Leakable Mnemonic Phrase: A New Orientation of Wallets Backup based on Biometric-key

No author given

***Abstract*—A Mnemonic phrase is a set of secret words that correspond one-to-one with the secret key of a user's crypto wallet. If this phrase is lost, the user cannot access the cryptocurrencies. Thus, the user wants to back up the phrase with multiple storage, but the risk of leakage increases. To solve this dilemma, this paper proposes a leakable mnemonic phrase system in which the phrase is encrypted with a secret key generated from the user's biometric information. Since the leakable mnemonic phrase can be decrypted only with the user's biometric information, it can be backed up to various external storage and devices to solve the contradictory problem of keeping the contents of the phrase secret while preventing its loss. In this paper, we also show the results of evaluating the performance of this system by implementing it on an actual biometric authentication device. The encryption/decryption processing time is fast (200 ms), and the system successfully decrypted the mnemonic phrase six months after enrollment.**

***Index Terms*—Crypto-wallet, Biometrics authentication, Fuzzy extractor**

I. Introduction

A *mnemonic phrase (or path phrase, secret phrase)* is a group of 12-24 words randomly generated each time a user creates a new crypto wallet, corresponding one-to-one with the secret key of the user address. Entering these mnemonic phrases in the correct order into the crypto wallet allows the user to access the cryptocurrency corresponding to the address. The purpose of the mnemonic phrase is to convert the binary value of the secret key into human-readable words, allowing it to be stored and backed up outside the computer using a memo or other method. This phrase must be kept secret because anyone who knows the mnemonic phrase of a user address can access that user's cryptocurrency.

The challenge with mnemonic phrase backup is that while one would like to use external storage such as cloud services or other backup methods to prevent loss, the risk of leakage increases the more multiple methods are used. Many users back up by writing the phrase on paper or metal plates and hiding them in the user's home.

In summary, the problem is to satisfy the following two conflicting conditions:

- Do not lose the mnemonic phrase.
- Keep the mnemonic phrase secret.

In this paper, we propose a leakable mnemonic phrase that solves this problem. Specifically, we encrypt a user's mnemonic phrase using a *fuzzy extractor*, a cryptographic technique that generates an encryption/decryption key from fuzzy information such as biometric data. This encrypted mnemonic phrase (we call it leakable mnemonic phrase) is stored in various external storage and devices to prevent loss. Since the leakable mnemonic phrase is encrypted with the user's biometric-key, it is difficult to recover it without the user's biometric information. As a result, this system can prevent the loss of the mnemonic phrase while keeping it secret. In addition, since the biometric-key is recovered from the user's biometric information and public information, called helper data, there is no need to store secret information to recover the biometric-key. In other words, the only information that must be kept secret is the user's biometric information.

Related work.

In crypto-currency, secret key management for wallets is one of the biggest unsolved problems. Many users use custodial wallets provided by third parties, such as exchanges. However, there are problems, such as fraud by administrators, and there are always leakage incidents [1]. On the other hand, non-custodial wallets, where users manage their secret keys, have the problems above, and there is currently no perfect solution. Many users use hardware/software wallets, physical paper, or metal plates to manage their secret keys and mnemonic phrases.

Ledger offers a service to store mnemonic phrases on network servers via a secret sharing scheme [2]. Soltani et al. [3] also proposed a wallet backup protocol using a secret sharing scheme. However, the possibility of fraud the collusion of administrators or others exists in the secret sharing schemes. Rezaeighaleh et al. [4] proposed a method of backing up mnemonic phrases to multiple hardware using NFC, but backing up in plain text increases the risk of leakage. Naganuma et al. [5] proposed a key-management scheme of using a biometric-key as a secret key for a crypto wallet, but this is for users who create a new wallet and cannot be used as a backup for users who already have a secret key and mnemonic phrase. Liu et al. [6] also propose a backup method to store short phrases in the user's brain. There are many other types of research on crypto-wallets secret key management and backup [7] [8] [9] [10] [11] [12], to the best of our knowledge, our proposal is the first scheme that stores a mnemonic phrase encrypted by biometric-key.

Our contributions.

We summarize our contributions.

- Leakable mnemonic phrase: We propose a leakable mnemonic phrase system in which a mnemonic phrase can be encrypted/decrypted only by the specified user using a biometric-key generated by a fuzzy extractor. By storing the leakable mnemonic phrase in multiple storage and devices such as external servers, it is possible to realize a backup scheme that prevents the loss of the phrase while keeping its contents secret.

- Implementation and evaluation: We implemented the leakable mnemonic phrase system using a finger vein authentication device [13], and confirmed that encryption/decryption of mnemonic phrases can be processed at high speed (200 ms). We also confirmed that the mnemonic phrase can be recovered with a biometric-key from biometric data six months after registration and encryption. These results show the practicality of our system.

  The QR code below is a mnemonic phrase of one of the author's MetaMask (a crypto wallet for Ethereum) [14] encrypted with his biometric-key. In this way, we can realize a secure backup by storing the encrypted mnemonic phrase[1].

Fig. 1. A Leakable Mnemonic Phrase of one of the author's MetaMask: This data is encrypted by his biometric-key.

What is the difference from ordinary biometrics authentication?

Many biometric hardware wallets already exist [15] [16]. The difference between our proposed scheme using a fuzzy extractor and an ordinal biometric wallet is whether the secret key is associated with the biometric body. In the ordinal biometric authentication technology, the biometric image input to the sensor is compared with the stored biometric image, and if the matching score is high, the stored secret key can be accessed. Since this secret key is a random bit sequence that has nothing to do with biometric information, it must be stored inside the hardware. Therefore, problems such as loss or theft of the hardware wallet can occur.

On the other hand, our proposed scheme generates the secret key directly from the user's biometric data using a fuzzy extractor, so there is no need to store the secret key in the device or hardware. When the private key is used, it is generated again from the user's biometric data. As a result, there are no problems with lost or stolen hardware wallets.

II. Preliminary

A. Mnemonic Phrase

In this paper, we focus on mnemonic phrases compliant with the BIP-39 specification [17] adopted by MetaMask [14] and others. In this specification, a phrase of 12 words is generated when the key size of the secret key is 128 bits and 24 words when the key size is 256 bits from a word list of 2048 words. The leakable mnemonic phrase system proposed in this paper is applicable to specifications other than BIP-039.

B. Fuzzy Extractor

Fuzzy extractor is a generic term for a function that takes fuzzy information, such as biometric data, as input and outputs a fixed-valued secret key needed for cryptography. A fuzzy extractor generates a random string R and helper data P based on the user's biometric data w at the enrollment phase. When reproducing phase, the same string R is generated using the close biometric information w' and helper data P as input. The definition of the fuzzy extractor is as follows. See [18] [19] for detailed.

Definition 1: Let $\mathcal{M}$ be a set of biometric data and $\mathrm{dist}(\cdot,\cdot)$ be a distance function over $\mathcal{M}$. An $(\mathcal{M}, m, l, t)$-fuzzy extractor $\mathcal{F}$ is a pair of randomized polynomial time algorithms $\mathcal{F} = (\mathrm{Gen}, \mathrm{Rep})$ with the following properties:

- The algorithm Gen on input $w \in \mathcal{M}$ outputs an extracted string $R \in \{0,1\}^l$ and a helper data string $P \in \{0,1\}^*$.
- The algorithm Rep takes an element $w' \in \mathcal{M}$ and a helper data $P \in \{0,1\}^*$ as inputs. For every pair (w, w') such that $\mathrm{dist}(w, w') \leq t$, for $(R, P) \leftarrow \mathrm{Gen}(w)$, then $\mathrm{Rep}(w', P) = R$. If $\mathrm{dist}(w, w') > t$, then no guarantee is provided about the output.
- For any distribution W on $\mathcal{M}$ of minimal entropy m, the string R, where $(R, P) \leftarrow \mathrm{Gen}(W)$, is nearly uniform even for those who observe the helper data P.

In this paper, we assume $\mathrm{dist}(w, w') \leq t$ when the same person's biometric data at enrollment is w and at recovery is w', and in other cases, we assume $\mathrm{dist}(w, w') > t$. The third condition in the above definition intuitively indicates that the string R is indistinguishable from a random number sequence and that the security is not affected even if the helper data is publicly available. In this paper, our system for encryption and decryption of mnemonic phrases is constructed using the fuzzy extractor proposed by Hitachi, Ltd [13] [5].

III. System Design

In this section, we propose a new backup scheme for mnemonic phrases using fuzzy extractor $\mathcal{F} = (\mathrm{Gen}, \mathrm{Rep})$. Our scheme mainly focuses on users who already have a crypto wallet and its mnemonic phrase, not on users who have created a new crypto wallet[2].

[1] If this paper is accepted, the author's wallet and mnemonic phrase information will be backed up in the proceeding of IEEE ICBC 2024.

[2] If a user creates a new crypto wallet, the secret key generated by fuzzy extractor can be converted directly into a mnemonic phrase.

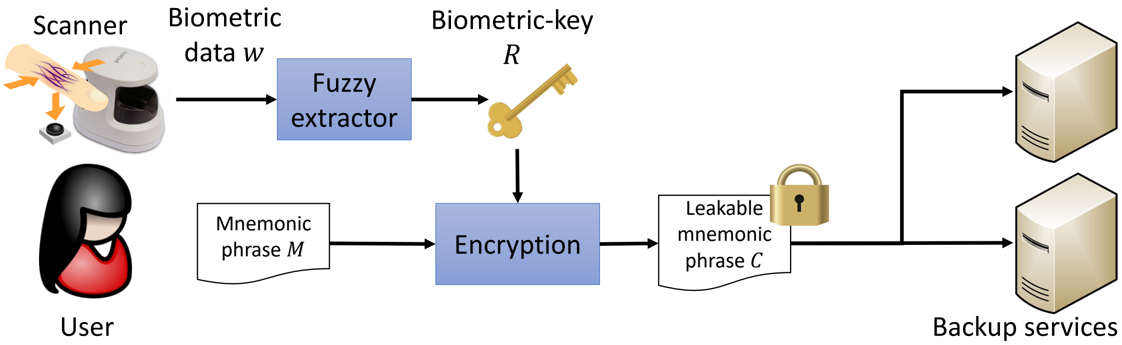


Fig. 2. Image of the Enrollment Phase

A. Enrollment Phase

The enrollment phase (see Fig. 2) consists of the following 4 steps.

1) **Wallet generation**
A user generates the mnemonic phrase M according to the crypto wallet specifications. Under normal circumstances, this operation is performed in advance by the user independently of this system.
2) **Registration**
The user inputs his/her biometric data w into the fuzzy extractor's Gen algorithm to generate a random string R of the required length and helper data P. For example, if AES with 256-bit secret key is used for encryption, the user generates a 256-bit R.
$$(R, P) \leftarrow \mathrm{Gen}(w).$$
3) **Generating a leakable mnemonic phrase**
The user generates the ciphertext C of the mnemonic phrase M using an encryption algorithm such as AES with R generated in step 2 as the secret key. We call the string R biometric-key.
$$C := \mathrm{Enc}(R, M).$$
4) **Backup**
The user stores the user's ID and the pair of ciphertext C and helper data P generated in steps 2 and 3 as a leakable mnemonic phrase (UserID, C, P) in multiple external storage devices such as backup servers.

B. Recovery Phase

When a user loses a mnemonic phrase M, the fuzzy extractor $\mathcal{F} = (\mathrm{Gen}, \mathrm{Rep})$ is used to recover the mnemonic phrase M and the crypto wallet. The recovery phase consists of the following 3 steps.

1) **Download the leakable mnemonic phrase**
The user downloads a leakable mnemonic phrase (UserID, C, P) from the backup server using the ID as a key.
2) **Generating the biometric-key**
The user re-extracts biometric-key R using a user's biometric data w' and helper data P.
$$R \leftarrow \mathrm{Rep}(w', P).$$
At this time, if it is the same user, the same biometric-key R is generated as at the time of enrollment because $\mathrm{dist}(w, w') \leq t$.
3) **Recovery**
The user decrypts the leakable mnemonic phrase C using the biometric-key R generated in Step 2 to obtain the original mnemonic phrase M.
$$M = \mathrm{Dec}(R, C).$$

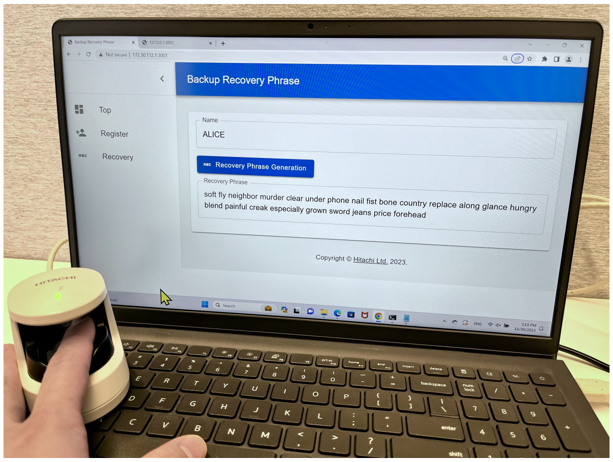
With the above procedure, the user can recover the mnemonic phrase M.

C. Security Analysis

In our proposed scheme, a leakable mnemonic phrase generated in the enrollment phase (UserID, C, P) is stored and managed in various external storage. UserID is usually public information such as e-mail address or name and thus do not affect the security of the mnemonic phrase M. Furthermore, no information can be obtained from the ciphertext C without the encryption/decryption key R. Also, the helper data P does not affect the security of R from the assumption of fuzzy extractor Section II-B. Therefore, in order for an attacker to obtain information on the mnemonic phrase M, information on the output value R of the fuzzy extractor is required. In other words, to obtain R, an attacker guesses the user's biometric information w, uses the fuzzy extractor, and recovers R. As a result, the security of the proposed method depends on the accuracy of the biometric authentication, the entropy of the biometric data space $\mathcal{M}$, and the probability that $\mathrm{dist}(w, w') \leq t$ for different users (False Acceptance Rate). Another security enhancing technology is to recover R, which requires helper data P. For example, we should employ another authentication, such as two-factor authentication, in Step 1 of the Recovery phase to download the user's helper data P.

IV. Implementation and Evaluation

We implemented a fuzzy extractor using a finger vein device from Hitachi, Ltd. [13] and implemented the leakable mnemonic phrase system proposed in Section III. We used 24-word mnemonic phrases compliant with the BIP-39 specification as input and AES 256-bit as the encryption scheme. In fact, Fig. 1 is the encrypted mnemonic phrase of one author's Metamask wallet with his own biometric-key. Both encryption and decryption took about 200 ms, which is a practical speed. Furthermore, the leakable mnemonic phrase was created and decrypted 6 months later, and it was confirmed that the correct original mnemonic phrase was recovered.


Name
ALICE

Recovery Phrase
soft fly neighbor murder clear under phone nail fist bone country replace along glance hungry blend painful creak especially grown sword jeans price forehead

Copyright © Hitachi Ltd. 2023.

Fig. 3. Implementation of our Leakable Mnemonic Phrase System

V. Conclusion

In this paper, we proposed the leakable mnemonic phrase system as a new backup scheme for crypto-wallet's mnemonic phrases. In the proposed system, a user's mnemonic phrase is encrypted with the user's biometric-key, so that only the user himself/herself can access the phrase. As a result, the leakable mnemonic phrase can be stored in multiple storage locations, protecting the information in the mnemonic phrase and preventing it from being lost. Future works are demonstration tests on real systems and security evaluation. We believe that there is no perfect solution to back up a crypto-wallet. Users should take various measures against leakage and loss, with our proposed method as one of the options. We hope that our system will be a framework for new crypto-wallet backup.

References

[1] "The 10 biggest crypto exchange hacks in history," https://crystalblockchain.com/articles/the-10-biggest-crypto-exchange-hacks-in-history/.

[2] "Ledger recover service," https://www.ledger.com/recover/.

[3] R. Soltani, U. T. Nguyen, and A. An, "Practical key recovery model for self-sovereign identity based digital wallets," in *2019 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech)*, 2019, pp. 320–325.

[4] H. Rezaeighaleh and C. C. Zou, "New secure approach to backup cryptocurrency wallets," in *2019 IEEE Global Communications Conference (GLOBECOM)*, 2019, pp. 1–6.

[5] K. Naganuma, T. Suzuki, M. Yoshino, K. Takahashi, Y. Kaga, and N. Kunihiro, "New secret key management technology for blockchains from biometrics fuzzy signature," in *15th Asia Joint Conference on Information Security, AsiaJCIS 2020, Taipei, Taiwan, August 20-21, 2020.* IEEE, 2020, pp. 54–58. [Online]. Available: https://doi.org/10.1109/AsiaJCIS50894.2020.00020

[6] Y. Liu, R. Li, X. Liu, J. Wang, L. Zhang, C. Tang, and H. Kang, "An efficient method to enhance bitcoin wallet security," in *2017 11th IEEE International Conference on Anti-counterfeiting, Security, and Identification (ASID)*, 2017, pp. 26–29.

[7] Y. Erinle, Y. Kethepalli, Y. Feng, and J. Xu, "Sok: Design, vulnerabilities, and security measures of cryptocurrency wallets," 2023.

[8] A. R. Sai, J. Buckley, and A. Le Gear, "Privacy and security analysis of cryptocurrency mobile applications," in *2019 Fifth Conference on Mobile and Secure Services (MobiSecServ)*, 2019, pp. 1–6.

[9] O. Pal, B. Alam, V. Thakur, and S. Singh, "Key management for blockchain technology," *ICT Express*, vol. 7, no. 1, pp. 76–80, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2405959519301894

[10] S. Suratkar, M. Shirole, and S. Bhirud, "Cryptocurrency wallet: A review," in *2020 4th International Conference on Computer, Communication and Signal Processing (ICCCSP)*, 2020, pp. 1–7.

[11] R. Belchior, A. Vasconcelos, S. Guerreiro, and M. Correia, "A survey on blockchain interoperability: Past, present, and future trends," 2021.

[12] H. Chen, M. Pendleton, L. Njilla, and S. Xu, "A survey on ethereum systems security: Vulnerabilities, attacks and defenses," 2019.

[13] "Hitachi h1 finger vein reader," https://www.m2sys.com/finger-vein-reader/.

[14] "Metamask," https://metamask.io/.

[15] "Authentrend," https://authentrend.com/.

[16] "D'cent," https://dcentwallet.com/.

[17] "Bip-39," https://github.com/bitcoin/bips/tree/master/bip-0039.

[18] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," *SIAM journal on computing*, vol. 38, no. 1, pp. 97–139, 2008.

[19] B. Fuller, X. Meng, and L. Reyzin, "Computational fuzzy extractors," Cryptology ePrint Archive, Paper 2013/416, 2013, https://eprint.iacr.org/2013/416. [Online]. Available: https://eprint.iacr.org/2013/416