2007－CSEC－39 (8)
2007／12／14

モバイルホストの負荷を軽減した失効機能をもつ匿名IEEE802.1X認証の実装

三木康平† 中西透†
川島潤† 舩曳信生†

インターネット接続のためのアクセスポイントにおけるモバイルホストの認証方式として，IEEE802.1X 認証が現在利用されている．従来の方式ではモバイルホストのプライバシー情報が通信事業者に漏洩する問題がある．我々はこの問題を解決するために，RSA 暗号に基づくグループ署名を用いた匿名認証方式を提案し，実装してきた．しかし，この匿名認証方式ではユーザ失効のためにシステムを利用するユーザ数に比例してモバイルホストの負荷が増大する問題がある．そこで本稿では，楕円曲線暗号に基づく署名者の負荷を軽減したグループ署名を利用することにより，モバイルホストの負荷を軽減した失効機能をもつ匿名 IEEE802.1X 認証の実装を行い，その評価を行う．

An Implementation of an Anonymous IEEE802.1X Authentication with User Revocation Reducing Mobile Host's Load

Kouhei Miki,† Toru Nakanishi,† Jun Kawashima† and Nobuo Funabiki†

The IEEE802.1X authentication has been used well as an authentication protocol in the Access Point for the Internet connection. There is a problem that mobile host's privacy information can be leaked to the Internet service provider in this protocol. To solve this problem, we have proposed and implemented an anonymous authentication with user revocation using the group signature. However, there is a problem of this method that mobile host's load increases in proportion to the number of moblie hosts in the system. In this paper, an anonymous IEEE802.1X authentication with a user revocation reducing mobile host's load is implemented by using a pairing-based group signature with verifier-local revocation, and the authentication time is evaluated.

1. はじめに

近年，モバイル端末の普及とともに，アクセスポイント（AP）と呼ばれる無線インターネット接続サービスが，インターネット接続事業者（ISP）により提供されている．AP の利用者は，あらかじめ ISP と契約してその利用権を得ることで，インターネットに接続できる．ISP は契約した利用者のみに接続サービスを提供するために，アクセス時にユーザ認証を行い，本人確認を行う．この認証規格の一つに IEEE802.1X があり[1]，現在，無線における AP での認証に利用されている．

AP におけるユーザ認証は，プライバシー問題を起こし得る．これは，利用者がどの場所の AP からいつ接続したか，インターネットでどこに接続したかを示す履歴を ISP が把握できるためである．もし，これらの履歴情報を第三者に漏洩されたとしても，ユーザは関知できない．さらに，ISP は利用者のプライバシー情報が大量となるため管理が繁雑となる．

このプライバシー問題を回避するため，我々はグループ署名と呼ばれる匿名認証技術を用いた匿名 IEEE802.1X 認証方式を提案・実装してきた[2]．さらに，失効可能なグループ署名を用い従来方式を拡張することで，ユーザ失効機能をもつ匿名 IEEE802.1X 認証方式（以下，従来方式）も提案・実装してきた[3]．この従来方式では，まずユーザ認証の際に認証サーバ（ISP）がモバイルホストに失効情報を送信する．次に，モバイルホストは受信した失効情報を基にグループ署名の作成を行い，認証サーバにグループ署名を送

† 岡山大学大学院自然科学研究科
Graduate School of Natural Science and Technology, Okayama University, E-mail:{miki, kawasima}@sec.cne.okayama-u.ac.jp, {nakanisi,funabiki}@cne.okayama-u.ac.jp

信する．このグループ署名を用いて認証サーバは匿名認証および失効を行う．

しかし，従来方式ではシステムを利用するユーザ数の増加に伴い，モバイルホストの負荷が増大するという問題がある．これは採用した RSA 暗号に基づくグループ署名方式（文献[4] 方式 1）の失効情報およびそれを基に作成されるグループ署名のデータサイズが，ユーザ数に依存し増加するためである．よって，ユーザ認証の際にモバイルホストは膨大なデータを送受信する必要がある．それに加え，ユーザ数に依存し，グループ署名を作成する時間も増加する．モバイルホストは一般に処理能力が低いため，その負荷の増大は大きな問題となる．

そこで本稿では，楕円曲線暗号に基づく署名者の負荷を軽減したグループ署名を利用し，失効機能をもつ匿名 IEEE802.1X 認証の実装を行う．その認証時間の評価を行い，有効性を示す．本実装では認証サーバの負荷が増す問題があるため，認証サーバの並列処理の有効性も示す．

以下，本稿の章構成を示す．2 章では IEEE802.1X 認証について示す．3 章では匿名認証を実現する従来方式とその問題点について示す．4 章ではモバイルホストの負荷を軽減した提案方式におけるユーザ失効，認証部分の実装方法と内部処理について示す．5 章では認証時間を示す．最後に 6 章で本稿のまとめを行う．

2. IEEE802.1X 認証

IEEE802.1X とは，LAN 内でユーザ認証を行うための方式を定めた規格である．IEEE802.1X では，EAP(Extensible Authentication Protocol) と呼ばれる通信プロトコルを認証に採用しており，「ユーザ ID・パスワード」による認証や，電子証明書による認証など，さまざまな認証方式に対応している．

未認証の端末は AP を通じて外部のネットワークには接続できない．認証サーバが端末の認証を完了すると，AP へ接続許可のパケットを送り，端末は AP を通じて外部のネットワークに接続が可能となる．

EAP には各種の認証方式が定義されている．その中で従来方式[3] では EAP-TTLS を利用している．

- EAP-TTLS
  認証端末は RADIUS 認証サーバから提供された電子証明書を利用してサーバ認証を行い，認証サーバはパスワードベースのユーザ認証を行う．この認証方式ではサーバ認証が行われるため，悪意を持つ第三者による認証サーバなりすましは回避できる．

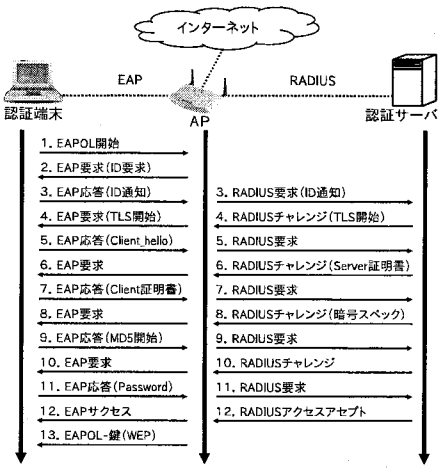

図 1 EAP-TTLS のプロトコルフロー

EAP-TTLS の処理の流れを図 1 に示す．従来方式は既存の EAP-TTLS 方式を基に実装されている．本研究では従来方式を拡張する．

3. 従来方式とその問題

以下，従来方式とその問題点を示す．

3.1 グループ署名を用いた匿名認証モデル

グループ署名では，グループ管理者（GM）と呼ばれる機関を必要とする．GM は，あるユーザがグループに加入し，メンバーとなることを許可する権限を持つ唯一の機関である．ユーザは GM からグループ証明書を発行してもらうことでグループ署名を作成可能となる．その署名を用いて匿名で正規ユーザであることを証明する．ただし，指定された追跡機関の検証者のみ，不正が発生した際に署名の作成者を特定できる（追跡可能性）．

従来方式のモデルを図 2 に示す．

- モバイルホスト
  ユーザのモバイル端末．認証時にはグループ署名の生成を行う．
- 認証サーバ
  RADIUS サーバ．認証時にはグループ署名の検証を行う．
- 管理サーバ
  GM．ユーザの個人情報を保持し，ユーザがグループに加入しメンバーとなることを許可する情報を管理する．また，追跡機関を兼ねており，不正発生時にはグループ署名の署名者を特定する．

3.2 失効機能をもつ匿名 IEEE802.1X 認証

従来方式に採用した失効機能を持つグループ署名方

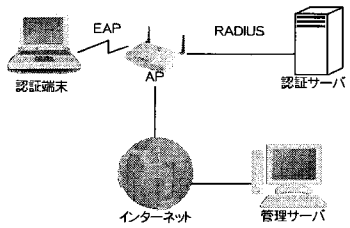

図 2 従来方式のモデル

式（文献[4] 方式 1）では失効発生時に GM が失効情報を生成し，署名者や検証者に配布する．そして最新の失効情報に基づいて失効されていないことを示す署名の作成や検証が行われる．したがって，グループ署名を用いてユーザ失効を行うためには GM である管理サーバが作成する失効情報をユーザと認証サーバに送信しなくてはならない．従来方式では，ユーザ失効時に管理サーバから認証サーバへ失効情報の送信を行い，ユーザ認証時に認証サーバからユーザへ失効情報を送信する．以下，採用したグループ署名およびそれぞれの処理について示す．

3.2.1 採用されたグループ署名

従来方式では，ユーザ失効可能であり高速に署名作成・検証が可能な文献[4] の方式 1 が用いられている．このグループ署名は以下の特徴がある．

- RSA 暗号ベースである
- ユーザごとに異なる素数情報を割り当てたグループ証明書を発行し，この素数情報に基づいてユーザの失効処理を実現する．失効情報は失効されていないユーザ全ての素数情報の積となる
- 失効可能な既存のグループ署名の中では比較的高速に署名の作成・検証が行える

実装において，鍵長は 2048bit である．また，文献[4] では方式 2 も提案されている．このグループ署名は以下の特徴がある．

- RSA 暗号ベースである
- 方式 1 と同様に，ユーザごとに素数情報を割り当てたグループ証明書を発行し，この素数情報に基づいて失効処理を実現する．失効情報は失効されたユーザ全ての素数情報の積となる
- 方式 1 に比べ高速に署名の作成・検証が行えるが，処理時間はユーザ数および失効されたユーザ数に依存する

比較のため，この文献[4] の方式 2 を用いた実装も行った．実装において，鍵長は 2048bit とした．

3.2.2 ユーザ失効

従来方式[3] における無線 LAN サービスを停止するためのユーザ失効処理について示す．管理サーバは，ユーザ失効が起こるたびに失効情報の更新を行う．更新後，全ての認証サーバに最新の失効情報を送信する．認証サーバでは最新の失効情報を認証に利用することでユーザ失効が可能となる．

3.2.3 ユーザ認証

従来方式[3] の認証処理について示す．

① 失効情報の送信
認証サーバは失効されたユーザに関する失効情報を保持している．この失効情報をユーザの認証端末に送信する．

② グループ署名の作成と送信
ユーザが保持しているグループ証明書と受信した失効情報を用いてグループ署名の作成を行う．その後，グループ署名を認証サーバに送信する．

③ グループ署名の検証
認証サーバにおいて，認証端末から受信したグループ署名の検証を行う．正しく検証が行われた場合，無線 LAN への接続を許可する．

3.3 モバイルホストの負荷増大の問題

従来方式において文献[4] の方式 1 を用いた場合の認証時間およびそのユーザ（モバイルホスト）の処理時間を図 3 に示す．ユーザの処理時間とは認証開始からグループ署名作成・送信までのユーザが認証に関与する時間のことを示す．ここで実験環境は 4.3 節と同じである．この認証方式では図 3 から分かるようにシステムを利用するユーザ数に比例してユーザの処理時間が増加する．これは採用したグループ署名方式（文献[4] 方式 1）の失効情報およびそれを基に作成されるグループ署名のデータサイズがユーザ数に比例し増加することが原因である．そのため，ユーザはユーザ認証の際に膨大なデータを送受信しなければならない．それに加え，グループ署名を作成する時間も増加する．よってユーザの負荷は増大する．

失効されたユーザ数が少ない場合の本問題の解決には，文献[4] 方式 2 の採用が考えられる．この方式は失効されたユーザが少ない場合に文献[4] の方式 1 に比べより高速に署名作成・検証可能であり，ユーザに与える負荷も小さい．よってより大規模なユーザ数に対しても実用的な時間で認証可能である．この方式を用いて 10%のユーザの失効状態を想定した場合の認証時間およびユーザの処理時間を図 4 に示す．

図 4 から分かるように，本方式でもユーザ数の増加に伴い認証時間およびユーザの処理時間が増加する．

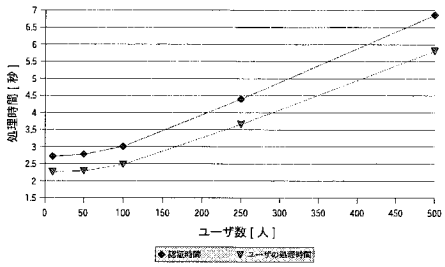

図 3 従来方式（文献[4] 方式 1）の認証時間

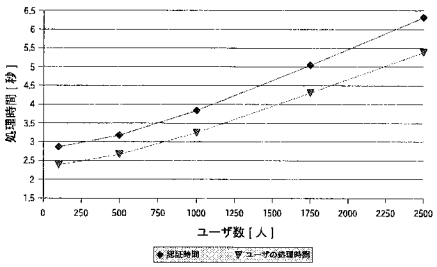

図 4 従来方式（文献[4] 方式 2）の認証時間

それに加え，この方式は失効されたユーザ数にも比例する．図 4 では 10%のユーザの失効状態を想定したが，20%，30%とより多くのユーザの失効状態では更に認証時間およびユーザの処理時間が増加する．これは，失効情報およびそれを基に作成されるグループ署名のデータサイズが，システムを利用するユーザ数と失効されたユーザ数に依存し増加することが原因である．よって，本方式でもユーザ負荷増大の問題は解決されない．一般にモバイルホストは固定端末に比べ処理能力が低い．そのため，このユーザの負荷・通信データ量の増大はモバイルホストをクライアントに想定した場合に大きな問題となる．

4. モバイルホストの負荷を軽減した失効機能をもつ匿名 IEEE802.1X 認証の実装

本研究では，楕円曲線暗号に基づく署名者の負荷を軽減したグループ署名を利用する．楕円曲線暗号ベースのグループ署名では，署名データサイズが RSA 暗号ベース方式に比べ小さくすることが可能である．それに加え採用するグループ署名方式では，Verifier-Local Revocation と呼ばれるユーザ失効法を用いている．この方法では，署名者の失効情報を GM がリスト化し，検証者のみに対して送信する．検証者は，その失効リストを用いて署名者の検証を行う．したがって，ユーザ失効を行うためには GM である管理サーバが作成する失効情報を認証サーバにのみ送信するだけでよい．これにより，従来方式のようにユーザ認証時に認証サーバからユーザへの失効情報の送信処理は不要となる．以下，採用したグループ署名および処理について示す．

4.1 採用したグループ署名

本実装では，楕円曲線暗号に基づく署名者の負荷を軽減した文献[5] の方式を用いた．このグループ署名は以下の特徴がある．

- 楕円曲線暗号ベースであるため，グループ署名のデータサイズを RAS 暗号ベースより短縮できる
- Verifier-Local Revocation と呼ばれる署名者に負荷のないメンバ失効法を用いている．
- 検証者は失効されたユーザ数に比例した計算を要する
- 検証者でのユーザ失効確認ステップの並列処理が容易に可能である

実装では，鍵長は RSA2048bit と同等のセキュリティレベルである 224bit 楕円曲線，埋め込み次数 12 に設定した．

4.2 ユーザ認証

提案方式の認証処理について示す．

① グループ署名の作成と送信
ユーザが保持しているグループ証明書を用いてグループ署名の作成を行う．その後，グループ署名を認証サーバに送信する．

② グループ署名を検証
認証サーバにおいて，失効情報のリストを基に認証端末から受信したグループ署名の検証を行う．正しく検証が行われた場合，無線 LAN への接続を許可する．失効されたユーザは検証に失敗するため，接続は許可されない．

提案方式では従来方式で必要なユーザへの失効情報の送信処理が不要となる．上記の①，②の認証処理については，従来方式で採用した EAP-TTLS を基に拡張し，新たに EAP-TTLS/GS として実装した．

4.2.1 EAP-TTLS/GS のパケットシーケンス

以下に，EAP-TTLS/GS の処理の流れを示す．EAP-TTLS からの変更点は図 1 の STEP10, STEP11, STEP12 の処理であり，他の処理は EAP-TTLS と同じである．

STEP10 ：EAP 要求 / RADIUS チャレンジ
認証サーバからユーザの認証端末へ 128bit の乱数を送信する．乱数は，認証サーバで保存する．

STEP11 ：EAP 応答 / RADIUS 要求

乱数の受信が終わった後に，認証端末はグループ署名の作成を行う (①の処理)．このとき，署名のメッセージとして認証サーバから受信した乱数を用いる．グループ署名作成後，認証端末から認証サーバへグループ署名の送信を行う．

STEP12 ：EAP 成功 / RADIUS アクセス許可

認証サーバは失効情報のリストと認証端末から受信したグループ署名を用いて，STEP10 の処理で保存した乱数をメッセージとして検証する (②の処理)．検証が成功した場合は認証サーバは AP に Access-Accept と呼ばれるコードの RADIUS パケットの送信を行い，失敗した場合は Access-Reject と呼ばれるコードの RADIUS パケットの送信を行う．

4.3 実装環境

認証端末，認証サーバの実装環境をそれぞれ表 1 に，表 2 に示す．認証端末は処理能力の低いモバイルホストを想定している．よって，本来の CPU (1.7GHz) のクロック周波数を 600MHz に強制設定して利用する．また，AP については BUFFALO WLM2-L11G を用いた．提案方式はオープンソースのソフトウェア Xsupplicant 及び FreeRADIUS に EAP-TTLS/GS に基づく通信処理とグループ署名作成・検証処理を組み込んだ．

表 1 認証端末の実装環境

認証端末	Xsupplicant-1.2.8 (+libdnet-1.10, Openssl-0.9.8d, gmp-4.2.1)
OS	GentooLinux kernel-2.6.16-gentoo-r7
CPU	PentiumM 600MHz
Mem	512MB
無線 LAN	Intel(R) PRO/Wireless LAN 2100 IEEE802.11b 11Mbps にて接続

表 2 認証サーバの実装環境

認証サーバ	FreeRADIUS-1.1.6 (+Openssl-0.9.8e, gmp-4.2.1)
OS	UbuntuLinux7.04 kernel-2.6.20.16-generic
CPU	Intel Xeon 1.86GHz
Mem	2.5GB
NIC	Intel(R) 82547EI. 100Mbps にて接続

5. 実行結果と評価

5.1 実行結果

本研究の提案方式の認証時間を図 5 に，ユーザの処理時間を図 6 に，通信データ量を 7 に示す．各図は 10%のユーザの失効状態を想定している．また，比較のため従来方式（文献[4] 方式 2）も各図に示す．

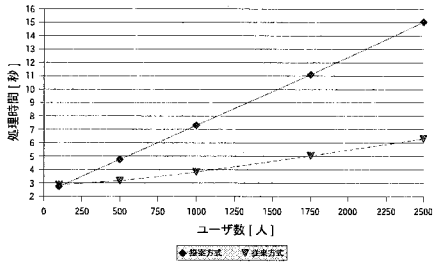

図 5 認証時間の比較

認証時間ではユーザ数が 100 人の場合，従来方式では約 2.86 秒，提案方式は約 2.74 秒であった．両方式に大きな差は無く，実用的と言える．ユーザ数が 2500 人の場合，従来方式では約 6.32 秒，提案方式は約 15.04 秒であった．提案方式のユーザ数増加に伴う認証時間の増加率は従来方式に比べ高い．これは提案方式での認証サーバにおける処理時間が失効されたユーザ数に大きく依存しているためである．しかし後で示すように高性能サーバを利用することにより，この処理時間は大きく軽減される．

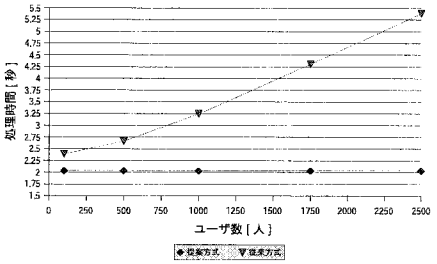

図 6 ユーザの処理時間の比較

ユーザの処理時間は，ユーザ数が 100 人の場合，従来方式では約 2.39 秒，提案方式では約 2.03 秒であった．ユーザ数が 2500 人の場合，従来方式では約 5.38 秒，提案方式では約 2.03 秒であった．従来方式はユーザ数の増加に伴い，ユーザの処理時間は増加している．それに対して提案方式では，ユーザ数に依存せず，約 2.03 秒となっている．これにより提案方式では従来方式に比べ非常に高速になっており，ユーザの負荷が大きく軽減されていることが分かる．

通信データ量ではユーザ数が 100 人の場合，従来方式では約 2044Byte，ユーザ数が 2500 人の場合，従来

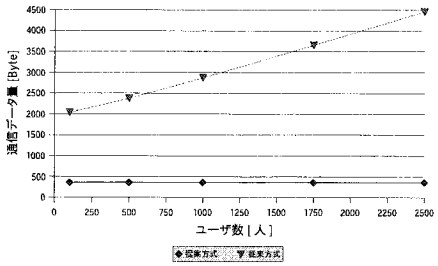

図 7 通信データ量の比較

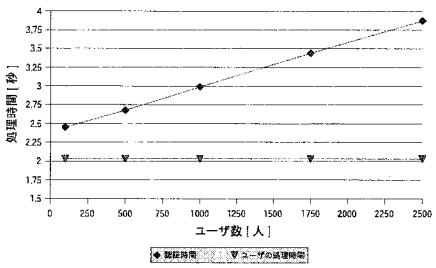

図 8 認証時間 (8 コア)

方式では約 4464Byte であった．従来方式はユーザ数増加に伴い，通信データ量は増大している．それに対して提案方式では，ユーザ数に依存せず 364Byte で一定となっており大幅に削減されている．EAP パケットサイズは Ethernet の MTU(1500Byte) に依存しており，一つの EAP パケットに入るデータの大きさは約 1460Byte である．従来方式は通信データが EAP パケットサイズを超えるためデータの分割送信が必須となるが，提案方式はデータサイズがユーザ数に依存せず 364Byte で一定であるため，一つのパケットで送信可能となる．よって，分割送信の負荷も無くなる．

以上より，ユーザ数増加に伴う認証時間の増加率は従来方式に比べ大きいが，ユーザの処理時間はおよび通信データ量は大きく改善されている．これは今回採用したグループ署名方式（文献[5]）において，ユーザの負荷である署名作成処理およびグループ署名のデータサイズがユーザ数に依存せず一定であるためである．よって，処理能力の低いモバイルホストをクライアントに想定した場合，ユーザの負荷を軽減した提案方式が有効であるといえる．

5.2 並列処理による効果

採用したグループ署名方式は署名検証の並列処理が可能である．よって，複数コアを持つ Xeon で並列処理を行った場合，署名検証の高速化が期待される．そこで認証サーバに Xeon を利用し，最大 8 コアを用いた場合の認証時間を図 8 に示す．

ユーザ数が 100 人の場合，認証時間は約 2.45 秒，2500 人の場合，認証時間は約 3.87 秒であった．並列処理を行うことでサーバの処理時間（署名検証）は大幅に削減され，認証時間は従来方式と同等の認証時間になった．これにより，並列処理を取り入れることによる有効性が確認できたといえる．但し，本環境では実用的な認証時間を 3 秒程度とすると，ユーザ数 1000 人程度（失効されたユーザ数 100 人程度）が実用的な認証時間の範囲といえる．

6. ま と め

本稿では，モバイルホストの負荷を軽減した失効機能をもつ匿名 IEEE802.1X 認証の実装を行った．提案方式では，楕円曲線暗号に基づく署名者の負荷を軽減したグループ署名を用いることで，モバイルホストの負荷であるグループ署名作成処理および通信データ量の両方の改善を実現した．また，提案方式の認証時間を測定し従来方式との比較を行った．認証時間に関しては従来方式に比べより時間を要するが，ユーザの処理時間は従来方式に比べ非常に高速であり，ユーザ数に依存せず約 2.03 秒であった．また，認証サーバにおいて複数コアによる並列処理を行うことで更なる高速化が可能であった．今後の課題として，より大規模なユーザ数に対しても高速に認証可能な方式への改良が挙げられる．

謝辞 本研究は総務省による受託研究「情報の来歴管理等の高度化・容易化に関する研究開発」の助成を受けて行われた．

参 考 文 献

1) Mattbew S. Gast 著，水野忠則 他訳，“802.11 Wireless Networks，” O'REILLY, 2004.
2) 高橋秀郎，川島潤，中西透，舩曳信生，“モバイルホストのプライバシーを秘匿する IEEE802.1X 認証の提案と実装，” SCIS, 2D4-3, Jan, 2006.
3) 三木康平，中西透，川島潤，舩曳信生，“ユーザ失効を考慮した匿名 IEEE802.1X 認証の実装，” CSEC, pp.129-134, 2007-3-1.
4) 濱田直人，中西透，舩曳信生，“所属無効化可能なグループ署名方式の素数情報を用いた高速化とその実装，” ISEC, pp.47-54, Jan,2006-12-13.
5) 平雄太，加藤英洋，中西透，野上保之，舩曳信生，森川良孝，“署名者の負荷を軽減した失効機能をもつペアリングを用いたグループ署名方式の実装，” ISEC, pp.69-76, Jan,2007-09.