УДК 004.056

Хамелеон-хэши: конструкции, свойства и применение в редактируемых блокчейнах

Малеев Л. Б., Клименко В. А.
Научный руководитель – канд. техн. наук, доцент Давыдов В.В.
Санкт-Петербургский государственный университет аэрокосмического приборостроения
leon.maleev2014@gmail.com, vadimklimenko318@gmail.com

Введение

Классический блокчейн задуман как неизменяемый журнал: любое изменение подтверждённых данных нарушает хэш-связность цепочки и подрывает доверие к истории. Однако на практике всё чаще требуется контролируемая редактируемость — из-за требований GDPR («право на забвение»), необходимости удаления противоправного контента, исправления ошибок и регламентной корректировки корпоративных журналов. Распространённые обходные решения (хардфорки, “пометки” об удалении, хранение данных вне цепи) обычно либо слишком дороги и сложны, либо не обеспечивают полноценного исправления/удаления данных и сохранения проверяемости, либо создают риски централизации; поэтому актуальны криптографические механизмы, позволяющие вносить правки без разрушения целостности цепи, с публичной проверяемостью, ограничением прав на редактирование и возможностью аудита. В тезисах рассматриваются современные подходы к построению редактируемых блокчейнов и сопутствующих примитивов.

Основная часть

Одним из практических механизмов, который решает данную проблему, являются «хамелеон-хэши»: это семейство хэш-функций с открытым ключом и некоторым секретом trapdoor, позволяющим владельцу эффективно находить коллизии и тем самым заменять зафиксированное сообщение на другое, оставив хэш неизменным. Для внешних проверяющих такой хэш остаётся стойким к коллизиям, при этом право на правку контролируется владением trapdoor и процедурами его ротации или распределения. Архитектура сводится к трём действиям: вычислить хэш, подобрать коллизию, используя trapdoor, и при необходимости сменить или отозвать ключ редактирования, чего достаточно для интеграции в блокчейн без математических деталей.

Существующие схемы хамелеон-хэшей основаны на различных криптографических примитивах. Классические схемы, основанные на задачах дискретного логарифмирования и факторизации [1], компактны и просты, но уязвимы к квантовым атакам. Конструкции на билинейных спариваниях дают короткие хэши и поддерживают гибкие политики доступа [2], однако их стойкость доказывается из специализированных предположений в группах билинейных отображений и обычно требует процедуры начальной генерации общих параметров с мастер-ключом, который должен быть уничтожен после выработки параметров. Постквантовые кодовые конструкции и конструкции, основанные на решётках [3], обеспечивают устойчивость к квантовым атакам и позволяют естественно реализовать обновление или ревокацию полномочий, но требуют более крупных параметров.

В данной работе рассматриваются алгоритмы построения хамелеон-хэшей Lattice-based revocable PCH, AWTCH и FB-PCH [3-5]. Lattice-based revocable Policy-Based Chameleon Hash [3] – постквантовый вариант на решётках (LWE/SIS): он устойчив к квантовым атакам, но параметры крупнее, чем у классических схем и основанных на

билинейных спариваниях. Его главное удобство – можно отозвать или заменить право редактирования, при этом уже записанные хэши остаются корректными. AWTCH (Accountable Weight Threshold Chameleon Hash) [4] решает проблему доверия: секрет редактирования делят между несколькими участниками, и правка возможна только если собрался кворум по “весам” голосов, причём схема позволяет выявить виновного, если кто-то злоупотребил правкой. FB-PCH (Forward/Backward-Secure Policy-Based Chameleon Hash) [5] – это хамелеон-хэш, основанный на билинейных спариваниях, где в сам хэш «встроено» правило, кому разрешено редактирование (политика доступа). Его плюс в том, что даже если секрет редактирования однажды утечёт, злоумышленник может воздействовать лишь на записи, относящиеся к периоду действия данного секретного ключа – ущерб ограничен этим периодом; после ротации злоумышленник не сможет переписать старые записи, а также подготовить правки на будущее.

В работе также проведён анализ преимуществ применения хамелеон-хэшей в редактируемых блокчейн-системах. К основным достоинствам относятся: контролируемая правка данных без потери проверяемости; сохранение целостности структуры хранения при разрешённой замене фрагмента содержимого за счёт адаптации хэша без нарушения связности и верифицируемости; прозрачность для аудита через фиксацию правок метаданными (например, Adapt/Update) с указанием, что изменено, когда, кем и на каком основании; разграничение полномочий, при котором изменения выполняются только уполномоченной стороной и строго в рамках заданных правил; гибкость для подписанных сообщений – возможность изменять отдельные части после предварительного подписания без перевыпуска подписи, если правка санкционирована политикой; поддержка отсроченных и коллективных правок с привязкой ко времени и ответственностью участников, что особенно полезно для журналирования и реестров.

Поскольку право редактирования в хамелеон-хэшах фактически определяется владением trapdoor, его компрометация напрямую означает потерю контроля над правками. Поэтому на практике управление trapdoor должно сопровождаться защитой в HSM/TEE (Hardware Security Module/ Trusted Execution Environment), регулярной ротацией ключей и, при необходимости, распределением секрета между несколькими участниками (пороговые/взвешенные схемы) с обязательным журналированием операций Adapt/Update/Revoke.

Выводы

Хамелеон-хэши позволяют совместить контролируемую редактируемость с публичной проверяемостью и становятся базовым примитивом для «гибких» блокчейнов и подписей. Ключевые направления развития – переход к постквантовым схемам, усиление временной привязки правок, поддержка ротации и отзыва полномочий, а также внедрение коллективного контроля с полноценным аудитом изменений; среди открытых задач – снижение размеров параметров постквантовых схем и выработка общих стандартов журналирования правок.

Литература

1. Hugo Krawczyk and Tal Rabin Chameleon Hashing and Signatures // Cryptology {ePrint} Archive, Paper 1998/010. – 1998
2. Chen M. et al. Building Traceable Redactable Blockchain with Time-Verifiable Chameleon Hash //Electronics. – 2025. – Т. 14. – №. 5. – С. 846.
3. Klamti J. B., Hasan M. A. Revocable policy-based chameleon hash using lattices //Journal of Mathematical Cryptology. – 2024. – Т. 18. – №. 1. – С. 20230012.
4. Ma Q. et al. Redactable blockchain from accountable weight threshold chameleon hash //High-Confidence Computing. – 2025. – Т. 5. – №. 3. – С. 100281.
5. Li N. et al. Practical and secure policy-based chameleon hash for redactable blockchains //The Computer Journal. – 2024. – Т. 67. – №. 11. – С. 3128-3139.