SAKA プロトコルにおけるパスワード認証実装と基礎 RSA 暗号との比較検証

島根大学　総合理工学部　数理・情報システム学科

応用情報学講座　田中研究室

s003046　塚定　尚之

目次

第１章　はじめに

コンピュータセキュリティにおける先行研究事例調査

コンピュータセキュリティに関する研究活動における目的には実に様々なものがあり、それら存在する目的それぞれに対して各々の研究者がまた多種多様な手法を用いて日々、研究努力を積み重ねている。このような、非常に多伎に渡る知的活動が行われているという混沌とした状況下において、大局を見て、過去から現在までに渡って為されてきた諸研究及び今後の見通し等についての知識を得、いくらかの概観を把握し理路整然とした展望を得ることは、今後、合理的な研究活動を進めていくためにも有益かつ重要なことでありまた、必要なことであると考える。

この論文においては、コンピュータセキュリティにおける調査を行い、実際の論文などから得た情報を編纂することに加えて、各文献などを統合した知識からの考察及び検証を行う。

最後にこの論文の構成を解説する。まず２章において、先行研究の調査過程について記す。続けて３、４章で実際の研究例をもとにして行った調査の詳細を記述し更に５章で、実際のそれ等を実装してシミュレートした例を示す。そして６章で考察し最後に７章で全体のまとめを行う。

第２章　先行研究の調査

まずはじめの段階として、既存の研究についての信頼できる情報を得るために、理工系書誌情報データベースである INSPEC を用いた検索を行うこととした。あらかじめ自身の興味に沿って選定した、複数の検索語を使用することによって文献の検索を行った。その具体的な過程について詳細を述べる。

２．１　INSPEC について

INSPEC とは 1969 年より IEE(Institution of Electrical Engineers)によって構成された、物理学、電気工学、エレクトロニクス、コンピュータ関連分野にわたる世界的な科学技術文献を網羅したリソースである。3500 誌を超える学術雑誌、 1500 以上の会議録、数多くの書籍、報告書、学位論文を収録し、約 700 万件の書誌情報を収録しており、 最新の研究情報から過去の貴重な情報までを包括的にカバーする情報源であり、毎年約 35 万件以上のレコードが追加されている。
（http://www.engineeringvillage2.org/controller/servlet/Controller?CID=quickSearch&database=INSPEC）

INSPEC は IEE という、電気通信などの分野において不動といってもよいであろうレベルの信頼性をもつコミュニティによって提供されており、また、実際に過去から現在に渡ってまでの間、多くの人々の間で幅広く利用されてきているというその事実から、データベース自体への信頼性も十分に期待でるであろうという判断理由をもって、今回このリソースを検索の対象として使用することとした。

２．２　検出過程の詳細

第 1 章に記した内容を達成するに適切だと予想される、複数のキーワードを選定し、最終的に検索語として Crypt、Encrypt、cipher、hide、code、encode、secure、network、system、human というこれらの語を用いて、INSPEC から論文の抽出を行った。その具体的な過程を表 1、表 2 に示す。なお、年代的に古すぎるものを除外するために、検索対象とする文献の発行年代を 1995 年から 2004 年までに限定している.また、検索日時は２００４年１０月１３日であり、表は最新のものではなく、その時点での INSPEC からの検索結果となっている。

検索結果

表１

該当件数	検索語
１１６４	(Crypt or encrypt or cipher or hide or code or encode) and secure and network and system
３７	(Crypt or encrypt or cipher or hide or code or encode) and secure and network and system and human

内訳

表２

1	Trust : a collision of paradigms [network security]
2	Information Security Applications. 4th International Workshop, WISA 2003. Revised papers.
3	Recent development using H.263 and wavelets for digital video/image compression and implementation
4	Adaptive digital watermarking using neural network technique
5	Privacy and security issues in a wide area health communications network
6	Human visual System features enabling watermarking
7	Human immune anomaly and misuse based detection for computer system operations : part2
8	Data security and patient confidentiality : the manager`s role
9	Effective neural network approach to image recognition and control
１０	Public-key cryptography and password protocols : the multi-user case
１１	KVM switch solves server expansion : insurance service company chooses remote access over more IT personnel
１２	ARGUS : an automated multi-agent visitor identification system
１３	Frangipani : ascalable distributed file system
１４	Effects of data hiding on remote data analysis
１５	A use-condition centered approach to authenticated global capabilities : security architectures for large-scale distributed collaboratory environments
１６	Approaches for a reliable high-performance distributed-parallel storage system

17	Secure management of a proxy server using SNMP and java applets
18	Data mining-based intrusion detectors : an overview of the Columbia IDS project
19	WaveNet processing brassboards for live via radio
20	Setting up a secure public workstation
21	Dynamic control of worm propagation
22	An introduction to face recognition technology
23	Lossy compression tolerant steganography
24	Fighting spam by encapsulating policy in email addresses
25	Jini security : a novel approach
26	PKI : coming to an enterprise near you?
27	Spontnet : experiences in configuring and securing small ad hoc networks
28	WaveNet processing brassborads for live video via radio
29	New audio secret sharing schemes with time division technique
30	Bank balances privacy, convenience
31	The open-end argument for private computing
32	Objectvideo forensics : activity-based video indexing and retrieval for physical security applications
33	Passeord authentication using multiple servers
34	Analysis of the DCS.v2 authentication protocol
35	Secure distributed configuration management with randomised scheduling of system-administration task
36	Design and implementation of user-authentication system in distributed systems
37	Depositing and delivering RSA private keys

２．３　選出結果

次段階として,検索結果表 1 及び２より、興味を持った論文（表２　１０番）を取り寄せ、さらに関連文献として、ACM、Boyarsky と入力４件の結果がでたのでそのなかから読み解くこととした。（表３）

そして最終的に実際に本論文中において参考とし、内容を直接とりあげたものについて表に記す。（表４）

表３

1	Public-key cryptography and password protocols : the multi-user case
2	Simple authenticated key agreement protocol resistant to password guessing attacks
3	Authentication and authorization : Securing passwords against dictionary attacks
4	Minimum time path planning for robot motion in obstacle strewn environment

表４

表題	Simple authenticated key agreement protocols resistant to password guessing attacks
表題訳	パスワード攻撃に抵抗力がある単純な認証プロトコル
著者	Her-Tyan Yeh,Hung-Min Sun
出所	ACM SIGOPS Operating Systems Review,　Volume36 Issue4　１４－２２
年度	２００２

この（表４）の論文は簡潔にわかりやすく書いてあったが理論のみ書かれていたために本研究で理論の検証を行うためにとりあげた。

第 3 章 SAKA プロトコルについての説明

（Simple Authenticated Key Agreement protocols）

３．１　SAKA プロトコルの原理　　（図１）　〔１〕

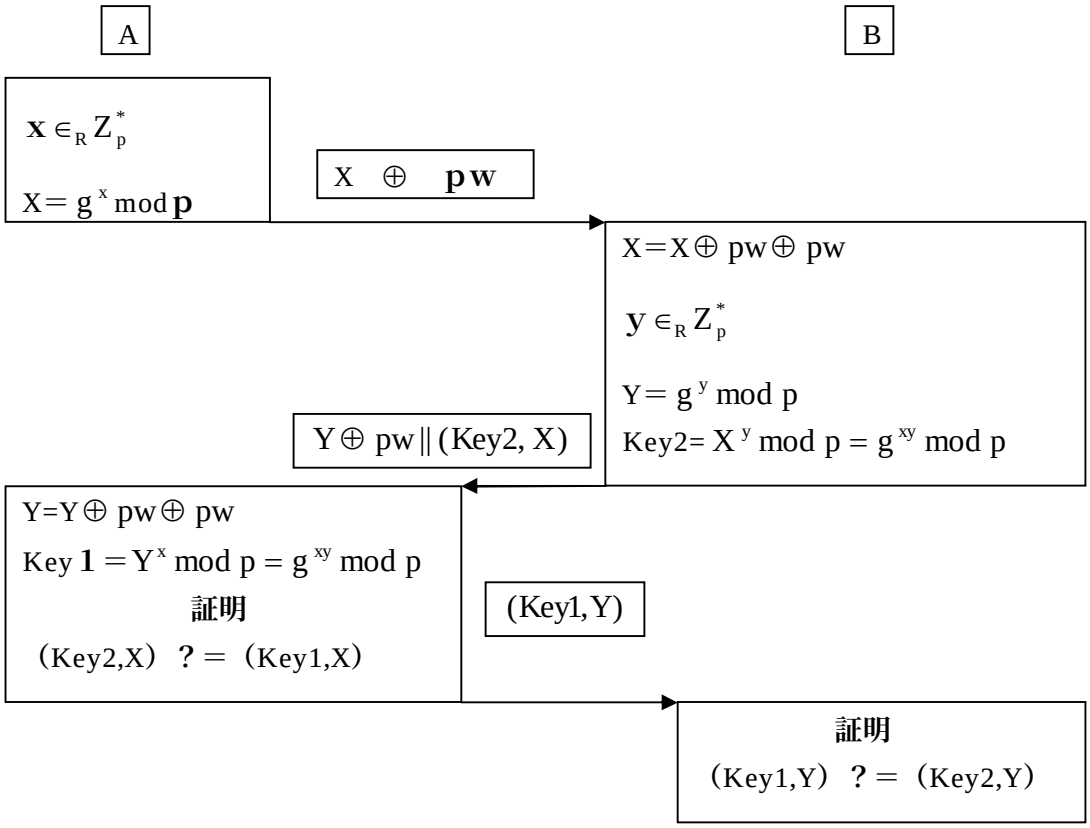

図１

図の記号

⊕ : xor

３．２　手順説明

まず当事者間（A―B）の間で以下の事項を決める
パスワード（pw、整数)、整数（g)、整数（p）

A―①　ランダム変数 x を作成しそこから X を計算し
pw で鍵をかけ B にそのデータを送る

B―①　データを受け取ったら pw で開錠し X を知る
そしてランダム変数 y を作成し、Y と Key２
を作成し Y に pw で鍵をかけそのデータと X
と Key2 の３データを A に送る。

A―②　送られてきたデータのうち Y を pw で開錠し
そのデータから Key1 を作成する。ここで
送られてきた（X、Key2）と自分の作った（X、Key1）
が同じなら B が B 本人であると証明される。
そして B に計算した Y と Key１を送る

B―②　送られてきた（Y、Key1）と自分の作った（Y、Key2）
が同じなら A が A 本人であると証明される。

第4章　基礎 RSA 暗号についての説明

４．１　基礎 RSA 暗号における認証の原理（図２）　〔２〕

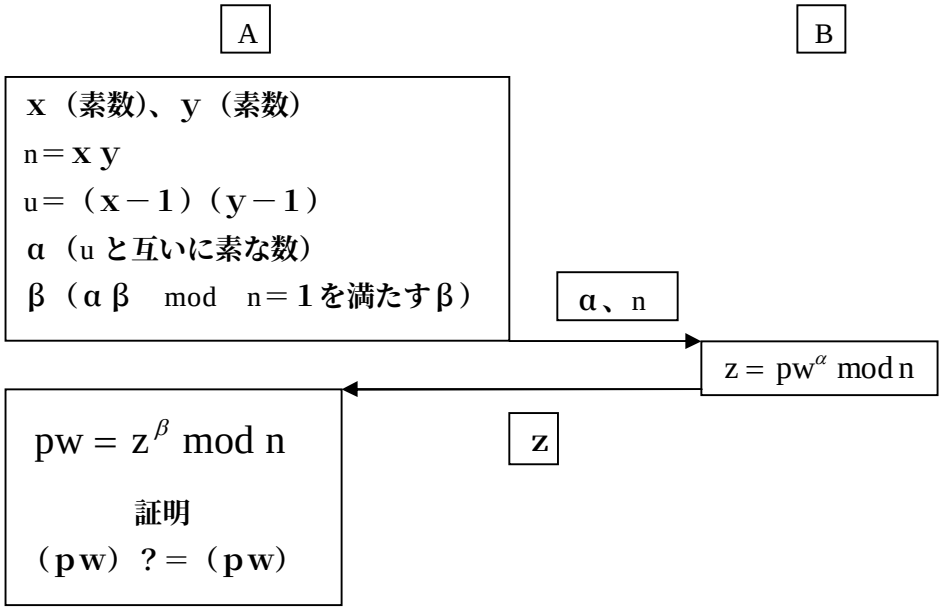

図２

４．２　手順説明　〔２〕〔３〕〔４〕

まず当事者間（A―B）の間で以下の事項を決める
パスワード（pw、整数）

A―①　素数を２つ決めるこれをｘ、ｙとする。そして公開鍵１として
n＝xy（公開法）を決め　u＝（ｘ－１）（ｙ－１）とし
u と互いに素な数　α（公開指数）を決めて開錠に必要な
秘密鍵βを　α β　mod　n＝１となるようにとる。
それから B に n とαを送る。

B―①　受け取った n とαを用いて pw に鍵をかけｚを作成します。
（ｚ＝ pw^{α}　mod　n）
そしてこのｚを A に送る。

A―②　受け取ったｚをβと n を用いて開錠し pw を得ます。
（ｐｗ＝ z^{β}　mod　n）
この計算から得たｐｗと自分の持っているｐｗが一致すれば
B が本物と証明される。

第5章　SAKA プロトコルと RSA 暗号の比較シミュレーション

５．１　実験方法

以下の図のようにサーバー、クライアント間で Java を使用した
サーブレット、アプレットを用いて相互認証を行った。（図３）

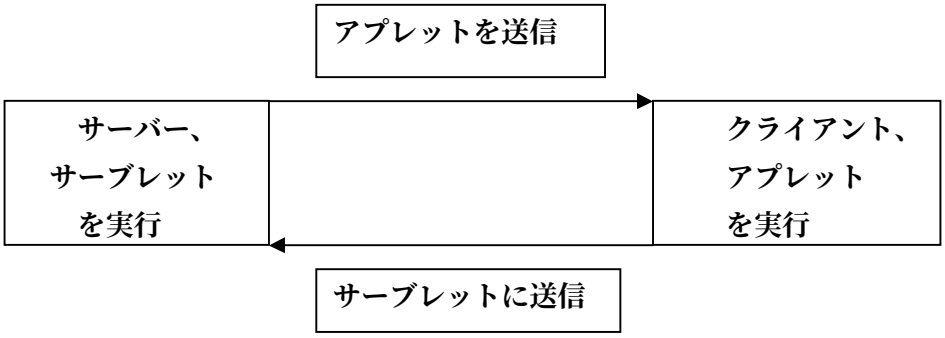

図３

何故、サーブレット　アプレットを用いて通信を行ったかというと、最初パソコン間で
数の引渡しを行う時　IE　、アプレット　、Java スクリプトの３つのうちどれかによって
行う予定だった。

まず　IE　だが　MSDN データベースで「IE による数の引渡し」を検索したところ
１００件の結果が返ってきたが、１００件というのは Q&A 最新１００件と考えら
れる内容だった。その内容を見たところ .net に関する内容で IE からの数の引渡し
に関係ないと判断した。そのため IE での数の引渡しに関しては見通しがたたないた
めに IE での数の引渡しをあきらめた。

次にサーブレット、アプレットで数の引渡しについて調べたが、まず島根大学の
卒業論文でサーブレット、アプレットでの数の引渡しについて書かれていたプログ
ラム探すとその方法があったので、この手法をとった。　〔５〕

最後に Java スクリプトについては上記で方法が見つかったために調べていない。

また実験に使用した PC のマシンスペックは以下の表（表５）のとおりである。

表５

環境	サーバー	クライアント
CPU	Celeron　1.70GHｚ	Celeron　2.40GHｚ
MEMORY	５１２MB	５１２MB
HD	４０GB	１６０GB
LAN	１００Base/T	１００Base/T
IP アドレス	192.168.1.200	192.168.1.110

そして、SAKA アルゴリズム及び基礎 RSA の実現には Java 言語による
アプレット、サーブレットにより可能にした。

サーブレットとはサーバーにおかれているプログラムで、クライアントがサーバーに要求をだすとサーバーが実行するプログラムである。

アプレットとはサーバーにおかれているプログラムだが、サーバーからクライアントに送られクライアントが実行するプログラムである。

この２つにより SAKA、RSA 両方の実現を可能にした。以下の図は
おおまかなアプレット、サーブレットの流れである。

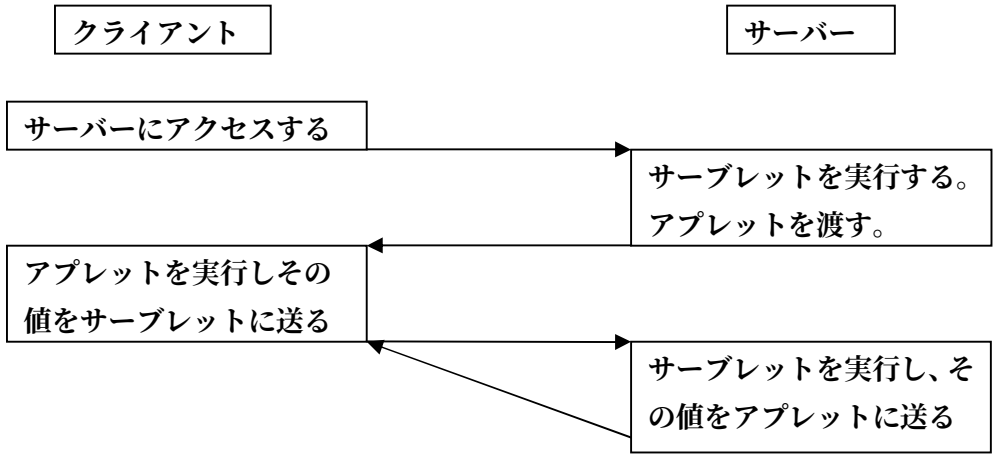

図４

SAKA プロトコル、基礎 RSA のサーブレット、アプレットの流れ

① クライアントがサーバーにアクセスする。
（今回の検証では HP にサーブレットにアクセスするパネルを設置した。）

② サーバーにおいてサーブレット１が実行される。
（このサーブレット１はクライアントにアプレット１を送るだけのもの）
サーブレット１が実行され、アプレット１がクライアントに送られる。

③ クライアントで送られてきたアプレット１が計算され、サーブレット２に値が送られる。
（サーブレット２は SAKA プロトコルの計算部分を実行するプログラム）

④ サーバーがサーブレット２を実行しアプレット１に値を送る。

③～④を繰り返して結果がでる。

＊ 今回の検証ではサーブレットサーバー環境が必要となる。
そのため今回の実験では Tomcat と呼ばれる http サーバーを用いた。
Tomcat を選んだ理由は Java サーブレットを起動させる事ができるからである

５．２　SAKA プロトコルにおけるパスワード認証経過時間

今回の実験で使った SAKA プロトコルでの注意点を書いておく

３２Bit である

ランダム変数ｘは０～２００００の間で実験を行った。

⊕：Xor　についての考え方は整数において
7⊕11　＝　00111　⊕　01011　＝　01100　＝12
12⊕11　＝　01100　⊕　01011　＝　00111　= 7
と考えた。

使った pw g p　などの値は２桁以内とした。
実際には pw＝７　ｇ＝３　ｐ＝６０として実験を行った

実験では手動でサーバーに１００回アクセスした。

１００回の平均認証時間は

２．８２（ms）となり

標準偏差は

６．０５２５７８となった。

５．３　基礎 RSA 暗号におけるパスワード認証経過時間

今回の実験で使った基礎 RSA 暗号での注意点を書いておく

３２Bit である。

素数はまずランダムで　０～２００００　の値を取りそこから奇数（ランダムが偶数をだしたとき＋１）にし＋２ずつして素数判定を行う。
同じ素数を選ばないようにするために後の素数作成で前の素数と同じになったときはさらに＋２していく。
この方法だと素数の範囲は　２～（２００１１）～２００２１　となる。

Pw の値は７として実験を行った。

実験では手動でサーバーに 100 回アクセスした

１００回の平均認証時間は

１１９４．６３（ms）となり

標準偏差は

８７１．２５７６となった。

第6章　考察

結果から大きな時間差がでている。これは SAKA プロトコルが暗号化、復号化の両方合わせた計算量が少ない事を示している。何故少なくなるか、これはお互いランダムな数を使うが（このランダムな数をｘ，ｙとする）、SAKA ではある値 N のｘ乗が計算で時間を取るが、RSA では復号（開錠）にひつようなβが大きい値をとる事が多いために N のβ乗に大きな時間をとっていると考えられる。それゆえに平均認証時間においては SAKA プロトコルの方が優秀であると言える。

第7章　まとめ

SAKA プロトコルが基礎 RSA よりはるかに早く認証できることが実証された。
しかし問題として、初めての相手に対する汎用性は基礎 RSA のほうが勝っている、
そして RSA のプログラムが現在最速と思われるプログラムより遅いために改善する必要がある、また今回は整数のみを対象としたので今後は実数や文字などにも対応できるようにしたい。

第8章　謝辞

本研究にあたり、最後まで熱心な御指導をいただきました田中教授には、心より御礼申し上げます。また、田中研究室在籍の院生及び、同期生の方々には、本研究に関して直接、及び間接的に数々の御協力と御助言をいただきました。この場で厚く御礼申し上げます。
なお、本論文、並びに関連する発表資料等のすべての知的財産権を、本研究の指導教官である田中教授に譲渡致します。

第9章　引用文献

〔1〕　Her-Tyan Yeh,Hung-Min Sun“Simple authenticated key agreement protocols resistant to password guessing attacks”ACM SIGOPS Operating Systems Review,　Volume36 Issue4　Oct 2002　　P14-22

〔2〕結城　浩　、暗号技術入門、ソフトバンクパブリッシング、２００３

〔3〕ブルース・シュナイアー、暗号技術大全、ソフトバンクパブリッシング、２００３

〔4〕公開鍵暗号 RSA 入門　（http://www.faireal.net/articles/5/24/#d20523）

〔5〕森本　誠人、クライアント・サーバー型 Web 対応画像解析システムの開発、
島根大学修士論文、２００１