Design and Analysis of a Protocol for Anonymous Sociometric Questionnaires

Marián Novotný

Institute of Computer Science
P.J. Šafárik University, Faculty of Science
Košice, Slovakia

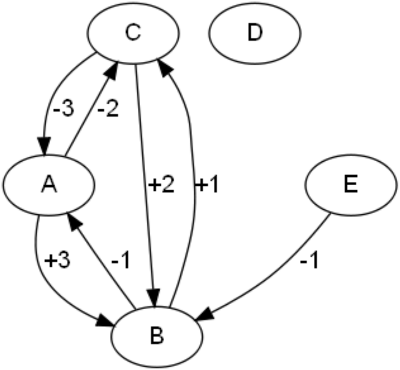
PrimeLife / IFIP Summer School 2009 – Privacy and Identity Management for Life

Introduction to Sociometry

- quantitative method for measuring social relationships (Jacob L. Moreno)
- can be used for management of a school class by a teacher or in a team-building
- is based on choices of individuals
- choices of responders are collected by a questionnaire from responders
- relations between individuals can be represented by a sociogram

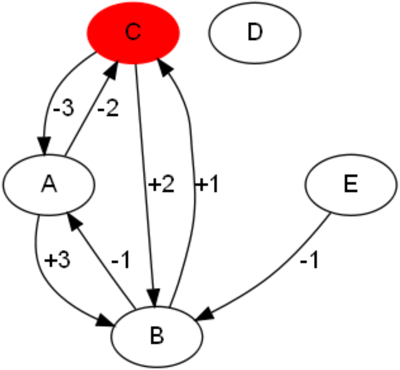
Representation of a Sociogram by Graph Theory

- weighted digraph $G = (V, E), E \subseteq V \times V$, where each node represents one responder
- social link is represented as a weighted arc
- the weight function $w : E \rightarrow \{-s, \ldots, -1, 1, \ldots, s\}$

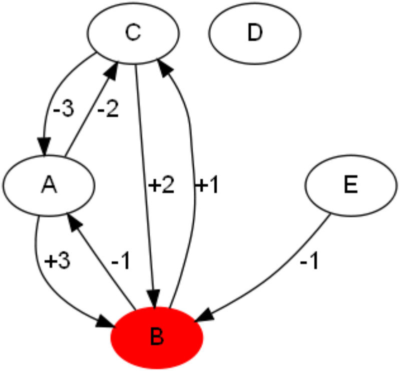


Node Characteristics – Indegrees

- positive indegree $deg^{In^+}(C) = 1$
- negative indegree $deg^{In^-}(C) = 1$
- indegree $deg^{In}(C) = deg^{In^+}(C) + deg^{In^-}(C) = 2$

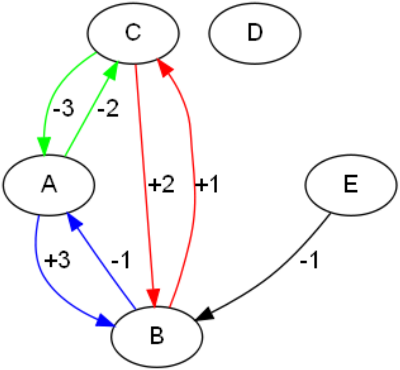


- positive weighted indegree $In^{+}(B) = 5$
- negative weighted indegree $In^{-}(B) = -1$



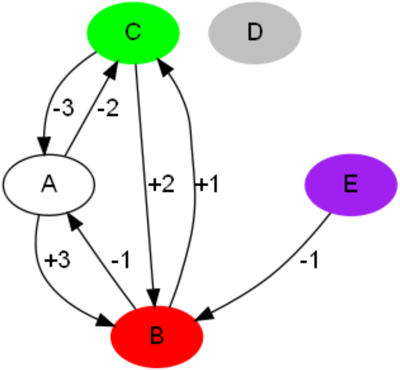
Mutual Choices

- positive mutual choice
- negative mutual choice
- combined mutual choice

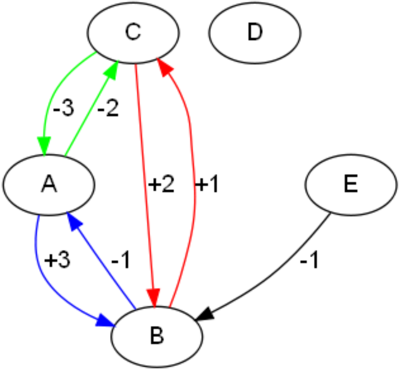


Individual Phenomena

- positive social status of B $\frac{In^{+}(B)}{|V|-1} = \frac{5}{4}$
- Star B – node with the maximal positive weighted indegree
- Outsider C – node with the minimal negative weighted indegree
- Ghost D – node with zero indegree and outdegree
- Isolate E – node with zero positive indegree, is not a ghost



- the set of positive $M^+(G)$, negative $M^-(G)$, combined $M^\pm(G)$ mutual choices
- positive coherence of a group G is defined as $coh^+(G) = \frac{|M^+(G)|}{\binom{|V|}{2}} = \frac{1}{\binom{|5|}{2}} = \frac{1}{10}$



Security Requirements for the Scheme

- Eligibility – only responders from the group are eligible to correctly fill in the questionnaire.
- Privacy – choices of a responder must not identify the responder and any traceability between the responder and his choices must be removed.
- Verifiability – responder should be able to verify whether his choices were correctly recorded, all valid choices of other responders were included and the counting process was accurate.
- Accuracy – the scheme must be error-free. The final computation of sociometric indices must corresponds with all choices of all responders.

The Homomorphic Public-Key System

- used for encryption of responders choices
- semantically secure, additively homomorphic, allows us once to use multiplication
- threshold version (t, a) – the private key is shared among a authorities
  - A ciphertext can be decrypted when at least $t + 1$ shareholders cooperate
  - the process of decryption is universally verifiable and does not reveal the secret key

Homomorphic Properties of the Public-Key System

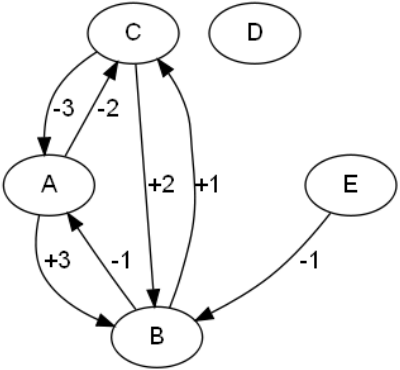
- given ciphertexts $C_1 = E_{Pk}(m_1), C_2 = E_{Pk}(m_2)$, anyone can create
  - $E_{Pk}(m_1 + m_2)$ by computing the product
    $C_1 \cdot C_2 = E_{Pk}(m_1 + m_2)$
  - $E_{Pk}(m_1 \cdot m_2)$ by computing the bilinear map
    $C_1 \star C_2 = E_{Pk}(m_1 \cdot m_2)$
  - $E_{Pk}(z \cdot m_1)$ by computing the exponentiation
    $C_1^z = E_{Pk}(z \cdot m_1)$

The Proposed Scheme – Registration, Key Generation

- for simplicity we assume that a trusted dealer first generates the public key Pk and the private key Sk, shares the private keys between a authorities and then deletes the private key
- registration of responders and questioner is based on digital signatures
- the questioner creates a questionnaire which contains obligatory properties
  - time for filing in, the list of responders with their unique identification, sociometric parameters such as the scale s for the weights of the arcs
- A responder using the application
  - authorizes by the questioner, downloads the parameters of the questionnaire
  - selects his choices
  - submits his selections encrypted under the key Pk

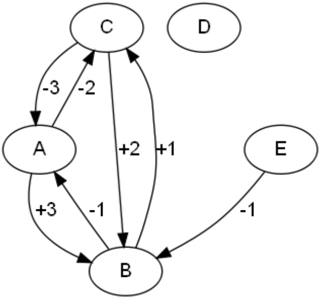
- to represent a weighted arc from the node R_i to node R_j we use $s + 2$ bits $b_{ij}^{+}, b_{ij}^{-}, b_{ij}^{w_1}, \ldots, b_{ij}^{w_s}$

$A \to B$	10001
$A \to C$	01010
no arc	00100



The Proposed Scheme – Encrypted Sociogram

	A	B	C	D	E
A	—	$E(1), E(0), E(3)$	$E(0), E(1), E(2)$	$E(0), E(0), E(1)$	$E(0), E(0), E(1)$
B	$E(0), E(1), E(1)$	—	$E(1), E(0), E(1)$	$E(0), E(0), E(1)$	$E(0), E(0), E(1)$
C	$E(0), E(1), E(3)$	$E(1), E(0), E(2)$	—	$E(0), E(0), E(1)$	$E(0), E(0), E(1)$
D	$E(0), E(0), E(1)$	$E(0), E(0), E(1)$	$E(0), E(0), E(1)$	—	$E(0), E(0), E(1)$
E	$E(0), E(0), E(1)$	$E(0), E(1), E(1)$	$E(0), E(0), E(1)$	$E(0), E(0), E(1)$	—

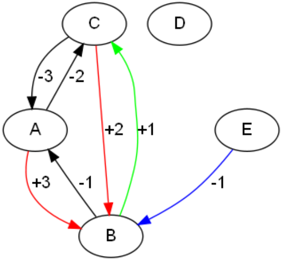


The Proposed Scheme – Verification of Submissions

- to represent a weighted arc from the node R_i to node R_j we use $s+2$ bits $b_{ij}^{+}, b_{ij}^{-}, b_{ij}^{w_1}, \ldots, b_{ij}^{w_s}$
- we need to verify, that
  - $b_{ij}^{\diamondsuit} \in \{0,1\} \equiv b_{ij}^{\diamondsuit} \cdot (b_{ij}^{\diamondsuit} - 1) = 0$
  - $b_{ij}^{+} \cdot b_{ij}^{-} = 0$
  - $\sum_{k=1}^{s} b_{ij}^{w_k} = 1 \equiv \sum_{k=1}^{s} b_{ij}^{w_k} - 1 = 0$
- We use the homomorphic properties for preparing ciphertexts of equations
- The equations can by checked by shareholders by cooperatively-made decryptions
- to save on computation, we check at once a batch of equations

Computation of Characteristics of Nodes

	A	B	C	D	E
A	—	$E(1), E(0), E(3)$	$E(0), E(1), E(2)$	$E(0), E(0), E(1)$	$E(0), E(0), E(1)$
B	$E(0), E(1), E(1)$	—	$E(1), E(0), E(1)$	$E(0), E(0), E(1)$	$E(0), E(0), E(1)$
C	$E(0), E(1), E(3)$	$E(1), E(0), E(2)$	—	$E(0), E(0), E(1)$	$E(0), E(0), E(1)$
D	$E(0), E(0), E(1)$	$E(0), E(0), E(1)$	$E(0), E(0), E(1)$	—	$E(0), E(0), E(1)$
E	$E(0), E(0), E(1)$	$E(0), E(1), E(1)$	$E(0), E(0), E(1)$	$E(0), E(0), E(1)$	—



$E(deg^{In^+}(B)) = E(1) \cdot E(1) \cdot E(0) \cdot E(0) = E(2)$

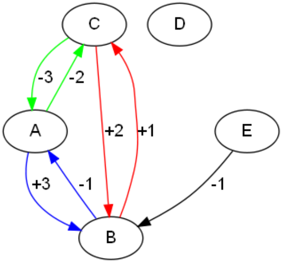
$E(deg^{In^-}(B)) = E(0) \cdot E(0) \cdot E(0) \cdot E(1) = E(1)$

$E(deg^{Out^+}(B)) = E(0) \cdot E(1) \cdot E(0) \cdot E(0) = E(1)$

$E(In^+(B)) = (E(1) \star E(3)) \cdot (E(1) \star E(2)) \cdot (E(0) \star E(1)) \cdot (E(0) \star E(1)) = E(3 \cdot 1 + 2 \cdot 1 + 0 \cdot 1 + 0 \cdot 1) = E(5)$

Computation of the Mutual Choices

	A	B	C	D	E
A	—	$E(1), E(0), E(3)$	$E(0), E(1), E(2)$	$E(0), E(0), E(1)$	$E(0), E(0), E(1)$
B	$E(0), E(1), E(1)$	—	$E(1), E(0), E(1)$	$E(0), E(0), E(1)$	$E(0), E(0), E(1)$
C	$E(0), E(1), E(3)$	$E(1), E(0), E(2)$	—	$E(0), E(0), E(1)$	$E(0), E(0), E(1)$
D	$E(0), E(0), E(1)$	$E(0), E(0), E(1)$	$E(0), E(0), E(1)$	—	$E(0), E(0), E(1)$
E	$E(0), E(0), E(1)$	$E(0), E(1), E(1)$	$E(0), E(0), E(1)$	$E(0), E(0), E(1)$	—



$$\prod_{i=1}^{N} \prod_{j\in J_i} c_{ij}^{+} * c_{ji}^{+} = \prod_{i=1}^{N} \prod_{j\in J_i} E_{Pk}(b_{ij}^{+} b_{ji}^{+}) = \prod_{i=1}^{N} E_{Pk}(\sum_{j\in J_i} b_{ij}^{+} b_{ji}^{+}) = E_{Pk}(\sum_{i=1}^{N} \sum_{j\in J_i} b_{ij}^{+} b_{ji}^{+}) = E_{Pk}(|M^{+}|)$$

Conclusions

- proposed a representation of a sociogram by a weighted digraph
- we designed the protocol for anonymous sociometric questionnaires
  - based on additively homomorphic public key cryptosystem, which allows us once to use multiplication
  - to compute local characteristics of nodes and the cardinality of sets of mutual choices
  - fulfils desired security requirements
- we are planning to formal analyze the scheme
- for a future design of the protocol looks promisingly recently announced fully homomorphic public key encryption scheme

Thank you for your attention