マルチメディア通信と分散処理 111－40
コンピュータセキュリティ　20－40
（２００３．２．２８）

時刻保証に推移性を満たしたタイムスタンプスキーム

菊池 浩明*　　杉原 尚明†　　中西 祥八郎 ‡

{kikn,higekatu}@ep.u-tokai.ac.jp

概要： 電子媒体による保存・管理が進んできている現在,電子文書などの存在証明・データの完全性を満たすタイムスタンプの必要性が生じている．Harberらによって提案されてきた一方向性ハッシュ関数を用いたチェーン構造の Linear Linking Scheme などでは,時刻証明の検証の際,検証コストがタイムスタンプ数に比例するという問題があった．本稿では,その LLS のチェーン構造とは異なり,離散対数問題の困難性に基づいたタイムスタンプスキームを提案する．提案方式の特徴は，検証時の通信コストが定数オーダーで抑えられ効率的であることである．

Transitive Time-Stamping Scheme

Hiroaki Kikuchi *　　Naoaki Sugihara †　　Shohachiro Nakanishi ‡

Abstract: In the age when documents are mainly dealt with digital media, a requirement of time stamping services are increasing in order to fulfill a proof existence and an integrity of digital documents. The Linear Linking Scheme proposed by Harber, the chain structure using the one way hash function, has a problem that verification cost is proportional to the number of timestamps. This paper proposes a time a stamping scheme based on discrete logarithm problem. The main feature of the proposed scheme is an efficiency for verification of which is a constant size for communication This scheme has transition when verification.

1　はじめに

1.1　背景

近年の急速なインターネットの普及に伴い，電子商取引きや行政行為を含め，多種多様な分野でのネットワークの利用がますます活発になってきている．それにより，文書の取り扱いにおいて従来の紙ベースの文書に比べて,作成，修正にかかるハンドリングコストの削減の効果がある電子文書への電子化が進んでいる．電子媒体によるデータの交換により，流通コスト

* 東海大学電子情報学部情報メディア学科,
Department of Information Media Technology, School of Information Technology and Electronics, Tokai University
† 東海大学大学院工学研究科,
Graduate School of Engineering, Tokai University
‡ 東海大学電子情報学部情報科学科,
Department of Human and Information Science, School of Information Technology and Electronics, Tokai University

の削減，更に保存・管理においてもハードディスクによる保存・管理となるためコストの削減が図れると言われている [ND 01].

更に, 総務省では, 住民や企業が 24 時間どこからでも行政手続きが出来る電子自治体への実現を目指し, 申請や届け出等の手続きのオンライン化を推進している．その施策として「電子自治体推進パイロット事業」を実施し, 電子的な申請や届け出等に用いる汎用受付システムの基本仕様の策定を進めている [CUC].

このように電子化によって, 行政手続きの利便性が向上すると考えられる．それと同時にデータの改竄や削除, 複製などの不正行為が, 今までの紙による管理よりも容易になると考えられる．電子文書やデータを改竄する事によって，あたかもその事が現実に起って無いかの様に，都合の悪いデータを削除したり，データを新たに付け加える事によって過去の事実の偽造したりといった不正が起こる．

このような，不正行為を防止し，時刻を保証する技術が，タイムスタンプ技術である．そのタイムスタンプについて様々な方式や安全性についての研究が進んでいる [KI 00][UM 00].

1.2 タイムスタンプの要求条件

タイムスタンプは，電子文書がある特定の時刻に存在していた事を次のように証明する．

1. ある電子文書が, ある時刻に存在したことの証明 (存在証明)
2. その作成された時刻以降にその電子文書が変更されていないことの証明と改竄, 削除の検出 (データの完全性)

この用件を満たす技術として，Linear Linking Scheme (以下 LLS)[HS 91] が良く知られている．LLS は，生成されたタイムスタンプが, それまでに Time Stamp Authority(タイムスタンプ発行局) (以下 $\mathcal{TSA}$) によって生成されたタイムスタンプに依存するようにリンク情報を生成する連鎖型スキームである．更に, 検証情報と，その証拠補強として，リンク情報を定期的に新聞などのメディアに公表する．そして, このスキームを用いた国家プロジェクトも海外では行なわれており，エストニアにおける国家プロジェクトとして行なわれている Cuculus は，LLS を採用している．更に，連鎖型スキームとしては，スペインで行なわれている PKITS は複数の TSA を用いたリンキングスキームを採用し，ベルギーで行なわれている TIMESEC はツリー構造のリンキングプロトコルを国家プロジェクトとして行なわれている [UMT 00].

1.3 問題点と改善策

LLS 方式における問題点として，$\mathcal{TSA}$ がタイムスタンプ要求データが来てからすぐにタイムスタンプを発行せず，ネットワークの遅延があって発行が遅れたかのように振る舞い，しばらくしてからタイムスタンプを発行するといったタイムスタンプ保留攻撃が挙げられる．更に，ハッシュ値によるリンク情報の鎖を生成し，タイムスタンプの生成を行なうため，タイムスタンプが n 人に発行された場合, n 人分の検証をする必要がある．この線形オーダの高い検証コストも問題である．

我々は，検証コストに関する問題に着目し，問題を解決する為に，離散対数問題の困難性に基づいた Linking Scheme を提案する．本提案の特徴は，検証に対して推移性を持たせる事が可能である点である．本稿の以下の構成は，まず, 2 節において LLS における基本的なタイムスタンプの生成, 検証を示す．続いて，3 節において, 本稿の提案プロトコルについて示す．4 節では提案プロトコルについての評価をし，5 節で以上のまとめを示す．

2 Linear Linking Scheme

以下に今回我々の提案プロトコルとの比較対象となる LLS のタイムスタンプ発行プロトコル，及び検証プロトコルを示す．タイムスタンプ生成要求者 $\mathcal{U}_i$ がその $\mathcal{TSA}$ において i 番目のタイムスタンプ生成要求をしたとする．以下，$H(\cdot)$ をハッシュ関数とする．

Step 1:(タイムスタンプ要求) $\mathcal{U}_i$ は $\mathcal{TSA}$ に対象データ m_i のハッシュ値 H_i に署名 $\sigma_{U_i}(H_i)$ をして送付する．

Step 2:(タイムスタンプ生成) $\mathcal{TSA}$ は受け取った H_i より

$$L_i = H(H_i, L_{i-1}, i) \tag{1}$$

を生成する．ただし, ここで L_i はリンク情報である．$\mathcal{TSA}$ は受け取った $\mathcal{U}_i$ の H_i と時刻 t_i, $\mathcal{U}_i$

のリンク情報 L_i を用いてタイムスタンプ TS_i

$$TS_i = \sigma_{TSA}(H_i, L_i, t_i, i)$$

を生成する.

Step 3:(タイムスタンプ検証) 検証者 $\mathcal{V}$ は,対象データ m_i とタイムスタンプ TS_i から,デジタル署名を検証する. さらに, $\mathcal{TSA}$ やメディアからタイムスタンプの検証に必要な情報であるリンク情報 "$L_1, \cdots, L_i$" を入手し, $\mathcal{TSA}$ の不正が無いことを検証する.

3 提案プロトコル

3.1 推移性

本提案プロトコルは, 離散対数問題 (以下 DLP) に基づくタイムスタンプスキームであり, タイムスタンプの時刻保証の検証において推移性を持たせる事が可能である.

時刻 i, j, k, $(i < j < k)$ におけるタイムスタンプ TS_i, TS_j, TS_k がある時 $i \leq j$ ならば, TS_i より TS_j が後から署名されている事を $TS_i < TS_j$ と書く. 今, $TS_i < TS_j$ と $TS_j < TS_k$ の両方が証明出来る時, $TS_i < TS_k$ の証拠を示す事が出来れば, このタイムスタンプスキームは推移性を満たすと言う.

LLS は推移性を満たしている. なぜならば, $TS_i < TS_j$ かつ $TS_j < TS_k$ ならば, 必ず, (1) 式を満たすリンク情報の数列

$$L_i < L_{i+1} < \cdots < L_j < \cdots < L_k$$

が存在し、これを証拠とすればよいからである. しかし, LLS における証拠は $k - i$ 個のハッシュ値から成り, 一般に $O(n)$ の長さを持つ.

そこで、以下に $O(1)$ の長さの証拠を示す事が出来るスキームを提案する.

タイムスタンプ要求データ m_i を持つ $\mathcal{U}_i$ が $\mathcal{TSA}$ にタイムスタンプを要求する事を考えよう. エンティティは, 鍵を生成する $Dealer$, タイムスタンプを生成・発行する $\mathcal{TSA}$, タイムスタンプ要求者 $\mathcal{U}_i$, そして検証者 $\mathcal{V}$ が挙げられる. $Dealer$ と $\mathcal{TSA}$ は, まったく別のエンティティであり $\mathcal{TSA}$ は鍵を生成できないものとする. また, $Dealer$ は信頼出来るが, $\mathcal{TSA}$ は不正を働く可能性があると仮定する.

3.2 タイムスタンプ発行プロトコル

3.2.1 鍵生成

$Dealer$ は, 大きな素数である p, q を生成し, $n = pq$,$\phi(n)$=$LCM(p-1, q-1)$ を生成する. n は公開, $\phi(n)$ は $Dealer$ の秘密情報とする. g を Z_n^* の $q|\phi(n)$ となる位数 q の乗法群の生成元とする. $Dealer$ は $q^* < q$ となる乱数 q^* を公開する.

ここで, 注意してもらいたいのは, リンク情報やタイムスタンプを生成する $\mathcal{TSA}$ は, $\phi(n)$ を知らないで,n のみでタイムスタンプの生成を行なう点である.

$\mathcal{TSA}$ は秘密情報 $x \in Z_g$ をランダムに選び, $G = g^x \bmod n$ を生成する. 更に, $\mathcal{TSA}$ は $\gamma_0 = 1$,$m_0 = 1$ となる $G_0 = G^G \bmod n$ を生成する.

ここで $\mathcal{TSA}$ は G, G_0, g を公開する.

3.2.2 タイムスタンプの生成・発行

$\mathcal{U}_i$ はタイムスタンプ要求対象データ m_i に対して署名をした $\sigma_{U_i}(H(m_i))$ を $\mathcal{TSA}$ に送信する.

$\mathcal{TSA}$ が, リンク情報 G_{i-1} を持っているとき, $\mathcal{U}_i$ のタイムスタンプ要求データである文書 m_i に対するタイムスタンプを次の様に定める.

$\mathcal{TSA}$ は, ある乱数 q^* 未満の乱数 γ_i を選び, リンク情報を

$$G_i = G^{G_{i-1} m_i \gamma_i} \bmod n \tag{2}$$

により求める. ここで,

$$G_{i-2} m_{i-1} \gamma_{i-1} < G_{i-1} m_i \gamma_i < q^* \tag{3}$$

を満たしているか検査し, していなければ別の γ_i を選び, 式 (3) が成立するまで繰り返す. ただし, γ_i は $\mathcal{TSA}$ が秘密に管理する. [1]

こうして定められたリンク情報 G_i について, 時刻 t_i のタイムスタンプ T_i を以下のように定める.

$$T_i = \sigma_{TSA}(H(m_i), G_i, t_i, i)$$

により定める.

そして, $\mathcal{TSA}$ は $\mathcal{U}_i$ に σ_{TSA} を送る. ここで, $\mathcal{TSA}$ による署名 σ_{TSA} は, 適切なデジタル署名とする.

$\mathcal{U}_i$ は T_i が自分のタイムスタンプ要求データ m_i について正しく発行されている事を T_i の署名から検証出来る.

[1] $\phi(n)$ を $\mathcal{TSA}$ は知らないので, 式 (3) は通常の整数の順序関係である事に注意せよ.

3.3 リンク情報の検証プロトコル

$\mathcal{TSA}$がリンク情報を偽らないで，タイムスタンプを正しく生成，発行している事を第三者に証明するプロトコルを示す．

3.3.1 プロトコル 1(逐次検証)

定理 **3.1** リンク情報 G_i,G_j について

$$G_j = G^{G_i \alpha_{i,j}} \bmod n$$

を満たす $\alpha_{i,j}$ を $T_i < T_j$ (すなわち T_j が T_i の後から発行された) 事の証拠 (witness) と言う．

補題 **3.1** T_i と T_{i+1} をタイムスタンプとする．$T_i < T_{i+1}$ ならば，その時に限り $\phi(n)$ を知らない $\mathcal{TSA}$ が証拠 $\alpha_{i,i+1}$ を作ることが出来る．

つまり，$\mathcal{TSA}$ が，リンク情報 G_i から G_{i+1} を正しく生成している事の証明を出来る．

(証明) $T_i < T_{i+1}$ ならば，$\mathcal{TSA}$ は $m_{i+1}\gamma_{i+1}$ を知っているので，G_i と G_{i+1} について $G_{i+1} = G^{G_i m_{i+1}\gamma_{i+1}}$ を満たす $\alpha_{i,i+1} = m_{i+1}\gamma_{i+1}$ を証拠として示す事が出来る．

逆に、$T_i < T_{i+1}$ でない時，すなわち，$T_{i+1} < T_i$ の時に，$\mathcal{TSA}$ が $G_i = (G^{G_{i+1}})^{\beta}$ を満たす β を知識の証明で示す事が出来ると仮定しよう．ここで，$G_i = G^{G_{i-1} m_i \gamma_i}$ なので，両辺の対数を取り，

$$G_{i+1}\beta = G_{i-1} m_i \gamma_i \bmod \phi(n)$$

を満たす β は

$$\begin{aligned} \beta &= \frac{G_{i-1}}{G_{i+1}} m_i \gamma_i \bmod \phi(n) \\ &= G^{(G_{i-2} m_{i-1}\gamma_{i-1}) - (G_i m_{i+1}\gamma_{i+1})} m_i \gamma_i \end{aligned}$$

となる一方，式 (3) の条件より

$$(G_{i-2} m_{i-1}\gamma_{i-1}) < (G_{i-1} m_i \gamma_i) < (G_i m_{i+1}\gamma_{i+1}) < q^*$$

なので，

$$(G_{i-2} m_{i-1}\gamma_{i-1}) - (G_i m_{i+1}\gamma_{i+1}) < 0$$

である．従って，必ず $\phi(n)$ での縮約 (reduction) が生じる為，これを知っている事は $\mathcal{TSA}$ が $\phi(n)$ を知らない前提に矛盾する．それゆえ，証拠を示す事が出来るならば，$T_i < T_{i+1}$ である．よって，証拠を示す事は $T_i < T_{i+1}$ の必要十分条件である． (証明終)

3.3.2 プロトコル 2(推移性)

補題 **3.2** G_i,G_j,G_k を $T_i < T_j < T_k$ となるタイムスタンプのリンク情報，$\alpha_{i-1,i}$, $\alpha_{i,j}$, $\alpha_{j,k}$ を各々の証拠とする．

この時,$T_i < T_k$ を証明する証拠 $\alpha_{i,k}$ は必ず存在し，($\phi(n)$ を知らなくても) 一意に決まる．

(証明) $G_k = G^{G_i \alpha_{i,k}} \bmod n$ を満たす $\alpha_{i,k}$ は，前提より，$G_k = G^{G_j \alpha_{j,k}}$ なので，

$$\begin{aligned} \alpha_{i,k} &= \frac{G_{j-1}\alpha_{j,k}}{G_i} \\ &= G^{(G_j \alpha_{i,j} - G_{i-1}\alpha_{i-1,i})} \alpha_{j,k} \bmod \phi(n) \end{aligned}$$

によって与えられる．(2) 式より，

$$q^* > G_i \alpha_{i,j} - G_{i-1}\alpha_{i-1,j} > 0$$

なので，$\phi(n)$ を知らなくても， $\alpha_{i,j}$ と $\alpha_{i-1,j}$ から一意に決まる． (証明終)

定理 **3.2** $\phi(n)$ を知らない $\mathcal{TSA}$ は任意の i, j について，$T_i < T_j$ ならば証拠 $\alpha_{i,j}$ を示す事が出来る．

(証明) 補題 1 より，任意の i について，$T_{i-1} < T_j$ の証拠 $\alpha_{i,j}$ と $T_i < T_{i-1}$ の証拠 $\alpha_{i,i+1}$ を示す事が出来る．この時，補題 2 より，$T_i < T_{i+2}$ の証拠も示すことが出来，結局 $i < j$ の任意の j について，$\alpha_{i,j}$ を示す事が出来る． (証明終)

$T_i < T_j$ の証拠 $\alpha_{i,j}$ を持つ時，検証者 $\mathcal{V}$ に対して，$\alpha_{i,j}$ を漏らさないで次の様にゼロ知識証明 $PK\{(\alpha) \mid G_j = G^{G_i \alpha}\}$ をする事が出来る．

1. $\mathcal{TSA}$ は，乱数 r を選び，$T = G^{G_i r} \bmod n$，$c = H(T)$，$z = r + c\alpha$ を求める ($\phi(n)$ を知らないので，z は通常の加算である事に注意)．PK に基づく署名，$SPK = (T, c, z)$ とする．

2. 検証者 (ユーザー) は SPK より，

$$\frac{G^{G_i z}}{G_j^c} = G^{G_i(r + c\alpha - \alpha c)} \stackrel{?}{=} T \bmod n$$

であるかを検証する．

4 評価

タイムスタンプの署名 σ_{TSA} により，秘密情報 γ_i を知らない不正者が，$\mathcal{TSA}$ に成りすまして署名は偽

造出来ない．一方，不正な$\mathcal{TSA}$がリンク情報を偽って，$T_i < T_j$に対して証拠$\alpha_{i,j}$を偽造出来る可能性は，離散対数問題の困難性に基づいて防止されている．提案方式は，タイムスタンプの時刻認証において効率的に推移性を満たしている．従って，任意の二点のタイムスタンプの前後関係，つまり，どちらが先に$\mathcal{TSA}$にタイムスタンプを発行してもらったのかという検証のコストの削減が図れたと考える．

LLSでは，一つの区間においてかかる検証コストは$O(n)$といった線形オーダであった．しかし，我々の提案プロトコルにおいては検証コストは$O(1)$である．

提案プロトコルでは，$\mathcal{TSA}$が不正な順序でタイムスタンプを発行する不正を防止する為に，タイムスタンプ生成者と鍵生成者$(Dealer)$とに分散した．そして，$\phi(n)$を$Dealer$が，$\mathcal{TSA}$に秘密にしたままタイムスタンプを生成させる事が出来た．しかし，タイムスタンプを生成する$\mathcal{TSA}$は$\phi(n)$を知らない為，タイムスタンプ生成の際の計算量が膨大になってしまい，リンク情報生成にかかる処理時間が多くかかるというデメリットが生じた．それゆえに，$\mathcal{TSA}$が$\mathcal{U}$からの要求データに対するリンク情報を生成し，タイムスタンプを発行するのに時間がかかるという問題点が挙げられる．故に，リアルタイム性が失われていて，タイムスタンプをすぐに発行せず，しばらくたってから発行して時刻遅延によって発行順序に誤差が出てしまったかのように$\mathcal{TSA}$が不正を出来てしまうタイムスタンプ保留攻撃を可能にしてしまう恐れがある．よって，今後の課題として，提案プロトコルにおいてリンク情報生成の際やタイムスタンプ発行における処理時間の縮小が挙げられる．

5 まとめ

本論文ではタイムスタンプの概要を説明し，その中でもLLSを比較対象として挙げ，LLSを解説した．タイムスタンプの中の相対的タイムスタンプの中でLLSにおける検証コストに着目し，検証コスト削減を目標としてタイムスタンププロトコルの提案をした．今回の提案である，DLPに基づくタイムスタンプスキームによって検証コストをタイムスタンプ数に依存しないように出来た．しかし，$Dealer$という鍵生成のエンティティを増やした為，タイムスタンプを発行する$\mathcal{TSA}$は，公開情報だけでタイムスタンプを生成しなくてはいけない為，処理時間がタイムスタンプ要求者の数に比例して増加するという問題点も残った．

電子政府実現に向けて着実に文書などの電子化が進んでいる現在，情報化社会に不可欠な基盤となるであろう時刻認証については生成においても検証においても迅速なやり取りが出来るようにする必要がある．故に，安全性と効率性のトレードオフをも考慮して，より使いやすいシステム構築に向けて今後も研究を進めて行きたいと考える．

参考文献

[OY 97] 岡本 龍明，山本 博資「現代暗号」，産業図書,1997.

[HS 91] Stuart Haber and W.Scott Stornetta, “ How to Time-Stamps a Digital Document”, J. of Cryptology ,Vol.3 ,No.2 ,pp.99-111,1991.

[KSN 02] 菊池 浩明，杉原 尚明，中西 祥八郎 “離散対数問題に基づくタイムスタンプスキーム”，SCIS2002, pp.617-620,2002.

[UM 00] 宇根 正志，松本 勉，“タイムスタンププロトコル Cuculus と PKITS の安全性に関する一考察”，CSS2000, pp.55-60,2000.

[UMT 00] 宇根 正志，松浦 幹太，田倉 昭 “最近のデジタルタイムスタンプの技術の現状と課題”，金融研究第19巻別冊第1号, pp.105-154,2000

[OO 95] 岡本 龍明，太田 和生 “暗号・ゼロ知識証明・教論”，情報処理学会,1995

[ND 01] NTTデータ経営研究所 ,“電子文書証明 eドキュメントの原本性確保”，NTT出版,2001.

[KI 00] 金谷 篤郎，今井 秀樹，“複数の検証パスを持つデジタルタイムスタンプ”，CSS2000, pp.235-242,2000.

[KT 02] 桑門 秀典，田中 初一，”有向木の構造を有するデータに適した fail-stop 署名方式”，CSS2002, pp.89-94,2002.

[DNA] http://www.jnotary.com/「日本電子公証機構」(2002.9 参照)

[VER] http://www.verisign.co.jp/onsite/notary 「日本ベリサイン電子公証サービス 」(2002.9 参照)

[CUC] http://www.city.urayasu.chiba.jp/denshi/denshi.html 「総務省電子自治体推進パイロット事業実証実験 」(2003.1 参照)