The rise and fall of the Random Oracle Methodology

Victor Glazer

October 28, 2004

Timeline

- **1984:** Shafi Goldwasser, Silvio Micali and Ron Rivest describe in [GMR84] (see [GMR88] for the journal version) the first signature scheme which is provably secure against adaptive chosen message attack under plausible complexity-theoretic assumptions. The specific assumption required is that *claw-free* trapdoor permutations exist, which is the case if factoring is hard. Note, however, that claw-free trapdoor permutations may fail to exist even if ordinary permutations (ones not based on the difficulty of integer factorization, that is) do. Unfortunately, GMR's "signature tree" construction is too inefficient to be practical.

- **1987:** Amos Fiat and Adi Shamir construct a practical signature scheme in [FS87] by removing the interaction from a canonical (i.e. three-round, public-coin) identification scheme using a cryptographic hash function. They show that the resulting signature scheme is secure against chosen message attack if factoring is hard (which implies that the underlying identification scheme is secure), *assuming that the hash function in question is truly random.* This approach to designing signature schemes later becomes known as the "Fiat-Shamir paradigm".

  Merkle proposes a tree-like signature scheme based on one-way functions in [Mer88], but does not provide a rigorous proof of security.

- **1988:** Mihir Bellare and Silvio Micali present a signature scheme based on trapdoor permutations which is secure if the underlying permutation is one-way.

- **1989:** Moni Naor and Moti Yung show in [NY89] how to construct secure signature schemes from weakly collision-resistant hash functinos, and describe how to obtain such hash functions from one-way permutations (actually, injective one-way functions, which need not be onto). Their construction is still "tree-like", stateful and inefficient.

- **1991:** Charlie Rackoff and Dan Simon present the first public-key encryption scheme secure against adaptive chosen ciphertext attack (i.e. CCA2-secure) in [RS92]. Danny Dolev, Cynthia Dwork and Moni Naor independently develop another CCA2-secure encryption scheme in [DDN91] (see [DDN00] for the journal version). However, both constructions are based on [BFM88]'s noninteractive zero-knowledge proofs of knowledge and therefore aren't practical.

- **1992:** Tatsuaki Okamoto develops in [Oka93] a canonical identification scheme which is provably secure if discrete log is hard, with a view towards converting it into a practical signature scheme as per the Fiat-Shamir paradigm.

- **1993:** Based on ideas from [FS87], Mihir Bellare and Phillip Rogaway propose in [BR93] a new approach to designing practical public-key signature and encryption schemes, which later becomes known as the "Random Oracle Methodology". In particular, they exhibit a public-key encryption scheme and a "hash-and-sign" signature scheme which are secure (against adaptive chosen-ciphertext and chosen-message attacks, respectively) assuming that the hash functions involved are "ideal", i.e. truly random.

- **1994:** Bellare and Rogaway propose a template for practical (i.e. efficient) public-key encryption schemes in [BR94], called Optimal Assymetric Encryption Padding or OAEP, which they claim yields PKEPs CCA2-secure in the random oracle model if instantiated using a one-way trapdoor permutation. OAEP-RSA, an instantiation of OAEP where RSA is the underlying trapdoor permutation, is later incorporated into version 2.1 of RSA Security's PKCS#1 cryptography standard, as well as IEEE's P1363-2000 public-key cryptography standard.

  Cynthia Dwork and Moni Naor present a provably secure practical signature scheme in [DN94].

- **1996:** Damgård and Cramer practical signature scheme RSA provably secure under RSA assumption (which one?) [Cr96].

- **1997:** Ran Canetti initiates program to develop hash functions which can implement random oracles under certain circumstances in [Can97].

  Bellare and Rogaway submit a tech report on OAEP-type constructions to the P1363 standard committee. Charlie thinks their Diffie-Hellman construction might be wrong.

- **1998:** Ran Cenetti, Daniele Micciancio and Omer Reingold refine some of the definitions of [Can97] in [CMR98]

  Ronald Cramer and Victor Shoup develop a practical public-key encryption scheme which is CCA2 secure (in the standard model) if the decisional Diffie-Hellman problem is hard in [CS98]. Their scheme is only slightly less efficient than RSA-OAEP.

  Ran Canetti, Oded Goldreich and Shai Halevi exhibit "uninstantiable" public key encryption and signature schemes in [CGH98]. That is, they construct public-key encryption and signature schemes which are secure in the random oracle model, yet insecure in the standard model *no matter what hash function ensemble is used to implement the random oracle*. However, both schemes use Silvio Micali's CS proofs ([Mic00]) and are rather contrived and unrealistic.

- **1999:** Cramer and Shoup signature scheme, secure under the "strong RSA assumption" [CS99]. A different signature scheme provably secure under the same assumption independently discovered by Gennaro, Halevi and Rabin [GHR99].

- **2001:**

- **2003:** Shafi Goldwasser and Yael Tauman Kalai show in [GK03] that there exist uninstantiable Fiat-Shamir signature schemes. They exhibit three contrived canonical identification schemes, one of which must be secure yet yield insecure signature schemes, no matter what hash function is used to eliminate the verifier's random move. Unfortunately, their proof has a somewhat nonconstructive flavour and their construction, which uses universal arguments ([BG02]) and tree committments ([Mer90]), is highly unrealistic.

In the beginning

Signature Schemes

In the late 80s, cryptographers agree that the "right" definition of security for signature schemes is "security against adaptive chosen-message attack". Several "tree-like" schemes that provably satisfy this strong requirement (under standard assumptions) are proposed, but they are inefficient and hence impractical. On the other hand, the widely-used "hash-and-invert" approach can't be proven secure under standard assumptions about hash functions (i.e. collision-resistance).

Fiat and Shamir develop a signature scheme (involving a hash function) which is provably secure if factoring is hard, assuming that the hash function is truly random. Although hash functions obviously *aren't* truly random (because they have short descriptions), the scheme is very efficient.

Public-key Encryption Schemes

In the early 90s, cryptographers agree that the "right" definition of security for public-key encryption schemes is "securiy against adaptive chosen-ciphertext attack" or, equivalently, "non-malleability". Schemes that provably satisfy this strong requirement (under standard assumptions) are proposed, but they use "noninteractive zero knowledge proofs of knowledge" and are too inefficient to be practical.

The Random Oracle Methodology is born

The state of affairs in the early nineties is as follows: provably secure constructions are inefficient, whereas practical ones lack proofs of security. Bellare and Rogaway suggest a compromise: schemes (involving hash functions) which are efficient, yet secure only if the underlying hash functions

The ROM outlives its usefulness

We now have efficient signature schemes which are provably secure under standard assumptions (both factoring and discrete log). We also have an efficient public-key encryption scheme (Cramer-Shoup) which is provably secure if discrete log is hard. Unfortunately, we *don't* have one which is secure assuming factoring is hard (i.e. one based on RSA or the Rabin function). This matters because discrete log may turn out to be easy. We also have RSA-OAEP, which is twice as fast (?) as Cramer-Shoup and ROM-secure under the standard RSA assumption.

Micali's computationally sound (CS) proofs are a nice tool widely used in theoretical cryptography, but they are only known to work in the random oracle model. Can we "instantiate" the oracle somehow, without losing the crucial "proof-of-knowledge" property?

References

[BFM88] Manuel Blum, Paul Feldman, and Silvio Micali. Non-interactive zero-knowledge and its applications. In *Proceedings of the twentieth annual ACM symposium on Theory of computing—STOC '88*, pages 103–112. ACM Press, 1988.

[BG02] Boaz Barak and Oded Goldreich. Universal arguments and their applications. In *Proceedings of the 17th IEEE Annual Conference on Computational Complexity—CCC '02*, pages 162–171. IEEE Computer Society, 2002.

[BR93] Mihir Bellare and Phillip Rogaway. Random oracles are practical: a paradigm for designing efficient protocols. In *Proceedings of the 1st ACM conference on Computer and communications security—CCS '93*, pages 62–73. ACM Press, 1993.

[BR94] Mihir Bellare and Phillip Rogaway. Optimal assymetric encryption. In *Proceedings of Advances in Cryptology—EUROCRYPT '94, Workshop on the Theory and Application of Cryptographic Techniques*, volume 950 of *Lecture Notes in Computer Science*, pages 92–111. Springer-Verlag, 1994.

[Can97] Ran Canetti. Towards realizing random oracles: Hash functions that hide all partial information. In *Proceedings of Advances in cryptology—CRYPTO '97*, volume 1294 of *Lecture Notes in Computer Science*, pages 455–469. Springer-Verlag, 1997.

[CGH98] Ran Canetti, Oded Goldreich, and Shai Halevi. The random oracle methodology, revisited (preliminary version). In *Proceedings of the thirtieth annual ACM symposium on Theory of computing—STOC '98*, pages 209–218. ACM Press, 1998.

[CMR98] Ran Canetti, Daniele Micciancio, and Omer Reingold. Perfectly one-way probabilistic hash functions (preliminary version). In *Proceedings of the thirtieth annual ACM symposium on Theory of computing—STOC '98*, pages 131–140. ACM Press, 1998.

[Cr96] Ronald Cramer and Ivan Damgård. New generation of secure and practical rsa-based signatures. In *Proceedings of the 16th Annual International Cryptology Conference on Advances in Cryptology—CRYPTO '96*, pages 173–185. Springer-Verlag, 1996.

[CS98] Ronald Cramer and Victor Shoup. A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. In *Proceedings of the 18th Annual International Cryptology Conference on Advances in Cryptology—CRYPTO '98*, volume 1462 of *Lecture Notes in Computer Science*, pages 13–25. Springer-Verlag, 1998.

[CS99] Ronald Cramer and Victor Shoup. Signature schemes based on the strong rsa assumption. In *Proceedings of the 6th ACM conference on Computer and communications security—CSS '99*, pages 46–51. ACM Press, 1999.

[DDN91] Danny Dolev, Cynthia Dwork, and Moni Naor. Non-malleable cryptography. In *Proceedings of the twenty-third annual ACM symposium on Theory of computing—STOC '91*, pages 542–552. ACM Press, 1991.

[DDN00] Danny Dolev, Cynthia Dwork, and Moni Naor. Nonmalleable cryptography. *SIAM J. Comput.*, 30(2):391–437, 2000.

[DN94] Cynthia Dwork and Moni Naor. An efficient existentially unforgeable signature scheme and its applications. In *Proceedings of the 14th Annual International Cryptology Conference on Advances in Cryptology—CRYPTO '94*, pages 234–246. Springer-Verlag, 1994.

[FS87] Amos Fiat and Adi Shamir. How to prove yourself: practical solutions to identification and signature problems. In *Proceedings of Advances in cryptology—CRYPTO '86*, volume 263 of *Lecture Notes in Computer Science*, pages 186–194. Springer-Verlag, 1987.

[GHR99] Rosario Gennaro, Shai Halevi, and Tal Rabin. Secure hash-and-sign signatures without the random oracle. In *Proceedings of Advances in Cryptology—EUROCRYPT'99: International Conference on the Theory and Application of Cryptographic Techniques*, volume 1592 of *Lecture Notes in Computer Science*, pages 123–139. Springer-Verlag, 1999.

[GK03] Shafi Goldwasser and Yael Tauman Kalai. On the (in)security of the fiat-shamir paradigm. In *Proceedings of the 44th Annual IEEE Symposium on Foundations of Computer Science—FOCS '03*, pages 102–113. IEEE Computer Society, 2003.

[GMR84] Shafi Goldwasser, Silvio Micali, and Ron L. Rivest. A paradoxical solution to the signature problem. In *Proceedings of the 25th Annual Symposium on Foundations of Computer Science—FOCS'84*, pages 441–449. IEEE Computer Society, 1984.

[GMR88] Shafi Goldwasser, Silvio Micali, and Ron L. Rivest. A digital signature scheme secure against adaptive chosen-message attacks. *SIAM Journal on Computing*, 17(2):281–308, 1988.

[Mer88] Ralph C. Merkle. A digital signature based on a conventional encryption function. In *A Conference on the Theory and Applications of Cryptographic Techniques on Advances in Cryptology—CRYPTO '87*, volume 293, pages 369–378. Springer-Verlag, 1988.

[Mer90] Ralph C. Merkle. A certified digital signature: That antique paper from 1979. In *Proceedings of Advances in Cryptology—CRYPTO '89, 9th Annual International Cryptology Conference*, volume 435 of *Lecture Notes in Computer Science*, pages 218–238. Springer-Verlag, 1990.

[Mic00] Silvio Micali. Computationally sound proofs. *SIAM J. Comput.*, 30(4):1253–1298, 2000.

[NY89] M. Naor and M. Yung. Universal one-way hash functions and their cryptographic applications. In *Proceedings of the twenty-first annual ACM symposium on Theory of computing—STOC '89*, pages 33–43. ACM Press, 1989.

[Oka93] Tatsuaki Okamoto. Provably secure and practical identification schemes and corresponding signature schemes. In *Proceedings of the 12th Annual International Cryptology Conference on Advances in Cryptology—CRYPTO '92*, pages 31–53. Springer-Verlag, 1993.

[RS92] Charles Rackoff and Daniel R. Simon. Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack. In *Proceedings of the 11th Annual International Cryptology Conference on Advances in Cryptology—CRYPTO '91*, pages 433–444. Springer-Verlag, 1992.