Vol.2018-CSEC-82 No.7
Vol.2018-SPT-29 No.7
2018/7/25

情報ハイディング可能なワンタイムパスワード認証方式

須賀 祐治[1,a)]

概要：2 者間（サーバ・クライアント形式）のプロトコルにおいて事前にセキュアチャネルを通して秘密の共有パラメータを交換しているという前提において，通常の通信に紛れ込ませ，第 3 者には何も情報を漏らすことなく秘密情報を交換する技術を一般的に情報ハイディング技術と呼ぶ．これを安全な暗号学的一方向性ハッシュ関数を用いて構成された計算量も通信量も非常に軽い Lamport ワンタイムパスワード認証方式に適用させることは検討されている．
本稿は，この検討において積極的に情報交換を行う「情報交換ファースト」ではなく，長期に渡って認証を何度か行うことでいつの間にか情報が交換されていたという「情報ハイディング」という副産物を着眼としていくつかのハイディング方式について検討を行う．既提案では事前共有された「ソーセージ」を無駄に食い尽くしていたが，これを大きく見直すことで Lamport 認証方式と同じ通信量で実現可能であり第 3 者からは Lamport 認証方式を行っているように見せかけて情報ハイディングを行う方式を提案する．またナイーブな提案方式では transable secret ratio を 1/3 程度であるが，さらに情報を埋め込む方式についても提案を行う．

キーワード：ワンタイムパスワード認証，ハッシュチェーン，Merkle Tree，情報ハイディング

A proposal of one-time password authentication schemes with information hiding

Yuji Suga[1,a)]

1. バックグラウンド

2 者間（サーバ・クライアント形式）のプロトコルにおいて事前にセキュアチャネルを通して秘密の共有パラメータを交換しているという前提において，通常の通信に紛れ込ませ，第 3 者には何も情報を漏らすことなく秘密情報を交換する技術を一般的に情報ハイディング技術と呼ぶ．これを 30 年以上前に提案されており，安全な暗号学的一方向性ハッシュ関数を用いて構成された計算量も通信量も非常に軽い Lamport ワンタイムパスワード認証方式 [1] に適用させることは検討されている [4]．

1.1 ソーセージ型認証

BWCCA2017 にて提案された方式について紹介する．ソーセージ型認証方式は Lamport-like なワンタイムパスワード方式の拡張である．Lamport 認証方式はハッシュ連鎖を一つ一つ解きほぐすことで得られたワンワイムパスワードをクライアントが送信し，サーバでの確認によりユーザ認証を行う方式であり，ハッシュ値（ダイジェスト）の羅列はちょうどハッシュチェーンと呼ばれる一つのパスとして実現されている．

ソーセージ型認証方式ではこのハッシュ値を保持するデータ構造を拡張しており L 分木（バイナリツリーを含む）とマークルツリーを合成して実現されている．図 1 はソーセージ型認証方式のデータ構造を示したものである．

[1] 株式会社インターネットイニシアティブ
Internet Initiative Japan Inc., Iidabashi Grand Bloom, 2-10-2 Fujimi, Chiyoda-ku, Tokyo 102-0071, Japan
[a)] suga@iij.ad.jp

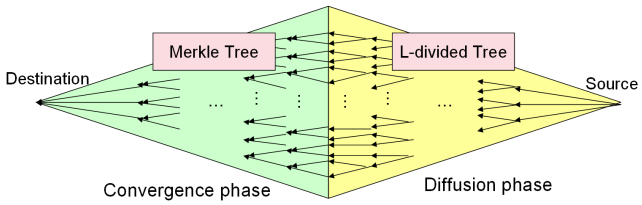

図 1 ソーセージ型認証の概略図

前半は拡散部と呼ばれ親ノードの元 p から L 個のノードの元 $p_i (i = 1, \ldots, L)$ を算出：

$$p_i := H(p||q_i)$$

することで得られる．ここで q_i はクライアントとサーバで共有されているものとし本稿では事前にサーバクライアントの両者で秘密裏に共有しているものとする．第 3 者が認証時に発生するデータを閲覧しても関係性が分からない，つまり第 3 者が検証できないという方式となる．この前提は本稿において情報ハイディングを目的として利用する場合に特化した前提条件であり q_i を公開しても認証方式としては実現できることに注意する．また，L 個の q_i を用意する意味は L 種類の安全なハッシュ関数を準備することを意味するが，実装の容易性からこのように親ノードの元の後ろに秘密情報を付加する方式を採用している．その観点から q_i はハッシュ値の長さ程度の長さの情報を用いることが推奨される．後半のマークルツリーの構成は収束部と呼ばれ L 個の子ノードの元 $p_i (i = 1, \ldots, L)$ から親ノードの元 p を以下のように算出する．

$$p := H(p_1|| \ldots ||p_L)$$

1.2 例：次元 $L = 2$，深さ $d = 3$

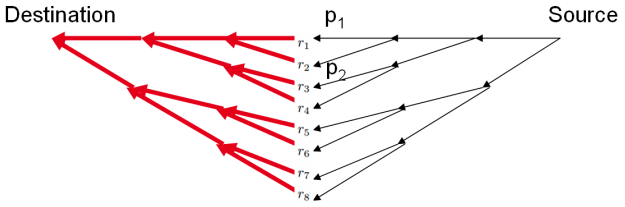

図 2 例：次元 $L = 2$，深さ $d = 3$

図 2 で示した構造において，拡散部と収束部の境界ノードは 8 点あり，これらを $r_1, \ldots, r_8$ とすると，起点の元 s から以下のように算出される．

- $r_1 := H(H(H(s||q_1)||q_1)||q_1)$
- $r_2 := H(H(H(s||q_1)||q_1)||q_2)$
- $r_3 := H(H(H(s||q_1)||q_2)||q_1)$
- $r_4 := H(H(H(s||q_1)||q_2)||q_2)$
- $r_5 := H(H(H(s||q_2)||q_1)||q_1)$
- $r_6 := H(H(H(s||q_2)||q_1)||q_2)$
- $r_7 := H(H(H(s||q_2)||q_2)||q_1)$
- $r_8 := H(H(H(s||q_2)||q_2)||q_2)$

さらに，ここから Merkle 木を構成すると最終的に終点の元 t は以下のようになる．

$$t := H(H(H(r1||r2)||H(r3||r4))||H(H(r5||r6)||H(r7||r8)))$$

1.3 モチベーション

ここで BWCCA2017 で提案された方式は，積極的に情報交換を行う「情報交換ファースト」ではあった．そのため事前共有された「ソーセージ」を無駄に食い尽くしていたとも言え，必ずしも効率性のよいものではなかった．

本稿では長期に渡って認証を何度か行うことでいつの間にか情報が交換されていたという「情報ハイディング」という副産物を着眼としていくつかのハイディング方式について検討を行う．既提案を大きく見直すことで Lamport 認証方式と同じ通信量で実現可能であり第 3 者からは Lamport 認証方式を行っているように見せかけて情報ハイディングを行う方式を検討する．

1.4 システムの前提条件

本稿では $L = 2$ つまりバイナリツリーのみを扱うものとする．これは $L > 2$ の場合にはマークルツリーの構造を考えると，秘密裏に共有すデータ量に比べて，無駄にノードを消費してしまうことを配慮しての選択となる．

2. 問題設定

2.1 提案 1: ナイーブな方式

図 2 における収束部を見ると $L^d - 1$ 個の L 分木，つまり 7 個のサブバイナリツリーが重なって構成されていることが分かる．一方で拡散部と収束部のノード数，つまり認証時に開示できるノード数はちょうど $3(L^d - 1)$ であることから ”Transable secret ratio”（1 回の認証時に秘密裏に提示可能なビット長）は $(L^d - 1)/3(L^d - 1) = 1/3$ であることが分かる．

2.2 提案 2

収束部の構造をに対して各図のように対応するノードにビット列をアサインすることで，開示するノードの順番に応じて情報を送信可能なことが分かる．

2.2.1 $d = 1$

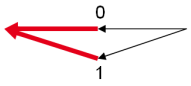

図 3 例：深さ $d = 1$ の場合のビット列

2.2.2 $d = 2$

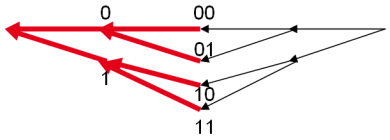

図 4　例：深さ $d = 1$ の場合のビット列

2.2.3 $d = 3$

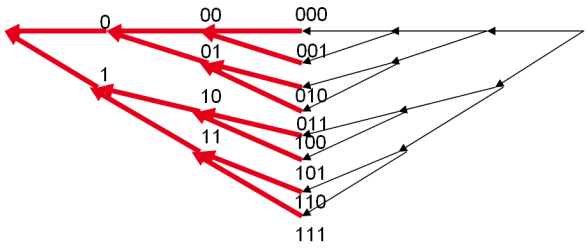

図 5　例：深さ $d = 3$ の場合のビット列

3. 今後について

今回収束部に着目して認証のたびにビット開示を行う方式を提案した．拡散部を含めさらなる余地を残しているため，別途報告を行う．

参考文献

[1] Leslie Lamport, ”Password Authentication with Insecure Communication”, Communications of the ACM 24.11, 770-772, 1981.
[2] Ralph Merkle, ”Secrecy, Authentication and Public Key Systems/ A certified digital signature”, Ph.D. dissertation, Dept. of Electrical Engineering, Stanford University, 1979.
[3] Michael Szydlo, ”Merkle Tree Traversal in Log Space and Time”, EUROCRYPT2004.
[4] Yuji Suga, Sausage-Style One-Time Authentication Schemes, Proceedings of the 12th International Conference on Broad-Band Wireless Computing, Communication and Applications (BWCCA-2017), pp. 658-667, 2017.