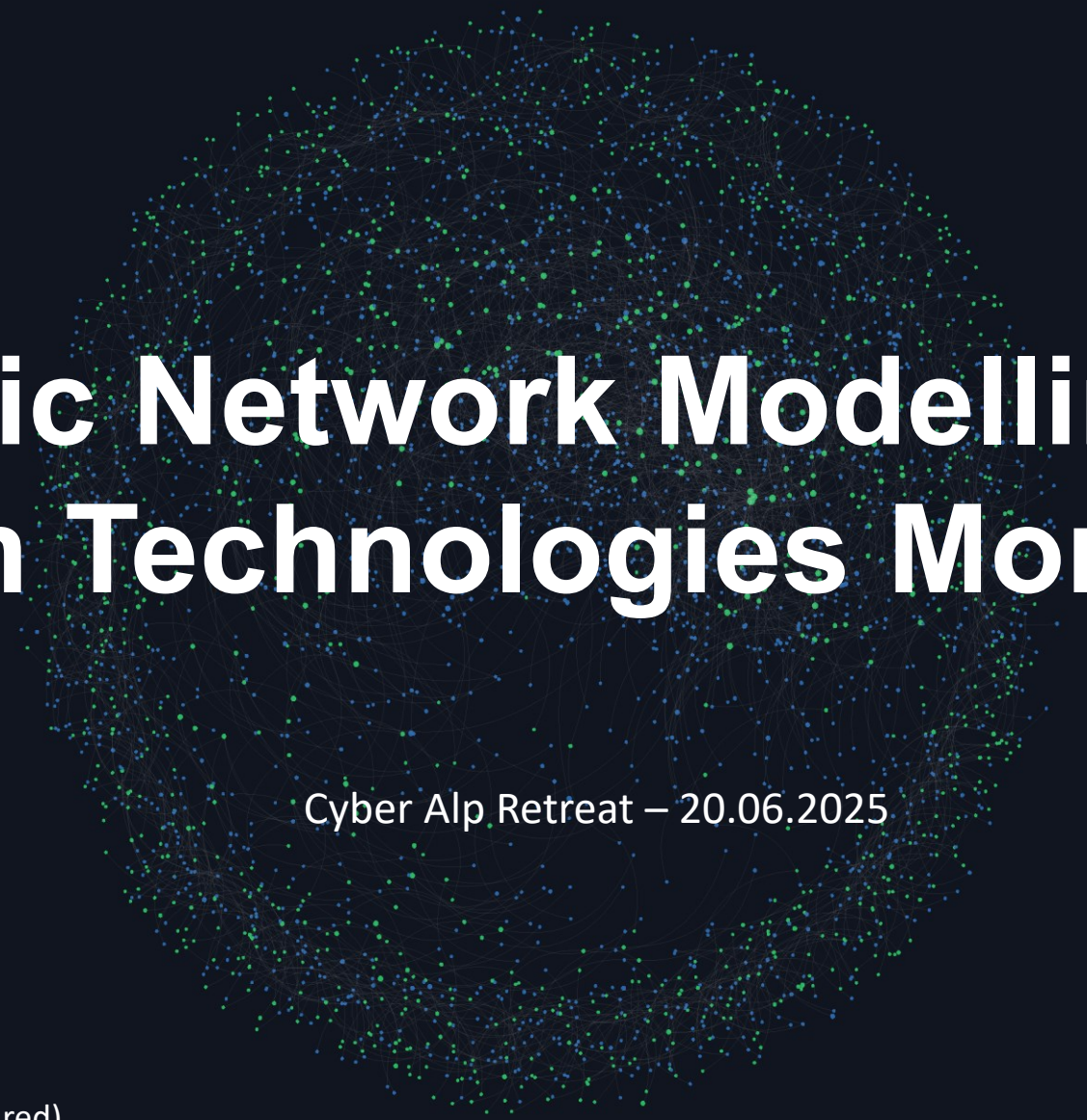


Dynamic Network Modelling for Quantum Technologies Monitoring

Cyber Alp Retreat – 20.06.2025

Jean-Marie Le Goff/PhD, Dphil CERN (retired)

Dtangle https://dtangle.ch

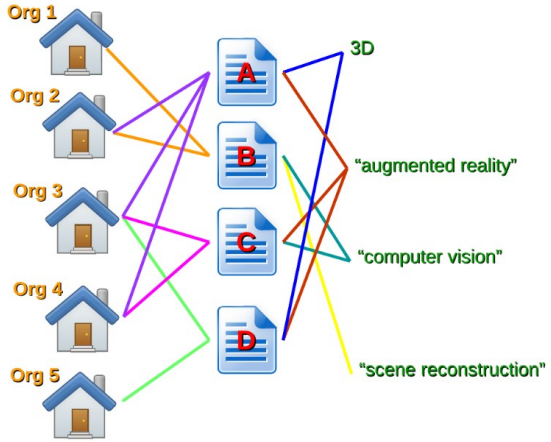
Graphs are best at representing networks but there are risk of loosing information

- Tabular data (incident matrix) contains more than the data elements. Connectivity: Data elements are connected together within a row

Incident matrix

PubRef	Organisations	Keywords
PubA	['Org2', 'Org3', 'Org4']	['3D', 'Augmented Reality']
PubB	['Org1', 'Org2']	['Computer Vision', 'Scene Reconstruction']
PubC	['Org3', 'Org4']	['Augmented Reality', 'Scene Reconstruction']
PubD	['Org3', 'Org5']	['3D', 'Augmented Reality']

a. A publication network



b. Co-occurrences of organizations with keyword as reference

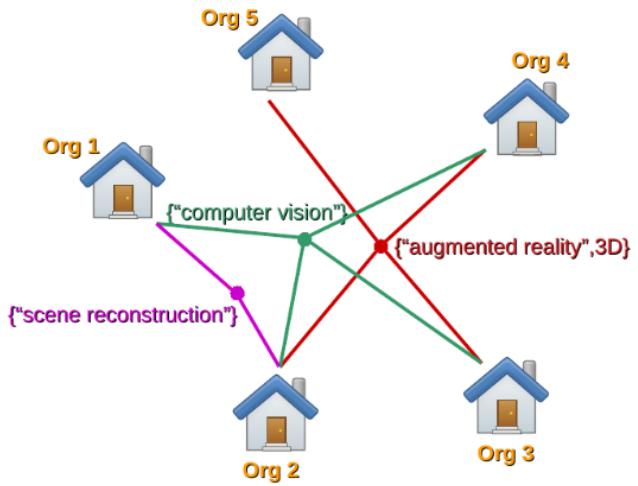
scene reconstruction	$\{\{\text{Org } 1^1, \text{Org } 2^1\}\}$
computer vision	$\{\{\text{Org}1^1, \text{Org}2^1, \text{Org } 3^1, \text{Org } 4^1\}\}$
augmented reality	$\{\{\text{Org } 2^1, \text{Org } 3^3, \text{Org } 4^2, \text{Org } 5^1\}\}$
3D	$\{\{\text{Org } 2^1, \text{Org } 3^2, \text{Org } 4^1, \text{Org } 5^1\}\}$

Edge colors highlight co-occurences in graph representation

Co-occurrence networks are accurately represented as hbgraphs where rows represent hyper bag (hb) edges

This kind of representation doesn't scale up. Complexity hinders insight.

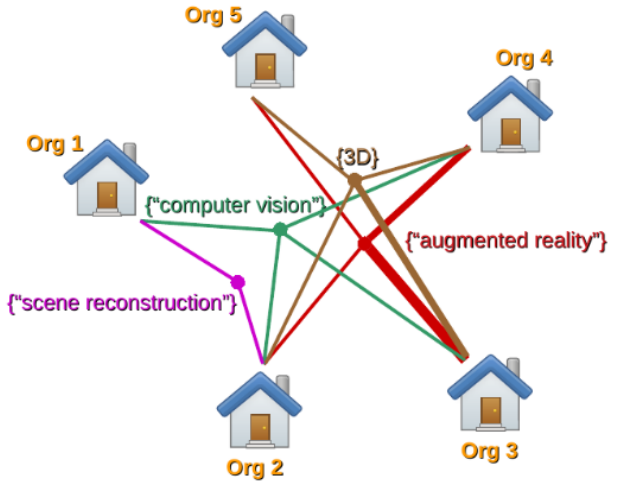
b.(i) Support hypergraph



Vertex weighted degree ranking:
1. Org 2;
2. Org 3; Org 4;
4: Org 5; Org 1.

Hyperedge weighted cardinality ranking:
1. CV, AR, 3D; 2. SR

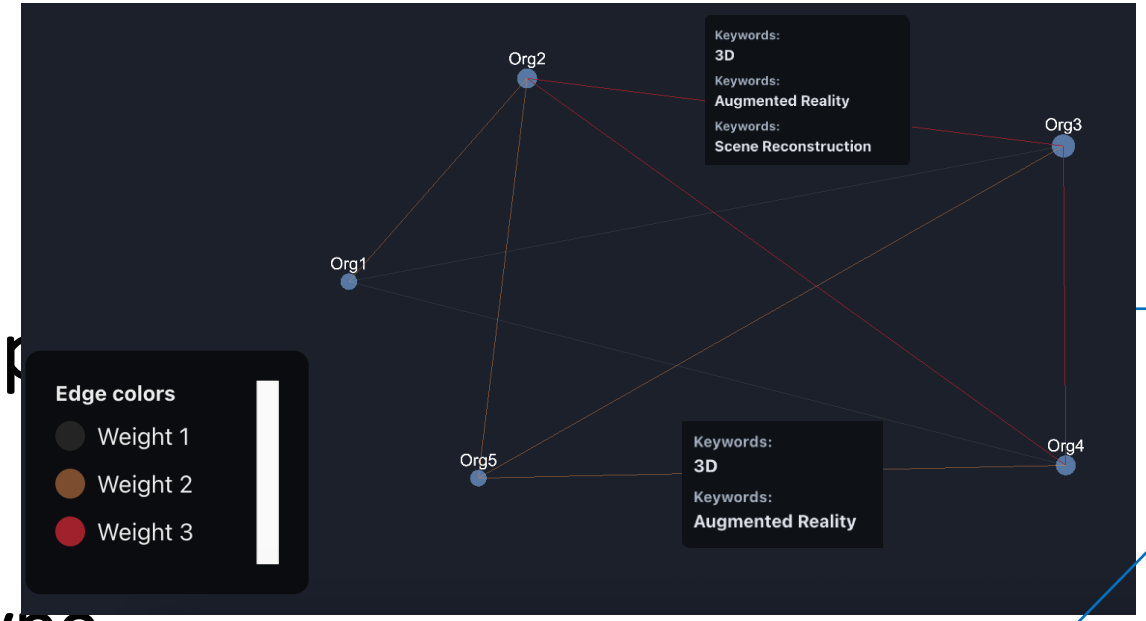
b.(ii) Hb-graph

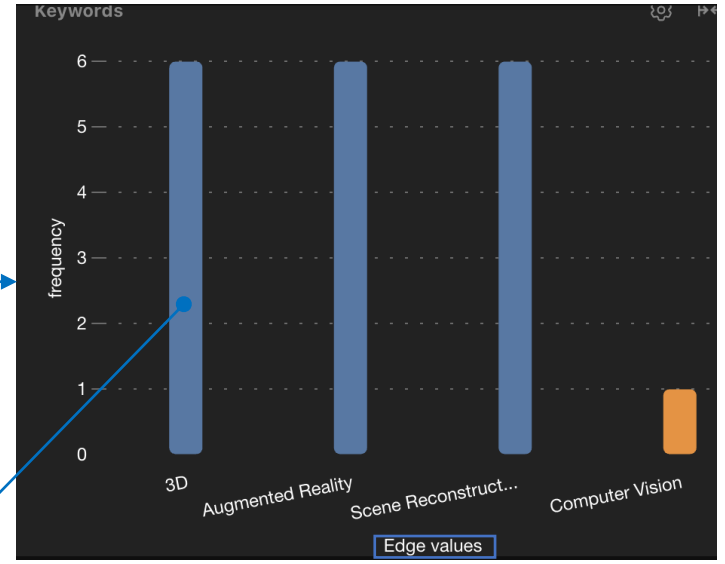


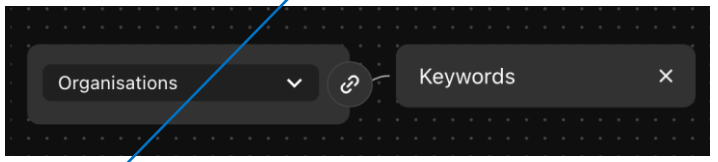
Vertex weighted m-degree ranking:
1. Org 3;
2. Org 2; Org 4;
4: Org 5; Org 1.

Hb-edge weighted m-cardinality ranking:
1. AR; 2: 3D; 3: CV; 4: SR

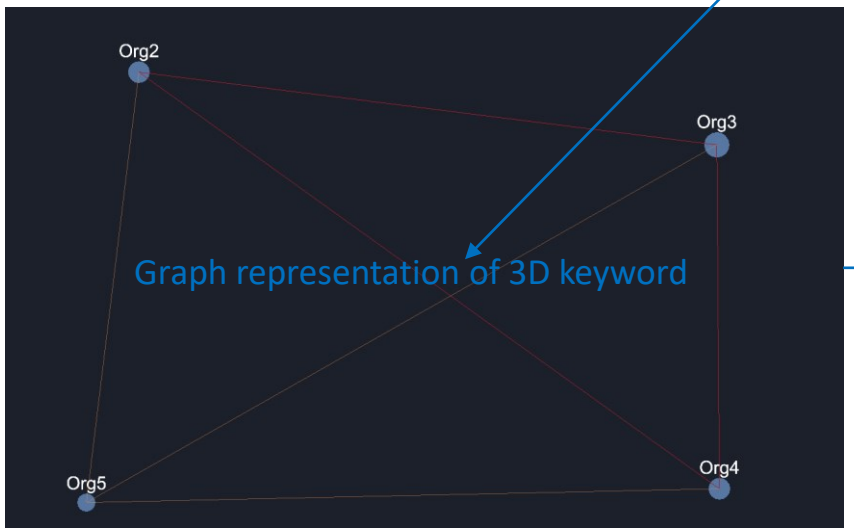
Support Hypergrap
information
is restored
in a single node type
Graph by adding a
feature on the edge
and using
interoperability
between chart and
graph

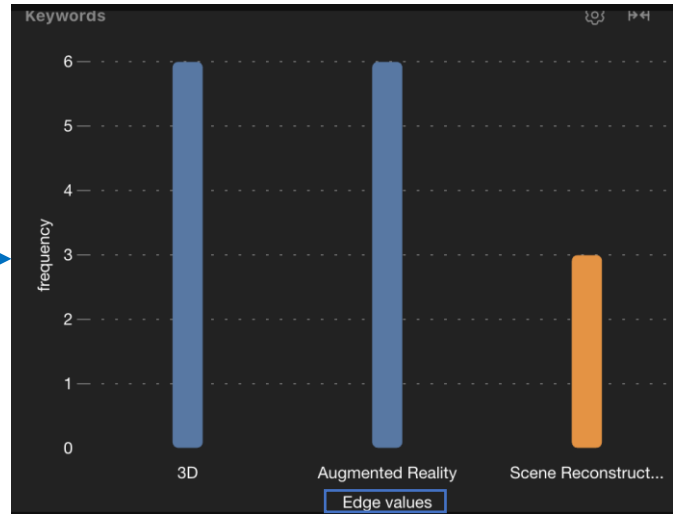






Graph schema



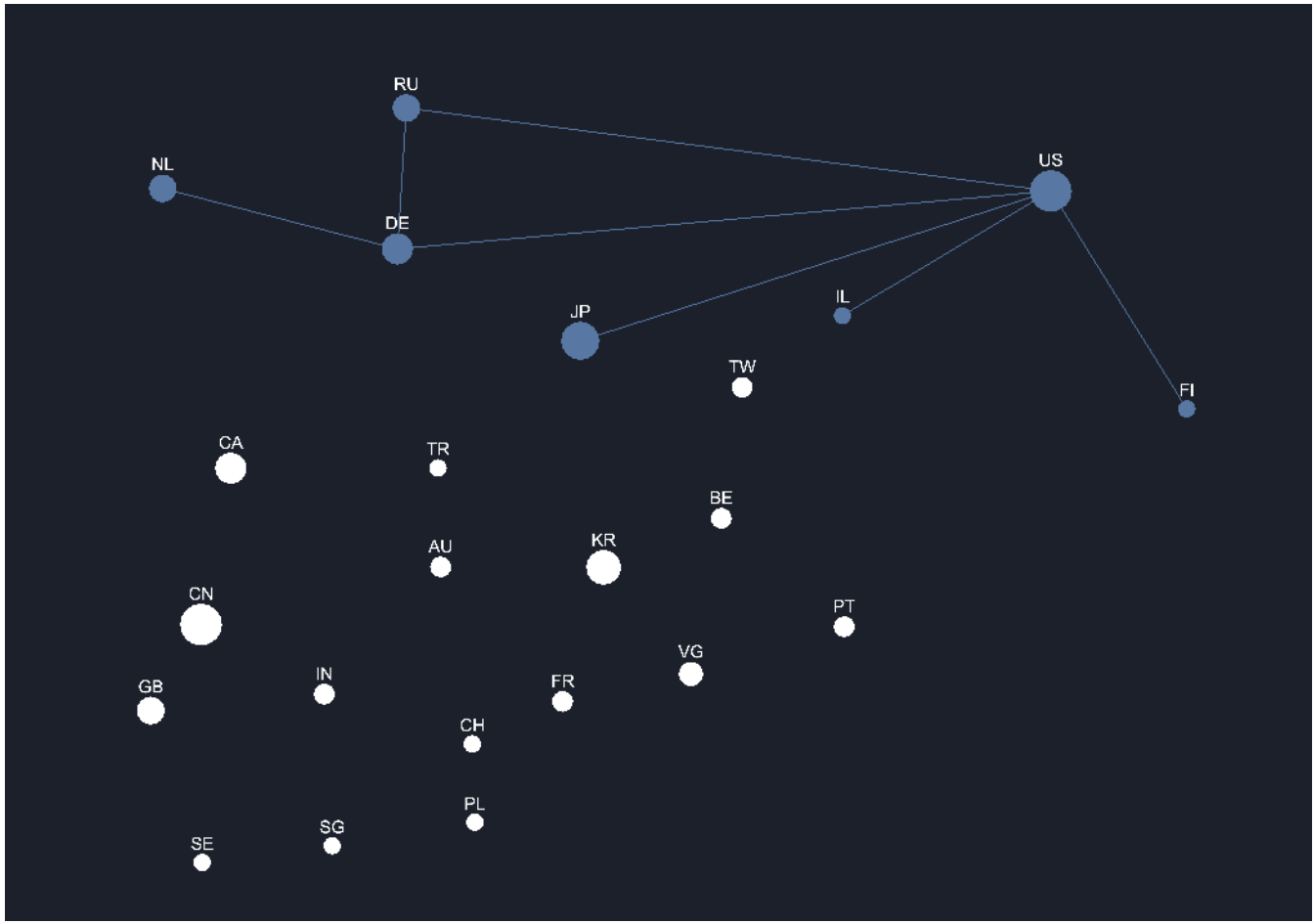


Cardinality relation between edges and hyperedge: n(n-1)/2

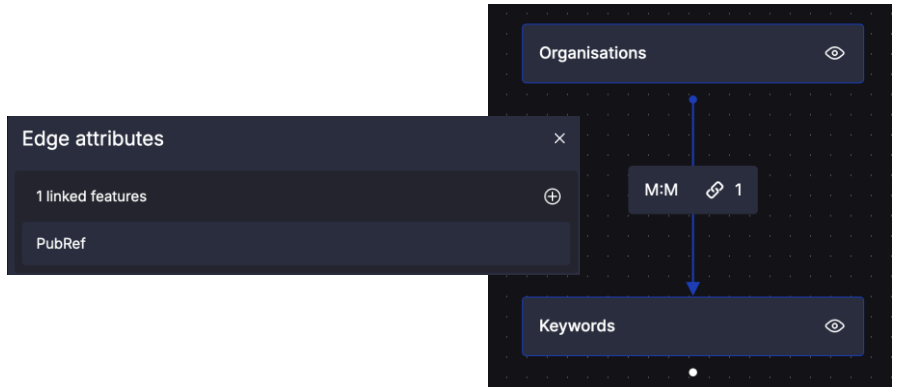
Example: Patent encoding and encryption landscape

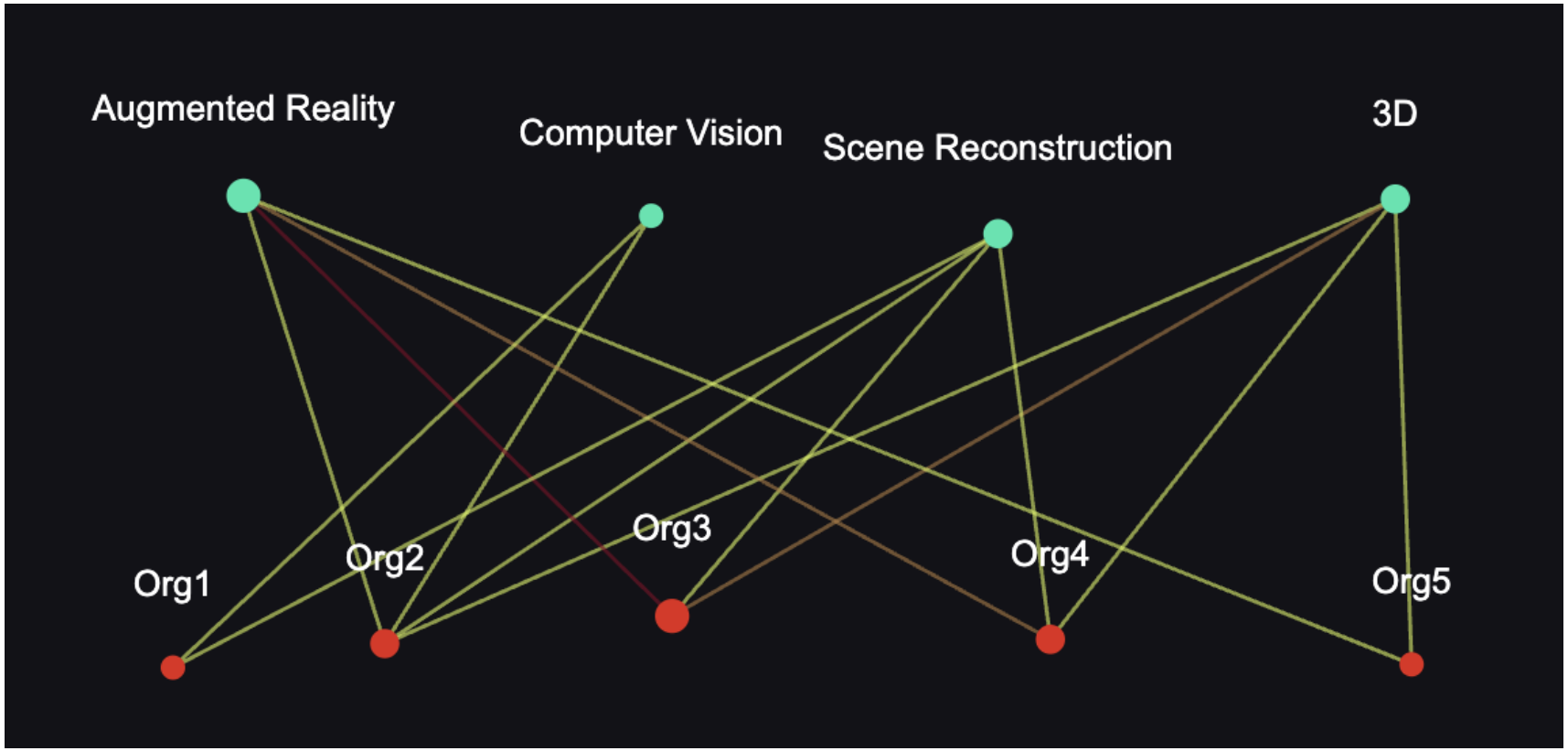
Title	Applicants	Applicants Origine
Title1	['App1', 'App2']	['Ori1', 'Ori2']
Title2	['App1', 'App3']	['Ori1', 'Ori3']
Title3	['App4', 'App5', 'App6']	['Ori1', 'Ori1', 'Ori4']

Using single node type graph and adding the feature Title on the edges to Visualise international collaborations

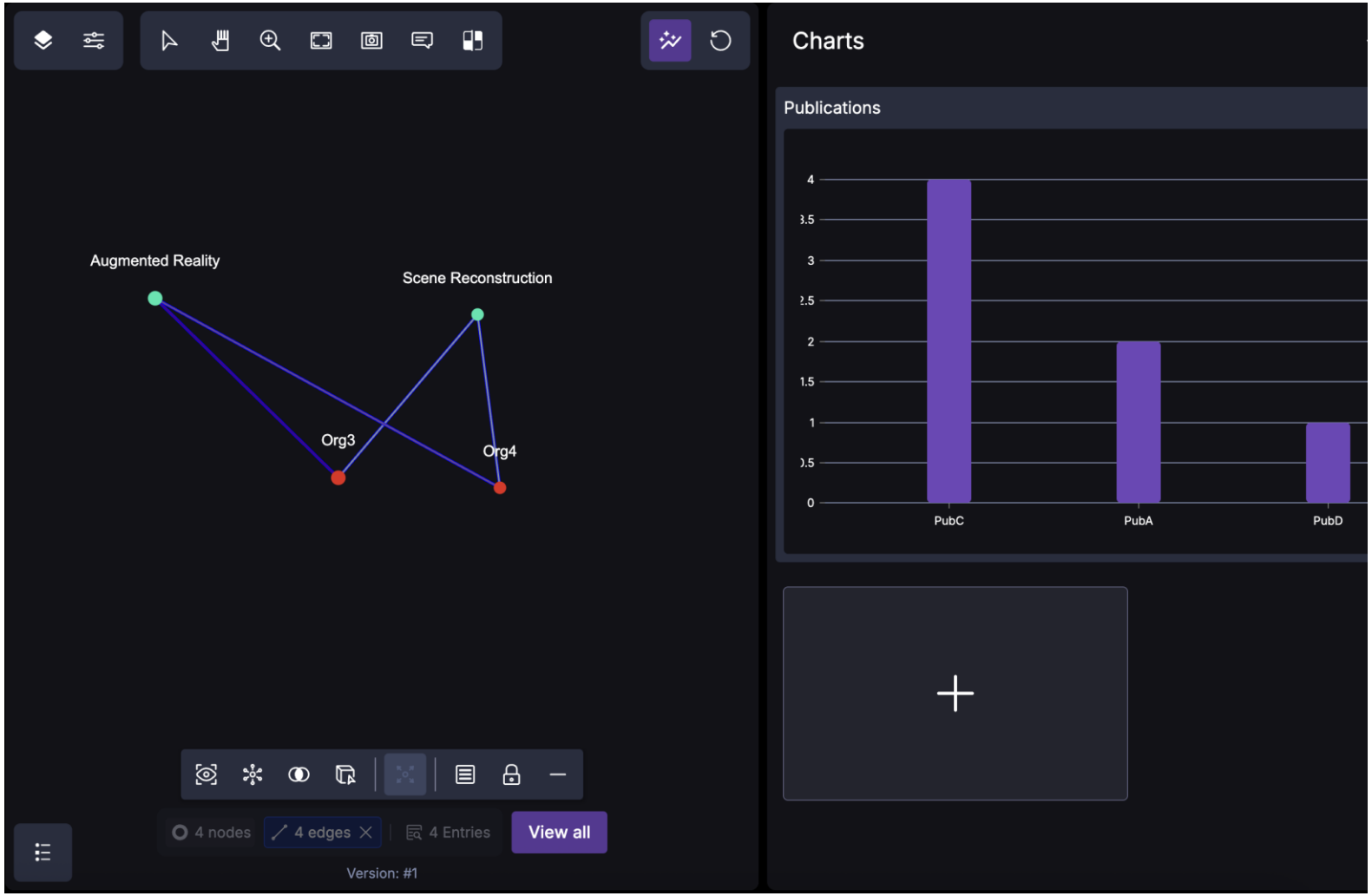


Hb-graph information is restored in dual node type Graph by adding a feature on the edge in the schema and …

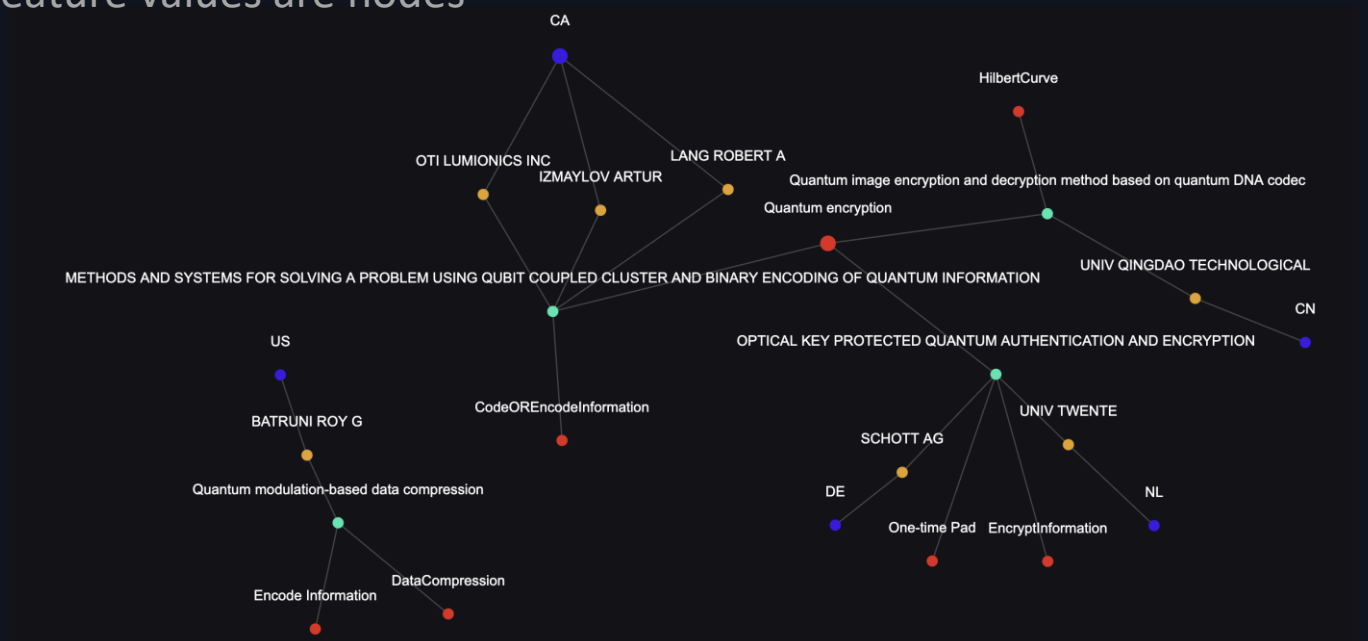




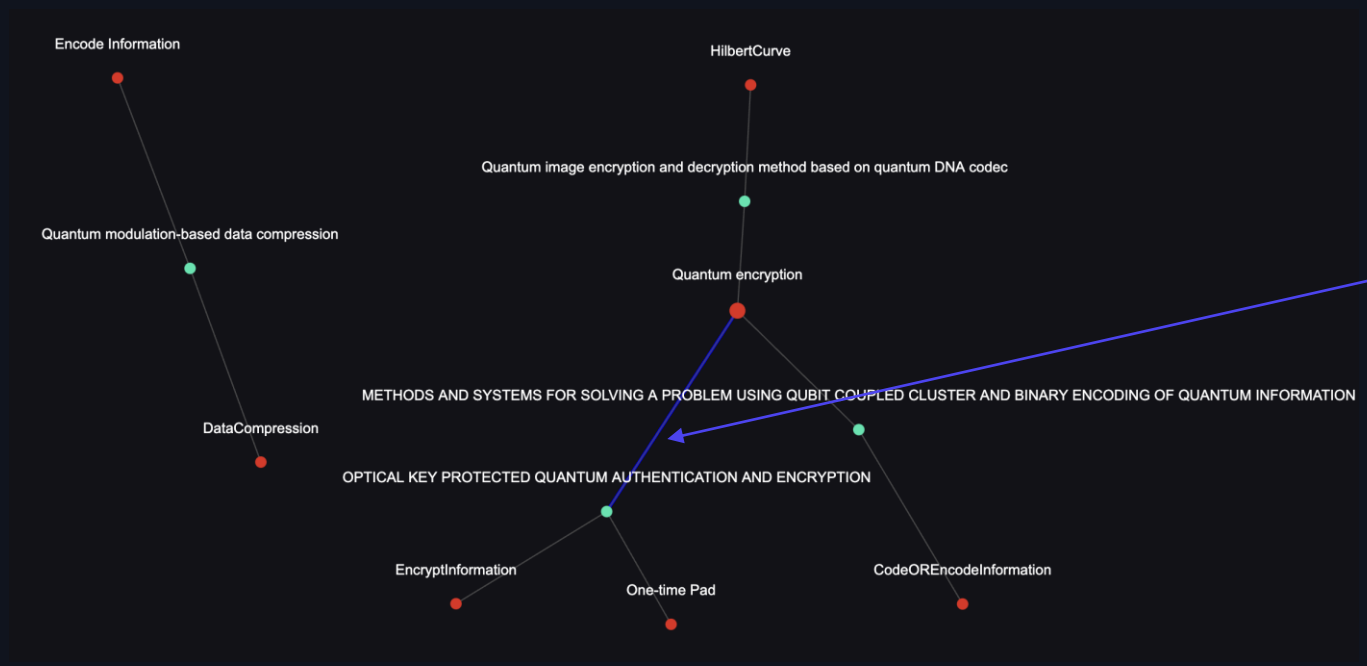
… Using Interoperability between Graph and Chart exploration

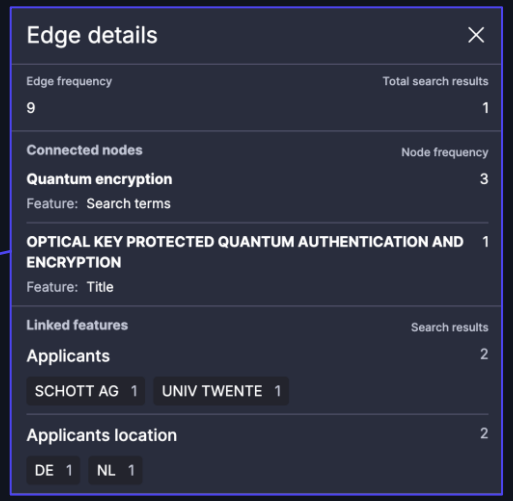


All feature values are nodes



Example: Qantum encryption patent landscape





Adding semantic information on the edges simplifies the network

Simplified network: Features Applicants & Applicants location are on edges

Dynamic Network Modelling: Schema-based graph generation
+ Chart, table and graph interoperability
+ In-graph search and trim operations

Retains all the information contained in the incident matrix

Reduces visual complexity

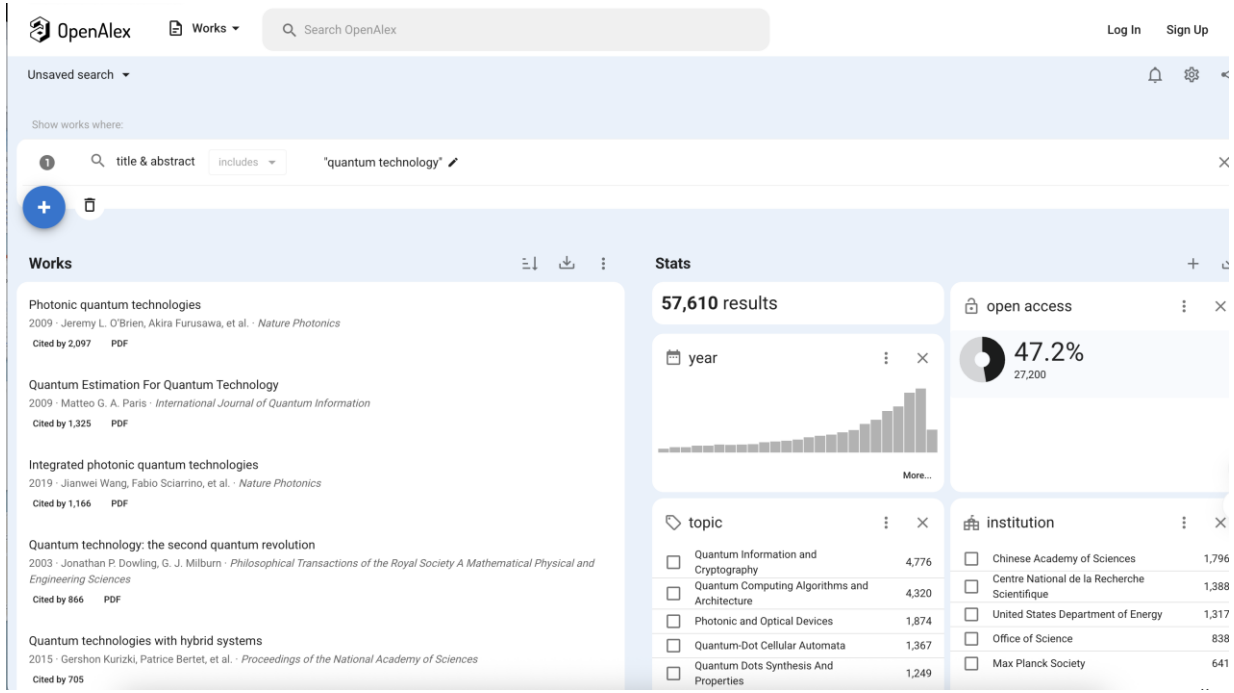
Enhances insight by selecting different perspectives (graph schemas)

Focuses on correlations of interest

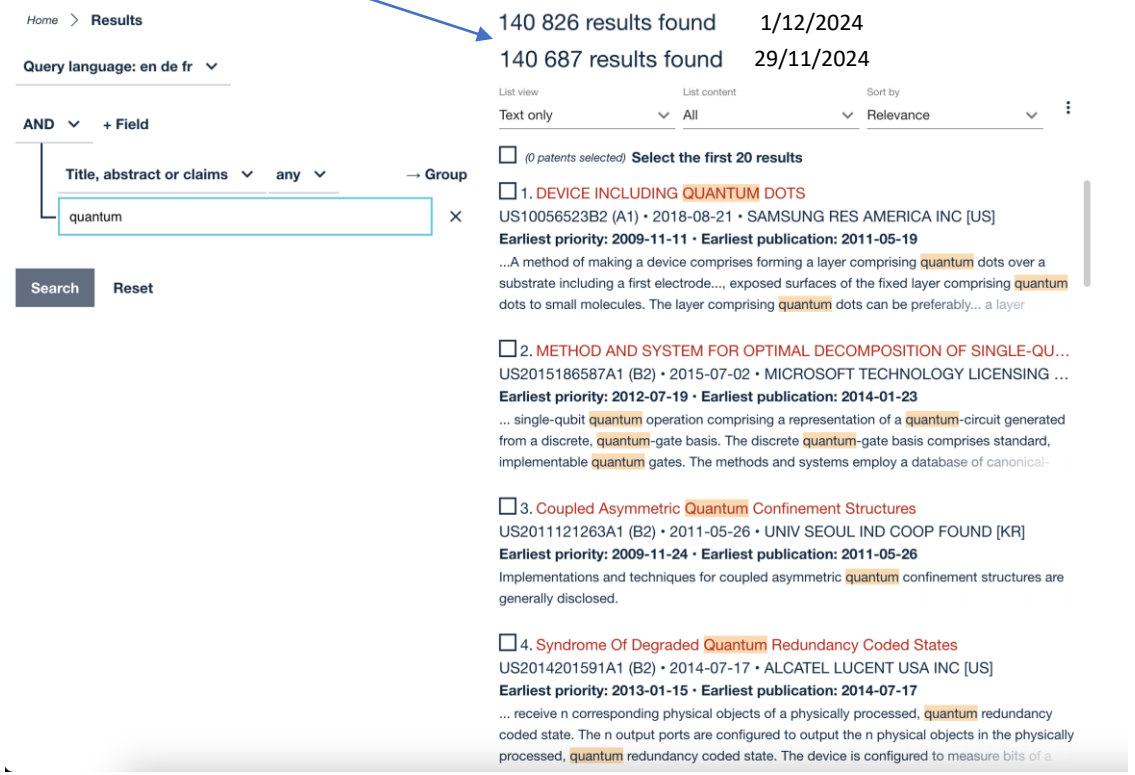
An overwhelming number of published items

Changing by the day

- Publications*



- Patents**

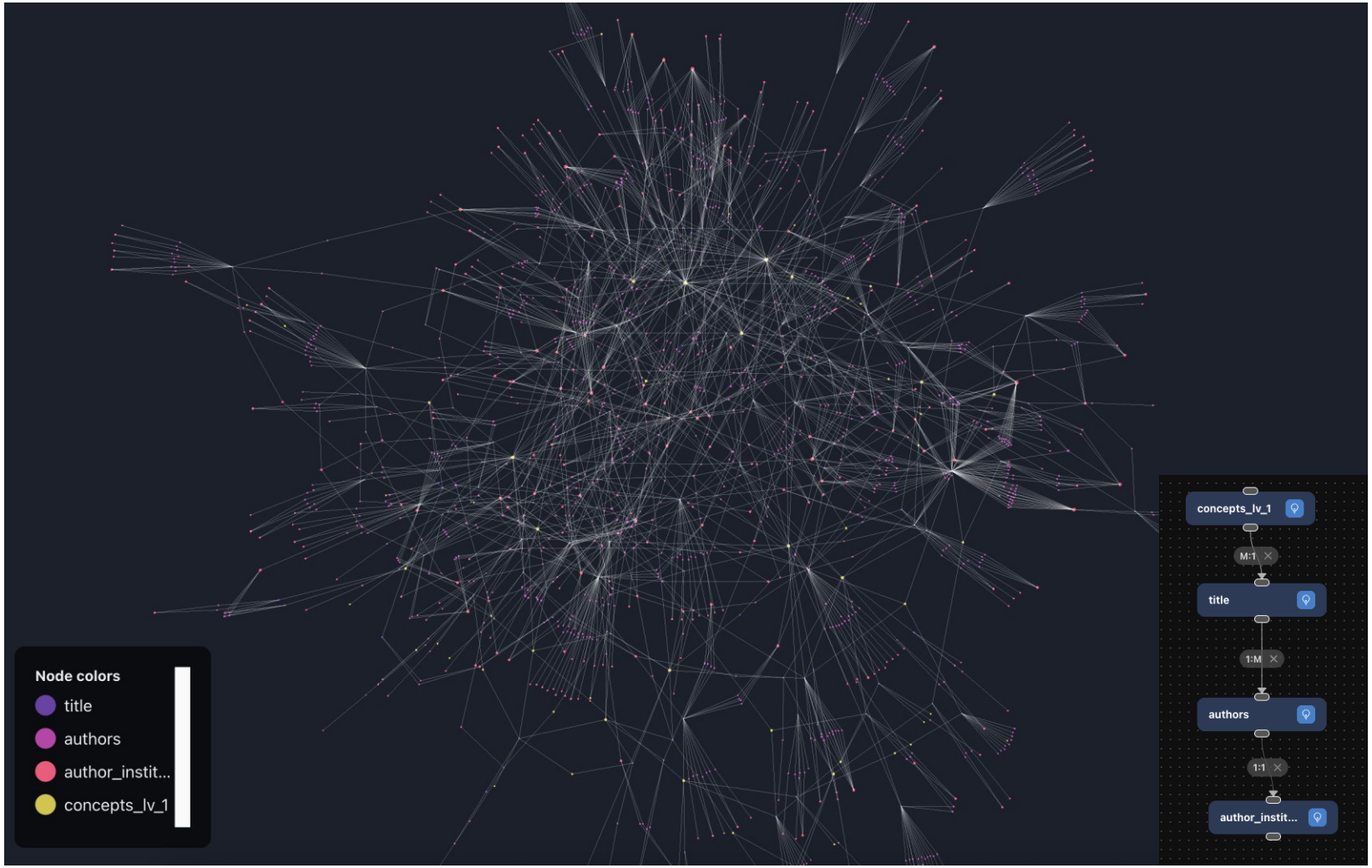


*OpenAlex: https://openalex.org/works?filter=default.search%3AQuantum%20technology

**EspaceNet Advanced Search: https://worldwide.espacenet.com/patent/search?q=ctxt any "Quantum"

Rational for dynamic network modelling

- The main component of a graph of publications from a search in quantum technology is far too complex to be insightful

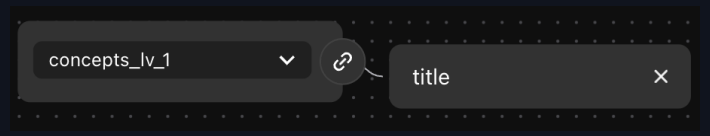


CSX visualisation tool developed at CERN by Aleksander Bobic

Co-occurrence network of Concepts & Publications

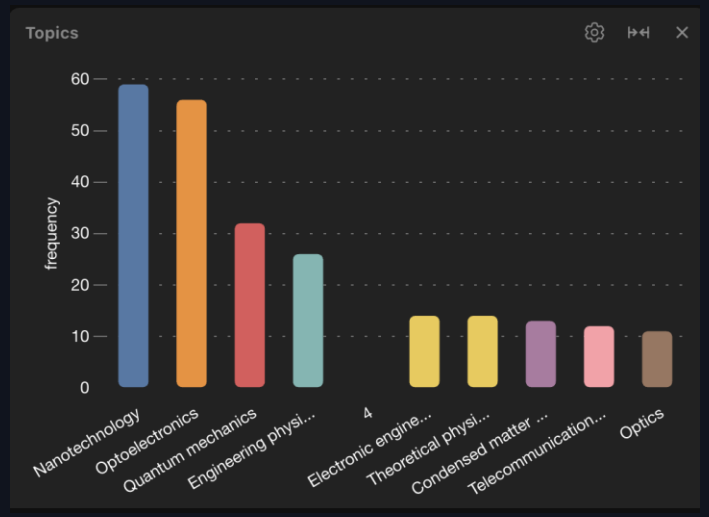
OpenAlex API, Search: “Qantum Technology” in titles

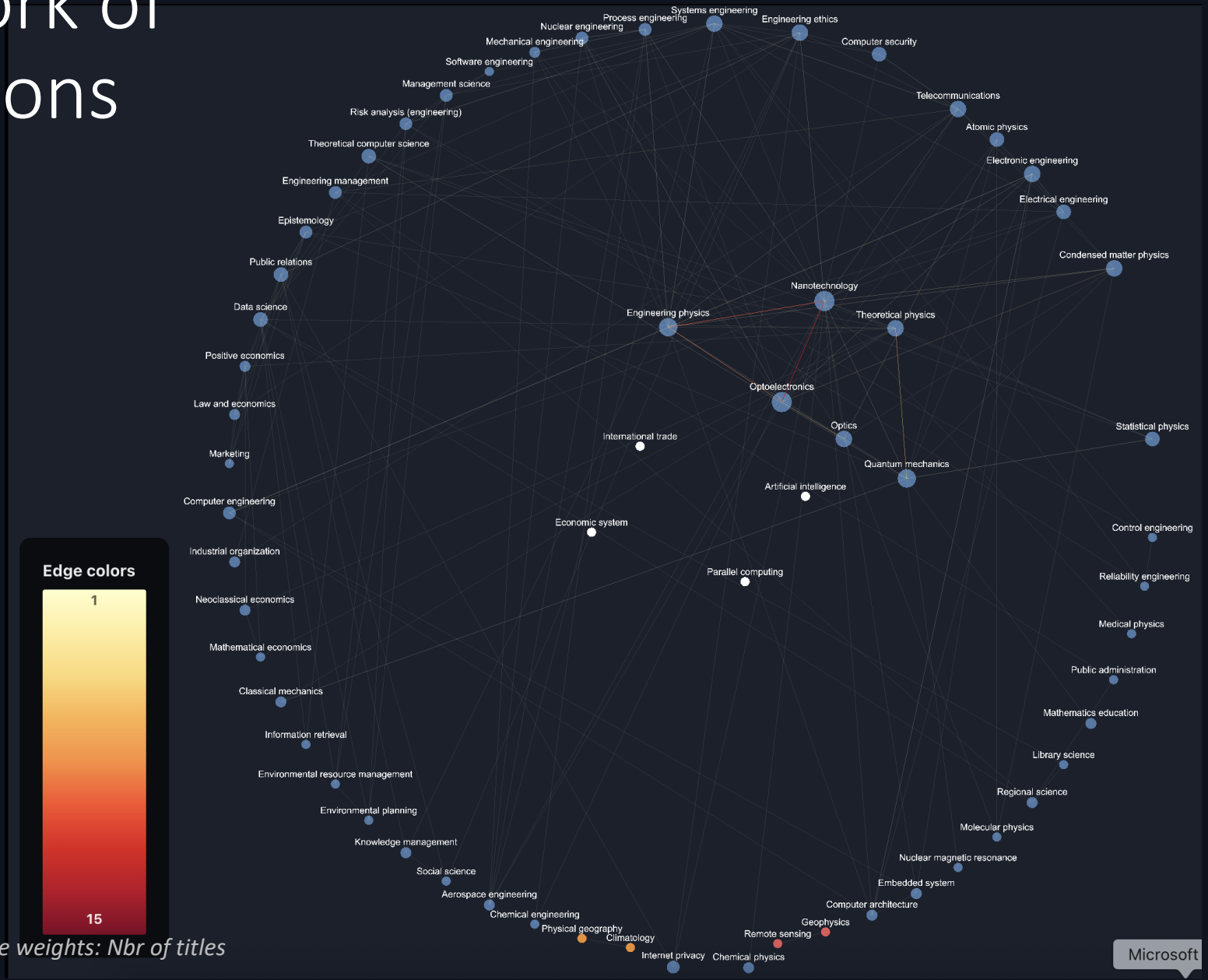
Network
Nodes: OpenAlex Concepts
Edges: Publication Titles (ranked)



Network schema

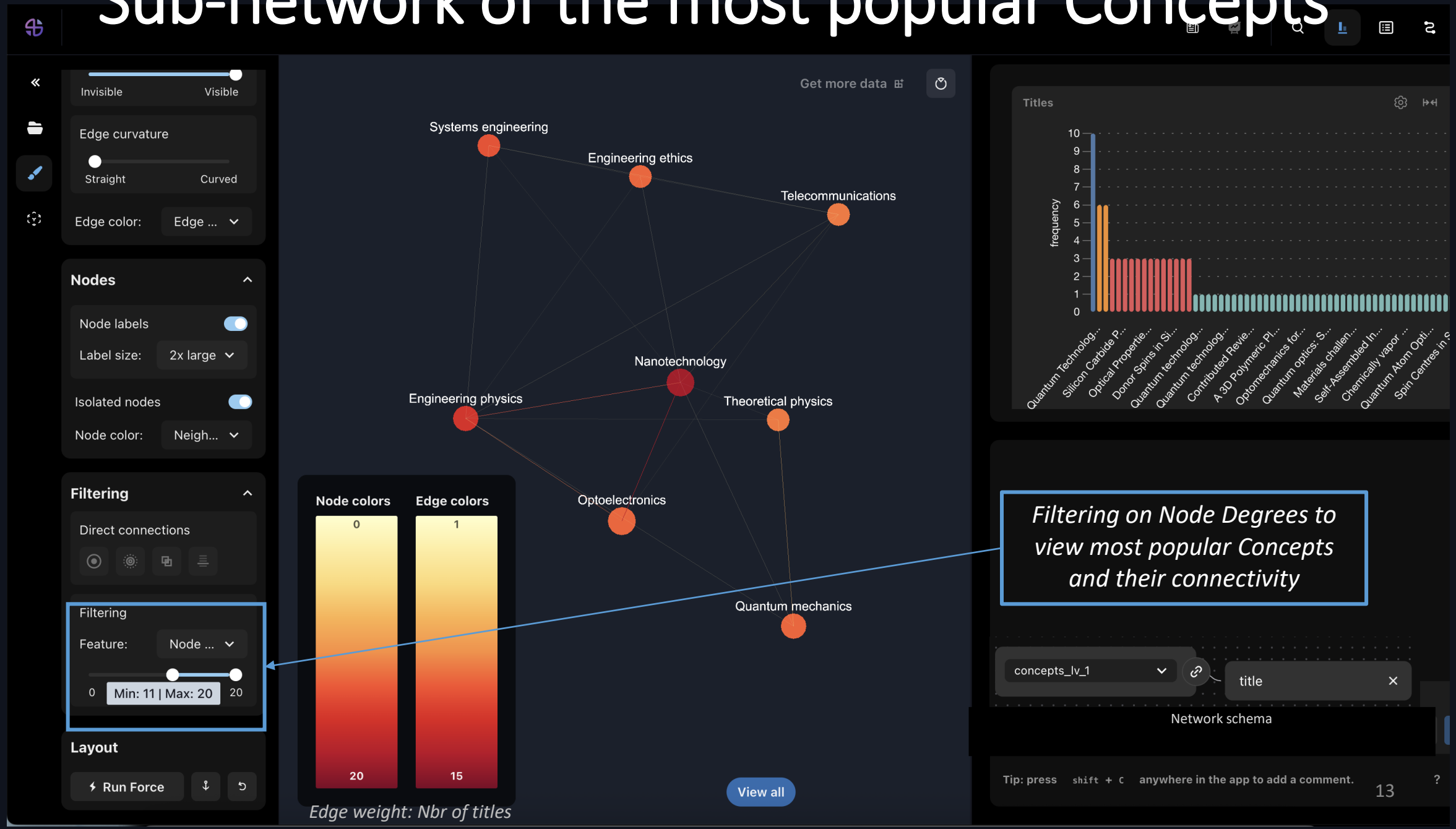
➔**Blue** Nodes: **C**onnected component of concepts linked by titles
➔**Yellow** and **Red** **Concepts** correspond to other components



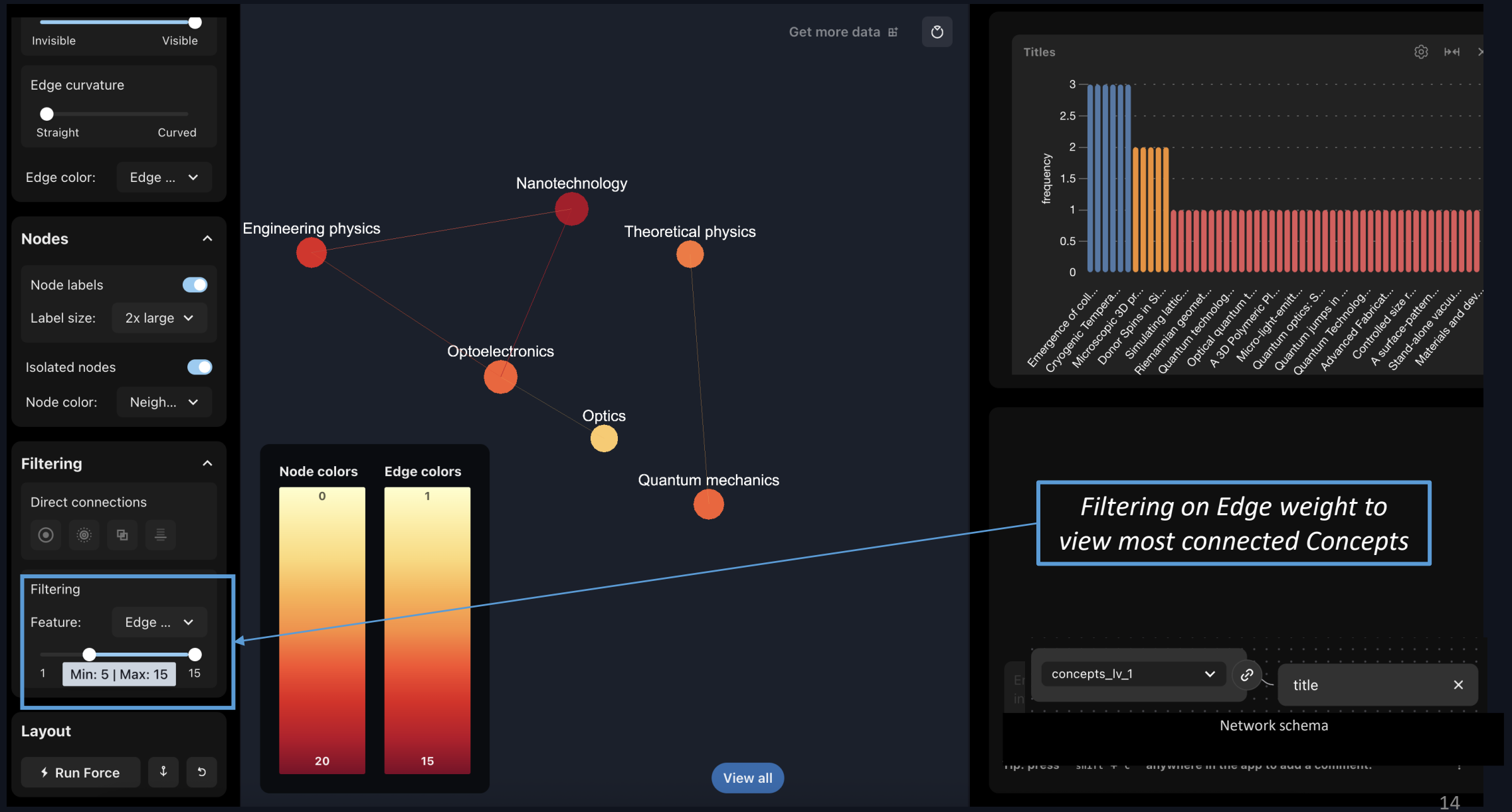


Edge weights: Nbr of titles

Sub-network of the most popular Concepts



Sub-network of the most connected Concepts



Edge weight: Nbr of titles

Trim &Expand Network to discover additional topics

OpenAlex API, Search: “Qantum cryptography” in titles
Filter on Concept: “Algorithm”

Network
Nodes: OpenAlex Concepts
Edges: Titles (ranked)

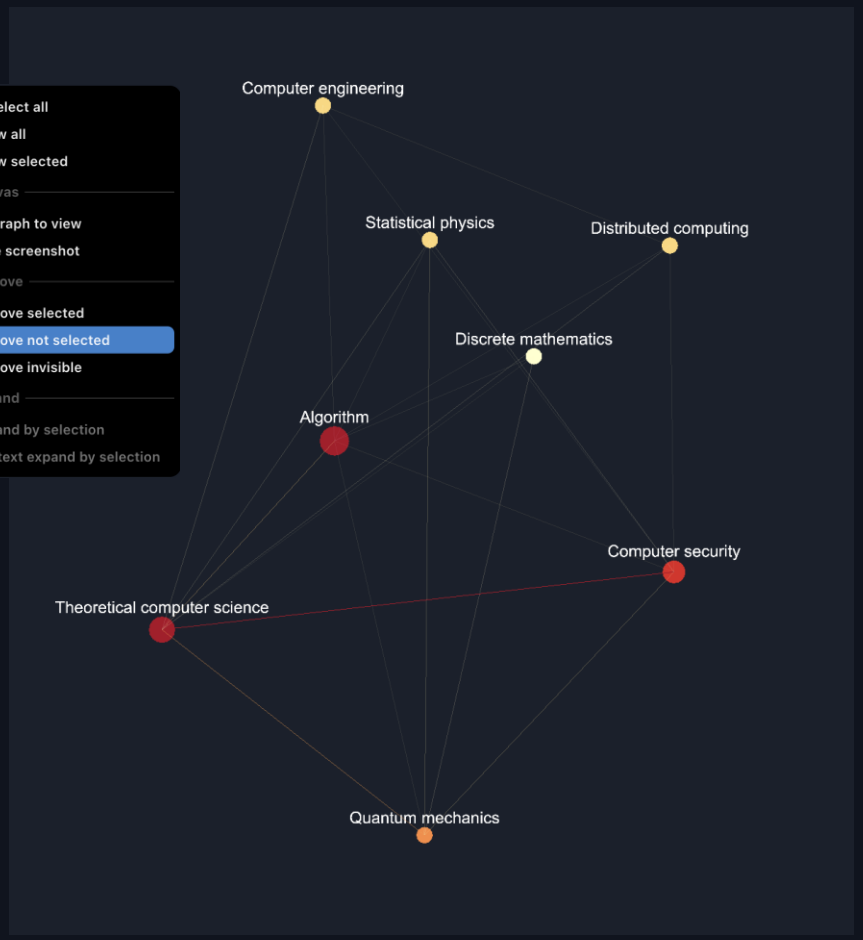
➔ *OpenAlex provides a ranking algorithm*
➔ *The first 200 titles will not fully address a particular Concept* ➔ ***Trim*** *and* ***Expand***
➔ *The first 200 titles may not contain the Concept you are looking for* ➔ ***Expand***

Step 1: Select Node for Triming the network

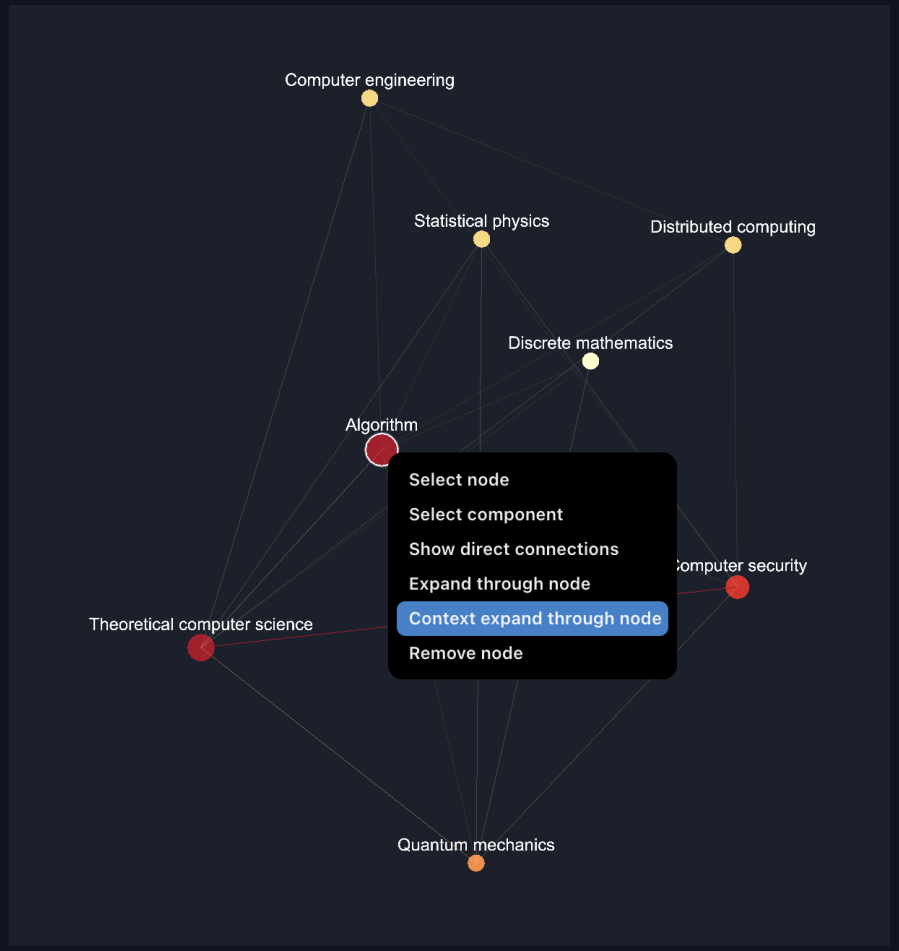
(See next slide for Step 2 and 3)

Trim & Expand to focus on Quantum Cryptography Algorithm

(In-graph search)

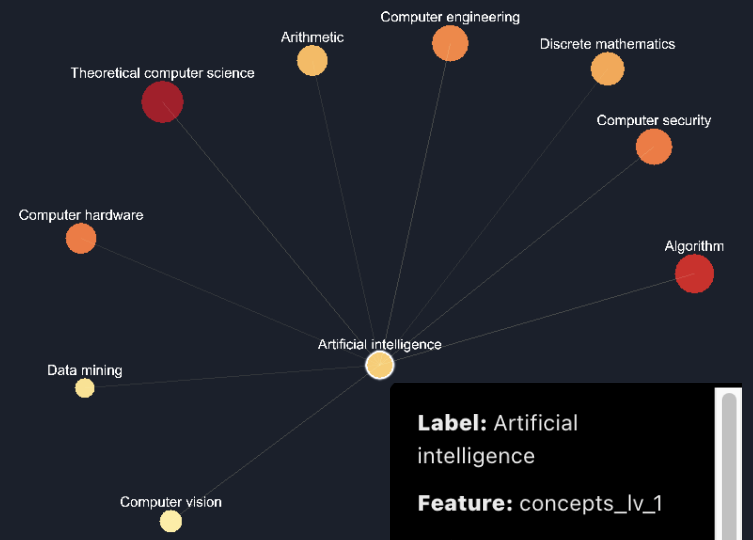


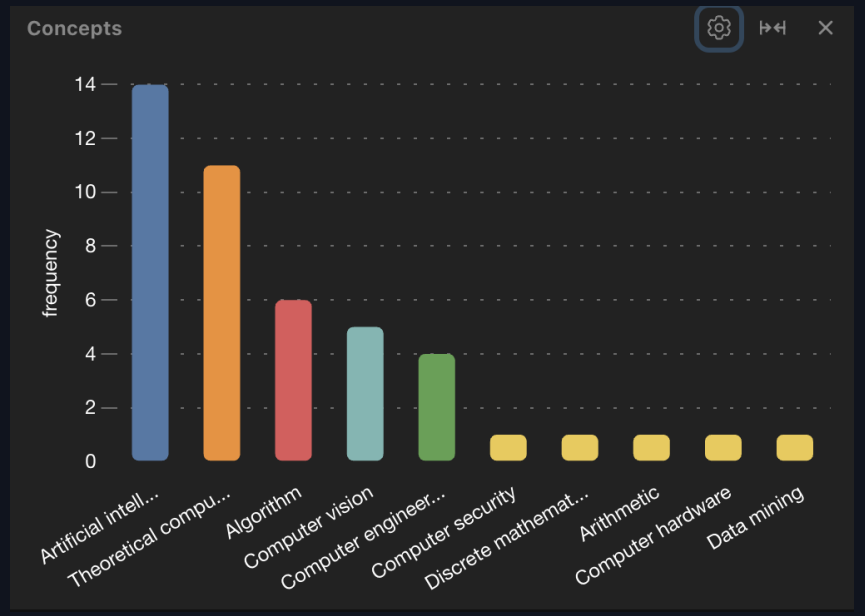
Step 2 Trim: Remove titles not related to Concept: “Algorithm”



Step 3 Expand: Search for more titles related to Concept: “Algorithm” in the context of “Quantum Encryption”

After triming and expansion: AI as an emerging Concept





***Egocentric view & corresponding chart**: AI Concept network after trimming and expanding the in-graph search for titles containing "Quantum Encryption" in the context of Concept "Algorithm"*

AI as an emerging concept

Sample of publications

TITLE Analysis of the applicability of artificial neural networks for the post-quantum cryptography algorithms development

DOI https://doi.org/10.1088/1742-6596/2032/1/012026

AUTHORS: Sabina Tarasenko | Nikita Andriyanov | A A Gladkikh

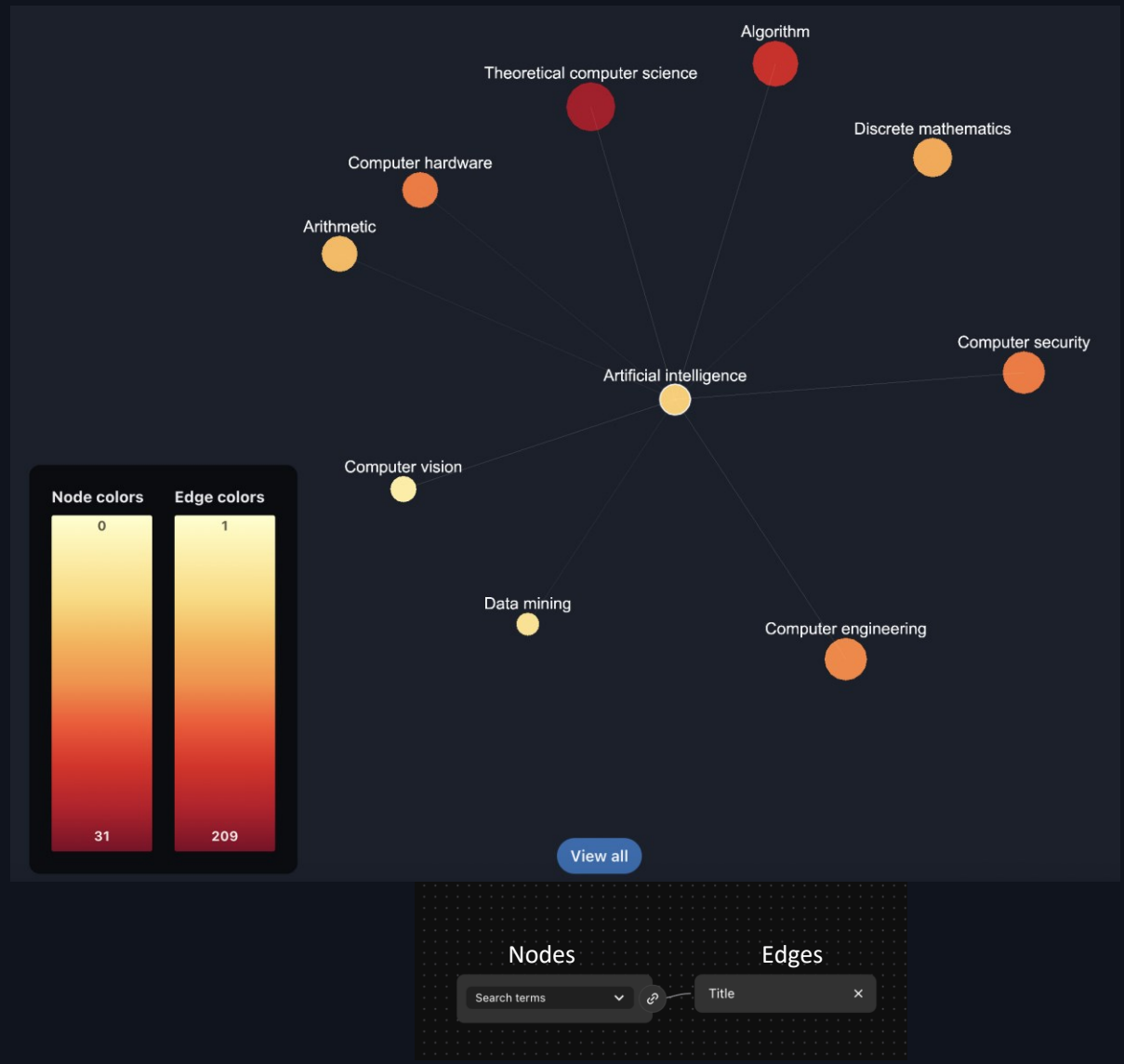
TITLE Machine Learning Method with Applications in Hardware Security of Post-Quantum Cryptography

DOI https://doi.org/10.1007/s10723-023-09643-4

AUTHORS: Haibo Yi

With the emergence of quantum computers, post-quantum cryptography is a subjet matter of concern

Egocentric view

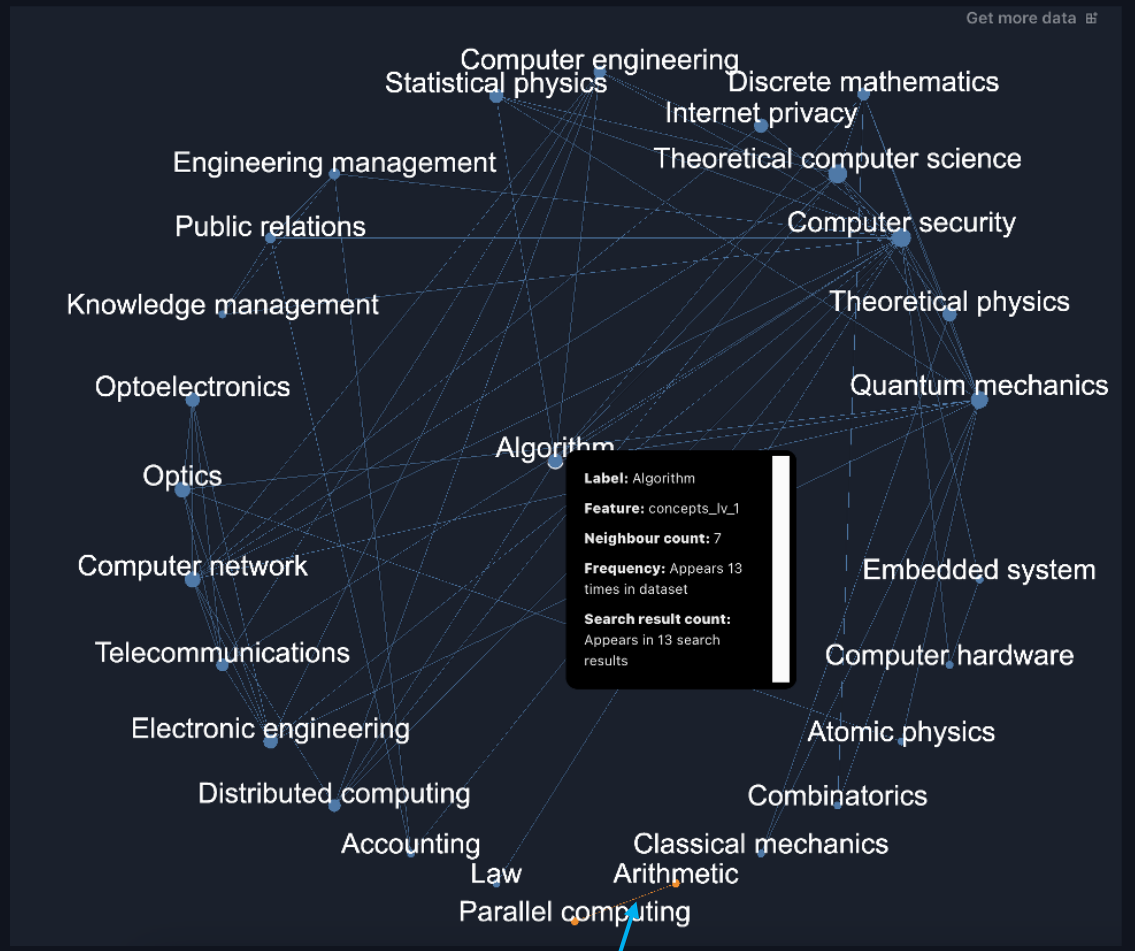


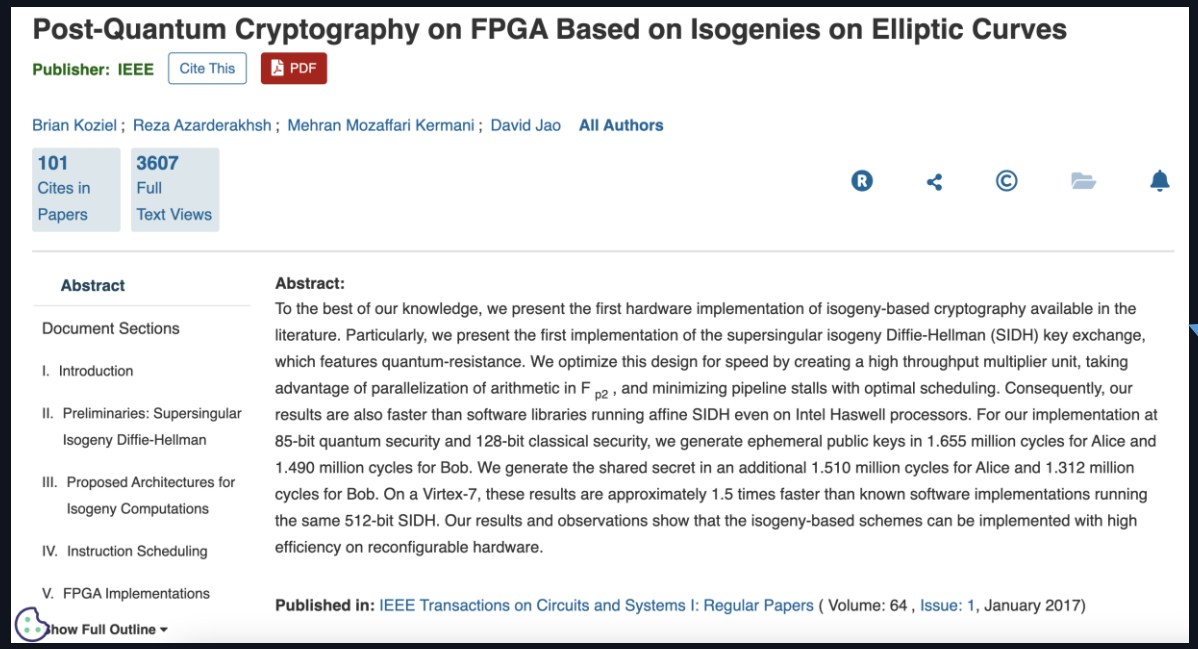
Outliers in Quantum Cryptography for strategic information

OpenAlex API,
Search: “Quantum Cryptography” in titles

Focus

Network
Nodes: OpenAlex Concepts
Edges: Titles (First 200 titles, ranked)





Post-Quantum Cryptography on FPGA Based on Isogenies on Elliptic Curves

Publisher: IEEE | Cite This | PDF

Brian Koziel ; Reza Azarderakhsh ; Mehran Mozaffari Kermani ; David Jao All Authors

101 Cites in Papers | 3607 Full Text Views

Abstract

Document Sections

I. Introduction

II. Preliminaries: Supersingular Isogeny Diffie-Hellman

III. Proposed Architectures for Isogeny Computations

IV. Instruction Scheduling

V. FPGA Implementations

Show Full Outline

Abstract:
To the best of our knowledge, we present the first hardware implementation of isogeny-based cryptography available in the literature. Particularly, we present the first implementation of the supersingular isogeny Diffie-Hellman (SIDH) key exchange, which features quantum-resistance. We optimize this design for speed by creating a high throughput multiplier unit, taking advantage of parallelization of arithmetic in F_{p2}, and minimizing pipeline stalls with optimal scheduling. Consequently, our results are also faster than software libraries running affine SIDH even on Intel Haswell processors. For our implementation at 85-bit quantum security and 128-bit classical security, we generate ephemeral public keys in 1.655 million cycles for Alice and 1.490 million cycles for Bob. We generate the shared secret in an additional 1.510 million cycles for Alice and 1.312 million cycles for Bob. On a Virtex-7, these results are approximately 1.5 times faster than known software implementations running the same 512-bit SIDH. Our results and observations show that the isogeny-based schemes can be implemented with high efficiency on reconfigurable hardware.

Published in: IEEE Transactions on Circuits and Systems I: Regular Papers (Volume: 64 , Issue: 1, January 2017)

TITLE Post-Quantum Cryptography on FPGA Based on Isogenies on Elliptic Curves

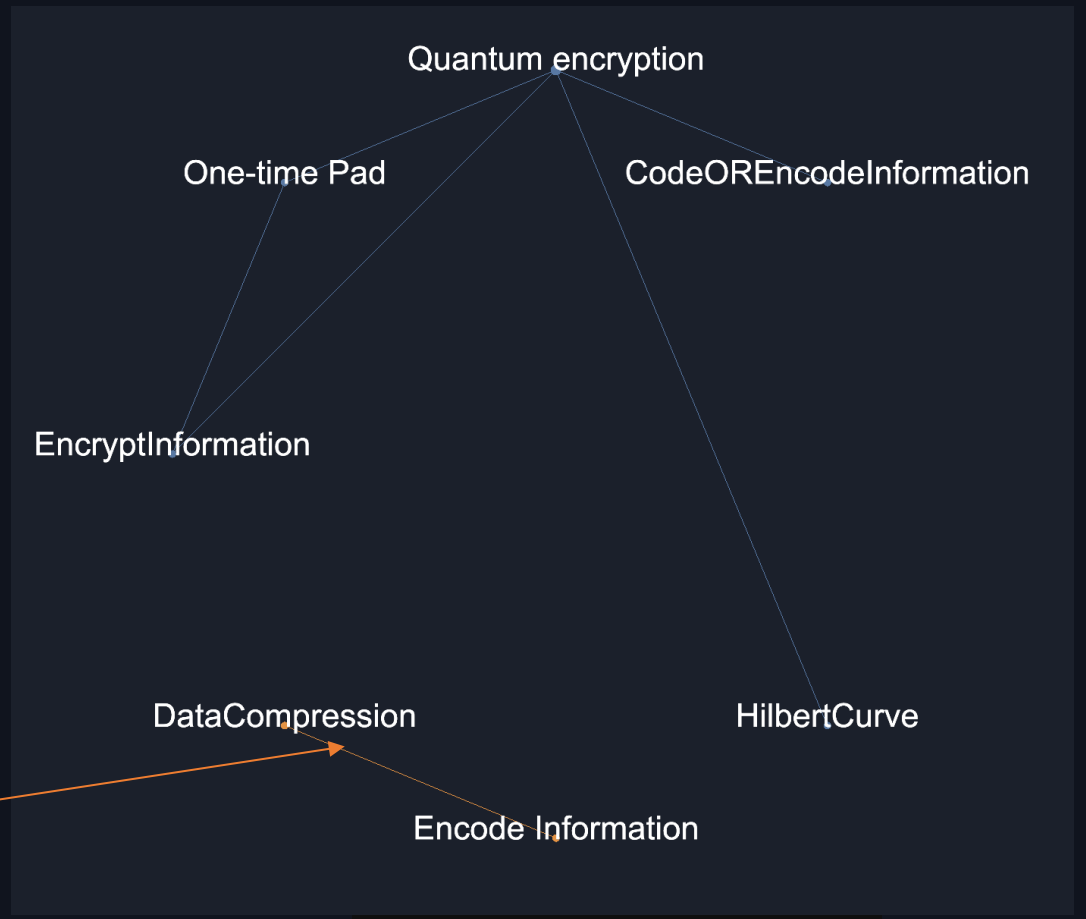
DOI https://doi.org/10.1109/tcsi.2016.2611561

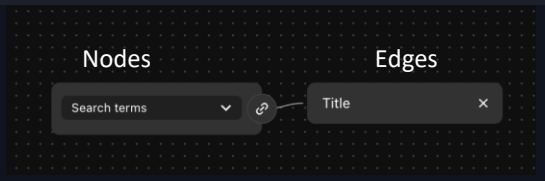
AUTHORS: Brian Koziel | Reza Azarderakhsh | Mehran Mozaffari Kermani | David Jao

Homomorphic Elliptic-based algorithm to resist quantum computer attacks

Searching in a corpus of 235 Patents on encryption and data compression those with “Quantum” in the title

- Two separate Components
  - 1 related to quantum encryption (blue edges)
  - 1 related to Data compression (orange edges)





TITLE Quantum modulation-based data compression

ABSTRACT Data compression includes: inputting data comprising a vector that requires a first amount of memory; compressing the vector into a compressed representation while preserving information content of the vector, including: encoding, using one or more non-quantum processors, at least a portion of the vector to implement a quantum gate matrix; and modulating a reference vector using the quantum gate matrix to generate the compressed representation, wherein the compressed representation requires a second amount of memory that is less than the first amount of memory; and outputting the compressed representation to be displayed, stored, and/or further processed.

PUBLICATION NUMBER https://worldwide.espacenet.com/patent/search/publication/US11580195B1

Thank you for your attention

Jean-Marie Le Goff

- Co-Founder & Co-CEO
- + 41 78 267 54 54
- jean-marie.legoff@dtangle.ch

Marc-André Siegrist

- Co-Founder & Co-CEO
- + 41 79 702 15 35
- marc.siegrist@dtangle.ch

Dtangle

Dtangle SA

- La Voie-du-Coin 28, 1218 Le Grand-Saconnex, Switzerland
- Website: https://dtangle.ch