One Way Functions –Conjecture, Status, Applications and Future Research Scope

Amit Sharma
AMIE CSE Research Scholar
The Institution of Engineers (INDIA), India

Sunil Kr. Singh
CSE Department, CCET
Degree Wing, Chandigarh, India

ABSTRACT

The conjecture that one way function exists is an open problem, the resolution of which holds the key for the solution of many unsolved problems in mathematics and cryptography. This paper presents the introduction of one way functions from complexity & modern cryptography theory viewpoint and their significance in cryptographic applications and research. This paper presents the features and limitations of proposed candidate functions, and the implications of proof of one way functions conjecture.

Keywords

Public Key Cryptography, RSA, one way functions, Pseudorandom generators, P vs NP, Digital signatures, MAC, Authentication, Zero error proofs.

1. INTRODUCTION

In modern cryptographic systems, the intractability of one way functions, the functions which are easy to compute but hard to invert, is a fundamental prerequisite for asymmetric key encryption schemes, security protocols, integrity, identification, authentication and digital signatures. Existence of one way functions is an open conjecture, the proof of which is imperative for many intricate problems of mathematics and computer science. If one way functions exist it would imply P≠NP and thus settling the most celebrated question of our time. Its existence would also imply the existence of pseudorandom generators, pseudorandom functions, bit commitment schemes, non-trivial zero knowledge proofs and many other important cryptographic tools. Over the years, various candidate functions have been proposed as one way functions, which have withstand the rigorous cryptanalysis tests and extensive research for finding their inverse and have been successfully implemented in prevalent cryptographic applications such as RSA.

2. ONE WAY FUNCTIONS

Mathematically, a function $f: A \to B$, $y = f(x)$ is a rule or mapping that associates each element in set A (domain) to exactly one element in set B (co-domain). A function f is invertible i.e. $f^{-1}: B \to A$, $x = f^{-1}(y)$ exists if it is one-one and onto (bijective function). If f and f^{-1} are inverse of each other then $f\left(f^{-1}(x)\right) = f^{-1}\left(f(x)\right) = x$

In modern cryptography, informally a function $f: \{0,1\}^* \to \{0,1\}^*$ is a one way function if

- For a given input x, the value $y = f(x)$ can be computed by a polynomial time algorithm.
- For a given y, it is hard to find x such that $x = f^{-1}(y)$ by a probabilistic polynomial time (PPT) algorithm.

A cryptographic one way function may not be bijective.

3. STRONG ONE WAY FUNCTION

A function $f: \{0,1\}^* \to \{0,1\}^*$ is a strong one way function[1] if

- There exists a PPT algorithm that evaluates $f(x)$ on input x.
- For every PPT algorithm A, there is a negligible function ν_A such that for sufficiently large k,

$$P[f(z) \neq y : x \xleftarrow[R]{} \{0,1\}^k; y \leftarrow f(x); z \leftarrow A(1^k, y)] \geq \frac{1}{Q(k)}$$

4. WEAK ONE WAY FUNCTION

A function $f: \{0,1\}^* \to \{0,1\}^*$ is a weak one way function[1] if

- There exists a PPT algorithm that evaluates $f(x)$ on input x.
- There is a polynomial function Q such that for every PPT algorithm A, and for sufficiently large k,

$$P[f(z) \neq y : x \xleftarrow[R]{} \{0,1\}^k; y \leftarrow f(x); z \leftarrow A(1^k, y)] \geq \frac{1}{Q(k)}$$

Weak one-way functions exist if and only if strong one way functions exists[1].

5. CANDIDANTE ONE WAY FUNCTIONS

Though the conjecture that one way functions exists is still unproven yet several functions have been proposed as one way functions and many practical cryptographic applications have been developed.

5.1 Prime factorization[2]

For two given large prime numbers p and q in binary notation, the proposed function calculates its product $f(p,q) = pq$. Inverting this function would require finding prime factors for a given large integer which is very hard to compute. As the number of digits in given integer increases the time complexity of finding prime factors increases exponentially. So far, no PPT algorithm exists that can resolve prime factorization. Various encryption schemes are based on one wayness of prime factorization.

5.2 Discreet Logarithm[3]

For a prime number p and a fixed primitive element α of finite field GF(p), let $y = \alpha^x \bmod p$, for $1 \leq x \leq p\text{-}1$, then x is referred to as discrete logarithm of y to the base α, mod p: $x = \log_\alpha y \bmod p$, for $1 \leq y \leq p\text{-}1$.For this function calculation of y from x is easy but computing x from y is very hard for carefully chosen value of p. The ElGamal encryption is based on the discrete logarithmic function.

5.3 The Rabin function[4]

The modular squaring or quadratic residue based Rabin function $Rabin\colon Z_N^* \to Z_N^*$ is defined as $Rabin(x) = x^2 \bmod N$ for each $N = pq$ a product of two primes p and q. Inverting the Rabin function is equivalent to factoring N and thus hard to compute. The Rabin cryptosystem is based on this function.

5.4 Discrete root extraction[5]

The function $f(p,q,e,y)= y^e \bmod pq$ for y in Z_{pq}^* and e in Z_{pq} and relatively prime to $(p-1)(q-1)$ where p and q are primes, is commonly known as RSA encryption. Basically, RSA function is the dual of discrete logarithmic function. Without knowing p and q finding the e^{th} root is believed to be hard.

5.5 Elliptic curves[6][7]

An elliptic curve is a set of points over a finite field described by the equation $y^2 = x^3 + ax + b$ where $4a^3+27b^2 \neq 0$, along with a distinguished point at infinity. The points on the curve under point addition form a group. For a point P on the curve, it is easy to calculate another point Q = nP (point multiplication) which is n-1 times repeated addition of the point P to itself where n is an integer. The security of elliptic curve one way function depends on intractability of determining n if P and Q are known. It is known as elliptic curve discrete logarithmic problem. ECC supported by all modern browsers and most SSL/TSL certification authorities has increasingly been used in recent times.

5.6 Cryptographic hash functions[8]

Cryptographic hash functions are designed to take variable length string as input and compute a fixed length hash value which is pre-image resistant and collision resistant. For a given hash value it is hard to find the string that produces it. One way hash functions are primarily used for digital signatures, authentication and identification. A number of one way hash functions notably SHA256, SHA512 etc provide fast and practical cryptographic solutions.

5.7 Physical one way functions[9]

Physical one way functions depend on the mesoscopic physics of physical microstructures which is used compute unique identifiers in the form of fixed length string of binary digits. Such functions are difficult to clone as the random physical factors generating a microstructure are uncontrolled and unpredictable thereby making them hardware analog of one way functions.

5.8 Quantum one way functions[10]

Most of the classical one way functions are vulnerable to attack by a quantum adversary. Quantum one way functions employ quantum mechanical properties to generate quantum output state which is impossible to invert even for a quantum computer. Quantum one way functions are implemented in several quantum cryptosystems such as BB84 for quantum key distributions.

Besides these several other candidate functions such as Goldreich's one way function based on expander graphs, one way functions based on intractability of decoding random linear codes, the subset sum problem etc. have been implemented in practical cryptosystems.

6. TRAPDOOR ONE WAY FUNCTIONS

Trapdoor functions are type of one way functions having the additional property that with the knowledge of a certain unique information or secret key known as trapdoor it is easy to compute the inverse which is otherwise computationally infeasible to find. The term Trapdoor functions was coined by Diffie and Hellman in their landmark paper *New directions in cryptography*[3] for asymmetric key exchange over an insecure channel in public key encryption.

7. IMPLICATIONS OF ONE WAY FUNCTIONS

7.1 Public key cryptosystems

Traditionally, symmetric ciphers have been used for exchange of secured information in which the sender and receiver share identical key which is used for both encryption and decryption. In such systems, key exchange between the sender and receiver over an insecure public channel has always been the problem. In 1976, Diffie and Hellman[3] proposed the idea of asymmetric key exchange in which the key used for encryption (public key) is different from key used for decryption (private) key. In asymmetric key exchange, receiver generates a public key using chosen one way function and a private key using trapdoor information. Public key is then distributed over an insecure public channel and is supposed to be known to everyone including the sender as well as the adversary. Sender using the public key encrypts the message and sends it over the public channel. Theoretically, that encrypted message can be decrypted only by the private key which is exclusively known to the receiver. First practical application of public key cryptography, RSA cryptosystem [11] was invented by Rivest, Shamir and Adelman in 1977 using RSA one way function. In 1997, British government declassified GCHQ research documents which reveal that in 1970 British cryptographer James Ellis conceived the idea of non-secret cryptosystem akin to public key cryptosystem. In 1973, GCHQ mathematician Clifford Cocks implemented non-secret cryptosystem using algorithm similar to RSA algorithm. In 1974, another GCHQ mathematician Malcolm Williamson invented what is now known as Diffie-Hellman key exchange. Due to classified nature of their work, these researches were not made public until 1997. Since then, many cryptosystems with candidate one way functions have been implemented and put to practical use. While asymmetric key cryptography is more secured, it is slower than symmetric key cryptography as it uses mathematical function for encryption and decryption. Thus, for large messages, asymmetric key cryptography is used for key exchange needed for symmetric key cryptography.

7.2 Digital signature schemes

The idea of digital signature scheme[14] stems from the papers of Diffie and Hellman[3] followed by Rivest, Shamir and Adelman[11]. In 1988, Goldwasser, Shafi and Rivest[13] formalized the notion of digital signature schemes. Digital signature schemes are used for message authentication, message integrity and non-repudiation. In digital signature schemes, the sender of the communication generates a public and private key pair using one way functions. The sender using the private key and signing algorithm signs the message digest. The receiver of the communication using sender's public key and verifying algorithms verifies the message. Digital signatures are primarily used for signing the certificates such as SSL/TSL etc issued by a certificate authority.

7.3 Pseudorandom generators

A pseudorandom generator (PRG) is a deterministic function which maps the random uniform bit input to a pseudorandom longer bit string output which cannot be distinguished from a uniform random string by any polynomial time algorithm[15].

In their seminal paper Håstad, Impagliazzo, Levin and Luby[16] proved that pseudorandom generators exist if and only if one way functions exist. Pseudorandom generators are used in many cryptographic systems and complex model which are essentially based on random number generation.

7.4 Pseudorandom function family

A pseudorandom function family (PRF)[17] is a collection of polynomial time computable functions for which no efficient algorithm can distinguish between a random chosen function from the family and a random function. Existence of one way functions implies the existence of pseudorandom function family. Existence of PRG imply the existence of PRF[18]. Numerous applications[17] such as dynamic hashing, memoryless authentication schemes have been devised using PRF.

7.5 Message authentication code (MAC)

MAC is appended to the message as a cryptographic tool for message authentication and integrity. MAC algorithm takes a message and a secret key as input and create a MAC value also known as tag. The tag is verified by the receiver using the secret key for authentication and integrity[19]. MAC uses symmetric key exchanges in contrast to digital signatures which are based on asymmetric key cryptography. Cryptographic hash one way functions such as HMAC are widely used to create MACs.

7.6 Zero knowledge proofs and P vs NP[20]

In 1985, Shafi GoldwAsser, Silvio Micali and Charles Rackoff paper[21] introduced zero knowledge proof system with randomized and interactive verification procedure. Goldreich, Micali and Wigderson[22] proved if we assume the existence of one way functions, then every set in NP has a zero knowledge proof. If one way function existence is proven it would imply FP ≠ FNP, which would imply P ≠ NP. However, Razborov and Rudich[23] proved that existence of one way functions implies that there cannot be any natural proof for P vs NP.

7.7 Bit commitment schemes

Commitment scheme[24] is a two phased protocol that allows sender to commit to a specific value which he cannot alter later and is kept secret from everyone. A message called commitment is sent from the sender to the receiver which reveals no information about committed value. Later when the sender reveals the value the protocol allows receiver to verify that value is indeed the one committed. Cryptographically secure and reliable commitment schemes have been developed using one way functions and pseudorandom generators. Bit commitment schemes are used in several cryptographic protocols such as coin flipping, zero knowledge proofs and secure multiparty communication.

8. CONCLUSION

In this paper, we have presented formal and informal definitions of One way functions, listed various proposed candidate functions and their widespread uses and implications in modern cryptography. Though the intractability of One way functions has not been proved yet but many candidate functions have withered the test of crypto analysis and have been used in widespread applications. However, with increasing computational power and efficiency of machines such functions are vulnerable to attacks unless One way function conjecture is conclusively proved. Moreover, implications of existence of One way functions will have far reaching consequences not just for cryptography but for theoretical computer science and mathematics. Future research possibility in one way function could be designing an efficient one way function which makes the public key cryptography faster so that it eventually eliminates the need of private key encryption schemes. Multiparty one way functions are another possibility as the need for it is growing by the day. Another dimension could be modeling the mathematical functions with biometric information to make it more secure.

9. REFERENCES

[1] S. Goldwasser, M. Bellare, Lecture notes on cryptography, MIT press, Cambridge, Massachusetts, 2001.

[2] C. Barski, and C. Wilmer, Bitcoin for the Befuddled, No starch press, 2014.

[3] W. Diffie, and M. Hellman, New directions in cryptography, IEEE trans. on information theory 22(6), 1976.

[4] M. Kao, Encyclopedia of algorithms, Springer-Verlag, New York Inc, 2008.

[5] E. Weisstein, One-Way Function, from MathWorld- http://mathworld.wolfram.com/One-WayFunction.html

[6] N. Koblitz, Elliptic curve cryptosystems, Mathematics of computation 48.177,1987.

[7] V. Miller, Use of Elliptic Curves in Cryptography, In Advances in Cryptology (CRYPTO '85), Hugh C. Williams (Ed.). Springer-Verlag, London, 1985.

[8] P. Rogaway, and T. Shrimpton, Cryptographic hash-function basics: Definitions, implications, and separations for preimage resistance, second-preimage resistance, and collision resistance, International Workshop on Fast Software Encryption, Springer Berlin Heidelberg, 2004.

[9] R. Pappu, B. Recht, J. Taylor, N. Gershenfeld, Physical one-way functions, Science 297(5589):2026-30, 2002.

[10] I. Hiroshi, and M. Hayashi, eds. Quantum computation and information: from theory to experiment, Vol. 102 Springer Science & Business Media, 2008.

[11] R. Rivest, A. Shamir, and L. Adleman, A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, Communications of the ACM 21 (2), 1978.

[12] S. Singh, The Code Book, Doubleday, 1999.

[13] S. Goldwasser, S. Micali, and R. Rivest, A digital signature scheme secure against adaptive chosen-message attacks, SIAM Journal on Computing, 17(2), 1988.

[14] B. Forouzan, Cryptography and network security, pub. McGraw-Hill companies, ISBN-13: 978-0-07-066046-5, 2009.

[15] T. Holenstein, Pseudorandom generators from one-way functions: A simple construction for any hardness, Theory of Cryptography Conference. Springer Berlin Heidelberg, 2006.

[16] J. Håstad, R. Impagliazzo, L. Levin, and M. Luby, A pseudorandom generator from any one-way function, SIAM Journal on Computing 28(4),1999.

[17] Pseudorandom function family, from Wikipedia web. https://en.wikipedia.org/wiki/One-way_function

[18] O. Goldreich, S. Goldwasser, and S. Micali, How to construct random functions, Journal of the ACM (JACM) 33.4, 1986.

[19] M. Bellare, R. Canetti, and H. Krawczyk, Keying hash functions for message authentication, Annual International Cryptology Conference,Springer Berlin Heidelberg, 1996.

[20] A. Sharma and S. Singh, P vs NP Solution – Advances in Computational Complexity, Status and Future Scope, to be published, 2016.

[21] S. Goldwasser, S. Micali, and C. Rackoff. The Knowledge complexity of interactive proof-systems. Proceedings of 17th ACM Symposium on the Theory of Computation, Providence, Rhode Island. 1985.

[22] O. Goldreich, M. Silvio, and A. Wigderson, Proofs that yield nothing but their validity, Journal of the ACM. 38 (3), 1991.

[23] A. A. Razborov and S. Rudich, Natural proofs, Journal of Computer and System Sciences. 55, 1997