検証者の秘密鍵を必要としない情報理論的に安全なブラインド認証方式

武井 教泰　　渡邉 洋平　　四方 順司

横浜国立大学大学院環境情報学府/研究院
240-8501 神奈川県横浜市保土ヶ谷区常盤台 79-7
{takei-noriyasu-mx, watanabe-yohei-xs, shikata}@ynu.ac.jp

あらまし ブラインド認証を実現する情報理論的に安全なプロトコルとしてブラインド認証方式 (BA-code) が提案されているが, ユーザ・認証子生成者・検証者がそれぞれ秘密鍵を持つ必要がある. 一方, Manual Channel モデルでは 2 者間で秘密情報を共有することなくメッセージ認証を実現することが可能である. 本稿では, Manual Channel モデルを利用した情報理論的に安全な BA-code を提案する. 具体的には, その数理モデル, 安全性の定式化, 構成法を示す. 本稿で提案する BA-code では, 検証者が秘密鍵なしで検証可能であり, そのためユーザは認証子を得た後に自由に検証者を選ぶことができるという利点をもつ.

Unconditionally Secure Blind Authentication Codes without Verifier's Secret Keys

Noriyasu Takei　　Yohei Watanabe　　Junji Shikata

Graduate School of Environment and Information Sciences,
Yokohama National University,
79-7 Tokiwadai, Hodogaya-ku, Yokohama, Kanagawa 240-8501, Japan
{takei-noriyasu-mx, yohei-watanabe-xs, shikata}@ynu.ac.jp

Abstract In this paper, we propose unconditionally secure blind authentication codes in the manual channel model (BA-codes in MC) in which a verifier can verify the validity of any authenticated message without his secret key. Specifically, we propose a model and a security definition of BA-codes in MC. Furthermore, we show a direct construction of BA-codes in MC. It should be noted that in our model it enables a user to arbitrarily select a verifier after getting an authenticated message from a signer, since a verifier needs no secret key.

1 はじめに

現在利用されている暗号技術の多くは計算量的安全性に基づいている. 計算量的安全性とは, 素因数分解問題や離散対数問題などの計算量的な問題の困難性に基づく安全性である. しかし, 近年の計算アルゴリズムやコンピュータ技術の発展を考慮すると, このような計算困難性に基づいた暗号技術では長期的な安全性を維持できない恐れがある. こうした理由から, 特に長期的な安全性を保証するため, 計算困難性によらない暗号技術を考える必要があり, そのようなものとして, 情報理論的に安全な暗号技術がある. 情報理論的安全性は計算量的な仮定を用いずに確率論や情報理論に基づいてその安全性を保証する. 情報理論的安全性に基づく暗号技術は計算量的安全性に基づく暗号技術に比べて一般的

に必要な記憶容量が多く，また全てのエンティティが自身の鍵を秘密に保持する必要がある．しかし計算量的な仮定を用いないために攻撃者の計算能力に関わらず定量的なセキュリティを長期間保証できるという利点がある．本稿では，情報理論的に安全な暗号プロトコルを扱う．

ブラインド認証とはユーザ第三者にメッセージの内容を見せずに署名（認証子）を生成してもらい，検証者がその検証をすることが可能な暗号プロトコルである．ブラインド認証は電子現金や電子投票などに利用され，電子現金ではユーザが誰がどこで何を買ったのかという情報を知られることなく金融機関から署名をもらい，商店で利用することができる．

ブラインド認証機能をもつ暗号技術として，初めに（計算量的に安全な）ブラインド署名が Chaum によって提案されている [2]．また，Pointcheval と Stern により [10] でランダムオラクルモデルにおけるブラインド署名が提案され，[6] ではスタンダードモデルにおけるブラインド署名が提案されている．また，情報理論的に安全なブラインド署名が原ら [3] によって提案されている．

一方で，2 者間での共通鍵を用いたブラインド認証を実現するプリミティブとして，計算量的に安全なものとしては Pinkas が Blind MAC [9] を，さらに情報理論的に安全なものとしては原らが Blind Authentication code(BA-code) [4] を提案している．[4] では，BA-code が情報理論的に安全な暗号化方式と A^2-code から一般に構成できることも示されている．A^2-code とは，情報理論的に安全な認証方式である A-code において送信者，または受信者の不正を考慮したものであり，詳しくは [7] や [5] などを参照されたい．

先にも述べたように，情報理論的に安全な暗号技術では各エンティティが自身の鍵を秘密に保持する必要があり，メッセージ認証技術 (A-code) においても同様である．近年，Vaudenay [12] によって，送信者と受信者が安全でない双方向通信路と一方向低容量通信路を利用するメッセージ認証用の通信モデルが提案された．このようなモデルを Manual Channel モデルといい，特に，一方向低容量通信路は Manual Channel と呼ばれる．攻撃者は Manual Channel 上のメッセージを盗聴, 遅延, 削除などを行うことが許されるが，改ざんを行うことは出来ないものとする．このような仮定は不自然ではなく，人がウインドウに表示された文字列をキーボードで入力したり，プリントアウトして運んだりといった何らかの現実的な操作を行うことが想定されている．例えば，Web で飛行機の予約を行った際に，最終的にプリンタでバーコードを印刷し，搭乗時にバーコードをかざすことで搭乗ゲートを通過することを Manual Channel の一例と見なすことが可能である．このように Manual Channel モデルは，現実社会でも応用例をもつ，一般的なモデルになってきており，無線 USB や Bluetooth における初期ペアリングなどでの利用が特にふさわしい例である．

理論研究においては，Manual Channel モデルを導入することで，ユーザ間の事前の鍵共有が必要ない A-code が提案されている [8]．情報理論的に安全な認証方式の最も基礎的なプリミティブは A-code であり，[8] の結果を，さらに複雑な構造をもつ認証システムに拡張することは重要である．ここで，ブラインド署名 [3] や BA-code[4] は，A-code よりも複雑な構造をもつ認証システムであり，これらのシステムにおいても，全エンティティが秘密鍵を保持する必要があった．秘密鍵を保持しなければならないエンティティの数を少なくすることは非常に有益であり，また中でも検証者の秘密鍵を無くすことができれば,（最初に決められたエンティティではなく）誰でも検証が可能となる．そこで本稿では，Manual Channel モデルを導入することで，検証者が自身の秘密鍵を必要としない BA-code の数理モデル，安全性の定式化，構成法の提案を行う．

2 準備

本節では，BA-code [4]，Manual Channel モデルにおける A-code [8] を紹介する．

2.1 BA-code のモデルと安全性

BA-code では，秘密鍵を生成し，それらを対応するエンティティに安全に配布する（信頼できる）第三者機関の存在を仮定する．これを TI モデル (Trusted Initializer モデル) という [11]．TI はプロトコルの開始時のみ登場し，各エンティティの代わりに秘密鍵を生成し，それらを対応するエンティティに安全に配送した後は登場しないエンティティである．

まず，モデルの概要を述べる．信頼機関 TI はユーザ，認証子生成者，検証者の秘密鍵を生成し，安全な通信路を通じて各エンティティに配布する．TI は配布後に鍵情報を消去し，各エンティティは自身の鍵を秘密に保持する．まず，ユーザはメッセージの内容を隠すために秘密鍵を用いてブラインドメッセージを生成し，認証子生成者へ送信する．認証子生成者はブラインドメッセージを受け取ると，秘密鍵を用いてブラインドメッセージに対する認証子（ブラインド認証子）を生成し，ユーザに返送する．ブラインド認証子を受け取ったユーザは，秘密鍵を用いて，ブラインド認証子から当初のメッセージに対する認証子を生成する．その後，まずユーザは秘密鍵を用いて生成した認証子の正当性を検証する．正当な認証子ならば，ユーザはメッセージと認証子を検証者へ送信する．検証者はユーザから情報を受け取った後，秘密鍵を用いてメッセージと認証子のペアが正当なものであるか検証する．正当なものである場合は受理し，そうでない場合は拒否する．[4] では，one-time モデルで考えられている．ここで one-time とは，認証子生成者が認証子を生成し，ユーザと検証者が検証を行う回数がそれぞれ 1 回のみであるということである．形式的な BA-code の定義は次の通りである．

定義 1 (BA-code). BA-code プロトコル Π は TI，S，U，V の 4 つのエンティティ，6 つのアルゴリズム (Gen，Blind，Sign，Unblind，UVer，VVer)，7 つの空間 M，M^*，Σ，M^*，E_S，E_U，E_V からなる．Gen 以外のアルゴリズムは全て決定的アルゴリズムであり，すべての空間は有限集合である．加えて，Π は次に示す 6 つのフェーズを実行する．

記法

- エンティティ: TI は信頼できる第三者機関，S は認証子生成者，U はユーザ，V は検証者である．
- 空間: M，M^*，Σ，Σ^*，E_U，E_S，E_V はそれぞれ，メッセージ，ブラインドメッセージ，認証子，ブラインド認証子，ユーザの秘密鍵，認証子生成者の秘密鍵，検証者の秘密鍵の集合である．
- アルゴリズム: Gen は鍵生成アルゴリズム，Blind: $M \times E_U \rightarrow M^*$ はブラインドメッセージ生成アルゴリズム，Sign: $M^* \times E_S \rightarrow \Sigma^*$ はブラインド認証子生成アルゴリズム，Unblind: $\Sigma^* \times E_U \rightarrow \Sigma$ は認証子生成アルゴリズム，UVer: $M \times \Sigma \times E_U \rightarrow \{true, false\}$ はユーザの検証アルゴリズム，Vver: $M \times \Sigma \times E_V \rightarrow \{true, false\}$ は検証者の検証アルゴリズムである．

鍵生成，鍵配布: 信頼機関 TI は Gen アルゴリズムを用いてユーザ U の秘密鍵 $e_u \in E_U$，認証子生成者 S の秘密鍵 $e_s \in E_S$，検証者 V の秘密鍵 $e_v \in E_V$ を生成し，安全な通信路により各エンティティに配布する．TI は配布後に鍵情報を消去し，各エンティティは自身の鍵を秘密に保持する．

ブラインドメッセージ生成: U はメッセージ $m \in M$ の内容を隠すために Blind アルゴリズムを用いて m と e_u からブラインドメッセージ $m^* = Blind(m, e_u) \in M^*$ を生成し，S へ m^* を送信する．

ブラインド認証子生成: S は受け取った m^* に対して Sign アルゴリズムを用いて e_s からブラインド認証子 $\sigma^* = Sign(m^*, e_s) \in \Sigma^*$ を生成し，U に (m^*, σ^*) を送信する．

認証子生成: σ^* を受け取った U は UnBlind アルゴリズムを用いて e_u から m に対する認証子 $\sigma = Unblind(\sigma^*, e_u) \in \Sigma$ を生成する．

ユーザによる検証: (m, σ) のペアを得た U は，その正当性を e_u を用いて UVer アルゴリズムにより検証する．$UVer(m, \sigma, e_u) = true$ のとき正当なものであるとみなして受理し，そうでな

い場合は拒否する．検証に受理した場合，U は (m, σ) のペアを V へ送信する．

検証者による検証: (m, σ) を得た V は，その正当性を e_v を用いて VVer アルゴリズムにより検証する．$VVer(m, \sigma, e_v) = true$ のとき正当なものであるとみなして受理し，そうでない場合は拒否する．

次に BA-code の安全性について述べる．BA-code では，Unforgeability，Undeniability，Blindness の 3 つの安全性を考えている．Unforgeability とは，ユーザ自身がメッセージに対する認証子を偽造できないという安全性であり，認証子生成者に認証子を生成してもらう前，すなわち正当なメッセージと認証子のペアを見ずに検証者に受理されるような不正なペアを生成する Impersonation Attack と，認証子生成者に認証子を生成してもらった後，すなわち正当なメッセージと認証子のペアを見た後に検証者に受理されるような不正なペアを生成する Substitution Attack を考える．Undeniability とは，認証子生成者が認証子を生成した事実を否認できないものとする安全性である．Blindness とは，認証子生成者がブラインドメッセージから元のメッセージを推測するのが困難であるという安全性である．これらの安全性は次のように定式化される．

定義 2 (BA-code の安全性). BA-code Π が以下に定義する $P_{\Pi,F}, P_{\Pi,D}, P_{\Pi,B}$ に対して，$\max(P_{\Pi,F}, P_{\Pi,D}, P_{\Pi,B}) \leq \epsilon$ を満たすとき，Π は ϵ-secure であるという．

1. *Unforgeability:* Impersonation Attack の攻撃成功確率を P_{Π,F_I} とし，P_{Π,F_I} を次のように定義する．

$$P_{\Pi,F_I} := \max_{e_u} \max_{(m,\sigma)} \Pr(\text{V accepts}(m, \sigma) \mid e_u).$$

Substitution Attack の攻撃成功確率を P_{Π,F_S} とし，P_{Π,F_S} を次のように定義する．

$$P_{\Pi,F_S} := \max_{e_u} \max_{(m,\sigma)} \max_{(m^*,\sigma^*)} \max_{(m',\sigma') \neq (m,\sigma)} \Pr(\text{V accepts}(m', \sigma') \mid e_u, (m, \sigma), (m^*, \sigma^*)).$$

また，$P_{\Pi,F} := \max(P_{\Pi,F_I}, P_{\Pi,F_S})$ とする．

2. *Undeniability:* 認証子生成者が，ユーザは受理するが検証者は拒否するような認証子を生成する攻撃を考える．その攻撃成功確率 $P_{\Pi,D}$ を次のように定義する．

$$P_{\Pi,D} := \max_{e_s} \max_{m^*} \max_{(m,\sigma)} Pr(\text{U accepts } (m, \sigma) \wedge \text{V rejects } (m, \sigma) \mid e_s, m^*)$$

3. *Blindness:* $P_{\Pi,B}$ を次のように定義する．

$$P_{\Pi,B} := \max_{e_s} \max_{m^*} \{ \sum_{m \in M} \mid Pr(m \mid e_s, m^*) - Pr(m) \mid \}$$

2.2 A-code in the Manual Channel Model のモデルと安全性

Manual Channel モデルを利用することで，事前に秘密鍵を共有する必要のない A-code を実現することができる．具体的には，送信者が受信者へメッセージを送信した後，両者は安全でない通信路を用いて複数回の相互通信を行う．最後に，Manual Channel と呼ばれる一方向低容量通信路を通じて送信者がある情報を受信者に送信する．その情報を用いて受信者はメッセージの正当性を検証する．これを A-code in the Manual Channel Model (A-code in MC) と呼び，モデルは以下のようになる．

モデル: 1 ラウンド目は送信者 S は受信者 R にメッセージ m と認証タグ x_1 を送信する．以降，偶数ラウンドは受信者から送信者へ，奇数ラウンドは送信者から受信者へ認証タグ x_i のみを送信し，これを $k-1$ ラウンド（k は奇数）まで繰り返す．その後，k ラウンド目には，S は Manual Channel を通じて文字列 s を送信し，R は認証を行う．

安全性は以下のように定義される．

定義 3 (A-code in MC の安全性). 上記の k ラウンドプロトコルが次の条件をみたすとき，unconditionally secure $(n, \lambda, k, \epsilon)$-authentication

protocol in the manual channel model という．ただし，メッセージを n ビット，Manual Channel の容量を λ ビットとする．

1. *Completeness:* 攻撃者の攻撃が一切行われていない正しい m を受信者が少なくとも 1/2 の確率で受理する．特に，確率 1 で受理する場合は，perfectly complete という．
2. *Unforgeability:* 無制限の計算能力を持つ攻撃者がメッセージ m を m' に改ざんしたとしても，受信者が m' を受理する確率が高々 ϵ である．

特に，perfectly complete であるとき，unconditionally perfectly secure $(n, \lambda, k, \epsilon)$- authentication protocol in the manual channel model という．

3 BA-code in the Manual Channel Model

本節では情報理論的に安全な Manual Channel モデルにおける BA-code (BA-code in MC) のモデル，安全性の定式化を提案する．

3.1 モデル

まず，モデルの概要を述べる．本方式は BA-code と同様，TI モデルを考え，大部分は BA-code と同様の流れで進む．信頼機関 TI はユーザと認証子生成者の秘密鍵を生成し，安全な通信路を通じてそれぞれに配布する．TI は配布後に鍵情報を消去し，ユーザと認証子生成者は自身の鍵を秘密に保持する．まず，ユーザはメッセージの内容を隠すために秘密鍵を用いてブラインドメッセージと，メッセージのコミット情報を生成し，これらを認証子生成者へ送信する．認証子生成者はブラインドメッセージとコミット情報を受け取ると，秘密鍵を用いてブラインドメッセージに対する認証子（ブラインド認証子）を生成し，ユーザに返送する．ブラインド認証子を受け取ったユーザは，秘密鍵を用いて，ブラインド認証子から当初のメッセージに対する認証子を生成する．その後，まずユーザは秘密鍵を用いて生成した認証子の正当性を検証する．正当な認証子ならば，ユーザは検証者を任意に選び，メッセージと認証子，更に自身の秘密鍵を検証者へ送信する．検証者はユーザから情報を受け取った後，まず認証子生成者へリクエストを出す．リクエストを受け取った認証子生成者は，自身の秘密鍵とメッセージのコミット情報を検証者へ送信する．この際の通信に Manual Channel モデルを利用する．その後，検証者は得られた全ての情報を用いて，ユーザからのメッセージと認証子のペアが正当なものであるかを検証し，正当なものである場合は受理し，そうでない場合は拒否する．BA-code と同様，本方式は one-time モデルとする．形式的な BA-code in MC の定義は次の通りである．ここで，ユーザは検証者をプロトコルの途中で任意に選ぶことが可能だが，以下では説明を簡単にするため，最初から検証者として V というエンティティを任意に選んで固定しておく．

定義 4 (BA-code in MC). BA-code in MC プロトコル Ψ は TI，S，U，V の 4 つのエンティティ，6 つのアルゴリズム (Gen，Blind，Sign，Unblind，UVer，VVer)，7 つの空間 M，M^*，Σ，Σ^*，Y，E_S，E_U からなる．Gen 以外のアルゴリズムは全て決定的アルゴリズムであり，すべての空間は有限集合である．加えて，Ψ は次に示す 7 つのフェーズを実行する．

記法

- エンティティ: BA-code と同様のエンティティが登場する．
- 空間: Y はコミット情報の集合であり，その他の集合は BA-code と同様である．
- アルゴリズム: Gen，Sign，Unblind，UVer は BA-code と同様のアルゴリズムであり，Blind: $M \times E_U \to (M^*, Y)$ はブラインドメッセージ生成アルゴリズム，Vver: $M \times \Sigma \times E_U \times E_S \times Y \to \{true, false\}$ は検証者の検証アルゴリズムである．

鍵生成，鍵配布: 信頼機関 TI は Gen アルゴリズムを用いてユーザ U の秘密鍵 $e_u \in E_U$，認証

子生成者 S の秘密鍵 $e_s \in E_S$ を生成し，安全な通信路により各エンティティに配布する．TI は配布後に鍵情報を消去し，各エンティティは自身の鍵を秘密に保持する．

ブラインドメッセージ生成: U はメッセージ $m \in M$ の内容を隠し，また第三者（検証者 V）にどのメッセージに対して S に認証子を生成してもらったのか証明するためのコミット情報を作成する．Blind アルゴリズムを用いて m と e_u からブラインドメッセージとメッセージのコミット情報のペア $(m^*, y) = Blind(m, e_u) \in M^* \times Y$ を生成し，S へ (m^*, y) を送信する．

ブラインド認証子生成: S は受け取った m^* に対して Sign アルゴリズムを用いてブラインド認証子 $\sigma^* = Sign(m^*, e_s) \in \Sigma^*$ を生成し，U に (m^*, σ^*) を返送する．また y は秘密に保持しておく．

認証子生成: σ^* を受け取った U は UnBlind アルゴリズムを用いて m に対する認証子 $\sigma = Unblind(\sigma^*, e_u) \in \Sigma$ を生成する．

ユーザによる検証: (m, σ) のペアを得た U は，その正当性を e_u を用いて UVer アルゴリズムにより検証する．$UVer(m, \sigma, e_u) = true$ のとき正当なものであるとみなして受理し，そうでない場合は拒否する．検証に受理した場合，U は (m, σ) と自身の鍵 e_u を V へ送信する．

Manual Channel Model を用いた通信: V は U から (m,σ)，e_u を受け取ると，S へと検証のための情報を送信してほしいというリクエストを出す．リクエストを受けた S は，自身の秘密鍵 e_s とユーザから受け取ったメッセージのコミット情報 y を定義 3 の A-code in the Manual Channel Model を用いて V へ送信する[1]．

検証者による検証: V は (m, σ) の正当性を e_u, e_s，y を用いて VVer アルゴリズムにより検証する．$VVer(m,\sigma, e_u, e_s, y) = true$ のとき (m,σ) のペアを正当なものであるとみなして受理し，そうでない場合は拒否する．

[1] この時，定義 3 におけるメッセージ m が (e_s, y) に対応する．

3.2 安全性

BA-code in MC では，Unforgeability，Blindness の 2 つの安全性について考える．ここで，BA-code の場合とは異なり，Undeniability は考えないことに注意されたい．その理由は，認証子生成者が認証子を生成した事実を否認する攻撃を考える場合，認証子生成者は検証者が検証に用いる情報全てを自由に改ざんすることが可能であり，Undeniability を理論的に実現出来ないからである．

Unforgeability に関しては，既存の BA-code の安全性定義（定義 2）と異なり，ユーザによる Substitution Attack のみを考える．Impersonation Attack を考えない理由として，本モデルでは認証子生成者と検証者間の通信が行われることから，検証者が認証子生成者に問い合せると，認証子生成者が認証子を生成していないことが明らかになるためである．

以上より，BA-code in MC の安全性の定式化を次のように定義する．

定義 5 (BA-code in MC の安全性). BA-code in MC Ψ が以下に定義する $P_{\Psi,F}$,$P_{\Psi,B}$ に対して $\max(P_{\Psi,F}, P_{\Psi,B}) \leq \delta$ を満たし，A-code in MC が unconditionally perfectly secure $(n, \lambda, k, \epsilon)$-authentication protocol であるとき，Ψ は $(n, \lambda, k, \epsilon, \delta)$-secure であるという．

1. *Unforgeability:* Substitution Attack の攻撃成功確率を $P_{\Psi,F}$ とし，$P_{\Psi,F}$ を次のように定義する．

$$P_{\Psi,F} := \max_{(m',\sigma')} \max_{(m',\sigma') \neq (m,\sigma)} \max_{e'_u} \max_{y} \Pr(VVer(m', \sigma', e'_u, e_s, y) = true \mid m, \sigma, e_u, y)$$

2. *Blindness:* $P_{\Pi,B}$ を次のように定義する．

$$P_{\Psi,B} := \max_{e_s} \max_{m^*} \max_{y} \{ \sum_{m \in M} \mid Pr(m \mid e_s, m^*, y) - Pr(m) \mid \}$$

4 構成法

本節では BA-codes in MC の具体的構成法を提案する．本構成は，A^2-code [7] とコミットメント [1] の構成法のアイデアを利用している．また，$GF(q)$ を要素数 q の有限体とする．以下では説明を省くが，構成における多くの要素は予め $GF(q)$ の元に符号化されていると仮定する．

Gen: セキュリティパラメータ 1^μ に対して，Gen は $e_1 = f_1 + e_3 f_3, e_2 = f_2 + e_4 f_3$ を満たすように $f = (f_1, f_2, f_3) \in GF(q)^3$，$e = (e_1, e_2, e_3, e_4) \in GF(q)^4$ をランダムに選択する．さらに，$y_1 = ax_1 + b$ を満たすように a，b，x_1，$y_1 \in GF(q)$ をランダムに選択し，$p \in GF(q)$ をランダムに選択する．ここで U の秘密鍵 $e_u = (f_1, f_2, f_3, a, b, p)$，S の秘密鍵 $e_s = (e_1, e_2, e_3, e_4, x_1, y_1)$ を出力する．

Blind: メッセージ $m \in GF(q)$，U の秘密鍵 e_u に対して，Blind はブラインドメッセージ $m^* = m + p$ とコミット情報 $y = m + a$ を計算し，出力する．

Sign: ブラインドメッセージ m^*，S の秘密鍵 e_s に対して，Sign は $(\sigma_1^*, \sigma_2^*) = (m^* e_3 + e_4, m^* e_1 + e_2)$ を計算し，ブラインド認証子 $\sigma^* = (\sigma_1^*, \sigma_2^*)$ を出力する．

Unblind: $\sigma := \sigma^*$ とする．つまり，Unblind は入力 $\sigma^* = (\sigma_1^*, \sigma_2^*)$ に対して，$(\sigma_1, \sigma_2) = (\sigma_1^*, \sigma_2^*)$ を出力する．

Uver: 認証子 σ と U の秘密鍵 e_u に対して，$\sigma_2 = m^* f_1 + f_2 + \sigma_1 f_3$ が成り立てば true を，そうでなければ false を出力する．

Manual Channel を用いての通信: [8] と同様に構成し，送信するメッセージ $\tilde{m} = (m_1, ..., m_k) \in GF(q)^k$ に対して，ハッシュ関数 $C_x(\tilde{m}) = \sum_{i=1}^{k} \tilde{m}_i x^i$ を利用する．ただし，以下ではラウンド数 $k = 7$ とし，文字列 u と v の連結を $\langle u, v \rangle$ と表記する．1 ラウンド目では S は $m_S^1 = (y, e_1, e_2, e_3, e_4, x_1, y_1) \in GF(q)^7$ を V へ送信し，V が受け取ったものを m_V^1 として表記する．その後，j ラウンド目 $(1 \leq j \leq 6)$ では以下の流れに従う．j が奇数のとき，S はランダムに i_S^j を選び V に送信し，V は $\hat{i_S^j}$ として受け取る．V はランダムに i_V^j を選び S に送信し，S は $\hat{i_V^j}$ として受け取る．情報を共有したのち，S は $m_S^{j+1} = \langle \hat{i_V^j}, C^j_{i_V^j}(m_S^j) + i_S^j \rangle$，V は $m_V^{j+1} = \langle i_V^j, C^j_{i_V^j}(m_V^j) + \hat{i_S^j} \rangle$ を計算する．j が偶数のとき，V はランダムに i_V^j を選び S に送信し，S は $\hat{i_V^j}$ として受け取る．S はランダムに i_S^j を選び V に送信し，V は $\hat{i_S^j}$ として受け取る．情報を共有したのち，S は $m_S^{j+1} = \langle i_S^j, C^j_{i_S^j}(m_S^j) + \hat{i_V^j} \rangle$，V は $m_V^{j+1} = \langle \hat{i_S^j}, C^j_{i_S^j}(m_V^j) + i_R^j \rangle$ を計算する．7 ラウンド目では S は Manual Channel を用いて m_S^7 を V に送信し，V は $m_S^7 = m_V^7$ であれば $m_S^1 = (y, e_1, e_2, e_3, e_4, x_1, y_1)$ を正しいメッセージとして受理する．

VVer: メッセージ m，認証子 σ，ユーザの秘密鍵 e_u，認証子生成者の秘密鍵 e_v，コミット情報 y に対して，VVer は $\sigma_2 = (m+p)f_1 + f_2 + \sigma_1 f_3$，$\sigma_1 = (m+p)e_3 + e_4$，$e_1 = f_1 + e_3 f_3$，$e_2 = f_2 + e_4 f_3$，$y = m + a$,$y_1 = ax_1 + b$ が全て成り立てば true を，そうでなければ false を出力する。

定理 1. 上記の BA-code in MC の構成法は $(n, \lambda, 7, \epsilon, \frac{1}{q})$-secure である．ただし，$n = \lfloor 7 \log q \rfloor$，$\lambda = \left\lceil 2 \log \frac{1}{\epsilon} + \log^{(6)} n \right\rceil$,$\epsilon = \frac{896 \log q}{q}$ である．

証明．A-code in MC が perfectly secure-$(n, \lambda, 7, \epsilon)$-authentication protocol であることは，[8] の TheoremIV.2 と同様に証明できる．次に $\delta \leq 1/q$ であることを示す．$P_{\Psi,B} = 0$ であることは [4] の定理 3 の証明と同様に証明できる．そこで，以下では $P_{\Psi,F} \leq 1/q$ であることを示す．不正なユーザが秘密鍵 e_u と正当なメッセージと認証子のペア (m, σ) を用いて，不正なメッセージと認証子のペア (m', σ') と秘密鍵 e_u' を生成することを考える．まず，ユーザは認証子生成者の秘密鍵 (e_1, e_2, e_3, e_4) を知らないため，$e_1 = f_1' + e_3 f_3'$，$e_2 = f_2' + e_4 f_3'$ を満たすような (f_1', f_2', f_3') を作成することは難しい．そのため，e_u を改ざんすることなく (m', σ') を生成することになる．そこで，(σ_1', σ_2') が (σ_1, σ_2) と等しくなるように，$m' + p' = m + p$ を満たすような p' を作成することを試みる．しかし，ユーザが $y = m' + a'$，$y_1 = a' x_1 + b'$ を満たすような b' を当てる確率

は $1/q$ 以下となる．そのため，$P_{\Psi,F} \leq 1/q$ である．よって,$\max(P_{\Psi,F}, P_{\Psi,B}) \leq 1/q$. □

5 まとめと今後の課題

本稿では，Manual Channel モデルを利用した情報理論的に安全な BA-code を提案した．具体的には，その数理モデル，安全性の定式化，構成法を示した．今後の研究として，各エンティティの秘密鍵の鍵長のタイトな下界を示し，その等号を満たすような（その意味で最適な）構成法を提案することを目指したい．

参考文献

[1] C. Blundo, B. Masucci, and D. Stinson, "Constructions and bounds for unconditionally secure non-interactive commitment schemes,"Designs, Codes and Cryptography, vol.26, pp.97-110, Springer, 2002.

[2] D. Chaum, "Blind signatures for untraceable payments,"Advances in Cryptology-CRYPTO'82, pp.199-203, 1982.

[3] Y. Hara, T. Seito, J. Shikata, and T. Matsumoto, "Unconditionally Secure Blind Signatures,"ICITS 2007, LNCS 4883, pp.23-43, Springer, 2009.

[4] Y. Hara, T. Ishiwata, J. Shikata, and T. Matsumoto, "Unconditionally Secure Blind Authentication Codes: The Model, Constructions, and Links to Commitment,"Formal to Practical Security, LNCS 5458, pp.116-137, Springer, 2009

[5] T. Johansson, "Further results on asymmetric authentication schemes,"Information and Computation, vol.151, pp.100-133, Elsevier, 1999.

[6] A. Juels, A. Luby, and R. Ostrovsky, "Security of blind digital signatures,"Advances in Cryptology-CRYPTO'97, LNCS 1294, pp.150-164, Springer, 1997.

[7] K. Kurosawa, "New bound on authentication code with arbitration,"Advances in Cryptology-CRYPTO'94, LNCS 839, pp.140-149, Springer, 1994.

[8] M. Naor, G. Segev, and A. Smith, "Tight bounds for unconditional authentication protocols in the manual channel and shared key models,"IEEE Transactions on Information Theory, vol.54, no.6, pp.2408-2425, 2008.

[9] B. Pinkas, "Fair secure two-party computation,"Advances in Cryptology-EUROCRYPT 2003. LNCS 2656, pp.87-105, Springer, 2003.

[10] D. Pointcheval and J. Stern, "Provably secure blind signature schemes,"Advances in Cryptology-ASIACRYPT'96, LNCS 1163, pp.252-265, Springer, 1996.

[11] R. Rivest, "Unconditionally Secure Commitment and Oblivious Transfer Schemes Using Private Channels and a Trusted Initializer, "manuscript, 1999. Available at `http://people.csail.mit.edu/rivest/Rivest-commitment.pdf`

[12] S. Vaudenay, "Secure communications over insecure channels based on short authenticated strings,"Advances in Cryptology - CRYPTO 2005, LNCS 3621, pp. 309-326, Springer, 2005.