ENCRYPTO
CRYPTOGRAPHY AND
PRIVACY ENGINEERING

MULTICENT

Secure and Scalable Computation of Centrality Measures on Multilayer Graphs

Andreas Brüggemann, Nishat Koti, Varsha Bhat Kukkala, Thomas Schneider

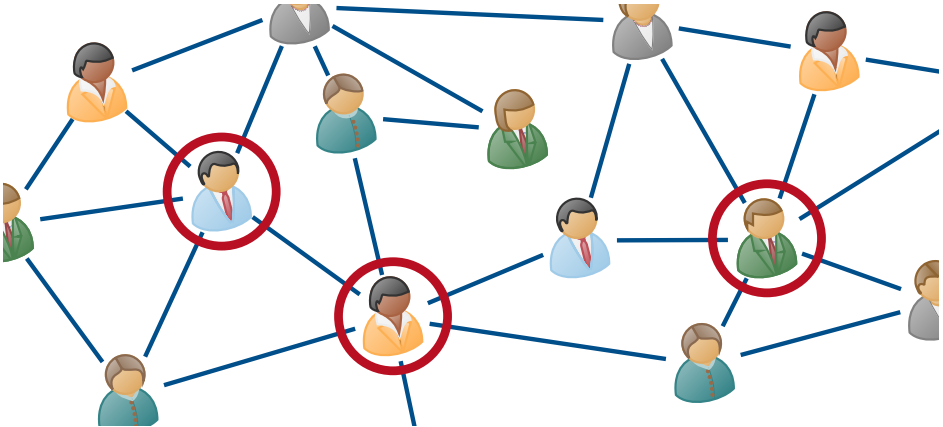
TECHNISCHE
UNIVERSITÄT
DARMSTADT

Contact

https://encrypto.de

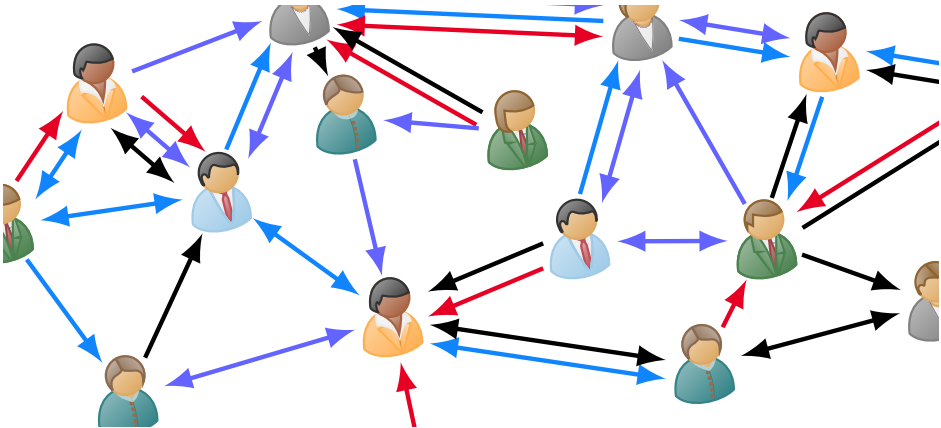
Identifying Important Nodes in Social Graphs

ENCRYPTO
CRYPTOGRAPHY AND
PRIVACY ENGINEERING

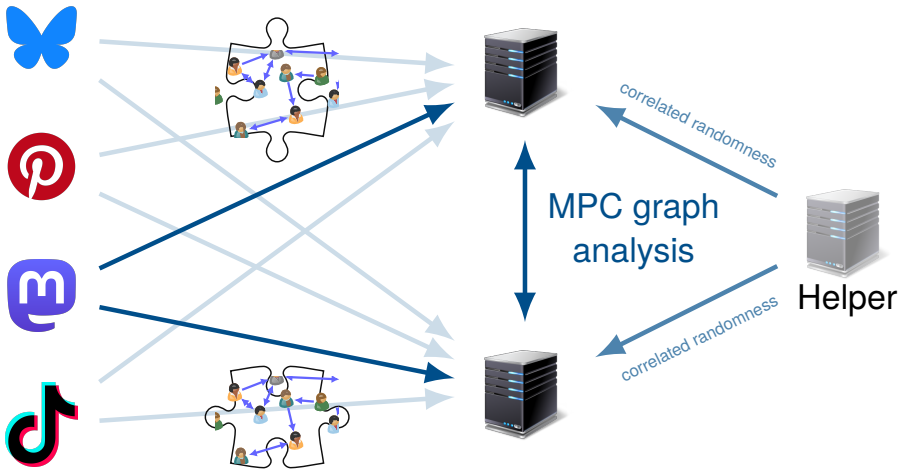


Social Networks as Multilayer Graphs

ENCRYPTO
CRYPTOGRAPHY AND
PRIVACY ENGINEERING



System Model



Centrality Measures

ENCRYPTO
CRYPTOGRAPHY AND
PRIVACY ENGINEERING

- **Reach Score**:
  # nodes reachable within some radius
- **Truncated Katz Score** [Kat53; FMP+01]:
  (Weighted) # outgoing paths within length bound
- **Multilayer Truncated Katz Score** [ABGT17]:
  More weight for edges of higher multiplicity

[Kat53] L. Katz. “A new status index derived from sociometric analysis”. *Psychometrika* 18.1 (1953)

[FMP+01] K. C. Foster, S. Q. Muth, J. J. Potterat, and R. B. Rothenberg. “A Faster Katz Status Score Algorithm”. *Computational & Mathematical Organization Theory* 7 (2001)

[ABGT17] G. Asharov, F. Bonchi, D. Garcia-Soriano, and T. Tassa. “Secure Centrality Computation Over Multiple Networks”. *WWW*. 2017

Our Contributions

ENCRYPTO
CRYPTOGRAPHY AND
PRIVACY ENGINEERING

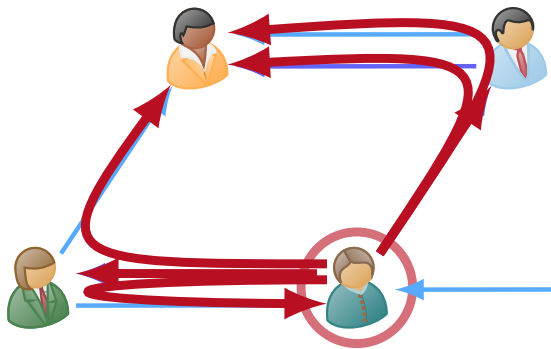
- **Keeping it Local**: Efficient vertex-centric computation by message-passing
- **Keeping it Compact**: Representing large graphs efficiently while allowing data-oblivious processing
- **Scalable Implementation**: Scalable, publicly available implementation & extensive benchmarks

Keeping it Local

Efficient vertex-centric computation by message-passing

Centrality Measures

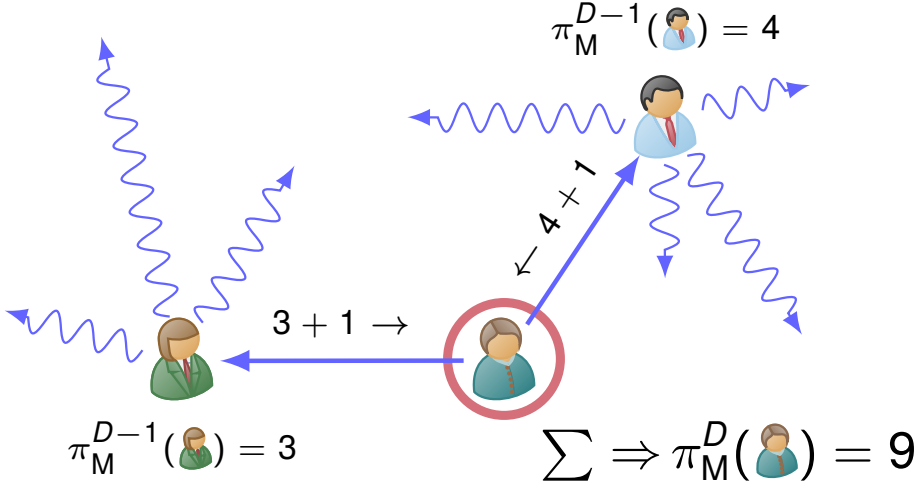
Example: Multilayer Truncated Katz Score



$$\pi^1_M(\text{person}) = \beta_1 \cdot 2$$
$$\pi^2_M(\text{person}) = \beta_1 \cdot 2 + \beta_2 \cdot 4$$

Inductively Computing Centrality Measures

Example: Multilayer Truncated Katz Score



Keeping it Compact

Representing large graphs efficiently while allowing data-oblivious processing

Graph Representation Matters

ENCRYPTO
CRYPTOGRAPHY AND
PRIVACY ENGINEERING

- Prior SOTA for multilayer centrality measures in MPC [ABGT17]: Adjacency matrices

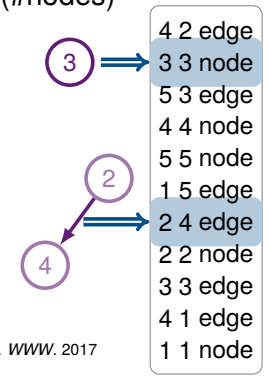
$$\begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

$\Rightarrow$ 100k nodes: **37 GiB** representation size, quadratic growth (#nodes)

- Better for **sparse graphs**: List-based representation

$\Rightarrow$ 100k nodes, 1M edges: **13 MiB** representation size, linear growth (#nodes + #edges)

- Extra care required to keep representation and control flow independent of graph structure



[ABGT17] G. Asharov, F. Bonchi, D. Garcia-Soriano, and T. Tassa. “Secure Centrality Computation Over Multiple Networks”. *WWW*. 2017

Message-Passing in MPC

ENCRYPTO
CRYPTOGRAPHY AND
PRIVACY ENGINEERING

- Identified Graphiti [KKP+24] as prior SOTA for message-passing

- Improved initialization (bottleneck) by SOTA sorting [AHI+22]
- Removed quadratic overhead of input phase
- Extended to multigraphs
- Embedded centrality measures

[KKP+24] N. Koti, V. B. Kukkala, A. Patra, and B. R. Gopal. “Graphiti: Secure Graph Computation Made More Scalable”. *CCS*. 2024

[AHI+22] G. Asharov, K. Hamada, D. Ikarashi, R. Kikuchi, A. Nof, B. Pinkas, K. Takahashi, and J. Tomida. “Efficient Secure Three-Party Sorting with Applications to Data Analysis and Heavy Hitters”. *CCS*. 2022

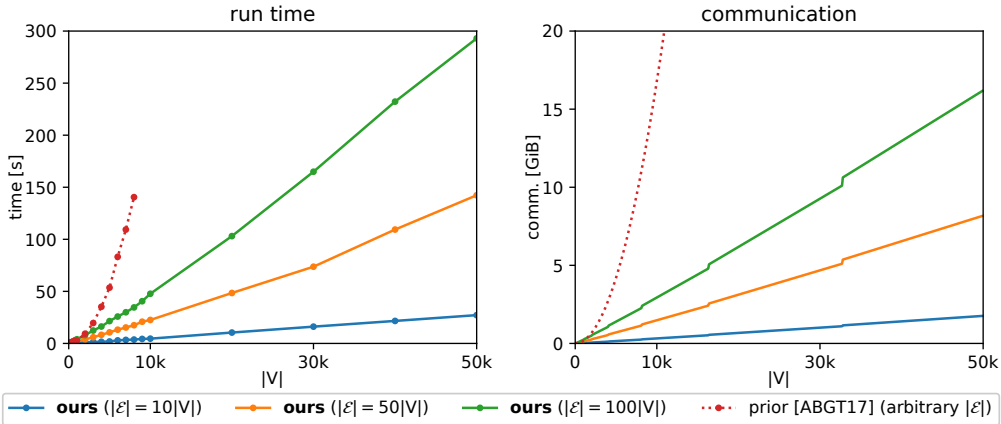
Scalable Implementation

Scalable, publicly available implementation & extensive benchmarks

Scalability Benchmarks (π_{M}^{10}: 10 Iterations)

ENCRYPTO
CRYPTOGRAPHY AND
PRIVACY ENGINEERING

LAN setting



even below 7 minutes for 500k nodes, 5M edges!

Implementations for MPC Message-Passing on Graphs

ENCRYPTO
CRYPTOGRAPHY AND
PRIVACY ENGINEERING

- 2015: GraphSC [NWI+15] ..... **Implementation available**
- 2021: SGAS [AFO+21] ..... **Implementation undisclosed**
- 2024: Graphiti [KKP+24] ..... **Microbenchmarking of some components**
- 2025: **MultiCent** ..... **Implementation available**

Source Code

`https://encrypto.de/code/MultiCent`

Artifact:
– **Available**
– **Functional**
– **Reproduced**

Stay tuned!
MPC message-passing framework under development!

[NWI+15] K. Nayak, X. S. Wang, S. Ioannidis, U. Weinsberg, N. Taft, and E. Shi. “GraphSC: Parallel Secure Computation Made Easy”. *S&P*. 2015
[AFO+21] T. Araki, J. Furukawa, K. Ohara, B. Pinkas, H. Rosemarin, and H. Tsuchida. “Secure Graph Analysis at Scale”. *CCS*. 2021
[KKP+24] N. Koti, V. B. Kukkala, A. Patra, and B. R. Gopal. “Graphiti: Secure Graph Computation Made More Scalable”. *CCS*. 2024

ENCRYPTO
CRYPTOGRAPHY AND
PRIVACY ENGINEERING

Keeping it Local **Keeping it Compact** **Scalable Implementation**

Check our paper for:

- All three centrality measures
- Details on expressing all centrality measures through message-passing
- Full details on MPC protocols
- Extensive evaluation results

https://eprint.iacr.org/2025/652

Questions?