SecGraph: A Uniform and Open-source Evaluation System for Graph Data Anonymization and De-anonymization

Shouling Ji, Weiqing Li, and Raheem Beyah
Georgia Institute of Technology

Prateek Mittal
Princeton University

Xin Hu
IBM Research
Introduction

- **Graph Data**
  - Social networks data
  - Mobility traces
  - Medical data
  - ......

- **Why data sharing/publishing**
  - Academic research
  - Business applications
  - Government applications
  - Healthcare applications
  - ......
Anonymization and De-anonymization

Utility

Anonymization vs DA

SecGraph: A Uniform and Open-Source Evaluation System
**Contribution**

- We studied and analyzed
  - 11 state-of-the-art graph anonymization techniques
  - 15 modern Structure-based De-Anonymization (SDA) attacks

- We developed and evaluated SecGraph
  - 11 anonymization techniques
  - 12 graph utility metrics
  - 7 application utility metrics
  - 15 de-anonymization attacks

- We released SecGraph
  - Publicly available at [http://www.ece.gatech.edu/cap/secgraph/](http://www.ece.gatech.edu/cap/secgraph/)
Outline

• Introduction
• Graph Anonymization
• Graph De-anonymization
• Anonymization vs. De-anonymization Analysis
• SecGraph
• Conclusion
Graph Anonymization

- Naïve ID Removal
- Edge Editing (EE) based anonymization
  - Add/Del
  - Switch
- **K-anonymity**
  - K-Neighborhood Anonymization (k-NA)
  - K-Degree Anonymization (k-DA)
  - K-automorphism (k-auto)
  - K-isomorphism (k-iso)
- Aggregation/class/cluster based anonymization
- Differential Privacy (DP) based anonymization
- Random Walk (RW) based anonymization
Utility Metrics

• Graph utility (12)
  – Degree (Deg.)
  – Joint Degree (JD)
  – Effective Diameter (ED)
  – Path Length (PL)
  – Local Clustering Coefficient (LCC)
  – Global Clustering Coefficient (GCC)
  – Closeness Centrality (CC)
  – Betweenness Centrality (BC)
  – Eigenvector (EV)
  – Network Constraint (NC)
  – Network Resilience
  – Infectiousness (Infe.)

• Application utility (7)
  – Role eXtraction (RX)
  – Influence Maximization (IM)
  – Minimum-sized Influential Node Set (MINS)
  – Community Detection (CD)
  – Secure Routing (SR)
  – Sybil Detection (SD)

Graph utility captures how the anonymized data preserve fundamental structural properties of the original graph

How useful the anonymized data are for practical graph applications and mining tasks
## Anonymization vs Utility

<table>
<thead>
<tr>
<th>Anonymization Techniques</th>
<th>graph utility</th>
<th>application utility</th>
<th>Resilient to DA attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Naive</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Add/Del [6]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switch [6]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>k-NA [7]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>k-DA [8]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>k-auto [9]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>k-iso [10]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Aggregation [12]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cluster [14]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DP [15]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DP [16, 17]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DP [18]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DP [19]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RW [20]</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Conditionally preserve the utility</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Partially preserve the utility</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not preserve the utility</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Notes:

- **Deg.** Degradation
- **JD** Joint Distribution
- **ED** Edge Distribution
- **PL** Path Length
- **LCC** Largest Connected Component
- **GCC** Global Clustering Coefficient
- **CC** Clustering Coefficient
- **BC** Betweenness Centrality
- **EV** Eigenvector Centrality
- **NC** Node Centrality
- **NR** Node Ranking
- **Infe** Influence
- **RX** Resource eXtraction
- **RE** Resource Evolution
- **IM** Information Management
- **MINS** Minimal Network Security
- **CD** Communication Distance
- **SR** Social Rank
- **SD** Social Distance

*SecGraph: A Uniform and Open-Source Evaluation System*
<table>
<thead>
<tr>
<th>Anonymization Techniques</th>
<th>Deg.</th>
<th>JD</th>
<th>ED</th>
<th>PL</th>
<th>LCC</th>
<th>GCC</th>
<th>CC</th>
<th>BC</th>
<th>EV</th>
<th>NC</th>
<th>NR</th>
<th>Infe.</th>
<th>RX</th>
<th>RE</th>
<th>IM</th>
<th>MINS</th>
<th>CD</th>
<th>SR</th>
<th>SD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Naive</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Add/Del [6]</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Switch [6]</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>k-NA [7]</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>k-DA [8]</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>k-auto [9]</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>k-iso [10]</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Aggregation [12]</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Cluster [14]</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>DP [15]</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>DP [16, 17]</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>DP [18]</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>DP [19]</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>RW [20]</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

- **Anonymization Techniques**
  - Naive
  - Add/Del [6]
  - Switch [6]
  - k-NA [7]
  - k-DA [8]
  - k-auto [9]
  - k-iso [10]
  - Aggregation [12]
  - Cluster [14]
  - DP [15]
  - DP [16, 17]
  - DP [18]
  - DP [19]
  - RW [20]

- **Resilient to DA attacks**
  - R2SDA

- **Conditionally preserve the utility**

- **Partially preserve the utility**

- **Not preserve the utility**

---

S. Ji, W. Li, P. Mittal, X. Hu, and R. Beyah

SecGraph: A Uniform and Open-Source Evaluation System

9
Outline

• Introduction
• Graph Anonymization
• Graph De-anonymization
• Anonymization vs. De-anonymization Analysis
• SecGraph
• Conclusion
Graph De-Anonymization (DA)

- **Seed-based DA**
  - Backstrom et al.’s attack (BDK)
  - Narayanan-Shmatikov’s attack (NS)
  - Narayanan et al.’s attack (NSR)
  - Nilizadeh et al.’s attack (NKA)
  - Distance Vector (Srivatsa-Hicks attack) (DV)
  - Randomized Spanning Trees (Srivatsa-Hicks attack) (RST)
  - Recursive Subgraph Matching (Srivatsa-Hicks attack) (RSM)
  - Yartseva-Grossglauser’s attack (YG)
  - De-Anonymization attack (Ji et al.’s attack) (DeA)
  - Adaptive De-Anonymization attack (Ji et al.’s attack) (ADA)
  - Korula-Lattanzi’s attack (KL)

- **Seed-free DA**
  - Pedarsani et al.’s attack (PFG)
  - Ji et al.’s attack (JLSB)

Figure source: E. Kazemi et al., Growing a Graph Matching from a Handful of Seeds, VLDB 2015
## DA Attacks

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>BDK [26]</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>A, P</td>
<td>✗</td>
<td>☐</td>
<td>✗</td>
</tr>
<tr>
<td>NS [2]</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
<td>P</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>NSR [21]</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
<td>P</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>NKA [22]</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
<td>P</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>DV [5]</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
<td>P</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>RST [5]</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
<td>P</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>RSM [5]</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
<td>P</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>PFG [23]</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>P</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>YG [27]</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
<td>P</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>ADA [25]</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
<td>P</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>KL [24]</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
<td>P</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>JLSB [3]</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>P</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

SF: seed-free  
AGF: auxiliary graph-free  
SemF: semantics-free  
A/P: active/passive attack  
Scal.: scalable  
Prac.: practical  
Rob.: robust to noise

- ✓ = true  
- ☐ = partially true  
- ♦ = conditionally true  
- ✗ = false
Outline

• Introduction
• Graph Anonymization
• Graph De-anonymization
• Anonymization vs. De-anonymization Analysis
• SecGraph
• Conclusion
# Anonymization vs. DA

**State-of-the-art Anonymization Techniques**

<table>
<thead>
<tr>
<th>Technique</th>
<th>Naive</th>
<th>EE</th>
<th>$k$-anony.</th>
<th>Cluster</th>
<th>DP</th>
<th>RW</th>
</tr>
</thead>
<tbody>
<tr>
<td>BDK [26]</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>X</td>
<td>✓</td>
<td>X</td>
</tr>
<tr>
<td>NS [2]</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>X</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>NSR [21]</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>X</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>NKA [22]</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>X</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>DV [5]</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>X</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>RST [5]</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>X</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>RSM [5]</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>X</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>PFG [23]</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>X</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>YG [27]</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>X</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>ADA [25]</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>X</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>KL [24]</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>X</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>JLSB [3]</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>X</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

**Modern DA Attacks**

- ✓: vulnerable
- ♦: conditionally vulnerable
- X: invulnerable

**DA attacks!**
Outline

- Introduction
- Graph Anonymization
- Graph De-anonymization
- Anonymization vs. De-anonymization Analysis
- SecGraph
- Conclusion
SecGraph: Overview & Implementation

Raw Data -> AM -> Anonymized Data -> UM/DM -> Publishing Data
Raw Data -> Publishing Data
Raw Data -> UM/DM -> AM -> Anonymized Data -> Publishing Data

19 Utility Metrics
15 DA Attacks

Utility Module (UM)
DA Module (DM)
Anonymization Module (AM)
Anonymized Data
Publishing Data

11 Anonymization Techniques
SecGraph: Evaluation

- **Datasets**
  - Enron (36.7K users, 0.2M edges): an email network dataset
  - Facebook – New Orleans (63.7K users, 0.82M edges): a Facebook friendship dataset in the New Orleans area

- **Evaluation settings**
  - Follow the same/similar settings in the original papers
  - See details in the paper and [http://www.ece.gatech.edu/cap/secgraph/](http://www.ece.gatech.edu/cap/secgraph/)

- **Evaluation scenarios**
  - Anonymization vs Utility
  - DA performance
  - Robustness of DA attacks
  - Anonymization vs DA
### SecGraph: Anonymity vs Utility

**C1:** existing anonymization techniques are better at preserving graph utilities

**C2:** all the anonymization techniques lose one or more application utility
SecGraph: DA Performance

Table 6: Performance of DA attacks. $s$ is the probability of generating the auxiliary and anonymized graphs from the original graph. Each value, e.g., 0.1277, in the table indicates the ratio of successfully de-anonymized users.

C1: the phase transitional (percolation) phenomena is attack-dependent
SecGraph: Robustness of DA Attacks

C1: global structure-based DA attacks are more robust to seed errors
SecGraph: Anonymization vs DA

<table>
<thead>
<tr>
<th></th>
<th>Enron</th>
<th>Facebook</th>
</tr>
</thead>
<tbody>
<tr>
<td>s</td>
<td>5</td>
<td>10</td>
</tr>
<tr>
<td>NS</td>
<td>.85</td>
<td>.0072</td>
</tr>
<tr>
<td></td>
<td>.90</td>
<td>.0077</td>
</tr>
<tr>
<td></td>
<td>.95</td>
<td>.3577</td>
</tr>
<tr>
<td>DV</td>
<td>.85</td>
<td>.1261</td>
</tr>
<tr>
<td></td>
<td>.90</td>
<td>.1546</td>
</tr>
<tr>
<td></td>
<td>.95</td>
<td>.2121</td>
</tr>
<tr>
<td>PFG</td>
<td>.85</td>
<td>.0667</td>
</tr>
<tr>
<td></td>
<td>.95</td>
<td>.1193</td>
</tr>
<tr>
<td>YG</td>
<td>.85</td>
<td>.1373</td>
</tr>
<tr>
<td></td>
<td>.90</td>
<td>.1716</td>
</tr>
<tr>
<td></td>
<td>.95</td>
<td>.1730</td>
</tr>
<tr>
<td>ADA</td>
<td>.85</td>
<td>.1262</td>
</tr>
<tr>
<td></td>
<td>.90</td>
<td>.1543</td>
</tr>
<tr>
<td></td>
<td>.95</td>
<td>.2139</td>
</tr>
<tr>
<td>KL</td>
<td>.85</td>
<td>.0904</td>
</tr>
<tr>
<td></td>
<td>.90</td>
<td>.1077</td>
</tr>
<tr>
<td></td>
<td>.95</td>
<td>.1381</td>
</tr>
<tr>
<td>JLSE</td>
<td>.85</td>
<td>.0692</td>
</tr>
<tr>
<td></td>
<td>.90</td>
<td>.0886</td>
</tr>
<tr>
<td></td>
<td>.95</td>
<td>.1846</td>
</tr>
</tbody>
</table>

**C1:** state-of-the-art anonymization techniques are vulnerable to one or several modern DA attacks

**C2:** no DA attack is general optimal. The DA performance depends on several factors, e.g., similarity between anonymized and auxiliary graphs, graph density, and DA heuristics
SecGraph: Release & Support

- **Website**
  - [http://www.ece.gatech.edu/cap/secgraph/](http://www.ece.gatech.edu/cap/secgraph/)
- **Software**
- **Datasets**
- **Documents**
- **Demo**
- **Q&A**

- **Modes**
  - GUI
  - Command line

- **Supporting**
  - Windows
  - Linux
  - Mac
Conclusion

We analyzed existing graph anonymization techniques and de-anonymization attacks

We implemented and evaluated SecGraph: a uniform and open-source evaluation system from graph data anonymization and de-anonymization

Acknowledgement

We thank the anonymous reviewers very much for their valuable comments!

We are grateful to the following researchers in developing SecGraph: Ada Fu, Michael Hay, Davide Proserpio, Qian Xiao, Shirin Nilizadeh, Jing S. He, Wei Chen, and Stanford SNAP developers
Thank you!

Shouling Ji

sji@gatech.edu

http://www.ece.gatech.edu/cap/secgraph/

http://users.ece.gatech.edu/sji/