様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成 ２７ 年　 ５ 月 ２０ 日現在

機関番号：２５４０３
研究種目：基盤研究(C)
研究期間：2012～2014
課題番号：２４５０００９２

研究課題名（和文）ハッシュ連鎖による柔軟で効率の良い認証法

研究課題名（英文）Flexible and Efficient Authentication with Hash Chains

研究代表者
双紙　正和（Soshi, Masakazu）

広島市立大学・情報科学研究科・准教授

研究者番号：００２９３１４２

交付決定額（研究期間全体）：（直接経費）　　3,800,000円

研究成果の概要（和文）：ハッシュ関数は，効率よく計算でき，暗号プロトコルを作る際の重要な要素技術である．特に，認証プロトコルにおいては，初期値にハッシュ関数を繰り返し適用した，ハッシュ連鎖と呼ばれる技術が重要な要素技術となっている．本研究は，ハッシュ連鎖の新しい構成法について研究してきた．本研究で提案するハッシュ連鎖の構成法においては，複数の方向および開始地点を複数にしたハッシュ連鎖が用意される．これによって，柔軟で効率の良い認証を実現できることを示した．また提案手法の応用として，Vehicular Adhoc Networks (VANET)における経路認証法等が実現できることを示した．

研究成果の概要（英文）：Hash functions are efficiently computable and are important cryptographic primitive. Especially, hash chains, which repeatedly apply a hash function to an initial value, are one of the most important cryptographic techniques when we develop authentication protocols. In this work we proposed simple and efficient authentication schemes with several novel elaborate hash chains. Furthermore, we devise, for example, a key generation scheme and path authentication based on our hash chain constructions.

研究分野：情報セキュリティ

キーワード：セキュリティ　プロトコル　認証　ネットワーク　ハッシュ関数　ユビキタス

１．研究開始当初の背景

ハッシュ関数は，効率よく計算でき，また，一方向性・衝突困難性を持つ暗号プリミティブである．さらに，ハッシュ連鎖とは，ある乱数を初期値とし（以降では種と呼ぶ），ハッシュ関数を繰り返し適用したものである．ハッシュ連鎖は，効率よく一定数の認証値を計算できることから，さまざまな認証プロトコルにおいて利用されているだけでなく，特に，モバイル端末やセンサー等，計算能力の高くない計算機器における認証技術として，最も重要なものの一つとなっている．しかしながら，ハッシュ連鎖には，(i) ハッシュ関数を順に適用して認証値を生成するといった単純な構成であるため，一部分の認証値を公開するといった柔軟な認証ができない，(ii) ハッシュ連鎖は，長いほど計算コストがかかる，(iii) ハッシュ連鎖における応用上の考察はいまだに不十分である，といった問題点がある．

そこで本研究は，その認証法をさらに発展・深化させ，かつ，その新たな応用について研究を進めていくことを目指す．

２．研究の目的

本研究では，以下の研究課題について研究開発を行う．

1. ハッシュ連鎖による柔軟で効率の良い認証法　（研究課題 1）
2. ハッシュ連鎖による認証法の応用　（研究課題 2）

３．研究の方法

（１）ハッシュ連鎖による柔軟で効率の良い認証法

通常のハッシュ連鎖を用いた認証法においては，一方向のハッシュ連鎖が 1 個だけ用意されるに過ぎない．一方，本研究で提案するハッシュ連鎖の構成法においては，複数の方向および開始地点を複数にしたハッシュ連鎖が用意される．そして，ノードの組合せに応じて，共通鍵作成のため，適切なハッシュ連鎖とハッシュ値の組合せを選択する．まずこの研究課題 1 においては，このようなハッシュ連鎖の構成法について研究する．

（２）ハッシュ連鎖による認証法の応用

ハッシュ連鎖はさまざまな認証プロトコルの要素技術となっているが，従来研究におけるハッシュ連鎖の利用は単純なものにとどまっている．そこで，ハッシュ連鎖のさらなる可能性を探るため，その応用と，今回提案する新たなハッシュ連鎖方式の応用について研究開発を行う．

４．研究成果

（１）まず，二つのノードが相互認証する場合を考える．この場合，二つのハッシュ連鎖を用意することが考えられる．すなわち，ノードの総数をnとし，ハッシュ関数h，異なる種s_1, s_2とする．そして，ノードi $(1 \le i \le n)$に，ハッシュ値$h^i(s_1)$, $h^{n-i+1}(s_2)$を与える．同様にノードj $(1 \le j \le n,\ i < j$と仮定$)$に，ハッシュ値$h^j(s_1)$, $h^{n-j+1}(s_2)$を与える．すると，ノードi,jは，いずれもハッシュ値$h^j(s_1)$, $h^{n-i+1}(s_2)$を導出できるので，それらから（たとえば何らかの一方向性関数を用いるなどして）ノードi,jの共通鍵を作成することができる．

ここで，上記の手法においては，攻撃者やノードk $(1 \le k < i$あるいは$j < k \le n)$は，ハッシュ関数の性質より，ノードi,jの共通鍵を作ることができないことが保証され，セキュアである．しかしながら，ノードk $(i \le k \le j)$は，ノードi,jの共通鍵を作成できてしまう．そこで，以下のような一般的な方式を提案した．

（２）提案手法の基本的なアイディアは，ノードi,jの共通鍵を作成することができるk $(i \le k \le j)$の範囲を，ハッシュ連鎖の構成を工夫することにより狭めていくというものである．紙面の都合で$n = 5$の場合を例として考える（ただし，n方向のハッシュ連鎖として，さらに一般的な構成が可能）．図 1 を参照せよ．

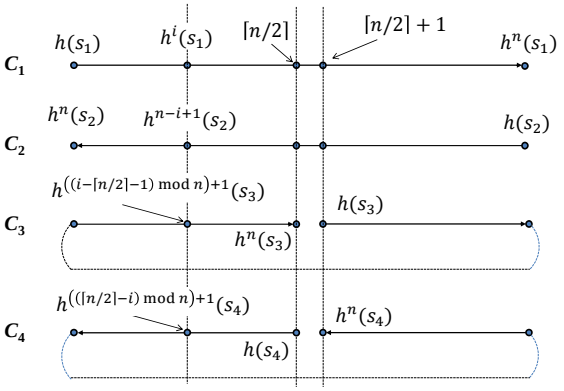

図 1　提案ハッシュ連鎖構成法

このとき，4 本のハッシュ連鎖C_1, C_2, C_3, C_4が作られる．ここで，s_1, s_2, s_3, s_4は，それぞれハッシュ連鎖C_1, C_2, C_3, C_4の種である．

表 1　$n = 5$の場合のハッシュ連鎖

	1	2	3	4	5
C_1	$h(s_1)$	$h^2(s_1)$	$h^3(s_1)$	$h^4(s_1)$	$h^5(s_1)$
C_2	$h^5(s_2)$	$h^4(s_2)$	$h^3(s_2)$	$h^2(s_2)$	$h(s_2)$
C_3	$h^3(s_3)$	$h^4(s_3)$	$h^5(s_3)$	$h(s_3)$	$h^2(s_3)$
C_4	$h^3(s_4)$	$h^2(s_4)$	$h(s_4)$	$h^5(s_4)$	$h^4(s_4)$

このようなハッシュ連鎖をまとめると，表 1 のようになる．特に，ハッシュ連鎖C_3, C_4に着目すると，ノードiのハッシュ値はそれぞれ$h^{((i-\lceil n/2 \rceil-1) \bmod n)+1}(s_3)$，$h^{((\lceil n/2 \rceil-i) \bmod n)+1}(s_4)$

のように与えられる．ここで，$\lceil x \rceil$ は実数 x以上の最小の整数を表す．すなわち，まとめると，ノードiに与えられるハッシュ値は，$h^{i}(s_1)$, $h^{n-i+1}(s_2)$ ， $h^{((i-\lceil n/2 \rceil-1) \bmod n)+1}(s_3)$ ， $h^{((\lceil n/2 \rceil-i) \bmod n)+1}(s_4)$の 4 個の値となる．

このとき，$1 \leq i \leq \lceil n/2 \rceil$, $\lceil n/2 \rceil < j \leq n$を満たすノード$i, j$は，ハッシュ連鎖$C_1, C_2, C_3, C_4$の構成により，$h^{j}(s_1)$ ， $h^{n-i+1}(s_2)$ ， $h^{((i-\lceil n/2 \rceil-1) \bmod n)+1}(s_3)$, $h^{((\lceil n/2 \rceil-j) \bmod n)+1}(s_4)$を導出することができるので，それらを用いて共通の鍵Kを計算することができるようになる．さらに，ノードi, j以外のノードが，Kを作成できないことも容易に確かめられる．

なお，ノードi, jが同じグループに所属するとき，すなわち，$1 \leq i < j \leq \lceil n/2 \rceil$あるいは$\lceil n/2 \rceil < i < j \leq n$となるとき，上記の基本方式と全く同様にして，ハッシュ連鎖鎖C_1, C_2のみを用いて共通鍵を生成するものとする．このようなハッシュ連鎖の構成は，さらに一般的にすることができる．

（3）提案ハッシュ連鎖による鍵生成

ここでは，特に$n = 4$の場合の提案ハッシュ連鎖構成法における鍵生成法を述べる．表 2 を参照せよ．

表 2　認証に用いるハッシュ値（$n = 4$）

ノードの組	ハッシュ値の組
1, 2	$C_{1,2}, C_{2,1}$
1, 3	$C_{1,3}, C_{3,1}$
1, 4	$C_{3,1}, C_{4,4}$
2, 3	$C_{1,3}, C_{2,2}$
2, 4	$C_{2,2}, C_{4,4}$
3, 4	$C_{1,4}, C_{2,3}$

表 2 において，$C_{i,j}$は，ハッシュ連鎖C_iにおけるj番目のハッシュ値を表すものとする．たとえば，$C_{3,1} = h^3(s_3)$, $C_{3,2} = h^4(s_3)$, $C_{3,3} = h(s_3)$, $C_{3,4} = h^2(s_3)$となる．またこのときユーザ 2 には，$C_{i,2}$ $(i = 1, \ldots, 4)$ が初期値として与えられる．具体的には，ユーザ 2 に$h^2(s_1), h^3(s_2), h^4(s_3), h(s_4)$が与えられる．そして，表 2 から分かるように，ユーザ 2, 3 が共通の鍵を生成するときには，ハッシュ値$C_{1,3}, C_{2,2}$を用いればよいことがいえる．

（4）このような高度なハッシュ連鎖を用意することで，鍵更新プロトコルにおける時限つきのキーエスクロー（政府や裁判所が認めた場合，鍵を強制的に公開する）や，センサーネットワークにおける効率の良い認証等を実現できるようになる

（5）ハッシュ連鎖による認証法の応用

前述したように，ハッシュ連鎖はさまざまな認証プロトコルの要素技術となっているが，従来研究におけるハッシュ連鎖の利用は単純なものにとどまっている．そこで，ハッシュ連鎖のさらなる可能性を探るため，その応用と，今回提案する新たなハッシュ連鎖方式の応用について研究開発を行った．特にここでは，我々が提案する OWCN について述べる．

すなわち，複数の種を用意し，それぞれにハッシュ関数を適用した，ハッシュ連鎖によるネットワークを構成する（図 2 参照）．我々はこれを One-way cross networks (OWCN) と呼んでいる．

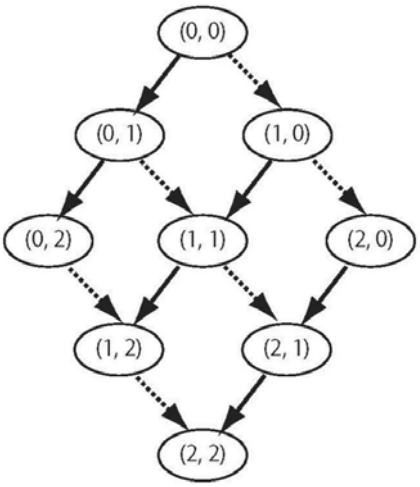

図 2　One-way Cross Networks (OWCN)

図 2 における OWCN は，二つのある種 (s_1, s_2とする）に，ハッシュ関数hを適用して構成されている．この図で，頂点はハッシュ関数の指数の組を表し，たとえば頂点(1, 1) から (1, 2) への辺によって，$(h^1(s_1), h^1(s_2))$から$(h^1(s_1), h^2(s_2))$が構成されることを意味する．このように OWCN では，認証のやり方に，方向性やネットワーク性を盛り込むことができるのである．このことを利用して，我々は，OWCN を用いた VANET における車の経路認証法を提案した．

５．主な発表論文等

（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計 24 件）

１．Atsuko Miyaji and Mazumder Rashed, A new (n, 2n) Double Block Length Hash Function based on Single Key Scheduling, The 29th IEEE International Conference on Advanced Information Networking and Applications (AINA2015), 査読有, pp. 564-570, 2015.

２．宮地充子, ユビキタスネットワークにおけるセキュリティ技術－ 積極的利用を促すセキュリティ技術－, 査読有, 電気評論, 夏季増刊号特集, 2014, pp. 12-15.

３．Kayoko Iwamoto, Masakazu Soshi, and Takashi Satoh, An efficient and adaptive IP traceback scheme, In IEEE International Workshop on Internet of Things Services (IoTS), 査読有, pp. 235-240, November 2014.

４．Jiageng Chen, Mohammad S.I. Mamun, Atsuko Miyaji, An efficient batch verification system for large scale VANET, Intl. J. of Security and Communication Networks SCN, 査読有, Wiley Publication. Available online: March 2014, DOI:10.1002/sec.980.
５．Atsuko Miyaji, Kazumasa Omote: Self-healing Schemes Suitable for Various WSNs, 査読有, IDCS 2013: 92-105.
６．Mohammad S. I. Mamun and Atsuko Miyaji, An Optimized Signature Verification System for Vehicle Ad hoc NETwork, The 8th International Conference on Wireless Communications, Networking and Mobile Computing, 査読有, WiCOM2012, IEEE, 1-8.
７．Tomoyuki Karasawa, Masakazu Soshi, and Atsuko Miyaji, A novel hybrid IP traceback scheme with packet counters, The 5th International Conference on Internet and Distributed Computing Systems (IDCS 2012), 査読有, volume 7646 of Lecture Notes in Computer Science, pp. 71-84. Springer-Verlag, 2012.
８．Atsushi Waseda and Masakazu Soshi, Consideration for multi-threshold multi-secret sharing schemes, 査読有, International Symposium on Information Theory and Applications (ISITA 2012), pp. 265-269, August 2012.

〔学会発表〕(計 26 件)
１．Atsuko Miyaji, Further Application on RFID with Privacy-Preserving, The 1st International Conference on Future Data and Security Engineering, FDSE 2014.(招待講演)　2014 年 11 月 19 日～2014 年 11 月 21 日.
２．宮地充子, 近澤武, 竜田敏男, 大熊健司, 渡辺創, 松尾真一郎　情報セキュリティの標準化動向について－ ISO/IEC JTC1/SC27/WG2 2014 年４月香港会議報告 － 第 27 回電子情報通信学会(招待講演) 2014 年 7 月 3 日～2014 年 7 月 4 日.
３．宮地充子, 安全・安心社会を実現するセキュリティ基盤, 情報処理学会第 13 回情報科学技術フォーラム(招待講演), 2014 年 9 月 3 日～2014 年 9 月 4 日.
４．西山翔稀, 双紙正和, ハッシュ連鎖の柔軟な構成法とそれによる鍵生成法, 信学技報, ICSS2014-98 (2015-03), pp.211-216, 2015 年 3 月 3 日(火)～4 日(水).
５．北山翔馬, 双紙正和, VANET におけるグループ one-way cross-networks を用いた経路認証手法の検討, 信学技報, ICSS2014-87 (2015-03), pp.145-150, 2015 年 3 月 3 日(火)～4 日(水).
６．白石良介, 佐藤敬, 下泉政樹, 双紙正和, 偽陽性の生じない Space-Time Encoding Schemes, 信学技報, vol. 114, no. 380, ISEC2014-71, pp. 11-15, 2014 年 12 月 19 日(金)
７．日浦博昭, 北山翔馬, 双紙正和, 大場充, 車車間通信における自律分散型認証手法の提案, 情報処理学会研究報告, 2014-CSEC-66, No.8, 2014 年 07 月 03 日(木)～04 日(金).

〔図書〕(計 1 件)
北上始(編), 双紙正和 (共著). 一般教育の情報 ― 情報の本質を見抜ける教師や社会人の育成へ.
現場と結ぶ教職シリーズ. あいり出版, 2013 年 10 月.

〔産業財産権〕
○出願状況 (計 0 件)

○取得状況 (計 0 件)

〔その他〕

６．研究組織
(1)研究代表者
双紙　正和 (SOSHI, Masakazu)
広島市立大学・大学院情報科学研究科・准教授
研究者番号：00293142

(2)研究分担者
宮地　充子 (Miyaji, Atsuko)
北陸先端科学技術大学院大学・情報科学研究科・教授
研究者番号： 10313701

(3)連携研究者
(　　)

研究者番号：