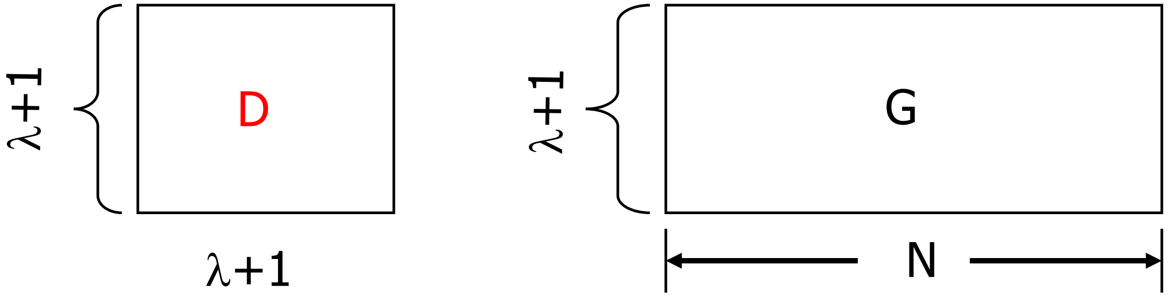
Deterministic Approaches

- Used to design the key pool and the key chains to provide better connectivity
  - Matrix Based Scheme [Blom 1985]
  - Polynomial Based Key Generation [Blundo et al. 1992]

Deterministic approaches: Blom's Scheme [B]

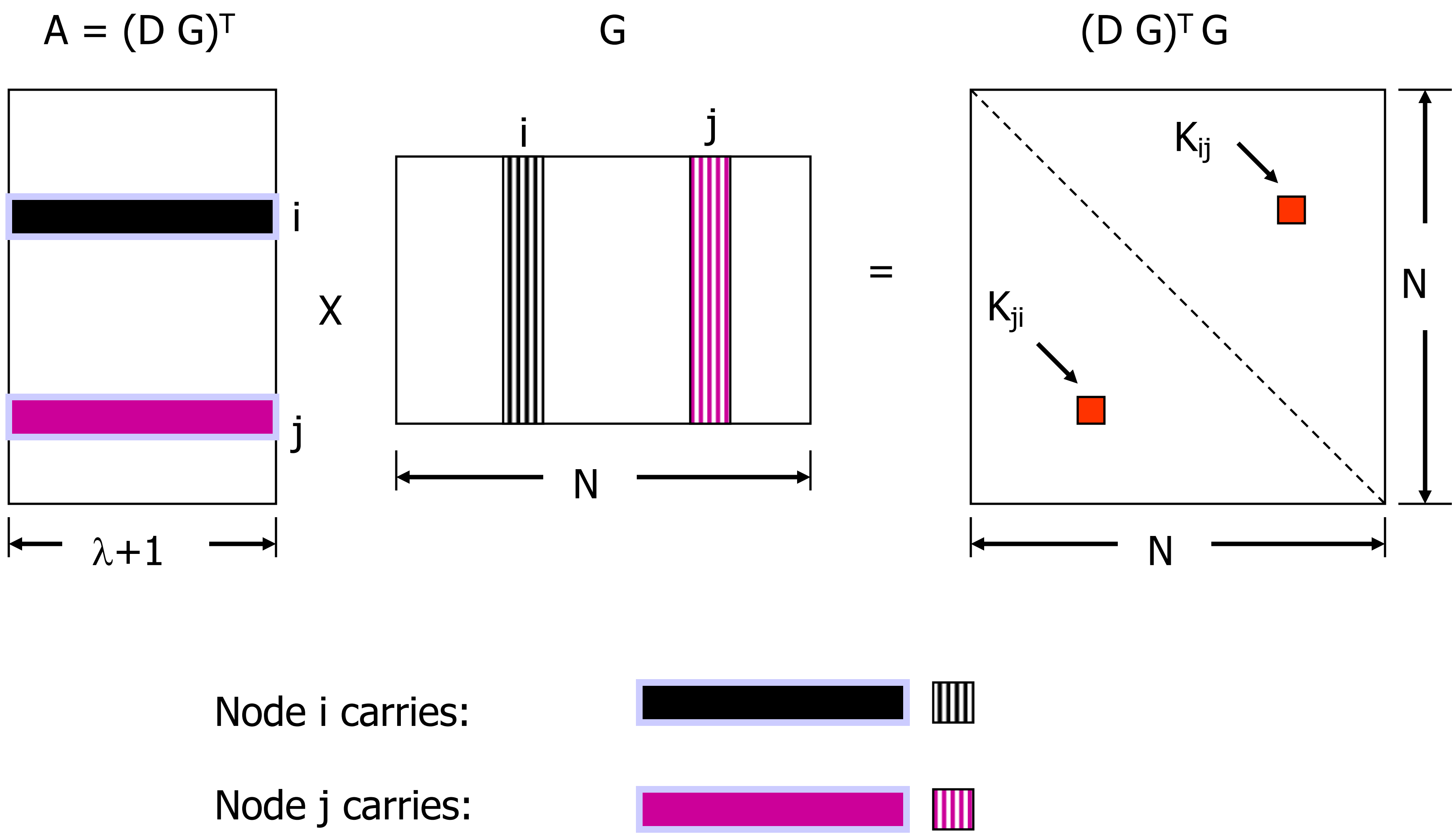
- Public matrix G
- Private matrix D (symmetric).



Let $A = (D\ G)^T$

$$A\,G = (D\,G)^T G = G^T D^T G = G^T D\,G = (A\,G)^T$$

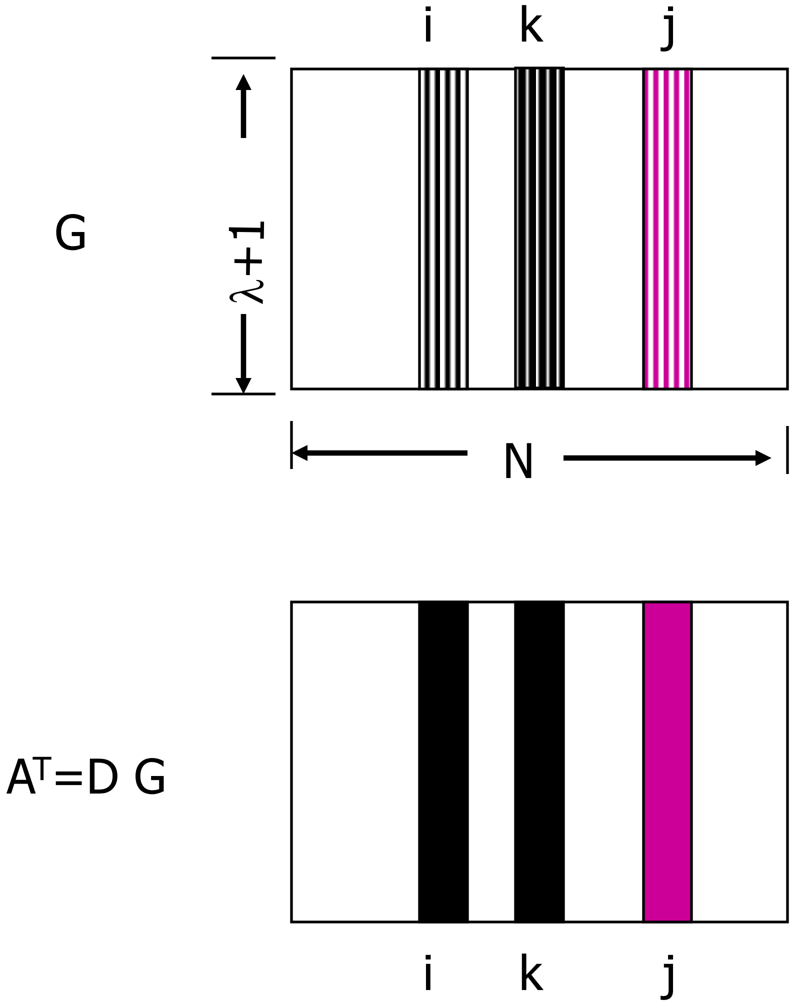
[B] Scheme



Node i carries:

Node j carries:

[B] λ-secure Property



Undesirable Situation:
if
u*G(i) + v*G(j) = G(k)

then
u*A(i) + v*A(j) = A(k)

this would allow
colluding nodes (i and j) to
impersonate other nodes (k)

[B] λ-secure Property

- **ALL** **λ+1** columns in G are linear independent.
  - Different from saying that G has rank **λ+1**
  - **Rank:** there are **λ+1** lineary independent columns
- Can tolerate compromise up to λ nodes.
  - Once **λ+1** nodes are compromised, the rest can be calculated if these **λ+1** columns are linear independent.
- How to find such a matrix G?

[B] Vandermonde Matrix

$$G = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ s & s^2 & s^3 & \cdots & s^N \\ s^2 & (s^2)^2 & (s^3)^2 & \cdots & (s^N)^2 \\ & & \vdots & & \\ s^\lambda & (s^2)^\lambda & (s^3)^\lambda & \cdots & (s^N)^\lambda \end{pmatrix}$$

[B] Properties of Blom Scheme

- Blom's Scheme
  - Network size is N
  - Any pair of nodes can directly find a secret key
  - Tolerate compromise up to λ nodes
  - Need to store λ+2 keys

Key distribution schemes for sensor networks

http://www.cs.rpi.edu/research/pdf/05-07.pdf

Problem	Approach	Mechanism	Keying style	Papers
Pair-wise	Probabilistic	Pre-distribution	Random key-chain	C, E, F, J K, N, S
			Pair-wise key	E
	Deterministic	Pre-distribution	Pair-wise key	G, M
			Combinatorial	P, Q
		Dynamic Key Generation	Master key	D, L
			Key matrix	A
			Polynomial	B, G
	Hybrid	Pre-distribution	Combinatorial	P, Q
		Dynamic Key Generation	Key matrix	H, M, R
			Polynomial	I, R
Group-wise	Deterministic	Dyn. Key Gen.	Polynomial	B, R

The papers are: A[Blom 1985], B[Blundo et al. 1992], C[Eschenauer and Gligor 2002], D[Lai et al. 2002], E[Chan et al. 2003], F[Pietro et al. 2003], G[Liu and Ning 2003c], H[Du et al. 2003], I[Liu and Ning 2003b], J[Zhu et al. 2003], K[Du et al. 2004], L[Dutertre et al. 2004], M[Lee and Stinson 2004b], N[Hwang et al. 2004], P[Camtepe and Yener 2004], Q[Lee and Stinson 2004a], R[Huang et al. 2004], S[Hwang and Kim 2004].