# 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 incur 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.