1X-04

ブロックチェーン上で適用可能な秘密計算方式の提案

吉田 祥悟 †　　塚田 恭章 ‡
関東学院大学 †　　関東学院大学 ‡

1　はじめに

本稿では, 特定の第三者を必要としないブロックチェーンに, 同じく特定の第三者を必要とせず秘密情報を秘匿することが可能な秘密分散技術を用いることで, 秘匿したい情報をブロックチェーン上で安全に運用する方式を提案する. さらに, 情報を秘匿したまま利活用する秘密計算を拡張し, ブロックチェーン上で適用できる新たな秘密計算方式を提案する.

2　提案方式：安全な秘密鍵の運用

提案方式の全体構成を図 1 に示す. 関連研究 [1][2] と同様, 公開可能な情報はブロックチェーンにより運用管理される. 暗号化された情報は分散ハッシュテーブルに格納される.

2.1　分散ハッシュテーブル

分散ハッシュテーブルは, 各ユーザ A が自身の個人情報を ElGamal 暗号で暗号化した暗号文 c_A と署名用公開鍵 pk_{sig}^A を登録する目的で利用される. この時, 分散ハッシュテーブル上の登録先アドレスとして, 対応する暗号文およびユーザの署名用公開鍵から生成されたハッシュ値を利用する.

$$h_A = H(c_A||pk_{sig}^A)$$

2.2　秘密鍵の分散管理

暗号文復号用の秘密鍵を含む情報をブロックチェーン上で分散管理することで, より安全なプライバシ保護ブロックチェーンモデルを提案する. ユーザ A の秘密鍵を s_A, 平文を m_A, 十分に大きな素数 p に対する原始元を g とし, 乱数を r_A とする. このとき, p と g は公開されすべてのユーザの暗号化に用いられる.

ユーザ A は, 自身の暗号文 $c_A := m_A g^{r_A s_A}$ を分散

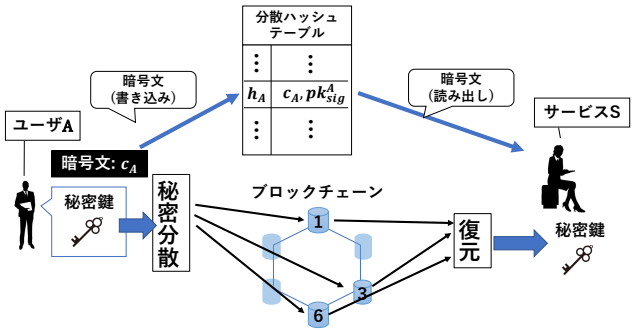

図 1　提案方式の全体構成

ハッシュテーブル上に保存する. その後, ユーザ A は, 自身の秘密鍵を含む情報, および異なる鍵同士での秘密計算を可能にするために必要な情報を以下の手順で秘密分散し, n 台のノードに送る. なお, 本提案方式では秘密分散として Shamir の (k, n) しきい値法を用いる.

1. ユーザ A は, $\mathbf{Z}/p\mathbf{Z}$ からランダムに k 個の乱数 $d_{A_1}, \ldots, d_{A_k}$ を選ぶ.
2. k 個の乱数 $d_{A_1}, \ldots, d_{A_k}$ より,
$$d_A = \sum_{i=1}^{k} d_{A_i} \mod p$$
を計算する.
3. d_A から, $g^{r_A(s_A+d_A)}$, $g^{r_A d_A}$ を計算し, さらに, $d_{A_1}, \ldots, d_{A_k}$ から $g^{r_A d_{A_1}}, \ldots, g^{r_A d_{A_k}}$ を計算し求める. その後, $g^{r_A(s_A+d_A)}$ を公開情報とする.
4. $g^{r_A d_A}$, $g^{r_A d_{A_1}}, \ldots, g^{r_A d_{A_k}}$ をそれぞれ秘密分散し, 各ノード N_i に分散値集合 $(\langle g^{r_A d_A}\rangle_i, \langle g^{r_A d_{A_1}}\rangle_i, \ldots, \langle g^{r_A d_{A_k}}\rangle_i)(i = 1, \ldots, n)$ を配布する.

サービスは復号クエリをブロックチェーン上に送る. その後, k 台のノードが対応する分散情報および暗号文から以下を計算し, その結果を復元クエリを依頼したサービスに送る.

$$m_A g^{r_A s_A} \times (g_A^{r_A(s_A+d_A)})^{-1} = m_A / g^{r_A d_A}$$

A Proposal for a Secure Computation Method Applicable on the Blockchain
† Shogo Yoshida, Kanto Gakuin University
‡ Yasuyuki Tsukada, Kanto Gakuin University

$$m_A/g^{r_A d_A} \times \langle g^{r_A d_A} \rangle_i = \langle m_A \rangle_i$$

計算結果より, サービスは直接 m_A を復元することができる.

3 提案方式：秘密計算

神宮ら [3] が提案した秘密計算方式では, 次数変化のない秘密計算を可能にしている. 本研究が提案する方式も, 同様に乗算時の復元に必要なノードの台数の増加を抑えている. 一方, [3] の方式では, 計算の途中結果を各サーバから集め復元する処理があり, 信頼できるディーラを設定する必要がある. ブロックチェーンでの利用を想定した場合, ディーラの設定は単一障害点を生むリスクがあると考えられる. 本研究で提案する秘密計算方式は, 計算過程において, 信頼できるディーラを必要としない. これらの特徴により, ブロックチェーン上での運用に適した秘密計算方式であるといえる.

3.1 乗算

1. 復元者である S_1 は,
$$g^{r_B(s_B+d_B)} \times g^{r_A(s_A+d_A)} = g^{r_A(s_A+d_A)+r_B(s_B+d_B)}$$
を計算する.
2. S_1 は暗号文同士を乗算しそれらを用いて以下の計算を行う
$$m_A m_B g^{r_A s_A + r_B s_B} \times (g^{r_A(s_A+d_A)+r_B(s_B+d_B)})^{-1} = m_A m_B / g^{r_A d_A + r_B d_B}$$
3. 任意の k 台のノード N_j $(1 \leq j \leq k)$ は,
$$(\langle g^{r_A d_{A_j}} \rangle_{n_1}, \ldots, \langle g^{r_A d_{A_j}} \rangle_{n_k}),$$
$$(\langle g^{r_B d_{B_j}} \rangle_{n_1}, \ldots, \langle g^{r_B d_{B_j}} \rangle_{n_k})$$
を k 台のノードから集め $g^{r_A d_{A_j}}$, $g^{r_B d_{B_j}}$ を復元する.
4. N_j は, $g^{r_A d_{A_j}} \times g^{r_B d_{B_j}}$ を計算し, サービス S_1 に送る.

乗算結果を復元する際には, k 台のノードからサービス S_1 が受け取った上記の計算結果を用いる. S_1 は, k 個の計算結果から

$$g^{r_A d_A + r_B d_B} = \prod_{j=1}^{k} g^{r_A d_{A_j} + r_B d_{B_j}}$$

を計算し,

$$m_A m_B / g^{r_A d_A + r_B d_B} \times g^{r_A d_A + r_B d_B} = m_A m_B$$

を求める. 以上より, 平文同士の乗算結果である $m_A m_B$ が得られる.

3.2 加減算

1. N_i は,
$$m_A g^{r_A s_A} \times (g^{r_A(s_A+d_A)})^{-1} = m_A / g^{r_A d_A}$$
を計算し, さらに,
$$m_A/g^{r_A d_A} \times \langle g^{r_A d_A} \rangle_i = \langle m_A \rangle_i$$
を計算する.
2. 同様に $\langle m_B \rangle_i$ を求めることで N_i は,
$$\langle m_A \rangle_i \pm \langle m_B \rangle_i = \langle m_A \pm m_B \rangle_i$$
を計算する.

加減算結果を復元する際には, k 台のノード N_j からサービス S_1 へ $\langle m_A \pm m_B \rangle_i$ を送る. S_1 は, 受け取った分散情報から $m_A \pm m_B$ を復元する.

4 まとめ

本研究では, 秘密鍵に秘密分散を施し, ブロックチェーン上で安全に秘密鍵を運用する方式を提案した. また, この秘密鍵の分散情報を用いる秘密計算とElGamal 暗号をベースとした準同型暗号を組み合わせることにより, ディーラを必要とせず乗算時の次数変化のない演算を可能とする新たな秘密計算方式を提案した. この計算方式は, お互いに信頼しないノードで構成されるブロックチェーン上で運用することが可能である.

参考文献

[1] Guy Zyskind, Oz Nathan, and Alex Pentland. Decentralizing privacy: Using blockchain to protect personal data. In *2015 IEEE Security and Privacy Workshops*, pp.180–184. IEEE, 2015.

[2] 今田丈雅, 松浦幹太. ブロックチェーンと秘密分散法を用いた情報ライフサイクル制御. コンピュータセキュリティシンポジウム 2017 論文集, 2017.

[3] 神宮武志, 青井健, ムハンマド カマル アフマド アクマル アミヌディン, 岩村恵市. 秘密分散法を用いた次数変化のない秘匿計算法. **情報処理学会論文誌**, 59(3):1038–1049, 2018.