# AN EFFICIENT PRIVACY-PRESERVING CREDIT SCORE SYSTEM BASED ON NON INTERACTIVE ZERO KNOWLEDGE PROO

**A.SRINISH REDDY[1], BANDI PARAMESWARA REDDY[2], AVVA YOGESHWAR[3], R. PARDHA SARDHI[4]**

**ASSISTANT PROFESSOR[1], UG SCHOLAR[2,3&4]**

**DEPARTMENT OF CSE, CMR INSTITUTE OF TECHNOLOGY, KANDLAKOYA VILLAGE, MEDCHAL RD, HYDERABAD, TELANGANA 501401**

**ABSTRACT**— Credit system is generally associated with the banking and financial institutions, although it has far reaching implications for residents of countries, such as U.S., particularly for those with a poor credit history. Specifically, a credit score computation (CSC) quantifies an individual's credit value or credit risk, which is used by banking and financial institutions, as well as other entities (e.g., during purchasing of insurance policies and application of rental properties), to facilitate their decision-making (e.g., whether to approve the insurance policy purchase or the level of premium). Although a number of CSC models have been proposed in the literature for supporting different application scenarios, privacy protection of CSC is rarely considered despite the potential for leakage of user private information (e.g., registration, hobbies, credit, relationships, and inquiry). Such information can then be abused for other nefarious activities, such as identity theft and credit card fraud. Thus, in this article, we first analyze the privacy strength of existing CSC models, prior to presenting the formal definition of a privacy-preserving CSC system alongside its security requirements. Then, we propose a concrete construction based on Paillier encryption with three proposed noninteractive zeroknowledge schemes. To demonstrate feasibility of our proposal, we evaluate both its security and performance.

**Index Terms**— Credit score computation (CSC), noninteractive zero knowledge (NIZK), Paillier encryption, privacy preserving.

**I. INTRODUCTION** T HE credit system is a platform that provides some form of credit evaluation for both individuals and nonindividual entities (e.g., organizations), which determines the "financial trustworthiness" of the individual and/or nonindividual entity [1], [2]. For instance, in the U.S., credit score is widely used in a broad range of applications, for example to determine whether an individual's application for, say a credit card, home/automobile loan, etc., will be approved or an individual has to pay a higher insurance premium or higher interest rate (due to low credit score). As shown in Fig. 1, a credit system generally comprises three types of participants (i.e., users, credit bureaus, and creditors). The user is a key part of the credit system, whose credit and loan activities (new account creation, account balance/credit card utilization, credit inquiries, and payment history) are reported to the credit bureaus. The latter is responsible for collecting, recording, and distributing relevant information (collectively referred to as "credit data") about the user's credit activities [3]. Such credit data are then requested by the creditors to compute the user's credit score, which is then used to inform some decision-making. In other words, the credit score represents the credit value/risk/health of an individual or entity, which is a reference value for trust assessment [4]. The score is generated by analyzing the user's credit data using an algorithm (i.e., risk model), a process known as credit score computation (CSC). Different models consider different factors and weights to compute the final credit score. For example, FICO scores are calculated based on the user's payment history (35%), amounts owed (30%), length of credit history (15%), new credit (10%), and credit mix (10%).1 There are different risk models in the literature, such as least squares support vector machines ensemble models for credit scoring [5], a measure of creditworthiness for sound financial decision-making [6], a partial credit model [7], and a fuzzy logistic regression based credit scoring model [8]. Using these models, creditors can take as input the credit data obtained from the bureaus and quickly obtain a credit score. However, these models do not consider the privacy protection of user credit data and their corresponding weights.

## II. LITERATURE SURVEY

### 1. An Efficient Privacy-Preserving Credit Score System Based on Noninteractive Zero-Knowledge Proof

Chao Lin, Min Luo, +2 authors De-biao He Published in IEEE Systems Journal 1 March 2022

Credit system is generally associated with the banking and financial institutions, although it has far reaching implications for residents of countries, such as U.S., particularly for those with a poor credit history. Specifically, a credit score computation (CSC) quantifies an individual's credit value or credit risk, which is used by banking and financial institutions, as well as other entities (e.g., during purchasing of insurance policies and application of rental properties), to facilitate their decision-making (e.g., whether to approve the insurance policy purchase or the level of premium). Although a number of CSC models have been proposed in the literature for supporting different application scenarios, privacy protection of CSC is rarely considered despite the potential for leakage of user private information (e.g., registration, hobbies, credit, relationships, and inquiry). Such information can then be abused for other nefarious activities, such as identity theft and credit card fraud. Thus, in this article, we first analyze the privacy strength of existing CSC models, prior to presenting the formal definition of a privacy-preserving CSC system alongside its security requirements. Then, we propose a concrete construction based on Paillier encryption with three proposed noninteractive zero-knowledge schemes. To demonstrate feasibility of our proposal, we evaluate both its security and performance.

### 2. Bulletproofs: Short Proofs for Confidential Transactions and More

Benedikt Bünz, Jonathan Bootle, +3 authors Gregory Maxwell Published in IEEE Symposium on Security… 20 May 2018

We propose Bulletproofs, a new non-interactive zero-knowledge proof protocol with very short proofs and without a trusted setup; the proof size is only logarithmic in the witness size. Bulletproofs are especially well suited for efficient range proofs on committed values: they enable proving that a committed value is in a range using only 2 log_2(n)+9 group and field elements, where n is the bit length of the range. Proof generation and verification times are linear in n. Bulletproofs greatly improve on the linear (in n) sized range proofs in existing proposals for confidential transactions in Bitcoin and other cryptocurrencies. Moreover, Bulletproofs supports aggregation of range proofs, so that a party can prove that m commitments lie in a given range by providing only an additive O(log(m)) group elements over the length of a single proof. To aggregate proofs from multiple parties, we enable the parties to generate a single proof without revealing their inputs to each other via a simple multi-party computation (MPC) protocol for constructing Bulletproofs. This MPC protocol uses either a constant number of rounds and linear communication, or a logarithmic number of rounds and logarithmic communication. We show that verification time, while asymptotically linear, is very efficient in practice. The marginal cost of batch verifying 32 aggregated range proofs is less than the cost of verifying 32 ECDSA signatures. Bulletproofs build on the techniques of Bootle et al. (EUROCRYPT 2016). Beyond range proofs, Bulletproofs provide short zero-knowledge proofs for general arithmetic circuits while only relying on the discrete logarithm assumption and without requiring a trusted setup. We discuss many applications that would benefit from Bulletproofs, primarily in the area of cryptocurrencies. The efficiency of Bulletproofs is particularly well suited for the distributed and trustless nature of blockchains. The full version of this article is available on ePrint.

**3. Making Sigma-Protocols Non-interactive Without Random Oracles**

Pyrros Chaidos, Jens Groth Published in International Conference on… 30 March 2015

Damgard, Fazio and Nicolosi (TCC 2006) gave a transformation of Sigma-protocols, 3-move honest verifier zero-knowledge proofs, into efficient non-interactive zero-knowledge arguments for a designated verifier. Their transformation uses additively homomorphic encryption to encrypt the verifier's challenge, which the prover uses to compute an encrypted answer. The transformation does not rely on the random oracle model but proving soundness requires a complexity leveraging assumption.

**IMPLEMENTATION**

Modules

Service Provider

In this module, the Service Provider has to login by using valid user name and password. After login successful he can do some operations such as Login, Browse Data Sets and Train & Test, View Trained and Tested Accuracy in Bar Chart, View Trained and Tested Accuracy Results, View All Antifraud Model for Internet Loan Prediction, Find Internet Loan Prediction Type Ratio, View Primary Stage Diabetic Prediction Ratio Results, Download Predicted Data Sets, View All Remote Users.

View and Authorize Users

In this module, the admin can view the list of users who all registered. In this, the admin can view the user's details such as, user name, email, address and admin authorizes the users.

Remote User

In this module, there are n numbers of users are present. User should register before doing any operations. Once user registers, their details will be stored to the database. After registration successful, he has to login by using authorized user name and password. Once Login is successful user will do some operations like REGISTER AND LOGIN, PREDICT PRIMARY STAGE DIABETIC STATUS, VIEW YOUR PROFILE.

## CONCLUSION

Credit score is increasingly been used in a number of countries and context, as a key determinant of one's (credit) worth in a credit system. To mitigate limitation of existing risk models, we focused on privacy protection of CSC in this article. Specifically, we designed a PCSC system and described its security requirements (i.e., weight confidentiality and credit confidentiality). To the best of authors' knowledge, this is the first such system with formal security definitions. We then presented a concrete construction based on Paillier encryption, with three purposefully designed NIZK schemes. We also gave the security proof of the proposal and evaluated its performance to demonstrate feasibility. However, the size of PIW and PED proofs increases significantly as the number of credit data items increases. This incurs significant storage and communication costs. Therefore, in our future research, we intend to enhance the design by having a constant proof size for better supporting the PCSC system.

## REFERENCES

[1] Z. Wang, S. Yan, and C. Zhang, "Active learning with adaptive regularization," Pattern Recognit., vol. 44, no. 10/11, pp. 2375–2383, 2011.

[2] B. Gutierrez-Nieto, C. Serrano-Cinca, and J. Camon-Cala, "A credit score system for socially responsible lending," J. Bus. Ethics, vol. 133, no. 4, pp. 691–701, 2016.

[3] L. Thomas, J. Crook, and D. Edelman, Credit Scoring and its Applications, vol. 2. Philadelphia, PA, USA: SIAM, 2017.

[4] R. Zeidan, C. Boechat, and A. Fleury, "Developing a sustainability credit score system," J. Bus. Ethics, vol. 127, no. 2, pp. 283–296, 2015.

[5] L. Zhou, K. K. Lai, and L. Yu, "Least squares support vector machines ensemble models for credit scoring," Expert Syst. Appl., vol. 37, no. 1, pp. 127–133, 2010.

[6] Y. Li, J. Gao, A. Z. Enkavi, L. Zaval, E. U.Weber, and E. J. Johnson, "Sound credit scores and financial decisions despite cognitive aging," Proc. Nat. Acad. Sci. USA, vol. 112, no. 1, pp. 65–69, 2015.

[7] G. N. Masters, "Partial credit model," in Handbook of Item Response Theory, vol. 1. London, U.K.: Chapman & Hall, 2016, pp. 137–154.

[8] S. Y. Sohn, D. H. Kim, and J. H. Yoon, "Technology credit scoring model with fuzzy logistic regression," Appl. Soft Comput., vol. 43, pp. 150–158, 2016. Authorized licensed use limited to: Carleton University. Downloaded on June 03,2021 at 06:32:51 UTC from IEEE Xplore. Restrictions apply. This article has been accepted for inclusion in a future issue of this journal. Content is final as presented, with the exception of pagination. 10 IEEE SYSTEMS JOURNAL

[9] H. J. Smith, T. Dinev, and H. Xu, "Information privacy research: An interdisciplinary review," MIS Quart., vol. 35, no. 4, pp. 989–1015, 2011.

[10] D. Malandrino and V. Scarano, "Privacy leakage on the web: Diffusion and countermeasures," Comput. Netw., vol. 57, no. 14, pp. 2833–2855, 2013.

[11] Y. Li, W. Dai, Z. Ming, and M. Qiu, “Privacy protection for preventing data over-collection in smart city,” IEEE Trans. Comput., vol. 65, no. 5, pp. 1339–1350, May 2016.

[12] D. Malkhi, N. Nisan, B. Pinkas, and Y. Sella, “Fairplay—A secure twoparty computation system,” in Proc. 13th Conf. USENIX Secur. Symp., vol. 13, no. 1, pp. 1–20, 2004.

[13] Y. Huang, D. Evans, J. Katz, and L. Malka, “Faster secure two-party computation using garbled circuits,” in Proc. 20th USENIX Secur. Symp., San Francisco, CA, USA, no.1, pp. 1–35, 2011.

[14] M. J. Freedman, K. Nissim, and B. Pinkas, “Efficient private matching and set intersection,” in Proc. Int. Conf. Theory Appl. Cryptographic Techn., 2004, pp. 1–19.

[15] B. Goethals, S. Laur, H. Lipmaa, and T. Mielikäinen, “On private scalar product computation for privacy-preserving data mining,” in Proc. 7th Int. Conf. Inf. Secur. Cryptology., Seoul, South Korea, 2004, pp. 104–120.

[16] R. Dowsley, J. van de Graaf, D. Marques, and A. C. A. Nascimento, “A two-party protocol with trusted initializer for computing the inner product,” in Proc. 11th Int. Workshop Inf. Secur. Appl., Jeju Island, South Korea, Aug. 2010 pp. 337–350.

[17] C. Gentry and D. Boneh, A Fully Homomorphic Encryption Scheme, vol. 20. Stanford, CA, USA: Stanford Univ. Press, 2009.

[18] M. van Dijk, C. Gentry, S. Halevi, and V. Vaikuntanathan, “Fully homomorphic encryption over the integers,” in Proc. 29th Annu. Int. Conf. Theory Appl. Cryptographic Techn., 2010, pp. 24–43.

[19] U. Feige, A. Fiat, and A. Shamir, “Zero-knowledge proofs of identity,” J. Cryptology, vol. 1, no. 2, pp. 77–94, 1988.

[20] I. Damgård, “On σ-protocols,” Lecture Notes, Dept. Comput. Sci., Univ. Aarhus, Aarhus, Denmark, 2002