様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　３０　年　１０　月　２５　日現在

機関番号：　２５４０３
研究種目：　基盤研究(C)（一般）
研究期間：　2015～2017
課題番号：　１５Ｋ００１８９

研究課題名（和文）ハッシュ連鎖の柔軟な構成法およびそれを応用した軽量認証法の研究

研究課題名（英文）Flexible and efficient hash chain constructions and its applications for lightweight authentication

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）　　3,500,000円

研究成果の概要（和文）：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、特に、IoT環境等における軽量認証技術として重要である。本課題では、ハッシュ連鎖の柔軟な構成法およびそれを応用した軽量認証法について研究開発を行った。我々の提案手法は、暗号プリミティブとしてハッシュ関数のみ使用しており、さらに、任意のユーザ同士で、通信することなく鍵共有・認証できるという利点を持つ。また、我々が提案している OWCN(One-Way Cross Networks) およびデュアル OWCN について研究開発を行った。その他、ハッシュ関数を用いたワンタイム署名や、ホワイトボックス暗号などの応用について研究を行った。

研究成果の概要（英文）：In recent years, the importance of lightweight and efficient authentication protocols for IoT environments has been increasing. In this work we propose a flexible hash chain construction, hash chain aggregation (HCA), and a scheme to set up a common key for two users with HCA. Our scheme uses only hash functions as cryptographic primitives. Furthermore, in our schemes no communication is required when a common key for two users is set up. We also evaluate security of the scheme extensively. Especially we show that our scheme is secure against a single attacker, but not against two attackers or more. We also show that our scheme is efficient. In this work we examine application of hash functions and lightweight authentication such as one time signatures and white-box cryptography.

研究分野：　セキュリティ

キーワード：　セキュリティ　ネットワーク　IoT　認証　プロトコル　ハッシュ関数　モバイルコンピューティング　ユビキタス

１．研究開始当初の背景

ハッシュ関数とは、一方向性および衝突困難性を持つような暗号プリミティブである。また、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、特に、モバイル端末やセンサー等、計算能力の高くない機器における軽量認証技術として、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) ハッシュ連鎖における応用上の考察はいまだに不十分である、等の問題点がある。

そこで本研究は、ハッシュ関数を用いた認証法をさらに発展・深化させ、 ハッシュ連鎖の柔軟な構成法およびそれを応用した軽量認証法について研究開発を行う。

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) ハッシュ連鎖の柔軟な構成法の基本とその形式的な評価（研究課題 1）
(2) 様々な、ハッシュ連鎖の柔軟な構成法およびそれを応用した軽量認証法（研究課題 2）
(3) ユビキタス環境における、ハッシュ連鎖の柔軟な構成法による軽量認証法の応用（研究課題 3）

３．研究の方法

(1) 研究課題 1

通常のハッシュ連鎖を用いた認証法においては、ハッシュ連鎖が 1 個だけ用意されるに過ぎない。一方、本研究におけるハッシュ連鎖の基本的な構成法においては、ある規則によって組み合わせられた複数のハッシュ連鎖が用意され、それによって柔軟で効率のよい認証が可能となる。しかしながら、形式的なセキュリティ評価についてはまだ検討の余地がある。そこで、この研究課題 1 では、上記のハッシュ連鎖構成の形式的な表現の確立およびそのセキュリティの評価を実施する。

(2) 研究課題 2

研究課題 1 のハッシュ連鎖構成法をさらに発展させる。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。これを One-way cross networks (OWCN) と呼ぶ。しかしながら、現段階では OWCN については十分な評価がなされていない。そこで研究課題 2 では、OWCN における基本的な方式を確立し、評価を行う。

(3) 研究課題 3

この研究課題では、OWCN など、より広範に、研究課題 1,2 で研究開発されたハッシュ連鎖の柔軟な構成法による軽量認証法等の応用を研究する。

４．研究成果

(1) 研究課題 1

一般的な、新たなハッシュ連鎖の構成法を提案した。以降では、ある正整数 m について、ユーザ数 $N = 2^m$ とし、ハッシュ連鎖の長さを ℓ とする。また、ある $Q = (q_1, ..., q_j)$ について、 i 番目の要素 q_i $(1 \le i \le j)$ を $Q[i]$ と書く。

次に、ハッシュ連鎖の型を定義する。ただし、s をハッシュ連鎖の種とし、ハッシュ関数を h とする。

・タイプ I ハッシュ連鎖 $C_\ell^{I}(s) := (v_1, ..., v_\ell)$ （ただし $v_i = h^i(s)$）

・タイプ II ハッシュ連鎖 $C_\ell^{II}(s) := (v_1, ..., v_\ell)$ （ただし $v_i = h^{\ell-i+1}(s)$）

・タイプ III ハッシュ連鎖 $C_\ell^{III}(s) := (v_1, ..., v_\ell)$ （ただし $v_i = h^{((i-\ell/2-1) \bmod \ell)+1}(s)$ ）

・タイプ IV ハッシュ連鎖 $C_\ell^{IV}(s) := (v_1, ..., v_\ell)$（ただし $v_i = h^{((\ell/2-i) \bmod \ell)+1}(s)$ ）

以上の定義を用いれば、ハッシュ連鎖リスト $L(\tau, k, s_1, ..., s_k)$ を $(C_{N/k}^{\tau}(s_1), ..., C_{N/k}^{\tau}(s_k))$ と定義できる。ここで、$\tau \in \{I, II, III, IV\}$ であり、$s_1, ..., s_k$ を、種の列とする。さらに、ハッシュ連鎖リストの列として、ハッシュ連鎖アグリゲーションを定義することが出来る。また、$\alpha(L, i) = \lceil ki/N \rceil$ とする。

以上より、提案するハッシュ連鎖アグリゲーション HCA を以下のように定義する。なお以下では、ハッシュ連鎖リスト $L(\tau, k, s_1, ..., s_k)$ を L と表す。

$HCA := (L_{(1)}, L_{(2)}, ..., L_{(2m-1)}, L_{(2m)})$

ここで、$L_{(1)} = (C_N^{I}(s_1))$, $L_{(2)} = (C_N^{II}(s_2))$, $L_{(3)} = (C_N^{III}(s_3))$, $L_{(4)} = (C_N^{IV}(s_4))$ であり、$i > 4$ のときの $L(i)$ は以下のように定義される。

・$i = 2j - 1$ のとき：

$L_{(2j-1)} := (C_{2\wedge(m-j+2)}^{III}(s_{2j-1,1}), \ldots, C_{2\wedge(m-j+2)}^{III}(s_{2j-1,2\wedge(j-2)}))$

・$i = 2j$ のとき：

$L_{(2j)} := (C_{2\wedge(m-j+2)}^{IV}(s_{2j,1}), \ldots, C_{2\wedge(m-j+2)}^{IV}(s_{2j,2\wedge(j-2)}))$

ここで、整数 a, b, c について、$s_a, s_{b,c}$ はすべて異なるランダムな種を表す。

このとき、任意のユーザ i, j は、いずれも以下の 4 個のハッシュ値を計算でき、それにより共通鍵を計算できる：

$\nu_1 := C_N^{I}(s_1)[j]$,

$\nu_2 := C_N^{II}(s_2)[i]$,

$\nu_3 := (L_{(2ku-1)}[\alpha(L_{(2ku-1)}, i)])[i - \beta_{i,2ku-1}]$,

$\nu_4 := (L_{(2ku)}[\alpha(L_{(2ku)}, i)])[j - \beta_{j,2ku}]$

ここで、$\beta_{i,j} := (N(\alpha(L_{(j)}, i)-1))/k_{L(j)}$ とおいた。また、$L_{(2ku-1)}[\alpha(L_{(2ku-1)}, i)]$, $L_{(2ku)}[\alpha(L_{(2ku)}, i)]$ は、i, j を同時に含むハッシュ

連鎖の中で、その長さが最も短いものである。このとき、ユーザ i, j 以外のユーザは、i, j の共通鍵を作成できないことを容易に確認できる。
提案方式のセキュリティについては、以下の定理1および2を示すことができる：
定理 1. 一人の攻撃者は、任意の i, j $(1 \le i < j \le N)$ について、ユーザ i, j の共通鍵を計算できない。
定理 2. ユーザ i, j $(1 \le i < j \le N)$ について、 $i < a_1 \le N(\alpha - 1)/k + N/2k,\ N(\alpha - 1)/k + N/2k + 1 \le a_2 < j$ を満たすユーザ a_1, a_2 は、結託してユーザ i, j の共通鍵を計算することができる。
定理 1 および 2 より、提案方式は、攻撃者が一人の場合は安全であるが、攻撃者が二人以上結託して攻撃を行う場合には安全でなくなることを示された。
提案方式の性能については、以下を示すことができる。
本提案手法では、各ユーザが保持するハッシュ値の数は、 $2\lceil \log_2 N \rceil$ である。共通鍵によって相互認証する自明な手法だと、各ユーザは $N - 1$ 個の秘密鍵を持たなければならないので、本提案手法は非常に効率が良い。
さらに、共通鍵計算に必要なハッシュ値の個数についても評価を行った。

(2) 研究課題 2

OWCN は、以下のように定義できる。
定義 1 (k-OWCN $(m_1, ..., m_k)$). h をハッシュ関数とし、$(s_1, ..., s_k)$ を、種の k 個組とする。 k-OWCN $(m_1, ..., m_k)$ とは、
$V_{r1,...,rk} := (h^{r1}(s_1), ..., h^{rk}(s_k))$
を頂点とする有向グラフ $G^O = (V^O, E^O)$ である。ただし、 $1 \le r_i \le m_i$ $(i = 1, ..., k)$ とする。なお、以降では、$V_{r1,...,rk}$ を V_a あるいは $(r_1, ..., r_k)$ などと略すことがある。ここで、ある $V_{p1,...,pk} = (h^{p1}(s_1), ..., h^{pk}(s_k))$, $V_{q1,...,qk} = (h^{q1}(s_1), ..., h^{qk}(s_k)) \in V^O$ について、あるただ一つの i $(1 \le i \le k)$ が存在して、 $p_i = q_i + 1$ であり、かつ、それ以外の j $(\neq i)$ のときには $p_j = q_j$ となるとき、その時に限り、辺 $(V_{q1,...,qk}, V_{p1,...,pk}) \in E^O$ である。
このような OWCN の定義により、Lamport のワンタイムパスワードと同様の手法により、OWCN を用いた経路認証を行える。
しかし、アドホックネットワークなど、中継が行われている通信環境では、OWCN に対して、バッファリングの攻撃が考えられる。そこで、デュアル OWCN による対策を考える。
定義 2 (デュアル k-OWCN$(m_1, ..., m_k)$). g をハッシュ関数とし、$(t_1, ..., t_k)$ を、種の k 個組とする。デュアル k-OWCN$(m_1, ..., m_k)$とは、
$W_{r1,...,rk} := (g^{m1-r1+1}(t_1), ..., g^{mk-rk+1}(t_k))$
を頂点とする有向グラフ $G^{DO} = (V^{DO}, E^{DO})$ である。ただし、 $1 \le r_i \le m_i$ $(i = 1, ..., k)$ とする。デュアル OWCN G^{DO} では、対応する OWCN G^O について、$(V_a, V_b) \in E^O$ のとき、そのときに限り、$(W_b, W_a) \in E^{DO}$ である。
ここで、OWCN における経路を以下のように定義する（デュアル OWCN についても同様）。$(V_i, ..., V_j)$ $(i < j)$ が経路であるとは、すべての k $(0 \le k \le j-i-1)$ について、$(V_{i+k}, V_{i+k+1}) \in E^O$ となるときである。
このとき、可能過去経路集合、可能未来経路集合を以下のように定義できる。
定義 3 (可能過去経路集合). k-OWCN G^O における V_a について、可能過去経路集合 $PPP(V_a)$ は以下のように定義される。
$PPP(V_a) := \{(V_i, ..., V_j) \mid V_i, ..., V_j \in V^O\ (i < j),\ V_i = V_{m1,...,mk},\ V_j = V_a,\ (V_j, ..., V_i)$ は経路$\}$
定義 4 (可能未来経路集合). デュアル k-OWCN G^{DO} における W_a について、可能未来経路集合 $PFP(W_a)$ は以下のように定義される。
$PFP(W_a) := \{(W_i, ..., W_j) \mid W_i, ..., W_j \in V^{OO}\ (i < j),\ W_i = W_a,\ W_j = W_{1,...,1},\ (W_i, ..., W_j)$ は経路$\}$
可能過去経路集合、可能未来経路集合によって直進経路の列を考えることができ、それにより、OWCN, デュアル OWCN による経路認証を行うことができる。

(3) 研究課題 3

研究課題 1 において提案した方式は、上で述べたように、攻撃者が 2 人以上いる場合、安全ではない。そこで、そのような攻撃への対策を検討した。その基本的なアプローチは以下のとおりである。まず、今まで述べてきたように、HCA を構築する。この段階で、あるユーザの組は、結託攻撃ができないようなハッシュ値が配られているため、残りのユーザの組に対して新たなハッシュ値を計算し、配布すればよい。具体的には、それらのユーザの組が、タイプ I（あるいはタイプ II）のハッシュ連鎖で隣接するようなハッシュ値をもてばよい。こうすれば、あまり効率はよくないが、二人以上の攻撃者による結託攻撃に対処できる。
さらに、研究の過程で、ハッシュ関数を用いたワンタイム署名や、ホワイトボックス暗号などに関する新たな着想を得た。

５．主な発表論文等
（研究代表者は下線）

〔雑誌論文〕（計 11 件）
Mazumder Rashed and Atsuko Miyaji, ``A New Scheme of Blockcipher Hash", The Institute of Electronics, Information and Communication Engineers (IEICE) Trans., Information and Systems. Vol. E99-D, No.4(2016), 796-804.
Rashed Mazumder, Atsuko Miyaji, Chunhua Su,``A simple authentication encryption scheme",Concurrency and Computation: Practice and Experience 2017

〔学会発表〕（計 21 件）
Chen-Mou Cheng, Kenta Kodera, and Atsuko Miyaji, ``On the Computational Complexity of ECDLP for Elliptic Curves in Various Forms Using Index Calculus",
The 20th Annual International Conference on Information Security and Cryptology (ICISC 2017), Lecture Notes in Computer Science, volume 10779(2017), Springer-Verlag, 245-263. 2017/11/29-12/1, Seoul, South Korea.

Hiroshi Nomaguchi, Atsuko Miyaji and Chunhua Su, ``Evaluation and Improvement of Pseudo-Random Number Generator for EPC Gen2", The 16th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom'17)}, IEEE, 721-728, 2017. 2017/8/3, Sydney, Australia.

Tomoaki Mimoto, Shinsaku Kiyomoto, Katsuya Tanaka and Atsuko Miyaji,
``(p, N)-identifiability: Anonymity under Practical Adversaries",
The 16th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom'17)}, IEEE, 996-1003, 2017. 2017/8/1, Sydney, Australia.
Yuta Kurihara and Masakazu Soshi. A Novel Hash Chain Construction for Simple and Efficient Authentication. In 14th Annual Conference on Privacy, Security and Trust, PST 2016, December 2016.
Hiroaki Anada, Shunsuke Tsumori, Samiran Bag, Masakazu Soshi, Atsushi Waseda, and Kouichi Sakurai. Short Merkle one-time signatures (poster). In The 12th International Workshop on Security (IWSEC), 2017.

〔図書〕（計１件）
Dieter Gollmann, Atsuko Miyaji, Hiroaki Kikuchi, Springer,
Applied Cryptography and Network Security - 15th International Conference, ACNS 2017, Kanazawa, Japan, July 10-12, 2017, Proceedings. Lecture Notes in Computer Science 10355, 2017, ISBN 978-3-319-61203-4

〔産業財産権〕

○出願状況（計　　件）

○取得状況（計　　件）

〔その他〕
ホームページ等

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)研究協力者
〔主たる渡航先の主たる海外共同研究者〕
宮地 充子（Miyaji, Atsuko）
大阪大学・工学系研究科・教授
研究者番号： 10313701

〔その他の研究協力者〕
（　　）