Time Stamping Preprint and Electronic Journal Server Environment

Takao Namiki (Hokkaido University)
Kazutsuna Yamaji (National Institute of Informatics)
Toshiyuki Kataoka (National Institute of Informatics)
Noboru Sonehara (National Institute of Informatics)

July 20, 2011
Towards a Digital Mathematics Library 2011

Backgrounds

- While many universities operate local preprint and journal servers, the security of these digital documents may be at risk.
- Cracking, disasters and careless operations cause the serious problem.
- Full text file may be diffused hands by hands with annotations or comments.
- Currently, most articles still have the printed issue in addition to digital file distribution.
- In this dual publication scheme, the printed issue is regarded as the trusted original version.

Backgrounds

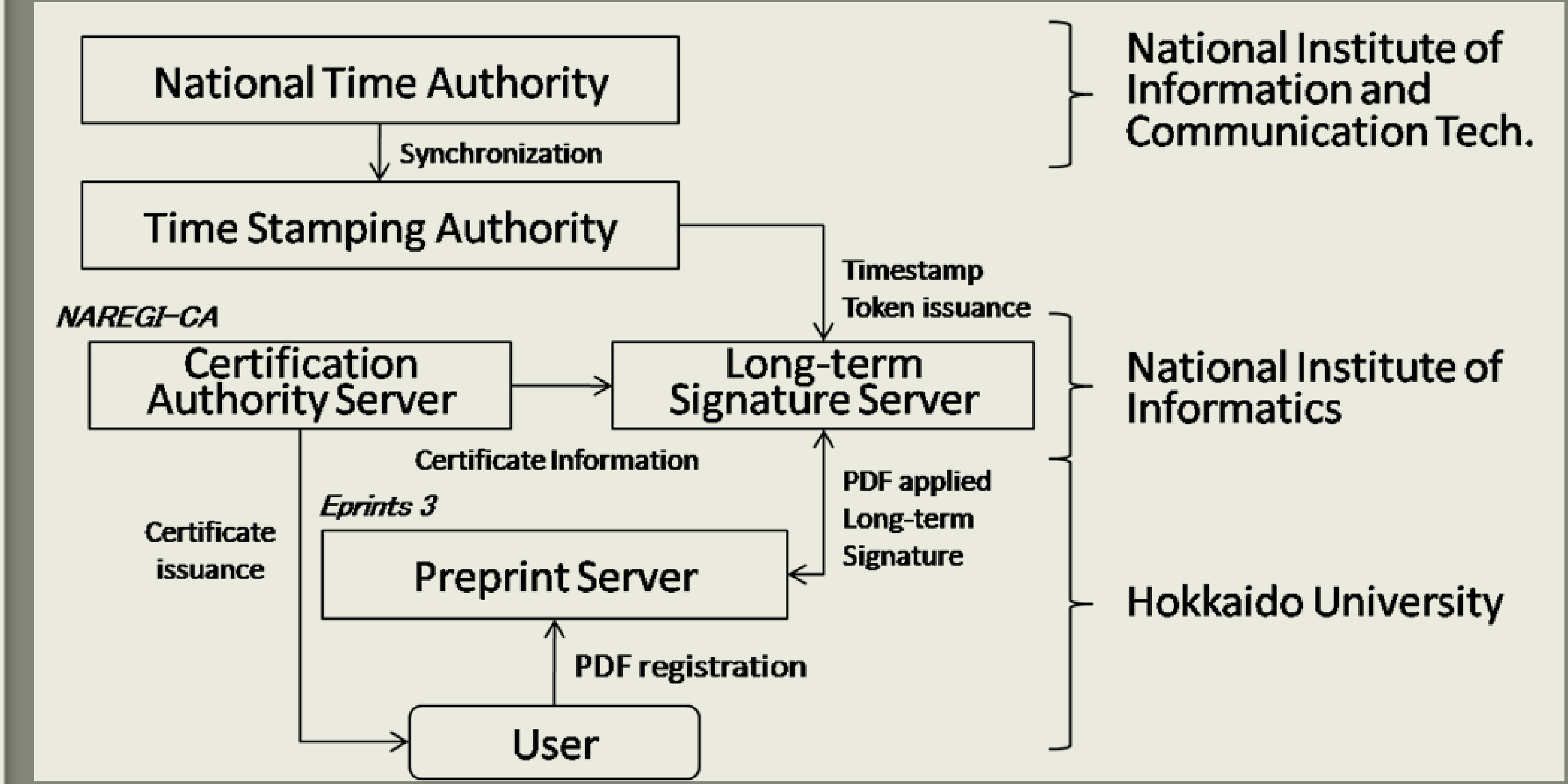
- However, in paperless publication, it is difficult to distinguish a copy from the original. That is, the security level of the preprint files has to be raised in order to protect the research results.
- In the field of business, the security of digital documents containing patentable ideas and intellectual property are guaranteed by means of an electronic signature and timestamp technique.
- These technologies can be applied to academic publishing to ensure reliable digital content.
- This study proposes a secured preprint server environment and describes its application to the mathematical e-journal and preprint service at Hokkaido University.

Possible Solutions

- Mirroring and backup
- Hash/Checksum
- Read only full text file
- Password protection
- There is no guarantee that nobody have changed the created time information of full text file.
- Cracking, disasters and careless operations will cause unrecoverable problem.

Overview of our Solution

- System architecture



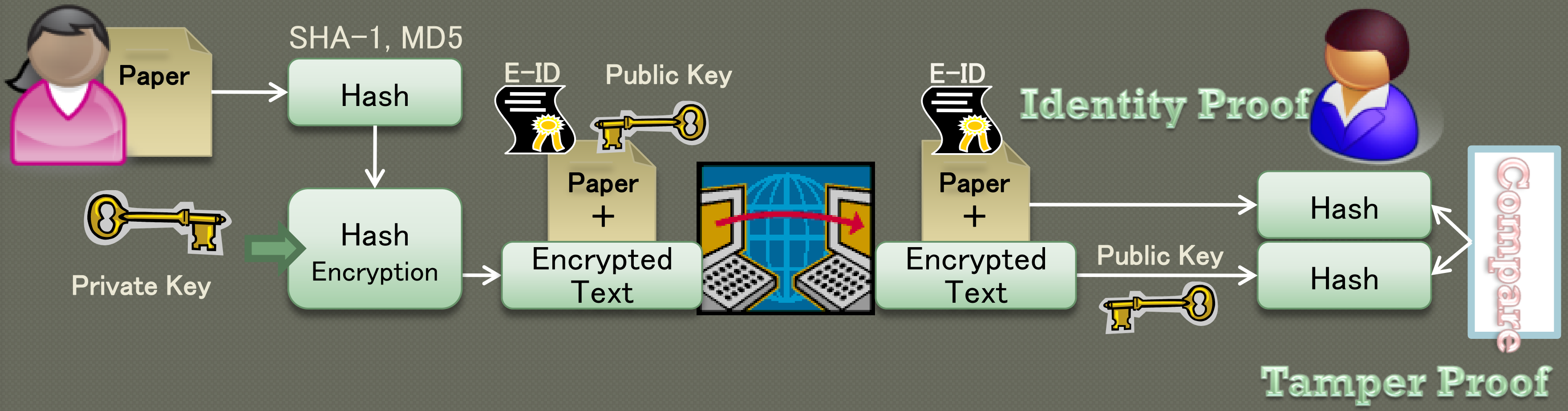
Electronic Signature

- One solution is Long-term Signature.
- The electronic signature (ES) ensures integrity and signer of a document.
- The digital signature is created from an encrypted hash value of a digital document.
- The recipient (client application) can detect a falsification of the document by comparing hash values calculated from the original document and decrypted from the digital signature

Electronic Signature

Electronic signature ensures integrity and signer of a document

ES by PKI (Public Key Infrastructure)



- Application of the ES to Article
  - Author (Editor)
  - Contents

can be certified

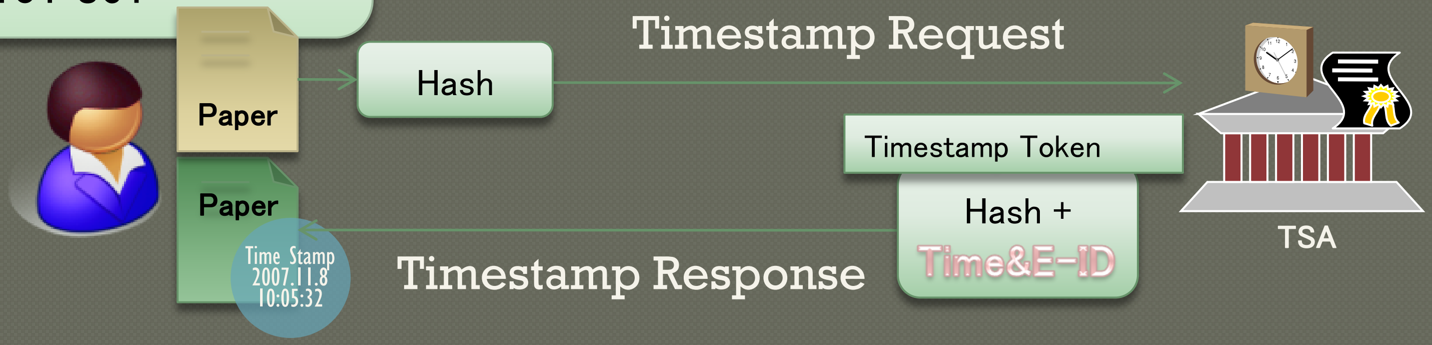
Timestamp

- The timestamp (TS) technology guarantees existential evidence of digital documents.
- The combination of ES and TS, as indicated by ES-T in Figure, ensures the authenticity of the digital documents.

Timestamp

Timestamp technology guarantees existential evidence of the digital documens

International Standard
- RFC 3161
- ETSI TS 101 861



Paper

Hash

Timestamp Request

TSA

Timestamp Token

Hash +
Time&E-ID

Timestamp Response

Paper

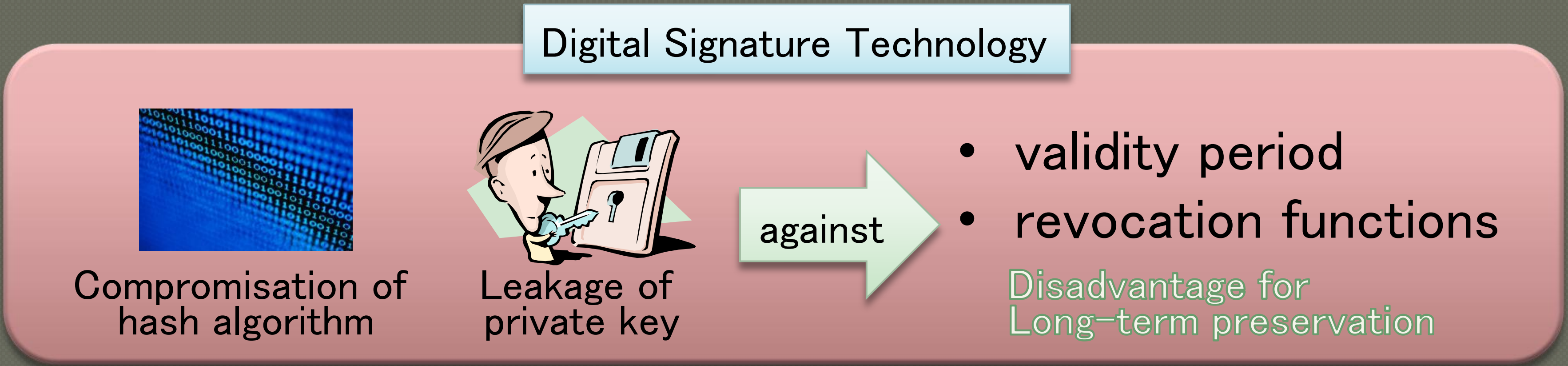
Time Stamp
2007.11.8
10:05:32

- Application of the TS to Research Paper
  - Publication Date
  - Contents

} can be certified

Disadvantage of ES&TS

Electronic signature and timestamp are useful technology however…



Digital Signature Technology

Compromisation of hash algorithm

Leakage of private key

against

- validity period
- revocation functions

Disadvantage for Long-term preservation

Long-term signature

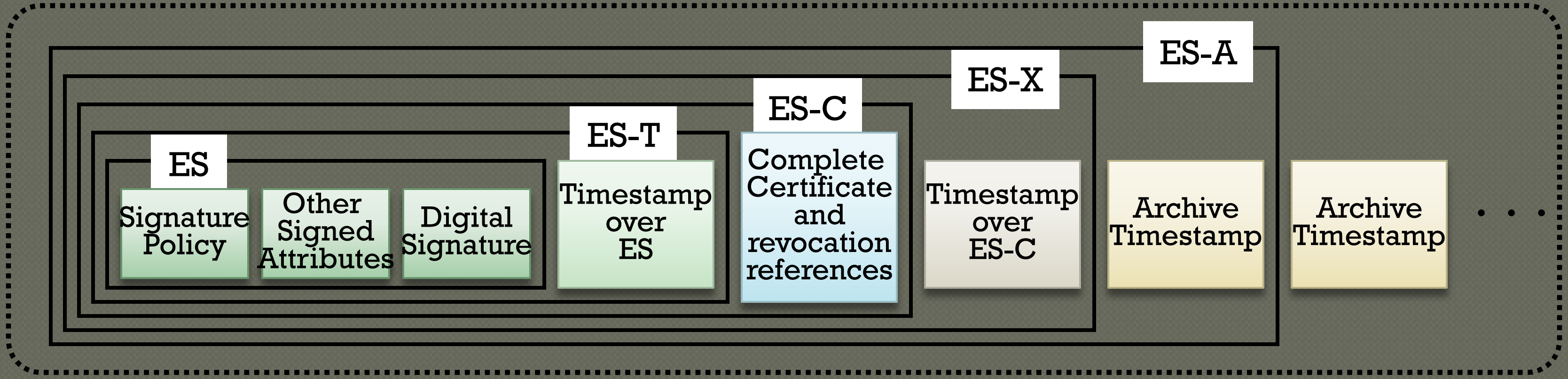
- solves disadvantage of ES and TS above
- embeds a complete certificate and revocation reference
- International standard RFC 3126

Long-Term Signature

- The ES and TS have a validity period and revocation functions. However, the temporary nature of these functions causes a problem for long-term preservation.
- To solve this problem, a long-term signature has been proposed.
- This signature format embeds a complete certificate and revocation references shown as ES-C.
- Therefore, ES and TS can be verified even after the signature expires.
- This study employed international standard RFC3126 as a long-term signature format and applied it to the article PDF documents.

Long-Term Signature

Long-term Signature Format(RFC3126)

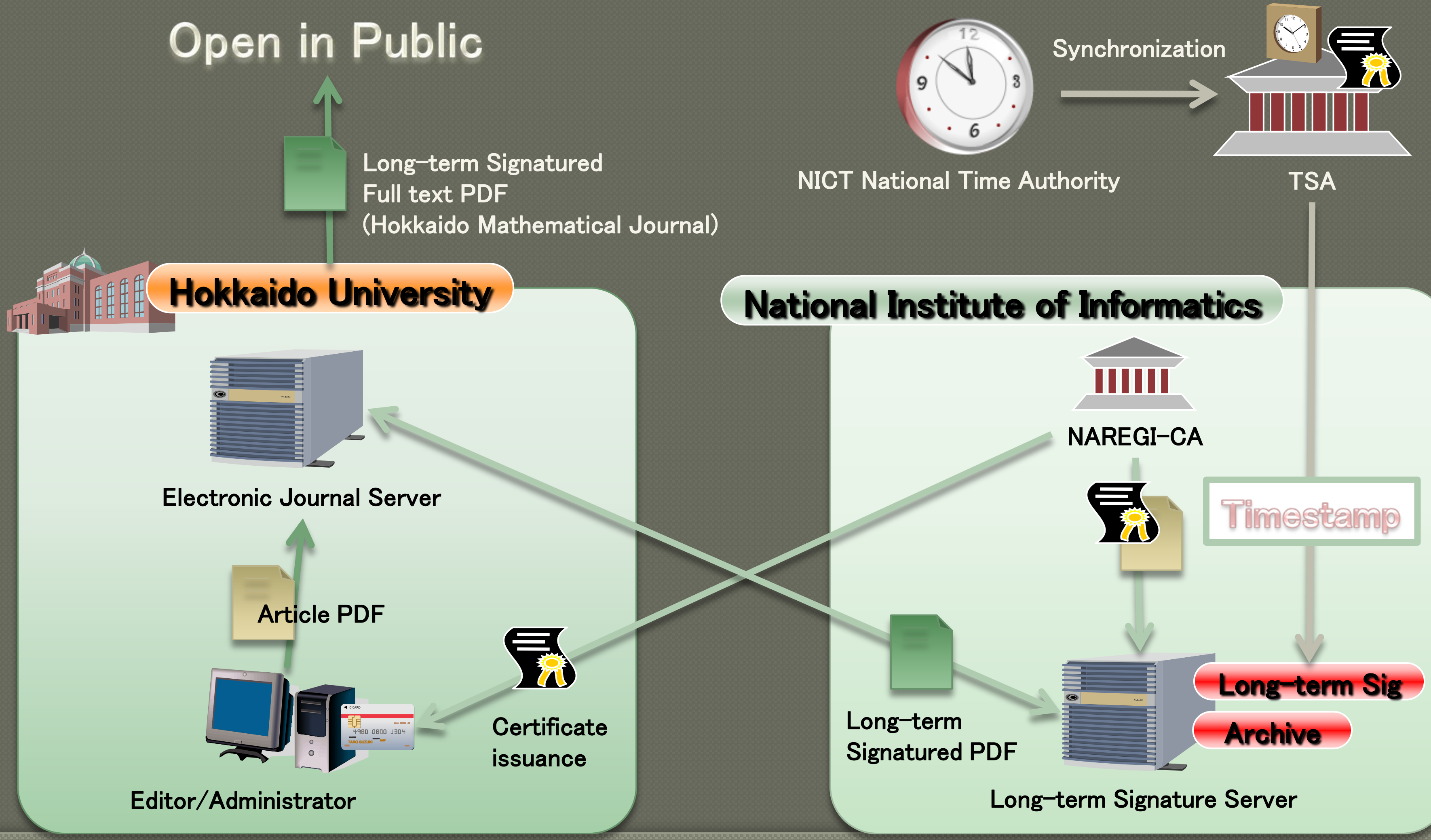


Application of LTS to Full text PDF

System Environment

- Application of the long-term signature requires a certification authority (CA) server and long-term signature server. The CA issues a digital certificate to a user who would like to register a document on the server.
- CA was established by NAREGI-CA which is an open source software originally developed for grid computing .
- The long-term signature server obtains a timestamp token from the time stamping authority managed by a trusted third party.

System Archtecture



Open in Public

Long-term Signatured
Full text PDF
(Hokkaido Mathematical Journal)

NICT National Time Authority

Synchronization

TSA

Hokkaido University

Electronic Journal Server

Article PDF

Editor/Administrator

Certificate
issuance

National Institute of Informatics

NAREGI-CA

Timestamp

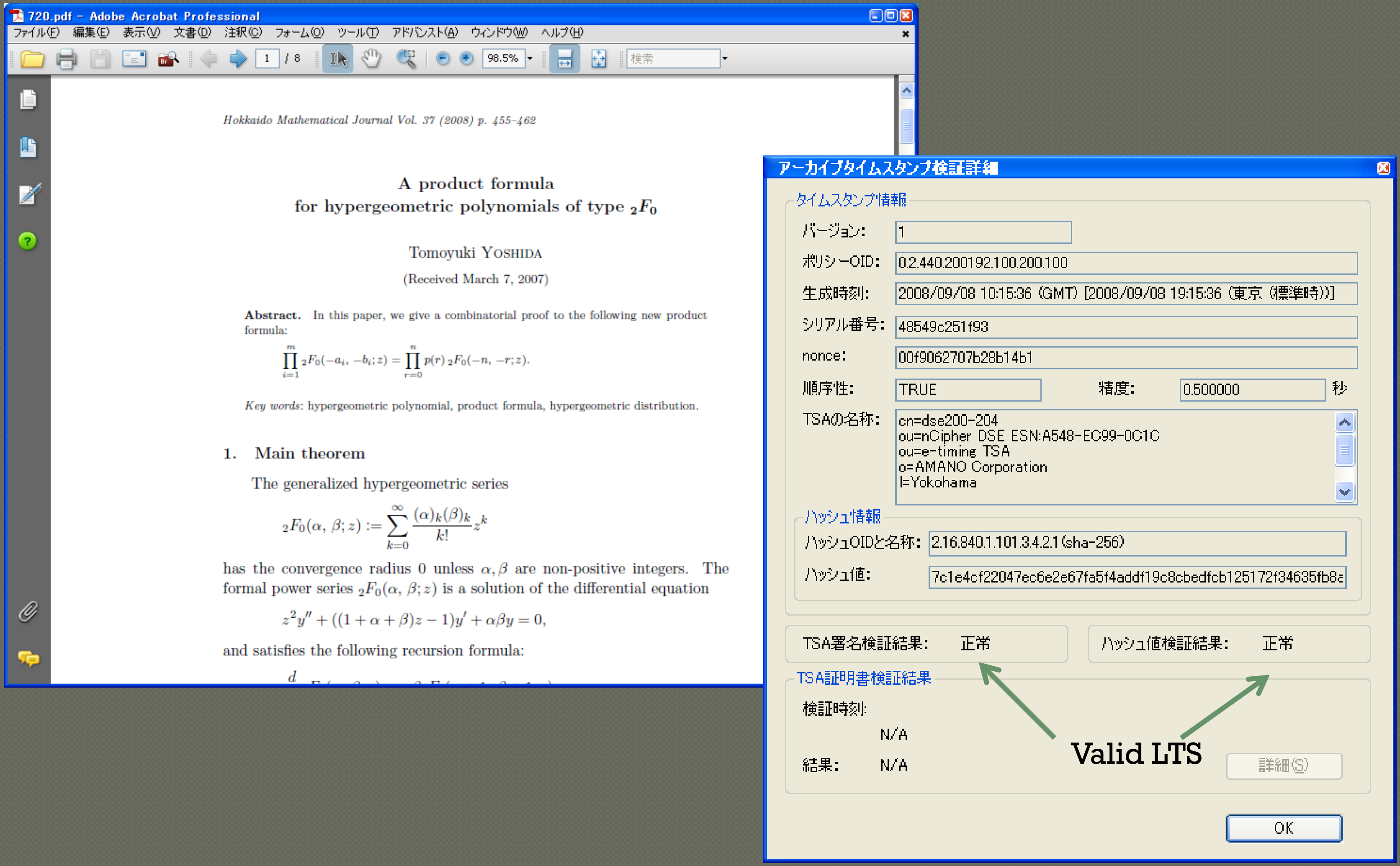
Long-term
Signatured PDF

Long-term Sig

Archive

Long-term Signature Server

LTSed Fulltext PDF Sample


720.pdf - Adobe Acrobat Professional
ファイル(F) 編集(E) 表示(V) 文書(D) 注釈(C) フォーム(O) ツール(T) アドバンスト(A) ウィンドウ(W) ヘルプ(H)
1 / 8
98.5%
検索
アーカイブタイムスタンプ検証詳細
詳細(S)
OK

Hokkaido Mathematical Journal Vol. 37 (2008) p. 455–462

A product formula for hypergeometric polynomials of type $_2F_0$

Tomoyuki YOSHIDA

(Received March 7, 2007)

Abstract. In this paper, we give a combinatorial proof to the following new product formula:

$$\prod_{i=1}^{m} {}_2F_0(-a_i,\ -b_i; z) = \prod_{r=0}^{n} p(r)\, {}_2F_0(-n,\ -r; z).$$

Key words: hypergeometric polynomial, product formula, hypergeometric distribution.

1. Main theorem

The generalized hypergeometric series

$$ {}_2F_0(\alpha,\ \beta; z) := \sum_{k=0}^{\infty} \frac{(\alpha)_k(\beta)_k}{k!} z^k $$

has the convergence radius 0 unless α, β are non-positive integers. The formal power series $_2F_0(\alpha,\ \beta; z)$ is a solution of the differential equation

$$ z^2y'' + ((1+\alpha+\beta)z - 1)y' + \alpha\beta y = 0, $$

and satisfies the following recursion formula:

タイムスタンプ情報

バージョン: 1
ポリシーOID: 0.2.440.200192.100.200.100
生成時刻: 2008/09/08 10:15:36 (GMT) [2008/09/08 19:15:36 (東京 (標準時))]
シリアル番号: 48549c251f93
nonce: 00f9062707b28b14b1
順序性: TRUE 精度: 0.500000 秒
TSAの名称: cn=dse200-204
ou=nCipher DSE ESN:A548-EC99-0C1C
ou=e-timing TSA
o=AMANO Corporation
l=Yokohama

ハッシュ情報

ハッシュOIDと名称: 2.16.840.1.101.3.4.2.1 (sha-256)
ハッシュ値: 7c1e4cf22047ec6e2e67fa5f4addf19c8cbedfcb125172f34635fb8a

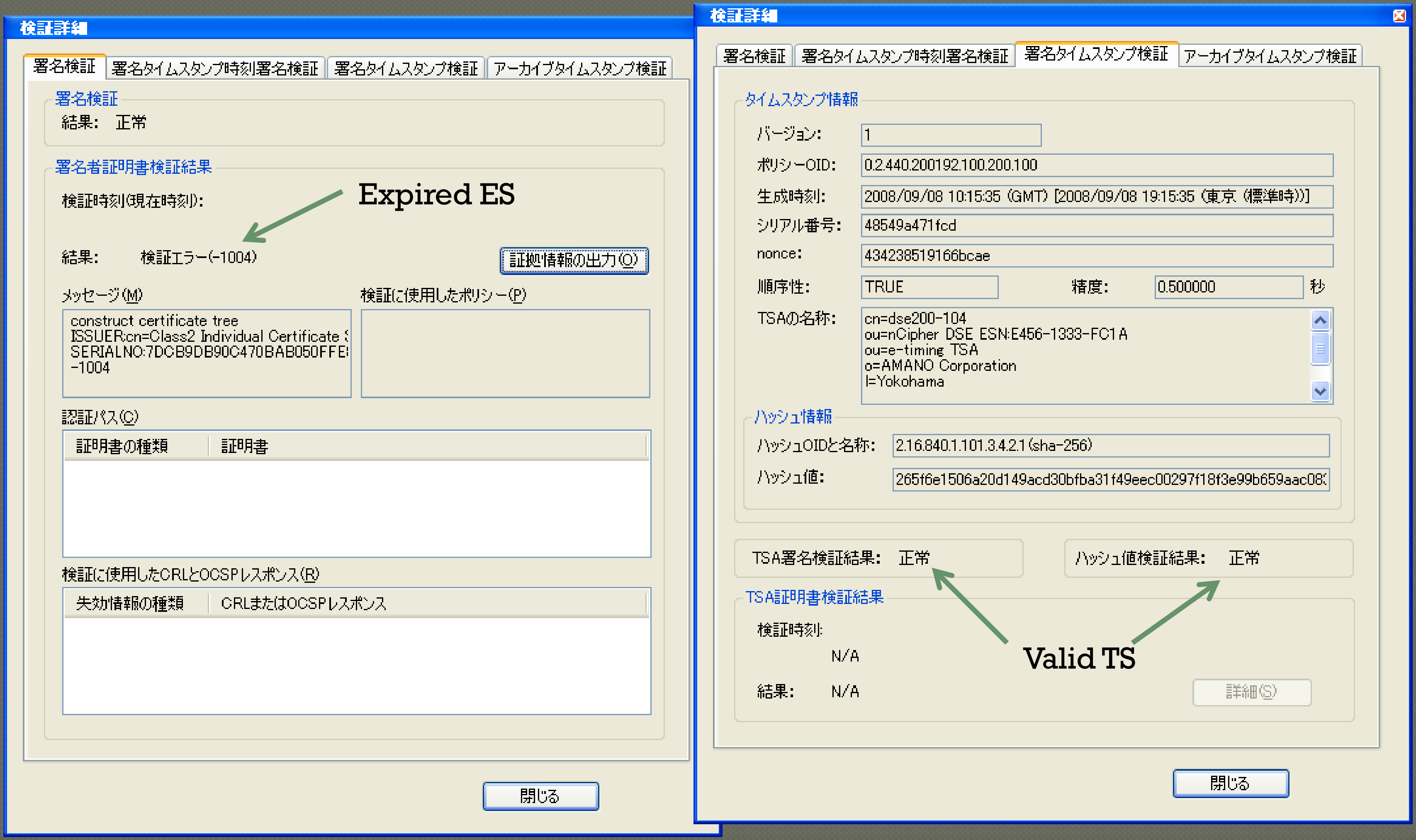
TSA署名検証結果: 正常
ハッシュ値検証結果: 正常

TSA証明書検証結果

検証時刻: N/A
結果: N/A

Valid LTS

Validation Example



検証詳細

署名検証 | 署名タイムスタンプ時刻署名検証 | 署名タイムスタンプ検証 | アーカイブタイムスタンプ検証

署名検証

結果:　正常

署名者証明書検証結果

検証時刻(現在時刻):

結果:　検証エラー(-1004)

Expired ES

証拠情報の出力(O)

メッセージ(M)

```
construct certificate tree
ISSUER:cn=Class2 Individual Certificate :
SERIALNO:7DCB9DB90C470BAB050FFE
-1004
```

検証に使用したポリシー(P)

認証パス(C)

証明書の種類	証明書

検証に使用したCRLとOCSPレスポンス(R)

失効情報の種類	CRLまたはOCSPレスポンス

閉じる

検証詳細

署名検証 | 署名タイムスタンプ時刻署名検証 | 署名タイムスタンプ検証 | アーカイブタイムスタンプ検証

タイムスタンプ情報

バージョン: 1

ポリシーOID: 0.2.440.200192.100.200.100

生成時刻: 2008/09/08 10:15:35 (GMT) [2008/09/08 19:15:35 (東京 (標準時))]

シリアル番号: 48549a471fcd

nonce: 434238519166bcae

順序性: TRUE　精度: 0.500000 秒

TSAの名称:
cn=dse200-104
ou=nCipher DSE ESN:E456-1333-FC1A
ou=e-timing TSA
o=AMANO Corporation
l=Yokohama

ハッシュ情報

ハッシュOIDと名称: 2.16.840.1.101.3.4.2.1 (sha-256)

ハッシュ値: 265f6e1506a20d149acd30bfba31f49eec00297f18f3e99b659aac08

TSA署名検証結果:　正常

ハッシュ値検証結果:　正常

Valid TS

TSA証明書検証結果

検証時刻:
N/A

結果:　N/A

詳細(S)

閉じる

Discussion

- Using Long-Term Signature technology published date and contents of full text PDF for electronic journal articles are certified.
- It works well even after embedded ES was expired.