УДК 004.056(075.8) DOI:10.31854/1813-324X-2021-7-2-102-109

Анализ гомоморфных криптосистем Бенало и Пэйе для построения системы электронного голосования

В.Д. Салман[1]*

[1]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, Санкт-Петербург, 193232, Российская Федерация
*Адрес для переписки: wasan.salman@mail.ru

Информация о статье
Поступила в редакцию 16.04.2021
Принята к публикации 28.05.2021

Ссылка для цитирования: Салман В.Д. Анализ гомоморфных криптосистем Бенало и Пэйе для построения системы электронного голосования // Труды учебных заведений связи. 2021. Т. 7. № 2. С. 102–109. DOI:10.31854/1813-324X-2021-7-2-102-109

Аннотация: *Проведен анализ двух криптографических алгоритмов (Пэйе и Бенало) с целью их применения для построения систем электронного голосования. Дано описание каждого алгоритма и их гомоморфных свойств. Сформулированы требования к системам электронного голосования и приведено их построение при использовании этих криптоалгоритмов. Сравнительный анализ систем голосования на основе схем Пэйе и Бенало показал, что схема Пэйе является лучшим и более простым методом построения безопасных электронных систем голосования, в то время как схема Бенало является более сложной.*

Ключевые слова: *гомоморфное шифрование, криптосистема Пэйе, криптосистема Бенало, электронная система голосования.*

Введение

Под гомоморфным шифрованием понимается криптографический примитив, представляющий собой функцию шифрования, удовлетворяющую дополнительному требованию гомоморфности относительно каких-либо алгебраических операций над открытыми сообщениями [1]. Гомоморфное шифрование используется во многих современных коммуникационных архитектурах. Они наиболее перспективны для построения безопасных систем электронного голосования [2]. Электронное голосование (ЭГ) – термин, определяющий различные виды голосования, охватывающий как электронные средства голосования, так и электронные средства подсчета голосов [2]. Технология электронного голосования позволяет ускорить процесс подсчета голосов, а также позволяет голосовать людям с ограниченными возможностями [3]. Важность применения гомоморфного шифрования заключается в том, что оно позволяет безопасно передавать, хранить и, главное, обрабатывать данные в зашифрованном виде без ущерба для конфиденциальности информации.

Первые гомоморфные системы были предложены Бенало в 1996 г. [4] и Пэйе в 1999 г. [5]. Эти схемы практичны, надежны и безопасны. Эти криптосистемы основаны на обычной модульной арифметике. В работе [6] представлен обзор гомоморфных методов шифрования с учетом времени шифрования, памяти и безопасности. Обобщены многие типы гомоморфных схем, в том числе Пэйе, Бенало и др., по их параметрам и свойствам. Вывод этой работы состоит в том, что эти схемы не всегда подходят для любого применения и необходимо учитывать их характеристики в каждом конкретном случае. В работе [7] анализируются частично и полностью гомоморфные криптосистемы: RSA, Пэйе и Эль-Гамаля. Подчеркивается преимущество гомоморфного шифрования, состоящее в возможности сохранения конфиденциальности при работе с криптограммами, а также отмечаются их недостатки: сложность, увеличенные размеры криптограмм и то, что некоторые из этих систем уязвимы для вредоносных программ. В работе [8] сравниваются гомоморфные схемы шифрования, основанные на схемах Голдвассера – Микали, Бенало, Наккаша – Штерна, Эль-Гамаля и Пэйе. Сравнение проведено по времени генерации ключа, времени шифрования, времени дешифрования и общему размеру криптограммы. Сравнение осуществлялось на основе шифрования 100 случайных чисел. Результаты показали, что схема Пэйе дает наиболее эффективные результаты среди всех алгоритмов.

Протокол Гелиос (Helios) в [9] предложен для построения системы голосования членов студенческого совета и для небольших выборов. Основывается на подходе Бенало к голосованию. Helios – это первая доступная реализация системы веб-голосования с открытым аудитом. В ней используется неинтерактивное доказательство нулевого знания для подтверждения голосования. Helios – это веб-приложение, написанное на языке программирования Python, работающее внутри сервера приложений CherryPy 3.0 с веб-сервером Lighttpd. Все данные хранятся в базе данных PostgreSQL. Недостатки этого протокола: требуется Firefox 2 (или более поздняя версия), а также сложность пользовательского интерфейса.

В работе [10] была реализована и протестирована двойная система голосования, основанная на традиционном и электронном голосовании, на двух выборах в студенческий совет с участием более 2000 избирателей и на выборах лидера политической партии в 2012 г. В этой работе использовалась криптосистема Бенало. Эта система удовлетворяет следующим требованиям безопасности: конфиденциальность, целостность, неразличимость, любой избиратель может проверить, что его голос был правильно записан и включен в подсчет, а также любой может проверить, что все записанные голоса правильно подсчитаны. Недостатком данной работы является частично используемая бумажная система.

В работах [11–15] предложена система электронного голосования, основанная на гомоморфном шифровании с использованием криптосистемы Пэйе и других методов. Свойство гомоморфного шифрования позволяет добавлять голоса в зашифрованном виде. Эта система удовлетворяет таким требованиям безопасности, как приемлемость, конфиденциальность, уникальность, целостность и точность.

В данной работе проведен анализ криптосистем Бенало и Пэйе, так как они являются наиболее часто используемыми гомоморфными криптосистемами и имеют высокие гарантии безопасности. Основным результатом данной работы является анализ и сравнение двух криптосистем применительно к построению системы электронного голосования.

Анализ принципов построения криптосистем Бенало и Пэйе

Криптосистема Бенало

В 1994 г. Д. Бенало [4], предложил гомоморфную схему шифрования, которая является вероятностным асимметричным алгоритмом для криптографии с открытым ключом.

Рассмотрим пошагово и поэтапно основные преобразования, характеризующие эту криптосистему: генерирование ключей, шифрование, расшифрование.

Генерирование ключей

Шаг 1. Выбираются два больших простых числа p, q и размер блока сообщения r (r-максимальное значение сообщения, представленного в виде числа). Число r выбирается таким образом, чтобы выполнялись условия:

$$(p-1)\bmod r = 0,$$
$$\gcd\left(r, \left(\frac{p-1}{r}\right)\right) = 1,\ \gcd(r, q-1) = 1.$$

Шаг 2. Вычисляется $n = pq$.

Шаг 3. Выбирается $y \in Z_n^*$, при $y^{\varphi/r} \neq 1 \bmod n$, $y^{\varphi/r} \neq 1$,где $\varphi(n) = (p-1)(q-1)$ – функция Эйлера от n.

Шаг 4. Вычисляется $x = y^{\varphi/r} \bmod n$.

Полагаем, что числа (y, n) являются открытым ключом, а (φ, x) – закрытым.

Шифрование

Если сообщение $m \in Z_r$, то шифрование производится путем выбора произвольного числа $u \in Z_n^*$ и вычисления криптограммы $c = y^m u^r \bmod n$.

Расшифрование

Расшифрование полученной криптограммы $c \in Z_n^*$ проходит в два этапа:

– вычисление $a = c^{\varphi/r} \bmod n$;

– подбор такого числа m, чтобы $m = \log_x a$,

Действительно, для любых $m \in Z_r, u \in Z_n^*$ можно записать выражение:

$$a = (c)^{\varphi/r} \equiv (y^m u^r)^{\varphi/r} \equiv (y^m)^{\varphi/r}(u^r)^{\varphi/r} \equiv$$
$$\equiv \left(y^{\varphi/r}\right)^m (u)^{\varphi} \equiv (x)^m (u)^0 \equiv x^m \bmod n.$$

Криптосистема Бенало гомоморфна относительно операции сложения открытых тестов [4]:

$$\varepsilon(x_1) \times \varepsilon(x_2) = (g^{x_1} u_1^r)(g^{x_2} u_2^r) = g^{x_1+x_2}(u_1 u_2)^r$$
$$= \varepsilon(x_1 + x_2) \bmod r,$$

где $\varepsilon(x)$ – функцией шифрования от сообщения x.

Рассмотрим пример построения схемы Бенало на основе вышеприведенных соотношений. (В приведенных ниже примерах случайные числа будем получать от датчика чисел в программе Mathcad. В реальных системах предполагается использование физического датчика).

Генерирование ключей

Шаг 1. Выберем размер блока сообщения $r < 100$ и два больших простых числа $p = 397, q = 191$.

Если $r = 99$, тогда выполняются условия:

$(397-1) \bmod 99 = 0$, $\gcd(99, \left(\frac{397-1}{99}\right) = 1$,

$\gcd(99, 191-1) = 1$.

Шаг 2. Вычислим $n = 397 \times 191 = 75827$, отсюда $\varphi(n) = 75240$.

Шаг 3. Выберем случайное целое число $y = 13213$, соответствующее требованию $y \in Z_n$ и проверим условие $y^{\varphi/r} \neq 1 \bmod n$.

Шаг 4. Определим x по выражению:

$$x = y^{\varphi/r} \bmod n = 13213^{75240/99} \bmod 75827 = 24640.$$

Таким образом, найден открытый (13213, 75827) и закрытый (75240,24640) ключ.

Шифрование

Пусть $m \in Z_r$, $m = 78$. С целью шифрования сообщения выберем произвольное $u \in Z_n^*$: $u = 66183$. Тогда $c = 13213^{78} 66183^{99} \bmod 75827 = 47158$.

Расшифрование

Расшифруем криптограмму $c \in Z_n^*$:

– $a = 67158^{75240/99} \bmod 75827 = 47178$,

– построим таблицу значений $x^m = a \bmod n$ для m = 0, 1, 2, …, 77, 78, …, 98 и проверим выполнение условия ($x^m = a \bmod n$?):

$$m = 0,\ 24640^0 \bmod 75827 = 1 \neq a$$
$$m = 1,\ 24640^1 \bmod 75827 = 24640 \neq a$$
$$m = 2, 24640^2 \bmod 75827 = 58638 \neq a$$
$$m = 78, 24640^{78} \bmod 75827 = 47178 = a$$

Проверка показала, что восстановлен открытый текст m = 78.

Криптосистема Пэйе

Криптосистема Пэйе [5], является вероятностным асимметричным алгоритмом для криптографии с открытым ключом. Она основана на задаче вычисления n-го класса вычетов, которая считается трудновыполнимой. Основные преобразования, характеризующие эту криптосистему, состоят в следующем.

Генерирование ключей

Шаг 1. Выбираются два больших простых числа p и q, удовлетворяющие условию:

$$\gcd(pq, (p-1)(q-1)) = 1.$$

Шаг 2. Вычисляются числа n и λ по выражениям:

$$n = pq, \lambda = \mathrm{lcm}(p-1, q-1),$$

где $\lambda(n)$ – функция Кармайкла от n; $\lambda = \frac{(p-1)(q-1)}{\gcd(p-1,q-1)}$; lcm – наименьшее общее кратное.

Шаг 3. Выбирается $y \in Z_{n^2}^*$.

Шаг 4. Вычисляется $x = \left(L\left(y^\lambda \bmod n^2\right)\right)^{-1} \bmod n$, где $L(u) = \left[\frac{u-1}{n}\right]$; а выражение в скобках определяется, как – наибольшее целое s число, удовлетворяющее условию $u - 1 \geq s \cdot n$.

После вычислений, полагаем: (y, n) – открытый ключ, (λ, x) – закрытый ключ.

Шифрование

Сообщение $m \in Z_n$ шифруется посредством выполнения двух действий:

– выбора произвольного числа $u \in Z_n^*$;

– вычисления криптограммы $c = y^m u^r \bmod n^2$.

Расшифрование

Полученная криптограмма $c \in Z_{n^2}^*$ расшифровывается путем вычисления по формуле:

$$m = L\left(c^\lambda \bmod n^2\right) \times x \bmod n.$$

Криптосистеме Пэйе присущи гомоморфные свойства [5], а именно:

– произведение двух шифротекстов будет расшифровано как сумма соответствующих им открытых текстов:

$$D\left(E(m_1, r_1) \cdot E(m_2, r_2)\right) \bmod n^2 = m_1 + m_2 \bmod n;$$

– шифротекст, возведенный в степень, равную другому шифротексту, будет расшифрован как произведение двух открытых текстов:

$$D\left(E(m_1, r_1)^{(m_2)} \bmod n^2\right) = m_1 m_2 \bmod n.$$

Рассмотрим пример построения схемы Пэйе.

Генерирование ключей:

Шаг 1. Выберем два простых числа p = 7, q = 5 и проверим соответствие заданному условию:

$$\gcd\left(pq, (p-1)(q-1)\right) = 1,$$

Шаг 2. Определим, что $n = pq = 35, n^2 = 1225$ и $\lambda = \mathrm{lcm}(6,4) = 12$.

Шаг 3. Выберем случайное целое число $y = 3$, соответствующее требованию $y \in Z_{n^2}^*$.

Шаг 4. Определим, что $x = \left(L\left(y^\lambda \bmod n^2\right)\right)^{-1} \times$ $\times \bmod n = 29$.

Таким образом, найден открытый (3, 35) и закрытый (12, 29) ключи.

Шифрование

Пусть $m \in Z_n, m = 8$. Выберем произвольное $u \in Z_n^*$, $u = 9$. Тогда $c = 3^8 \times 9^{35} \bmod 1225 = 939$.

Расшифрование

Расшифровывание криптограммы $c \in Z_{n^2}^*$ выполняем по формуле:

$$m = L(939^{12} \bmod 1225) \times 29 \bmod 35 = 8,$$

т. е. открытый текст m = 8 восстановлен правильно.

Сравнение криптосистем Пэйе и Бенало

Сравнение криптосистем Пэйе и Бенало по некоторым свойствам приведено в таблице 1. Из таблицы видно, что обе криптосистемы схожи: имеют примерно одинаковый размер ключей и обладают гомоморфными свойствами. Однако в практическом плане система Пэйе является более простой, поскольку при дешифровании криптограм-

мы не нужно решать задачу дискретного логарифмирования для чисел относительно небольшого размера.

ТАБЛИЦА 1. Сравнение криптосистем Пэйе и Бенало

TABLE 1. Comparison of Paillier and Benaloh Cryptosystem

Свойства	Схема	
	Пэйе	Бенало
Стойкость	Основана на задаче факторизации больших чисел	Основана на трудно-решаемой задаче о вычетах высокой степени
Удобство использования	Особенностью алгоритма является простота понимания и использования	
Время выполнения операций	Для дешифрования работает значительно быстрее	Операция дешифрования требует решения задачи дискретного логарифмирования для чисел относительно небольшого размера, что увеличивает время выполнения операции
Недостатки	Увеличение размера шифротекста по отношению к входному тексту	Является более сложной и трудоемкой для вычисления
Сходство	Используют шифрование с открытым ключом Обладают свойством гомоморфизма	

Электронная система голосования

Это удаленная система, использующая Интернет, мобильные компьютеры, смартфоны для того, чтобы дать возможность избирателям голосовать на выборах дистанционно.

Система электронного голосования состоит из следующих элементов:

1) *избиратели* – физические лица, имеющие законное право голоса;

2) *кандидаты* – лица, которые стремятся избраться на должность и имеют законное право на нее (кандидат избирается, если он был выбран по наибольшему числу отданных за него голосов);

3) *сервер* выполняет функцию перемножения криптограмм, полученных от избирателей и хранит зашифрованные голоса (рекомендуется использовать сервер с большой памятью и высокоскоростным процессором, поскольку сервер должен обрабатывать большое количество потоков для обслуживания большого количества избирателей за один раз);

4) *избирательная комиссия* (ИК) определяет, что избиратель имеет право на получение права голоса, гарантирует то, что избиратель голосует только один раз на данных выборах, осуществляет подсчет голосов избирателей и объявляет результаты выборов;

5) *наблюдатели* следят за соблюдением закона при проведении голосования и подсчете голосов (в случае выявления нарушений наблюдатель должен либо постараться их пресечь, либо зафиксировать).

Для построения безопасной системы электронного голосования необходимо выполнить аутентификацию, а также соблюдать тайну голосования, целостность, точность, анонимность, уникальность, подтверждение голоса [13, 16–18].

Схема голосования при использовании системы с аддитивным гомоморфизмом, описанная в [19], в общем виде представляет из себя последовательности действий избирателей и избирательной комиссии, а также операций сервера. Избиратели проходят авторизацию в избирательной комиссии, получают бюллетени и ключ (ключи), зашифровывают свои бюллетени публичным ключом избирательной комиссии, после чего отправляют свои зашифрованные бюллетени на сервер. Сервер обрабатывает все зашифрованные бюллетени и отправляет получившийся результат в ИК. Избирательная комиссия с помощью секретного ключа расшифровывает криптограмму, содержащую сумму бюллетеней и объявляет победителя выборов. На рисунке 1 показана простая модель системы электронного голосования.

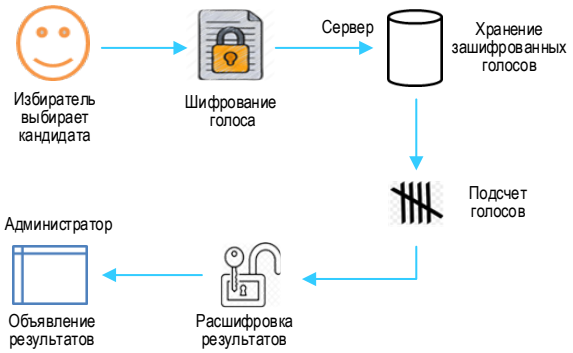

Рис. 1. Модель системы электронного голосования

Fig. 1. Electronic Voting System Model

Рассмотрим, как может быть построена избирательная система на криптосхемах Пэйе и Бенало.

Примеры построения систем электронного голосования на криптосхемах Бенало и Пэйе

Гомоморфная система голосования на основе схемы Пэйе

Введем обозначения для описания системы электронного голосования:

N_v – количество избирателей;

N_c – количество кандидатов;

b – основание системы счисления, которое должно выбираться из условия: $b > N_v$, (т. е. должно быть больше, чем число избирателей).

Предположим, что избираются 2 члена для союза студентов из пяти кандидатов. Выбор одного кандидата или оставление бюллетеня пустым также возможен. Пусть $N_v = 9$, $N_c = 5$, $b = 10$, $b > N_v$. Результаты голосования избирателей представлены в таблице 2.

ТАБЛИЦА 2. Результаты голосования избирателей

TABLE 2. Results of Voter's Choice

Избиратели	Кандидаты					Шифрование сообщения
	C_1 10^0	C_2 10^1	C_3 10^2	C_4 10^3	C_5 10^4	
V_1		•				$m = 10^1 = 10$
V_2			•		•	$m = 10^2 + 10^4 = 10100$
V_3						$m = 0$
V_4				•		$m = 10^3 = 1000$
V_5	•			•		$m = 10^0 + 10^3 = 1001$
V_6		•		•		$m = 10^1 + 10^3 = 1010$
V_7			•	•		$m = 10^2 + 10^3 = 1100$
V_8		•		•		$m = 10^1 + 10^3 = 1010$
V_9	•					$m = 10^0 = 1$
Итого:	2	3	2	5	1	

Каждому кандидату C_i присваивается идентификатор – число b^i, где i – номер кандидата в списке. В данном случае выбираем десятичную систему счисления $b = 10$.

Согласно правилу выборов (голосовать можно не более чем за двух кандидатов), максимальное сообщение о голосовании, которое может быть зашифровано избирателем $m_{\max} = 10^3 + 10^4 = 11000$. А максимально возможная сумма голосов всех избирателей $T_{\max}$ определяется как:

$$T_{\max} = N_v \times m_{\max} = 9 \times 11000 = 99000.$$

Поэтому выберем модуль $n > T_{\max}; n > 99000$.

Используя шаги, описанные в криптосистеме Пэйе для генерации ключей, получим ключи:

– для шифрования бюллетеней – открытый (6497955158, 126869);

– для расшифровки криптограммы избирательной комиссией - закрытый (31536, 53022).

Для шифрования сообщения $m \in Z_n$ каждый избиратель выбирает (программой) произвольное $u \in Z_n^*$ и создает криптограмму c.

Так, криптограмму первого избирателя можно записать в виде выражения:

$$c_i = 6497955158^{m_i} \times u_i^{126869} \bmod 16095743161.$$

Каждый избиратель отправляет криптограмму на сервер. Криптограммы всех избирателей сведены в таблицу 3.

Сервер вычисляет произведение полученных от избирателей криптограмм c_i и отправляет результат в избирательную комиссию:

$$\mathrm{c} = \prod_{i=1}^{N_v} c_i \bmod n^2 =$$

$$= (13039287935 \times 848742150 \times 7185465039 \times$$
$$\times 8093326 \times 722036441 \times 350667930 \times$$
$$\times 4980449314 \times 7412822644 \times$$
$$\times 3033281324) \bmod 16095743161 = 2747997353.$$

ТАБЛИЦА 3. Криптограммы избирателей в системе Пэйе

TABLE 3. Cryptograms of All Voters

Избиратель	Сообщение избирателя	Случайное число u_i	Криптограмма c_i
V_1	$m = 10^1 = 10$	35145	13039287935
V_2	$m = 10^2 + 10^4 = 10100$	74384	848742150
V_3	$m = 0$	96584	7185465039
V_4	$m = 10^3 = 1000$	10966	80933260
V_5	$m = 10^0 + 10^3 = 1001$	17953	722036441
V_6	$m = 10^1 + 10^3 = 1010$	7292	350667930
V_7	$m = 10^2 + 10^3 = 1100$	24819	4980449314
V_8	$m = 10^1 + 10^3 = 1010$	4955	7412822644
V_9	$m = 10^0 = 1$	118037	3033281324
Общая сумма голосов	15232		

Избирательная комиссия, используя закрытый ключ, проводит расшифрование криптограммы произведения:

$$T_{m\ \text{общ.}} = L\left(c^{\lambda} \bmod n^2\right) \times x \bmod n =$$
$$= \left(\frac{(2747997353^{31536} \bmod 16095743161) - 1}{126869}\right) \times$$
$$\times 53022 \bmod 126869 = 15232.$$

Далее расшифрованное сообщение записывается как сумма разрядов в десятичной системе счисления:

$$15232 = 1 \times 10^4 + 5 \times 10^3 + 2 \times 10^2 + 3 \times 10^1 + 2 \times 10^0.$$

Наибольшие значения имеют коэффициенты при степенях 10^3 и 10^1. Это означает, что победителями выборов являются кандидаты C_2 и C_4.

Гомоморфная система голосования на основе схемы Бенало

Условия голосования такие же, как при рассмотрении схемы Пэйе (N_v =9, N_c = 5). Выберем основание системы счисления $b = 10$, $b > N_v$.

Используя шаги, описанные в криптосистеме Бенало избирательная комиссия генерирует ключи:

– открытый - (62369, 20205597437);

– закрытый - (20205310716, 6922019540).

Открытый ключ передается всем избирателям, закрытый остается в ИК.

Выбрав произвольное $u \in Z_n^*$, избиратели шифруют сообщения $m \in Z_r$ и создают криптограммы.

В качестве примера криптограмма первого избирателя представлена в виде:

$$c_i = 15^{m_i} \times u_i^{62369} \bmod 20205597437.$$

Криптограммы всех избирателей приведены в таблице 4.

ТАБЛИЦА 4. Криптограммы избирателей в системе Бенало

TABLE 4. Cryptograms of All Voters

Избиратель	Сообщение избирателя	Случайное число u_i	Криптограмма c_i
V_1	$m = 10^1 = 10$	35145	183946066
V_2	$m = 10^2 + 10^4 = 10100$	74384	10050175893
V_3	$m = 0$	96584	16340434784
V_4	$m = 10^3 = 1000$	10966	8189135103
V_5	$m = 10^0 + 10^3 = 1001$	17953	4202784310
V_6	$m = 10^1 + 10^3 = 1010$	7292	14220855747
V_7	$m = 10^2 + 10^3 = 1100$	24819	7937933779
V_8	$m = 10^1 + 10^3 = 1010$	4955	15466873618
V_9	$m = 10^0 = 1$	118037	1049803439
Общая сумма голосов	15232		

Обработка криптограмм на сервере проводится аналогично обработке криптограмм на основе схемы Пэйе по выражению:

$$T = \prod_{i=1}^{N_v} c_i \bmod n^2 =$$

$$= (183946066 \times 10050175893 \times 1634043784 \times$$
$$\times 8189135103 \times 4202784310 \times 14220855747 \times$$
$$\times 7937933779 \times 15466873618 \times$$
$$\times 1049803439) \bmod 20205597437 = 4249761249.$$

С целью расшифровки криптограммы $c \in Z_n^*$ необходимо вычислить a_i:

$$a_i = 4249761249^{323964} \bmod 20205597437 =$$
$$= 2281530556,$$

после чего – для m = 0, 1, 2, 3, 4, ….., 15232, 15777, 16123, 20000, 24565, 30567 построить таблицу значений $x^m \bmod n$, и проверить выполнение сравнения ($x^m \bmod n = a$?).

Из таблицы следует, что восстановленный открытый текст m = 15232. Из анализа этого числа $15232 = 1 \times 10^4 + 5 \times 10^3 + 2 \times 10^2 + 3 \times 10^1 + 2 \times 10^0$. Наибольшие значения имеют коэффициенты при степенях 10^3 и 10^1, из этого следует, что кандидаты C_2 и C_4 являются победителями.

ТАБЛИЦА 5. Значение функции x^m для m = 1, ….., 15232

TABLE 5. The Values of the Function x^m для m = 1, ….., 15232

m	$x^m \bmod n$
0	$6922019540^0 \bmod 20205597437 = 1 \neq a$
1	$6922019540^1 \bmod 20205597437 = 6922019540 \neq a$
2	$6922019540^2 \bmod 20205597437 = 12864689861 \neq a$
3	$6922019540^3 \bmod 20205597437 = 17168902137 \neq a$
.....	.....
15232	$6922019540^{15232} \bmod 20205597437 = 2281530556 = a$

Из приведенных выше примеров, объясняющих применение этих схем при построении защищенной электронной системы голосования, можно сделать вывод, что эти схемы отвечают следующим требованиям:

– конфиденциальность обеспечивается за счет шифрования бюллетеня избирателем;

– анонимность обеспечивается тем, что при расшифровании известна сумма голосов, но не известен голос отдельного избирателя.

Заключение

В работе проведен анализ криптосистем Пэйе и Бенало и возможности их применения в системах электронного голосования. Между криптосистемами Пэйе и Бенало существует много общего: шифрование с открытым ключом, свойство гомоморфизма, конфиденциальность и анонимность голосования. Схема Бенало требует выполнения большего объема математических вычислений при дешифровании криптограммы, что в свою очередь занимает много времени, поэтому на практике распространение получила криптосистема Пэйе.

Дальнейшие исследования следует провести в направлении обеспечения требований безопасности, которые не в полном объеме выполняются в криптосистеме Пэйе: аутентификация избирателей, подтверждение поданного голоса, предотвращение раннего дешифрования криптограмм избирательной комиссией и решение вопросов масштабирования этой системы.

Список используемых источников

1. Коржик В.И, Яковлев В.А. Основы криптографии: учебное пособие. СПб.: ИЦ Интермедия, 2016. 296 с.
2. Jabbar I., Alsaad N.S. Design and Implementation of Secure Remote e-Voting System Using Homomorphic Encryption // International Journal of Network Security. 2017. Vol. 19. № 5. PP. 694–703. DOI:10.6633/IJNS.201709.19(5).06
3. Singh A., Ramakanth K., Cholli P., Nagaraj G. Empowering E-governance with E-voting // Indonesian Journal of Electrical Engineering and Computer Science. 2018. Vol.12. PP. 1081–1086. DOI:10.11591/ijeecs.v12.i3.pp1081-1086
4. Benaloh J.C. Verifiable Secret-Ballot Elections. PhD Thesis. Yale University, 1996. 134 p.
5. Gennaro R., Halevi S., Rabin T. Secure Hash-and-Sign Signatures without the Random Oracle // Proceedings of the International Conference on the Theory and Application of Cryptographic Techniques (EUROCRYPT 1999, Prague Czech Republic, 2–6 May 1999). Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, 1999. PP. 123–139. DOI:10.1007/3-540-48910-X_9
6. Fontaine C., Galand F. A Survey of Homomorphic Encryption for Nonspecialists // EURASIP Journal on Information Security. 2007. Vol. 2007. DOI:10.1155/2007/13801
7. Morris L. Analysis of Partially and Fully Homomorphic Encryption. Rochester: Rochester Institute of Technology, 2013.

8. Bhumika P., Dharmendra B. Homomorphic Encryption: Privacy Preserving Amicable E-voting System // International Journal of Computer Sciences and Engineering. 2019. Vol. 7. Iss. 12. PP. 46–50. DOI:10.26438/ijcse/v7i12.4650
9. Adida B. Helios: Web-based Open-Audit Voting // Proceedings of the 17th USENIX Security Symposium (USA, San Joce, 28 jule–1 august 2008). 2008. PP. 335–348.
10. Ben-Nun J., Fahri N., Llewellyn M., Riva B., Rosen A., Tashma A., Wikström D. A new implementation of a dual (paper and cryptographic) voting system // Proceedings of the 5th International Conference on Electronic Voting (EVOTE2012, Bregenz, Austria, 11–14 July 2012). 2012. PP. 315–329.
11. Hussien H., Aboelnaga H. Design of a secured e-voting system // International Conference on Computer Applications Technology (ICCAT, Tunisia, Sousse, 20–22 January 2013). IEEE, 2013. DOI:10.1109/ICCAT.2013.6521985
12. Sharma T. E-Voting using Homomorphic Encryption Scheme // International Journal of Computer Applications. 2016. Vol. 141. No. 13.
13. Huszti A. A homomorphic encryption-based secure electronic voting scheme // Publicationes Mathematicae. 2011. Vol. 79. PP. 479–496.
14. Varun M., Rahul S., Lawrence S., Kevin Zhu. Apollo. A secure, anonymized voting system using the Paillier cryptosystem // Project Report. 2016. PP. 1–12.
15. Ryan P.Y.A. Prêt à Voter with Paillier encryption // Mathematical and Computer Modelling. 2008. Vol. 48. Iss. 9-10. PP. 1646–1662. DOI:10.1016/j.mcm.2008.05.015
16. Htet N.O., Aye M. A. A Survey of Different Electronic Voting Systems // International Journal of Scientific Engineering and Technology Research. 2014. Vol. 3. PP. 3460–3464.
17. Qadah G.Z, Taha R. Electronic voting systems: Requirements, design, and implementation // Computer Standards and Interfaces. 2007. Vol. 29. Iss. 3. PP. 376–386. DOI:10.1016/j.csi.2006.06.001
18. Hao F., Ryan P.Y.A. Real-World Electronic Voting: Design, Analysis and Deployment. Boca Raton: Taylor & Francis Group, 2016. 461 p.
19. Toapanta S.M.T, Chalén L.J.Ch., Rojas J.G.O., Gallegos L.E.M. A Homomorphic Encryption Approach in a Voting System in a Distributed Architecture // IEEE International Conference on Power, Intelligent Computing and Systems (ICPICS, China, Shenyang, 28–30 July 2020). IEEE, 2020. PP. 206–210. DOI:10.1109/ICPICS50287.2020.9202073

* * *

Analysis of Homomorphic Cryptosystems of Benaloh and Paillier for the Construction of an Electronic Voting System

W. Salman[1]

[1]The Bonch-Bruevich Saint-Petersburg State University of Telecommunications,
St. Petersburg, 193232, Russian Federation

Article info
DOI:10.31854/1813-324X-2021-7-2-102-109
Received 16th April 2021
Accepted 28th May 2021

For citation: Salman W. Analysis of Homomorphic Cryptosystems of Benaloh and Paillier for the Construction of an Electronic Voting System. *Proc. of Telecom. Universities.* 2021;7(2):102–109. (in Russ.) DOI:10.31854/1813-324X-2021-7-2-102-109

Abstract: *The analysis of the performance of two cryptographic algorithms (Paillier and Benaloh), in order to apply them in the construction of electronic voting systems is carried out. A description of each system and their homomorphic properties is given. Electronic voting systems based on these schemes are described. The requirements for the voting system are formulated and a comparative analysis of the voting systems based on the schemes of Paillier and Benaloh is carried out. The analysis showed that the Paillier scheme is the best and simplest method for building secure electronic voting systems, while the Benaloh scheme is more complex and computationally more time-consuming.*

Keywords: *homomorphic encryption, Paillier cryptosystem, Benaloh cryptosystem, electronic voting system.*

References

1. Korzhik V.I., Yakovlev V.A. *Fundamentals of Cryptography*. St. Petersburg: IC Intermedia Publ.; 2016. 296 p. (in Russ.)
2. Jabbar I., Alsaad N.S. Design and Implementation of Secure Remote e-Voting System Using Homomorphic Encryption. *International Journal of Network Security*. 2017;19(5):694–703. DOI: 10.6633/IJNS.201709.19(5).06
3. Singh A., Ramakanth K., Cholli P., Nagaraj G. Empowering E-governance with E-voting. *Indonesian Journal of Electrical Engineering and Computer Science*. 2018;12:1081–1086. DOI:10.11591/ijeecs.v12.i3.pp1081-1086
4. Benaloh J.C. *Verifiable Secret-Ballot Elections*. PhD Thesis. Yale University; 1996. 134 p.
5. Gennaro R., Halevi S., Rabin T. Secure Hash-and-Sign Signatures without the Random Oracle. *Proceedings of the International Conference on the Theory and Application of Cryptographic Techniques, EUROCRYPT 1999, 2–6 May 1999, Prague, Czech Republic. Lecture Notes in Computer Science*. Berlin, Heidelberg: Springer; 1999. p.123–139. DOI:10.1007/3-540-48910-X_9
6. Fontaine C., Galand F. A Survey of Homomorphic Encryption for Nonspecialists. *EURASIP Journal on Information Security*. 2007;2007. DOI:10.1155/2007/13801
7. Morris L. *Analysis of Partially and Fully Homomorphic Encryption*. Rochester: Rochester Institute of Technology; 2013.
8. Bhumika P., Dharmendra B. Homomorphic Encryption: Privacy Preserving Amicable E-voting System. *International Journal of Computer Sciences and Engineering*. 2019;7(12):46–50. DOI:10.26438/ijcse/v7i12.4650
9. Adida B. Helios: Web-based Open-Audit Voting. *Proceedings of the 17th USENIX Security Symposium, 28 Jule–1 August 2008, USA, San Joce*. 2008. p.335–348.
10. Ben-Nun J., Fahri N., Llewellyn M., Riva B., Rosen A., Tashma A., Wikström D. A new implementation of a dual (paper and cryptographic) voting system. *Proceedings of the 5th International Conference on Electronic Voting, EVOTE2012, 11–14 July 2012, Bregenz, Austria*. 2012. p.315–329.
11. Hussien H., Aboelnaga H. Design of a secured e-voting system. *International Conference on Computer Applications Technology, ICCAT, 20–22 January 2013, Tunisia, Sousse*. IEEE; 2013. DOI:10.1109/ICCAT.2013.6521985
12. Sharma T. E-Voting using Homomorphic Encryption Scheme. *International Journal of Computer Applications*. 2016;141(13).
13. Huszti A. A homomorphic encryption-based secure electronic voting scheme. *Publicationes Mathematicae*. 2011;79:479–496.
14. Varun M., Rahul S., Lawrence S., Kevin Zhu. Apollo. A secure, anonymized voting system using the Paillier cryptosystem. *Project Report*. 2016:1–12.
15. Ryan P.Y.A. Prêt à Voter with Paillier encryption. *Mathematical and Computer Modelling*. 2008;48(9-10):1646–1662. DOI:10.1016/j.mcm.2008.05.015
16. Htet N.O., Aye M. A. A Survey of Different Electronic Voting Systems. *International Journal of Scientific Engineering and Technology Research*. 2014;3:3460–3464.
17. Qadah G.Z, Taha R. Electronic voting systems: Requirements, design, and implementation. *Computer Standards and Interfaces*. 2007;29(3):376–386. DOI:10.1016/j.csi.2006.06.001
18. Hao F., Ryan P.Y.A. *Real-World Electronic Voting: Design, Analysis and Deployment*. Boca Raton: Taylor & Francis Group; 2016. 461 p.
19. Toapanta S.M.T, Chalén L.J.Ch., Rojas J.G.O., Gallegos L.E.M. A Homomorphic Encryption Approach in a Voting System in a Distributed Architecture. *Proceedings of the International Conference on Power, Intelligent Computing and Systems, ICPICS, 28–30 July 2020, China, Shenyang*. IEEE; 2020. p.206–210. DOI:10.1109/ICPICS50287.2020.9202073

Сведения об авторе:

САЛМАН Васан Давуд

аспирант кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича,
wasan.salman@mail.ru
https://orcid.org/0000-0003-4454-7844