社団法人 情報処理学会 研究報告
IPSJ SIG Technical Reports

2006－CSEC－34 (51)
2006／7／21

プライバシを保護した授業評価アンケートの実装

谷川 浩司† 中西 透† 舩曳 信生†

† 岡山大学大学院自然科学研究科，700-8530 岡山県岡山市津島中 3-1-1

あらまし 多くの大学において紙ベースの授業評価アンケートが行われているが，集計の手間や経費が大きいという問題があり，授業評価アンケートの WEB システム化が求められている．その一方で，授業評価アンケートでは，回答者のプライバシを保護する必要がある．そこで本論文では，Paillier 暗号を用いることにより，回答内容を暗号化したまま集計可能な WEB アンケートシステムの実装を行う．Paillier 暗号を用いることにより，従来方式と比較して，暗号化コストを削減している．そして，著者らの属する学科での試用実験の結果によりその有用性を示す．

キーワード 授業評価アンケート，Paillier 暗号，準同型性暗号

An Implementation of a Privacy Enhancing Questionnaire System for Evaluating Classes

Koji TANIGAWA†, Toru NAKANISHI†, and Nobuo FUNABHIKI†

† Graduate School of Natural Science and Technology, Okayama University, Tsushimanaka 3-1-1, Okayama-shi, 700-8530 Japan

Abstract Lots of universities execute of the paper-based class evaluation questionnaires, which require lots of time and expenditure. Thus, a WEB-based questionnaire system is required. On the other hand, it is necessary to protect respondents' privacy. Therefore, we adopt a voting protocol using the Paillier cryptosystem which is one of homomorphic cryptosystems, and implement a questionnaire system based on it. The encryption cost has been reduced by Pailllier cryptosystem compared with the previous protocols. In addition, the practicality is shown by the result of the trial experiment.

Key words class evaluation questionnaire, Paillier cryptosystem, homomorphic cryptosystem

1. まえがき

近年多くの大学において，学生が自分の受講した授業の内容を評価する，いわゆる授業評価が盛んに行われている．授業評価の目的は授業内容の改善を促すこと，学生の学習意欲を確かめることなど様々である．そして評価内容を教員にフィードバックすることで，授業内容の改善や向上が期待できる．著者らの属する大学において，アンケート方式による学生授業評価を行っており，最終試験実施時にアンケート用紙を学生に配布し，試験の終了時やアンケート回収箱によりアンケート回収を行っている．

しかし，紙ベースでアンケートを行った場合，集計を手作業で行う必要があり，また光学式文字読取装置 (OCR) を用いてコンピュータで行う場合にも経費負担が大きくなってしまう．このため，基本的に１つの授業に対し１回のアンケートしか行えず，アンケート結果が教員にフィードバックされるのは，次年度に開講される授業以降となる．本来問題となっている今年度の授業には反映されない．

そこで本研究では，これらの問題を改善するために，授業評価アンケートの WEB システム化を行う．それによりペーパーレス化，省力化を図り，１つの授業において複数回のアンケートを実施することで，その年の授業自体にフィードバックをかけ，授業の改善・向上を目指すことを目的とする．

一方，授業評価アンケートでは回答者のプライバシ保護を考える必要がある．従来，WEB ベースでのプライバシを強化したアンケートの実装として，次の２つが提案されている．

（1） 北川らによる講義評価の匿名アンケートシステム [1]

２種類のブラインド署名と受領書を用いることにより，プライバシを維持しながら各学生が回答したか否かの識別を可能としたアンケートシステム．本システムでは，匿名通信路を用意する必要がある．

（2） 中里らによる電子匿名アンケートシステム [2]

準同型性をもつ ElGamal 暗号を利用した電子投票プロトコルに基づいたアンケートシステム

本論文で扱うアンケートシステムでは，後者の準同型性を満たした公開鍵暗号を用いる方式によって実現する．前者のブラインド署名と匿名性通信路を用いる方式では，アンケート形式に制約がない反面，匿名通信路の設置のための大きなコストを要する．文献 [1] では登録端末と独立した共用端末により回答を行うという運用上の工夫により擬似的に匿名通信を実現しているが，やはり，コストが大きくなることは避けられない．これに対し，後者の方式では匿名通信路を用いず，コストを軽減できる．また，集計サーバでは暗号化されたデータが管理されるためデータの秘匿性も保証することができる．

しかし，中里らの方式で利用している ElGamal 暗号が満たすのは乗法の準同型性であるため，復号の際に離散対数問題を解く必要がある．効率化のため複数の選択肢をまとめて暗号化する場合，復号時のオーバヘッドが大きくなってしまう．このため，選択肢をまとめるのが困難であり，設問数が増加すると送信する暗号文の数が増大してしまうという問題がある．

そこで本研究では Paillier 暗号 [3] を用いてシステムの構築を試みる．Paillier 暗号では加法の準同型性が成り立ち，復号時に離散対数を計算する必要がないため，復号の際のオーバヘッドも小さく抑えられ，1 つの暗号文により多くの選択肢に対する回答を含めさせることができる．

本研究室では現在，教室での対面授業を前提に，教員による教育活動を支援することを目的とした WEB システム NOBASU(NetwOrk-Based Assistant System for University education) [4] の開発・運用を行っている．本研究では，NOBASU にアンケート機能を追加実装することで，アンケートの WEB システム化を実現する．Paillier 暗号を用いた投票プロトコルによるアンケートシステムの NOBASU への追加実装では，クライアント側である学生や担当教員には Java アプレットを，集計を行う WEB サーバである NOBASU には Java サーブレットをそれぞれ用いた．これにより，必要な暗号化処理をクライアント側で行うことができ，サーバ側にアンケート内容を秘匿することが可能になる．また，実装したシステムを岡山大学工学部通信ネットワーク工学科の「プログラミング演習 III」の授業で実際に利用し，ユーザビリティについて評価を行い，システムの改善点を検討した．

最後に本論文の章構成について述べる．まず，2 章で授業評価アンケートのモデルと要件を示し，3 章で利用する暗号技術と投票プロトコルについて説明する．次に，4 章で NOBASU およびその構築における基盤技術を説明し，5 章で実装したシステムについて述べる．そして 6 章でシステムの評価を示し，最後に 7 章で本論文をまとめる．

2. 授業評価アンケートのモデルと要件

2.1 モデル

本論文で対象とするアンケートシステムは第 4 章で述べる教育支援システム NOBASU の機能の 1 つとして追加する．ここで，NOBASU の運営・管理が学生によって行われているため，その学生に各学生のアンケートの回答内容を秘匿し，誰がどのように回答したかを特定できないようにする必要がある．一方で，アンケート対象の授業を行っている教員に対しても，誰がどのような回答を行ったかは秘匿したい．

今回のモデルとしては，ブラウザを用いて回答する回答者 (学生)，回答者からのアンケートデータの集計・管理を行う集計サーバ，暗号化された回答の集計結果の復号を行えるプライバシ管理者 (授業の担当教員) を想定する．ここで，集計サーバとプライバシ管理者が結託しないことを仮定する．このモデルは文献 [2] に基づいており，他の環境においても適応可能である．

また，アンケートの設問は授業評価アンケートで主に使われている N 個の選択肢の中から 1 つのみを選ぶ *1-out-of-N* と呼ばれる形式の設問に限定する．

2.2 授業評価アンケートの要件

上述のモデルにおいて授業評価アンケートシステムを考える場合に，満たすべき要件を以下に示す．

（1） 回答者の不正回答防止:
1 人の回答者は 2 回以上回答する多重回答を行えないこと．また，アンケートに回答する権利のないユーザが回答を行えないこと．

（2） 集計サーバへのデータの秘匿性:
集計サーバにおいて，外部からの攻撃や内部犯に対してもデータの秘匿性が保証されること．

（3） プライバシ管理者へのデータの秘匿性:
プライバシ管理者は復号したアンケート結果から「誰がどの回答を行ったか」ということを特定できないこと．

（4） 回答者の識別:
集計サーバはどの学生が回答し，どの学生が回答していないかを検知できること．

3. 利用する暗号技術と投票プロトコル

本研究では，Paillier 暗号 [3] を用いてアンケートデータを暗号化したまま保管・管理し，さらに暗号化したまま集計も行う．これにより，NOBASU 管理者や，WEB の設定ミスにより情報が漏洩しても，安全性を保つことがでる．また，Paillier 暗号を用いることで複数の設問に対する回答を 1 つにまとめて暗号化・復号を行うことができる．

3.1 ElGamal 暗号に基づいたプロトコルにおける問題

比較のため，文献 [2] で用いられている，準同型性を満たす暗号である変形 ElGamal 暗号のアルゴリズムを示す．ElGamal 暗号では乗法における準同型性を満たし，暗号化関数を E とすると E 上での，$\otimes$ の演算に対して，$E(m_1) \otimes E(m_2) = E(m_1 \times m_2)$ が成立する．このとき，ある底 $\tilde{G}$ に対して $\tilde{G}^m$ を ElGamal 暗号化することにより，加法の準同型性が得られる．このような方式を変形 ElGamal 暗号と呼ぶ．

以下に変形 ElGamal 暗号の各アルゴリズムを示す．

公開鍵として長さ $l_{\tilde{p}}$ の素数の法 $\tilde{p}$，素数位数 $\tilde{q}$ の元 $\tilde{g}, \tilde{G} \in Z_{\tilde{p}}^*$(ただし $\tilde{q} | \tilde{p}-1$) を選ぶ．さらに秘密鍵 $\tilde{x} \in Z_{\tilde{q}}$ を選び，$\tilde{g}$ と $\tilde{x}$ より公開鍵 $\tilde{y}$ を $\tilde{y} = \tilde{g}^{\tilde{x}} \bmod \tilde{p}$ として求める．

メッセージ $\tilde{m}$ に対して乱数 $\tilde{r} \in_R Z_{\tilde{q}}$ を選び，変形 ElGamal 暗号の暗号文 $\tilde{E}(\tilde{m})$ は以下のようになる．

$$\tilde{E}(\tilde{m}) = (\tilde{g}^{\tilde{r}} (\mathrm{mod}\ \tilde{p}),\ \tilde{y}^{\tilde{r}} \tilde{G}^{\tilde{m}} (\mathrm{mod}\ \tilde{p}))$$

また，復号は

$$\frac{\tilde{y}^{\tilde{r}} \tilde{G}^{\tilde{m}}}{(\tilde{g}^{\tilde{r}})^{\tilde{x}}} \bmod \tilde{p} = \tilde{G}^{\tilde{m}}$$

となる．このように変形 ElGamal 暗号では復号が行われた時点では元のメッセージそのものを得ることはできず，離散対数問題を解くことによって得ることができる．このため，$\tilde{m}$ の値を小さくする必要がある [2] [5].

3.2 Paillier 暗号

利用するプロトコルでは，加法における準同型性を満たす暗号アルゴリズムである Paillier 暗号を用いる．ここで加法における準同型性とは，E 上での，$\otimes$ の演算に対して，$E(m_1) \otimes E(m_2) = E(m_1 + m_2)$ が成立することである．以下に暗号方式の各アルゴリズムを示す．ただし，RSA のセキュリティパラメータを l_n とする．

鍵生成アルゴリズム：

長さ ℓ_n の RSA の法 $n = pq$ (p, q は素数) と，位数が n の倍数であるような素数 $g \in Z^*_{n^2}$ を選び，公開鍵 (n, g) と秘密鍵 $\lambda(n) = \mathrm{lcm}(p-1, q-1)$ を出力する．

暗号化アルゴリズム：

メッセージ $m \in Z_n$ に対して，乱数 $r \in_R Z_n$ を選び，以下のようにして暗号文 $E(m)$ を計算する．

$$E(m) = g^m r^n \bmod n^2$$

復号アルゴリズム：

暗号文 $c = E(m)$ の復号は，以下のようにして行う．ここで，関数 L は $L(u) = (u-1)/n$ と定義される．

$$\frac{L(c^\lambda \bmod n^2)}{L(g^\lambda \bmod n^2)} \bmod n = m$$

以下に示すように，Paillier 暗号は加法において準同型性を満たす．

$$E(m_1) \times E(m_2) = (g^{m_1} r_1^n)(g^{m_2} r_2^n)$$

$$= g^{m_1+m_2}(r_1 r_2)^n = E(m_1 + m_2)$$

3.3 利用する投票プロトコル

ここでは利用する投票プロトコル [6] [7] を説明する．

まず，今回のアンケートの設問では，N 個の選択肢の中から 1 つのみを選ぶことを仮定している．このような設問の総数を L とする．この場合，全アンケート中では選択肢の総数は LN となり，これらを $i = 1, 2, \cdots, LN$ により表すとする．このとき，各選択肢 i を値 $(T+1)^{i-1}$ で表現することを考える．ここで，T は回答者数の上限である．回答者は L 個の各設問に対して 1 つ候補を選ぶことになるため，候補 LN 個の中から L 個を選んで回答することになる．この際，回答者は選んだ L 個の候補に対応する L 個の値 $(T+1)^{i-1}$ の和 (回答内容) を Paillier 暗号により暗号化して回答する．ここで $(T+1)^{LN} < n$ を仮定する．もし，$(T+1)^{LN} \geq n$ の場合，複数の暗号文となる．

集計の際には，全回答者の暗号文を乗算することにより準同型性から，すべての票の和 $v_1 + v_2(T+1) + \cdots + v_L N(T+1)^{LN-1}$ (ただし v_i : 選択肢 i に対する得票数) の暗号文を得る．これを復号した値を $(T+1)^{i-1}$ $(i = 2, \cdots, LN)$ で除算していくことで，各選択肢 i の得票数 v_i を求めることができる．

ElGamal 暗号でこの投票方法を利用した場合，メッセージ $\tilde{m}$ が大きくなってしまい，復号時の離散対数問題を解く時間が非常に大きくなってしまう．このため，多数の選択をまとめて暗号化するのは困難である．

これに対し，Paillier 暗号では復号した際にそのまま，メッセージ m を得ることができるため，ElGamal 暗号に比べ高速に集計結果を得ることができる．

本研究では，暗号文の正当性は保証されるものと仮定する．そうでない場合，正当性を証明するゼロ知識証明が必要となる．文献 [6] の効率的な方式が採用可能であるが，その実装は今後の課題とする．

4. NOBASU およびその構築における基盤技術

本章では，提案するアンケートシステムを追加実装する WEB ベースの教育支援システム NOBASU，および Java アプレットについて述べる．

4.1 NOBASU

NOBASU とは本研究グループで独自に開発と運用を進めている，本学科の教育に適した，授業・演習を対象とする WEB ベースの教育支援システムである．本システムは，対面授業の存在を前提として，それを補完・拡張することで，大学での教育サービスの改善や一層の充実を図り，同時に教員負荷を軽減することを目的としたものである．NOBASU の機能には，学生サービス機能として，授業資料ダウンロードやレポート提出機能，教員サービス機能として，メール送信機能や成績一覧表示機能プログラミング課題の検証支援機能などがある．

図 1 に NOBASU の動作環境を示す．NOBASU は，サービスを利用する学生，教員，システム管理者から成るクライアントコンピュータ群と，サービスを提供する側であるサーバコンピュータ群で構成される．NOBASU の動作環境として，サーバ OS には Linux，WEB サーバには Apache，アプリケーションサーバには Tomcat を利用し，サーバプログラムには Java サーブレット/JSP を用いて記述されている．また，データベースには MySQL が用いられている．

4.2 Java アプレット

今回は NOBASU で従来使用しているソフトウェアに加え，Java アプレットも利用している．

もし Java サーブレット/JSP のみで実装した場合，集計サー

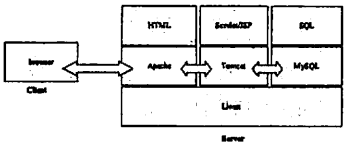

図1 NOBASU の動作環境

バ側で処理が行われるため，アンケート内容の暗号化も集計サーバ側で行われることになる．このままでは集計サーバに対しアンケート内容を秘匿できない．クライアント側で暗号化を行うため本アンケートシステムの実装では，Java アプレットを用いる．Java アプレットとは，WEB ページの HTML ソースコードから参照されるプログラムを指す．WEB サーバからブラウザに動的にダウンロードされ，ブラウザの環境で実行される．これにより，クライアント側でアンケート内容の暗号化や秘密鍵の生成を行うことができ，それらの情報を集計サーバ側に秘匿することが可能となる．

5. 実　　装

5.1 システム概要

本システムは鍵生成フェーズ，回答フェーズ，復号フェーズの3つから成る．各フェーズの概要は以下のとおりである．

- 鍵生成フェーズ

プライバシ管理者はパスワードを入力することで n の元となる素数 p, q を生成し，公開鍵 $n = pq$ を生成する．次に，n を用いて公開鍵 g を生成する．作成した2つの公開鍵 n, g のデータを集計サーバに送り，集計サーバは公開鍵をデータベースに保存する．また，最後にプライバシ管理者は p, q を破棄する．これによりプライバシ管理者もデータとして秘密鍵を保持しないため，セキュリティコストを下げることができる．

- 回答フェーズ

回答者はアンケートの回答を行い，公開鍵 (p, q) を用いてアンケート内容の暗号化を行う．暗号化された回答データは集計サーバに送信される．

集計サーバは受信した値をユーザごとに暗号化された状態でデータベースに保存する．

- 復号フェーズ

回答期間が終了した後に，プライバシ管理者は鍵生成時のパスワードを再入力し，鍵生成フェーズと同じ p, q を生成する．この2つより秘密鍵 $\lambda(n)$ を生成する．一方，集計サーバは準同型性を用いて集計結果の暗号文を作成し，それをプライバシ管理者に送信する．

プライバシ管理者は受け取った暗号文を先ほど生成した秘密鍵 $\lambda(n)$ により復号し，アンケートの結果を得る．また，この結果を集計サーバに送信し，NOBASU より公開する．

図2にシステムの概要を示す．回答者とプライバシ管理者はそれぞれのフェーズ用のアプレットにより各自の処理を行う．また，集計サーバ側では各フェーズの機能ごとにサーブレットを用意して処理を行う．

5.2 提案システムのデータベース構成

本章では，提案システムで利用する MySQL 上の各データベースのテーブルの構成について述べる．

- ユーザ情報テーブル

NOBASU におけるユーザの基本情報を格納するテーブルである．このテーブルは NOBASU で既に用意されている．

データ項目:

- ユーザ ID
- ユーザ名
- パスワード
- メールアドレス
- ロール

- ユーザ授業テーブル

ユーザが受講している授業名を格納するテーブルである．このテーブルも NOBASU で既に用意されている．

データ項目:

- ユーザ ID
- ユーザ名
- 受講授業

- アンケート情報テーブル

本システムを利用してアンケートの回答を行う際に，教員が予め登録する必要がある，アンケートの情報を格納するテーブルである．本テーブルは，授業ごとに独立している．

データ項目:

- アンケート番号
- アンケートタイトル
- 回答期限
- 暗号化に使用する公開鍵 n, g

- アンケート回答テーブル

暗号化されたアンケートの回答内容，回答日時を格納するテーブルである．本テーブルは，授業ごと，アンケートごとに独立している．

データ項目:

- ユーザ ID
- ユーザ名
- 暗号化されたアンケートの回答内容
- 回答日

5.3 実装システム

本システムは，NOBASU に従来から実装してあるユーザ認証機能やデータベースの一部を用いる．また，集計サーバである NOBASU では，従来サーバ側ですべての処理が行われていたが，本システムでは暗号化の際には回答者側で暗号化の処理を行う必要がある．このため，Java サーブレット/JSP だけでなく Java アプレットを併用することでこれを解決する．本システムには鍵生成，回答，復号の各フェーズごとにアプレットを1つずつ用意し，集計サーバ側では鍵生成フェーズ，回答フェーズの設問および公開鍵転送，同フェーズの回答データ保存，復号フェーズのそれぞれに対してサーブレットを用意した．これらの暗号化および復号の処理では，Java の BigInteger オ

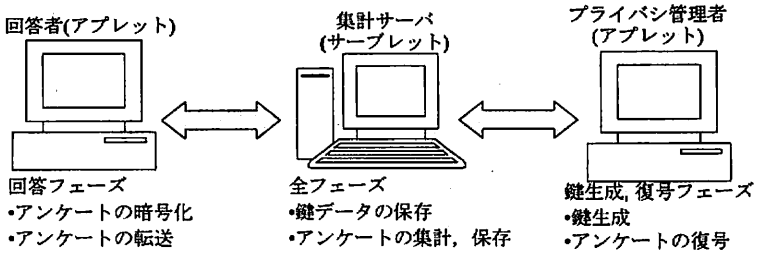

図 2　システムの概要

表 1　集計サーバの実行環境

CPU	AMD Athlon XP 1900+　(1.6GHz)
Memory	1GB
servlet	Tomcat5.0.28

ブジェクトにより多倍長の演算を行う．

本システムは J2SDK1.5.0_06 を用いて開発を行った．また，集計サーバの実行環境を表 1 にまとめる．

5.4　各フェーズの詳細

各フェーズを行う際に，そのフェーズを行うプライバシ管理者または回答者は，始めに NOBASU に元々実装されているパスワードベースのユーザ認証機能により正当な NOBASU 利用者であることを証明する．このユーザ認証機能は SSL 通信でベーシック認証を用いて行われている．

5.4.1　鍵生成フェーズ

まず，鍵生成を行うプライバシ管理者は，NOBASU においてユーザ認証を行いログインする．

次に NOBASU のメニューから「アンケート登録」を選択し，鍵生成用のアプレットを起動する．まずサーブレットから担当授業リストを受け取る．その後，アンケートを生成する授業名を選択し，アンケートの回数，パスワードをそれぞれ入力する．パスワードは任意の文字列とし，パスワードからハッシュ関数を用いて長さが $l_n/2$ の p, q をそれぞれ一意に生成する．この際，それぞれパスワードの後に異なる特定の文字列を付加し，それをハッシュ関数 SHA-1 により 160bit に変換したものを 3 つずつ用意し，それを繋げて 480bit に伸長する．これを偶数の場合，1 を加えることで奇数にし，そして 2 ずつ加えながら素数判定を行う．以上の処理を 2 回行い，素数 p, q を生成する．

次に，$n = pq$ として法 n を生成する．この際，$l_n = 960$ となる．さらに位数が n の倍数であるような底 $g \in_R Z^*_{n^2}$ を選ぶ．最後に公開鍵 (n, g) を集計サーバに送信し，集計サーバはこの公開鍵をデータベースに保存する．

5.4.2　回答フェーズ

回答者はまず，NOBASU のログイン画面より認証を行う．ログイン後，回答する権利のあるアンケートがあればそのアンケートの回答用アプレットへ移る．

アプレットの起動直後，鍵生成フェーズで作成された公開鍵などをサーブレットから受け取る．アンケートは 5 つの選択肢の中から 1 つを選ぶ 1-*out-of*-5 の形とし，ラジオボタンで選択するようにする．

アンケートの回答が終了すると，回答に対して暗号化を行う．暗号文は第 3 章の Paillier 暗号に従い，

$$E(m) = g^m r^n \bmod n^2$$

となり，各パラメータ g, m, r, n も第 3 章に基づく．

ここでメッセージ m は 3.2 節で既述したように選択した候補 i に対して値が $(T+1)^{i-1}$ となるようにし，それを各設問の選択した選択肢ごとに計算し和をとる．このようにして生成した 1 つのメッセージを暗号化し，それを回答データとして集計サーバに送信する．

5.4.3　復号フェーズ

鍵生成フェーズと同様に復号を行うプライバシ管理者は NOBASU においてユーザ認証を行いログインする．

プライバシ管理者は鍵生成時のパスワードを再入力し，復号用アプレットから復号用サーブレットに回答の集計データの送信要求を行う．これを受けてサーブレットはデータベースに格納された暗号文の集計を行う．集計は 3 章で述べた暗号プロトコルに従い，それぞれの選択肢ごとに回答された暗号データを掛け合わせることにより，暗号化された状態で集計結果を得る．これと公開鍵 g をアプレットに送信する．

アプレットでは，先ほど入力されたパスワードから，p, q を回答フェーズと同様の処理により生成し，秘密鍵 $\lambda(n) = (p-1)(q-1)$ を計算し，これにより受け取った集計データを復号する．

この回答結果は学生側にも公開できるよう集計サーバに送り，結果を NOBASU より公開する．

5.5　システムの安全性について

（1）　不正回答防止

回答者による不正回答としては，1 人の回答者が 2 回以上回答する多重回答と，回答権のない回答者が回答を行う非権利者による回答の 2 つが考えられる．

まず，多重回答について考察する．回答フェーズにおいて集計サーバは受信した値をユーザごとに暗号化された状態でデータベースに保存する．ユーザごとにデータを格納することにより，同じ回答者から再回答されたデータは訂正された回答内容として上書きされる．これにより，同じ回答者からの多重回答を防止している．

次に非権利者による回答について考察する．各アンケート回

表 2 演算速度比較の実行環境

CPU	AMD Sempron(tm) Processor 2600+ (1.6GHz)
Memory	768MB

答時には，NOBASU の認証機能によりどの NOBASU 利用者であるか確認されている．そして，その利用者が回答できるアンケートのみ回答可能である．このため，他のユーザのパスワードを知らない限り，非権利者はアンケートの回答を行えない．

（2） 集計サーバのデータの秘匿性

集計サーバでは，各回答者のアンケート内容は暗号化されたままアンケート回答テーブルに保存されている．このため，外部からの攻撃や NOBASU 管理者などの内部からの不正を防止することができる．

（3） プライバシ管理者のデータの秘匿性

プライバシ管理者は，集計サーバから暗号化された集計データを受け取る．このため「誰がどの回答を行ったか」は特定できない．

（4） 回答者の識別

集計サーバは，アンケート回答テーブルに各回答者ごとの回答日時が保存している．これを確認することで回答を行った人と行っていない人を区別することができる．

6. 実験および評価

本章では，2 つの実験を実施しシステムの評価を行う．まず，Paillier 暗号と ElGamal 暗号のそれぞれをアンケートシステムに用いた場合の演算処理速度について計測を行う．さらに，実際に授業評価アンケートとして本システムを利用し，システムのユーザビリティおよびスケーラビリティについてのアンケートを実施し，その評価を行う．

6.1 実 験 1

まず，実験 1 では同一条件下で，アンケートに Paillier 暗号を用いた場合と ElGamal 暗号を用いた場合において演算速度を計測した．この実験の実行環境を表 2 に示す．選択肢数 $N = 5$ で固定し，設問数 L を 1 から 12 まで変化させて，それぞれの演算時間を計測した．ここでは，ElGamal 暗号の場合，1 つの選択肢を 1 つの暗号文に変換する場合を計測している．

その結果を図 3 に示す．ElGamal 暗号では設問が 1 つ増えるごとに暗号文が 5 個 (データとしては 10 個) 増加するため，1 つの設問の増加につき演算時間としては平均 88msec の増加となる．これに対し，Paillier 暗号では設問が増加しても暗号文の数自体は 1 つのままで変わらないが，メッセージ m の長さが増加するため，1 つの設問の増加につき平均 8msec の増加となった．ElGamal 暗号では生成元を複数個用意して暗号文の数を減らすことが考えられるが復号の際のオーバヘッドが大きくなってしまう．

以上のことから Paillier 暗号の使用は有効と考える．

6.2 実 験 2

次に実験 2 として，本システムの運用を想定し，岡山大学工学部通信ネットワーク工学科の 2 年次生 (41 人) に対して本システムを利用してもらい，一斉にアンケートの送信を行った．その後で使用感などについてのアンケートを行い，その回答を得た．

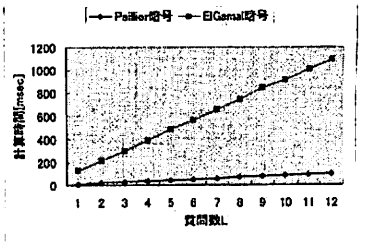

図 3 設問数による演算時間の比較

使用感に関するアンケートの項目は以下のとおりである．

（1） アプレットの起動時間 (5 段階評価)

（2） 「送信」ボタンを押してからの待ち時間 (5 段階評価)

（3） アンケートフォームの体裁 (5 段階評価)

（4） システムの利便性 (5 段階評価)

（5） 何か気づいた点 (自由記述)

また，図 4 に実際のアンケートフォームを示す．

まず項目 1 と 2 の速度に関するアンケートの結果を表 3 に示す．表 3 よりアプレットの起動時間も「送信」ボタンを押してからの待ち時間に関しても，回答者が気にならない程度であることが分かった．以上より，現在のシステムでは回答者に対してそれほど大きな負担にはならないことが分かった．

次に，アンケートフォームの体裁に関するアンケート結果を表 4 に示す．表 4 より，体裁に関しては表示部分が OS やブラウザに依存してしまうため，場合によっては見づらいという人もいた．また，チェックボックスの位置が設問ごとにばらついているために見づらいという意見もあった．OS やブラウザに依存して表示されることを考慮して，ユーザインターフェースの改善は今後必要であると考えられる．

最後に，本システムを通しての利便性に関するアンケート結果を表 5 に示す．表 5 より，アンケートシステムを通してのユーザビリティは低くはないと考えられる．しかし，先ほども述べた体裁のばらつきがあること，送信されたかどうか分かりにくい，送信時に確認ダイアログが出てほしい，などといったユーザインターフェースに関する意見が多く寄せられていることから，その改善が今後の課題である．

7. むすび

本論文では，集計サーバとプライバシ管理者が異なる場合における授業評価アンケートシステムを Paillier 暗号を用いて教育支援システム NOBASU の新機能として実装し，その評価を行った．設問の数に対し比例的に演算時間の増える ElGamal 暗号に比べ，Paillier 暗号では設問数が増えても演算時間を抑えることができた．

また，アンケートの評価結果より，送信時のレスポンスなどといった速度に関する項目は概ね良好な回答が得られたが，体

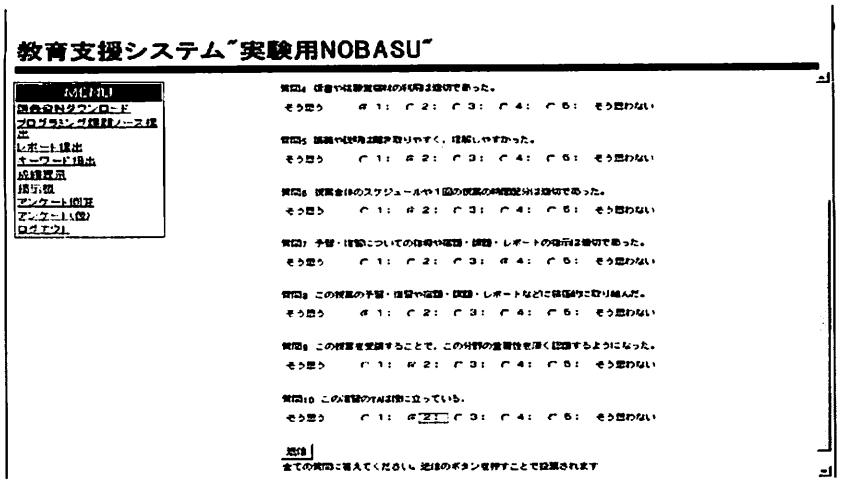

図 4 アンケートフォーム

表 3 速度に関するアンケート結果

	遅い	少し遅い	普通	少し速い	速い
アプレットの起動時間	0	4	25	3	9
送信時間	1	4	20	5	11

表 4 体裁に関するアンケート結果

	非常に見づらい	見づらい	普通	見やすい	非常に見やすい
アンケートの体裁	0	5	16	15	5

表 5 利便性に関するアンケート結果

	使いづらい	少し使いづらい	普通	少し使いやすい	使いやすい
システムの利便性	0	5	13	10	13

裁などのユーザインターフェース部分に関しては改善の余地があることが分かった.

今後の課題として, まず前述したシステムのユーザインターフェースの向上が挙げられる. また, 集計フェーズに関するユーザビリティの評価を行う必要もある.

さらに, ゼロ知識証明技術を導入することで, 暗号化されたアンケートの回答の正当性を検証することも挙げられる. これは集計サーバに届いたアンケート内容は暗号化されているため, 本当に正しいデータかどうかわからず, 1 人の回答者が 1 回の回答で, 不正に何票分ものデータを送ったり, 暗号文として正しくないデータを送信することで集計結果を正しく復号できなくなる恐れがあるためである. Paillier 暗号に対するゼロ知識証明は, 文献 [6] で本研究グループが提案している方法により, 効率的に実現可能であると考える.

文 献

[1] 北川 隆, 岡 博文, 楫 勇一 : "大学における講義評価アンケートプロトコルとその試作", 情処論, Vol.44, No.9, pp.2353-2363(2003).

[2] 中里 純二, 藤本 賢司, 菊池 浩明 : "個人情報を漏洩する Web アンケートのセキュリティ強化", 情処論, Vol.46, No.8, pp.2068-2077(2005).

[3] P.Paillier : "Public-Key Cryptosystems Based on Composite Degree Residuosity Classes", Proc. EUROCRYPT'99, LNCS 1592, pp.223-238, 1999.

[4] 高橋 紀行, 舩曳 信生, 中西 透 : "講義・演習を対象とした WEB ベースの教育支援システム", 新学技報, Vol.ET2004-44, pp.45-50, 2004

[5] Cramer,R., Gennaro,R. and Schoenmakers,B. : "A Secure and Optimally Efficient Multiauthority Election Scheme", Advances in Cryptology EUROCRYPT'97, LNCS 1233, pp.103-118(1997).

[6] 中武 真治, 中西 透, 舩曳 信生 : "投票内容の正当性証明に要するコスト軽減した電子投票プロトコル", CSS 2005 論文集, pp.517-522,2005.

[7] J.Camenisch and J.Groth : "Group Signatures: Better Efficiency and New Theoretical Aspects", Proc. SCN 2004, LNCS 3352, pp.120-133, Springer, 2005.