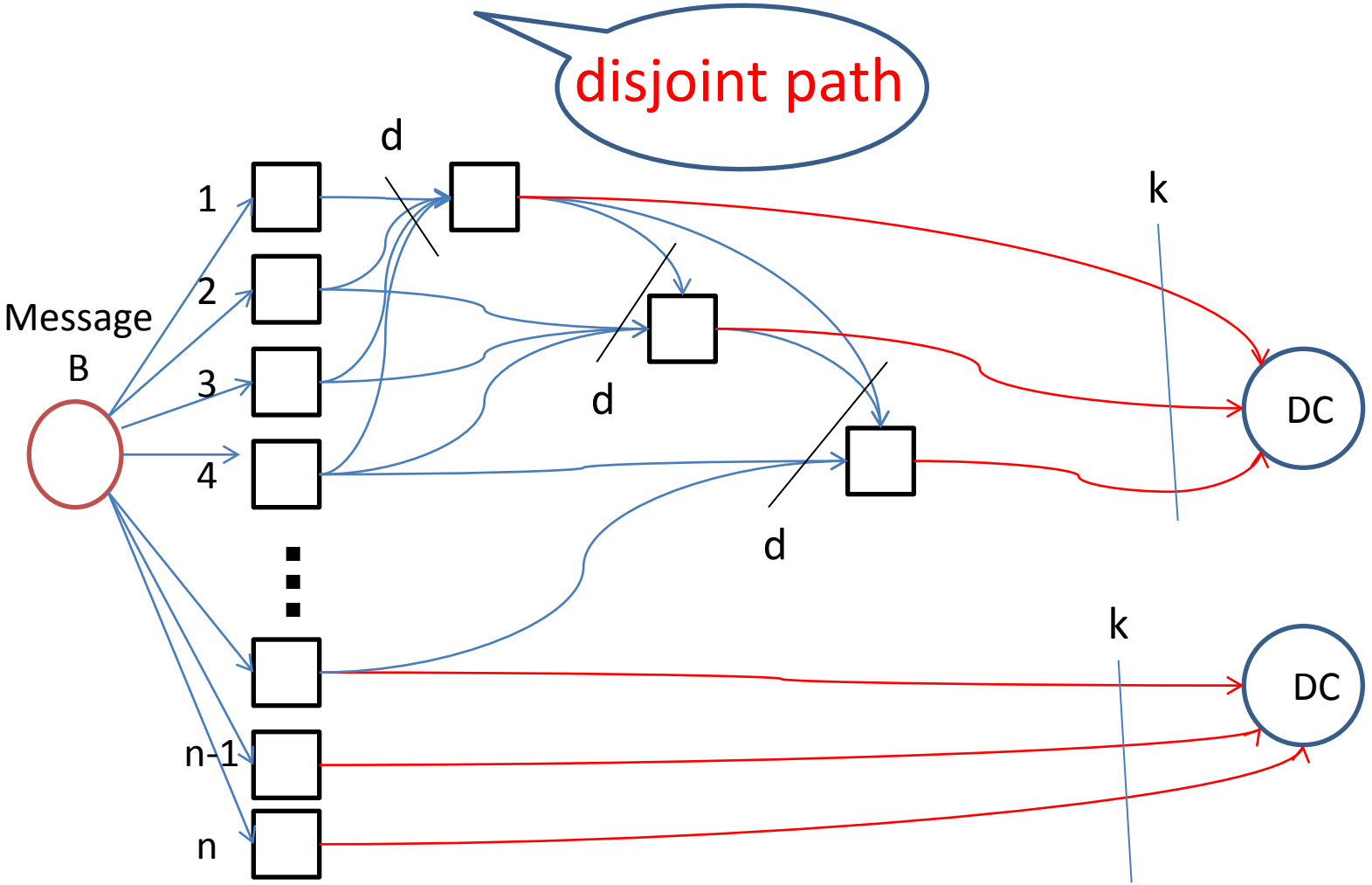
Repairable distributed storage system (Network coding for multicast)(2/3)



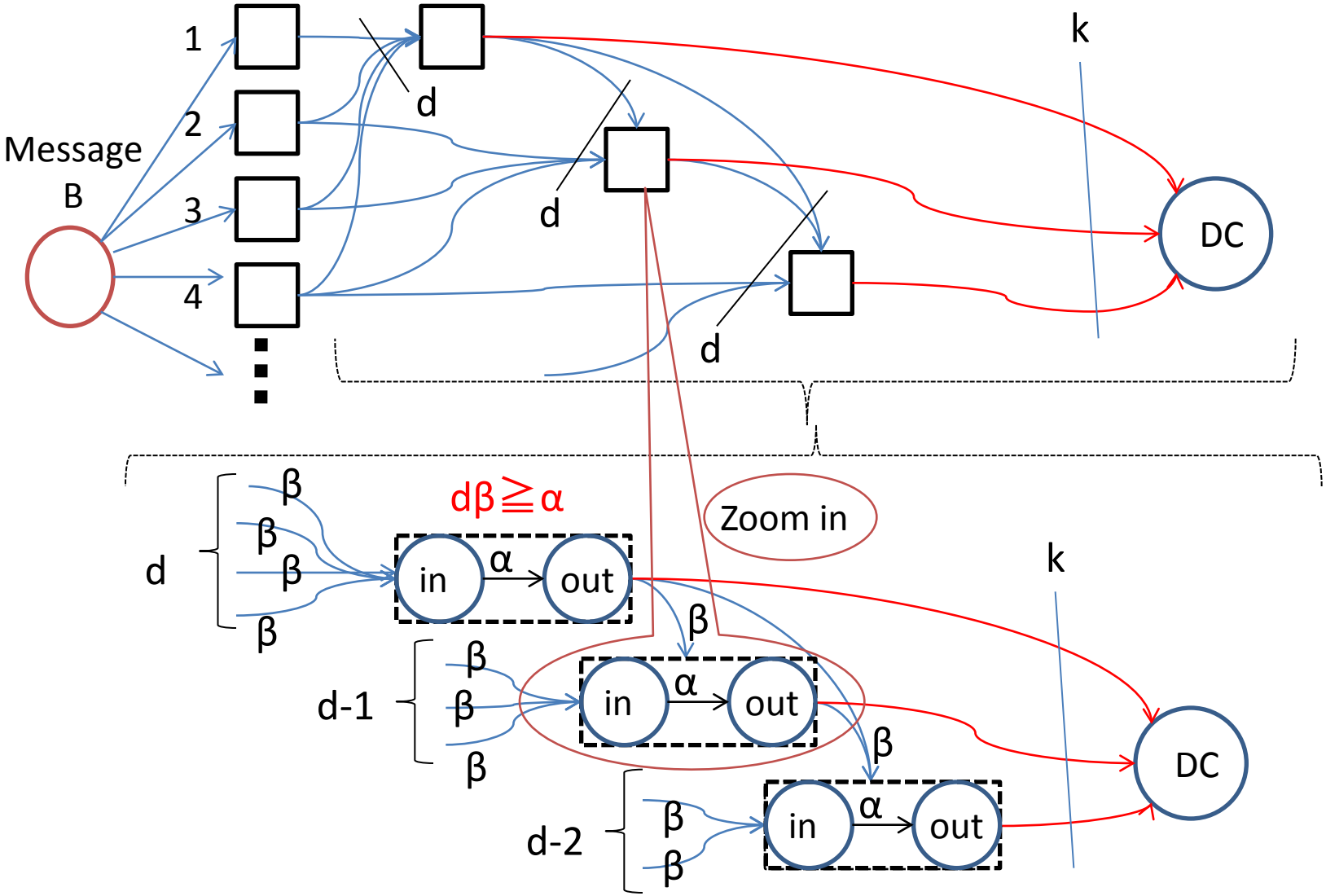
Repairable distributed storage system (Network coding for multicast)(3/3)



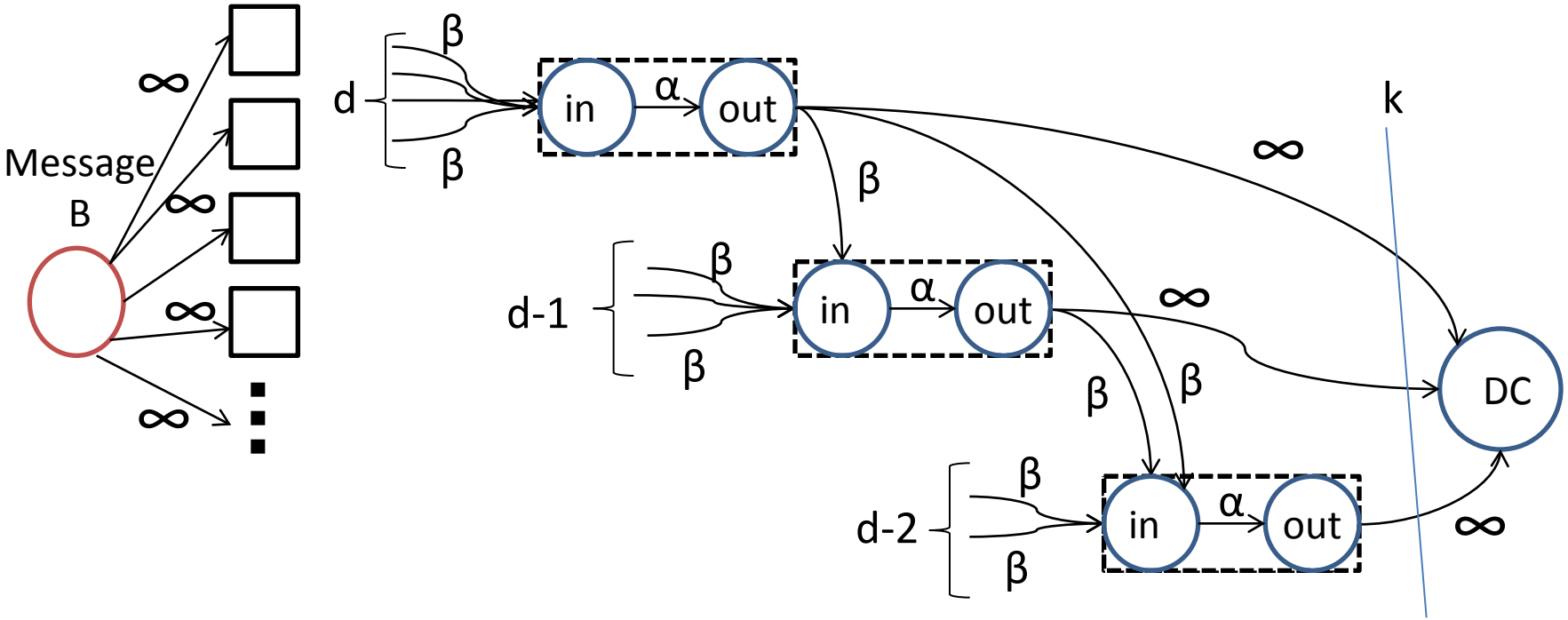
Capacity for (n,k,d,α,β,B)Regenerating Codes(1/5)



Capacity for (n,k,d,α,β,B)Regenerating Codes(2/5)



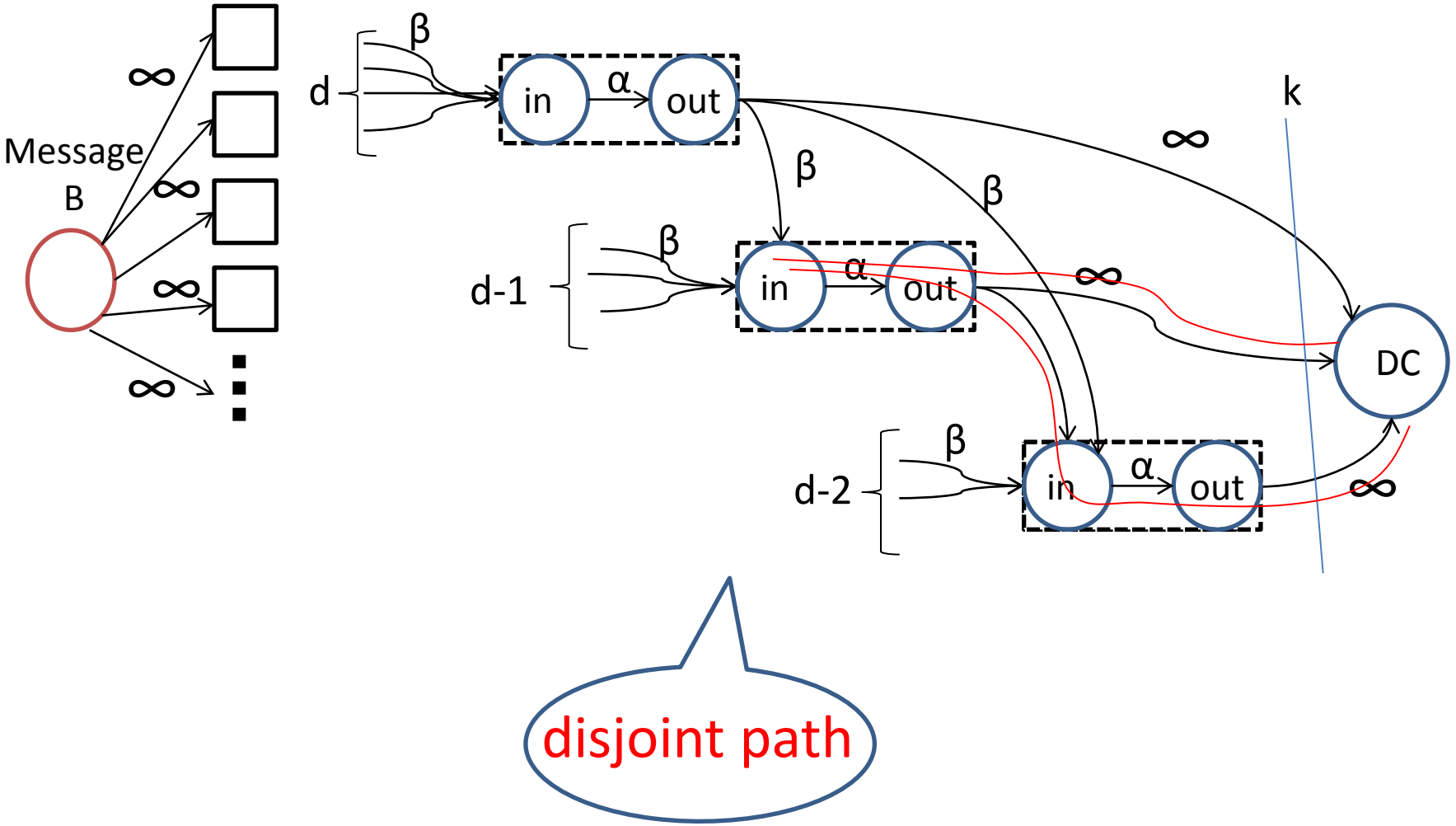
Capacity for (n,k,d,α,β,B)Regenerating Codes(3/5)



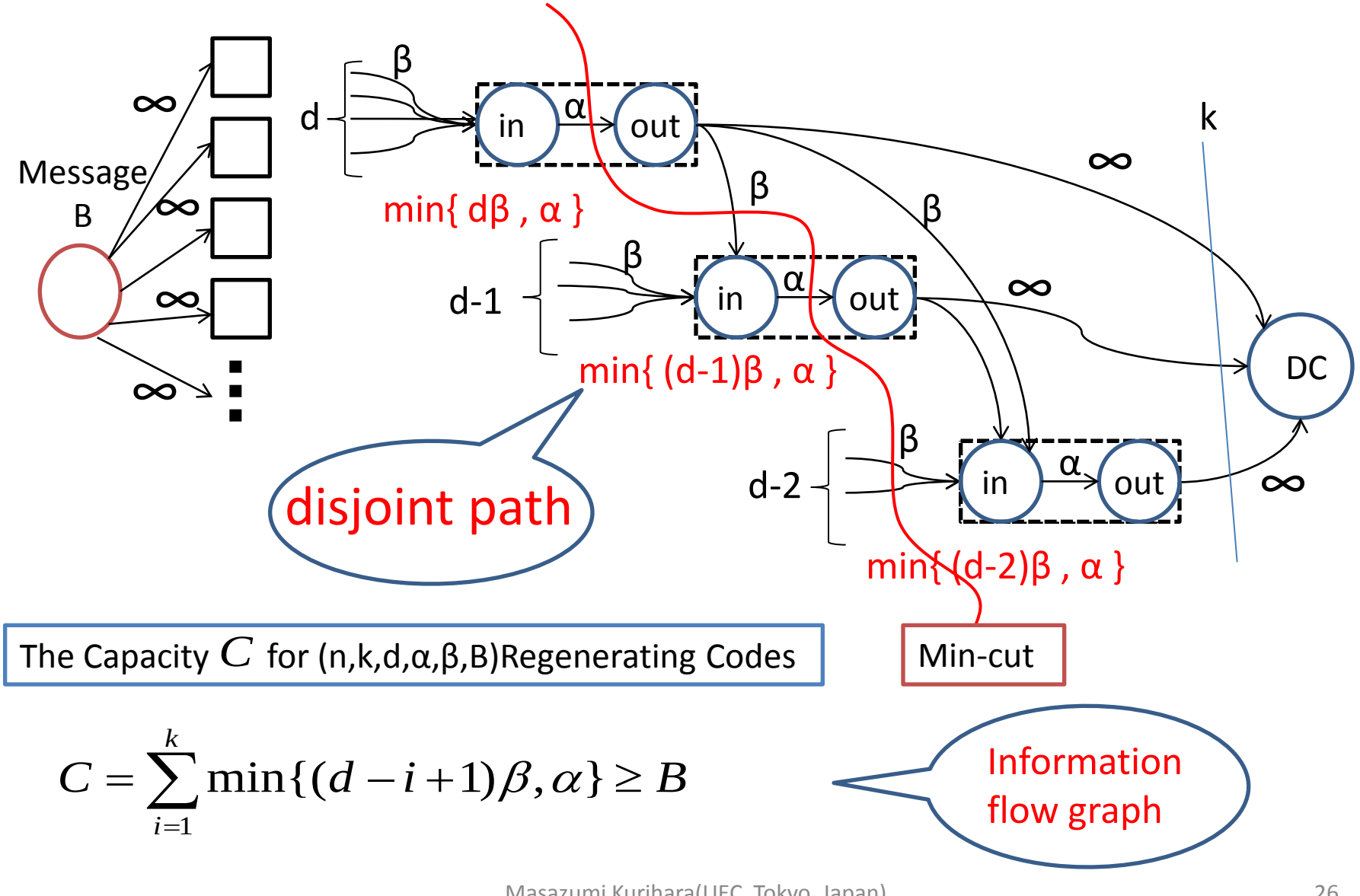
disjoint path

Flow from Source to DC

Capacity for (n,k,d,α,β,B)Regenerating Codes(4/5)



Capacity for (n,k,d,α,β,B)Regenerating Codes(5/5)



The Capacity C for (n,k,d,α,β,B)Regenerating Codes

$$C = \sum_{i=1}^{k} \min\{(d-i+1)\beta, \alpha\} \geq B$$

Information flow graph

MSR and MBR points (α,dβ)

- Capacity for (n,k,d,α,β,B) regenerating codes

$$C = \sum_{i=1}^{k} \min\{(d-i+1)\beta, \alpha\}$$

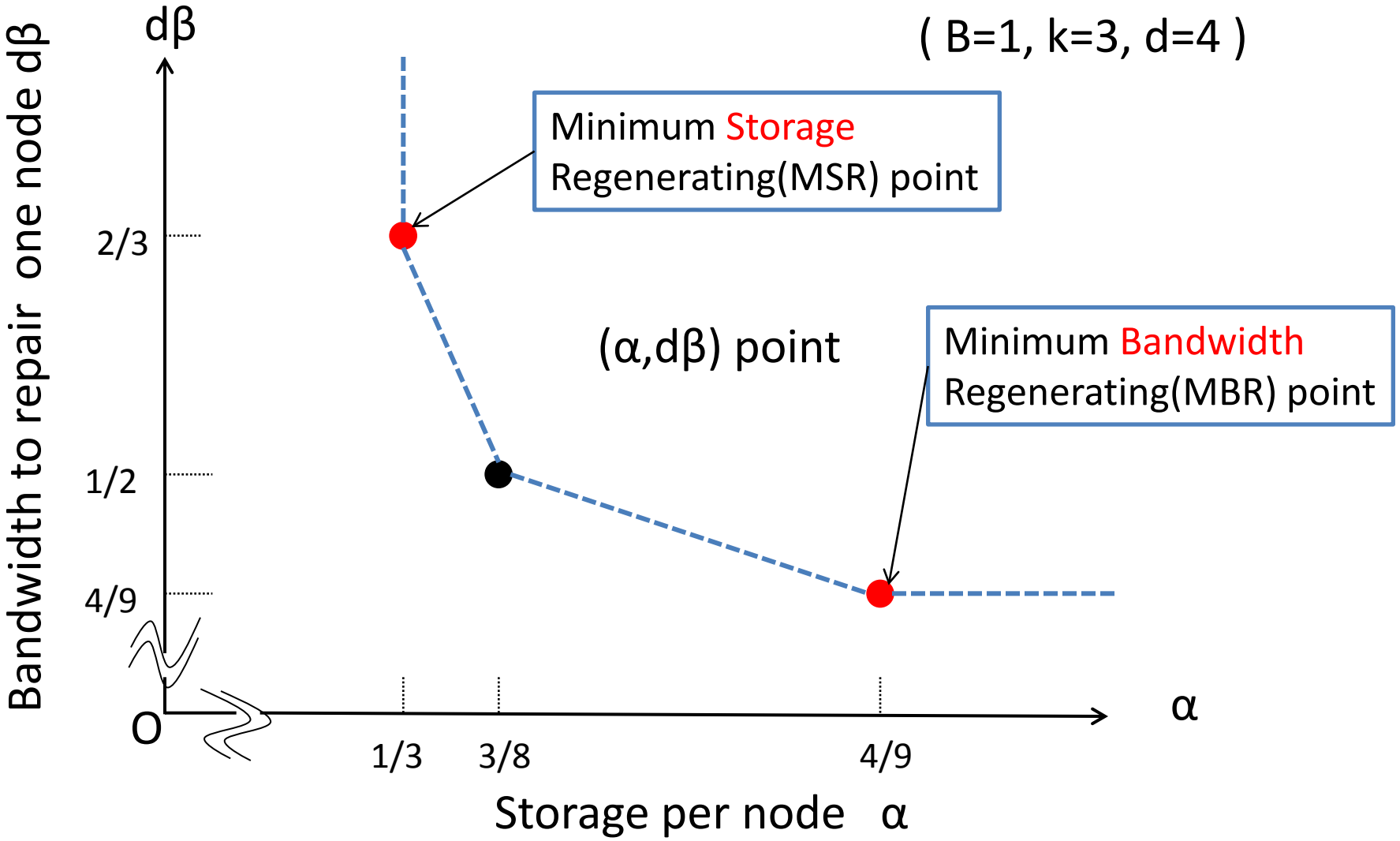
- Minimum Storage Regenerating(MSR) point

$$\left(\alpha = \frac{B}{k}, \quad d\beta = d\frac{\alpha}{(d-k+1)} \right)$$

- Minimum Bandwidth Regenerating(MBR) point

$$\left(\alpha = d\beta, \ d\beta = d\frac{2B}{k(2d-k+1)} \right)$$

Tradeoff between Storage, α, and Repair-Bandwidth, dβ



Contents

1. Concept of regenerating codes
2. Relation between network-coding and distributed-storage
3. Several current regenerating codes
4. Secret sharing scheme based on regenerating codes
   (Secure regenerating codes)

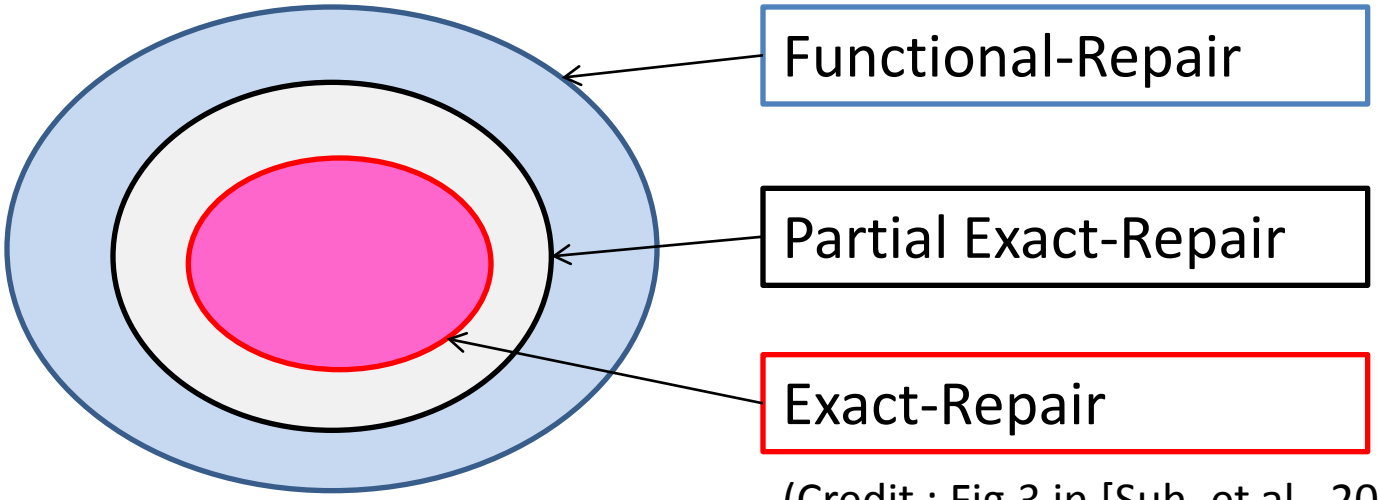
Exact vs. Functional Regeneration [Rashmi, et al.,2011]

- Functional-Regeneration(Functional-Repair)

  The resulting network of n nodes continues to possess reconstruction and regeneration properties

- Exact-Regeneration(Exact-Repair)

  The repaired node stores exactly the same data as was stored in it prior to failure.



(Credit : Fig.3 in [Suh, et al., 2010])

Codes for regenerations

- **Functional-Regeneration**
  - Network Coding for multicast

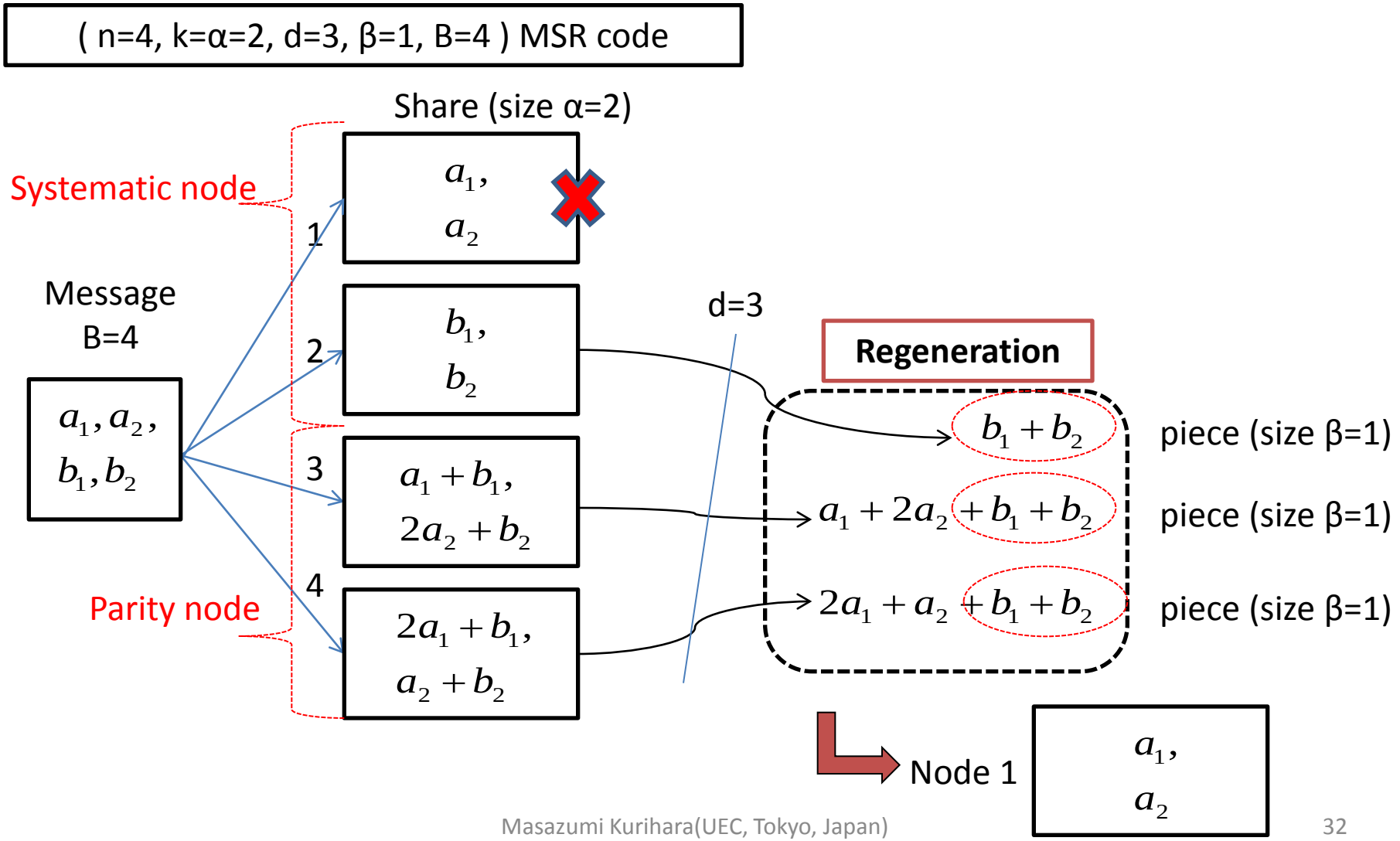
    (Multicasting Problem on information flow graph)

    [Dimakis, et al.,2007],[Wu, et al.,2007] → [Dimakis, et al.,2010]
- **Partial Exact-Regeneration**
  - Interference alignment (MSR codes, d=n-1)[Shah, et al.,2010]

    (MSR codes with systematic-nodes and parity-nodes)
- **Exact-Regeneration**
  - Interference alignment (MSR codes) [Suh, et al.,2011], [Shah, et al.,2012b]
  - Complete graph and MDS code (MBR codes) [Shah, et al., 2012a]
  - Product-Matrix framework [Rashmi, et al.,2011]
    - (n,k,d) MBR codes for all values of (n,k,d)
    - (n,k,d) MSR codes for all values of (n,k,d), d>=2k-2

  (the first-, general-, explicit-, exact-constructions of MSR and MBR codes)

MSR codes
by Interference alignment (Fig.4 in [Suh, et al.,2010])



MBR and MSR codes on Product-Matrix framework [Rashmi, et al.,2011]

- Using the property of symmetric matrices such that if a matrix M is a symmetric matrix, then

$$(AM)^t = MA^t$$

where

$$\begin{cases} M : d \text{ x } d \text{ symmetric matrix} \\ A : d \text{ x } d \text{ matrix} \end{cases}$$

since

$$M\ A^{\mathrm{t}} = (A\,M^t)^t = (A\,M)^t$$

$$M = M^t$$

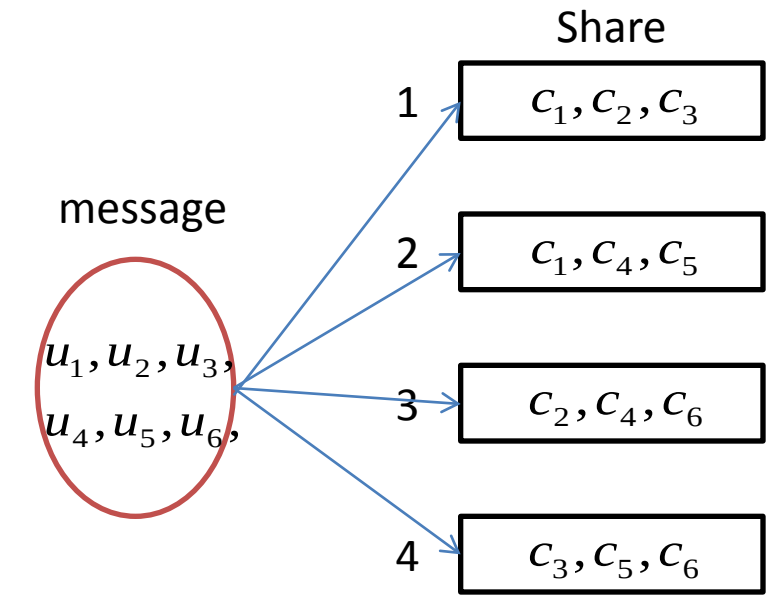
$$AB \neq BA$$

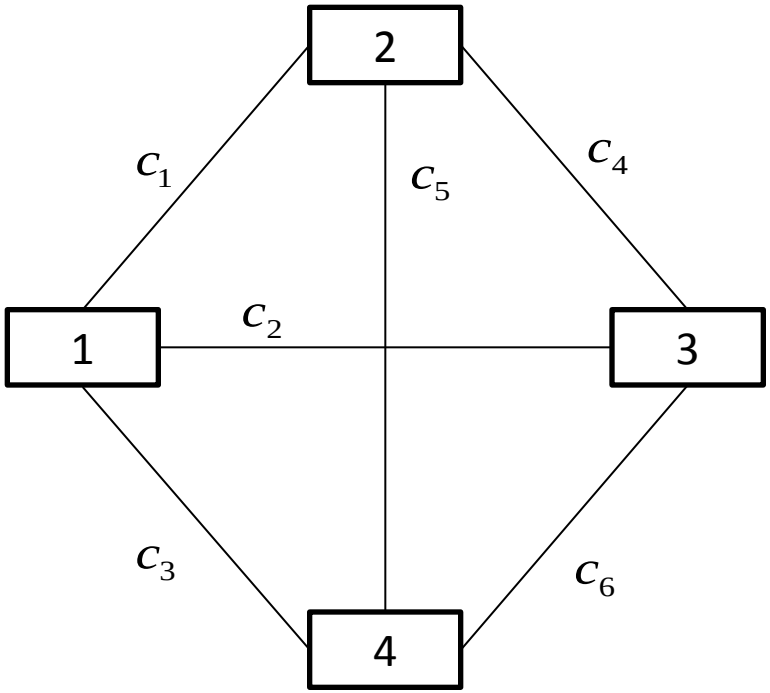
$$(AB)^t \neq BA^t$$

(n, k)MBR codes by complete graph and ($\binom{n}{2}$, B)MDS code[Shah, et al.,2012](1/2)

(d=α=n-1, β=1, B= (n-1)k - $\binom{k}{2}$)

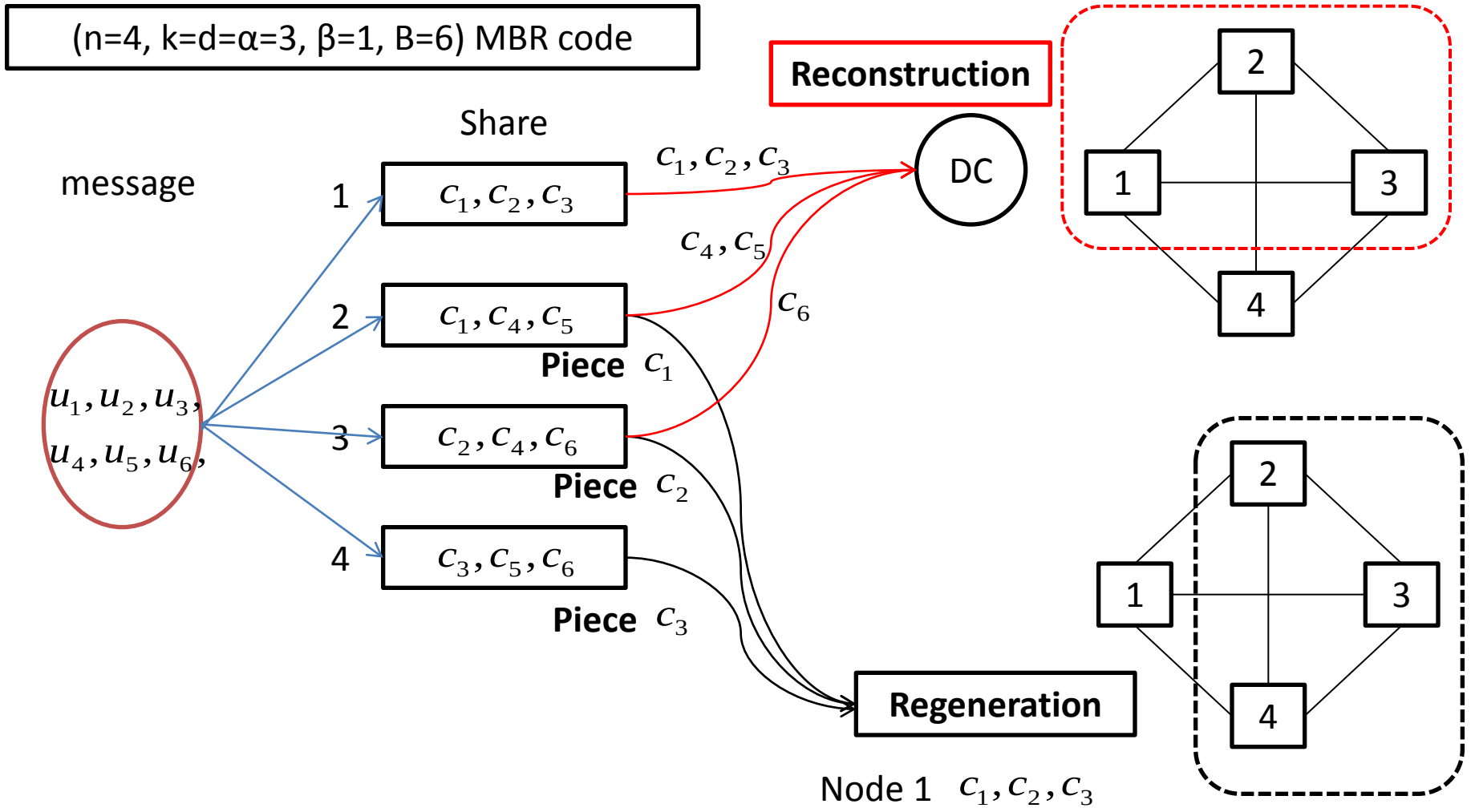
(n=4, k=d=α=3, β=1, B=6) MBR code





Complete graph with n=4 nodes and $\binom{n}{2}$ edges

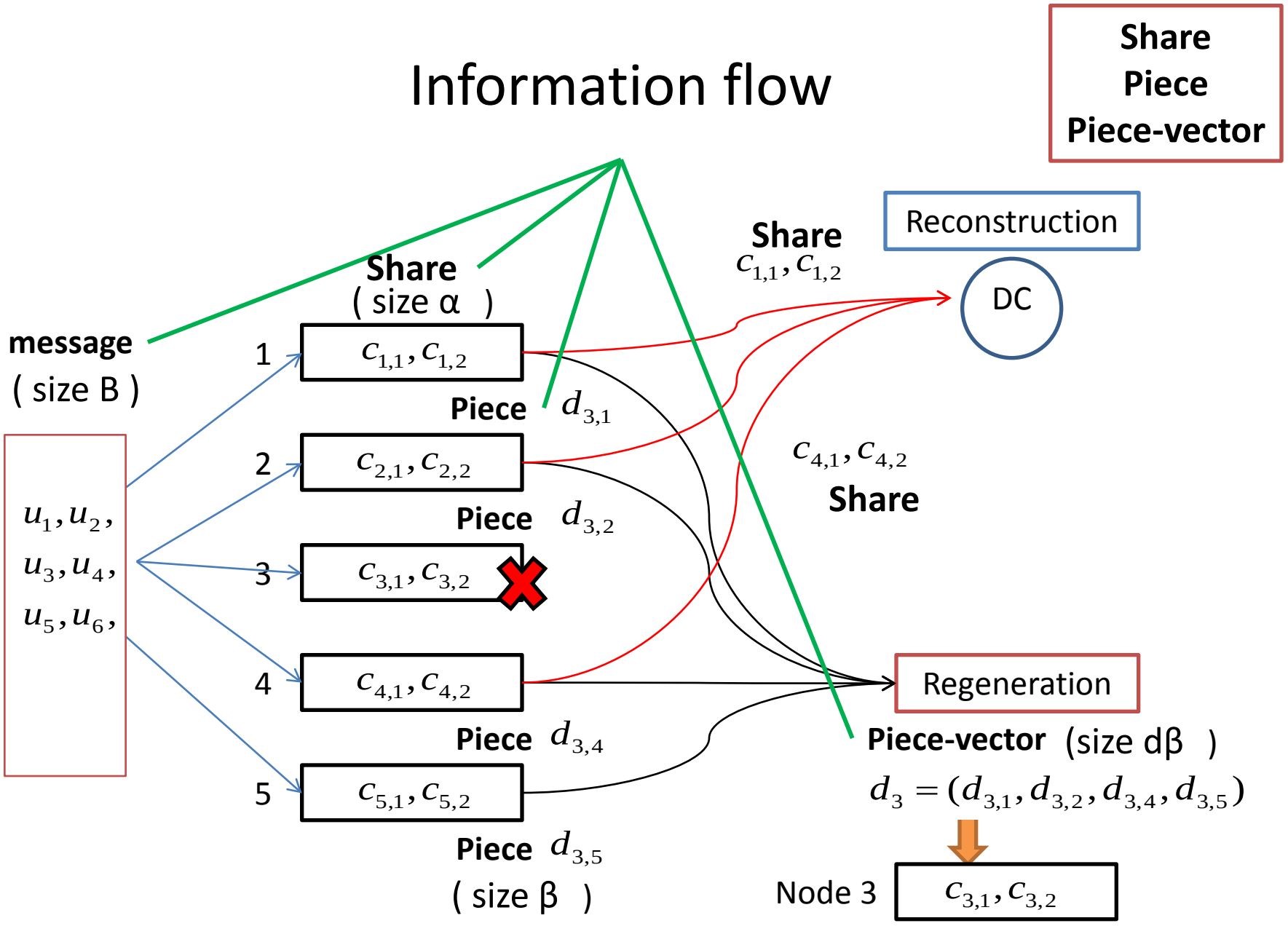
MBR codes
by Complete graph and MDS code (2/2)



Contents

1. Concept of regenerating codes
2. Relation between network-coding and distributed-storage
3. Several current regenerating codes
4. Secret sharing scheme based on regenerating codes
   (Secure regenerating codes)

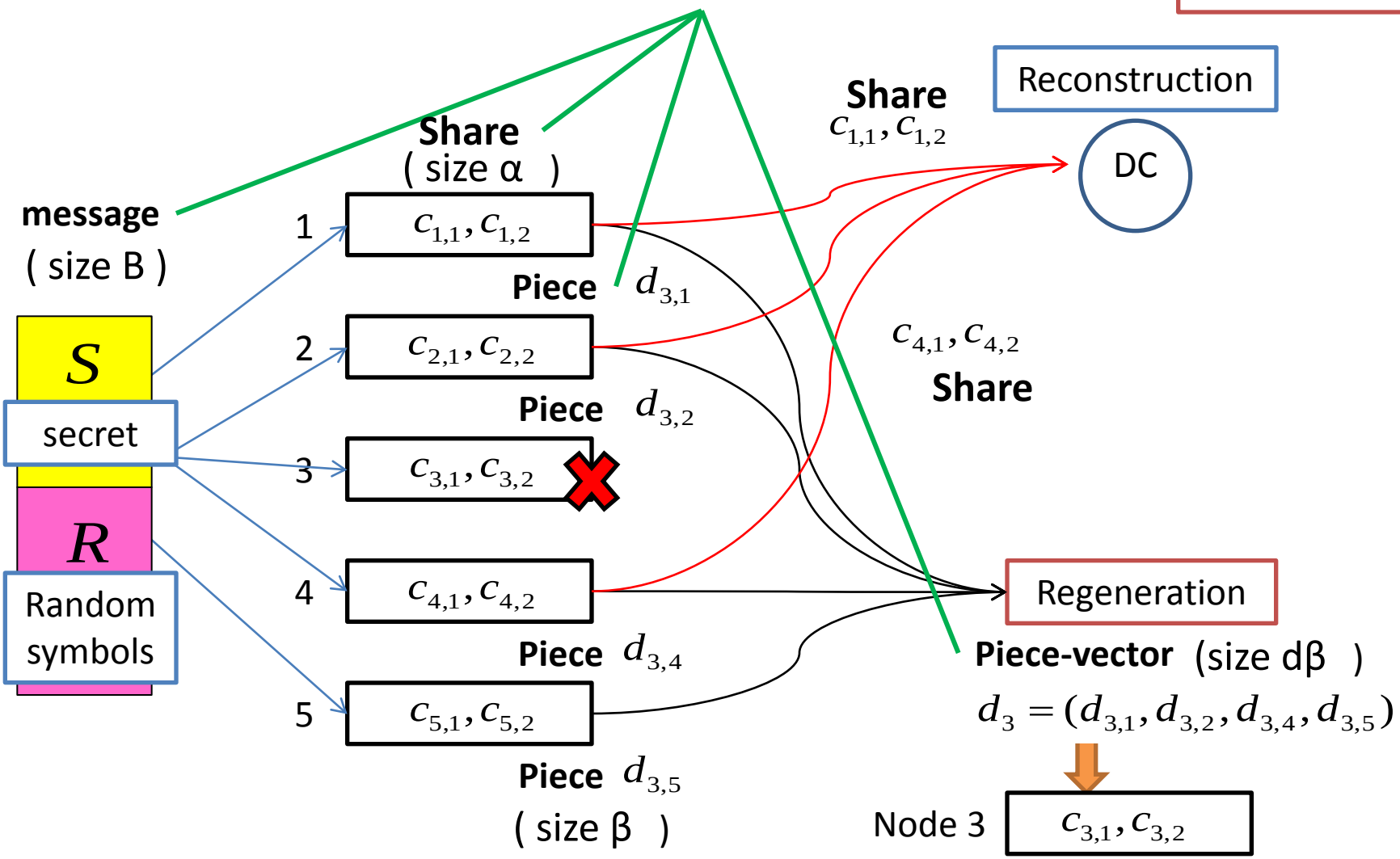
Information flow



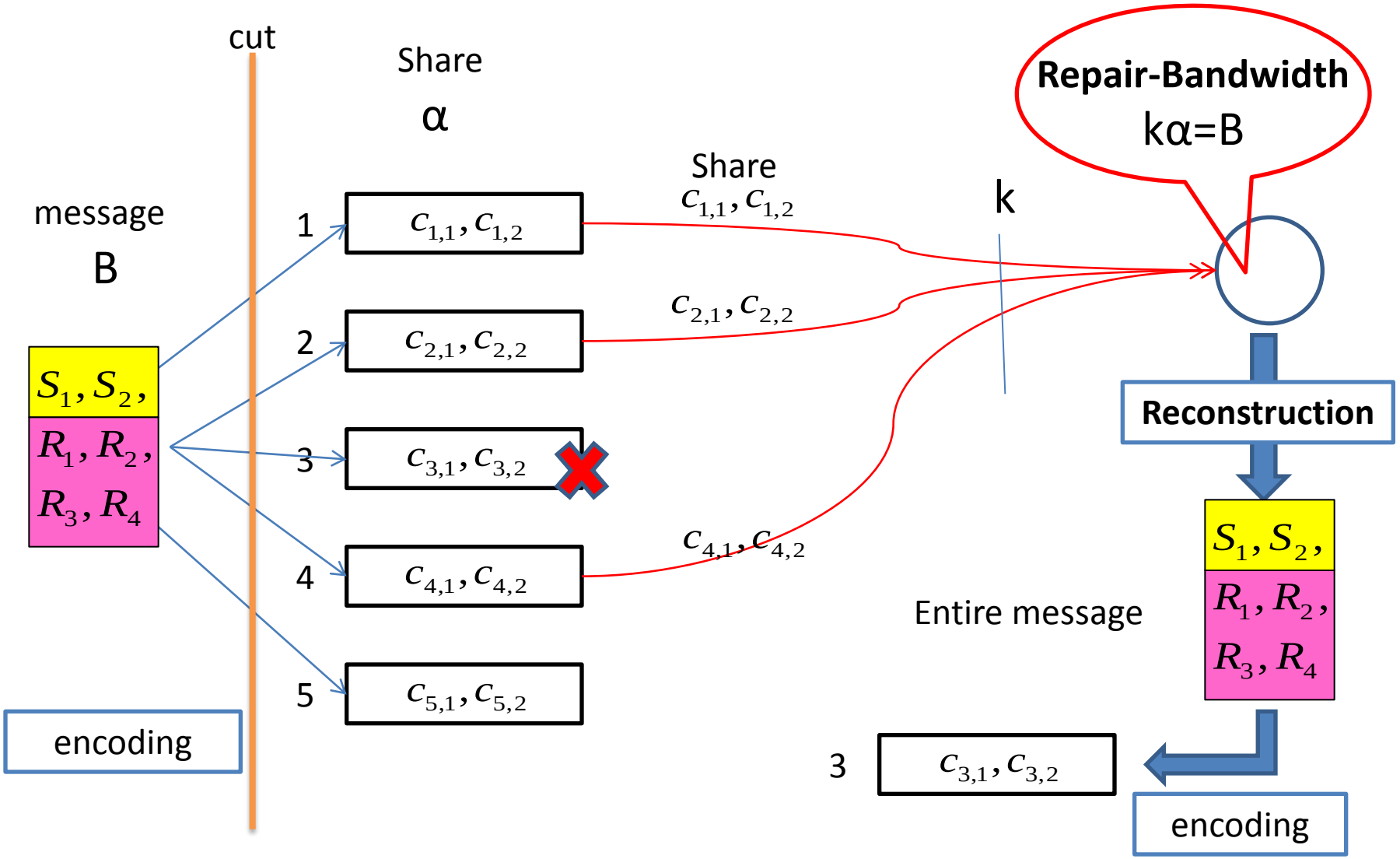
Secure Regenerating Codes

(Secret Sharing based on Regenerating Codes)

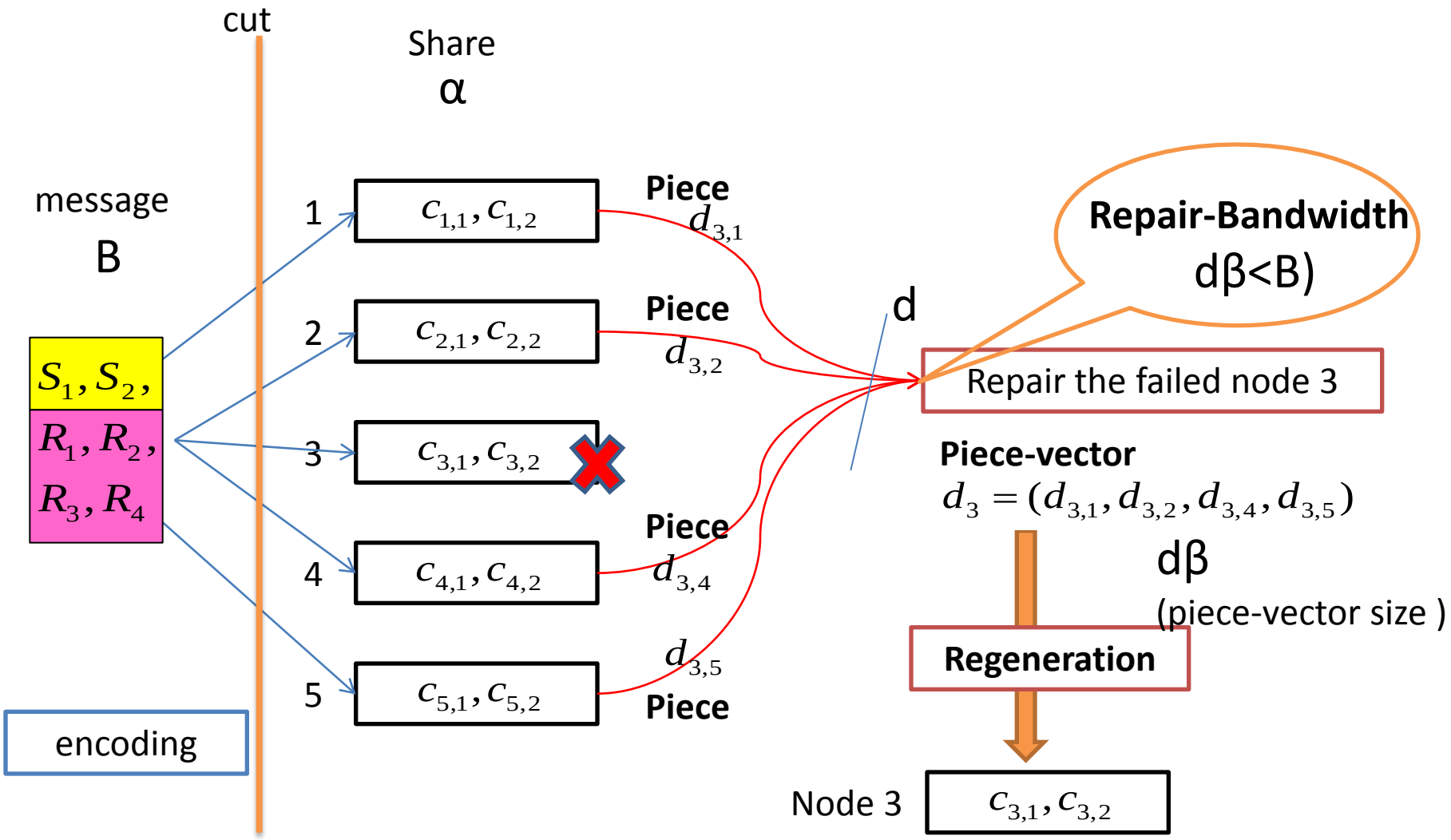
Share
Piece
Piece-vector



Regeneration by reconstruction



Regeneration by regenerating codes



Secure Regenerating Codes (Secret sharing based on Regenerating codes)

- **Exact-Regeneration(MSR and MBR codes)**
- **Informationally secure regenerating codes**
  - **Secure MBR codes**
    - Complete graph and MDS code : [Pawar, et al., 2011]
    - Product-Matrix framework :

      [Kurihara and Kuwakado,2011d](**non-linear ramp scheme**),

      [Shah, et al., 2011]
  - **Secure MSR codes**
    - Product-Matrix framework : [Kurihara and Kuwakado,2011a,b],

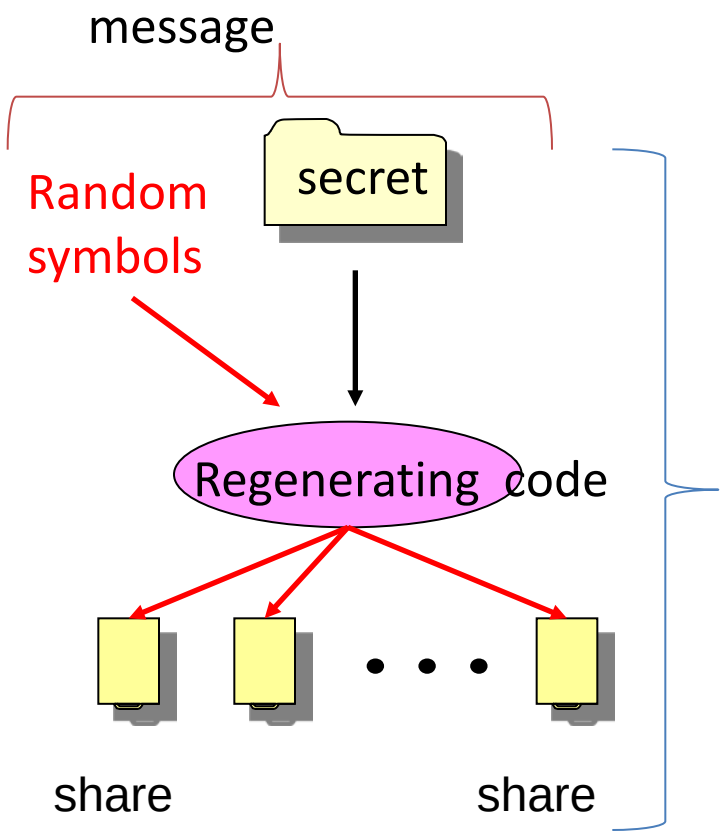
      [Kuwakado and Kurihara,2011],

      [Shah, et al., 2011]
- **Computationally secure regenerating codes**

  [Kuwakado and Kurihara,2011]

Computationally-Secure Regenerating(CS-R) codes

[Kuwakado and Kurihara,2011]

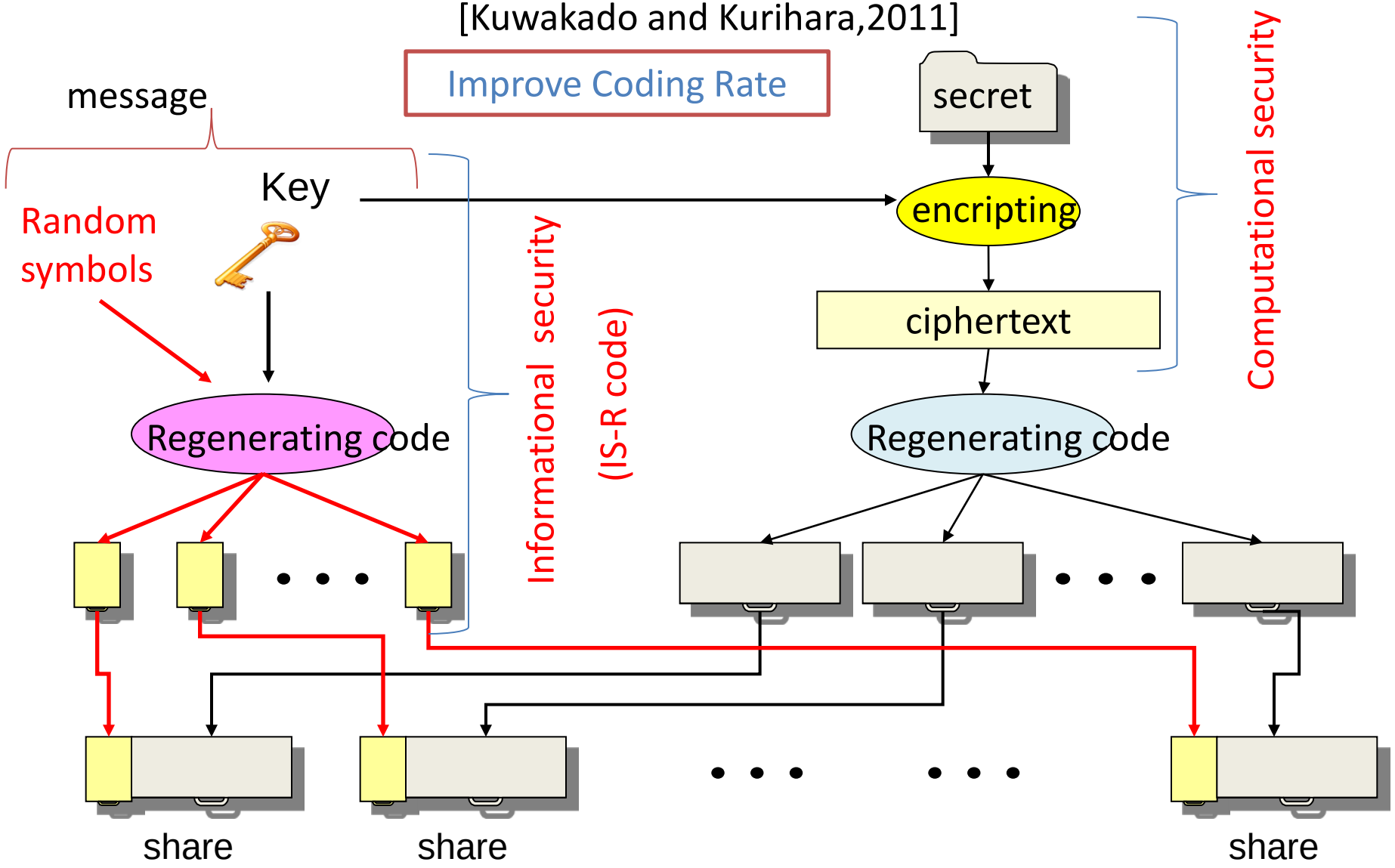


Informationally-Secure Regenerating(IS-R) code

Credit: Kuwakado and Kurihara , “Computationally-Secure Regenerating code,” CSS2011

Computationally-Secure Regenerating(CS-R) codes

[Kuwakado and Kurihara,2011]

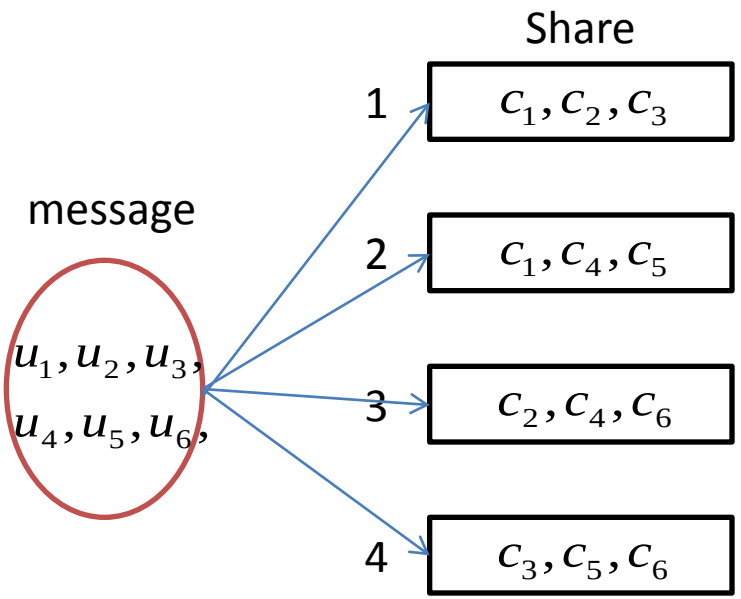


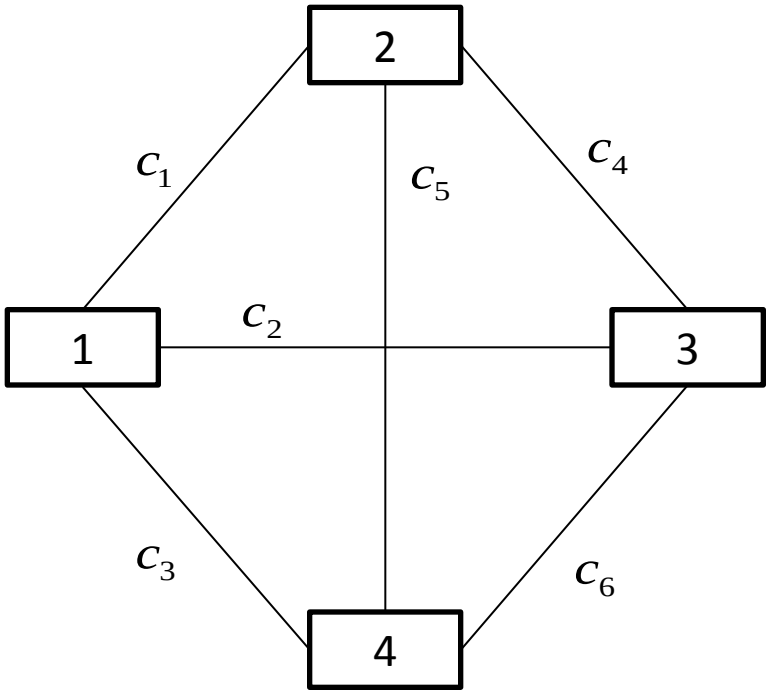
Credit: Kuwakado and Kurihara , “Computationally-Secure Regenerating code,” CSS2011

Recall (n, k)MBR codes by complete graph and ($\binom{n}{2}$, B)MDS code[Shah, et al.,2012a]

(d=α=n-1, β=1, B= (n-1)k - $\binom{k}{2}$)

(n=4, k=d=α=3, β=1, B=6) MBR code

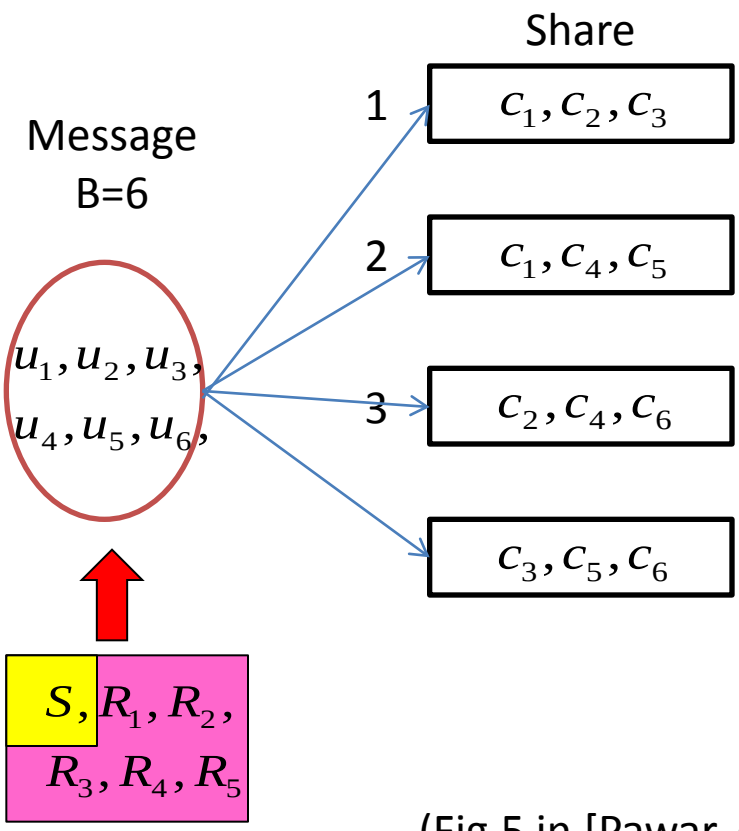




Complete graph with n=4 nodes and $\binom{n}{2}$ edges

Secure (n, k)MBR codes [Pawar, et al., 2011] by Complete graph and MDS code

(n=4, k=d=α=3, β=1, l= 2) secure MBR code



Setting :

S : Secret,

$R_1, R_2, \ldots, R_5$: Random symbols

Perfect secrecy for at most two shares

Encoding :

$$c_i = R_i \text{ for } i = 1,2,\ldots,5,$$

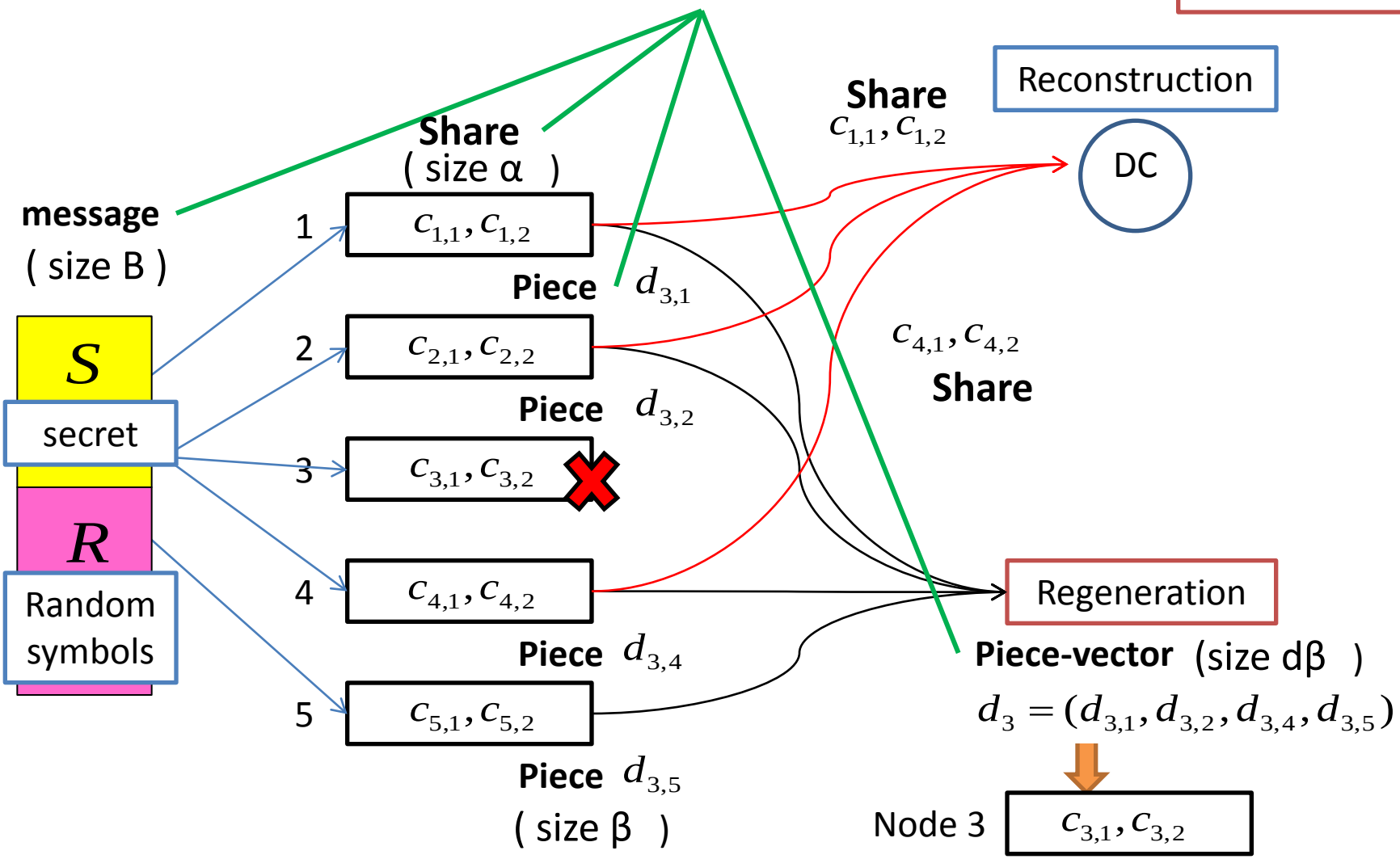
$$c_6 = S + R_1 + R_2 + \ldots + R_5$$

(Fig.5 in [Pawar, et al., 2011])

Secure Regenerating Codes

(Secret Sharing based on Regenerating Codes)

Share
Piece
Piece-vector



Secrecy Capacity for secure regenerating code [Pawar, et al., 2011](1/3)

- Random variables

  - Secret : S

  - Share : $C_i \quad (i = 1,2,\ldots,n)$

  - Piece : $D_{f,h} \; (f \in \{1,\ldots,n\}, h \in \{1,\ldots,n\} \setminus \{f\})$

  - Piece-Vector : $D_f = (D_{f,1},\ldots,D_{f,d}) \; , (f \in \{1,\ldots,n\})$

- Reconstruction Property

  For any k shares $C_1,\ldots,C_k$,

  $$H(S \mid C_1,\ldots,C_k) = 0$$

- Regeneration Property (failed node f)

  For any d pieces $D_{f,1},\ldots,D_{f,d}$ for repair the failed node f ,

  that is, piece-vector D_f ,

  $$H(C_f \mid D_f) = 0$$

Secrecy Capacity for secure regenerating code [Pawar, et al., 2011](2/3)

- Regeneration Property (failed node f)

  For any d pieces $D_{f,1}, \ldots, D_{f,d}$ for repair the failed node f ,
  that is, piece-vector D_f ,

$$H(C_f \mid D_f) = 0$$

(The share C_f is uniquely determined from the piece-vector D_f.)

- In general, $H(S \mid D_f) \le H(S \mid C_f)$, i.e., $I(S; D_f) \ge I(S; C_f)$,
  since the Markov chain $S \to D_f \to C_f$.
  Thus, if $I(S; D_f) = 0$ then $I(S; C_f) = 0$, because

$$H(S) = H(S \mid D_f) \le H(S \mid C_f) \le H(S)$$

- However, it is not always true that $H(D_f \mid C_f) \neq 0$.

Secrecy Capacity for secure regenerating code [Pawar, et al., 2011](3/3)

- Secrecy property

  For m piece-vector $D_{f1},\ldots,D_{fm}$ for any m repaired nodes $f_1,\ldots,f_m$,

$$H(S \mid D_{f1},\ldots,D_{fm}) = H(S)$$

- Secrecy capacity C_S for (n, k, d, α, β, B ; m) secure regeneration code :

$$C_S = \sup_{\substack{H(S \mid C_1,\ldots,C_k)=0 \\ H(S \mid D_1,\ldots,D_m)=H(S)}} H(S)$$

Reconstruction Property

- **The upper bound** of the secrecy capacity:

$$C_S \le \sum_{i=m+1}^{k} \min\{(d-i+1)\beta, \alpha\}$$

Information flow graph

Conclusions

- Regenerating codes for distributed storage [Dimakis, et al.,2010]
  - Reconstruction and Regeneration(repair failed node)
  - Reducing bandwidth to repair
  - Tradeoff between Storage and Repair-Bandwidth
    - MSR and MBR codes
- Network coding for distributed storage [Dimakis, et al.,2010]
  - Capacity for regenerating codes
  - Linear network coding for multicast
- Exact-regeneration vs. Functional-regeneration
- Secure Regenerating Codes
  - Secret sharing based on (exact-)regenerating codes
  - Share, piece, and piece-vector

References(1/3)

- [Dimakis, et al.,2010] Dimakis, A.G.; Godfrey, P.B.; Yunnan Wu; Wainwright, M.J.; Ramchandran, K.;
  Network Coding for Distributed Storage Systems
  Information Theory, IEEE Transactions on, Volume: 56 , Issue: 9 , Publication Year: 2010 , Page(s): 4539 – 4551

- [Dimakis, et al.,2007]A. G. Dimakis , P. B. Godfrey , Y. Wu , M. Wainwright and K. Ramchandran
  "Network coding for distributed storage systems", Proc. IEEE INFOCOM, 2007

- [Wu, et al.,2007]Y. Wu , A. G. Dimakis and K. Ramchandran
  "Deterministic regenerating codes for distributed storage",
  Proc. Allerton Conf. Control, Computing and Communication, 2007

- [Rashmi, et al.,2011] Rashmi, K.V.; Shah, N.B.; Kumar, P.V.;
  Optimal Exact-Regenerating Codes for Distributed Storage at the MSR and MBR Points via a Product-Matrix Construction
  Information Theory, IEEE Transactions on , Volume: 57 , Issue: 8, Publication Year: 2011 , Page(s): 5227 - 5239

- [Suh, et al.,2011] Changho Suh; Ramchandran, K.;
  Exact-Repair MDS Code Construction Using Interference Alignment
  Information Theory, IEEE Transactions on ,Volume: 57 , Issue: 3, Publication Year: 2011 , Page(s): 1425 - 1442

References(2/3)

- [Shah, et al.,2010]N. B. Shah, K. V. Rashmi, P. V. Kumar, and K. Ramchandran,
  "Explicit codes minimizing repair bandwidth for distributed storage,"
  in Proc. IEEE Information Theory Workshop, Cairo, Egypt, Jan.2010.

- [Shah, et al.,2011] Shah, N.B.; Rashmi, K.V.; Kumar, P.V.;
  Information-Theoretically Secure Regenerating Codes for Distributed Storage
  Global Telecommunications Conference (GLOBECOM 2011), 2011 IEEE , Publication Year: 2011 , Page(s): 1 – 5

- [Shah, et al.,2012a] Shah, N.B.; Rashmi, K.V.; Vijay Kumar, P.; Ramchandran, K.;
  Distributed Storage Codes With Repair-by-Transfer and Nonachievability of Interior Points on the Storage-Bandwidth Tradeoff
  Information Theory, IEEE Transactions on , Volume: 58 , Issue: 3, 2012 , Page(s): 1837 - 1852

- [Shah, et al.,2012b] Shah, N. B.; Rashmi, K. V.; Kumar, P. V.; Ramchandran, K.;
  Interference Alignment in Regenerating Codes for Distributed Storage: Necessity and Code Constructions
  Information Theory, IEEE Transactions on , Volume: 58 , Issue: 4 , 2012 , Page(s): 2134 - 2158

- [Pawaer, et al.,2011] Pawar, S.; El Rouayheb, S.; Ramchandran, K.;
  Securing Dynamic Distributed Storage Systems Against Eavesdropping and Adversarial Attacks
  Information Theory, IEEE Transactions on , Volume: 57 , Issue: 10 , 2011 , Page(s): 6734 - 6753

References(3/3)

- [Kurihara and Kuwakado,2011a]M.Kurihara and H.Kuwakado,
  ``On regenerating codes and secret sharing for distributed storage,''
  IEICE Technical Report(in Japanese), IT2010-56(2011-01), pp.13-18(in Japanese), Jan. 2011.

- [Kurihara and Kuwakado,2011b]M.Kurihara and H.Kuwakado,
  `On an extended version of Rashmi-Shah-Kumar regenerating codes and secret sharing for distributed storage,''
  IEICE Technical Report, IT2010-114(2011-03), pp.303-310(in Japanese), Mar. 2011.

- [Kurihara and Kuwakado,2011c]M.Kurihara and H.Kuwakado,
  ``On ramp secret sharing schemes for distributed storage systems under repair dynamics,''
  IEICE Technical Report, IT2011-17(2011-7), pp.41-46(in Japanese), July 2011.

- [Kurihara and Kuwakado,2011d]M.Kurihara and H.Kuwakado,
  ``Ramp secret sharing schemes based on MBR codes,''
  IEICE Technical Report, ISEC2011-43(2011-11), pp.61-68(in Japanese), Nov. 2011.

- [Kuwakado and Kurihara and,2011]H.Kuwakado and M.Kurihara,
  ``Computationally-Secure Regenerating Code,''
  Proceedings of Computer Security Symposium 2011, pp.131-136, 19-21 Oct. 2011.

The last slide

Deleted 6 pages in which recent results ware written. [Kurihara and Kuwakado, 2012]

(See the full version)