Random oracle

In cryptography, a **random oracle** is an oracle (a theoretical black box) that responds to every *unique query* with a (truly) random response chosen uniformly from its output domain. If a query is repeated, it responds the same way every time that query is submitted.

Stated differently, a random oracle is a mathematical function chosen uniformly at random, that is, a function mapping each possible query to a (fixed) random response from its output domain.

Random oracles as a mathematical abstraction were first used in rigorous cryptographic proofs in the 1993 publication by Mihir Bellare and Phillip Rogaway (1993).[1] They are typically used when the proof cannot be carried out using weaker assumptions on the cryptographic hash function. A system that is proven secure when every hash function is replaced by a random oracle is described as being secure in the **random oracle model**, as opposed to secure in the standard model of cryptography.

Contents

Applications

Random oracles are typically used as an idealised replacement for cryptographic hash functions in schemes where strong randomness assumptions are needed of the hash function's output. Such a proof often shows that a system or a protocol is secure by showing that an attacker must require impossible behavior from the oracle, or solve some mathematical problem believed hard in order to break it. However, it only proves such properties in the random oracle model, making sure no major design flaws are present. It is in general not true that such a proof implies the same properties in the standard model. Still, a proof in the random oracle model is considered better than no formal security proof at all.[2]

Not all uses of cryptographic hash functions require random oracles: schemes that require only one or more properties having a definition in the standard model (such as collision resistance, preimage resistance, second preimage resistance, etc.) can often be proven secure in the standard model (e.g., the Cramer–Shoup cryptosystem).

Random oracles have long been considered in computational complexity theory,[3] and many schemes have been proven secure in the random oracle model, for example Optimal Asymmetric Encryption Padding, RSA-FDH and Probabilistic Signature Scheme. In 1986, Amos Fiat and Adi Shamir[4] showed a major application of random oracles – the removal of interaction from protocols for the creation of signatures.

In 1989, Russell Impagliazzo and Steven Rudich[5] showed the limitation of random oracles – namely that their existence alone is not sufficient for secret-key exchange.

In 1993, Mihir Bellare and Phillip Rogaway[1] were the first to advocate their use in cryptographic constructions. In their definition, the random oracle produces a bit-string of infinite length which can be truncated to the length desired.

When a random oracle is used within a security proof, it is made available to all players, including the adversary or adversaries. A single oracle may be treated as multiple oracles by pre-pending a fixed bit-string to the beginning of each query (e.g., queries formatted as "1|x" or "0|x" can be considered as calls to two separate random oracles, similarly "00|x", "01|x", "10|x" and "11|x" can be used to represent calls to four separate random oracles).

Limitations

According to the Church–Turing thesis, no function computable by a finite algorithm can implement a true random oracle (which by definition requires an infinite description because it has infinitely many possible inputs, and its outputs are all independent from each other and need to be individually specified by any description).

In fact, certain artificial signature and encryption schemes are known which are proven secure in the random oracle model, but which are trivially insecure when any real function is substituted for the random oracle.[6][7] Nonetheless, for any more natural protocol a proof of security in the random oracle model gives very strong evidence of the *practical* security of the protocol.[8]

In general, if a protocol is proven secure, attacks to that protocol must either be outside what was proven, or break one of the assumptions in the proof; for instance if the proof relies on the hardness of integer factorization, to break this assumption one must discover a fast integer factorization algorithm. Instead, to break the random oracle assumption, one must discover some unknown and undesirable property of the actual hash function; for good hash functions where such properties are believed unlikely, the considered protocol can be considered secure.

Random Oracle Hypothesis

Although the Baker–Gill–Solovay theorem[9] showed that there exists an oracle A such that $P^A = NP^A$, subsequent work by Bennett and Gill,[10] showed that for a *random oracle* B (a function from $\{0,1\}^n$ to $\{0,1\}$ such that each input element maps to each of 0 or 1 with probability 1/2, independently of the mapping of all other inputs), $P^B \subsetneq NP^B$ with probability 1. Similar separations, as well as the fact that random oracles separate classes with probability 0 or 1 (as a consequence of the Kolmogorov's zero–one law), led to the creation of the **Random Oracle Hypothesis**, that two "acceptable" complexity classes C_1 and C_2 are equal if and only if they are equal (with probability 1) under a random oracle (the acceptability of a complexity class is defined in BG81[10]). This hypothesis was later shown to be false, as the two acceptable complexity classes IP and PSPACE were shown to be equal[11] despite $IP^A \subsetneq PSPACE^A$ for a random oracle A with probability 1.[12]

Ideal cipher

An *ideal* cipher is a random permutation oracle that is used to model an idealized block cipher. A random permutation decrypts each ciphertext block into one and only one plaintext block and vice versa, so there is a one-to-one correspondence. Some cryptographic proofs make not only the "forward" permutation available to

all players, but also the "reverse" permutation.

Recent works showed that an ideal cipher can be constructed from a random oracle using 10-round[13] or even 8-round[14] Feistel networks.

Quantum-accessible Random Oracles

Post-quantum cryptography studies quantum attacks on classical cryptographic schemes. As a random oracle is an abstraction of a hash function, it makes sense to assume that a quantum attacker can access the random oracle in quantum superposition.[15] Many of the classical security proofs break down in that quantum random oracle model and need to be revised.

See also

- Sponge function
- Oracle machine
- Topics in cryptography

References

1. Bellare, Mihir; Rogaway, Phillip (1993). "Random Oracles are Practical: A Paradigm for Designing Efficient Protocols" (http://www.cs.ucsd.edu/users/mihir/papers/ro.html). *ACM Conference on Computer and Communications Security*: 62–73.
2. Katz, Jonathan; Lindell, Yehuda (2015). *Introduction to Modern Cryptography* (2 ed.). Boca Raton: Chapman & Hall/CRC. pp. 174–175, 179–181. ISBN 978-1-4665-7027-6.
3. Bennett, Charles H.; Gill, John (1981), "Relative to a Random Oracle A, P^A != NP^A != co-NP^A with Probability 1", *SIAM Journal on Computing*, **10** (1): 96–113, doi:10.1137/0210008 (https://doi.org/10.1137%2F0210008), ISSN 1095-7111 (https://www.worldcat.org/issn/1095-7111)
4. Fiat, Amos; Shamir, Adi (1986). "How to Prove Yourself: Practical Solutions to Identification and Signature Problems". *CRYPTO*. pp. 186–194.
5. Impagliazzo, Russell; Rudich, Steven (1989). "Limits on the Provable Consequences of One-Way Permutations". *STOC*: 44–61.
6. Ran Canetti, Oded Goldreich and Shai Halevi, The Random Oracle Methodology Revisited, STOC 1998, pp. 209–218 (PS and PDF) (https://arxiv.org/abs/cs.CR/0010019).
7. Craig Gentry and Zulfikar Ramzan. "Eliminating Random Permutation Oracles in the Even-Mansour Cipher" (https://www.iacr.org/cryptodb/archive/2004/ASIACRYPT/218/218.pdf). 2004.
8. Koblitz, Neal; Menezes, Alfred J. (2015). "The Random Oracle Model: A Twenty-Year Retrospective" (http://cacr.uwaterloo.ca/~ajmeneze/anotherlook/papers/rom.pdf) (PDF). *Another Look*. Retrieved 6 March 2015.
9. Baker, Theodore; Gill, John; Solovay, Robert (1975). "Relativizations of the P =? NP Question". *SIAM J. Comput*. SIAM. **4** (4): 431–442. doi:10.1137/0204037 (https://doi.org/10.1137%2F0204037).
10. Bennett, Charles; Gill, John (1981). "Relative to a Random Oracle A, P != NP != co-NP with Probability 1". *SIAM J. Comput*. SIAM. **10** (1): 96–113. doi:10.1137/0210008 (https://doi.org/10.1137%2F0210008).
11. Shamir, Adi (October 1992). "IP = PSPACE" (http://portal.acm.org/citation.cfm?doid=146585.146609). *Journal of the ACM*. **39** (4): 869–877. doi:10.1145/146585.146609 (https://doi.org/10.1145%2F146585.146609). S2CID 315182 (https://api.semanticscholar.org/CorpusID:315182).

12. Chang, Richard; Oded Goldreich, Benny Chor; Hartmanis, Juris; Hastad, Johan; Ranjan, Desh; Rohatgi, Pankaj (August 1994). "The Random Oracle Hypothesis is False" (http://citeseer.ist.psu.edu/282397.html). *Journal of Computer and System Sciences*. **49** (1): 24–39. doi:10.1016/S0022-0000(05)80084-4 (https://doi.org/10.1016%2FS0022-0000%2805%2980084-4). ISSN 0022-0000 (https://www.worldcat.org/issn/0022-0000).
13. Dachman-Soled, Dana; Katz, Jonathan; Thiruvengadam, Aishwarya (2016). "10-Round Feistel is Indifferentiable from an Ideal Cipher". *EUROCRYPT 2016*. Springer. pp. 649–678. doi:10.1007/978-3-662-49896-5_23 (https://doi.org/10.1007%2F978-3-662-49896-5_23).
14. Dai, Yuanxi; Steinberger, John (2016). "Indifferentiability of 8-Round Feistel Networks". *CRYPTO 2016*. Springer.
15. Dan Boneh, Özgür Dagdelen, Marc Fischlin, Anja Lehmann, Christian Schaffner, and Mark Zhandry (2011). *Random oracles in a quantum world*. Springer. pp. 41–69. arXiv:1008.0931 (https://arxiv.org/abs/1008.0931). doi:10.1007/978-3-642-25385-0_3 (https://doi.org/10.1007%2F978-3-642-25385-0_3).
