SCIS 2022 2022 Symposium on Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics, Information and Communication Engineers

金銭的ペナルティに基づく公平な秘密計算におけるラウンド数の改善
Improving Round Complexity in Secure Computation with Penalties

中井 雄士 * 品川 和雅 †‡
Takeshi Nakai Kazumasa Shinagawa

キーワード 秘密計算, 公平性, ビットコイン

あらまし

秘密計算は，複数の参加者がそれぞれ持つ情報を秘匿したまま，参加者同士で協調してそれらの情報を入力値とした関数の計算を行う暗号技術である．公平性とは，攻撃者のみが出力値を得てアボートするような攻撃ができないことを要求する，秘密計算における重要な安全性の一つである．しかし，通常の秘密計算のモデルでは，公平性は Honest Majority を満たさなければ達成できないことが知られている．

ビットコインをベースに秘密計算を構成し，出力値を得てアボートしたパーティに対し金銭的なペナルティを課し honest なパーティには補償金を与えることで，公平性の達成を目指す研究分野が存在する．Bentov と Kumaresan [1] は，このような秘密計算を「金銭的ペナルティに基づく秘密計算 (secure computation with penalties)」として定式化した．また，同研究においてビットコインによる構成を想定した条件付送金の理想機能 $\mathcal{F}_{\mathrm{CR}}^{*}$ を定義し，$(\mathcal{F}_{\mathrm{OT}}, \mathcal{F}_{\mathrm{CR}}^{*})$-hybrid モデルにおいて，金銭的ペナルティに基づく秘密計算を任意の関数に対し，$O(n)$-round，$O(n)$-broadcast で実現できることを示した ($\mathcal{F}_{\mathrm{OT}}$ は紛失通信の理想機能を表す)．その後，Kumaresan と Bentov [2] は，ビットコインで実装できる新たな理想機能 $\mathcal{F}_{\mathrm{ML}}^{*}$ を定義し，$(\mathcal{F}_{\mathrm{OT}}, \mathcal{F}_{\mathrm{ML}}^{*})$-hybrid モデルにおいて，$O(1)$-round，$O(n^2)$-broadcast で金銭的ペナルティに基づく秘密計算を実現できることを示した．彼らは同研究の中で以下のような未解決問題を示した．

金銭的ペナルティに基づく秘密計算を $O(1)$-round，$O(n)$-broadcast で実現できるであろうか．

本研究では，金銭的ペナルティに基づく秘密計算における要求条件を僅かに緩めた「非等価な金銭的ペナルティに基づく秘密計算 (secure computation with non-equivalent penalties)」を提案する．従来の金銭的ペナルティに基づく秘密計算では，攻撃者に対しペナルティが発生した際，各 honest なパーティが同額の補償金を得られることを要求する．一方，本研究が提案する非等価な金銭的ペナルティに基づく秘密計算では，攻撃者に対しペナルティが発生した際，各 honest なパーティが事前に確定した金額以上の補償金を受け取ることができることを要求する．つまり，すべての honest なパーティが一定額以上の補償金を得られることは保証するが，補償金額がパーティ毎に異なることを許容する．

本研究で，任意の関数について，非等価な金銭的ペナルティに基づく秘密計算を $(\mathcal{F}_{\mathrm{OT}}, \mathcal{F}_{\mathrm{CR}}^{*})$-hybrid モデルにおいて，$O(1)$-round，$O(n)$-broadcast を達成できることを示す．つまり，補償金に関する条件をわずかに緩めた設定の下で，上記の未解決問題に対しポジティブな解が得られることを示す．特に，金銭的ペナルティに基づく秘密計算の構成において重要な役割を果たす，秘密情報の公平な再構築プロトコル [1] のラウンド数の改善を行うことで，本成果を実現する．

* 電気通信大学, 〒 182-8585 東京都調布市調布ケ丘 1-5-1, The University of Electro-Communications, 1-5-1, Chofugaoka, Chofu-shi, Tokyo, 182-8585, Japan.
† 茨城大学, 〒 316-8511 茨城県日立市中成沢町 4-12-1. Ibaraki University, 4-12-1 Nakanarusawa, Hitachi, Ibaraki, 316-8511, Japan.
‡ 産業技術総合研究所, 〒 135-0064 東京都江東区青海 2-3-26, National Institute of Advanced Industrial Science and Technology (AIST), 2-3-26 Aomi, Koto-Ku, Tokyo, 135-0064, Japan

参考文献

[1] I. Bentov and R. Kumaresan, "How to use bitcoin to design fair protocols," in *Advances in Cryptology – CRYPTO 2014* (J. A. Garay and R. Gennaro, eds.), (Berlin, Heidelberg), pp. 421–439, Springer Berlin Heidelberg, 2014.

[2] R. Kumaresan and I. Bentov, "How to use bitcoin to incentivize correct computations," in *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, CCS '14, (New York, NY, USA), p. 30–41, Association for Computing Machinery, 2014.