A Privacy-Aware Protocol for Sociometric Questionnaires*

Marián Novotný

Institute of Computer Science, Pavol Jozef Šafárik University, Jesenná 5,
041 54 Košice, Slovakia
marian.novotny@upjs.sk

Abstract. In the paper we design a protocol for sociometric questionnaires, which serves the privacy of responders. We propose a representation of a sociogram by a weighted digraph and interpret individual and collective phenomena of sociometry in terms of graph theory. We discuss security requirements for a privacy-aware protocol for sociometric questionnaires. In the scheme we use additively homomorphic public key cryptosystem [2], which allows single multiplication. We present the threshold version of the public key system and define individual phases of the scheme. The proposed protocol ensures desired security requirements and can compute sociometric indices without revealing private information about choices of responders.

1 Introduction

Sociometry is a quantitative method for measuring social relationships. It was developed by the psychotherapist Jacob L. Moreno in his studies of the relationship between social structures and psychological well-being [9].

This method is based on *choices* of individuals from a certain social group. Responders are asked to choose one or more persons from the group according to specific criteria known in the whole group. The choices of responders are collected by a *questionnaire*. Relations between individuals can be represented by a *sociogram* – a graphic representation of social links that persons have.

Sociometric techniques can be used for effective management of a school class by a teacher or in team-building in organizations by managers. They can help to discover information about the group or individuals. On the other hand, it is desirable to protect the *privacy* of responders and shield them from misusing delicate information. Our aim is to develop a cryptographic protocol for collection and evaluation of sociometric questionnaires which ensures the desired security requirements, placing emphasis on the privacy of responders.

This paper is organized as follows. The next section introduces a representation of the sociogram in terms of *graph theory*. The section following next describes the proposed scheme for anonymous sociometric questionnaires. In the last section, we present our conclusions and suggestions for the future work.

* This work was supported in part by Slovak VEGA grant number 1/0035/09.

Mathematical and Engineering Methods in Computer Science (MEMICS), Znojmo, Czech Republic, 2009.
Petr Hliněný, Vashek Matyáš, Tomáš Vojnar (Eds.)
Schloss Dagstuhl - Leibniz-Zentrum für Informatik, Germany
Digital Object Identifier: 10.4230/DROPS.MEMICS.2009.2355

2 Representation of a Sociogram by Graph Theory

A sociogram can be represented by a *weighted digraph* [7] $G = (V, E)$, where nodes from V represent individuals from the social group. Each social link is represented by a *weighted arc* from the set $E \subseteq V \times V$. A weight function $w : E \to \{-s, \ldots, -1, 1, \ldots, s\}$ expresses rates of social links. Common values of the parameter *scale* s include $1, 3$, or 5. We say that an arc is *positive* (*negative*) if and only if the weight of the arc is positive (negative).

2.1 Characteristics of a Node

The number of tail endpoints adjacent to a node v is called *indegree* of the node v, i.e., $\deg^{In}(v) = |\{u \in V; \langle u, v\rangle \in E\}|$. It stands for the number of social links to the corresponding person. We distinguish between the *positive indegree* $\deg^{In^+}(v)$ and the *negative indegree* $\deg^{In^-}(v)$ of a node v, where $\deg^{In}(v) = \deg^{In^+}(v) + \deg^{In^-}(v)$. The positive (negative) indegree expresses the number of positive (negative) arcs incident to the node.

The number of head endpoints adjacent from a node v is called *outdegree* of the node v, i. e., $\deg^{Out}(v) = |\{u \in V; \langle v, u\rangle \in E\}|$. It stands for the number of social links from the person. Analogically, we define *positive* (*negative*) *outdegree* of a node v $\deg^{Out^+}(v)$ ($\deg^{Out^-}(v)$).

We also distinguish between *positive* and *negative weighted indegree* (*outdegree*). The sum of weights of all positive arcs incident to a node v is called positive weighted indegree, i. e., $In^+(v) = \sum_{u \in V, \langle u,v\rangle \in E, w(u,v)>0} w(u, v)$. The sum of weights of all negative arcs incident from a node v is called negative weighted outdegree, i. e., $Out^-(v) = \sum_{u \in V, \langle v,u\rangle \in E, w(v,u)<0} w(v, u)$. Similarly, we define for a node v negative weighted indegree $In^-(v)$ and positive weighted outdegree $Out^+(v)$.

2.2 Sociometric Indices and Objects

There exist two approaches to a sociogram – *individual* and *collective phenomena*. Individual phenomena include individual sociometric indices and objects such as *stars, isolates, ghosts*. In the latter case, collective phenomena include group sociometric indices and structures such as *dyads* and *mutual choices*.

Individual sociometric indices can be computed from the above defined characteristics of a node. For example, *positive social status* of a node p is defined as $\frac{In^+(p)}{|V|-1}$. In similar way, objects such as stars, outsiders, ghosts and isolates can be recognized from individual characteristics of nodes.

A star q is a node with the maximal positive weighted indegree, i. e., $In^+(q) = max\{In^+(v); v \in V\}$. An outsider o is a node with the minimal negative weighted indegree, i. e., $In^-(o) = min\{In^-(v); v \in V\}$. A ghost g is a node with zero

indegree and outdegree, i. e., $\deg^{In}(g) + \deg^{Out}(g) = 0$. Finally, an isolate i is a node with zero positive indegree, which is not a ghost, i. e., $\deg^{In^+}(i) = 0 \wedge \deg^{Out}(i) > 0$.

A *dyad* is the smallest and the most elementary social unit, i. e., a group of two members with a mutual choice. We distinguish between *positive, negative* and *combined mutual choices*. In the positive (negative) mutual choice the members positively (negatively) choose each other. In the combined mutual choice, one member chooses positively, but the other one chooses negatively.

A set of positive mutual choices M^+ is defined as $M^+ = \{\{u, v\} \subseteq V, \{\langle u, v\rangle, \langle v, u\rangle\} \subseteq E, w(u, v) > 0, w(v, u) > 0\}$. Similarly, we define a set of negative mutual choices M^- and a set of combined mutual choices $M^{\pm}$. A set of all mutual choices M is defined as $M = M^+ \cup M^- \cup M^{\pm}$.

Using above mentioned definitions, we define a group sociometric index – a *coherence* of the group. A *positive coherence* of a group is defined as $coh^+ = \frac{|M^+|}{\binom{|V|}{2}}$. Similarly, we define a *negative (combined) coherence* coh^- ($coh^{\pm}$).

3 The Proposed Scheme

3.1 The Homomorphic Public-Key System

For encryption of responders' choices we use the homomorphic public-key system from the paper [2], which is *additively homomorphic*. Moreover, it allows us to use a single multiplication. Inter alia, this property is used for computing the cardinality of the set of mutual choices. The encryption system is *semantically secure* assuming the *subgroup decision assumption* [2].

The Key Generation. The construction of the homomorphic scheme from the paper [2] requires to use certain finite groups of composite order that support a *bilinear map*. Let $\mathbb{G}$ and $\mathbb{G}_1$ be two multiplicative cyclic groups of finite order n, where g is a generator of $\mathbb{G}$. Let e denote a bilinear map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_1$. It holds, that for all $u, v \in \mathbb{G}$ and $a, b \in \mathbb{Z}$, we have $e(u^a, v^b) = e(u, v)^{ab}$. Moreover, $e(g, g)$ is a generator of $\mathbb{G}_1$.

The key setup works as follows:

- Generate two random primes q_1, q_2 and set $n = q_1 \cdot q_2 \in \mathbb{Z}$.
- Generate a bilinear group $\mathbb{G}$ of order n following the paper [2]. Let g, u be random generators of $\mathbb{G}$ and $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_1$ be the bilinear map. Then $h = u^{q_2}$ is a random generator of the subgroup $\mathbb{G}$ of order q_1.
- The public key is $Pk = (n, \mathbb{G}, \mathbb{G}_1, e, g, h)$. The private key is $Sk = q_1$.

Encryption and Decryption. To encrypt a message $m \in \{0, \ldots, q_2 - 1\}$, a sender chooses a random number $r \in \mathbb{Z}_{n-1}$ and computes the ciphertext $C = g^m h^r \in \mathbb{G}$. To decrypt the ciphertext C using the private key $Sk = q_1$, observe that $C^{q_1} = (g^m h^r)^{q_1} = (g^{q_1})^m$. It is sufficient to compute the discrete logarithm

of C^{q_1} base g^{q_1} in order to recover the plaintext m. For our purposes, the message space is bounded by the value $b = \max\{s(|V|-1), \binom{|V|}{2}\}$[1], where s is the scale and $|V|$ is the number of nodes in a sociogram. This way it is sufficient to precompute the table of powers $(g^{q_1})^0, \ldots, (g^{q_1})^b$. Using binary-search, one can find an appropriate m in the logarithmic time according to the number of nodes.

Homomorphic Properties. The encryption system is clearly additively homomorphic. Given ciphertexts $C_1, C_2 \in \mathbb{G}$ which are encryptions of plaintexts m_1, m_2, anyone can create an encryption of $m_1 + m_2 \bmod n$ by computing the product $C_1C_2 = g^{m_1}h^{r_1}g^{m_2}h^{r_2} = g^{m_1+m_2}h^{r_1+r_2}$. Note that we can multiply an encrypted message m by an integer $z \in \mathbb{Z}^+$. Given the ciphertext $C = g^m h^r$, anyone can create an encryption of $zm \bmod n$ by computing the exponentiation $C^z = g^{zm}h^{zr}$.

Anyone can once multiply two encrypted messages m_1, m_2 using the bilinear map e. Set $g_1 = e(g,g) \in \mathbb{G}_1$ and $h_1 = e(g,h) \in \mathbb{G}_1$. Then, g_1 is of order n and h_1 is of order q_1. For given ciphertexts $C_1 = g^{m_1}h^{r_1}, C_2 = g^{m_2}h^{r_2} \in \mathbb{G}$ we build an encryption of $m_1 \cdot m_2$ as $C_1 * C_2 = e(C_1, C_2) = e(g^{m_1}h^{r_1}, g^{m_2}h^{r_2}) = e(g^{m_1+\alpha q_2 r_1}, g^{m_2+\alpha q_2 r_2}) = g_1^{m_1 m_2} h_1^{m_1 r_2 + r_2 m_1 + \alpha q_2 r_1 r_2} \in \mathbb{G}_1$, where $h = g^{\alpha q_2}$. Note that the system is still additively homomorphic in $\mathbb{G}_1$.

The Robust Threshold Version. The goal of the *threshold* version (t, l) of the cryptosystem is to share the private key q_1 among l authorities by a threshold secret sharing scheme. A ciphertext can be decrypted when at least $t+1$ shareholders cooperate on decryption in the group $\mathbb{G}_1$. Note that it is sufficient to decrypt only in the group $\mathbb{G}_1$ since we can use the bilinear map to move the ciphertext from $\mathbb{G}$ to the group $\mathbb{G}_1$ without changing the plaintext.

For simplicity, we assume that a trusted dealer first generates the public key including $n = q_1 \cdot q_2$ and the private key q_1. The dealer distributes shares of the private key between l authorities. The shares are created following the technique [13, 5], which is a modification of the *Shamir secret sharing* scheme [12] over $\mathbb{Z}_n$. The dealer sets $a_0 = q_1$ and chooses a_i at random from $\{0, \ldots, n-1\}$ for $i \in \{1, \ldots, t\}$. The numbers $a_0, \ldots, a_t$ define the polynomial $f(X) = \sum_{i=0}^{t} a_i X^i \in \mathbb{Z}[X]$. For each shareholder $i \in \{1, \ldots, l\}$ the dealer computes $s_i = f(i) \bmod n$. Let $\Delta = l!$ and $\Delta^\star = \Delta^{-1} \bmod n$. For any subset P of $t+1$ indices from $\{1, \ldots, l\}$ the modified *Lagrange coefficients* are defined as $\lambda_{i,P} = \Delta \frac{\prod_{i' \in P/\{i\}} -i'}{\prod_{i' \in P/\{i\}} i - i'} \bmod n$. From the *Lagrange interpolation* we have $\Delta \cdot f(0) = \sum_{i \in P} \lambda_{i,P} f(i) \bmod n$, i. e., $\Delta \cdot q_1 = \sum_{i \in P} \lambda_{i,P} s_i \bmod n$.

Moreover, a shareholder i which possesses the secret s_i publishes $y_i = g_1^{s_i}$ in order to make a process of decryption verifiable. To decrypt a ciphertext $C = g_1^m h_1^r \in \mathbb{G}_1$ without reconstructing the secret q_1 each shareholder i publishes $u_i = C^{s_i}$ and following the Chaum-Pedersen protocol [3] proves that $\log_{g_1} y_i = \log_C u_i$. From any subset of $t+1$ participants P who passed the proof

[1] The value $s(|V|-1)$ is the maximal possible absolute value of weighted degrees and $\binom{|V|}{2}$ is the maximum cardinality of the set of mutual choices.

the value $g_1^{\Delta q_1 m}$ is computed as as $\prod_{i \in P} u_i^{\lambda_{i,P}} = \prod_{i \in P} C^{\lambda_{i,P} s_i} = C^{\sum_{i \in P} \lambda_{i,P} s_i} = (g_1^m h_1^r)^{\Delta \cdot q_1} = g_1^{\Delta q_1 m}$. After computing $(g_1^{\Delta q_1 m})^{\Delta^\star} = g_1^{q_1 m}$, the plaintext m can be recovered by comparing with pre-computed tables of powers of $g_1^{q_1}$ as mentioned above.

The zero-knowledge proofs of correct partial decryption [3] from each shareholder can be performed interactively between shareholders and transcripts of such interactions are made public for verification. In order to make these proofs non-interactive, the verifier could be implemented using either a trusted *source of random bits* [10] or using the *Fiat-Shamir heuristic* [4] which requires a hash function. In the latter case security is obtained from the *random oracle model* [8].

3.2 Security Requirements for a Scheme

The scheme is expected to satisfy certain security requirements which are relevant for a privacy-aware protocol for sociometric questionnaires. The social group which consists of responders is defined in the questionnaire. It also contains a selection criterion and other parameters such as the deadline for filling. We enumerate and informally discuss security requirements in the following list.

- *Eligibility.* Only valid responders who are defined as members of the group are eligible to correctly fill in the questionnaire.
- *Privacy.* In the evaluation process, choices of a responder must not identify the responder and any traceability between the responder and his choices must be removed.
- *Verifiability.* Any responder should be able to *individually* verify whether his choices were correctly recorded and accounted. Moreover, anyone can *universally* verify that in the evaluation process only valid choices of eligible responders were recorded and the counting process was accurate.
- *Accuracy.* The scheme must be error-free. The final computations of sociometric indices must correspond with all choices of all responders.

Note that these requirements are similar to security requirements for e-voting protocols [11]. However, the submission of choices and computations of the results differ from usual e-voting protocols. On the other hand, a scheme does not need to ensure requirements such as *receipt-freeness* or *incoercibility* [11], because we do not expect "choice-buying" of responder's choices.

3.3 The Proposed Scheme

The realization of the scheme consists of various phases. First, the *questioner* creates a questionnaire in which he defines a social group of responders $R_1, \ldots, R_N$ and sociometric indices which have to be computed. He also sets the deadline for filling and the sociometric parameters such as the scale s for the weights of the arcs. Then, he registers the questionnaire by the *collector*. The collector collects submissions of responders, checks signatures, leads the computations and

publishes results. The registration of responders $R_1, \ldots, R_N$ is based on digital signatures. Therefore, we assume a pre-established *Public Key Infrastructure* with registered conceivable responders and other participants with relevant *certificates* of public keys for digital *signature* [8].

For encryption of choices, we use the above mentioned robust threshold (t, l) version of the public-key scheme [2], where the private key $Sk = q_1$ is shared between l authorities. For simplicity, we assume that a trusted dealer first generates the public key Pk and the private key $Sk = q_1$. Then, the dealer creates and distributes shares of the private key between l authorities and finally deletes the private key.

The process of decryption is realized by cooperation of at least $t+1$ authorities and is universally verifiable as mentioned above. Note that we do not specify who should be shareholders, since it depends on the usage of the protocol. However, the robust threshold version of the cryptosystem ensures the robustness of the protocol.

Submitting Choices. A responder R_i fills in the questionnaire, i. e., defines all relations from the node R_i in the sociogram. To represent a relation from the node R_i to node R_j we use $s + 2$ bits $b_{ij}^+, b_{ij}^-, b_{ij}^{w_1}, \ldots, b_{ij}^{w_s}$, where s is the scale as defined in Section 2. The bits b_{ij}^+, b_{ij}^- indicate whether the weight of the arc is positive, negative, or there is missing arc. The bit $b_{ij}^{w_{|w_{ij}|}} = 1$ defines the absolute value of the weight of the arc $|w_{ij}|$. We consider three possible relations from the node R_i to the node R_j:

- The arc $\langle R_i, R_j \rangle$ has a positive weight $w_{ij} > 0$, then $b_{ij}^+ = 1, b_{ij}^{w_{w_{ij}}} = 1$, and other bits are 0;
- The arc $\langle R_i, R_j \rangle$ has a negative weight $w_{ij} < 0$, then $b_{ij}^- = 1, b_{ij}^{w_{|w_{ij}|}} = 1$, and other bits are 0;
- There is missing arc $\langle R_i, R_j \rangle$, then an arbitrary bit $b_{ij}^{w_a} = 1$, where $a \in \{1, \ldots, s\}$ and other bits are 0.

Note that, when the parameter scale $s = 1$, it is sufficient to represent a relation from the node R_i to the node R_j with just two bits b_{ij}^+, b_{ij}^-.

For each responder $R_j, j \neq i$ each bit $b_{ij}^\diamondsuit, \diamondsuit \in \{+, -, w_1, \ldots, w_s\}$ is encrypted by responder R_i using the public key Pk as $c_{ij}^\diamondsuit = E_{Pk}(b_{ij}^\diamondsuit)$. All these encrypted bits are sent along with the signature of the encrypted bits by the responder R_i to the collector.

Verification of Submissions. The collector checks the validity of signatures of all submissions of responders $R_1, \ldots, R_N$. If the responder R_i does not submit his choices in time, or his signature is incorrect, then he is disqualified from the set of responders. The encrypted relations to the node R_i are excluded as well. Finally, the collector publishes submissions with correct signatures in order to verification.

In the e-voting protocols based on homomorphic encryption, are usually used zero-knowledge proofs for verification of validity of ballots [11]. These proofs are used in the non-interactive version using Fiat-Shamir heuristic [4]. As a bonus of the public key system, we do not need to use these proofs according to verification of validity of submissions.

The submissions of responders in the bit representation are valid, if the following conditions hold:

1. $b_{ij}^{\diamondsuit} \in \{0,1\}$, which is equivalent to the formula $b_{ij}^{\diamondsuit} \cdot (b_{ij}^{\diamondsuit} - 1) = 0$, where $i \neq j, \diamondsuit \in \{+,-,w_1,\ldots,w_s\}$;
2. $b_{ij}^{+} \cdot b_{ij}^{-} = 0$, where $i \neq j$;
3. $\sum_{k=1}^{s} b_{ij}^{w_k} = 1$, which is equivalent to the formula $\sum_{k=1}^{s} b_{ij}^{w_k} - 1 = 0$, where $i \neq j$.

We need to verify all these equations of the form – left side le is equal to zero. We can use the homomorphic properties for preparing ciphertexts of le for $(s+2)N(N-1)$ equations of the first type, $N(N-1)$ of the second and $N(N-1)$ of the third type. We have to check $v = (s+4)N(N-1)$ equations total.

To prepare ciphertexts of equations of first and third type the collector publishes a deterministic encryption of $-1 \bmod n$. The equations can be checked by shareholders by v cooperatively-made decryptions. To decrease the computation complexity, the shareholders check simultaneously a batch of equations $\sum_{i=1}^{v} r_i \cdot le_i = 0$, where r_i are chosen cooperatively by shareholders. They can run a binary search to identify the invalid submissions following the technique from [1]. This way, in the optimistic scenario (when all submissions are valid) is used just one decryption of shareholders.

Computations of the Sociometric Indices. We define computations in the bit representation of a sociogram as shown in Table 1. Let J_i denote the set $\{1,\ldots,N\}/\{i\}$. A relation from a node R_i to a node R_j is represented by bits $b_{ij}^{+}, b_{ij}^{-}, b_{ij}^{w_1}, \ldots, b_{ij}^{w_s}$. If there exists an arc $\langle R_i, R_j \rangle$, the value $|w_{ij}| = \sum_{k=1}^{s} k \cdot b_{ij}^{w_k}$ represents the absolute value of the weight of the arc $\langle R_i, R_j \rangle$. If there is no arc $\langle R_i, R_j \rangle$, the value $|w_{ij}| = \sum_{k=1}^{s} k \cdot b_{ij}^{w_k} = a$, since exactly one arbitrary chosen bit $b_{ij}^{w_a} = 1$ as defined above. Note that it is easy to show that the definitions of

Table 1. Computations in the bit representation of a sociogram

$\deg^{In^+}(R_i) = \sum_{j \in J_i} b_{ji}^{+}$ $\deg^{Out^-}(R_i) = \sum_{j \in J_i} b_{ij}^{-}$ $In^{+}(R_i) = \sum_{j \in J_i} b_{ji}^{+} \cdot \lvert w_{ji} \rvert$	$\deg^{In^-}(R_i) = \sum_{j \in J_i} b_{ji}^{-}$ $\deg^{In}(R_i) = \sum_{j \in J_i} b_{ji}^{+} + b_{ji}^{-}$ $In^{-}(R_i) = -\sum_{j \in J_i} b_{ji}^{-} \cdot \lvert w_{ji} \rvert$	$\deg^{Out^+}(R_i) = \sum_{j \in J_i} b_{ij}^{+}$ $\deg^{Out}(R_i) = \sum_{j \in J_i} b_{ij}^{+} + b_{ij}^{-}$
$\lvert M^{+} \rvert = \sum_{i=1}^{N} \sum_{j>i} b_{ij}^{+} \cdot b_{ji}^{+}$ $\lvert M^{-} \rvert = \sum_{i=1}^{N} \sum_{j>i} b_{ij}^{-} \cdot b_{ji}^{-}$	$\lvert M^{\pm} \rvert = \sum_{i=1}^{N} \sum_{j>i} (b_{ij}^{-} \cdot b_{ji}^{+}) + (b_{ij}^{+} \cdot b_{ji}^{-})$ $\lvert M \rvert = \sum_{i=1}^{N} \sum_{j>i} (b_{ij}^{-} \cdot b_{ji}^{+}) + (b_{ij}^{+} \cdot b_{ji}^{-}) + (b_{ij}^{+} \cdot b_{ji}^{+}) + (b_{ij}^{-} \cdot b_{ji}^{-})$	

computations from Table 1 correspond with the definitions from Section 2.

Computations on Encrypted Sociogram. The collector computes the value c_{ij}^{w} from encrypted values $c_{ij}^{w_1}, \ldots, c_{ij}^{w_s}$, i. e., $c_{ij}^{w} = \prod_{k=1}^{s}(c_{ij}^{w_k})^k = \prod_{k=1}^{s} E_{Pk}(b_{ij}^{w_k})^k = \prod_{k=1}^{s} E_{Pk}(k \cdot b_{ij}^{w_k}) = E_{Pk}(\sum_{k=1}^{s} k \cdot b_{ij}^{w_k}) = E_{Pk}(|w_{ij}|)$. For an encrypted representation of a relation from the node R_i to R_j we use values $c_{ij}^{+}, c_{ij}^{-}, c_{ij}^{w}$ in the encrypted sociogram.

The ciphertext of the positive indegree of a node R_i is computed as $\prod_{j \in J_i} c_{ji}^{+} = \prod_{j \in J_i} E_{Pk}(b_{ji}^{+}) = E_{Pk}(\sum_{j \in J_i} b_{ji}^{+}) = E_{Pk}(\deg^{In^+}(R_i))$. Similarly, we can compute the ciphertext of the negative indegree $E_{Pk}(\deg^{In^-}(R_i))$. Finally the ciphertext of the indegree of the node R_i is $E_{Pk}(\deg^{In}(R_i)) = \prod_{j \in J_i} c_{ji}^{+} c_{ji}^{-}$. Analogously, we can compute ciphertexts of outdegrees, for example the encryption of the positive outdegree $E_{Pk}(\deg^{Out^+}(R_i)) = \prod_{j \in J_i} c_{ij}^{+}$.

To compute encryptions of weighted degrees, we use also the multiplicative property of the homomorphic system. The ciphertext of positive weighted indegree of the node R_i can be computed as $\prod_{j \in J_i} c_{ji}^{+} * c_{ji}^{w} = \prod_{j \in J_i} E_{Pk}(b_{ji}^{+}|w_{ji}|) = E_{Pk}(\sum_{j \in J_i} b_{ji}^{+}|w_{ji}|) = E_{Pk}(In^{+}(R_i))$. Similarly, we can compute other weighted degrees.

Anyone can compute the encrypted value of the cardinality of the set of positive mutual choices as $\prod_{i=1}^{N} \prod_{j>i} c_{ij}^{+} * c_{ji}^{+} = \prod_{i=1}^{N} \prod_{j>i} E_{Pk}(b_{ij}^{+} b_{ji}^{+}) = \prod_{i=1}^{N} E_{Pk}(\sum_{j>i} b_{ij}^{+} b_{ji}^{+}) = E_{Pk}(\sum_{i=1}^{N} \sum_{j>i} b_{ij}^{+} b_{ji}^{+}) = E_{Pk}(|M^{+}|)$. The set of negative and the set of combined mutual choices are defined similarly. The ciphertext of the cardinality of the set of all mutual choices one can count as $\prod_{i=1}^{N} \prod_{j>i} (c_{ij}^{+} * c_{ji}^{+})(c_{ij}^{+} * c_{ji}^{-})(c_{ij}^{-} * c_{ji}^{+})(c_{ij}^{-} * c_{ji}^{-})$.

This way we derived encrypted values of individual and collective phenomena with respect to definitions from Section 2 only by using homomorphic properties of the encryption system. Note that the process of computations is universally verifiable by anyone. After computing and publishing encrypted sociometric indices, the shareholders of the private key $Sk = q_1$ individually verify the correctness of computation and cooperate to decrypt the desired sociometric indices. The process of decryption is universally verifiable by anyone including the responders, the collector and the questioner. Finally, the collector publishes obtained sociometric indices which express quantitative information about individuals or the group.

4 Conclusions

In this paper we designed the protocol for anonymous sociometric questionnaires. In the protocol each responder sends only one message. To prepare the submission costs $(N-1)(s+2)$ encryptions of the cryptosystem [2] and one digital signature, where N is the number of responders and s is the parameter scale. The protocol guarantees the security requirements from Section 3. 2. The eligibility property is ensured by digital signatures of the submissions by responders and checking of the validity of submissions. The signatures are checked by the collector and verified by anyone. The validity of submissions is checked by shareholders and verified by anyone. The privacy of responders is provided by

the public key cryptosystem [2], which is semantically secure and homomorphic operations are also commutative. The process of computation and decryption of sociometric indices is universally verifiable according to universal verifiability of the threshold version of the cryptosystem and the defined computations on encrypted sociogram.

In the future work we are planning to formal model and analyze the scheme in the *applied pi-calculus*. For a future design of the protocol, recently announced fully homomorphic public key encryption scheme [6] looks promisingly. The results from the paper were presented as a talk on Primelife/IFIP Summer School 2009 – Privacy and Identity Management for Life

References

1. Bellare, M., Garay, J., Rabin, T.: Fast batch verification for modular exponentiation and digital signatures. EUROCRYPT'98, LNCS, vol. 1403. Springer (1998)
2. Boneh, D., Goh, E.-J., Nissim, K.: Evaluating 2-DNF formulas on ciphertexts. TCC '05. LNCS, vol. 3378. Springer (2005)
3. Chaum, D., Pedersen, T.: Wallet databases with observers. CRYPTO '92. LNCS, vol. 740. Springer (1993)
4. Fiat, A., Shamir, A.: How to prove yourself: practical solutions to identification and signature problems. Advances in cryptology—CRYPTO '86. LNCS, vol. 263. Springer (1987)
5. Gang, Q., et al.: Information-theoretic secure verifiable secret sharing over RSA modulus. Wuhan University Journal of Natural Sciences, vol. 11. Springer (2006)
6. Gentry, C.: Fully homomorphic encryption using ideal lattices. STOC '09. ACM (2009)
7. Hanneman, R. A., Riddle, M.: Introduction to social network methods. Riverside, University of California (2005)
8. Mao, W.: Modern Cryptography: Theory and Practice. Prentice Hall Professional Technical Reference (2003)
9. Moreno, J. L.: Who Shall Survive? Foundations of Sociometry, Group Psychotherapy and Sociodrama. Beacon House, Inc. (1953)
10. Rabin, M. O.: Transaction Protection by Beacons. Journal of Computer and System Sciences, vol. 27(2). Elsevier (1983)
11. Sampigethaya, R., Poovendran, R.: A Framework and Taxonomy for Comparison of Electronic Voting Schemes. Elsevier Computers & Security, vol. 25 (2006)
12. Shamir, A.: How to share a secret, Commun. ACM 22, vol. 11 (1979)
13. Shoup, V.: Practical Threshold Signatures. EUROCRYPT 2000. LNCS, vol. 1807. Springer (2000)