УДК 004.056.55

ОБЗОР И АНАЛИЗ ПОДХОДОВ К ПОСТРОЕНИЮ ЧАСТИЧНО СЛЕПЫХ ПОДПИСЕЙ

Бахшиева Е.З.[1], Ерина Л.А.[1]

Научный руководитель – канд. техн. наук, доцент Давыдов В.В

[1] Санкт-Петербургский Государственный Университет Аэрокосмического Приборостроения

babah.eva@yandex.ru, ya-whiteflower@yandex.ru

Введение

Цифровая подпись обеспечивает подтверждение подлинности данных и защиту их целостности. В классических схемах подписант имеет полный доступ к содержимому подписываемого сообщения. Однако в ряде прикладных задач – например, в электронных платежах, анонимных удостоверениях и системах электронного голосования – требуется, чтобы подписант не знал содержимое сообщения.

Впервые для решения этой задачи учёным D.Chaum была предложена слепая подпись [1], позволяющая получать подпись на сообщении, скрытом от подписанта. Их развитием стали частично слепые подписи, в которых часть информации (публичная метка, например, срок действия или назначение подписи) заранее согласуется сторонами и включается в подпись, тогда как основное сообщение остаётся скрытым. Такой механизм сочетает анонимность пользователя и контроль определённых параметров со стороны подписанта.

Понятие частично слепой подписи впервые было введено в работе Abe и Fujisaki в 1996 году [2]. Первые схемы частично слепых подписей с формальными доказательствами стойкости были построены на основе задачи дискретного логарифмирования. Одной из таких схем стала подпись Abe-Okamoto [3]; позднее было пересмотрено доказательство стойкости схемы в модели случайного оракула [4]. В дальнейшем были предложены конструкции на иных математических предположениях, включая схемы на решётках и изогениях между эллиптическими кривыми.

Основная часть

Частично слепая подпись – схема цифровой подписи, при которой подписант возвращает подпись на сообщение пользователя в ходе интерактивного протокола с заранее согласованной публичной меткой info, не раскрывающей содержимое самого сообщения. Схема должна обеспечивать корректность, стойкость к подделке (включая ограничение числа подписей) и частичную слепоту, то есть невозможность связать подпись с конкретной сессией её получения, за исключением метки info.

В данной работе проведён краткий обзор и анализ подходов к построению частично слепых подписей. Рассматриваются подписи Abe-Okamoto [3], Li-Gao-Li [5], Zhang-Safavi-Naini-Susilo [6] и CSI-Otter [7], основанные на модульной арифметике, решётках, билинейных спариваниях и изогениях соответственно. В работе подробно рассматриваются все указанные схемы: анализируются используемые математические конструкции и механизмы достижения частичной слепоты, а также обсуждаются их ключевые достоинства и ограничения. При анализе особое внимание уделяется оценке криптографической стойкости указанных схем.

Выводы

Проведены обзор и анализ подходов к построению частично слепых подписей. Рассмотрены четыре схемы частично слепой подписи, проведен анализ их конструкций и сравнение используемого математического аппарата, размеров ключей и подписей, вычислительной сложности и уровня стойкости (в терминах NIST).

Проведённый анализ показывает, DLP- и pairing-конструкции (Abe-Okamoto, Zhang-Safavi-Naini-Susilo) отличаются компактностью параметров, высокой вычислительной эффективностью и зрелой доказательной базой, однако, они основаны на стандартных

предположениях и не обладают квантовой стойкостью. Схемы, основанные на решётках и изогениях (Li-Gao-Li, CSI-Otter), обеспечивают защиту от квантовых атак, но характеризуются увеличенными размерами ключей и подписей, большей вычислительной сложностью и более сложным математическим аппаратом.

Литература

1. Chaum D. Blind signatures for untraceable payments // Advances in Cryptology: Proceedings of Crypto 82. – Boston, MA : Springer US, 1983. – С. 199-203.
2. Abe M., Fujisaki E. How to date blind signatures // International Conference on the Theory and Application of Cryptology and Information Security. – Berlin, Heidelberg : Springer Berlin Heidelberg, 1996. – С. 244-251.
3. Pointcheval D., Stern J. Provably secure blind signature schemes // International Conference on the Theory and Application of Cryptology and Information Security. – Berlin, Heidelberg : Springer Berlin Heidelberg, 1996. – С. 252-265.
4. Kastner J., Loss J., Xu J. The Abe-Okamoto partially blind signature scheme revisited // International Conference on the Theory and Application of Cryptology and Information Security. – Cham : Springer Nature Switzerland, 2022. – С. 279-309.
5. Li P., Gao J., Li X. A new lattice-based partially blind signature with more complete proof // Journal of Information and Intelligence. – 2024. – Т. 2. – №. 3. – С. 236-252.
6. Zhang F., Safavi-Naini R., Susilo W. Efficient verifiably encrypted signature and partially blind signature from bilinear pairings // International Conference on Cryptology in India. – Berlin, Heidelberg : Springer Berlin Heidelberg, 2003. – С. 191-204.
7. Katsumata S. et al. CSI-Otter: Isogeny-based (partially) blind signatures from the class group action with a twist // Designs, Codes and Cryptography. – 2024. – Т. 92. – №. 11. – С. 3587-3643.