様式Ｃ－１９

科学研究費助成事業（科学研究費補助金）研究成果報告書

平成 25 年 3 月 31 日現在

機関番号：１４５０１
研究種目：基盤研究（C）
研究期間：2010～2012
課題番号：２２５６０３７６
研究課題名（和文）　ライトウエイトハッシュ関数の設計技術及び安全性解析技術に関する研究
研究課題名（英文）　Research on design and analysis of lightweight hash functions

研究代表者
桑門　秀典（Kuwakado Hidenori）
神戸大学・工学研究科・准教授
研究者番号：30283914

研究成果の概要（和文）：超小型電子機器によるネットワークにおいて，安全な通信を実現するために回路規模が極めて小さい暗号プリミティブが必要とされている．本研究では，回路規模が小さいハッシュ関数（ライトウエイトハッシュ関数）を二つ提案（Lesamta-LW, DbMMO）し，その安全性解析を行った．そして，既存のブロック暗号 KATAN が DbMMO で仮定された安全性の一つを満足するかどうかを計算機実験により調べた．また，量子計算機が安全性に与える影響について検討行い，ブロック暗号の構成によっては，古典計算機のみの場合よりも少ない計算量で安全性が損なわれる可能性を明らかにした．

研究成果の概要（英文）：Lightweight cryptographic primitives are required to achieve secure communication in the resource-constrained network such as a sensor network and an RFID network. In this research, lightweight hash functions (Lesamnta-LW, DbMMO) are proposed and are analyzed in terms of security under an appropriate model. On the other hand, we analyze the security of KATAN, which is a lightweight blockcipher, from the viewpoint of DbMMO's requirements. Furthermore, we show that a quantum computer compromises the security of some blockciphers by analyzing the internal structure of a blockcipher.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2010 年度	1,700,000	510,000	2,210,000
2011 年度	800,000	240,000	1,040,000
2012 年度	800,000	240,000	1,040,000
年度			
年度			
総　計	3,300,000	990,000	4,290,000

研究分野：工学
科研費の分科・細目：電気電子工学・通信・ネットワーク工学
キーワード：暗号・セキュリティ

１．研究開始当初の背景

RFID やセンサネットワーク用端末のような通信機能をもつ超小型の電子機器によるネットワークが広がりつつある．これら超小型電子機器の通信を安全にしたいという潜在的な要求は高いが，回路規模の制約から従来の暗号方式を実装することができない場合が多い．そのため，回路規模が極めて小さい暗号方式（ライトウエイト暗号）の研究開発が着目され始めている．

ライトウエイト暗号は，ブロック暗号とハッシュ関数に大別される．現在の研究状況と

しては，ライトウエイトブロック暗号の具体的な方式が幾つか提案されている．これらは，従来のブロック暗号とは大きく異なる構造をもつので，新しい安全性解析技術が必要である．

ハッシュ関数の場合，その安全性と回路規模には密接な関係がある．現在，米国国立標準技術研究所が行っている次世代ハッシュ関数選定における候補は，回路規模が 8 [Kgates]以上なので，SHA-3 は超小型電子機器上の実装には向かない．

本研究は，SHA-3 が実装不可能な回路規模で実現できるハッシュ関数の設計・解析技術の開発を目的とする．本研究が対象としている回路規模で，実現できるハッシュ関数は，世界的にもまだ存在しないが，今後，具体的な方式の提案がなされると予想している（実際に，2010 年頃からいくつか提案された）．研究代表者は，(独)情報通信研究機構からの受託研究として，ハッシュ関数ファミリー「Lesamnta」の開発を行い，その中でライトウエイトハッシュ関数の開発を行った．しかし，確立された設計・解析技術がないため，検討すべき課題が多数残されており，引き続きライトウエイトハッシュ関数の研究開発を行うことが重要であると考えた．

２．研究の目的

ライトウエイト暗号は，その厳しい回路規模制約のため，従来の暗号方式とは大幅に異なる構造になるので，設計・安全性評価手法において，不明の部分が非常に多い．本研究では，下記の二つの観点からライトウエイトハッシュ関数の設計・安全性評価手法の不明な点を明らかにしていく．

構造の安全性証明：暗号方式は，長期にわたる安全性が求められるので，安全性の証明は重要である．暗号プリミティブから安全なライトウエイトハッシュ関数を構成する方法を網羅的に検討する．これを遂行するために，安全性評価の前提となる適切なモデル設定と証明技法を確立する．

攻撃による安全性検証：ライトウエイトブロック暗号とライトウエイトハッシュ関数には，共通化できる設計・安全性評価手法があると予想される．ライトウエイトブロック暗号への攻撃評価を通じて，評価手法のノウハウを蓄積し，ライトウエイトハッシュ関数への適用を検討する．例えば，非線形関数の代数次数及びその多項式を効率的に求める攻撃(cube attack)が有力であると考えられるので，ライトウエイトハッシュ関数に適用可能性を明らかにすることである

３．研究の方法

研究方法を構造の安全性証明と攻撃による安全性検証の二つの観点から述べる．

構造の安全性証明：ハッシュ関数の構成法は，専用の構成部品を想定した構成法と既存の構成部品（ブロック暗号等）を想定した構成法に分類できる．それぞれにおいて，構成法を検討し，適当なモデルを仮定して，安全性証明を行う．

攻撃による安全性検証：上記の構造の安全性証明における構成部品が仮定されたモデルにおいて妥当であるかどうかを調査する．つまり，構成部品の候補となりうるものに対して，攻撃を行い，その安全性を明らかにする．本研究では，古典計算機を前提にした解析だけでなく，量子計算機も含めて安全性の検討を行う．

４．研究成果

（１）構造の安全性証明

①専用ブロック暗号を用いたハッシュ関数の構成法

ハッシュ関数をハードウエア実装した場合，回路規模を決定する主要因は，レジスタのサイズである．ブロック暗号を用いる場合，少なくとも二種類のレジスタ（鍵用レジスタ，平文用レジスタ）が必要である．鍵のビット長，平文のビット長をそれぞれ k,n とおくと，既存のブロック暗号には，$n \leq k$ の関係がある．しかし，ハッシュ関数の構成部品として使用する場合，その関係は必ずしも必要ない．さらに，ハッシュ関数の構成部品として使用する場合，鍵または平文を暗号文に XOR すると，安全性が高くなることがあるので，しばしば，そのような構成にする．しかし，鍵または平文を保存しておくレジスタが必要になるので，回路規模の削減ためには，このような構成法は向かない．以上の検討結果に基づき，下記のような構成のハッシュ関数 Lesamnta-LW を提案し，その安全性解析を行った（文献[3]）．

$n = 2k$ とする．ハッシュするメッセージを m とおく．m の最後に 1 を 1 個と 0 を $t + k/2 - 1$ 個付加する．ここで，t は，メッセージの長さを l ビットとするとき，$l + t \equiv 0 \pmod{k}$ を満たす最小の整数である．さらに l の $k/2$ ビットの 2 進数表現を付加する．この操作により，m は k の倍数のビット長になるので，k ビット毎に分割したメッセージブロックを $m_1, m_2, \cdots, m_N$ とおく．

u_0, v_0 をそれぞれ $n/2$ ビットの固定値とする．$i = 1,2,\cdots,N$ に対して，

$$u_i \,|\, v_i = E(u_{i-1}, m_i \,|\, v_{i-1})$$

とする(**エラー！ 参照元が見つかりません。**)．

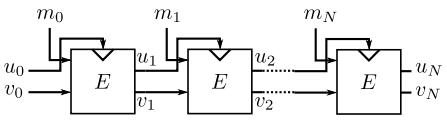

図 １ハッシュ関数 Lesamnta-LW

ここで，E は暗号化関数であり，u_{i-1} は鍵で

あり，$m_i \mid v_{i-1}$は平文に相当する．なお，|は連接記号である．$u_N \mid v_N$がmに対するダイジェスト（ハッシュ値）になる．

このハッシュ関数の構成法の特徴は二つある．一つめは，回路規模削減のために，鍵長が短いブロック暗号を使用している点である．このハッシュ関数を疑似ランダム関数として使用する場合，メッセージブロックの入力が鍵入力になっていないことが重要である．二つめは，回路規模削減のため，フィードフォワードがない点である．そのため，圧縮関数自身は可逆である．

このハッシュ関数の原像困難性，衝突困難性は，Eが ideal cipher であるという仮定の下で解析されている．この仮定は，攻撃者が暗号化関数の内部構造を考慮せずに攻撃する場合に相当する．

衝突困難性：攻撃者 A がEに対してq回質問できるとき，A が衝突を発見する確率は下記の式で与えられる．

$$Adv_{LW}^{col}(A) \le \frac{2^n nq}{2^{2n}-q} + \frac{q^2}{2^{2n}-q} + \frac{q}{n!\cdot 2^n}$$

つまり，大雑把には，攻撃者の質問回数が2^n回より大幅に少ないときは，衝突を発見できる確率は小さい．また，この式は，ハッシュ関数 LW の衝突困難性が，nビットのダイジェストを生成する理想的なハッシュ関数に近い安全性を達成していることを意味する．

原像困難性：攻撃者 A がEに対してq回質問できるとき，一様分布に従って選ばれたダイジェストの原像を A が発見する確率は上の式とほとんど同じである．したがって，ハッシュ関数 LW の衝突困難性が，nビットのダイジェストを生成する理想的なハッシュ関数のおよそ半分の安全性を達成していることを意味する．これは，ハッシュ関数 LW にフィードフォワードがないことの副作用である．つまり，ハッシュ関数 LW は，回路規模削減のために，原像困難性を犠牲にしているとも考えられる．しかし，$n = 256$とすれば，原像困難性は約2^{120}の計算量（質問回数）が必要であるから，現実的にこれが問題になることはないと考えらえる．

衝突困難性，原像困難性の証明及びハッシュ関数 LW を疑似ランダム関数として使用した場合の安全性は，文献[3]を参照されたい．また，圧縮関数の構造毎に網羅的に安全性を検討した結果については文献[5][7]を参照されたい．

（注）ハッシュ関数 LW の開発の一部は，研究代表者が株式会社日立製作所，国立大学法人福井大学と共同受託した（独）情報通信研究機構からの受託研究で行った成果である．

②既存のライトウエイトブロック暗号を用いた構成法

本研究課題の申請前後に，ライトウエイトブロック暗号の多数の提案がなされた．これらは，概ね 3 [Kgates]以下の回路規模を想定して設計されており，AES が実装できないような資源制約が厳しいデバイスへの応用を目的としている．そのような場合，別にハッシュ関数を実装するよりも，ライトウエイトブロック暗号を利用してハッシュ関数を実現する方が，総合的に回路規模が小さくできる見込みがある．

提案済みのライトウエイトブロック暗号は，回路規模削減のため，64～128 ビットの鍵，32～64 ビットの平文をサポートしている．特に，80 ビットの鍵，64 ビットの平文をサポートするライトウエイトブロック暗号が多い．したがって，ライトウエイトブロック暗号をハッシュ関数に利用するときは，平文長が短いので，暗号化関数を 2 回使用する double-block-length 圧縮関数を構成する必要がある．

double-block-length 圧縮関数によるハッシュ関数の研究には約 35 年の歴史がある．当初は，構成法の提案のみで十分な安全性解析がなかったが，2002 年頃から ideal cipher を用いた安全性解析手法が始まり，現在では ideal-cipher model での安全性解析が定着している．ideal-cipher model での安全性解析は，上述のように，そのハッシュ関数の安全性に対して一定の評価を与えているが，ideal cipher を実際の暗号に置き換えた場合の安全性を必ずしも保証できないという問題がある．

そこで，より現実に近いモデルでハッシュ関数の安全性を解析することは重要である．しかし，「使用するブロック暗号が疑似ランダム関数である」という合理的な計算量的仮定の下では，それを用いたハッシュ関数が衝突困難であることを示せない，という結果が明らかになっている．

ここで，「示せない」ことが証明されている安全性は，衝突困難性だけである点に注意すべきである．我々は，RFID のアプリケーションの場合，その安全性はハッシュ関数の衝突困難ではなく，原像困難性に依存する場合が多く，ハッシュ関数が HMAC のような疑似ランダム関数の構成部品と使われることが多いということに着目した．本研究では，ブロック暗号の計算量的な安全性を仮定して，原像困難性と疑似ランダム性を証明できるハッシュ関数 DbMMO を提案する．

鍵長がκ，平文長がnのブロック暗号Eを考える．典型的なパラメータは，多くのライトウエイトブロック暗号がサポートする$\kappa = 80$，$n = 64$である．ハッシュする，長さℓビットのメッセージをmとおく．mの最後に 1 を 1 個と 0 をt個付加する．ここで，tは

$$t=\begin{cases} n+\kappa-(\ell+1) & if\ \ \ell\le\kappa-1 \\ n-(\ell+1-\kappa \bmod n) & if\ \ \ell\ge\kappa \end{cases}$$

を満たす最小の整数である．この操作の後の系列の最初の ℓ ビットを m_0，残りを n ビット毎に $m_1,m_2,\cdots,m_l$ とする．$i=1,2,\cdots,l$ に対して，

$$x_1=tr\left(E(m_0,\ m_1)\right)\|tr\left(E(m_0\oplus c_1,m_1)\right)$$

$$x_i=tr\left(E(x_{i-1},m_i)\right)\|tr\left(E(x_{i-1}\oplus c_2,m_i)\right)$$

$$d=tr\left(E(x_l\oplus c_2,a_1)\right)\|tr\left(E(x_l\oplus c_2,a_2)\right)$$

とする（図 2）．ここで，tr は n ビットを $\kappa/2$ ビットに短縮する関数（例えば先頭 $\kappa/2$ ビットを取り出す関数）であり，c_1,c_2,c_3 は相異なる κ ビットの非零の定系列である．

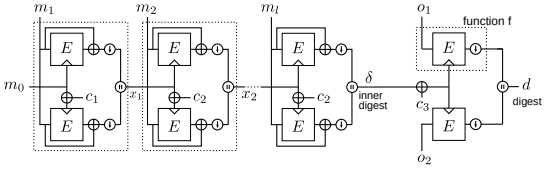

図 2 ハッシュ関数 DbMMO

ハッシュ関数 DbMMO の原像困難性と疑似ランダム性に関する結果を以下に示す．その証明は，平成 25 年度に発表予定である．

原像困難性：長さ ℓ ビット以下のメッセージ空間から一様分布に基づき選ばれたメッセージのダイジェスト d が与えられた攻撃者 A が長さ ℓ ビット以下の原像を発見できる確率は，

$$Adv_H^{pre}(A)\le 1dxH(\ell)Adv_E^{4-prp-rka}(B)+\frac{\phi_{tr\circ E}}{\phi_E}Adv_E^{2-kr-kp}(C)$$

である．ここで，$1dxH(\ell)$ は，長さ ℓ ビットのメッセージをメッセージブロックにしたときの最後のメッセージブロックのインデックスを表す．$Adv_E^{4-prp-rka}(B)$ は，攻撃者 B が鍵 k に対する下記の関連鍵攻撃により E がランダム置換と識別できる確率である．

$$\{k,k\oplus c_1,k\oplus c_2,k\oplus c_3\}$$

c_i はハッシュ関数 DbMMO で使用されている定数である．B は E に 2 回質問が可能であり，計算時間は，$\tau_A+O\left(\left(1dxH(\ell)+1dxH(\hat{\ell})\right)\tau_E\right)$ である．ここで，τ_A は A の計算時間，τ_E は暗号化関数 E を計算する時間である．ϕ_E は，

$$\phi_E=\frac{1}{2^\kappa}\sum_{k\in\{0,1\}^\kappa}\#\{a_i,y_i\}_{i=1}^{l}$$

であり，$\#\{a_i,y_i\}_{i=1}^{l}$ は，a_i はハッシュ関数 DbMMO で使用されている定数であり，

$$y_i=E(k,a_i)$$

を満たす k の個数である．$\phi_{tr\circ E}$ も同様に定義される．$Adv_E^{2-kr-kp}(C)$ は，攻撃者 C が o_1,o_2 の暗号文を与えられたとき，それらから鍵 k を求められる確率である．C の計算時間は，$\tau_A+O\left(1dxH(\hat{\ell})\tau_E\right)$ である．したがって，右辺の各項は，E の計算量的仮定と統計的仮定である．

疑似ランダム性：攻撃者 A が，m_2 にメッセージブロックではなく，鍵を入力する関数 $\hat{H}$ をランダム関数と識別できる確率は，

$$Adv_{\hat{H}}^{prf}(A)\le (l_{\max}+1)\left(qAdv_E^{4-prp-rka}(C)+\frac{2^{\kappa/2}}{1-\frac{2e}{\theta}}\left(\frac{2e}{\theta}\right)^{\theta}\right)$$

である．ここで，A は，$\hat{H}$ に $q<2^{n/2}$ 回の質問が可能であり，1 回の質問のメッセージのブロック数の最大値が ℓ_{max} である．$\theta=2^{n-\kappa/2}+1$ であり，e は自然対数の底である．

右辺の項で，E に関する安全性要件は，関連鍵攻撃時のランダム置換との識別困難性であり，計算量的な仮定である．

③スポンジ構造について

スポンジ構造に基づくハッシュ関数の構成法についても研究を行った．その結果，小さい置換を複数用いることで回路規模は小さくできるが，高い安全性を示すことはできなかった（文献[8]）．

（2）攻撃による安全性検証

①ライトウエイトブロック暗号 KATAN の cube attack に対する安全性評価

KATAN は，鍵長が 80 ビット，平文長が 32, 48, 64 ビットをサポートするライトウエイトブロック暗号である（文献[10]）．その構造はストリーム暗号でしばしば使用される非線形シフトレジスタに基づいている．その非線形関数の次数が低いため，cube attack（文献[11]）は有力な攻撃法である．

KATAN をハッシュ関数 DbMMO に使用する場合には，関連鍵攻撃への安全性を検討する必要がある．そこで，前述の関連鍵に限定せずに，cube attack を用いた関連鍵攻撃に対する安全性評価を計算機実験により行った．その結果を表 1 に示す．

KATAN のラウンド数は，252 である．したがって，cube attack に対して KATAN は十分な安全性を有していることが判明した（文献[6]）．この意味で，KATAN はハッシュ関数 DbMMO に適したライトブロック暗号である．

表 1 KATAN への cube attack

平文長[bits]	攻撃可能なラウンド数
32	87
48	75
64	69

②量子アルゴリズムを用いた Even-Masor 暗

号の安全性評価

Even-Mansor 暗号は，ランダム置換をp，鍵をk，平文をxとするとき，暗号文yを下記の式で生成する（図 3, 文献[12]）．

$$y = p(x \oplus k_1) \oplus k_2$$

ここで，$k = k_1 | k_2$である．これは，ラウンド数を 1 段に短縮した AES やライトウエイト暗号 LED とみなすことができる．

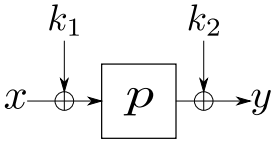

図 3 Even-Mansor 暗号

k_iのビット数を$n/2$とするとき，暗号化・復号化の回数をq_e, pまたはp^{-1}の計算回数をq_pとおく．このとき，鍵を求められる確率は，$O((q_e q_p)/2^{n/2})$であることが示されている．実際，これに近い攻撃法も示されている（文献[13]）．

しかし，古典計算機と量子計算機を併用すれば，古典的計算量N_c，量子計算量N_qが，

$$N_c = O\left(n 2^{\frac{n}{6}}\right), N_q = O\left(2^{\frac{n}{6}}\right)$$

である攻撃法が存在することを示した（文献[1][9]）．したがって，量子計算機を併用すれば，計算時間を古典計算機のみを使用する場合の計算時間の約 3 乗根で鍵を求めることができる．

なお，本研究では，量子計算機を用いた攻撃に対する Feistel 暗号の安全性評価もおこなった（文献[2]）．

参考文献

[1] H. Kuwakado and M. Morii, "Quantum Key Search on the Even-Mansour Cipher," Proceedings the 22th Quantum Information Technology Symposium, pp. 17-22, 2010.

[2] H. Kuwakado and M. Morii, "Quantum Distinguisher Between the 3-Round Feistel Cipher and the Random Permutation," Proceedings of the 2011 IEEE International Symposium on Information Theory, pp. 2682-2685, 2010.

[3] S. Hirose, K. Ideguchi, H. Kuwakado, T. Owada, B. Preneel, and H. Yoshida, "A Lightweight 256-bit Hash Function for Hardware and Low-end Devices: Lesamnta-LW," Proceedings of the 13th Annual International Conference on Information Security and Cryptology, ICISC 2010, Lecture Notes in Computer Science, vol. 6584, pp. 151-168, 2011.

[4] H. Kuwakado and M. Morii, "Distinguishing Attack and Key-Recovery Attack on the 3-Round Feistel Cipher," Proceedings of the 2010 Symposium on Information Theory and its Applications, pp. 208-213, 2010.

[5] S. Hirose, H. Kuwakado, and H. Yoshida, "Model of Blockcipher-Based Hash Functions Suitable for Memory-Constrained Devices," Proceedings of The 2011 Symposium on Cryptography and Information Security, 4B1-1, 2011.

[6] H. Kuwakado and S. Hirose, "Related-Key Cube Attack on KATAN48," 電子情報通信学会 2011 年ソサエティ大会講演論文集, 2011.

[7] S. Hirose, H. Kuwakado, and H. Yoshida, "Compression Functions Using a Dedicated Blockcipher for Lightweight Hashing," Information Security and Cryptology - ICISC 2011, Lecture Notes in Computer Science, vol. 7259, pp. 346-364, 2012.

[8] H. Kuwakado and S. Hirose, "Sponge Construction Using Multiple Primitives," Proceedings of The 2012 Symposium on Cryptography and Information Security, 1C1-5, 2012.

[9] H. Kuwakado and M. Morii, "Security on the Quantum-type Even-Mansour Cipher," Proc. of the 2012 International Symposium on Information Theory and its Applications, pp. 312-316, 2012.

[10] C. Canniere, O. Dunkelman, and M. Knezevic, "KATAN and KTANTAN - A Family of Small and Efficient Hardware-Oriented Block Ciphers," Cryptographic Hardware and Embedded Systems - CHES 2009, 11th International Workshop, Lecture Notes in Computer Science, vol. 5747, pp. 272-288, 2009.

[11] I. Dinur and A. Shamir, "Cube Attacks on Tweakable Black Box Polynomials," Advances in Cryptology - EUROCRYPT 2009, Lecture Notes in Computer Science, vol. 5479, pp. 278-299, 2009.

[12] S. Even and Y. Mansour, "A Construction of a Cipher From a Single Pseudorandom Permutation," Journal of Cryptology, vol. 10, no. 3, pp. 151-161, 1997.

[13] J. Daemen and L. Esat, "Limitations of the Even-Mansour Construction," Advances in Cryptology - ASIACRYPT '91, Lecture Notes in Computer Science,

vol.739, pp.495-498, 1993.

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９件）

1. H.Kuwakado and M.Morii, "Security on the Quantum-type Even-Mansour Cipher," Proc. of the 2012 International Symposium on Information Theory and its Applications, 査読有, pp.312-316, 2012.
2. H.Kuwakado and S.Hirose, "Sponge Construction Using Multiple Primitives," Proceedings of The 2012 Symposium on Cryptography and Information Security, 査読無, 1C1-5, 2012.
3. S.Hirose, H.Kuwakado, and H.Yoshida, "Compression Functions Using a Dedicated Blockcipher for Lightweight Hashing," Information Security and Cryptology - ICISC 2011, Lecture Notes in Computer Science, 査読有, vol.7259, pp.346-364, 2012.
4. H.Kuwakado and S.Hirose, "Related-Key Cube Attack on KATAN48," 電子情報通信学会 2011 年ソサエティ大会講演論文集, 査読無, 2011.
5. S.Hirose, H.Kuwakado, and H.Yoshida, "Model of Blockcipher-Based Hash Functions Suitable for Memory-Constrained Devices," Proceedings of The 2011 Symposium on Cryptography and Information Security, 査読無, 4B1-1, 2011.
6. S.Hirose, K.Ideguchi, H.Kuwakado, T.Owada, B.Preneel, and H.Yoshida, "A Lightweight 256-bit Hash Function for Hardware and Low-end Devices: Lesamnta-LW," Proceedings of the 13th Annual International Conference on Information Security and Cryptology, ICISC 2010, Lecture Notes in Computer Science, 査読有, vol.6584, pp.151-168, 2011.
7. H.Kuwakado and M.Morii, "Distinguishing Attack and Key-Recovery Attack on the 3-Round Feistel Cipher," Proceedings of the 2010 Symposium on Information Theory and its Applications, 査読無, pp.208-213, 2010.
8. H.Kuwakado and M.Morii, "Quantum Distinguisher Between the 3-Round Feistel Cipher and the Random Permutation," Proceedings of the 2011 IEEE International Symposium on Information Theory, 査読有, pp.2682-2685, 2010.
9. H.Kuwakado and M.Morii, "Quantum Key Search on the Even-Mansour Cipher," Proceedings the 22th Quantum Information Technology Symposium, 査読無, pp.17-22, 2010.

〔学会発表〕（計０件）

〔図書〕（計０件）

〔その他〕
なし

６．研究組織
(1)研究代表者

桑門　秀典（Kuwakado Hidenori）
神戸大学・工学研究科・准教授
研究者番号：30283914

(2)研究分担者
なし　　（　　）
研究者番号：

(3)連携研究者
なし　　（　　）
研究者番号：