レベル2準同型暗号の平文バイナリ制約を与えるコンパクトな非対話ゼロ知識証明

光成 滋生[1,a)]　坂井 祐介[2]　Jacob C. N. Schuldt[2]

概要：準同型暗号において，暗号化対象となる平文空間を制限したいことがある．特に 0, 1 の要素からなるビットベクトルを扱うプロトコルでは 0, 1 以外の暗号文を排除したい．ここで平文空間を $\{0,1\}$ に制限することを平文バイナリ制約, 平文バイナリ制約を実現するゼロ知識証明をバイナリ範囲証明と呼ぶ．暗号文ごとに対応するバイナリ範囲証明を与える手法が提案されている．このときバイナリ範囲証明のサイズは暗号文の個数に比例する．本論文では，いくつかの条件を満たすレベル 2 準同型暗号に対して，n 個の暗号文に対する平文バイナリ制約を与える定数サイズの非対話ゼロ知識証明の構築手法を提案する．そして ASIACCS2018 で Attrapadung たちが提案したレベル 2 準同型暗号に対してそのゼロ知識証明を具体的に構築する．

キーワード：レベル 2 準同型暗号, バイナリ範囲証明, 非対話ゼロ知識証明

A Compact Non-Interactive Zero-Knowledge Binary Range Proof for Multiple Messages based on 2-Level Homomorphic Encryption

Mitsunari Shigeo[1,a)]　Sakai Yusuke[2]　Jacob C. N. Schuldt[2]

Abstract: Some applications of encryption schemes require that only messages from a restricted range are encrypted. In particular, some applications require that ciphertexts verifiably encrypts only a binary value [6]. This requirement can be addressed by attaching to the ciphertext, a non-interactive zero-knowledge proof demonstrating that the corresponding plaintext is either 0 or 1. We will refer to such a proof as a "binary range proof". However, existing proposals lead to a combined proof size that is proportional to the number of ciphertexts. In this paper, we firstly present a generic construction of a new constant-size binary range proof for multiple ciphertexts based on a 2-level homomorphic encryption scheme which satisfies some properties. Secondly, we provide a concrete instantiation based on the recent 2-level homomorphic encryption scheme by Attrapadung et al. (ASIACCS2018).

Keywords: L2 homomorphic encryption, binary range proof, non-interactive zero-knowledge proof

1. 概要

準同型暗号を使うと，ある値を暗号化した暗号文 2 個からそれらの和や積の値の暗号文を計算できる．応用上，暗号化対象となる平文空間に制約を与えたいことがある．特に 0, 1 の要素からなるビットベクトルを扱うプロトコルでは悪意ある攻撃から防御するために 0, 1 以外の暗号文を排除したい [6]．本論文では平文空間を $\{0,1\}$ に制限することを平文バイナリ制約と呼ぶことにする．

lifted-ElGamal 暗号については暗号文ごとに対応する非対話ゼロ知識証明を付与することで平文バイナリ制約を実現する手法が提案されている [5]．本論文では，いくつかの性質を満たすレベル 2 準同型暗号に対して，n 個の暗号文に対する平文バイナリ制約を与える定数サイズの非対話ゼロ知識証明の構築方法を提案する．そして ASIACCS2018

[1] サイボウズ・ラボ株式会社 Cybozu Labs, Inc.
[2] 産業技術総合研究所　情報技術研究部門 Information Technology Research Institute, AIST
[a)] herumi@nifty.com

で Attrapadung たちが提案したレベル 2 準同型暗号に対してそのゼロ知識証明を具体的に構築する．

2. L2 準同型暗号での平文バイナリ制約

2.1 コアアイデア

平文空間の大きさが p であり，暗号文と平文が 1 対 1 に対応する L2 準同型暗号を考える．ここで L2 準同型暗号とは暗号文同士の加算を多項式回，暗号文同士の乗算を 1 回可能な準同型暗号である．h を $\mathbb{Z}/p\mathbb{Z}$ への暗号学的なハッシュ関数とする．n 個のビット列 $\{ m_i \}$ ($m_i = 0$ または 1) について暗号文 $\{ c_i := \mathrm{Enc}(m_i) \}$ を生成し，$h_i := h(c_1, \ldots, c_n, i)$ として

$$X := \sum_{i=1}^{n} h_i c_i (\mathrm{Enc}(1) - c_i) \tag{1}$$

とおく．暗号文の準同型性から

$$X = \mathrm{Enc}\left(\sum_{i=1}^{n} h_i m_i (1 - m_i) \right)$$

となる．従って全ての $\{ m_i \}$ が 0 か 1 のとき $X = \mathrm{Enc}(0)$ となる．逆に $X = \mathrm{Enc}(0)$ とすると，$\mathrm{Dec}(X) = 0$. すなわち

$$\mathrm{Dec}(X) = \sum_{i=1}^{n} h_i m_i (1 - m_i) = 0.$$

ハッシュ関数の性質から $m_i \notin \{ 0, 1 \}$ の整数に対してこの等式を満たす $\{ m_i \}$ を見つけるのは極めて難しい．

したがって $X = \mathrm{Enc}(0)$ であることを検証可能な Σ プロトコルが存在すれば，n 個の暗号文 $c_i = \{ \mathrm{Enc}(m_i) \}$ に対して，

$$X = \sum_{i=1}^{n} h_i c_i (\mathrm{Enc}(1) - c_i)$$

を計算し，それが $\mathrm{Enc}(0)$ に等しいことを検証することで n 個の平文バイナリ制約を実現できる．

2.2 確定的アルゴリズム

X と対応するゼロ知識証明を計算するときに証明者と検証が同一の X を必要とする場合，X の算出に用いられる演算は確定的アルゴリズムでなければならない．そのため計算中に使われる $\mathrm{Enc}(1)$ の暗号化も利用する乱数を 0 などの両者で共有される固定の値で計算する必要がある．同様に準同型演算も乱数を伴わない方法で計算する．

検証完了後に用いられるプロトコルでは通常の乱数を用いた確率的アルゴリズムを用いて準同型演算をすればよい．

2.3 関連研究

Alice がビットベクトルの暗号文 $\{ c_i \}$ を Bob に渡し，Bob が 2 次多項式 $f(x_1, \ldots, x_n)$ に $\{ c_i \}$ を代入して結果 $f(c_i)$ を返すことを考える．悪意ある Alice の不正な暗号文への対策として [3] では乱数 r_i を選び $f(c_i) + \sum_i r_i c_i (1 - c_i)$ を返す方法が提案されている．$\mathrm{Dec}(c_i) \neq 0, 1$ の暗号文が含まれていると返された値は乱数となる．[1] の 9 節「悪意あるクライアントに対する防御」の中でも同様のアイデアが紹介されている．[4] では Confidential transactions などに利用可能な，信頼できるセットアップが不要で効率のよい非対話ゼロ知識証明を提案している．

3. 健全性

L2 準同型暗号について 2.1 節のアイデアを多少一般化した次の定理を示す．

定理 1. n を整数，$\mathrm{HE} = (\mathrm{KeyGen}, \mathrm{Enc} : \mathcal{M} \to \mathcal{C}, \mathrm{Dec} : \mathcal{C} \to \mathcal{M})$ を平文空間 $\mathcal{M}$ が素数位数 p である L2 準同型暗号で完全正当性（$\mathrm{Dec}(\mathrm{Enc}(m)) = m$ *for* $m \in \mathcal{M}$）とする．$f_1, \ldots, f_t$ を次数が高々 2 の n 変数多項式とする．次の攻撃者 $\mathcal{A}$ を考える：セキュリティパラメータ k に対して $(pk, sk) \leftarrow \mathrm{KeyGen}(1^k)$ が与えられたとき，

$$X := \sum_{i=1}^{t} h(c, i) f_i(c) = \mathrm{Enc}(0) \tag{2}$$

を満たす L1 暗号文 $c = (c_1, \ldots, c_n)$ を出力する．ここで $f(x) = (\sum_{i \leq j} \alpha_{ij} x_i x_j) + (\sum_i \beta_i x_i) + \gamma$ のとき

$$f(c) := (\sum_{i \leq j} \alpha_{ij} c_i c_j) + (\sum_i \beta_i c_i) \,\mathrm{Enc}(1) + \gamma \,\mathrm{Enc}(1)^2$$

とする．

このとき h がランダムオラクルとしてモデル化され，$\mathcal{A}$ が高々 q 回のクエリをするなら

$$P(\mathrm{Dec}(f_i(c)) \neq 0 \text{ となる } i \text{ が存在する}) \leq \frac{(q+1)}{p}.$$

ここで確率は $\mathcal{A}$ のランダムコインとランダムオラクル上で考える．

証明 $m_i := \mathrm{Dec}(c_i)$, $m := \mathrm{Dec}(c) := (m_1, \ldots, m_n)$ とすると HE の完全正当性から任意の $c = (c_1, \ldots, c_n) \in \mathcal{C}^n$ について式 (2) を満たす必要十分条件は

$$\sum_{i=1}^{t} h_i f_i(m) = 0 \text{ where } h_i := h(c, i).$$

出力 c に対して $S_c := \{ i \in \{ 1, \ldots, t \} \mid f_i(\mathrm{Dec}(c)) \neq 0 \}$ とすると HE の完全正当性から定理の左辺の確率は $P(S_c \neq \emptyset)$ に等しい．

c を $\mathcal{A}$ の出力，E^* を上記確率を与える事象とする．更に Q を「全ての $i \in S_c$ に対して (c, i) をランダムオラクルに問い合わせている事象」とする．

$$\begin{aligned} P(E^*) &\leq P(E^*|Q)P(Q) + P(E^*|\overline{Q})P(\overline{Q}) \\ &\leq P(E^*|Q) + P(E^*|\overline{Q}). \end{aligned}$$

事象 Q でないときに E^* が起きたとすると (c, j) をクエリしていない $j \in S_c$ が存在する．$f_j(m) \neq 0$ なので

$$h_j = -(f_j(m))^{-1}(\sum_{i\in S_c\setminus\{j\}} h_i f_i(m)).$$

$\mathcal{A}$ は (c,j) をランダムオラクルに問い合わせていないので出力 c は h_j と無関係である．後者はランダムに選ばれるので等式が成り立つ確率は $1/p$. よって $P(E^*|\overline{Q}) \le 1/p$.

次に事象 Q が起きたとする．すなわち $\mathcal{A}$ は全ての $i \in S_c$ に対して (c,i) をランダムオラクルに問い合わせている．

$\mathcal{A}$ が出力した全ての暗号文ベクトル $c' = (c'_1, \ldots, c'_n)$ を考える．これらのベクトルの総数を k ($k \le q$ に注意) とする．更にこれらのベクトルに対して E^* と同様にイベント $E_1, \ldots, E_k$ を考える．Q の下で $\mathcal{A}$ が出力する c が E^* となる確率は

$$P(E|Q) \le P(E_1 \vee \cdots \vee E_k) \le \sum_i P(E_i).$$

任意の暗号文ベクトル c' と対応する事象 E_i に対して $l \in S_{c'}$ を $\mathcal{A}$ がクエリした最後のインデックスとする．

$$h'_{i_l} = -(f_{i_l}(m'))^{-1} \sum_{i\in S_{c'}\setminus\{i_l\}} h'_i f_i(m') \text{ where } h'_i := h(c', i).$$

(c', i_l) がクエリされたとき，右辺は確定しているので左辺は右辺と独立である．よって $P(E_i) \le 1/p$. k の最大値は q なので $P(E^*|Q) \le q/p$. よって $P(E^*) \le (q+1)/p$. □

前節の X は $f_i(m) := m_i(1-m_i)$ としたときに該当する．

4. ペアリングベースの L2 準同型暗号 AHM+

この節ではまず [2] で提案されたペアリングベースの L2 準同型暗号以下（AHM+と記す）を紹介する．次節以降でこの暗号方式に平文バイナリ制約を与えるゼロ知識証明を具体的に構成する．

4.1 記法

G_1, G_2, G_T をそれぞれ素数位数 r の乗法巡回群，g_1, g_2 をそれぞれ G_1, G_2 の生成元とする．

$$G_1 = \langle g_1 \rangle, \quad G_2 = \langle g_2 \rangle. \quad |G_1| = |G_2| = p.$$

$e : G_1 \times G_2 \to G_T$ を非退化双線形写像（ペアリング）で G_1 と G_2 の間に効率的に計算可能な同型写像が存在しないと仮定する（タイプ 3 のペアリングと呼ばれる）．

$g := e(g_1, g_2)$ とすると g は G_T の生成元である．

$$e : G_1 \times G_2 \to G_T.$$

任意の整数 a, b に対して

$$e({g_1}^a, {g_2}^b) = e(g_1, g_2)^{ab} = g^{ab}.$$

g を生成元とする群 G の元 $y = g^n$ に対して $n = \mathrm{DLP}_g(y)$ とかく．小さい n に対して効率的に DLP が計算できることを仮定する．

集合 S に対して S から一様ランダムにサンプリングすることを $x \xleftarrow{\mathrm{U}} S$ とかく．位数 p の有限体を $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ とかく．

4.2 lifted ElGamal 暗号

AHM+のアルゴリズムは lifted ElGamal 暗号を利用するため lifted ElGamal 暗号の暗号化，復号アルゴリズムを確認する．位数 p の乗法群 G に対して $s \xleftarrow{\mathrm{U}} {\mathbb{F}_p}^\times$ をとり，$h := g^s$ とする．s が秘密鍵で h が公開鍵である．

平文 $m \in \mathbb{F}_p$ に対して乱数 $r \xleftarrow{\mathrm{U}} \mathbb{F}_p$ をとり

$$\mathrm{Enc}(m) := (g^m h^r, g^r) = (g^{m+rs}, g^r) \in G^2$$

とする．Enc は G^2 への全射である．復号は暗号文 $c := (S, T)$ に対して $\mathrm{dec}(c) := S/T^s$ とし，$\mathrm{Dec}(c) := \mathrm{DLP}_g(\mathrm{dec}(c))$ とする．

$$\mathrm{dec}(\mathrm{Enc}(m)) = \mathrm{dec}((g^{m+rs}, g^r)) = g^{m+rs}/(g^r)^s$$
$$= g^{m+rs-rs} = g^m.$$

よって $\mathrm{Dec}(\mathrm{Enc}(m)) = \mathrm{DLP}_g(\mathrm{dec}(\mathrm{Enc}(m))) = m$.

lifted-ElGamal 暗号は加法準同型性を持つ．2 個の暗号文 $c_1 := (S_1, T_1)$, $c_2 := (S_2, T_2)$ に対して

$$c_1 + c_2 := (S_1 S_2, T_1 T_2)$$

とする．暗号文に使った乱数 r を明記して $\mathrm{Enc}(m; r)$ とかくと 2 個の暗号文 $\mathrm{Enc}(m_1; r_1)$, $\mathrm{Enc}(m_2; r_2)$ に対して

$$\mathrm{Enc}(m_1; r_1) + \mathrm{Enc}(m_2; r_2) = (g^{m_1+r_1 s}, g^{r_1}) + (g^{m_2+r_2 s}, g^{r_2})$$
$$= (g^{m_1+r_1 s+m_2+r_2 s}, g^{r_1+r_2})$$
$$= (g^{(m_1+m_2)+(r_1+r_2)s}, g^{r_1+r_2}) = \mathrm{Enc}(m_1+m_2; r_1+r_2).$$

4.3 AHM+アルゴリズム

4.3.1 構成

システム初期化 セキュリティパラメータ k を受け取り $(G_1, G_2, G_T, g_1, g_2, e)$ を出力する．

鍵生成 $s_1, s_2 \xleftarrow{\mathrm{U}} {\mathbb{F}_p}^\times$ をとり $h_i := {g_i}^{s_i}$ とする．(s_1, s_2) を秘密鍵，(h_1, h_2) を公開鍵として出力する．$h_3 := e(h_1, h_2) = g^{s_1 s_2}$ とおく．

L1 暗号化 平文 $m \in \mathbb{F}_p$ に対して乱数 $r_i \xleftarrow{\mathrm{U}} {\mathbb{F}_p}^\times$ をとり，群 G_1, G_2 に対する lifted ElGamal 暗号文を作る．

$$\mathrm{Enc}_i(m) := ({g_i}^m {h_i}^{r_i}, {g_i}^{r_i}) = ({g_i}^{m+r_i s_i}, {g_i}^{r_i}) \in {G_i}^2.$$

出力する L1 暗号文はこの 2 個のペアである：

$$\mathrm{Enc}_A(m) := (\mathrm{Enc}_1(m), \mathrm{Enc}_2(m)) \in {G_1}^2 \times {G_2}^2.$$

L1 暗号文の復号 L1 暗号文 $c = (c_1, c_2)$ の復号は c_1 を G_1

の lifted ElGamal 暗号文として復号すればよい．

L1 暗号文の加算　2 個の L1 暗号文 $c_1 = (C_1, C_1')$, $c_2 = (C_2, C_2')$ に対して

$$c_1 + c_2 := (C_1 + C_2, C_1' + C_2')$$

とする（lifted ElGamal 暗号文同士の加算）．

L1 暗号文の乗算　G_1, G_2 の lifted ElGamal 暗号文 $c_1 := (S_1, T_1) \in {G_1}^2$ と $c_2 := (S_2, T_2) \in {G_2}^2$ の乗算を

$$c_1 \times c_2 := (e(S_1, S_2), e(S_1, T_2), e(T_1, S_2), e(T_1, T_2))$$

とする．乗算後の暗号文は ${G_T}^4$ の元となる．

L2 暗号文の復号　乗算後の L2 暗号文 $c = (s, t, u, v) \in {G_T}^4$ に対して

$$\mathrm{dec}_M(c) := (sv^{s_1 s_2})/(t^{s_2} u^{s_1})$$

として $\mathrm{Dec}_M(c) := \mathrm{DLP}_g(\mathrm{dec}_M(c))$ とする．

L2 暗号文の直接生成　平文 m と乱数 $\alpha, \beta, \gamma \underset{\mathrm{U}}{\leftarrow} {\mathbb{F}_p}^\times$ に対して

$$\mathrm{Enc}_M(m; \alpha, \beta, \gamma) := (g^m g^{s_1 s_2 (\alpha+\beta-\gamma)}, g^{s_1 \alpha}, g^{s_2 \beta}, g^\gamma).$$

この $\mathrm{Enc}_M : \mathbb{F}_p\mathbb{Z} \to {G_T}^4$ は全射である．

L2 暗号文の加算　2 個の L2 暗号文 $c_1 = (s_1, t_1, u_1, v_1)$, $c_2 = (s_2, t_2, u_2, v_2)$ に対して次のように定義する：

$$c_1 + c_2 := (s_1 s_2, t_1 t_2, u_1 u_2, v_1 v_2).$$

4.3.2 正当性

乗算後の暗号文が正しく復号できることを確認する．$c_i := \mathrm{Enc}_i(m_i) = (S_i, T_i) = ({g_i}^{m_i + r_i s_i}, {g_i}^{r_i})(i = 1, 2)$ に対して $(s, t, u, v) := c_1 \times c_2$ とすると

$$\begin{aligned} s &= e(S_1, S_2) = g^{(m_1 + r_1 s_1)(m_2 + r_2 s_2)}, \\ t &= e(S_1, T_2) = g^{(m_1 + r_1 s_1) r_2}, \\ u &= e(T_1, S_2) = g^{(m_2 + r_2 s_2) r_1}, \\ v &= e(T_1, T_2) = g^{r_1 r_2}. \end{aligned}$$

よって

$$\begin{aligned} &\mathrm{Dec}_M((s, t, u, v)) = \mathrm{DLP}_g((sv^{s_1 s_2})/(t^{s_2} u^{s_1})) \\ &= (m_1 + r_1 s_1)(m_2 + r_2 s_2) + r_1 r_2 s_1 s_2 \\ &- ((m_1 + r_1 s_1) r_2 s_2 + (m_2 + r_2 s_2) r_1 s_1) = m_1 m_2. \end{aligned}$$

以降明らかなときは Enc_M や Dec_M の M を略す．

5. AHM+の平文バイナリ制約

5.1 平文バイナリ制約を与える方程式

AHM+の暗号文 $c = (C, C')$ は 2 種類の lifted ElGamal 暗号文 C, C' のペアである．

lifted ElGamal 暗号文の空間は G^2 全てである（任意の $(x, y) \in G^2$ は正しい暗号文となる）．それに対して AHM+の暗号文空間 Δ は ${G_1}^2 \times {G_2}^2$ の真部分集合 $\Delta := \{\, (\mathrm{Enc}_1(m), \mathrm{Enc}_2(m)) \mid m \in \mathbb{F}_p \,\}$ である．

したがってこの暗号文が正当であるためには C と C' が同じ平文を暗号化したものでなければならない．つまり，この暗号文 $c = (\mathrm{Enc}_1(m), \mathrm{Enc}_2(m'))$ が平文バイナリ制約を満たす必要十分条件は「$m = m'$」かつ「$m \in \{\, 0, 1 \,\}$」である．

よって 2.1 節の式 (1) は次のように修整される．自然数 n をとり $m = (m_1, m_1', m_2, m_2', \ldots, m_n, m_n')$ とし $c_i := (\mathrm{Enc}_1(m_i), \mathrm{Enc}_2(m_i'))$, $c := (c_1, \ldots, c_n)$ とする．各 c_i は ${G_1}^2 \times {G_2}^2$ 全体を動く．h をハッシュ関数として

$$\begin{aligned} h_i &:= h(c_1, \ldots, c_n, i), \\ h_i' &:= h(c_1, \ldots, c_n, i + n), \\ X' &:= \sum_i \big(h_i c_i (\mathrm{Enc}_2(1) - c_i') + h_i' \cdot (c_i - c_i') \big) \end{aligned} \tag{3}$$

とおく．ただし

$$\begin{aligned} &\mathrm{Enc}_2(1) = (g_2, 1), \\ &c_i - c_i' = \mathrm{Enc}_1(m_i) - \mathrm{Enc}_2(m_i') \\ &:= \mathrm{Enc}_1(m_i) \times \mathrm{Enc}_2(1) - \mathrm{Enc}_1(1) \times \mathrm{Enc}_2(m_i') \\ &= ({g_1}^{m_i + r_i s_1}, {g_1}^{r_i}) \times (g_2, 1) - (g_1, 1) \times ({g_2}^{m_i' + r_i' s_2}, {g_2}^{r_i'}) \\ &= (g^{m_i + r_i s_1}, 1, g^{r_i}, 1) - (g^{m_i' + r_i' s_2}, g^{r_i'}, 1, 1) \\ &= (g^{(m_i - m_i') + r_i s_1 - r_i' s_2}, g^{-r_i'}, g^{r_i}, 1) \end{aligned}$$

と計算する．

$$X' = \mathrm{Enc}_M\big(\sum_i (h_i m_i (1 - m_i') + h_i' (m_i - m_i')) \big)$$

と変形できる．

定理 2. 平文空間が素数位数 p である AHM+準同型暗号に対して整数 n をとり次の攻撃者 $\mathcal{A}$ を考える：セキュリティパラメータ k に対して $(pk, sk) \leftarrow \mathrm{KeyGen}(1^k)$ が与えられたとき，式 (3) で与えられる X' が $X' = \mathrm{Enc}(0)$ を満たす $\{\, (c_i, c_i') \,\} \in {G_1}^2 \times {G_2}^2$（$i = 1, \ldots, n$）を出力する．

このとき h がランダムオラクルとしてモデル化され，$\mathcal{A}$ が高々 q 回のクエリをするなら

$$P(m_i = m_i' \in \{\, 0, 1 \,\} \text{でない } i \text{ が存在する}) \le (q + 1)/p.$$

証明　$2n$ 個の 2 次多項式を

$$f_i(m) := \begin{cases} m_i(1 - m_i') & \text{for } i = 1, \ldots, n, \\ m_i - m_i' & \text{for } i = n + 1, \ldots, 2n \end{cases} \tag{4}$$

とすると $f_1(m) = \cdots = f_{2n}(m) = 0$ となる必要十分条件は $i = 1, \ldots, n$ に対して $m_i = m_i' \in \{\, 0, 1 \,\}$ である．また式 (3) の X' は $X' = \sum_{i=1}^{2n} h(c, i) f_i(c)$ となる．$f_1, \ldots, f_{2n}$ に対して定理 1 を適用する（定理 1 と異なり 2 種類の暗号

文空間が混在するが同様にできる)．

$$P(m_i = m'_i \in \{0,1\} \text{でない } i \text{ が存在する})$$
$$= P(\mathrm{Dec}(f_i(c)) \neq 0 \text{ となる } i \text{ が存在する}) \leq (q+1)/p.$$

□

5.2 ゼロ知識証明を用いて示すべき等式

前節の記号の下で，$X' = (s,t,u,v)$ として計算すると

$$\begin{aligned}
\mathrm{DLP}_g(s) &= \sum_i h_i(m_i + r_i s_1)((1-m'_i) + r'_i s_2) \\
&\quad + \sum_i h'_i((m_i - m'_i) + r_i s_1 - r'_i s_2) \\
&= \sum_i \big(h_i m_i(1-m'_i) + h'_i(m_i - m'_i)\big) \\
&\quad + s_1 \sum_i \big(h_i(1-m'_i) + h'_i\big) r_i \\
&\quad + s_2 \sum_i \big(h_i m_i - h'_i\big) r'_i \\
&\quad + s_1 s_2 \sum_i h_i r_i r'_i. \\
\mathrm{DLP}_g(t) &= \sum_i h_i(m_i + r_i s_1) r'_i - \sum_i h'_i r'_i \\
&= \sum_i (h_i m_i - h'_i) r'_i + s_1 \sum_i h_i r_i r'_i. \\
\mathrm{DLP}_g(u) &= \sum_i h_i\big((1-m_i) + r'_i s_2\big) r_i + \sum_i h'_i r_i \\
&= \sum_i \big(h_i(1-m_i) + h'_i\big) r_i + s_2 \sum_i h_i r_i r'_i. \\
\mathrm{DLP}_g(v) &= \sum_i h_i r_i r'_i
\end{aligned}$$

となる．よって

$$\begin{aligned}
w_0 &:= \sum_i \big(h_i m_i(1-m'_i) + h'_i(m_i - m'_i)\big), \\
w_1 &:= \sum_i (h_i(1-m'_i) + h'_i) r_i, \\
w_2 &:= \sum_i (h_i m_i - h'_i) r'_i, \\
w_3 &:= \sum_i h_i r_i r'_i
\end{aligned} \tag{5}$$

とおくと $m_i = m'_i \in \{0,1\}$ のとき $w_0 = 0$ なので

$$\begin{aligned}
\mathrm{DLP}_g(s) &= w_1 s_1 + w_2 s_2 + w_3 s_1 s_2, \\
\mathrm{DLP}_g(t) &= w_2 + w_3 s_1, \\
\mathrm{DLP}_g(u) &= w_1 + w_3 s_2, \\
\mathrm{DLP}_g(v) &= w_3
\end{aligned}$$

となる．w_1, w_2, w_3 は暗号文作成者は計算できる．すなわち (s_1, s_2) が未知で $g^{s_1}, g^{s_2}, g^{s_1 s_2}$ が既知のときに (w_1, w_2, w_3) を教えずに $s = (g^{s_1})^{w_1}(g^{s_2})^{w_2}(g^{s_1 s_2})^{w_3}$, $t = g^{w_2}(g^{s_1})^{w_3}$, $u = g^{w_1}(g^{s_2})^{w_3}$, $w = g^{w_3}$ のゼロ知識証明を構成できればよい．次節で構成する．

5.3 Enc(0) を与えるゼロ知識証明の構成

素数位数 p の乗法巡回群 $G = \langle g \rangle$ について s_1, s_2 を秘密として

$$(g, x, y, z) := (g, g^{s_1}, g^{s_2}, g^{s_1 s_2})$$

が公開されているとする．このとき G の 4 個の元 (s,t,u,v) がある w_1, w_2, $w_3 \in \mathbb{F}_p$ を用いて

$$(s,t,u,v) = (x^{w_1} y^{w_2} z^{w_3}, g^{w_2} x^{w_3}, g^{w_1} y^{w_3}, g^{w_3}) \tag{6}$$

の形であることを w_1, w_2, w_3 の情報を与えずに示すゼロ知識証明を構成する．

証明　$\rho_1, \rho_2, \rho_3 \xleftarrow{\mathrm{U}} \mathbb{F}_p$ をとる．

$$\begin{aligned}
&(R_1, R_2, R_3, R_4) := (x^{\rho_1} y^{\rho_2} z^{\rho_3}, g^{\rho_2} x^{\rho_3} g^{\rho_1} y^{\rho_3}, g^{\rho_3}), \\
&c := h(g, x, y, z, s, t, u, v, R_1, R_2, R_3, R_4), \\
&\sigma_i := \rho_i + c w_i
\end{aligned}$$

とおき $\pi := (c, \sigma_1, \sigma_2, \sigma_3)$ を出力する．

検証　与えられた $\pi := (c, \sigma_1, \sigma_2, \sigma_3)$ を元に

$$\begin{aligned}
R'_1 &:= x^{\sigma_1} y^{\sigma_2} z^{\sigma_3} s^{-c}, \\
R'_2 &:= g^{\sigma_2} x^{\sigma_3} t^{-c}, \\
R'_3 &:= g^{\sigma_1} y^{\sigma_3} u^{-c}, \\
R'_4 &:= g^{\sigma_3} v^{-c}, \\
c' &:= h(g, x, y, z, s, t, u, v, R'_1, R'_2, R'_3, R'_4)
\end{aligned} \tag{7}$$

を計算し $c = c'$ なら証明を受理，そうでないなら棄却する．

5.4 証明の完全性

$\pi := (c, \sigma_1, \sigma_2, \sigma_3)$ がプロトコルに従って作られていれば

$$\begin{aligned}
R'_1 &= x^{\rho_1 + c w_1} y^{\rho_2 + c w_2} z^{\rho_3 + c w_3} (x^{w_1} y^{w_2} z^{w_3})^{-c} \\
&= x^{\rho_1} y^{\rho_2} z^{\rho_3} = R_1, \\
R'_2 &= g^{\rho_2 + c w_2} x^{\rho_3 + c w_3} (g^{w_2} x^{w_3})^{-c} = g^{\rho_2} x^{\rho_3} = R_2, \\
R'_3 &= g^{\rho_1 + c w_1} y^{\rho_3 + c w_3} (g^{w_1} y^{w_3})^{-c} = g^{\rho_1} y^{\rho_3} = R_3, \\
R'_4 &= g^{\rho_3 + c w_3} (g^{w_3})^{-c} = g^{\rho_3} = R_4
\end{aligned}$$

となり $c' = c$ となる．

5.5 証明の健全性

任意の $(s,t,u,v) \in G^4$ は，ある w_1, w_2, w_3, $w'_3 \in \mathbb{F}_p$ を用いて

$$(s,t,u,v) = (x^{w_1} y^{w_2} z^{w'_3}, g^{w_2} x^{w_3}, g^{w_1} y^{w_3}, g^{w_3})$$

とかける．なぜなら任意の v に対して w_3 がただ一つ決まり，任意の u に対して w_1，t に対して w_2，s に対して w'_3 が決まるからである．式 (7) の検証に受理すれば無視できる確率を除いて $w_3 = w'_3$ であることを示す．

定理 3. セキュリティパラメータ k に対してある素数位数 p の乗法群 $G = \langle g \rangle$ と (s_1, s_2) を生成し $(x, y, z) := (g^{s_1}, g^{s_2}, g^{s_1 s_2})$ としたとき式 (7) を満たす $(s, t, u, v) \in G^4$, $\pi := (c, \sigma_1, \sigma_2, \sigma_3)$ を出力する攻撃者 $\mathcal{A}$ を考える．このとき h がランダムオラクルとしてモデル化され，$\mathcal{A}$ が高々 q 回のクエリをするなら

$$P(w_3' \neq w_3) \leq (q+1)/p.$$

証明　与えられた $\pi := (c, \sigma_1, \sigma_2, \sigma_3)$ が検証に従って受理されたとする．

$\rho_3 := \sigma_3 - cw_3$ とおくと $R_4' = g^{\sigma_3 - cw_3} = g^{\rho_3}$.

$\rho_1 := \sigma_1 - cw_1$ とおくと $R_3' = g^{\sigma_1 - cw_1} y^{\sigma_3 - cw_3} = g^{\rho_1} y^{\rho_3}$.

$\rho_2 := \sigma_2 - cw_2$ とおくと $R_2' = g^{\sigma_2 - cw_2} x^{\sigma_3 - cw_3} = g^{\rho_2} x^{\rho_3}$.

このとき

$$R_1' = g^{\sigma_1 - cw_1} y^{\sigma_2 - c_r 2} z^{\sigma_3 - cw_3'} = g^{\rho_1} y^{\rho_2} z^{\rho_3 + c(w_3 - w_3')}.$$

w_1, w_2, w_3, w_3', c, σ_1, σ_2, σ_3（すなわち ρ_1, ρ_2, ρ_3）を自由に動かして証明を受理するには

$$c = h(g, x, y, z, x^{w_1} y^{w_2} z^{w_3'}, g^{w_2} x^{w_3}, g^{w_1} y^{w_3}, g^{w_3}, g^{\rho_1} y^{\rho_2} z^{\rho_3 + c(w_3 - w_3')}, g^{\rho_2} x^{\rho_3}, g^{\rho_1} y^{\rho_3}, g^{\rho_3}) \quad (8)$$

となる w_1, w_2, w_3, w_3', c, ρ_1, ρ_2, ρ_3 を見つける必要がある．E を $w_3' \neq w_3$ となる事象，Q を $\mathcal{A}$ が出力したパラメータに対してクエリをしている事象とする．

$$P(E) \leq P(E|Q) + P(E|\overline{Q}).$$

Q でないとき E が起こったとすると，式 (8) が成り立つ確率は $1/p$．よって $P(E|\overline{Q}) = 1/p$．Q のとき E が起こったとすると，1 回のクエリで式 (8) が成り立つ確率は $1/p$ なので q 回クエリしたとき，その中の一つが成り立つ確率は q/p 以下．よって $P(E) \leq q/p + 1/p = (q+1)/p$.　□

5.6 証明のゼロ知識性

以下のゲームを考える．

ゲーム 1. 攻撃者 $\mathcal{A}$ はセキュリティパラメータ k に対して $(pk, sk) \leftarrow \mathrm{KeyGen}(1^k)$ が与えられ，証明オラクルにアクセスが許される．証明オラクルは，式 (6) を満たす $((s, t, u, v), (w_1, w_2, w_3))$ をクエリとして受け取り，式 (7) に従って証明 $\pi = (c, \sigma_1, \sigma_2, \sigma_3)$ を生成し，π を $\mathcal{A}$ へ返す．また $\mathcal{A}$ はランダムオラクルへのアクセスも許され，その応答はハッシュリストによって管理される．ハッシュリストは，組 $(g, x, y, z, s, t, u, v, R_1, R_2, R_3, R_4, c)$ の集合から成り，この組はランダムオラクル h が $h(g, x, y, z, s, t, u, v, R_1, R_2, R_3, R_4) = c$ を満たすことを表す．$\mathcal{A}$ はビット b を出力して停止する．

ゲーム 2. 同じく攻撃者 $\mathcal{A}$ はセキュリティパラメータ k に対して $(pk, sk) \leftarrow \mathrm{KeyGen}(1^k)$ が与えられ，証明オラクルにアクセスが許される．証明オラクルは，同じく $((s, t, u, v), (w_1, w_2, w_3))$ を入力として受け取る．証明オラクルは，c, σ_1, σ_2, $\sigma_3 \leftarrow \mathbb{Z}_p$ を選び，

$$R_1' := x^{\sigma_1} y^{\sigma_2} z^{\sigma_3} s^{-c},$$
$$R_2' := g^{\sigma_2} x^{\sigma_3} t^{-c},$$
$$R_3' := g^{\sigma_1} y^{\sigma_3} u^{-c},$$
$$R_4' := g^{\sigma_3} v^{-c}$$

とし，ハッシュリストに $(g, x, y, z, s, t, u, v, R_1, R_2, R_3, R_4, c)$ を追加し，$\pi = (c, \sigma_1, \sigma_2, \sigma_3)$ を $\mathcal{A}$ へ返す．もしある c' に対して既に組 $(g, x, y, z, s, t, u, v, R_1, R_2, R_3, R_4, c')$ がハッシュリストに存在していたら，$\perp$ を $\mathcal{A}$ へ返す．$\mathcal{A}$ はビット b を出力して停止する．

ゲーム 1 で $b = 1$ となる事象を E_1，ゲーム 2 で $b = 1$ となる事象を E_2 と書く．$|\Pr[E_1] - \Pr[E_2]|$ が無視できることを示す．q_h を $\mathcal{A}$ のランダムオラクルへのクエリの回数とする．ゲーム 2 で証明オラクルが $\perp$ を返す事象を F と書くと，$|\Pr[E_1] - \Pr[E_2]| \leq \Pr[F]$．$i$ 回目の証明オラクルへのクエリにおいて $\perp$ が返る事象を F_i とすると，$\Pr[F_i] \leq (q_\mathrm{h} + i)/p$．$q_\mathrm{p}$ を証明オラクルへのクエリ回数とすると，$\Pr[F] \leq \Pr[F_1] + \cdots + \Pr[F_{q_\mathrm{p}}] = q_\mathrm{p}(q_\mathrm{h} + q_\mathrm{p} + 1)/2p$.　□

6. 全体の証明

定理 4. 4.1 節の記法に従う平文空間が素数位数 p であるペアリングベースの L2 準同型暗号に対して整数 n をとり次の攻撃者 $\mathcal{A}$ を考える：セキュリティパラメータ k に対して $(pk, sk) \leftarrow \mathrm{KeyGen}(1^k)$ が与えられたとき，

「式 (3) の $X' = (s, t, u, v)$ を計算し，式 (7) で求めた c' が c に等しい」条件を満たす $\{ (\mathrm{Enc}_1(m_i), \mathrm{Enc}_2(m_i')) \}$ $(i = 1, \ldots, n)$ と $\pi := (c, \sigma_1, \sigma_2, \sigma_3) \in \mathbb{F}_p$ を出力する．

このとき h がランダムオラクルとしてモデル化され，$\mathcal{A}$ が高々 q 回のクエリをするなら $m_i = m_i' \in \{0, 1\}$ でない i が存在する事象を E とすると

$$P(E) \leq 2(q+1)/p.$$

証明　$X' = \mathrm{Enc}(0)$ となる事象を F とすると $P(E) = P(E|F) + P(E|\overline{F})$．$P(E|F)$ は定理 2 の確率で $P(E|\overline{F})$ は定理 3 の確率なので

$$P(E) \leq (q+1)/p + (q+1)/p = 2(q+1)/p.$$

□

7. サイズの比較

AHM+で暗号文とバイナリ制約を与えるゼロ知識証明のサイズの比較を行い表 1 に記した．A.1 で AHM+の 1 個の暗号文 $c = (\mathrm{Enc}_1(m), \mathrm{Enc}_2(m'))$ のバイナリ制約を与える方法を記した．これは [5] で提案された lifted ElGamal 暗号文のバイナリ制約に $m = m'$ を組み合わせたものである．$n = 1$ のときでも提案方式は A.1 よりサイズが小さい．n が十分大きく $|p| \approx |r|$ のとき，提案方式は A.1 に比べて

表 1 n 個の暗号文とその暗号文にバイナリ制約を与えるゼロ知識証明のサイズ比較

方式	n 個の暗号文のサイズ	ゼロ知識証明のサイズ
lifted ElGamal	$2n\|p\|^{\dagger}$	$4n\|r\|^{*}$
付録 A.1‡	$6n\|p\|$	$7n\|r\|$
this work	$6n\|p\|$	$4\|r\|$

† それぞれの暗号は p 上定義された楕円曲線上の位数 r の群を利用しているものとする．ペアリングに 254-bit BN 曲線を用いている場合およそ $|p| = |r| = 256$（ビット）である．

* ゼロ知識証明は [5] の方式による．

‡ 1 個の AHM+暗号文にバイナリ制約を与える方式

$(6n|p| + 4)/(6n|p| + 7n|r|) \approx 6/13$ のデータ送信量ですむ．

8. 応用

8.1 一般の範囲制約

平文空間を $0 \le m < 2^l$ の範囲に制約したい場合，m を 2 進数展開する．

$$m = \sum_{i=0}^{l-1} m_i 2^i.$$

$\mathrm{Enc}(m)$ の代わりに $\{\mathrm{Enc}(m_i)\}$ とそのバイナリ制約を与えるゼロ知識証明を求める．その検証を受理したら，$\sum_i \mathrm{Enc}(m_i)2^i = \mathrm{Enc}(m)$ により m の範囲制約ができる．

したがって l 個の暗号文と定数サイズのゼロ知識証明を用いて 0 以上 2^l 未満の範囲制約ができる．

8.2 ハミング重み制約

n 個のビットベクトル m_i の重みが $k := \sum_i m_i$ となる制約を与えるには次のようにすればよい．

1. $m_i = 0, 1$ であるバイナリ制約を与えるゼロ知識証明を構成する．
2. $\sum_i(\mathrm{Enc}(m_i)) - \mathrm{Enc}(k) = \mathrm{Enc}(0)$ となるゼロ知識証明を構成する．

一つ目は本論文の提案手法である．二つ目は $\mathrm{Enc}(k)$ を乱数を 0 として計算することで 5.3 節の手法を適用できる．どちらも n に寄らない定数サイズのゼロ知識証明となり，n 個のビットベクトルのハミング重みが k である制約を定数サイズのゼロ知識証明を用いて構成できる．

あるいは定理 2 の多項式 $f_1, \ldots, f_{2n}$ に $f_{2n+1}(m) = (\sum_i m_i) - k$ を追加して制約条件を与えることで，両者をまとめた一つのゼロ知識証明も構成できる．

9. まとめ

本論文では L2 準同型暗号に対して，平文空間を $\{0, 1\}$ に制約する非対話ゼロ知識証明のアイデアを紹介し，それを [2] で提案したペアリングベースの L2 準同型暗号に適用して具体的に構成した．n 個の暗号文に対するゼロ知識証明の大きさが定数サイズとなるため既存手法に比べて効率がよい．なお, 本研究の一部は JST CREST JPMJCR1688 の支援を受けている．

参考文献

[1] N. Attrapadung, G. Hanaoka, S. Mitsunari, Y. Sakai, K. Shimizu, and T. Teruya.
Efficient two-level homomorphic encryption based on pairings (in japanese).
In *2018 Symposium on Cryptography and information Security (SCIS 2018)*, pages 1A2–5, January 2018.

[2] N. Attrapadung, G. Hanaoka, S. Mitsunari, Y. Sakai, K. Shimizu, and T. Teruya.
Efficient two-level homomorphic encryption in prime-order bilinear groups and a fast implementation in webassembly.
In *Proceedings of the 2018 on Asia Conference on Computer and Communications Security*, ASIACCS '18, pages 685–697, New York, NY, USA, 2018. ACM.

[3] D. Boneh, E. Goh, and K. Nissim.
Evaluating 2-DNF formulas on ciphertexts.
In J. Kilian, editor, *TCC 2005*, volume 3378 of *LNCS*, pages 325–341. Springer, 2005.

[4] B. Bünz, J. Bootle, D. Boneh, A. Poelstra, P. Wuille, and G. Maxwell.
Bulletproofs: Short proofs for confidential transactions and more.
Cryptology ePrint Archive, Report 2017/1066, 2017.
`https://eprint.iacr.org/2017/1066`.

[5] Y. Sakai, K. Emura, G. Hanaoka, Y. Kawai, and K. Omote.
Methods for restricting message space in public-key encryption.
IEICE Trans., 96-A(6):1156–1168, 2013.

[6] K. Shimizu, K. Nuida, H. Arai, S. Mitsunari, N. Attrapadung, M. Hamada, K. Tsuda, T. Hirokawa, J. Sakuma, G. Hanaoka, et al.
Privacy-preserving search for chemical compound databases.
BMC bioinformatics, 16(Suppl 18):S6, 2015.

付　　録

A.1 1 個の AHM+暗号文に対する平文バイナリ制約

この節では AHM+に対して OR-proof を適用してバイナリ制約を実現するゼロ知識証明を構成する（詳細は略）．

A.1.1 記法

s_i が秘密鍵で $h_i := {g_i}^{s_i}$ が公開鍵.

$$\mathrm{Enc}_i(m) := ({g_i}^m {h_i}^{r_i}, {g_i}^{r_i}),$$
$$\mathrm{Enc}(m) := (\mathrm{Enc}_1(m), \mathrm{Enc}_2(m)) = ((c_1, c_2), (c_3, c_4)).$$

A.1.2 ゼロ知識証明

暗号文 $C := ((c_1, c_2), (c_3, c_4))$ と $m = 0$ または 1 に応じて

$$\begin{aligned}
&d_{1-m},\, v_{1-m} \xleftarrow[\mathrm{U}]{} \mathbb{F}_p,\\
&R_{1-m} := {g_1}^{v_{1-m}} / {c_2}^{d_{1-m}},\\
&S_{1-m} := {h_1}^{v_{1-m}} / (c_1 / {g_1}^{1-m})^{d_{1-m}},\\
&w,\, t_1,\, t_2,\, t \xleftarrow[\mathrm{U}]{} \mathbb{F}_p,\\
&R_m := {g_1}^{w}, \quad S_m := {h_1}^{w},\\
&T_1 := {g_1}^{t_1}, \quad U_1 := {g_1}^{t} {h_1}^{t_1},\\
&T_2 := {g_2}^{t_2}, \quad U_2 := {g_2}^{t} {h_2}^{t_2},\\
&c := h(pk, C, R_0, R_1, S_0, S_1, T_1, T_2, U_1, U_2),\\
&d_m := c - d_{1-m},\\
&v_m := w + d_m r_1,\\
&u_1 := t_1 + c r_1, \quad u_2 := t_2 + c r_2,\\
&u := t + cm.
\end{aligned}$$

を計算し，$\pi := (d_0, d_1, v_0, v_1, u_1, u_2, u)$ を暗号文 C に対応するゼロ知識証明として出力する.

A.1.3 検証

任意の $C = (c_1, c_2, c_3, c_4) \in {G_1}^2 \times {G_2}^2$ と証明 $\pi = (d_0, d_1, v_0, v_1, u_1, u_2, u) \in {\mathbb{F}_p}^7$ が与えられたときに

$$\begin{aligned}
&c := d_0 + d_1,\\
&R'_i := {g_1}^{v_i} / {c_2}^{d_i} \text{ where } i = 0, 1,\\
&S'_0 := {h_1}^{v_0} / {c_1}^{d_0},\\
&S'_1 := {h_1}^{v_1} / (c_1 / g_1)^{d_1},\\
&T'_1 := {g_1}^{u_1} / {c_2}^{c}, \quad U'_1 := {g_1}^{u} {h_1}^{u_1} / {c_1}^{c},\\
&T'_2 := {g_2}^{u_2} / {c_4}^{c}, \quad U'_2 := {g_2}^{u} {h_2}^{u_2} / {c_3}^{c}
\end{aligned}$$

として $c = h(pk, C, R'_0, R'_1, S'_0, S'_1, T'_1, T'_2, U'_1, U'_2)$ ならば受理，そうでなければ棄却する.

A.1.4 正当性

正しいゼロ知識証明に対して $i = 1 - m$ のとき

$$R'_{1-m} = {g_1}^{v_{1-m}} / {c_2}^{d_{1-m}} = R_{1-m}.$$

$i = m$ のとき $c_2 = {g_1}^{r_1}$ なので

$$R'_m = {g_1}^{v_m} / {g_1}^{d_m r_1} = {g_1}^{v_m - d_m r_1} = {g_1}^{w} = R_m.$$

$c_1 = {g_1}^{m} {h_1}^{r_1}$ なので $m = 0$ のとき

$$\begin{aligned}
S'_0 &= {h_1}^{v_0} / {h_1}^{d_0 r_1} = {h_1}^{v_0 - d_0 r_1} = {h_1}^{w} = S_0,\\
S'_1 &= {h_1}^{v_1} / (c_1 / g_1)^{d_1} = S_{1-0}.
\end{aligned}$$

$m = 1$ のとき

$$\begin{aligned}
S'_1 &= {h_1}^{v_1} / {h_1}^{d_1 r_1} = {h_1}^{v_1 - d_1 r_1} = {h_1}^{w} = S_1,\\
S'_0 &= {h_1}^{v_0} / {c_1}^{d_0} = S_{1-1}.
\end{aligned}$$

$$\begin{aligned}
T'_1 &= {g_1}^{u_1} / {g_1}^{c r_1} = {g_1}^{u_1 - c r_1} = {g_1}^{t_1} = T_1,\\
T'_2 &= {g_2}^{u_2} / {g_2}^{c r_2} = {g_2}^{u_2 - c r_2} = {g_2}^{t_2} = T_2,\\
U'_1 &= {g_1}^{u - cm} {h_1}^{u_1 - c r_1} = {g_1}^{t} {h_1}^{t_1} = U_1,\\
U'_2 &= {g_2}^{u - cm} {h_2}^{u_2 - c r_2} = {g_2}^{t} {h_2}^{t_2} = U_2.
\end{aligned}$$

よって $c = h(pk, C, R'_0, R'_1, S'_0, S'_1, T'_1, T'_2, U'_1, U'_2)$ が成り立つ.

A.1.5 健全性

${G_1}^2 \times {G_2}^2$ の任意の元 $C = (c_1, c_2, c_3, c_4)$ は $C = ({g_1}^m {h_1}^{r_1}, {g_1}^{r_1}, {g_2}^{m'} {h_2}^{r_2}, {g_2}^{r_2})$ とかける．C と $\pi := (d_0, d_1, v_0, v_1, u_1, u_2, u)$ が検証を通れば $m = m' \in \{0, 1\}$ であることを示す．$c := d_0 + d_1$ とおく．$w_i := v_i - d_i r_1$ とおくと

$$\begin{aligned}
R'_i &= {g_1}^{v_i - d_i r_1} = {g_1}^{w_i},\\
S'_0 &= {h_1}^{v_0 - d_0 r_1} {g_1}^{-m d_0} = {h_1}^{w_0} {g_1}^{-m d_0},\\
S'_1 &= {h_1}^{v_1 - d_1 r_1} {g_1}^{(1-m) d_1} = {h_1}^{w_1} {g_1}^{(1-m) d_1}.
\end{aligned}$$

$c = d_0 + d_1 = h(\ldots, S'_0, S'_1, \ldots)$ なので $m \neq 0, 1$ のとき左辺は d_0, d_1 に依存する値となり，等号が成り立つ d_0, d_1 を見つけるのは難しい．よって $m = 0$ または 1 となる.

$t_i := u_i - c r_i$ とおくと

$$T'_i = {g_i}^{u_1 - c r_i} = {g_i}^{t_i}.$$

$t := u - cm$ とおくと

$$\begin{aligned}
U'_1 &= {g_1}^{u - cm} {h_1}^{u_1 - c r_1} = {g_1}^{t} {h_1}^{t_1},\\
U'_2 &= {g_2}^{u - cm'} {h_2}^{u_2 - c r_2} = {g_2}^{t + c(m - m')} {h_2}^{t_2}.
\end{aligned}$$

$m \neq m'$ のとき左辺は c に依存する値となり，等号が成り立つ c を見つけるのは難しい．よって $m = m'$ となる.