Математические структуры и моделирование
2023. № 4 (68). С. 111–119

УДК 004.056.5+004.42
DOI 10.24147/2222-8772.2023.4.111-119

МОДЕЛЬ АРХИТЕКТУРЫ ПРИЛОЖЕНИЯ, РЕАЛИЗУЮЩЕГО СХЕМУ ЭЛЕКТРОННОГО ТАЙНОГО ГОЛОСОВАНИЯ HE-SU

Д.Д. Лаврова[1]
студент, e-mail: drlvrv@gmail.com
Д.Н. Лавров[2]
канд. техн. наук, доцент, e-mail: dmitry.lavrov72@gmail.com

[1]Омский государственный университет им. Ф.М. Достоевского, Омск, Россия

[2]Нижневартовский государственный университет, Нижневартовск, Россия

Аннотация. В статье предлагается описание объектно-ориентированной модели приложения, реализующего схему электронного тайного голосования на основе схемы He-Su. Для реализации схемы нужно выбрать три базовых криптографических схемы: хэширования, симметричную криптосистему и асимметричную криптосистему с возможностью подписания вслепую. На основе анализа построенной модели предложена архитектура на основе абстракций, позволяющая легко выбирать и заменять одни базовые криптографические системы на другие, используемые в схеме.

Ключевые слова: электронное тайное голосование, слепая подпись, криптосистемы, криптографические протоколы, схема He-Su.

Введение

Процесс голосования, как правило, проводится вживую, так как на данный момент это самый проверенный способ сохранить в тайне личность голосующего. Однако для современного состояния мира (возникновение пандемий, с одной стороны, и цифровой трансформации экономики и других сфер жизни – с другой) удобнее, если это все проводилось бы в дистанционной форме или, как говорят, в электронной форме, подразумевая использование компьютерных сетей для проведения данной процедуры. При этом проблема обеспечения тайности (анонимности) голосования становиться ещё более актуальной.

В настоящее время известно несколько схем электронного тайного голосования.

1. Тривиальный алгоритм. Представляет собой переписку между избирательной комиссией и избирателями с использованием алгоритмов электронно-цифровой подписи. Требует полного доверия избирательной комиссии.

2. ANDOS (1987). Стойкость схемы усиливается за счёт замены заранее выбранного шифрования с секретным ключом на хеширование пользовательской функцией [1]. К недостаткам можно отнести то, что избирательная комиссия

может распределять по своему выбору голоса тех, кто заявил о своём намерении принять участие в голосовании, но так и не совершил свой выбор, а избиратель имеет соблазн продажи голосов, так как имеет возможность убедиться в результате сделки.

3. Протокол двух агенств (1991). Основная идея состоит в замене одного избирательного агентства двумя, чтобы они контролировали друг друга. К сожалению, избирательная комиссия может манипулировать голосованием: может специально не принимать сообщения от некоторых избирателей. Присутствует и проблема «мёртвых душ», когда проголосовать могут за тех, кто не пришёл на выборы.

4. Fujioka-Okamoto-Ohta (1992). Базируется на протоколе двух агентств и криптографической подписи вслепую. Частично решает проблему сговора регистратора и избирательной комиссии. Маскирующее преобразование должно быть перестановочным с электронной подписью, т. е. $\mathrm{sign}(\mathrm{blind}(B)) = \mathrm{blind}(\mathrm{sign}(B))$ [2]. Имеется проблема «мёртвых душ». Необходима дополнительная доработка, чтобы позволить избирателю переголосовать, например, из-за технической ошибки.

5. He-Su (1998). Использует идею слепой подписи, но подписывается не бюллетень избирателя, а его ключ. Это позволяет голосующим изменять своё решение до конца голосования. Маскирующее преобразование должно быть перестановочным с электронной подписью избирателя: $\mathrm{sign}(\mathrm{blind}(B)) = \mathrm{blind}(\mathrm{sign}(B))$, а также подпись должна обладать свойством мультипликативности: $\mathrm{sign}(A \cdot B) = \mathrm{sign}(A) \cdot \mathrm{sign}(B)$ [3]. Избиратели могут переголосовать до объявления окончания выборов. Кроме требовательности к ресурсам, других недостатков не отмечается.

Из краткого описания протоколов видно, что наиболее защищёнными и изученными являются схемы Fujioka-Okamoto-Ohta и He-Su. За основу нашей программной реализации был выбрана схема He-Su.

Схема электронного тайного голосования He-Su представляет собой систему, состоящую из трёх протоколов, в которых для обеспечения сохранения личности голосующего используются алгоритмы электронной подписи и хэширования. Замена одних криптографических систем на другие делает приложение более расширяемым. В частности, позволяет произвести переход на постквантовые алгоритмы криптографии и избавиться от проблемы «взлома из будущего» [4]. Достичь расширяемости можно, как будет показано далее, с использованием программных абстракций. Таким образом, целью данной статьи является представление объектно-ориентированной модели архитектуры программного обеспечения, реализующей схему He-SU с выполнением требования расширяемости кода на основе абстракций.

1. Описание схемы He-Su

При описании схемы будем в основном следовать оригинальной работе [3], указывая на особенности, влияющие на реализацию. Схема описывает взаимодействие между тремя исполнителями:

– избиратель (V – Voiter) – гражданин, имеющий право голоса;

– регистратор (A – Authority) – комиссия, проверяющая право избирателя голосовать, подписывающая «вслепую» подписываемый ключ избирателя для голосования, т. е. без возможности узнать и использовать этот ключ от имени избирателя;

– счётная комиссия (T – Tallier) – комиссия, принимающая заполненные бюллетени избирателей, подсчитывающая голоса и публикующая результаты выборов.

Схема состоит из трёх протоколов:

– протокол регистрации;

– протокол подсчёта ключей;

– протокол подсчёта голосов и объявления результатов.

Рассмотрим каждый из них более подробно.

1.1. Протокол регистрации

Протокол регистрации используется для того, чтобы избиратели могли зарегистрироваться для участия в выборах.

Регистратор A должен сгенерировтаь свои ключи зашифрования и расшифрования: E_a и D_a.

Избиратель V (Voter):

1. Генерирует пару ключей D_v, E_v, где D_v – ключ голосования (секретный ключ), используемый для подписи бюллетеня, и E_v – публичный ключ зашифрования для подсчёта голосов, который должен быть вслепую подписан регистратором A.
2. Генерирует случайное число R, для маскирования подписи своего ключа зашифрования.
3. Вычисляет: $E_a(R) \times (h(E_v))$ и отправляет его в орган A.

Регистратор A :

1. Проверяет право голосования избирателя V.
2. Если V имеет право голосовать, то A подписывает данные, полученные от V:

$$D_a(E_a(R) \times (h(E_v))) \to R \times D_a(h(E_v))$$

и отправляет подписанные данные $R \times D_a(h(E_v))$ обратно избирателю V.

Избиратель V:

1. Удаляет R из $R \times D_a(h(E_v))$:

$$R \times D_a(h(E_v)) \times R^{-1} \to D_a(h(E_v)).$$

2. Проверки:

$$h(E_v) = E_a(D_a(h(E_v))).$$

Если равенство выполняется, избиратель V может быть уверен, что $D_a(h(E_v))$ является подписью его ключа подсчёта голосов E_v.

По истечении времени, отведённого на процедуру регистрации, регистратор A публикует список всех зарегистрированных избирателей.

1.2. Протокол регистрации ключей

В этом протоколе избиратели предоставляют счётной комиссии (T) свои ключи для подсчёта голосов с прикреплённой подписью, вслепую подписанной избирательной комиссией (A). В дальнейшем ключи для подсчёта голосов будут использоваться для проверки действительности бюллетеней.

Избиратель V:

1. Отправляет счётной комиссии T:

$$(E_v, D_a(h(E_v)).$$

Счётная комиссия T:

1. Проверяет подлинность ключа счета V путём вычисления:

$$h(E_v) = E_a(D_a(h(E_v))).$$

2. Если равенство выполняется, ключ для подсчёта голосов E_v авторизован.

Примечание. По истечении крайнего срока подачи счётная комиссия публикует все авторизованные счётные ключи.

1.3. Протокол голосования и подсчёта голосов

Избиратели подписывают свои бюллетени своим ключом для голосования и отправляют свои бюллетени вместе с подписью. Этап голосования и подсчёта голосов разделяется на два подэтапа. Вместо того, чтобы отправлять бюллетени напрямую, избиратели просто отправляют зашифрованные бюллетени с подписью на первом подэтапе. Прежде чем избиратели представят свои ключи для расшифровки зашифрованных бюллетеней, счётная комиссия публикует все зашифрованные бюллетени с прикреплёнными подписями, чтобы каждый избиратель мог проверить, подсчитан ли его бюллетень. Таким образом, у избирателей будет возможность исправить ошибочно подсчитанные бюллетени, не раскрывая бюллетень.

Избиратель V:

1. Отправляет в счётную комиссию T:

$$E_v, K_v(B_v), D_v(h(K_v(B_v))).$$

Счётная комиссия T:

1. Проверяет, находится ли E_v в списке авторизованных ключей подсчёта, затем проверяет подлинность подписи $D_v(h(K_v(B_v)))$ зашифрованного бюллетеня $K_v(B_v)$ путём проверки равенства:

$$E_v(D_v(h(K_v(B_v)))) = h(K_v(B_v)).$$

2. Если E_v находится в списке авторизованных ключей для подсчёта голосов и равенство справедливо для всех избирателей, счётная комиссия публикует:

$$E_v, K_v(B_v), D_v(h(K_v(B_v))).$$

Избиратель V:

1. Проверяет, был ли его зашифрованный бюллетень включён в опубликованный зашифрованный список для голосования. Если нет, то может исправить это, опубликовав:

$$E_v, K_v(B_v), D_v(h(K_v(B_v))).$$

2. Отправляет T:

$$E_v, K_v, D_v(h(K_v)).$$

Счётная комиссия T:

1. Проверяет подлинность K_v путём вычисления:

$$E_v(D_v(h(K_v))) = h(K_v).$$

2. Если K_v действителен, T расшифровывает $K_v(B_v)$ следующим образом:

$$K_v^{-1}(K_v(B_v)) \to B_v.$$

Публикует все аутентифицированные данные:

$$B_v, K_v(B_v), K_v, D_v(h(K_v(B_v))), D_v(h(K_v)), E_v$$

для всеобщей проверки.

2. Модели протоколов схемы He-Su

Как видно из предыдущего раздела, схема He-Su состоит из трёх протоколов, описание которых есть не что иное как описание трёх вариантов использования (трёх прецедентов). Методика разработки на основе анализа прецедентов представлена в [5]. На основе этой методики разработана концептуальная модель предметной области на языке UML (рис. 1).

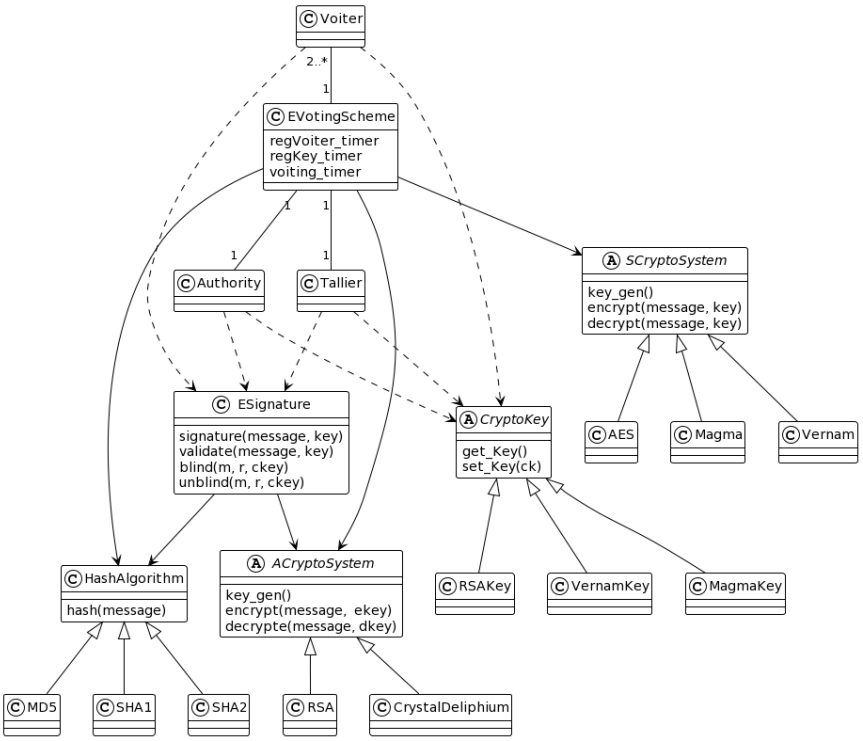

Рис. 1. Модель понятий предметной области, построенная на основе анализа протоколов электронного тайного голосования схемы He-Su

Рис. 2. Диаграмма последовательности протокола регистрации избирателей

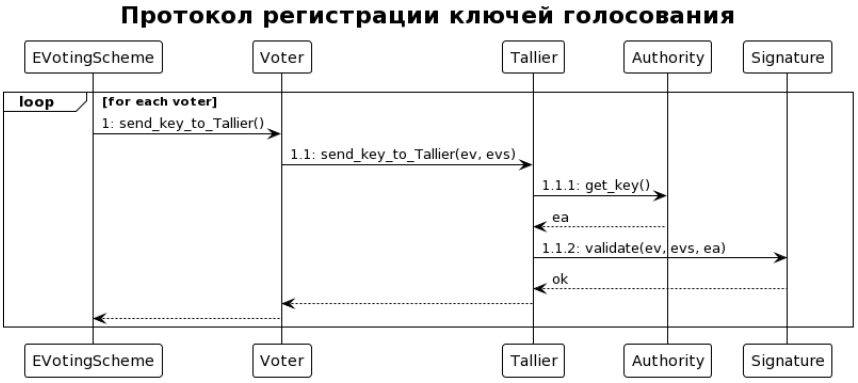

Рис. 3. Диаграмма последовательности протокола регистрации ключей голосования

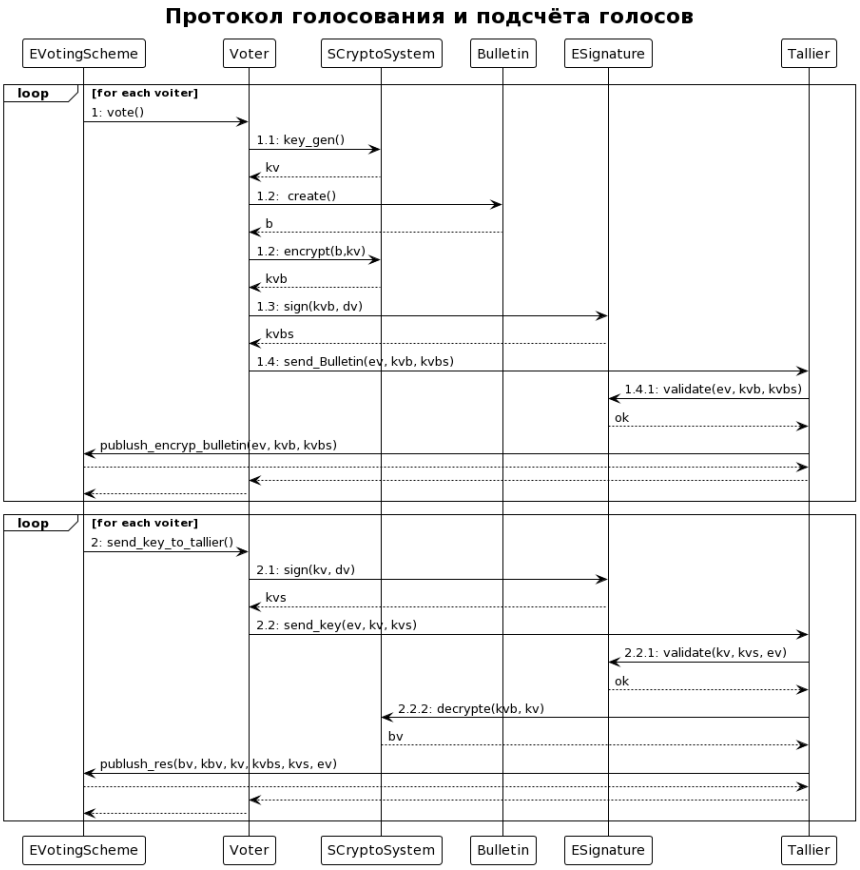

Рис. 4. Диаграмма последовательности протокола голосования и подсчёта голосов

В данной модели архитектуры заложена возможность изменения конкретных реализаций криптографических алгоритмов за счёт использования абстракций в основной схеме электронного тайного голосования.

Описание протоколов схемы He-Su можно представить на UML-диаграммах последовательностей. Предполагается, что в реализации каждый класс Voter, Authority и Tallier будет работать как отдельный сервис или клиент.

Протокол регистрации избирателей представлен на диаграмме последовательности (рис. 2). На диаграмме для упрощения представления опущены обращения к объекту HashAlgorithm. С точки зрения схемы голосования он состоит всего из трёх шагов: 1) генерация пары ключей для зашифрования и расшифрования регистратором; 2) генерация пары ключей для зашифрования и расшифрования избирателем; 3) «слепое» подписание ключа голосующего. Но второй и третий шаги повторяются в цикле для каждого избирателя.

Алгоритм регистрации ключей голосования (рис. 3) сводится к валидации электронной подписи ключа голосования.

3. Заключение

Основными результатами данной работы является:

- объектная декомпозиция схемы He-Su;
- расширяемая архитектура приложения, которая достигается за счёт использования абстракций в основной схеме;
- модели работы протоколов регистрации избирателей, регистрации ключей голосования, голосования и подсчёта голосов представлены в виде диаграмм последовательностей.

По результатам представленной разработки был создан прототип приложения на языке Python, реализующий схему He-Su с электронной подписью на основе криптосистемы RSA и хэширования SHA-1. Шифрование бюллетеней реализовано на базе шифра Вернама, используемого в режиме одноразового блокнота.

Литература

1. Brassard G., Crepeau C., Robert J.-M. All-or-Nothing Disclosure of Secrets // Crypto.cs.mcgill.ca. URL:`https://crypto.cs.mcgill.ca/~crepeau/PDF/ASPUBLISHED/BCR86.pdf` (дата обращения: 26.11.2023).
2. Fujioka, A., Okamoto, T., Ohta, K. A practical secret voting scheme for large scale elections // ASIACRYPT'92 : Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques: Advances in Cryptology. Berlin; Heidelberg : Springer-Verlag, 1992. P. 244–251.
3. He Q., Su Z. A New Practical Secure e-Voting Scheme // Cs.cmu.edu. URL:`http://www.cs.cmu.edu/~qihe/paper/e_voting` (дата обращения: 19.11.2023).
4. Лаврова Д.Д. Требования к реализации электронного тайного голосования // Молодёжь третьего тысячелетия : сборник научных статей. Т. 1. Ч. 1. Омск : Издательство Омского государственного университета, 2023. URL: `https://www.elibrary.ru/download/elibrary_54140614_81386086.pdf` (дата обращения: 26.11.2023).
5. Ларман К. Применение UML 2.0 и шаблонов проектирования. М. : Издательский дом «Вильямс», 2004. 624 с.

ARCHITECTURE MODEL OF AN APPLICATION IMPLEMENTING THE HE-SU ELECTRONIC SECRET VOTING SCHEME

D.D. Lavrova[1]
Student, e-mail: drlvrv@gmail.com
D.N. Lavrov[2]
Ph.D. (Techn.), Associate Professor, e-mail: dmitry.lavrov72@gmail.com

[1]Dostoevsky Omsk State University, Omsk, Russia
[2]Nizhnevartovsk State University, Nizhnevartovsk, Russia

Abstract. The article offers a description of an object-oriented model of an application that implements an electronic secret voting scheme based on the He-Su scheme. To implement the scheme, you need to choose three basic cryptographic schemes: hashing, a symmetric cryptosystem and an asymmetric cryptosystem with the ability to blindly sign. Based on the analysis of the constructed model, an architecture based on abstractions is proposed, which makes it possible to easily select and replace some basic cryptographic systems with others used in the scheme.

Keywords: electronic secret voting, blind signature, cryptosystems, cryptographic protocols, He-Su scheme.

Дата поступления в редакцию: 23.11.2023