RESUME

Name	Vipul Goyal
E-mail address	vipul.goyal@cse04.itbhu.org
Alternate E-mail	vipul_goyal1@yahoo.com
Home Page	www.geocities.com/vipul_goyal1/apply.htm
Current Professional Status	Cryptography Research Analyst Offshore Security Partners Global, Mumbai

List of Publications

IMPORTANT NOTE: This list is likely to be significantly updated in Mid-Jan. For an updated list, visit URL: www.geocities.com/vipul_goyal1/apply.htm. You may also download my recent papers from this link.

Papers Accepted/Published

Book Chapters

1. Vipul Goyal, Ajith Abraham, Sugata Sanyal, "Cryptographic Signature Schemes in the Quantum Computing World", Progress in Quantum Cryptography Research, Frank Columbus (Ed.), Nova Science Publishers, USA.

Conference Publications

2. Vipul Goyal, "Certificate Revocation using Fine Grained Certificate Space Partitioning", The First Information Security Practice and Experience Conference (ISPEC 2005), Singapore, April 2005, Lecture Notes in Computer Science, Springer-Verlag. (Acceptance Rate: 40/120)

3. Vipul Goyal, "Construction and Traversal of Hash Chains with public links", The First Information Security Practice and Experience Conference (ISPEC 2005), Singapore, April 2005, Lecture Notes in Computer Science, Springer-Verlag. (Acceptance Rate: 40/120)

4. Vipul Goyal, Virendra Kumar, Mayank Singh, "An Efficient Solution for the ARP Cache Poisoning Problem", The First Information Security Practice and Experience Conference (ISPEC 2005), Singapore, April 2005, Lecture Notes in Computer Science, Springer-Verlag. (Acceptance Rate: 40/120)

5. Vipul Goyal, "Extending CRS for Real Time Revocation Information", 20th International IFIP Conference on Information Security (SEC-2005), Japan, May 2005, Kluwer. (Acceptance Rate: 29 %)

6. Vipul Goyal, Virendra Kumar, Mayank Singh, Ajith Abraham, Sugata Sanyal, "CompChall: Addressing Password Guessing Attacks", Information Assurance and Security Track (IAS'05), IEEE International Conference on Information Technology: Coding and Computing (ITCC'05), USA, April 2005, IEEE Computer Society.

7. Vipul Goyal, Ajith Abraham, Sugata Sanyal, Sang Yong Han, "The N/R One Time Password System", Information Assurance and Security Track (IAS'05), IEEE International Conference on Information Technology: Coding and Computing (ITCC'05), USA, April 2005, IEEE Computer Society.

8. Vipul Goyal, Virendra Kumar, Mayank Singh, "Fighting Spam: An Origin Server Authentication Based Approach", 4th IEEE International Conference on Networking (ICN 2005), Reunion Island, April 2005, Lecture Notes in Computer Science, Springer-Verlag.

9. Vipul Goyal, “Fast Digital Certificate Revocation”, Proceedings of 19th International IFIP Conference on Information Security (SEC-2004), held as part of IFIP World Computer Congress (WCC-2004), Toulouse, France, August 2004, pp 489-500, Kluwer. (Acceptance Rate: 22 %. Also got the conference fellowship of 1,500 Euro for attending the conference)

10. Vipul Goyal, "On Encryption by Microprocessors", 3rd International Trusted Internet Workshop (TIW-2004), held in conjunction with 11th International Conference on High Performance Computing (HiPC-2004), Bangalore, India, Dec 2004. (Acceptance Rate: 30 %)

11. Vipul Goyal, "Soft Enforcement of Access Control Policies in Distributed Environments", Poster Proceedings of 11th International Conference on High Performance Computing (HiPC-2004), Bangalore, India, Dec 2004.

12. Vipul Goyal, “A One Time Password System”, 7th International Conference on Information Technology (CIT-2004), Hyderabad, India, Dec 2004. (Acceptance Rate: 26 %)

13. Omkant Pandey, Vipul Goyal, “Cache Poisoning in S-ARP and modifications”, 5th International Conference on Information & Computer Science (ICICS-2004), Saudi Arabia, Nov 2004. (Acceptance Rate: 49 %)

14. Vipul Goyal, “Certificate Revocation Lists or Online Mechanisms?”, Proceedings of the 2nd International Workshop on Security in Information Systems (WOSIS-2004), held in conjunction with 6th International Conference on Enterprise Information Systems (ICEIS-2004), Portugal, April 2004, pp. 261-268. (Acceptance Rate: 48 %)

15. Vipul Goyal, Sugata Sanyal, Dharma P. Agarwal, "Vcache: Caching Dynamic Documents", Proceedings of the 6th International Conference on Information Technology (CIT-2003), India, Dec 2003, pp. 338-342. (Acceptance Rate: 29 %)

Papers under Submission

1. Vipul Goyal, "Certificate Revocation using Fine Grained Certificate Space Partitioning"
   This is a new certificate revocation technique. The basic idea is to divide the certificate space into a number of partitions. Each day, either a partition would expire or be renewed by the CA by exposing a hash chain link. The number of partitions is the key parameter in our scheme and represents a tradeoff between the CA to Directory communication and the query communication. It is possible to strike the right balance between these two communication costs by choosing the number of partitions intelligently. We demonstrate that in the case of a distributed CA having a number of directories to answer the user queries, the overall system communication cost is lower in our scheme as compared to CRS, CRT and CRL. One more contribution of this paper is an improvement to the Crypto'98 scheme by Aiello et al.

2. Vipul Goyal, "Construction and Traversal of Hash Chains with public links"
   Present hash chain traversal techniques require that the intermediate hash chain links be stored secretly on a trusted storage. This may be an unrealistic assumption in scenarios like Lamport's One Time Password system. We design a new construction of hash chains in which the intermediate links may be made public and be stored on a non-trusted device. Interestingly, we also propose a method to apply present hash chain traversal techniques to our construction without any significant changes in the computational and storage requirements. We achieve provable security by replacing the hash function with a MAC Function like HMAC.

3. Vipul Goyal, "Bulk Message Signing".

This is a signature scheme for servers which handle a large number of digital signature generations per second. We sign a set of messages with just a single signature generation and a number of hash function computation to significantly reduce the computational requirements of the system. With this technique, a system which was earlier able to handle only say 20 signature generations per seconds will be able to handle approximately 50,000 signature generations per second. The downside is the slight increase in signature length and response time. This technique can be profitably employed in payment systems, e-banking / e-commerce, signing routing messages and OCSP etc to result in significant cost reduction for the server. We also include a proof of security.

4. Vipul Goyal, Virendra Kumar, Mayank Singh, "A New Architecture for Address Resolution".
   This is a new and provably secure method to solve the long standing problem of ARP cache poisoning problem. For maintaining efficiency, only collision resistant hash functions are used throughout and no PKC is employed. The technique is based on the use of Merkle trees and a secure broadcast authentication protocol such as TESLA. Further, our system does not require the periodic refreshing of ARP cache mappings as in traditional ARP.

5. Vipul Goyal, "Password Based Authentication without Public Key Cryptography".
   A new password based authentication system using one way hash functions is designed. The system is secure against both active and passive adversaries as well as server password file compromise. It does not have the problems associated with Lamport's OTP scheme and is especially suitable for mobile devices.

6. Vipul Goyal, "More Efficient Server Assisted One Time Signatures".
   The recently designed server assisted one time signature scheme had the problems of high storage requirements for the virtual server and high memory requirements for the mobile client. We significantly reduce these requirements. This is done by employing a new dispute resolution technique and generating the OTS keys pseudorandomly.

7. Vipul Goyal, "How to Re-initialize a Hash Chain".
   Currently, hash chains suffer from the limitation that they have a finite number of links which when exhausted requires the system to be re-initialized. We construct a new kind of hash chain called a Re-initializable Hash Chain (RHC) having the property that if its links are exhausted, it can be securely re-initialized in a non-repudiable manner to result in another RHC.

Current Research Work

1) A Full-fledged Digital Signature Scheme using Hash Functions only
   I am working towards the construction of a full fledged (i.e. with no limits on the number of signatures that can generated) signature scheme using hash functions (without trapdoors) only. Such a scheme was designed by Merkle in 1987 using infinitely growing one time signature trees. However, this scheme was of theoretical interest only due to high computation, storage and signature size. My approach is based on an infinitely growing set of interconnected Merkle trees. As we generate more and more signatures, new Merkle trees are simultaneously constructed and added to the set. I provide a computation and storage tradeoff with which, it is possible to compute a signature with as low as 300 hash function evaluations, all of which may be done offline. Apart from being more efficient, such signatures do not require any number theoretic assumptions and are even secure against quantum computers.

2) How to Cheat the Cheater or Probabilistic-Information Leakage
   This is an interesting new problem being considered. Often, cryptanalysis is possible because the adversary can usually identify the correct {key, plaintext} pair when obtained (as plaintext obtained with incorrect keys is usually garbage). We suggest that the encryption algorithms be designed in such a way that for

every ciphertext, there are multiple {key, plaintext} pairs which make sense to the adversary. While Shannon's perfect secrecy concept is concerned with message secrecy, we are concerned with key secrecy.

Conference Participations

1) Served as a Reviewer for
   a) Information Assurance and Security Track (IAS'05), IEEE International Conference on Information Technology (ITCC 2005), Nevada, USA, 2005
   b) Ninth IEEE Symposium on Computers and Communications, Egypt, 2004
   c) International Conference on Information & Computer Science, Saudi Arabia, 2004

2) Attended the following conferences:
   a) 5th International Conference on Cryptology in India (Indocrypt-2004), Chennai
   b) 11th International Conference on High Performance Computing (Hipc-2004), Bangalore
   c) 7th International Conference on Information Technology (CIT-2004), Hyderabad
   d) 19th International IFIP Conference on Information Security (SEC-2004), France
   e) 4th International Conference on Cryptology in India (Indocrypt-2003), New Delhi
   f) 10th International Conference on High Performance Computing (Hipc-2003), Hyderabad
   g) 6th International Conference on Information Technology (CIT-2003), Bhubaneswar.

Academic Record (Absolute Scale)

DGPA	: 8.07/10
GPA (Majors)	: 8.46/10
12th Standard	: 79.6 % (Science subjects - 93 %)
10th Standard	: 80.8 % (Science & Mathematics - 94 %)

List of Awards/Achievements

- Highest paid job offer in the 2003-2004 placement session on the campus at IT-BHU.
- Secured 1st position in Open Software Contest in Technex-2003 (Technical festival and National Engineering Model Exhibition, IT-BHU) for "A Secure Electronic Payment System". This software was given the Malviya Best Software Award in Technex-2003.
- Secured 1st position among 102 participants in my institute in the C/C++ Quiz organized by IEEE, IT-BHU Student Chapter in September-2002.
- Secured 1st position in my institute in the Overnight Programming Contest organized by Computer Engineering Society in September-2002.
- Secured 1st position in my institute in the Programming Contest Organized by IEE, IT-BHU Student Chapter in September-2001.
- Nominated to represent IT-BHU in the Intel Student Research Contest for 2003-2004.
- Awarded the Certificate of Appreciation by Talisma Corporations for "Pitgame" (Talisma campus challenge). The software was appreciated for its efficient algorithm used by the computer for playing the game.
- Cleared IIT-JEE in the first attempt and was placed among the top 1 % of about 0.2 million students participating.
- Ranked 92 out of 96,000 candidates in the first attempt in the Engineering Entrance Examination of U.P. State (MNR-2000).

Industrial Experience

1) RemotePay™ Card – A New Internet Payment System

Abstract: This is a new electronic payment system. The only requirement for the customer is to purchase a RemotePay payment card (available as scratch cards) which will be made available at various outlets. This scheme does not require the user to possess a credit-card or even a bank account. This system is targeted at users in developing countries who do not possess a credit-card or the users who are security sensitive and hesitate to give out their card information on the internet. Using RemotePay Card, it is also possible for the customer to make payment to the vendors which support credit cards as the only payment mechanism. This is done by assigning the customers a temporary credit-card number against the RemotePay card number. With a modification, the scheme can be made to provide security against an un-trusted merchant. The system security is based on a two system architecture, one connected but having no secrets and the other having the system secrets but not connected to the outside world.

This project is being done at OSP Global, Mumbai. I am one of the main system designers. This product is scheduled to be launched in India and China in April, 2005.

Other Projects Completed

1) Caching Dynamically Generated Documents

Abstract: Web caching is currently limited to static HTML documents. A dynamic document is generated on the fly from a server side script and may have different contents on different accesses and hence cannot be cached. However different instances of a dynamic document have large common HTML code sections in most cases. This fact was exploited to design a language independent and fully automatic caching technique for dynamic documents based on their decomposition into a hierarchy of templates and bindings. This decomposition is done at the server by parsing the source code of the server script and then using the branch flow statistics analysis technique. The templates can then be cached while bindings are non-cacheable. This approach reduces the response time, load on server and network bandwidth consumption for both client and server. Currently, a journal version of this work is under preparation.

2) Summer Internship (May-June 2003)

Guide-
Prof Sharat Chandran
Department of Computer Science & Engg
Indian Institute of Technology, Bombay

"Fast Reconstruction 3D Objects with Radial Basis Functions using Fast Multipole Methods"

Abstract: The 3D object is represented with a single RBF. The RBF is found by interpolating the point cloud data representing the object. The interpolation problem is highly computationally intensive, however the storage and computation order can be highly reduced using FMM. GMRES iteration method coupled with FMM is used for solving the interpolation problem. The implementation of this method was done in C++.

3) Summer Internship (May-June 2002)

Guide-
Prof Sharat Chandran
Department of Computer Science & Engg
Indian Institute of Technology, Bombay

a) Development of an interactive e-book on Machine Vision

Abstract: Each chapter in the book is presented in four stages Theory, Experiment, Demonstration and Analysis. The experiment part was implemented using Java Applets. I developed chapters on Compositing and Colors. The learner could read the theory part and then could play with various applets in experiment part to get a feel of the topic.

b) Online processing of course feedback forms and response statistics display using bar graphs

Abstract: The students taking a course could fill up the course feedback form on the web. The system could automatically draw several bar graphs for different sections and in different formats using the responses submitted by the students. CGI-PERL was used for server side processing and bar graphs were implemented as Java Applets. This system is practically being used by IIT Bombay for course feedback.

4) Programmable high precision calculation system

Abstract: This is a Fully Programmable Calculation System with facility of user defined size of numbers especially useful for Scientific and Statistical Uses. The user has the facility of programming the calculation system for his specific uses and to define custom functions. Since the program may use very large numbers, special care was given to designed efficient routines for calculation. This project was done in C++.

This project was presented in Technex-2002 and was also selected for Techfest-2002, IIT Bombay.

5) Pitgame

Abstract: This was done for Talisma Campus Challenge. The computer had to play either against a human or against another computer using a LAN. An efficient algorithm was designed for playing the game based on solution space search upto a user specified depth and an optimized static evaluation function. A Certificate of appreciation was awarded by Talisma for this project.

6) Secure-DOS

Abstract: This was a security system in MS-DOS totally based on Terminate Stay Resident facilitating differential access rights to different users as in Unix. The access rights of each user (except root) were restricted to his/her home directory using this software. However, the system was found to have some security loopholes.

Software Written

1) A Secure Electronic Payment System (in Cgi-Perl and C++)
2) A Fully Programmable Scientific Calculation System with user defined size of numbers. Especially useful for making calculations on big numbers (e.g. 1000 digit long). An interpreter was also implemented to enable the user define her own custom functions. A GUI was also provided. (in C++)
3) Pit-game - A software to in which the user could play the "Pit-ball" game against the computer (in Java)
4) DOS based library implementing all common data structures in addition to graphics classes for making windows, menu, buttons etc. (in C++)
5) Online Course Feedback System - Currently being used at IIT Bombay for course evaluation (with Prof. Sharat Chandran, in Cgi-Perl and java)
6) E-book on machine vision – two chapters and java applets in the Machine Vision e-book project (with Prof. Sharat Chandran, in java)

Others

1) Served as the Lab Assistant for IEEE Programming Lab for 1st year students during the session 2002-2003.
2) A project contributor and a member of Comprehensive Perl Archive Network (CPAN).
3) Member of the Cryptographic Research Society of India (CRSI).
4) Co-founder of the Student Crypto Group, IT-BHU.