L-006

双方向放送サービスのための効率的なプロバイダ認証
An Efficient Provider Authentication for Bidirectional Broadcasting Service

大竹 剛† 花岡 悟一郎‡ 小川 一人†
Go Ohtake Goichiro Hanaoka Kazuto Ogawa

1. はじめに

双方向放送サービスにおいて，視聴者の個人情報を安全に送受信するため，放送局へのなりすましを防止するプロバイダ認証が必要である．放送局の署名鍵が漏洩した場合に備え，署名鍵の更新が必要であるが，一般的な署名方式の場合，検証鍵の更新・再配布のコストが非常に高い．この課題を解決するため，我々は Key-Insulated 署名[1]を用いたプロバイダ認証システムを提案した[2]．提案システムでは，放送局が署名鍵を更新しても検証鍵の更新が不要であり，コストの削減が可能である．一方，双方向放送サービスの場合，署名長に関する効率性が強く要求される．本稿では，我々が提案した，署名長が短い効率的な Strong Key-Insulated 署名[3][4]を上記のプロバイダ認証システムに実装し，性能評価実験を行ったので報告する．

2. プロバイダ認証システム

文献[2]で提案した，Key-Insulated 署名を用いたプロバイダ認証システムを図 1 に示す．

2.1 提案システムの概要

放送局の鍵管理サーバにおいて，マスター鍵，検証鍵，初期署名鍵を生成する．マスター鍵を安全に管理しておくとともに，初期署名鍵を個人情報管理サーバに送信する．また，コンテンツの暗号を解くための復号鍵と，プロバイダ認証に必要な検証鍵を格納した CAS カードを視聴者に配布しておく．コンテンツサーバはネットワークを通して暗号化コンテンツを配信する．受信端末では，挿入された CAS カードを用いてコンテンツを復号し，視聴する．一方，鍵管理サーバはマスター鍵と時刻情報を用いて任意の時間に部分鍵を生成し，個人情報管理サーバに送信する．個人情報管理サーバは部分鍵と以前に使用した署名鍵を用いて署名鍵を更新する．署名鍵は次の更新時期まで有効な署名鍵となる．受信端末に対し個人情報のリクエストを送信する際に，有効期限付き署名鍵を用いて放送局の署名を付加する．受信端末では，署名生成時刻と検証鍵を用いて，署名検証（プロバイダ認証）を行う．検証に成功した場合のみ，受信端末で管理している視聴者の個人情報を，ネットワークを通して個人情報管理サーバに送信する．署名鍵更新の期間は任意であるが，例えば利便性を考慮し，毎日 1 回更新する．この場合，その日の署名が付加されたリクエスト以外は全て受信端末で無視する．これにより，署名鍵の有効期間を 1 日に設定することが可能となる．

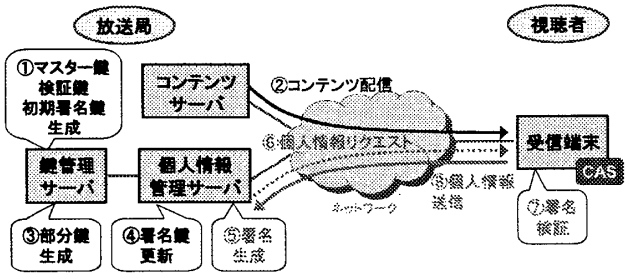

図1．プロバイダ認証システム

2.2 提案システムの特徴

本システムでは，プロバイダの署名鍵漏洩に対し，速やかに復旧を行うため，Key-Insulated 署名を採用している．署名鍵漏洩・更新時に，従来の PKI を用いた放送システムにおいて必要とされた，署名鍵失効を通知するための CRL をカルーセル伝送する必要がなく，伝送容量を有効に活用できる．また，署名鍵を更新しても検証鍵は変化せず，CAS カードの再配布が不要となる．鍵更新は任意の時刻に，時間的ロスを伴うことなく実行可能であり，リアルタイム性を有する放送に適している．さらに，鍵更新機能を有する Forward-Secure 署名[5]では実現できない Backward-Security を実現している．すなわち，漏洩した署名鍵から過去に使用した署名鍵，もしくは，今後使用する署名鍵の偽造を不可能とし，署名鍵漏洩の被害を最小限にしている．

3. 効率的な Strong Key-Insulated 署名

文献[3][4]で提案した，効率的な Strong Key-Insulated 署名について述べる．通常の Key-Insulated 署名は署名鍵の漏洩のみ耐性があるのに対し，Strong Key-Insulated 署名はマスター鍵の漏洩にも耐性がある．

3.1 提案方式の構成

【鍵生成アルゴリズム】

素数 $p,q(q|p-1)$ と，乗法群 Z_p^* の元 g を選ぶ．ここで，g は Z_p^* 上に構成される位数 q の部分群の生成元となるものとする．次に，x, x_0 を Z_q からランダムに選び，マスター鍵 $x_0 = x - x'$ をセキュアデバイス内に管理し，x' を署名者が管理する．そして，$y_0 = g^{x_0} \bmod p$，$y' = g^{x'} \bmod p$ を求め，検証鍵 $VK = \langle p,q,g,y_0,y',G(\cdot,\cdot),H(\cdot,\cdot,\cdot,\cdot)\rangle$ を公開する．ここで，G，H はハッシュ関数 $G: Z_p^* \times \{0,1\}^* , H: Z_p^* \times Z_p^* \times \{0,1\}^* \times \{0,1\}^*$ である．

【部分鍵生成アルゴリズム】

セキュアデバイス内において，乱数 r_1 を Z_q からランダムに選び，$v_1 = g^{r_1} \bmod p$ を求める．次に，時刻情報 T を用いて $c_1 = G(v_1, T)$ を求め，さらにマスター鍵 x_0 を用いて部分鍵 $x_1 = c_1 r_1 + x_0 \bmod q$ を求め，x_1, v_1, T を署名者に送る．署名者は $c_1 = G(v_1, T)$ を求め，$g^{x_1} = v_1^{c_1} y_0 \bmod p$ が成り立つかどうか検証を行う．

【鍵更新アルゴリズム】

部分鍵の検証に成功した場合のみ，x' を用いて時刻 T の署名鍵 $SK_T = x_1 + x' \bmod q$ を求め，署名鍵の更新を行う．

† 日本放送協会 Japan Broadcasting Corporation
‡ 産業技術総合研究所 National Institute of Advanced Industrial Science and Technology

【署名生成アルゴリズム】
署名者は，乱数 r_s を Z_q からランダムに選び，$v_s = g^{r_s} \bmod p$ を求める．次に，メッセージ m と署名生成時刻 T を用いて $c_s = H(v_1, v_s, T, m)$，$\sigma_s = c_s r_s + SK_T \bmod q$ を求め，$m, (\sigma_s, c_s, v_1), T$ を検証者に送る．
【署名検証アルゴリズム】
検証者は $c_1 = G(v_1, T)$ を求め，
$$c_s = H(v_1, (g^{\sigma_s}(v_1^{c_1} y_0 y')^{-1})^{1/c_s} \bmod p, T, m)$$
が成り立つかどうか検証を行う．

3.2 提案方式の特徴

本方式は，署名鍵の漏洩だけでなく，マスター鍵の漏洩も考慮した Strong Key-Insulated 署名である．従来の Strong Key-Insulated 署名に比べ，鍵長，署名長，計算量の点で効率的な方式であり，特に署名長が短いため，多数の署名付きメッセージが送受信される双方向放送サービスに適した方式である．なお，本方式は離散対数問題が困難であるという仮定の下で，安全性が証明可能である．

4. 性能評価実験

3 章で述べた署名長が短い効率的な Strong Key-Insulated 署名を，2 章で述べたプロバイダ認証システムに実装し，性能評価実験を行った．

4.1 実験の概要

PC 3 台を用いて図 1 のプロバイダ認証システムを構築し，3.1 節で述べた Strong Key-Insulated 署名のアルゴリズムを C++言語を用いて実装した．システムの諸元を表 1 に示す．本システムを用いて，3.1 節の各アルゴリズムの処理時間を測定し，効率性の検証を行った．

4.2 実験結果・考察

実験結果を表 2 に示す．表の 1 列目は Strong Key-Insulated 署名のアルゴリズムを表しており，Gen は鍵生成，Upd*は部分鍵生成，Upd は鍵更新，Sign は署名生成，Vrfy は署名検証のアルゴリズムをそれぞれ表す．2 列目は各アルゴリズムを実行するエンティティを表しており，KMS は鍵管理サーバ，PIMS は個人情報管理サーバ，UT は受信端末を表す．3 列目は各アルゴリズムの処理時間を表す．表 2 に示す通り，Gen と Upd*は KMS で実行され，Upd と Sign は PIMS で実行され，Vrfy は UT で実行される．放送局の検証鍵は UT に挿入されている CAS カードに格納されるが，Vrfy は（CAS カードではなく）UT の内部で実行される．なお，Upd*-Upd は KMS における Upd*から PIMS における Upd までの一連の（サーバ間通信を含む）鍵更新処理を表す．また，処理時間については，各アルゴリズムを 1000 回実行し，平均を求めた値である．KMS－PIMS 間および PIMS－UT 間のネットワークは TCP/IP で接続する．

実験の結果，Gen の処理時間が 2183.450 (msec) と長いことが分かった．しかし，Gen が実行されるのはシステムの初期化の時のみであり，システムに与える影響は少ない．Upd*, Upd, Sign, Vrfy の処理時間はそれぞれ 3.791(msec), 7.461 (msec), 3.463 (msec), 15.520 (msec)となっており，非常に短い．Sign, Vrfy の処理は双方向番組の放送時間中に送信される個人情報リクエストの際に実行されるが，その回数は 1 時間に数回程度である．10 万人の視聴者に対するリクエストに署名を生成する時間は，最長でも 3.463 (msec)×10^5 = 346.3 (sec) ≒ 6 (min) であり，PIMS の負担は少ない．Upd*-Upd の処理時間は 218.352 (msec)と長いが，そのほとんどは 2 つのサーバ間の通信に要する処理時間である．2 章で述べたとおり，本システムでは放送局の署名鍵更新の頻度は 1 日 1 回であるため，Upd*-Upd の処理も 1 日 1 回だけ実行される．従って，3 章の Strong Key-Insulated 署名は，計算量の点においても実用的であることが，システム実装による性能評価実験で分かった．

表 1．システム諸元

鍵管理サーバ（KMS）	
CPU	Intel Core2 Duo (E4400) 2.00GHz
メモリ	512MB
OS	Windows XP SP2
個人情報管理サーバ（PIMS）	
CPU	Intel Core2 Duo (E4400) 2.00GHz
メモリ	512MB
OS	Windows XP SP2
受信端末（UT）	
CPU	Intel Pentium 4 2.80GHz
メモリ	512MB
OS	Windows XP SP2

表 2．実験結果

アルゴリズム	エンティティ	処理時間 (msec)
Gen	KMS	2183.450
Upd*	KMS	3.791
Upd	PIMS	7.461
Upd*-Upd	KMS, PIMS	218.352
Sign	PIMS	3.463
Vrfy	UT	15.520

5. まとめ

本稿では，我々が提案した，署名長が短い効率的な Strong Key-Insulated 署名をプロバイダ認証システムに実装し，性能評価実験を行った．提案する Strong Key-Insulated 署名方式は，署名長や鍵長の効率性だけでなく，計算量の点においても実用的であり，双方向放送サービスにおいて効率的なプロバイダ認証が実現可能である．今後は，実際の放送システムへの適用を検討する予定である．

参考文献

[1]Y. Dodis, J. Katz, S. Xu, and M. Yung, “Strong Key-Insulated Signature Schemes.”, Proc. of PKC2003, LNCS 2567, pp.130–144. (2002).
[2]G. Ohtake, G. Hanaoka, and K. Ogawa, “Provider Authentication for Bidirectional Broadcasting Service with Fixed Verification Key.”, Proc. of ISITA2006, pp.155–160. (2006).
[3]大竹剛,花岡悟一郎,小川一人, “双方向放送サービスのための効率的な Strong Key-Insulated 署名”, 信学技報, Vol. 107, No. 141, ISEC2007-65, pp. 133–139 (2007).
[4]G. Ohtake, G. Hanaoka, and K. Ogawa, “An Efficient Strong Key-Insulated Signature Scheme and Its Application”, Proc. of EuroPKI2008, LNCS 5057, pp.150–165. (2008).
[5]M Bellare, and S. Miner, “A Forward-Secure Digital Signature Scheme.”, Proc. of Crypto1999, LNCS 1666, pp.431–448. (1999).