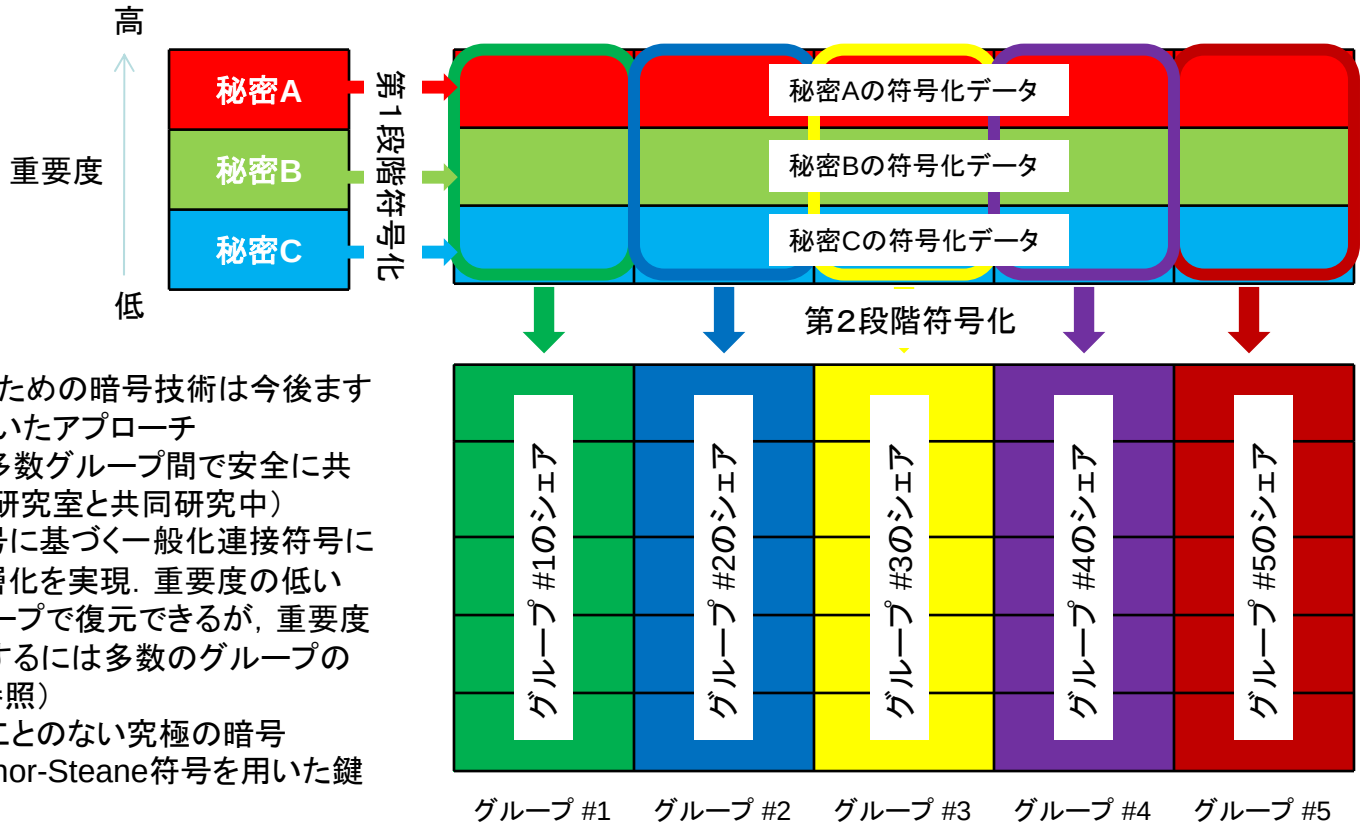
誤り訂正符号の暗号技術への応用： 秘密分散と量子暗号

システムデザイン学部情報通信システム工学コース　助教
藤田　八郎　　西谷研究室
E-mail hfujita@center.tmu.ac.jp



＜概要＞

安全・安心な社会を実現するための暗号技術は今後ますます重要： 誤り訂正符号を用いたアプローチ

- 階層構造をもつ秘密情報を多数グループ間で安全に共有（職業能力開発大学校松嶋研究室と共同研究中）
  - ✓ Reed-Solomon符号に基づく一般化連接符号により秘密情報の階層化を実現．重要度の低い秘密は少数のグループで復元できるが，重要度の高い秘密を復元するには多数のグループの協力が必要（右図参照）
- 量子暗号は絶対に破られることのない究極の暗号
  - ✓ 拡張Calderbank-Shor-Steane符号を用いた鍵生成レートの改善