属性ベース署名を用いたブロックチェーン

川合 豊[1] 小関 義博[1] 柴田 陽一[1] 大松 史生[1]

A Blockchain Protocol using Attribute-Based Signatures

Yutaka Kawai[1] Yoshihiro Koseki[1] Yoichi Shibata[1] Fumio Omatsu[1]

1. 初めに

1.1 背景

ブロックチェーンは、Bitcoin [2] において、P2P ネットワーク上のユーザ間のみの通信によってプロトコルを実現するために提案されたもので、ネットワーク上で過去に行われたすべての取引（トランザクション）を記録した「分散管理台帳」となっている。ブロックチェーンは、ディジタル署名を利用しユーザ間での取引記録を複数まとめたブロックをハッシュ関数により連鎖させることで、連続した取引記録の集合である元帳の改ざんを防ぐとともに、互いに信頼できない複数のユーザ間で元帳を分散管理する技術である。各取引の正当性は取引元ユーザのディジタル署名を検証することによって可能となる。上記のようにディジタル署名を検証することで、第三者によって取引内容の偽造や改ざんがされていないことの検証・成りすまし防止・否認防止、が可能となっている。

1.2 動機

ブロックチェーンは、ディジタル署名の能力によって取引履歴の正当性を保障し、改ざんを防止している。しかしながら、ディジタル署名の性質上、複数人と取引を行う場合（Bitcoin であれば、複数人に対して共通に使用できる Bitcoin を配布するなど)、複数の公開鍵に対して署名を生成する必要があり、取引する全てのユーザの公開鍵を事前に収集する必要がある。加えて、どの公開鍵に対して取引をしたか記録されるという匿名性上の問題がある。

1.3 貢献

本稿では、複数のユーザからなるグループ間でブロックチェーンによる取引において、匿名性確保と、複数の公開鍵をブロックチェーン上に記録する必要がない方式を検討する。具体的には、ディジタル署名の代わりに、属性ベース署名 [1], [3], [4] を用いて達成する。

[1] 三菱電機株式会社 情報技術総合研究所 情報セキュリティ技術部
Kawai.Yutaka@da.MitsubishiElectric.co.jp

2. ブロックチェーンとディジタル署名

2.1 ブロックチェーン

ブロックチェーンとは、ある順序づけられたレコード（これをブロックと呼ぶ）に前のレコードと何かしらのリンクを持たせることで、連続的に関連付けられた分散データベースである。ブロックを連鎖させることにより、すでに記録されたブロックが改変されたことを検知することが可能であり、ブロックの改ざん防止が可能となっている。具体的には、各ブロックには、チェーンの前のブロックのハッシュ値が入っており、ブロックが改ざんされるとハッシュ値が変化することを利用している。ブロックチェーンは、サトシナカモトにより Bitcoin において分散管理台帳を実現するために提案された。

2.2 ディジタル署名

ディジタル署名とは、の偽造や改ざんがされていないことの検証・成りすまし防止・否認防止等が可能な暗号技術であり、次のようなアルゴリズムから構成される。

DS.KG セキュリティパラメータ k（例えば鍵のビット長など）を入力とし、公開鍵と秘密鍵のペア $(\mathsf{pk}, \mathsf{sk})$ を出力する確率的アルゴリズム。

DS.Sign メッセージ m、秘密鍵 sk、を入力として、署名 σ を出力する確率的アルゴリズム。

DS.Ver メッセージ m、公開鍵 pk、署名 σ を入力とし、署名 σ が正当であれば 1 を、不正であれば 0 を出力する決定的アルゴリズム。

ディジタル署名の安全性. 安全なディジタル署名とは、直感的には、秘密鍵を持たないユーザが、メッセージとその正当な署名のペア (m, σ)（つまり $1 \leftarrow \mathsf{DS.Ver}(m, pk, \sigma)$ となる m と σ）を生成できない偽造不可能性を持つ方式の事

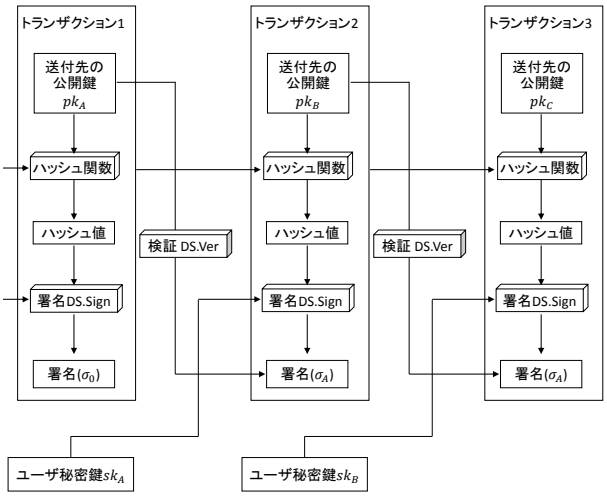

図 1 トランザクション内のディジタル署名の使われ方

を指す。

2.3 ブロックチェーンとディジタル署名

Bitcoin などで用いられるブロックチェーンの各ブロックはトランザクションの集まりからなる。トランザクションにおいて、ディジタル署名を用いることで改ざんや成りすましを防いでいる。トランザクションには、取引内容が記載されており、その取引内容が正当であることをディジタル署名を用いて保証する。例えば、ユーザ A からユーザ B に対する取引内容をトランザクションに記述する場合、ユーザ A はディジタル署名の公開鍵 $(\mathsf{pk}_A, \mathsf{sk}_A)$ を生成し、sk_A を用いて取引内容に対して署名 σ を生成する。トランザクションには送付先のユーザ B のアドレス、取引内容、そしてそれら対する署名 σ を記入する。この署名を検証することでトランザクションがユーザ A からユーザ B に対するものであることや、取引内容が改ざんされていないことなどを検証することができる。

3. 属性ベース署名

本章では属性ベース署名 (Attribute Based Signature, ABE) について説明する。属性ベース署名は、通常のディジタル署名と異なり、秘密鍵に “属性集合”、署名に “アクセス条件” が埋め込まれている。そして、署名検証では “アクセス条件を満たすような属性集合を持つ秘密鍵で生成された署名” であることのみを検証できる。属性集合とは属性の集まりであり、所属や肩書などの情報の集まりである。アクセス条件は、例えば論理式であらわされる条件式などを指す。属性ベース署名のアルゴリズムは以下のようなる。

ABS.Setup: セキュリティパラメータを入力として、マスター秘密鍵 msk、公開鍵 pk を出力する確率的アルゴリズム。

ABS.KG 属性の集合 Γ、公開鍵 pk、マスター秘密鍵 msk を入力とし、Γ と対応したユーザ秘密鍵 sk_Γ を出力する確率的アルゴリズム。

ABS.Sign メッセージ m、署名鍵 sk_Γ、Γ を受理するようなアクセス条件 $\mathcal{S}$、公開鍵 pk を入力とし、署名 σ を出力する確率的アルゴリズム。

ABS.Ver メッセージ m、アクセス条件 $\mathcal{S}$、公開鍵 pk、署名 σ を入力とし、署名 σ が正当であれば 1 を、不正であれば 0 を出力する決定的アルゴリズム。

属性ベース署名の完全性. 上記属性ベース署名は、任意の $(\mathsf{msk}, \mathsf{pk}) \leftarrow \mathsf{ABS.Setup}(1^k)$、任意のメッセージ m、任意の属性集合 Γ、そして Γ に対するユーザ秘密鍵 $\mathsf{sk}_\Gamma \leftarrow \mathsf{ABS.KG}(\mathsf{msk}, \Gamma)$、任意の Γ を満たすようなアクセス条件 $\mathcal{S}$ と、それらから生成される任意の署名 $\sigma \leftarrow \mathsf{ABS.Sign}(\mathsf{pk}, \mathsf{sk}_\Gamma, \mathcal{S}, m)$ に対して、確率 1 で $1 \leftarrow \mathsf{ABS.Ver}(\mathsf{pk}, \sigma, m, \mathcal{S})$ となる。

属性ベース署名の安全性. 属性ベース署名の安全性は、秘密鍵を持たないユーザが署名を生成できない偽造不可能性と、署名からでは署名生成時の属性 Γ がわからない完全匿名性がある。偽造不可能性とは、$\mathcal{S}$ を受理するような属性 Γ のユーザ秘密鍵 sk_Γ を持たない攻撃者が、$1 \leftarrow \mathsf{ABS.Ver}(\mathsf{pk}, \sigma, m, \mathcal{S})$ となるようなメッセージと署名のペア (m, σ) を偽造できないことを指す。完全匿名性とは、2 つの属性に対するユーザ秘密鍵 $\mathsf{sk}_{\Gamma_1}, \mathsf{sk}_{\Gamma_2}$、及びそれぞれの属性を受理するようなアクセス条件 $\mathcal{S}$ に対して作られた、2 つの署名 $\sigma_1 \leftarrow \mathsf{ABS.Sign}(\mathsf{pk}, \mathsf{sk}_{\Gamma_1}, \mathcal{S}, m)$ と $\sigma_2 \leftarrow \mathsf{ABS.Sign}(\mathsf{pk}, \mathsf{sk}_{\Gamma_2}, \mathcal{S}, m)$ の見分けがつかないことを指す。つまり、完全匿名性は、属性ベース署名の署名 σ からは属性情報 Γ が漏れないことを意味する。

具体的イメージ. ここでは属性ベース署名の利用例を示す。属性集合 Γ として $\Gamma = \{$A 部、1 課、課長、女性 $\}$ という属性を考える。属性集合 Γ を持つユーザは、ABS.Setup にて、属性集合に対してユーザ秘密鍵 sk_Γ が発行される。次に、このユーザはメッセージ m に対して署名を生成する。この際に、アクセス条件 $\mathcal{S}$ として、「(A 部 or B 部) and 課長以上)」という条件式を設定し、メッセージ m に対して署名 σ を生成する。ここで、Γ は $\mathcal{S}$ を満たすため、正しく署名を生成することができる。この署名 σ は、メッセージ m、アクセス条件 $\mathcal{S}$ を元に検証を行う。ここで検証者は、アクセス条件 $\mathcal{S}$ を満たす属性を持つユーザが署名を生成したことまでは分かるが、属性集合 Γ に関する情報はそれ以上漏れない。

4. 属性ベース署名を用いたブロックチェーン

本章では、前章で説明した属性ベース署名をブロックチェーンに図 2 に示す。各トランザクションには、従来公開鍵の代わりに、公開鍵 pk と送付先のアクセス条件 $\mathcal{S}$ を

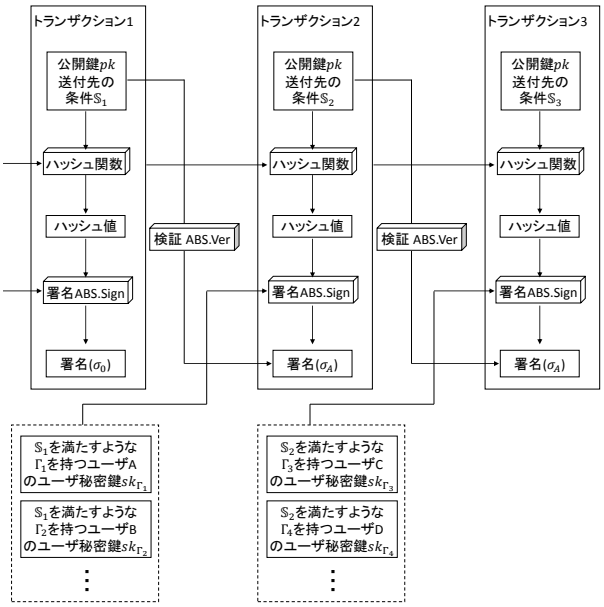

図 2 提案方式概念図

挿入する[*1]。

- 属性 Γ を持つユーザ A は、Γ から生成されたユーザ秘密鍵 sk_Γ を受け取る。
- ユーザ A は取引を行うユーザの集合をアクセス条件 $\mathcal{S}'$ で指定する。
- 取引内容、及び $\mathcal{S}'$ をメッセージとして、sk_Γ、Γ が満たすようなアクセス条件 $\mathcal{S}$ を入力として属性ベース署名 σ を生成し、トランザクションの中に含める。
- 属性ベース署名 σ は、属性ベースの検証 $\mathsf{ABS.Ver}(m, \mathsf{pk}, \mathcal{S})$ によって正当性を検証することができる

属性ベースの性質上、特定のユーザではなく、アクセス条件 $\mathcal{S}'$ を満たすユーザに対して署名を生成できるため、複数のユーザからなるグループ間の取引をトランザクションに記述することができる。加えて、属性ベース署名の特性上、署名 σ からは $\mathcal{S}$ の条件を満たす誰かが署名したことしかわからないため、匿名性を担保することができる。

5. まとめ

本稿では、属性ベース署名を用いることで複数のユーザからなるグループ間でブロックチェーンによる取引を実現できることを示した。加えて属性ベース署名の持つ “完全匿名性” により、ブロックチェーンの一つの問題とされている匿名性の問題も解消することができる。

参考文献

[1] J. Li, M. H. Au, W. Susilo, D. Xie, and K. Ren. Attribute-based signature and its applications. In *ASIACCS 2010*, pages 60–69. ACM, 2010.

[2] S. Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. In https://bitcoin.org/bitcoin.pdf, 2008.

[3] T. Okamoto and K. Takashima. Efficient Attribute-Based Signatures for Non-Monotone Predicates in the Standard Model. In *Public Key Cryptography - PKC 2011*, volume 6571 of *LNCS*, pages 35–52. Springer, 2011.

[4] G. Shanqing and Z. Yingpei. Attribute-based signature scheme. In *Information Security and Assurance - ISA 2008*, pages 509–511. IEEE, 2008.

[*1] もし、全体で同じシステムパラメータしか用いないのであれば pk は必要ない。