弱い情報源を用いた調停者付き認証符号の構成

村上 和羽[1,a)]　渡邉 洋平[1,2]　岩本 貢[1]

概要：認証符号（A-code）とは，外部の攻撃者によるメッセージの改ざんを受信者が検知できる技術であり，送信者と受信者が互いに信頼しない状況を加味した認証符号を調停者付き認証符号（A^2-code）と呼ぶ．A^2-code では，送受信者がそれぞれ異なる鍵を持ち，信頼できる第三者（調停者）を介在させることで送受信者間で主張が異なる場合に，調停者がどちらの主張が正しいかを判断する．Dodis–Wichs は，最小エントロピーで制約された未知の情報源（弱い情報源）の出力を鍵として用いた A-code を構成した．この構成では，弱い情報源を一様な鍵に変換するために，頑強性をもつ乱数抽出器 (non-malleable extractor) を新たに提案している．本研究では，弱い情報源から出力された鍵を用いた A^2-code を構成する．提案する A^2-code では，弱い情報源から生成された互いに異なる鍵を用いて一様な鍵を共有する必要があり，これを可能にするプロトコルと，その安全性証明を示す．

キーワード：乱数抽出器, 頑健性をもつ乱数抽出器, 認証，認証符号，調停者つき認証符号

A Construction of Authentication Code with the Arbitration Using Weak Source

Kazuha Murakami[1,a)]　Yohei Watanabe[1,2]　Mitsugu Iwamoto[1]

Abstract: An authentication code (A-code) is a cryptographic technique that allows a receiver to detect if a message has been tampered with by an external attacker. An authentication code with an arbitrator (A^2-code) is an A-code designed for scenarios where the sender and receiver do not trust each other. In an A^2-code, the sender and receiver each hold different keys, and a trusted third party (the arbitrator) can resolve disputes by determining which party's claim is correct. Dodis and Wichs constructed an A-code that uses keys derived from a weak source—an unknown source constrained by minimum entropy. To convert the output from the weak source into a uniform key, their construction introduced a novel non-malleable extractor. In this paper, we construct an A^2-code that uses keys generated from a weak source. A key challenge in our proposed A^2-code is the need to share a uniform key derived from the parties' distinct keys, which are themselves generated from a weak source of randomness. We present a protocol that enables this and provide a formal security proof.

Keywords: Extractor, Non-malleable extractor, Authentication, A-code, A^2-code

1. はじめに

1.1 研究の背景

認証符号（Authentication code; A-code）とは，送信者が受信者に送るメッセージが，第三者によって改ざんされた場合に検知する暗号技術であり，Gilbert らにより先駆け的研究がなされ [3]，Simmons によりゲーム理論的，情報理論的に体系化された [8]．このとき，A-code では送信者と受信者が互いに信頼し，協力して第三者の攻撃に対抗していた．一方，送信者と受信者が互いに信頼できないものとし，信頼できる調停者を別に置くことで，第三者による攻撃の他に送信者と受信者の攻撃も検知できるようにし

[1] 電気通信大学
The University of Electro-Communications
[2] 国立研究開発法人 産業技術総合研究所
National Institute of Advanced Industrial Science and Technology
[a)] ka.murakami@uec.ac.jp

た A-code が，調停者付き認証符号（Authentication code with the Arbitration; A^2-code）であり，Simmons によって提案された [9]．送信者の攻撃としては自分に都合の悪いメッセージを送ったことを否定すること，受信者の攻撃としては自分に都合の良いメッセージを受け取ったと主張することなどがある．調停者は送信者の鍵や受信者の鍵などの情報にアクセスでき，送信者・受信者間で上記のような争いが起こった場合に両者の主張の正誤を自分のアクセスできる情報から判断する．これにより，A^2-code は外部の攻撃者の他にも内部の送信者や受信者の攻撃も検知できるようになっている．

Dodis と Wichs は一様ではないが一定以上のエントロピーを持つ弱い情報源を共有している二者間での認証符号（メッセージ認証符号）を構成した．[2]．この構成では，通常の認証符号に加えて新たに導入された non-malleable な乱数抽出器が使われている．Non-malleable な乱数抽出器は，k-source と短い一様乱数（シード）から長い一様乱数を生成する乱数抽出器の要請を強めたものである．Dodis らによる発表の段階ではその存在性のみ示されていたが，後の研究 [1] によってその構成が示された．

Dodis らは k-source を用いた A-code を構成した一方で，k-source を用いた A^2-code については構成していない．k-source を用いた A^2-code の研究としては石川ら [12] によるものがあるが，この研究では鍵の分布が既知で鍵長が 1 ビットである場合を考えており，鍵の分布が k-source の範囲内で未知であり，鍵長が 2 ビット以上の場合の A^2-code の構成については与えられていない．そこで，本研究では送信者と受信者の鍵が k-source である場合に，安全性を保証できる A^2-code の構成を検討する．

1.2 本研究の貢献

本稿では non-malleable な乱数抽出器と 情報理論的に安全な A-code，既存の A^2-code の構成 [5] を使うことで，k-source を用いた A^2-code を構成できることを示した．また，本稿の構成における攻撃成功確率の上限を示し，構成の安全性を評価した．

1.3 本稿の構成

本稿の構成は以下の通りである．2 節では準備として乱数抽出器と A-code，そして A^2-code のモデルと具体的構成について説明する．3 節では k-source を用いた A^2-code のモデルと具体的構成を提案し，構成の安全性を評価する．

2. 準備

2.1 記法

本稿では，特に断りのない限り確率変数を X のように大文字で，その実現値を x のように小文字で表す．特に，集合 $\mathcal{X}$ 上に一様分布する確率変数を $U_{\mathcal{X}}$ と表記する．また，集合 $\mathcal{X}$ から元 x を一様ランダムに選ぶ操作を $x \leftarrow\!\!\$\ \mathcal{X}$ と表記する．これらの記法は，適宜使い分ける．確率の表記について，必要に応じて $\Pr[X = x] = P_X(x)$ と略記し，特に一様分布の場合 $\Pr[U_{\mathcal{X}} = x] = \Pr_{x \leftarrow\!\!\$\, \mathcal{X}}[x]$ と書く場合がある．確率変数 X についての期待値は $\mathbb{E}_X[\cdot]$ と表す．また，集合 $\mathcal{X} \subset \mathbb{R}$ 上の確率変数 X の台 $\{x \in \mathcal{X} : \Pr[X = x] > 0\}$ を $\mathrm{Supp}(X)$ と表記する．x を入力として取る（確率的）アルゴリズム A の出力が y であることを $y \leftarrow A(x)$ と表記する．

2.2 最小エントロピーと統計距離

確率変数の最小エントロピーは以下のように定義される．

定義 1 (最小エントロピー)**.** $\mathcal{X}$ 上の確率変数 X の最小エントロピーを次で定義する．

$$\mathrm{H}_\infty(X) \coloneqq \min_{x \in \mathcal{X}} \{-\log \Pr[X = x]\}$$

最小エントロピーを用いて k-source は次のように定義される．

定義 2 (k-source)**.** 確率変数 X が $\mathrm{H}_\infty(X) \geq k$ を満たすとき，X を k-source であるという．

確率変数間の統計距離は次で定義される．

定義 3 (統計距離)**.** X_1, X_2 を $\mathcal{X}$ 上の確率変数とする．このとき，X_1 と X_2 間の統計距離 $\Delta(X_1; X_2)$ を次で定義する．

$$\Delta(X_1; X_2) \coloneqq \frac{1}{2} \sum_{x \in \mathcal{X}} |\Pr[X_1 = x] - \Pr[X_2 = x]|$$

また，$\mathcal{Y}$ 上の確率変数 Y に対し，Y によって条件付けされた X_1, X_2 間の条件付き統計距離を次で定義する．

$$\begin{aligned}&\Delta(X_1; X_2 \mid Y)\\ &\coloneqq \frac{1}{2}\, \mathbb{E}_Y \left[\sum_{x \in \mathcal{X}} \big| \Pr[X_1 = x \mid Y] - \Pr[X_2 = x \mid Y] \big| \right]\end{aligned}$$

このとき，$\Delta(X_1; X_2 \mid Y) = \Delta((X_1, Y); (X_2, Y))$ であることが示せる．

また，統計距離は単調性と呼ばれる次の性質を持つことが知られている．

命題 1 (統計距離の単調性)**.** X_1, X_2 を $\mathcal{X}$ 上の確率変数とする．任意の集合 $\mathcal{Y}$，任意の写像 $f : \mathcal{X} \to \mathcal{Y}$ に対し，次式が成り立つ．

$$\Delta(X_1; X_2) \geq \Delta(f(X_1); f(X_2))$$

統計距離の性質として，以下の性質も知られている．

命題 2. X_1, X_2, Y_1, Y_2 を $\mathcal{U}$ 上の確率変数とする．X_1 と X_2，Y_1 と Y_2 が互いに独立なとき，次式が成り立つ．

$$\Delta((X_1, X_2); (Y_1, Y_2)) \leq \Delta(X_1; Y_1) + \Delta(X_2; Y_2)$$

2.3 乱数抽出器

乱数抽出器とはシードと呼ばれる一様乱数を用いて，一様とは限らない情報源から一様に近い乱数を抽出する関数であり，次で定義される．

定義 4 (乱数抽出器)．関数 $\mathsf{Ext} : \mathcal{X} \times \mathcal{R} \to \mathcal{Y}$ が，任意の $\mathcal{X}$ 上の k-source X に対し，

$$\Delta\left(\mathsf{Ext}(X, U_{\mathcal{R}}); U_{\mathcal{Y}}\right) \leq \varepsilon$$

を満たすとき，Ext を (k, ε)-乱数抽出器と呼ぶ．

また，同様に任意の $\mathcal{X}$ 上の k-source X に対して，

$$\Delta\left(\mathsf{Ext}(X, U_{\mathcal{R}}); U_{\mathcal{Y}} \mid U_{\mathcal{R}}\right) \leq \varepsilon$$

を満たすとき，Ext を (k, ε)-強乱数抽出器という．

ここで，定義 5 で定義されるユニバーサルハッシュ関数族が強乱数抽出器を実現することが知られている（命題 3）．

定義 5 (ユニバーサルハッシュ関数族)．関数族 $\mathcal{H} \coloneqq \{h : \mathcal{X} \to \mathcal{Y}\}$ が，任意の相異なる $x_1, x_2 \in \mathcal{X}$ に対し，

$$\Pr_{h \leftarrow\!\$ \mathcal{H}}[h(x_1) = h(x_2)] \leq \rho$$

を満たすとき，$\mathcal{H}$ を ρ-ユニバーサルハッシュ関数族と呼ぶ．

命題 3 (Leftover hash lemma [4])．関数族 $\mathcal{H} = \{h : \mathcal{X} \to \mathcal{Y}\}$ を $|\mathcal{Y}|^{-1}$-ユニバーサルハッシュ関数族とし，X を $\mathcal{X}$ 上の k-source，$\mathsf{cp}(X)$ を X の衝突確率とする．このとき，$\mathsf{Ext}(x, h) \coloneqq h(x)$ は (k, ε)-強乱数抽出器である．ここで，$\varepsilon \leq 2^{-1}\sqrt{|\mathcal{Y}| \cdot \mathsf{cp}(X)} \leq 2^{-1}\sqrt{|\mathcal{Y}| \cdot 2^{-k}}$ である

2.4 認証符号（*A*-code）

認証符号 (Authentication Code; A-code, [9]) とは，送信者が受信者に送るメッセージ m が送信者・受信者以外の敵対者による改ざんを受けていないこと（メッセージの完全性）を担保する技術である．そのための認証は，以下の手順で行われる．

(1) 送信者もしくは受信者が秘密鍵 $k \in \mathcal{K}$ をある確率分布に基づいて選び，認証済み秘密通信路で共有する．

(2) 送信者は秘密鍵 k とメッセージ m からタグ $t \leftarrow \mathsf{MAC}_k(m)$ を得る．

(3) 送信者は (m, t) を未認証公開通信路で受信者に送る．

(4) 受信者は改ざんされている可能性のある (m', t') を受け取り，検証アルゴリズム Vf を実行する．$\mathsf{Vf}_k(m', t') = 1$ ならば受信者はメッセージを受理し，それ以外ならば却下する．

この手順において，攻撃者は (3) と (4) の間で (m, t) を別のメッセージとタグ (m', t') に改ざんして受信者に送り，それが受信者の検証に通ることを目指す．

A-code が満たすべき正当性と安全性を以下で定義する．

定義 6 (正当性をもつ A-code)．A-code が次の性質を満たすとき，正当性をもつ A-code であるという．

任意の $m \in \mathcal{M}, k \in \mathcal{K}$ に対し，$t = \mathsf{MAC}_k(m)$ ならば $\mathsf{Vf}_k(m, t) = 1$ が成り立つ．

定義 7 (δ-安全な A-code)．A-code が次の性質を満たすとき，δ-安全な A-code であるという．

任意の $m \neq m', t, t'$ に対し，次の不等式が成り立つ．

$$\Pr[\mathsf{Vf}_K(m', t') = 1 \mid \mathsf{MAC}_K(m) = t] \leq \delta$$

ただし，K は $\mathcal{K}$ 上の確率変数である．

定義 5 のユニバーサルハッシュ関数族を使うことで，正当かつ安全な A-code を構成できることが知られている [11]．

2.5 *k*-source を用いた *A*-code

鍵に k-source を用いた A-code を構成するにあたり，Dodis らは，強乱数抽出器と A-code を組み合わせた構成では能動的攻撃に耐えられない点を指摘し，新たに定義 8 の non-malleable な乱数抽出器を導入し，安全性を確保した．これは，シードに加えて別の関連するシードに対する non-malleable な乱数抽出器の出力を見たとしても，出力が一様乱数と見分けがつかないことを要請する．例えば強乱数抽出器が線形性を保つ場合（定義 5 のユニバーサルハッシュ関数はその一例である），あるシード r に対する出力と，別のシード r' に対する出力の差分を取ることで，シード r に対する出力と一様乱数を判別することができる．

定義 8 (Non-malleable な乱数抽出器 [2])．関数 $\mathsf{nmExt} : \mathcal{X} \times \mathcal{R} \to \mathcal{Y}$ が集合 $\mathcal{X}$ 上に値をとる任意の k-source X，および任意の不動点を持たない写像 $f : \mathcal{R} \to \mathcal{R}$ に対して

$$\Delta\left(\mathsf{nmExt}(X, U_{\mathcal{R}}); U_{\mathcal{Y}} \mid U_{\mathcal{R}}, \mathsf{nmExt}(X, f(U_{\mathcal{R}}))\right) \leq \varepsilon$$

を満たすとき，nmExt を (k, ε)-non-malleable な乱数抽出器と呼ぶ．

命題 4 (k-source を用いた A-code の存在 [2])．(k, ε)-non-malleable な乱数抽出器と δ-安全な A-code が存在するとする．このとき，$2(\varepsilon + \delta)$-安全な k-source を用いた A-code が構成できる．

A-code はユニバーサルハッシュ関数族を用いて構成できることが知られており [11]，non-malleable な乱数抽出器も明示的構成が知られているため [7]，命題 4 により k-source を用いた A-code は実際に構成できる．

2.6 A^2-code のモデル

調停者付き認証符号（Authentication code with Arbitration; A^2-code）は，送信者と受信者がそれぞれ不正をすることを想定したメッセージ認証符号である．A^2-code のモデルでは，送信者と受信者が不正をした場合に調停する調停者を置く．調停者は必ず信頼できるとするものとし，送信者がメッセージ $m \in \mathcal{M}$ を受信者に送る状況を考え

る．このモデルにおける認証と調停の手順は，以下の通りである．

(1) 調停者は (k_s, k_r) を $\mathcal{K}_S \times \mathcal{K}_R$ からある確率分布に従って選ぶ．

(2) 調停者は送信者と k_s を，受信者と k_r を認証済み秘密通信路で共有する．

(3) 送信者はアルゴリズム $\mathsf{MAC}_{k_s} : \mathcal{M} \to \mathcal{T}$ によってメッセージ m からタグ $t \leftarrow \mathsf{MAC}_{k_s}(m)$ を生成し，受信者に認証されていない公開通信路で送る．

(4) 受信者は $\mathsf{Vf}_{k_r} : \mathcal{M} \times \mathcal{T} \to \{0,1\}$ を用いて $\mathsf{Vf}_{k_r}(m,t) = 1$ であればメッセージ m を受理する．

(5) 送信者と受信者間で争いが起こった場合，調停者は $\mathsf{AVfS}_{k_s} : \mathcal{M} \times \mathcal{T} \to \{0,1\}$ を用いて $\mathsf{AVfS}_{k_s}(m,t) = 1$ ならば (m,t) が送信者の鍵 k_s によって生成されたものだと判断し，$\mathsf{AVfR}_{k_r} : \mathcal{M} \times \mathcal{T} \to \{0,1\}$ を用いて $\mathsf{AVfR}_{k_r}(m,t) = 1$ ならば (m,t) が受信者の鍵 k_r によって受理されるものだと判断し，送信者と受信者のどちらの主張が正しいか調停する．

A^2-code の正当性と安全性は以下のように定義される．

定義 9 (A^2-code の正当性)．A^2-code の正当性は，任意の $k_s \in \mathcal{K}_S$ に対し，MAC_{k_s} が単射であり，かつ，任意の $(k_s, k_r) \in \mathrm{Supp}(K_s, K_r)$，任意の $m \in \mathcal{M}$ に対し，$\mathsf{Vf}_{k_r}(m, \mathsf{MAC}_{k_s}(m)) = 1$ を満たすことと定義する．

定義 10 (A^2-code の安全性)．以下で定義する 5 種類の攻撃に対する成功確率が十分小さいことで A^2-code の安全性を定義する．

敵対者によるなりすまし (I) 敵対者が送信者からのメッセージとは独立に受信者にメッセージを送り，受理される．

敵対者によるすり替え (S) 敵対者が送信者によるメッセージを見た上でメッセージを変更して送り，それが受信者に受理される．

送信者によるなりすまし (T) 送信者が受信者にメッセージを送り，送ったことを否定する．

受信者によるなりすまし ($\mathbf{R_0}$) 受信者は送信者が送っていないメッセージを受け取ったと主張する．

受信者によるすり替え ($\mathbf{R_1}$) 受信者は送信者が送ったメッセージとは異なるメッセージを受け取ったと主張する．

これらの攻撃に関する成功確率をそれぞれ $P_I, P_S, P_T, P_{R_0}, P_{R_1}$ とおくと，これらは以下のように定義できる [6].

$$P_{\mathrm{I}} \coloneqq \max_{\substack{m \in \mathcal{M} \\ t \in \mathcal{T}}} \Pr[\mathsf{Vf}_{K_r}(m,t) = 1]$$

$$P_{\mathrm{S}} \coloneqq \mathbb{E}_M \left[\max_{\substack{M \neq m' \\ t'}} \Pr[\mathsf{Vf}_{K_r}(m',t') = 1 \mid t = \mathsf{MAC}_{K_s}(M)] \right]$$

$$P_{\mathrm{T}} \coloneqq \max_{k_s,m,t} \Pr \left[\begin{array}{l} \mathsf{Vf}_{K_r}(m,t) = 1 \\ \wedge\ t \neq \mathsf{MAC}_{K_s}(m) \end{array} \middle| K_s = k_s \right]$$

$$P_{\mathrm{R}_0} \coloneqq \max_{k_r,m,t} \Pr[t = \mathsf{MAC}_{K_s}(m) \mid K_r = k_r]$$

$$P_{\mathrm{R}_1} \coloneqq \max_{k_r} \mathbb{E}_M \left[\max_{\substack{M \neq m' \\ t,t'}} \Pr \left[\begin{array}{c} t' = \\ \mathsf{MAC}_{K_s}(m') \end{array} \middle| \begin{array}{c} K_r = k_r, t = \\ \mathsf{MAC}_{K_s}(M) \end{array} \right] \right]$$

2.7 A^2-code の具体的構成

有限体 $\mathbb{F}_q$ 上における A^2-code の具体的構成として，以下の方式 [5] が知られている．

$\mathcal{K}_S, \mathcal{K}_R, \mathcal{M}, \mathcal{T}$ を $\mathcal{K}_S \coloneqq \mathbb{F}_q^4, \mathcal{K}_R \coloneqq \mathbb{F}_q^3, \mathcal{M} \coloneqq \mathbb{F}_q, \mathcal{T} \coloneqq \mathbb{F}_q^2$ として，

$$e_3 = f_1 + e_1 f_3 \tag{1}$$

$$e_4 = f_2 + e_2 f_3 \tag{2}$$

を満たす $(k_s, k_r) \coloneqq ((e_1, e_2, e_3, e_4), (f_1, f_2, f_3)) \in \mathcal{K}_S \times \mathcal{K}_R$ の集合を $\mathcal{K} \subset \mathcal{K}_S \times \mathcal{K}_R$ と書く．

このとき，2.6 節の (1)〜(5) に基づき認証と，必要に応じて調停を行うが，(1) は具体的に以下のように操作する．

(1) 調停者は (k_s, k_r) を $\mathcal{K}$ から一様分布に従って選ぶ．

また，(3) の MAC_{k_s} は次で定める関数である．

$$\mathsf{MAC}_{k_s}(m) \coloneqq (t_1, t_2) \coloneqq (e_1 + me_2, e_3 + me_4)$$

(4) の Vf_{k_r} は次で定める関数である．

$$\mathsf{Vf}_{k_r}(m,t) \coloneqq \begin{cases} 1 & \text{if } t_2 = f_1 + mf_2 + t_1 f_3 \\ 0 & \text{otherwise} \end{cases}$$

そして，(5) の $\mathsf{AVfS}_{k_s}, \mathsf{AVfR}_{k_r}$ は以下の式で与えられる．

$$\mathsf{AVfS}_{k_s}(m,t) \coloneqq \begin{cases} 1 & \text{if } t = (e_1 + me_2, e_3 + me_4) \\ 0 & \text{otherwise} \end{cases}$$

$$\mathsf{AVfR}_{k_r}(m,t) \coloneqq \begin{cases} 1 & \text{if } t_2 = f_1 + mf_2 + t_1 f_3 \\ 0 & \text{otherwise} \end{cases}$$

この構成での攻撃の成功確率は次で与えられる [5].

$$P_{\mathrm{I}} = P_{\mathrm{S}} = P_{\mathrm{T}} = P_{\mathrm{R}_0} = P_{\mathrm{R}_1} = \frac{1}{q} \tag{3}$$

3. k-source を用いた A^2-code

3.1 k-source を用いた A^2-code のモデル

Dodis らは事前に共有した鍵が攻撃により一部が漏洩す

る場合等を考慮し，送信者と受信者が共通の鍵を持っており，その鍵が分布は未知であるが k-source に制限されていることのみ分かっている場合の A-code を提案した [2]．しかし，Dodis らは k-source を鍵として用いる A^2-code については考えていない．そこで，本研究では k-source を鍵として用いる A^2-code の構成を提案する．k-source を用いた A^2-code の手順は，2.6 節の手順 (1)〜(5) と同じであるが，(1) に対応する手順を

(1_{w})　調停者は (k_s, k_r) を $\mathcal{K}_S \times \mathcal{K}_R$ から k-source であるような確率分布に従って選ぶ．

とし，(3) と (4) の間に次の操作を行う．

(2.5_{w})　送信者と調停者，受信者と調停者が認証なし公開通信路を用いて通信を行う．

それ以外は手順は 2.6 節の (1)〜(5) プロトコルと同様である．

また，Dodis らは敵対者によるシードへの能動的攻撃を考慮し，任意の敵対者の能動的な攻撃戦略に対し安全であるようなメッセージ認証プロトコルを提案した．そのため，本研究で扱う k-source を用いた A^2-code の安全性としては，敵対者，送信者，受信者それぞれの任意の能動的な攻撃戦略に対し安全であることを要求する．ただし，評価する攻撃成功確率 $P_{\mathrm{I}}, P_{\mathrm{S}}, P_{\mathrm{T}}, P_{\mathrm{R}_0}, P_{\mathrm{R}_1}$ については，定義 10 のものを用いる．

3.2　提案プロトコルの構成

定理 1. $(k, \varepsilon_{\mathrm{nm}})$-non-malleable な乱数抽出器が存在し，δ-安全な A-code が存在するとする．このとき，$P_{\mathrm{I}}, P_{\mathrm{S}}, P_{\mathrm{T}}, P_{\mathrm{R}_1}, P_{\mathrm{R}_0}$ が

$$P_{\mathrm{I}} \leq \frac{1}{r} + 2(\varepsilon_{\mathrm{nm}} + \delta) + \frac{3}{2}\sqrt{\frac{r(q+p-1)}{2^k p}} \tag{4}$$

$$P_{\mathrm{S}} \leq \frac{1}{r} + 2(\varepsilon_{\mathrm{nm}} + \delta) + \frac{3}{2}\sqrt{\frac{r(q+p-1)}{2^k p}} + 4\sqrt{\frac{q}{2^k}} + 4\frac{r}{q} \tag{5}$$

$$P_{\mathrm{T}} \leq \frac{1}{r} + 2(\varepsilon_{\mathrm{nm}} + \delta) + \frac{3}{2}\sqrt{\frac{r(q+p-1)}{2^k p}} + 4\sqrt{\frac{q}{2^k}} + 4\frac{r}{q} \tag{6}$$

$$P_{\mathrm{R}_0} \leq \frac{1}{r} + 2(\varepsilon_{\mathrm{nm}} + \delta) + 4\sqrt{\frac{q}{2^k}} + 4\frac{r}{q} \tag{7}$$

$$P_{\mathrm{R}_1} \leq \frac{1}{r} + 2(\varepsilon_{\mathrm{nm}} + \delta) + 4\sqrt{\frac{q}{2^k}} + 4\frac{r}{q} \tag{8}$$

である $\mathbb{Z}_p$ 上の k-source を用いた A^2-code を構成できる．ただし，q, r は素数で $p > q > r$ を満たすものとする．

提案プロトコルは 2.7 節の構成を元にしており，ユニバーサルハッシュ関数 $h_{a,b}(x) \coloneqq ax + b \mod q, h'_{a,b}(x) \coloneqq ax + b \mod r$ を利用する．以下にその構成を示す．

(1)　調停者は (k_s, k_r) を $\mathcal{K}_S \times \mathcal{K}_R$ から k-source であるような確率分布に従って選ぶ．

(2)　調停者は送信者と k_s を，受信者と k_r を認証済み秘密通信路で共有する．

(2.5)　送信者・調停者間，調停者・受信者間のシード共有

(a)　送信者は一様乱数シード a, b, a', b' を生成し，Dodis らの k-source を用いた A-code（命題 4）[2] を用いて調停者と共有する．

(b)　調停者は a, b, a', b' を Dodis らの k-source を用いたメッセージ認証プロトコル [2] を用いて受信者と共有する．

(3)　送信者はシードを用いて送信者鍵 k_s を変換して k'_s を得る．そして，$\mathsf{MAC}_{k'_s}$ を用いてメッセージ m からタグ t を生成し，受信者に認証されていない公開通信路で送る．

(a)　送信者は $e'_i = h_{a,b}(e_i), i = 1, 2, 3, 4$ を計算する．

(b)　送信者は $e''_i = e'_i \mod r, i = 1, 2, e''_j = a'e''_j + b'(e'_{j-2} + 1) \mod r, j = 3, 4$ を計算する．

(c)　送信者は $k'_s \coloneqq (e''_1, e''_2, e''_3, e''_4)$ を送信者の鍵とする．

(4)　受信者はシードを用いて受信者鍵 k_r を変換して k'_r を得る．そして，$\mathsf{Vf}_{k'_r}$ を用いてメッセージ m と タグ t を認証する．

(a)　受信者は $f'_i = af_i + b(f_3 - 1) \mod q, (i = 1, 2), f'_3 = f_3 \mod q$ を計算する．

(b)　受信者は $f''_i = h'_{a',b'}(f'_i), i = 1, 2, 3$ を計算する．

(c)　受信者は $k'_r \coloneqq (f''_1, f''_2, f''_3)$ を受信者の鍵とする

(5)　送信者と受信者間で争いが起こった場合，調停者は調停者は 2 で共有したシード a, b, a', b' を用いて k'_s, k'_r を計算する．そして，$\mathsf{AVfS}_{k'_s} : \mathcal{M} \times \mathcal{T} \to \{0, 1\}$ を用いてメッセージとタグが送信者の鍵 k'_s によって生成されたものかを判断することで，$\mathsf{AVfR}_{k'_r} : \mathcal{M} \times \mathcal{T} \to \{0, 1\}$ を用いてメッセージとタグが受信者の鍵 k'_r によって受理されるものかを判断し，送信者と受信者のどちらの主張が正しいか調停する．

4.　定理 1 の証明

4.1　準備

定理 1 を証明するために，3.2 節の構成の整理を行う．3.2 節の (1) において，調停者は $k_s = (e_1, e_2, e_3, e_4)$, $k_r = (f_1, f_2, f_3)$ を k-source であるような分布に従って選んでいる．ここで，鍵は $e_1, e_2, e_3, e_4, f_1, f_2, f_3$ のうち 5 つ

を $\mathbb{F}_q$ から k-source であるような分布に従って選ぶことで，式 (1), (2) により残りの 2 つの鍵はただ一つに決まる．次で示す補題 1 により k-source にどのような分布の確率変数を足しても結果は k-source になるため，式 (1), (2) より残り 2 つの鍵は k-source となる．したがって，送信者と受信者の鍵の要素のすべては k-source として扱ってよい．

補題 1. $\mathbb{F}$ 上の互いに独立な k-source X, Y と $a, b \in \mathbb{F}$ に対し，$a \neq 0$ または $b \neq 0$ ならば $aX + bY$ は k-source である．

証明. Z について，$\max_z P_Z(z) \leq 2^{-k}$ であることを示せば良い．X, Y の独立性から，次が成り立つ．ここで，$a \neq 0$ として一般性を失わない．

$$\begin{aligned} P_Z(z) &= \Pr[aX + bY = z] \\ &= \sum_{y \in \mathbb{F}} \Pr[aX + by = z] P_Y(y) \\ &\leq \frac{1}{2^k} \sum_{y \in \mathbb{F}} \Pr[X = a^{-1}(z - by)] \leq \frac{1}{2^k} \end{aligned} \tag{9}$$

ここで，式 (9) は X が k-source であることによる． □

また，3.2 節の (4b) においてユニバーサルハッシュ関数を用いているが，(4a) の処理によって f_1', f_2', f_3' は k-source ではなくなっている．次の補題 2 によって f_1', f_2', f_3' は $(k + \log p - \log(p + m - 1))$-source であることを示せる．

補題 2. $\mathbb{Z}_p$ 上の k-source X，自然数 m に対し，$Y := X \bmod m$ は $(k + \log p - \log(p + m - 1))$-source である．

証明. $P_Y(y)$ が $2^{-k}(p + m - 1)/p$ で抑えられることを示せば良い．

$$\begin{aligned} P_Y(y) &= \Pr[y = X \bmod m] \\ &= \sum_{x \in \mathbb{Z}_p} \Pr[y = x \bmod m] \Pr[X = x] \\ &\leq \left\lceil \frac{m}{p} \right\rceil P_X(x) \\ &= \frac{p + m - 1}{p} \cdot \frac{1}{2^k} \end{aligned}$$

□

4.2 定理 1 の安全性証明

定理 1 による安全性を評価を以下の手順で行う．

(1) 3.2 節の (3) と (4) で得られた鍵 k_s', k_r' の一様乱数からの統計距離を $\varepsilon_s, \varepsilon_r$ と置いたときの $P_{\mathrm{I}}, P_{\mathrm{S}}, P_{\mathrm{T}}, P_{\mathrm{R}_0}, P_{\mathrm{R}_1}$ の上限を求める．

(2) 鍵 k_s, k_r を k_s', k_r' に変換した際の統計距離 $\varepsilon_s, \varepsilon_r$ の上限を求める．

(3) (2) で求めた $\varepsilon_s, \varepsilon_r$ の上限を，(1) で求めた $P_{\mathrm{I}}, P_{\mathrm{S}}, P_{\mathrm{T}}, P_{\mathrm{R}_0}, P_{\mathrm{R}_1}$ の上限に代入する．

確率的アルゴリズムの乱数として一様乱数の代わりに一様乱数との統計距離が ε であるような乱数を用いる場合の失敗確率の評価として以下のことが知られている．

命題 5 ([10], Prop. 6.4)**.** $A(w; r)$ を $f(w)$ を計算する確率的アルゴリズムとする．ただし，r は A のアクセスする乱数を明示したものである．$\mathcal{R}$ 上に値をとり，$\Delta(R; U_{\mathcal{R}}) \leq \varepsilon$ を満たす確率変数を R とする．また，$\mathcal{R}$ 上に一様分布する確率変数を $U_{\mathcal{R}}$ とする．確率的アルゴリズム $A(w; r)$ について次の式を満たすとする．

$$\Pr[A(w; U_{\mathcal{R}}) \neq f(w)] \leq \gamma$$

このとき，次の式が成り立つ．

$$\Pr[A(w; R) \neq f(w)] \leq \gamma + \varepsilon$$

よって，$\mathsf{A}_1^{\text{player}}$ を player が 3.2 節の 2 における送信者と調停者間のシード共有に対して攻撃を成功させる事象，$\mathsf{A}_2^{\text{player}}$ を player（敵対者 O，送信者 S，もしくは受信者 R）が 3.2 節の (2) における調停者と受信者間のシード共有に対して攻撃を成功させる事象と置き，最終的な送信者の鍵 k_s''，受信者の鍵 k_r'' の一様分布からの統計距離をそれぞれ $\varepsilon_s, \varepsilon_r$，$k$-source を用いた A-code の安全性を δ と置くと，以下の不等式が成立する．

$$\begin{aligned} P_{\mathrm{I}} &= \max_{m,\sigma} \Pr[\mathsf{Vf}_{K_r}(m, \sigma) = 1 \mid \mathsf{A}_2^{\mathsf{O}}] \Pr[\mathsf{A}_2^{\mathsf{O}}] \\ &+ \max_{m,\sigma} \Pr[\mathsf{Vf}_{K_r}(m, \sigma) = 1 \mid \neg\mathsf{A}_2^{\mathsf{O}}] \Pr[\neg\mathsf{A}_2^{\mathsf{O}}] && (10) \\ &\leq \delta + \max_{m,\sigma} \Pr[\mathsf{Vf}_{K_r}(m, \sigma) = 1 \mid \neg\mathsf{A}_2^{\mathsf{O}}] && (11) \\ &\leq \delta + \epsilon_r + \max_{m,\sigma} \Pr[\mathsf{Vf}_{U_{K''_R}}(m, \sigma) = 1 \mid \neg\mathsf{A}_2^{\mathsf{O}}] && (12) \\ &\leq \delta + \epsilon_r + \frac{1}{r} && (13) \end{aligned}$$

式 (10) は $\mathsf{A}_2^{\mathsf{O}}$ の真偽による場合分けによる．式 (11) は k-source を用いた A-code の安全性による．式 (12) は 命題 5 により，式 (13) は 式 (3) による．

$$\begin{aligned} P_{\mathrm{S}} &\leq \mathbb{E}_M \left[\max_{\substack{M \neq m' \\ t'}} \Pr \left[\begin{array}{c} \mathsf{Vf}_{K_r}(m', t') \\ = 1 \end{array} \middle| \begin{array}{c} t = \mathsf{MAC}_{K_s}(M) \\ \mathsf{A}_2^{\mathsf{O}} \end{array} \right] \Pr[\mathsf{A}_2^{\mathsf{O}}] \right] \\ &+ \mathbb{E}_M \left[\max_{\substack{M \neq m' \\ t'}} \Pr \left[\begin{array}{c} \mathsf{Vf}_{K_r}(m', t') \\ = 1 \end{array} \middle| \begin{array}{c} \neg\mathsf{A}_2^{\mathsf{O}}, t = \\ \mathsf{MAC}_{K_s}(M) \end{array} \right] \right. \\ &\left. \Pr[\neg\mathsf{A}_2^{\mathsf{O}}] \right] && (14) \\ &\leq \mathbb{E}_M \left[\delta + \max_{\substack{M \neq m' \\ t'}} \Pr \left[\begin{array}{c} \mathsf{Vf}_{K_r}(m', t') \\ = 1 \end{array} \middle| \begin{array}{c} \neg\mathsf{A}_2^{\mathsf{O}}, t = \\ \mathsf{MAC}_{K_s}(M) \end{array} \right] \right] && (15) \\ &\leq \mathbb{E}_M \left[\max_{\substack{M \neq m' \\ t'}} \Pr \left[\mathsf{Vf}_{U_{K'_R}}(m', t') = 1 \middle| \begin{array}{c} t = \mathsf{MAC}_{U_{K'_S}}(M) \\ \neg\mathsf{A}_2^{\mathsf{O}} \end{array} \right] \right] \\ &+ \delta + \varepsilon_r + \varepsilon_s && (16) \end{aligned}$$

$$\leq \delta + \varepsilon_r + \varepsilon_s + \frac{1}{r} \tag{17}$$

式 (14) は $\mathsf{A}_2^{\mathrm{O}}$ の真偽による場合分けによる．式 (15) は k-source を用いた A-code の安全性による．式 (16) は 命題 5 により，式 (17) は 式 (3) による．

$$P_{\mathrm{T}} \leq \max_{k_s,m,\sigma} \Pr\left[\begin{array}{l|l} \mathsf{Vf}_{K_r}(m,\sigma)=1 & k_s \\ \wedge\sigma \neq \mathsf{MAC}_{k_s}(m) & \mathsf{A}_2^{\mathrm{S}} \end{array}\right] \Pr[\mathsf{A}_2^{\mathrm{S}}]$$
$$+ \max_{k_s,m,\sigma} \Pr\left[\begin{array}{l|l} \mathsf{Vf}_{K_r}(m,\sigma)=1 & k_s \\ \wedge\sigma \neq \mathsf{MAC}_{k_s}(m) & \neg\mathsf{A}_2^{\mathrm{S}} \end{array}\right] \Pr[\neg\mathsf{A}_2^{\mathrm{S}}] \tag{18}$$
$$\leq \delta + \max_{k_s,m,\sigma} \Pr\left[\begin{array}{l|l} \mathsf{Vf}_{K_r}(m,\sigma)=1 & k_s \\ \wedge\sigma \neq \mathsf{MAC}_{k_s}(m) & \neg\mathsf{A}_2^{\mathrm{S}} \end{array}\right] \tag{19}$$
$$\leq \delta + \varepsilon_r + \max_{k_s,m,\sigma} \Pr\left[\begin{array}{l|l} \mathsf{Vf}_{U_{\mathcal{K}_r}}(m,\sigma)=1 & k_s \\ \wedge\sigma \neq \mathsf{MAC}_{k_s}(m) & \neg\mathsf{A}_2^{\mathrm{S}} \end{array}\right] \tag{20}$$
$$\leq \delta + \varepsilon_r + \frac{1}{r} \tag{21}$$

式 (18) は $\mathsf{A}_2^{\mathrm{O}}$ の真偽による場合分けによる．式 (19) は k-source を用いた A-code の安全性による．式 (20) は 命題 5 により，式 (21) は 式 (3) による．

$$P_{\mathrm{R}_0} = \max_{k_r,m,\sigma} \Pr[\sigma = \mathsf{MAC}_{K_s}(m) \mid k_r, \mathsf{A}_1^{\mathrm{S}}] \Pr[\mathsf{A}_1^{\mathrm{S}}]$$
$$+ \max_{k_r,m,\sigma} \Pr[\sigma = \mathsf{MAC}_{K_s}(m) \mid k_r, \neg\mathsf{A}_1^{\mathrm{S}}] \Pr[\neg\mathsf{A}_1^{\mathrm{S}}] \tag{22}$$
$$\leq \delta + \max_{k_r,m,\sigma} \Pr[\sigma = \mathsf{MAC}_{K_s}(m) \mid k_r, \neg\mathsf{A}_1^{\mathrm{S}}] \tag{23}$$
$$\leq \delta + \varepsilon_s + \max_{k_r,m,\sigma} \Pr[\sigma = \mathsf{MAC}_{U_{K''_s}}(m) \mid k_r, \neg\mathsf{A}_1^{\mathrm{S}}] \tag{24}$$
$$\leq \delta + \varepsilon_s + \frac{1}{r} \tag{25}$$

式 (22) は $\mathsf{A}_1^{\mathrm{O}}$ の真偽による場合分けによる．式 (23) は k-source を用いた A-code の安全性による．式 (24) は 命題 5 により，式 (25) は 式 (3) による．

$$P_{\mathrm{R}_1} = \max_{k_r} \mathbb{E}_M \left[\max_{\substack{M\neq m' \\ t,t'}} \Pr\left[\begin{array}{l|l} t' = & K_r = k_r, \mathsf{A}_1^{\mathrm{S}} \\ \mathsf{MAC}_{K_s}(m') & t = \mathsf{MAC}_{K_s}(M) \end{array}\right] \Pr[\mathsf{A}_1^{\mathrm{S}}] \right]$$
$$+ \max_{k_r} \mathbb{E}_M \left[\max_{\substack{M\neq m' \\ t,t'}} \Pr\left[\begin{array}{l|l} t' = & K_r = k_r, \neg\mathsf{A}_1^{\mathrm{S}} \\ \mathsf{MAC}_{K_s}(m') & t = \mathsf{MAC}_{K_s}(M) \end{array}\right] \Pr[\neg\mathsf{A}_1^{\mathrm{S}}] \right] \tag{26}$$
$$\leq \max_{k_r} \mathbb{E}_M \left[\max_{\substack{M\neq m' \\ t,t'}} \Pr\left[\begin{array}{l|l} t' = & K_r = k_r, \neg\mathsf{A}_1^{\mathrm{S}} \\ \mathsf{MAC}_{K_s}(m') & t = \mathsf{MAC}_{K_s}(M) \end{array}\right] \right] + \delta \tag{27}$$
$$\leq \max_{k_r} \mathbb{E}_M \left[\max_{\substack{M\neq m' \\ t,t'}} \Pr\left[\begin{array}{l|l} t' = & K_r = k_r, \neg\mathsf{A}_1^{\mathrm{S}} \\ \mathsf{MAC}_{U_{\mathcal{K}'_s}}(m') & t = \mathsf{MAC}_{U_{\mathcal{K}'_s}}(M) \end{array}\right] \right]$$
$$+ \delta + \varepsilon_r \tag{28}$$
$$\leq \delta + \varepsilon_r + \frac{1}{r} \tag{29}$$

式 (26) は $\mathsf{A}_2^{\mathrm{O}}$ の真偽による場合分けによる．式 (27) は k-source を用いた A-code の安全性による．式 (28) は 命題 5 により，式 (29) は 式 (3) による．

以上より，$P_{\mathrm{I}}, P_{\mathrm{S}}, P_{\mathrm{T}}, P_{\mathrm{R}_0}, P_{\mathrm{R}_1}$ は k-source を用いた A-code の安全性パラメータ δ，変換した送信者鍵の一様乱数からの統計距離 ε_s，変換した受信者鍵の一様乱数からの統計距離 ε_r，変換した送信者鍵・受信者鍵の分布する有限体の位数 r によって表せることが分かった．

次に，変換した受信者鍵・送信者鍵 k'_r, k'_s の一様乱数からの統計距離 $\varepsilon_r, \varepsilon_s$ について評価する．以降，$\mathbb{Z}_p$ 上に一様分布する確率変数を A, B としその実現値を a, b，$\mathbb{Z}_q$ 上に一様分布する確率変数を A', B' としその実現値を a', b' とする．

まず，送信者鍵 $k'_s = (e''_i)_{i=1}^4$ の一様乱数との統計距離 ε_s を得るために，3.2 節の (3a) で得られる $(e'_i)_{i=1}^4$ の一様乱数との統計距離の上限 ε_1 を求める．$E'_i = h_{A,B}(E_i), i \in \{1,2,3,4\}$ の一様分布からの統計距離は，命題 3 より，

$$\Delta\left(h_{A,B}(E_1); U_{\mathbb{Z}_q} \mid A, B\right) \leq \frac{1}{2}\sqrt{\frac{q}{2^k}}$$

であるので，$i = 1,2,3,4$ について，次式が成立する．

$$\Delta\left(E'_i; U_{\mathbb{Z}_q} \mid A, B\right) \leq \frac{1}{2}\sqrt{\frac{q}{2^k}}$$

次に，$E'_i, i = 1,2,3,4$ と一様乱数との統計距離 ε_1 を用いて 3.2 節の (3b) で得られる $E''_i, i = 1,2,3,4$ と一様乱数との統計距離 ε_s を求める．変換における剰余演算の統計距離への影響を評価するために補題 3 を，線形結合の影響を評価するために補題 4 を示す．

補題 3. $\mathbb{Z}_n$ 上の確率変数 X，$m \leq n$ となる任意の m，$Y \coloneqq X \bmod m$ に対し，$\Delta(X; U_{\mathbb{Z}_n}) \leq \varepsilon$ ならば次が成り立つ．

$$\Delta(Y; U_{\mathbb{Z}_m}) \leq \varepsilon + \frac{m}{n} \tag{30}$$

証明． 仮定と補題 1 より，

$$\Delta(Y; U_{\mathbb{Z}_n} \bmod m) \leq \varepsilon. \tag{31}$$

また，

$$\begin{aligned} &\Delta(U_{\mathbb{Z}_n} \bmod m; U_{\mathbb{Z}_m}) \\ &= (n \bmod m)\left(\left\lceil \frac{n}{m} \right\rceil \frac{1}{n} - \frac{1}{m}\right) \\ &\leq (m-1)\left(\left(\frac{n}{m} + \frac{m-1}{m}\right)\frac{1}{n} - \frac{1}{m}\right) \\ &= (m-1)\cdot\frac{1}{n}\left(1 - \frac{1}{m}\right) < \frac{m}{n} \end{aligned} \tag{32}$$

が成り立つ．よって，式 (31), (32) と三角不等式より，式 (30) が導かれる． □

補題 4. X, Y を $\mathbb{Z}_n$ 上の互いに独立な確率変数とし，$a, b \in \mathbb{Z}_n$ とすると，$\Delta(X; U_{\mathbb{Z}_n}) \leq \varepsilon_1, \Delta(Y; U_{\mathbb{Z}_n}) \leq \varepsilon_2$ ならば，次式が成り立つ．

$$\Delta(aX + bY; U_{\mathbb{Z}_n}) \leq \varepsilon_1 + \varepsilon_2 \tag{33}$$

証明. 補題 1 と補題 2 より式 (33) が導かれる． □

補題 3，補題 4 より $i = 1, 2$ に対して次が成り立つ．

$$\Delta(E_i''; U_{\mathbb{Z}_r} \mid A, B, A', B') \leq \frac{1}{2}\sqrt{\frac{q}{2^k}} + \frac{r}{q}$$

$i = 3, 4$ に対しては次式が成り立つ．

$$\Delta(E_i''; U_{\mathbb{Z}_r} \mid A, B, A', B') \leq \sqrt{\frac{q}{2^k}} + \frac{r}{q}$$

したがって，ε_s は上から次のように抑えられる．

$$\begin{aligned}\varepsilon_s &= \Delta\left(E_1'', E_2'', E_3'', E_4''; U_{\mathbb{Z}_r}^{(1)}, U_{\mathbb{Z}_r}^{(2)}, U_{\mathbb{Z}_r}^{(3)}, U_{\mathbb{Z}_r}^{(4)} \middle| A, B, A', B'\right) \\ &\leq \sum_{i=1}^{4} \Delta(E_i''; U_{\mathbb{Z}_r} \mid A, B, A', B') \\ &\leq 3 \cdot \sqrt{\frac{q}{2^k}} + 4 \cdot \frac{r}{q}\end{aligned} \tag{34}$$

受信者鍵 $k_r' = (f_1'', f_2'', f_3'')$ の一様乱数との統計距離 ε_r を求める．3.2 節の (4) の (4a) で得られる F_1', F_2', F_3' は，補題 1 と補題 2 より $k' = (k + \log p - \log(p+q-1))$-source である．よって，3.2 節の (4) の (4b) で得られる F_1'', F_2'', F_3'' の一様乱数との統計距離は，命題 3 より次のように得られる．$i = 1, 2, 3$ に対し，

$$\Delta\left(F_i''; U_{\mathbb{Z}_q} \mid A, B, T_1\right) \leq \frac{1}{2}\sqrt{\frac{r}{2^{k'}}} = \frac{1}{2}\sqrt{\frac{r \cdot (q+p-1)}{2^k \cdot p}}$$

したがって，ε_r は上から次のように抑えられる．

$$\begin{aligned}\varepsilon_r &= \Delta\left(F_1'', F_2'', F_3''; U_{\mathbb{Z}_r}^{(1)}, U_{\mathbb{Z}_r}^{(2)}, U_{\mathbb{Z}_r}^{(3)} \middle| A, B, A', B'\right) \\ &\leq \sum_{i=1}^{3} \Delta(F_i''; U_{\mathbb{Z}_r} \mid A, B, A', B') \\ &\leq \frac{3}{2}\sqrt{\frac{r \cdot (q+p-1)}{2^k \cdot p}}\end{aligned} \tag{35}$$

式 (34) と式 (35) を式 (13), (17), (21), (25), (29) に代入し，これらの式の δ に命題 4 の結果を適用することで，定理 1 の式 (4), (5), (6), (7), (8) を得る．

謝辞 本研究は JSPS 科研費 JP23H00468, JP23H00479, JP23K17455, JP23K21644, JP23K24846 の助成，および AIP チャレンジプログラムを含む JST CREST JPMJCR23M2 の支援を受けたものです．

参考文献

[1] Dodis, Y., Li, X., Wooley, T. D. and Zuckerman, D.: Privacy Amplification and Non-malleable Extractors via Character Sums, *IEEE 52nd Annual Symposium on Foundations of Computer Science, FOCS 2011, Palm Springs, CA, USA, October 22-25, 2011* (Ostrovsky, R., ed.), IEEE Computer Society, pp. 668–677 (online), DOI: 10.1109/FOCS.2011.67 (2011).

[2] Dodis, Y. and Wichs, D.: Non-malleable extractors and symmetric key cryptography from weak secrets, *Proceedings of the forty-first annual ACM symposium on Theory of computing*, STOC '09, New York, NY, USA, Association for Computing Machinery, pp. 601–610 (online), DOI: 10.1145/1536414.1536496 (2009).

[3] Gilbert, E. N., MacWilliams, F. J. and Sloane, N. J.: Codes which detect deception, *bell system technical journal*, Vol. 53, No. 3, pp. 405–424 (1974).

[4] Håstad, J., Impagliazzo, R., Levin, L. A. and Luby, M.: A Pseudorandom Generator from any One-way Function, *SIAM J. Comput.*, Vol. 28, No. 4, pp. 1364–1396 (online), DOI: 10.1137/S0097539793244708 (1999).

[5] Johansson, T.: On the construction of perfect authentication codes that permit arbitration, Advances in cryptology — CRYPTO' 93 (Stinson, D. R., ed.), Berlin, Heidelberg, Springer Berlin Heidelberg, pp. 343–354 (1994).

[6] Kurosawa, K. and Obana, S.: Combinatorial Bounds on Authentication Codes with Arbitration, *Des. Codes Cryptogr.*, Vol. 22, No. 3, pp. 265–281 (2001).

[7] Li, X.: Non-Malleable Extractors and Non-Malleable Codes: Partially Optimal Constructions, *34th Computational Complexity Conference, CCC 2019, July 18-20, 2019, New Brunswick, NJ, USA* (Shpilka, A., ed.), LIPIcs, Vol. 137, Schloss Dagstuhl - Leibniz-Zentrum für Informatik, pp. 28:1–28:49 (online), DOI: 10.4230/LIPICS.CCC.2019.28 (2019).

[8] Simmons, G. J.: Authentication Theory/Coding Theory, *Advances in Cryptology, Proceedings of CRYPTO '84, Santa Barbara, California, USA, August 19-22, 1984, Proceedings* (Blakley, G. R. and Chaum, D., eds.), Lecture Notes in Computer Science, Vol. 196, Springer, pp. 411–431 (online), DOI: 10.1007/3-540-39568-7_32 (1984).

[9] Simmons, G. J.: A Cartesian Product Construction for Unconditionally Secure Authentication Codes that Permit Arbitration, *J. Cryptol.*, Vol. 2, No. 2, pp. 77–104 (online), DOI: 10.1007/BF00204449 (1990).

[10] Vadhan, S. P.: Pseudorandomness, *Found. Trends Theor. Comput. Sci.*, Vol. 7, No. 1-3, pp. 1–336 (online), DOI: 10.1561/0400000010 (2012).

[11] Wegman, M. N. and Carter, L.: New Hash Functions and Their Use in Authentication and Set Equality, *J. Comput. Syst. Sci.*, Vol. 22, No. 3, pp. 265–279 (online), DOI: 10.1016/0022-0000(81)90033-7 (1981).

[12] 石川美穂，四方順司：非一様ランダム鍵を用いた情報理論的に安全な調停者付き認証符号について，電子情報通信学会技術研究報告; 信学技報， Vol. 117, No. 488, pp. 231–236 (2018).