An infinite phase-size BMAP/M/1 queue and its application to Secure Communication

豊泉　洋

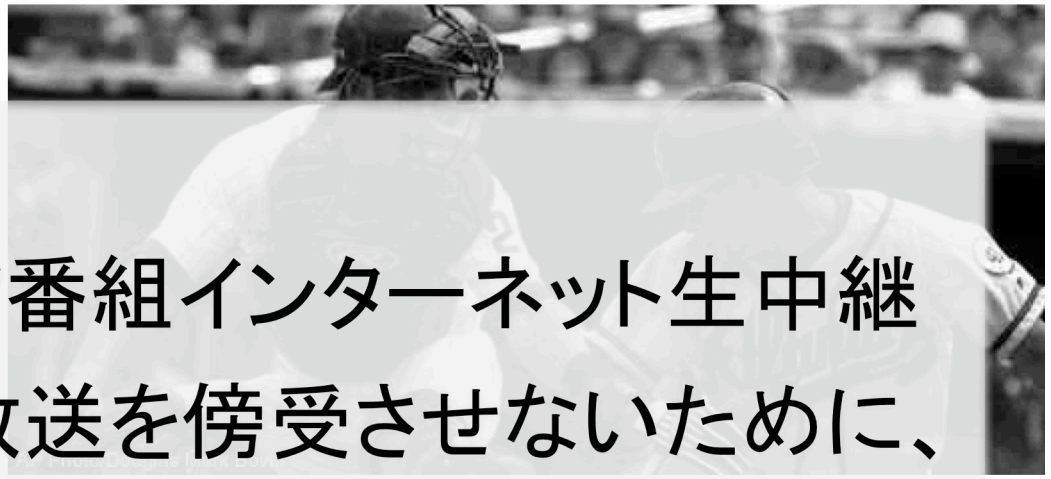
早稲田大学　大学院会計研究科

toyoizumi@waseda.jp

なぜグループで？

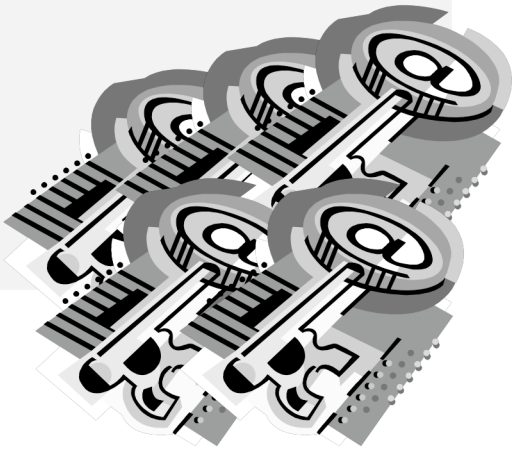
- コミュニティーを作って自由に通信
  - 特定のグループ内の通信においても暗号化が必要
  - 人気番組のインターネット上での有料配信
  - 企業内の秘密情報のネット[illegible]上での共有

スポーツリアルタイム社



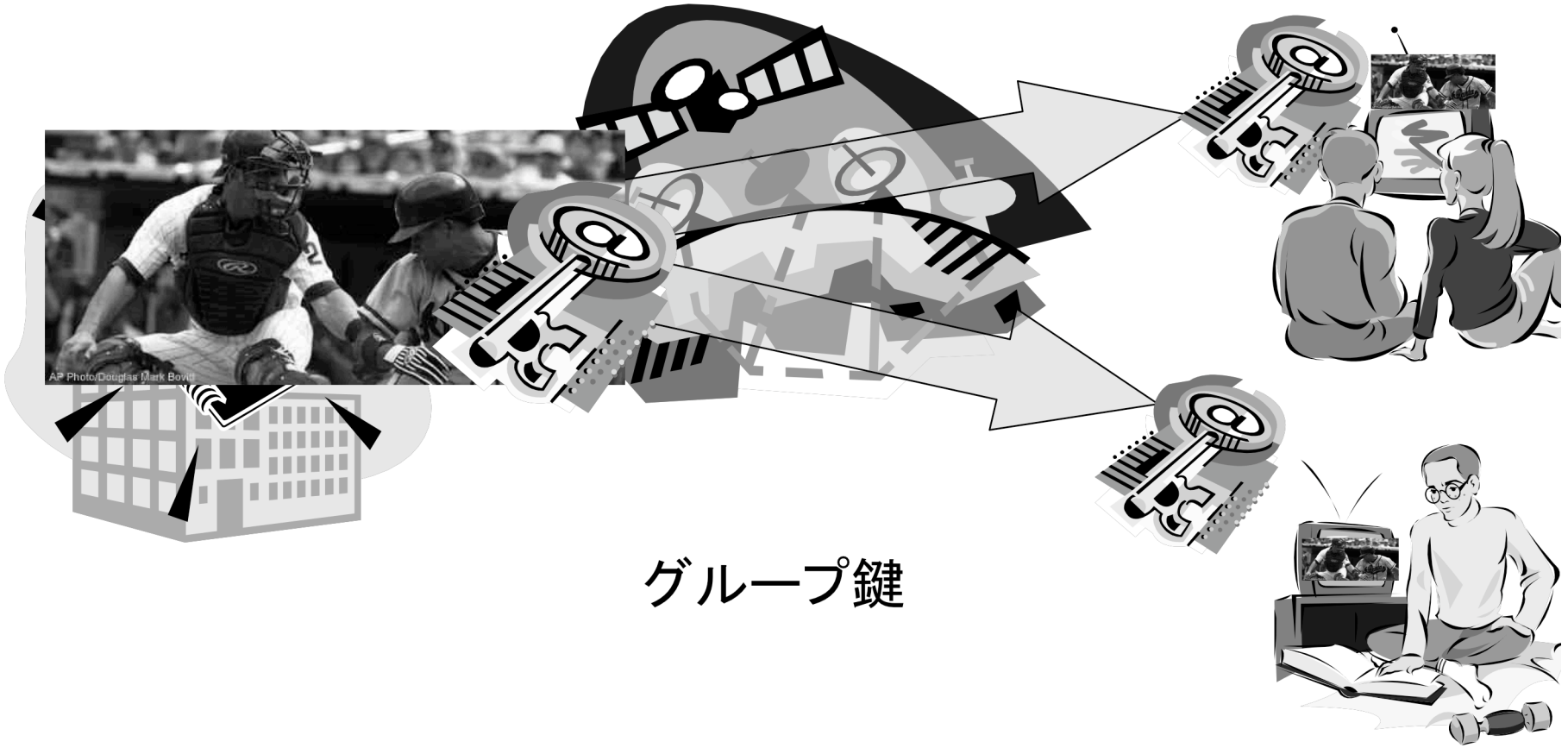
- １万人の顧客
- 有料でスポーツ番組インターネット生中継
- 不正な手段で放送を傍受させないために、１万人へ暗号化されたデータを送信する。

- 1万個の鍵で別々に暗号化？



グループ鍵

- グループ共通の鍵でデータを暗号化

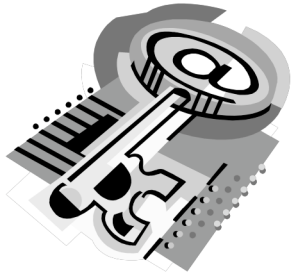


グループ鍵の問題点

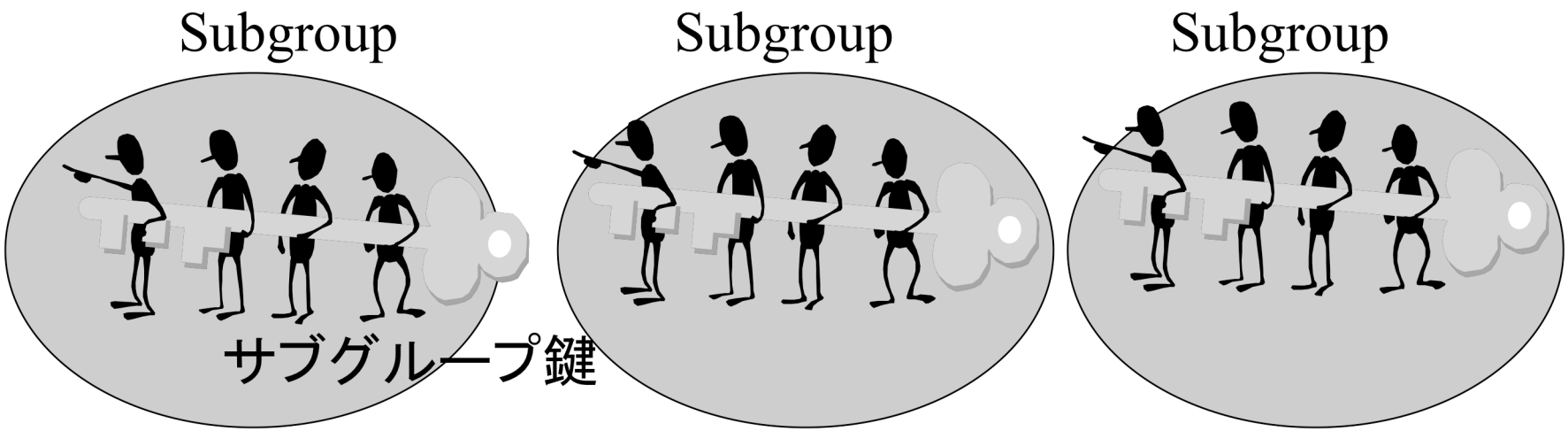
- 参加・脱退
  - スポーツ番組の生中継は、
    - 途中から見たいと言ってくる人
    - つまらないから見るのを止めるという人
- 悪意のユーザー
  - 最初に鍵を受け取る
  - 途中から見るのを止めると言う
  - 最初に手に入れた鍵を使って無料でスポーツ番組をみる。
- 参加・脱退時にグループ鍵の更新が必要！

グループセキュリティ通信の方式

- Wong [6] 、RFC2627 [4]の方法

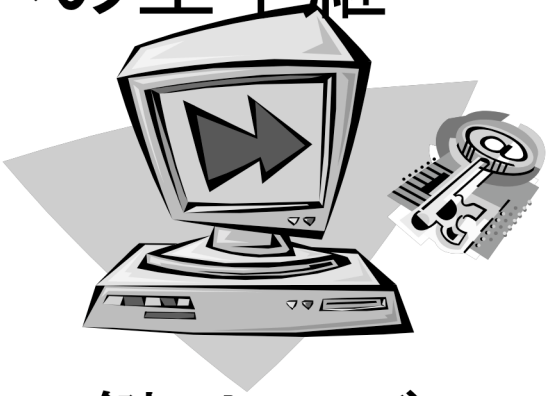


グループ鍵



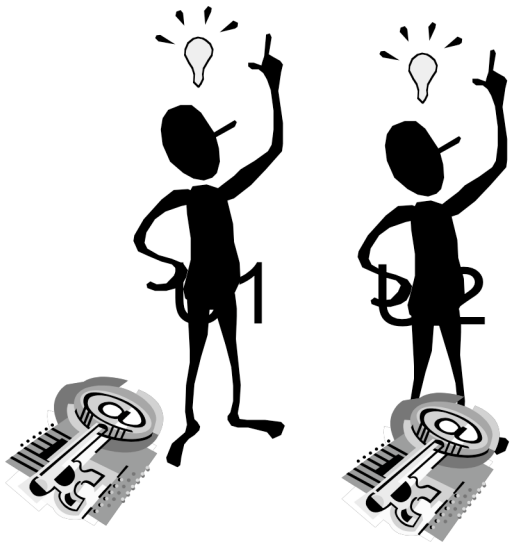
生中継の準備

15人のユーザーへの生中継

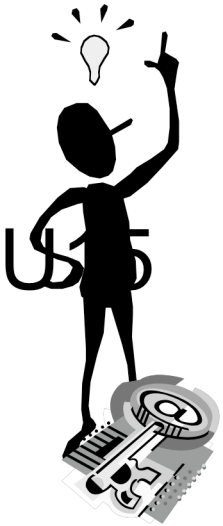


グループ鍵G(C

鍵サーバー



…

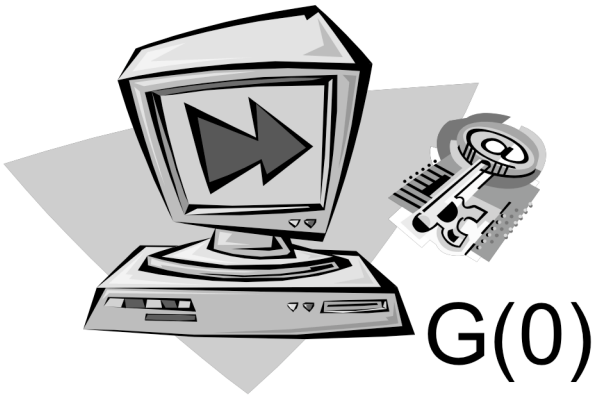


サブグループ無しの場合

- U15の脱退

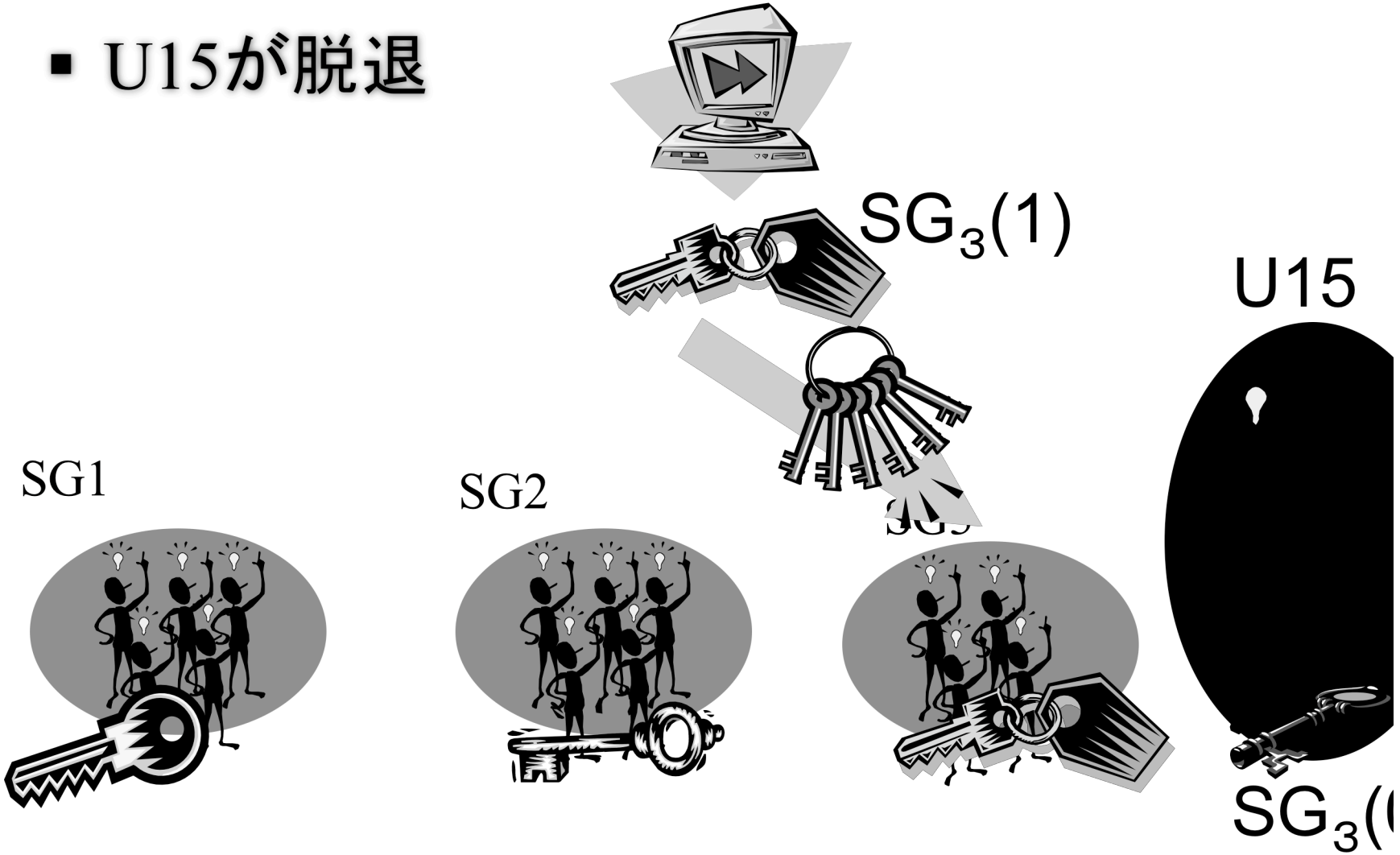
サブグルーピング

- サブグループが3つ



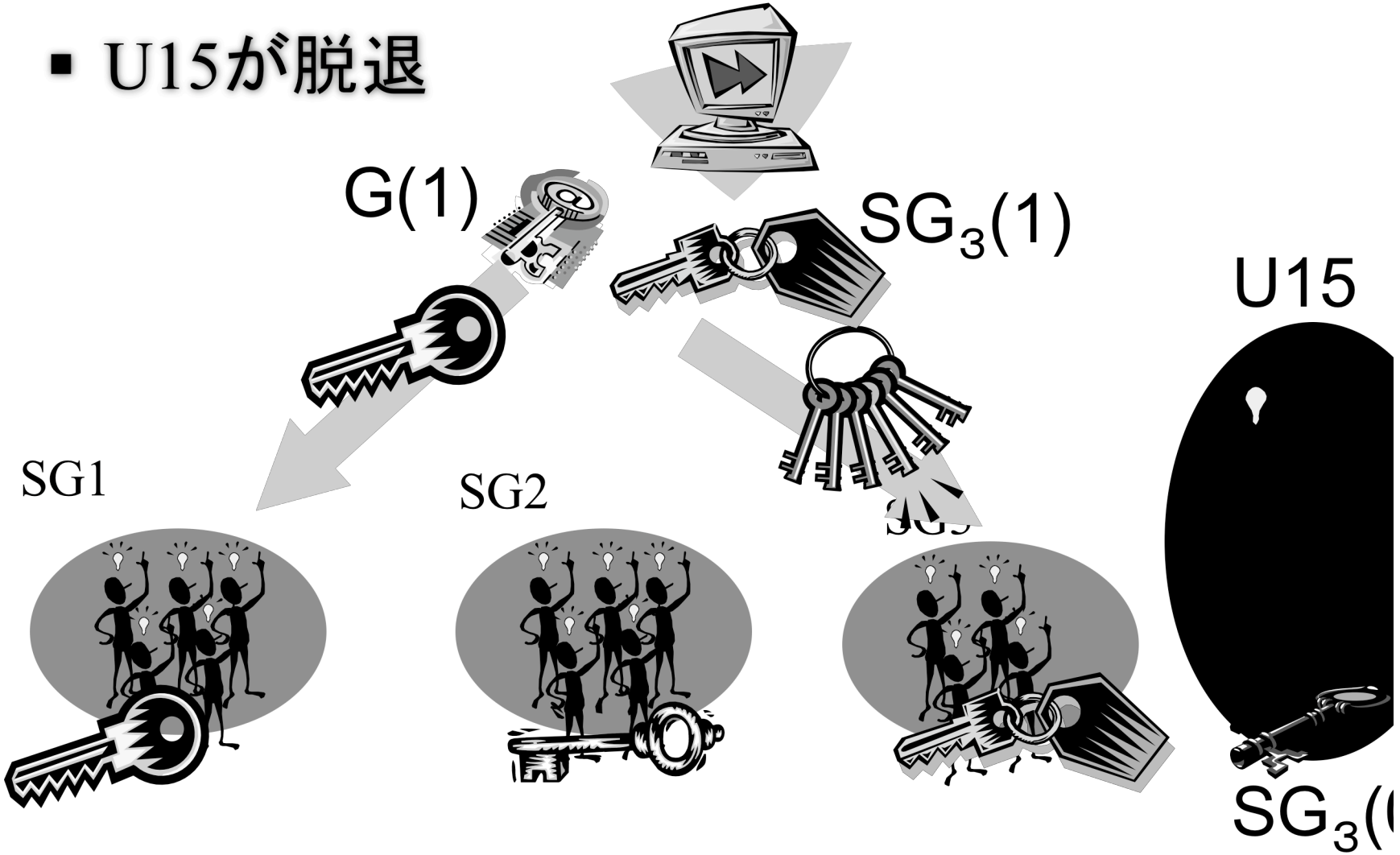
脱退

- U15が脱退



脱退

- U15が脱退



脱退

- U15が脱退

暗号化回数は7回で済む！
（脱退時のサブグループ内の人数に依存）

サブグループと暗号化回数

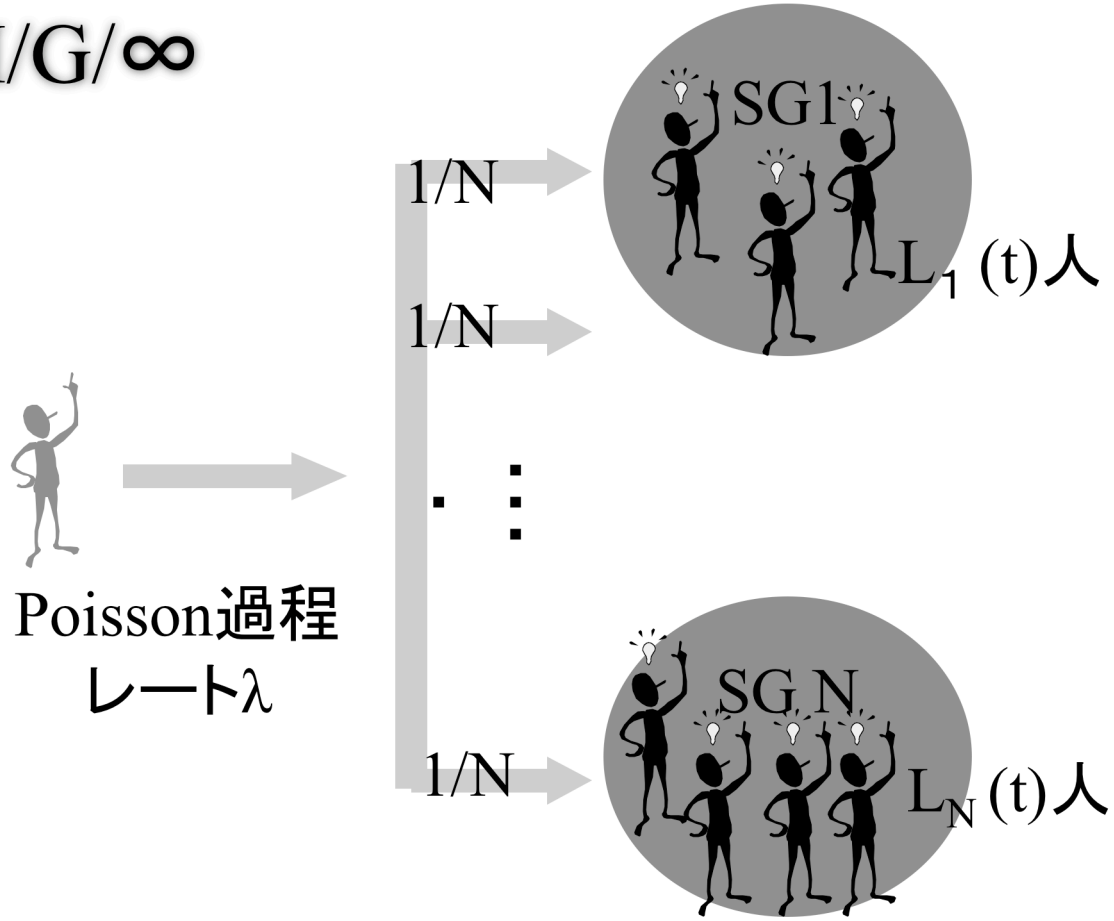
- ユーザが脱退・参加した場合のグループ全体の暗号化の回数

方式	A15 (U15 脱退)	B16 (U16 参加)	合計
サブグループ無し	14	2	16
サブグループ有り	7	4	11

脱退の時が問題！

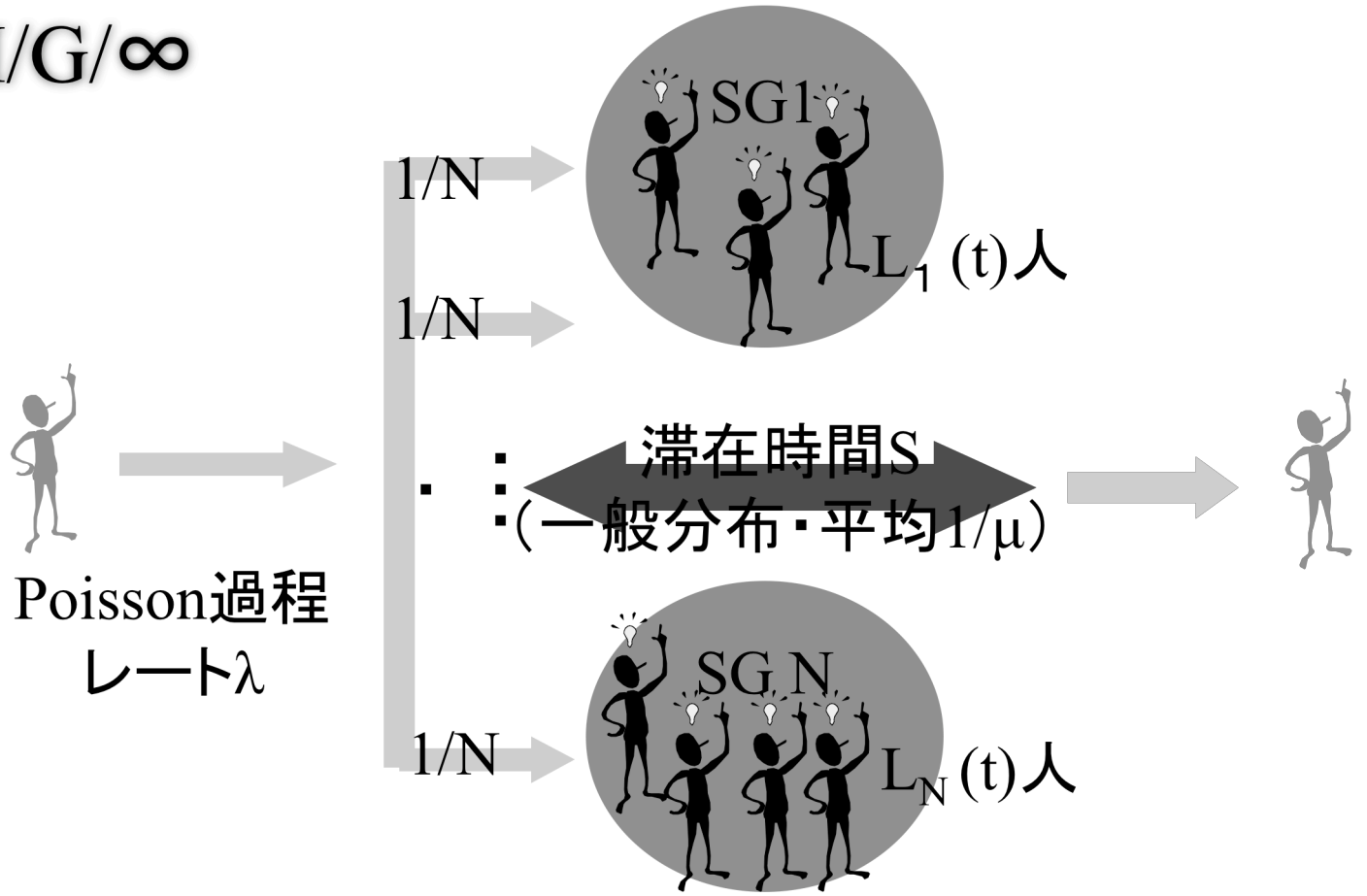
グループセキュリティ通信の待ち行列モデル（Poisson arrival）

- M/G/∞



グループセキュリティ通信の待ち行列モデル（Poisson arrival）

- M/G/∞



最適なサブグループ数
(Poisson arrival)

- 暗号化回数が最小になるサブグループ数は

  平均のユーザー数の平方根!

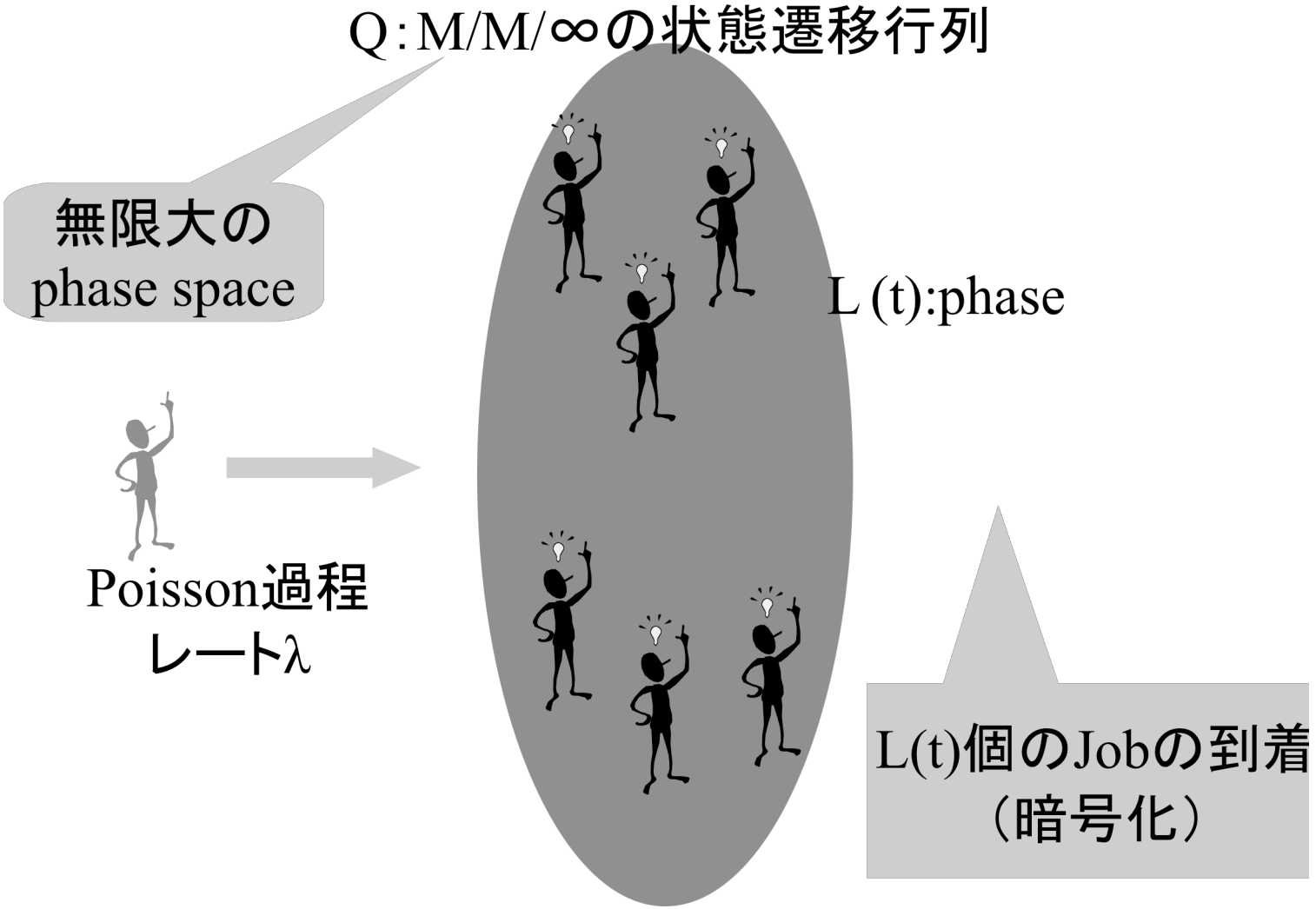
$$N^{min} = \left(\frac{\lambda}{\mu}\right)^{1/2} = (E[L(t)])^{1/2}.$$

- H. Toyoizumi and M. Takaya, JORSJ, Vol. 47, No. 1, 38-50, 2004

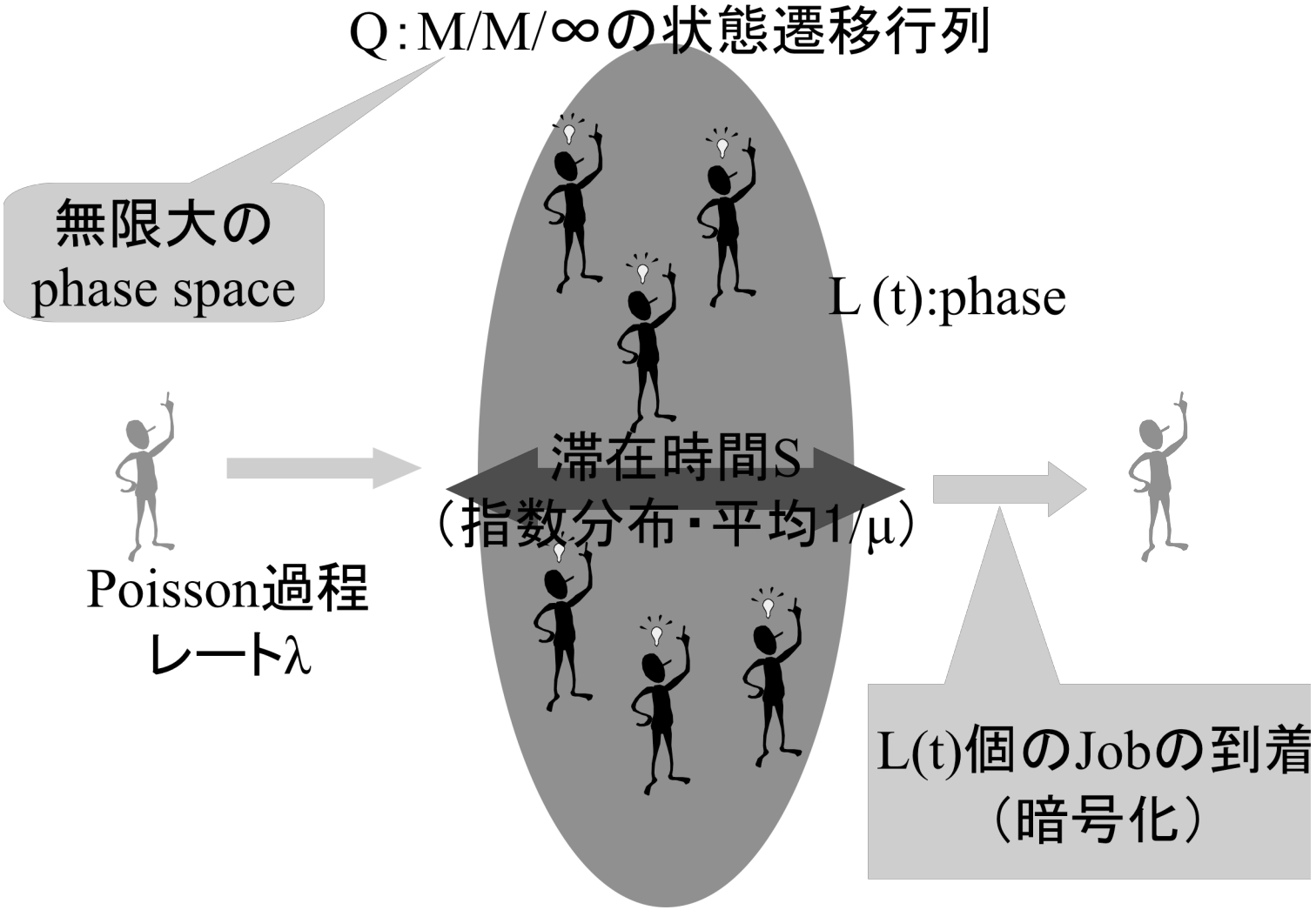
暗号化回数の分布は？

- 暗号化回数の平均は、初等的な方法で求めることができた。
- 暗号化回数が多くなることがある場合には、その処理にかかる時間内でセキュリティーが甘くなっている。
- より厳密な解析が必要

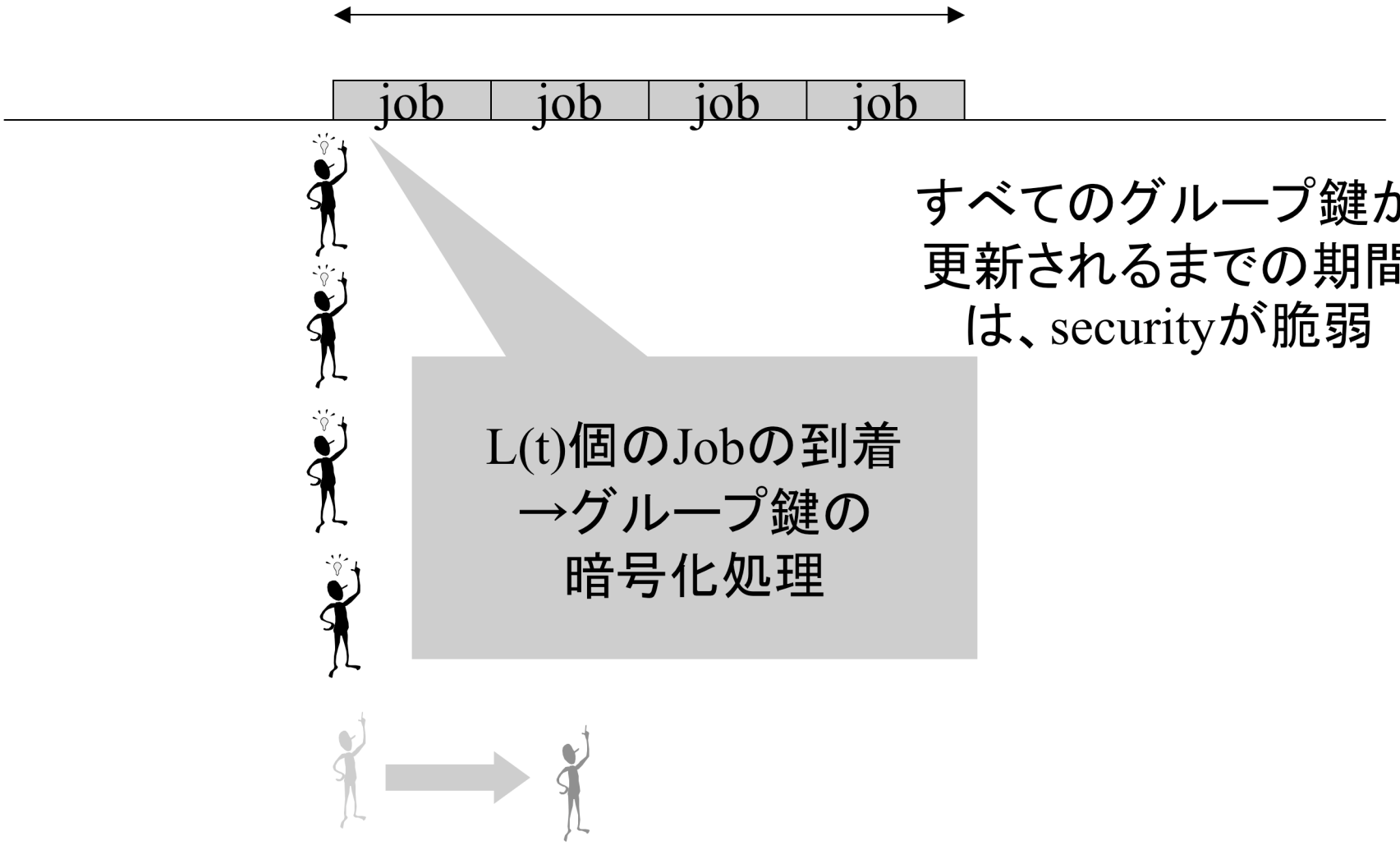
BMAP/M/1 Queueing Model



BMAP/M/1 Queueing Model



Degradation of secutity



Notations

- L(t) : the number of customers in the group,
- M(t) be the number of jobs in the system (key encryption server) at time t.
- X(t) = (L(t), M(t)) is a Markov process.
- π_{l,m} = P[L = l, M = m]

$$\pi_m = (\pi_{m0}, \pi_{m1}, \ldots).$$

$$\pi = (\pi_0, \pi_1, \ldots) = (\pi_{00}, \pi_{01}, \ldots, \pi_{10}, \pi_{11}, \ldots, \pi_{m0}, \pi_{m1}, \ldots).$$

Steady State Equation

- $\pi Q = 0$,where Q is the infinitesimal generator of the Markov Process X(t) = (L(t), M(t)).

$$\mathbf{Q} = \begin{pmatrix} \mathbf{D}_0 & \mathbf{D}_1 & \mathbf{D}_2 & \mathbf{D}_3 & \cdots \\ \sigma\mathbf{I} & \mathbf{D}_0 - \sigma\mathbf{I} & \mathbf{D}_1 & \mathbf{D}_2 & \cdots \\ & \sigma\mathbf{I} & \mathbf{D}_0 - \sigma\mathbf{I} & \mathbf{D}_1 & \cdots \\ & & \sigma\mathbf{I} & \mathbf{D}_0 - \sigma\mathbf{I} & \ddots \\ & & & \ddots & \ddots \end{pmatrix}.$$

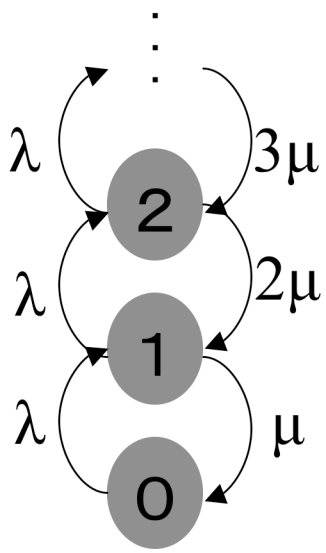
$$\mathbf{D}_l = \begin{matrix} \\ \\ l+1 \end{matrix} \begin{pmatrix} & & l \\ & & \vdots \\ \cdots & (l+1)\mu & \end{pmatrix},$$

$$\mathbf{D}_0 = \begin{pmatrix} -\lambda & \lambda & & & \\ \mu & \lambda - \mu & \lambda & & \\ & & -\lambda - 2\mu & \lambda & \\ & & & \ddots & \ddots \end{pmatrix},$$

Phase transition

$\mathbf{D} = \sum_{l=0}^{\infty} \mathbf{D}_l$: the generator of the phase transitions, is the infinitesimal generator of an M/M/∞ queue, and its stationary probability vector is Poisson distribution with its mean λ/μ.

L (t):phase, the number of customers in the group.



Z-transform and stationary equation

- $\mathbf{\Pi}(z) = \sum_{m=0}^{\infty} z^m \pi_m.$:z-transform of stationary vector.
- Stationary equation

$$\sigma\left(1-\frac{1}{z}\right)\pi_0 + \mathbf{\Pi}(z)\left\{\mathbf{D}(z) - \left(1-\frac{1}{z}\right)\sigma I\right\} = \mathbf{0},$$

$$\mathbf{D}(z) = \begin{pmatrix} -\lambda & \lambda & & & \\ \mu & \lambda-\mu & \lambda & & \\ & 2z\mu & -\lambda-2\mu & \lambda & \\ & & 3z^2\mu & -\lambda-3\mu & \lambda \\ & & & \ddots & \ddots & \ddots \end{pmatrix}.$$

Double z-transform

z:jobの変数

$$\pi(z,y)=\sum_{l=0}^{\infty}y^{l}\Pi_{l}(z)=\sum_{l,m}z^{m}y^{l}\pi_{l,m}=E[z^{M}y^{L}].$$

:double z-transform of stationary vector

y:phaseの変数

π(0,y):M=0とphaseの同時分布

π(1,y):phaseの周辺分布

Linear operator calculus

$f(y) = \sum_{j=0}^{\infty} f_j y^j$ formal power series.

The linear operator U corresponding to a matrix U by

$$[Uf](y) = \sum_{i,j} f_i [\mathbf{U}]_{ij} y^j.$$

The linear operator for D(z):

$$[D(z)f](y) = \mu f_y(zy) + \lambda y f(y) - \lambda f(y) - \mu y f_y(y).$$

$$[D(1)f](y) = \mu(1-y) f_y(y) - \lambda(1-y) f(y).$$

Phase 遷移の
オペレーター

Differentiation by parts

- 合成関数の微分の公式

$$\frac{\partial}{\partial z}[U(z)f(z)](y) = \frac{\partial}{\partial z}\left\{\sum_{i,j} f_i(z)[\mathbf{U}(z)]_{ij}y^j\right\} = [U'(z)f(z)](y) + [U(z)f_z(z)](y).$$

$$f(z,y) = \sum_j f_j(z)y^j.$$

Theorem 1.

- The double z-transform of the stationary probability π(z, y) should satisfy the following equation:

$$\sigma\left(1-\frac{1}{z}\right)\{\pi(0,y)-\pi(z,y)\}+[D(z)\pi(z)](y)=0,$$

$$[D(z)\pi(z)](y)=\mu\pi_y(z,zy)+\lambda y\pi(z,y)-\lambda\pi(z,y)-\mu y\pi_y(z,y).$$

$\pi(1,y)=e^{\frac{\lambda}{\mu}(y-1)}$: phaseのmarginal distribution

$$[D(1)\pi(1)](y)=0.$$

Utilization

- $\rho = P[M > 0]$:使用率

$$\rho = \frac{\lambda^2}{\sigma\mu} = \frac{1}{\sigma}\lambda E[L]$$

到着率×平均客数

Operator A and its inverse

- [Af](y) = [D(1)f](y) + f(1)π(1, y)
- Inverse of A

$$[A^{-1}g](y) = \pi(1,y)\left\{g(1) - \int_y^1 \frac{g(u)e^{-\frac{\lambda}{\mu}(u-1)} - g(1)}{\mu(1-u)}du\right\}$$

u=1に見かけ上の特異点

$$\lim_{u\to 1}\frac{g(u)e^{-\frac{\lambda}{\mu}(u-1)} - g(1)}{\mu(1-u)} = \frac{g'(1) - \frac{\lambda}{\mu}g(1)}{-\mu}$$

- π(1, y) = e^{μ (y−1)} is the fixed point of the operator A

Theorem 3

- The mean queue length of encryption jobs E[M] can be obatined by

$$E[M] = \frac{\rho}{1-\rho} + \frac{1}{\sigma(1-\rho)}\Big\{\sigma^2\rho^2 + \frac{1}{2}[D''(1)\pi(1)](1) - \sigma[D'(1)A^{-1}\pi(0)](1) - [D'(1)A^{-1}D'(1)\pi(1)](1)\Big\}$$

形は複雑に見えるが、
通常のBMAP/M/1と同形

Matrix analysis

1. 基本行列Gが満足する行列方程式をみつける。
2. その方程式を使ってGをiterationで求める。
3. Gの定常分布を求める。
4. 系内客数定常分布の導出。
5. A にあたる行列の逆行列を求める。
6. モーメントの計算

問題点

- Group Securityのモデルは、phaseがM/M/∞である。そのため、Gに相当するのが、operatorになってしまう。
- 本質的に、高次元（１万人の客？）を相手にするため、打ち切りをしても数値的に安定した解が得られるか不明。

解決策

- Aのinverse operatorの陽表現が得られている。
- Theorem 3で平均客数を求める式が得られている。π(1,y)は既知。

$$E[M] = \frac{\rho}{1-\rho} + \frac{1}{\sigma(1-\rho)}\Big\{\sigma^2\rho^2 + \frac{1}{2}[D''(1)\pi(1)](1) - \sigma[D'(1)A^{-1}\pi(0)](1) - [D'(1)A^{-1}D'(1)\pi(1)](1)\Big\}$$

π(0,y)の項を無視する!

Term by term

$$E[M] = \frac{\rho}{1-\rho} + \frac{1}{\sigma(1-\rho)}\Big\{\sigma^2\rho^2 + \frac{1}{2}[D''(1)\pi(1)](1) - \sigma[D'(1)A^{-1}\pi(0)](1) - [D'(1)A^{-1}D'(1)\pi(1)](1)\Big\}$$

A,D,πの性質より

$$\begin{cases} [D''(1)\pi(1)](1) = \lambda\left(\frac{\lambda}{\mu}\right)^2 \\ [D'(1)A^{-1}\pi(0)](1) = \left(\frac{\lambda}{\mu}\right)\left[(1-\rho)\left\{\lambda + \frac{3}{2}\left(\frac{\lambda}{\mu}\right)\right\} - \pi_y(0,1)\right] \\ [D'(1)A^{-1}D'(1)\pi(1)](1) = \lambda(\lambda-1)\left(\frac{\lambda}{\mu}\right)^2 \end{cases}$$

$$0 \le \pi_y(0,1) = E[L(t)1_{(M(t)=0)}] \le E[L(t)] = \lambda/\mu.$$

→ Bounds of E[M]

Theorem 4

- The bounds of mean queue length E[M] can be found by

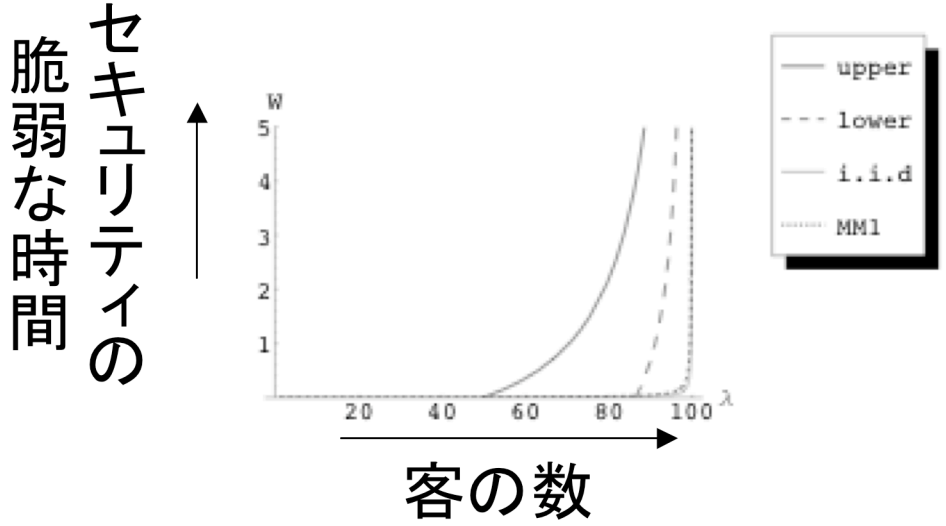
$$E[M] \leq \frac{\rho}{1-\rho} + \frac{1}{2(1-\rho)}\left\{\sigma\rho^2 + (1-3\rho)\left(\frac{\lambda}{\mu}\right)^2 + \rho\left(\frac{\lambda}{\mu}\right)\right\}, \tag{35}$$

and

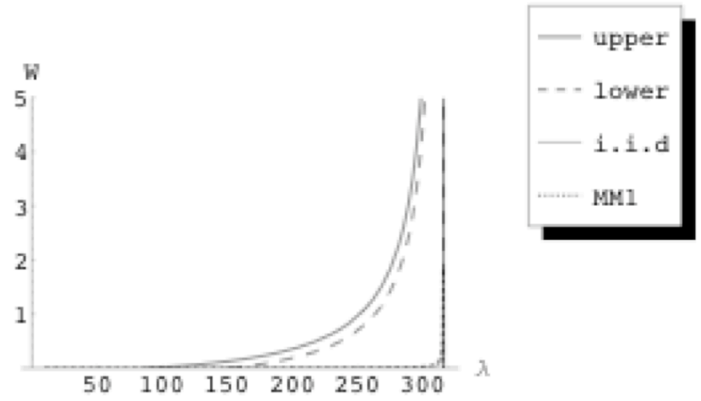
$$E[M] \geq \frac{\rho}{1-\rho} + \frac{1}{2(1-\rho)}\left\{\sigma\rho^2 + 3(1-\rho)\left(\frac{\lambda}{\mu}\right)^2 + \rho\left(\frac{\lambda}{\mu}\right)\right\}. \tag{36}$$

Upper bound and lower bound of E[W] when $\mu = 1$

- In the following, we fixed the service rate of the encryptions to be $\sigma = 10,000$.
- The lines “upper ” and “lower” are the upper and lower bounds of mean waiting time respectively. The line “i.i.d” corresponds to the batch arrival M/M/1 queue where the batch size is independent and identically to Poisson distribution with its mean λ/μ.



Upper bound and lower bound of E[W] when μ = 10.



Upper bound and lower bound of E[W] when μ = 100.