Commitment

Claude Crépeau *

1 Commitment [B]

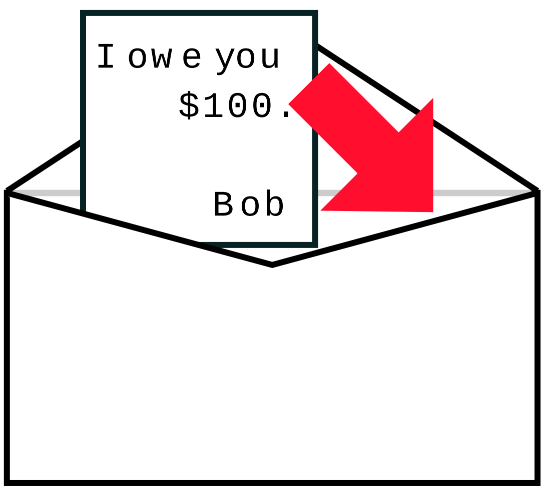
A commitment scheme is a two-phase cryptographic protocol between two parties, a sender and a receiver, satisfying the following constraints. At the end of the Commit phase the sender is committed to a specific value (often a single bit) that he cannot change later on (Commitments are binding) and the receiver should have no information about the committed value, other than what he already knew before the protocol (Commitments are concealing). In the Unveil phase, the sender sends extra information to the receiver that allows him to determine the value that was concealed by the commitment. Bit commitments are important components of zero-knowledge protocols [GMW91, BCC88], and other more general two-party cryptographic protocols [Kil88].

A natural intuitive implementation of a commitment is performed using an envelope (see Figure 1). Some information written on a piece of paper may be committed to by sealing it inside an envelope. The value inside the sealed envelope cannot be guessed (envelopes are concealing) without modifying the envelope (opening it) nor the content may be modified (envelopes are binding).

Unveiling the content of the envelope is achieved by opening it and extracting the piece of paper inside (see Figure 2).

The terminology of commitments, influenced by the legal vocabulary, first appeared in the contract signing protocols of Shimon Even [Eve82], although it seems fair to attribute the concept to Manuel Blum [Blu82] who implicitly uses it for coin flipping around the same time. In his Crypto 81 paper, Even refers to Blums contribution saying: In the summer of 1980, in a conversation, M. Blum suggested the use of randomization for such protocols. So apparently Blum introduced the idea of using random hard problems to commit to something (coin, contract, etc). However, one can also argue that the earlier work of Shamir, Rivest and Adleman [SRA81] on mental poker implicitly used commitments as well, since in order to generate a fair deal of cards, Alice encrypts the card names under her own encryption key, which is the basic idea for implementing commitments.

Under such computational assumptions, commitments come in two dual flavours : binding but computationally concealing commitments and concealing but computationally binding commitments.



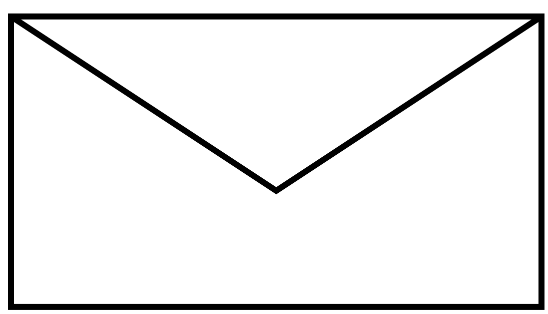


Figure 1: Committing with an envelope.

* School of Computer Science, McGill University, Montréal (Qc), Canada H3A 2A7. e-mail: crepeau@cs.mcgill.ca.

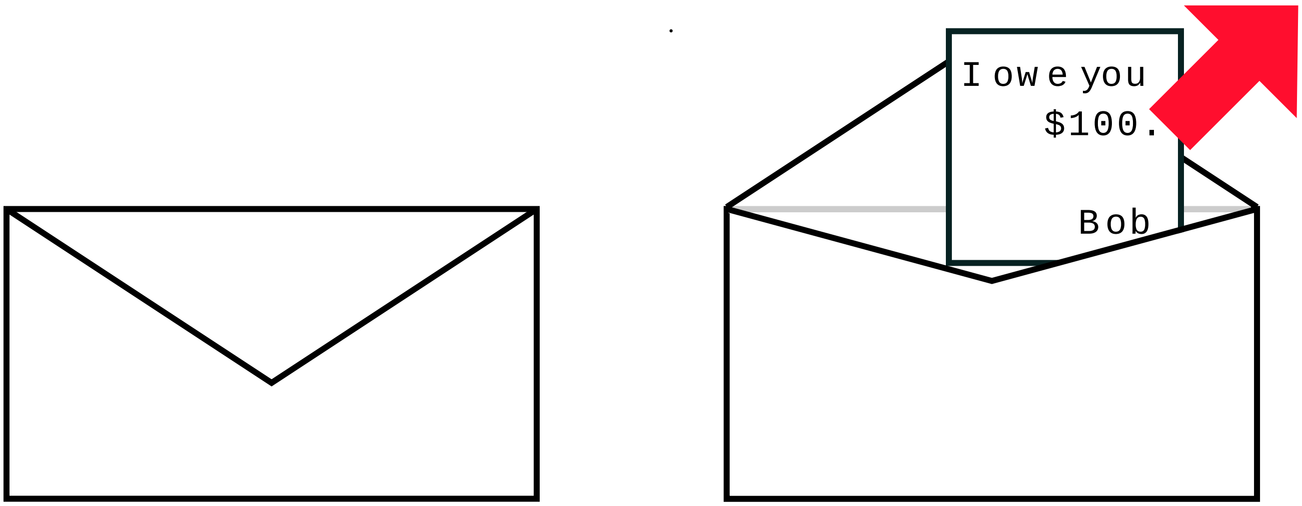


Figure 2: Unveiling from an envelope.

Commitments of the first type may be achieved from any one-way function [Nao91, HILL98] while those of the second type may be achieved from any one-way permutation (or at least regular one-way function) [NOVY93] or any collision-free hash function [HM96] (see also collision resistance and hash function). It is still an open problem to achieve commitments of the second type from one-way functions only.

A simple example of a bit commitment of the first type is obtained using the Goldwasser-Micali probabilistic encryption scheme with ones own pair of public keys (n, q) such that n is an RSA modulus and q a random quadratic non-residue modulo n with Jacobi symbol +1. Unveiling is achieved by providing a square root of each quadratic residue and of quadratic non-residue multiplied by q. A similar example of a bit commitment of the second type is constructed from someone elses pair of public keys (n, r) such that n is an RSA modulus and r a random quadratic residue modulo n. A zero bit is committed using a random quadratic residue mod n while a one bit is committed using a random quadratic residue multiplied by r modulo n. Unveiling is achieved by providing a square root of quadratic residues committing to a zero and of quadratic residues multiplied by r used to commit to a one.

Unconditionally binding and concealing commitments can also be obtained under the assumption of the existence of a binary symmetric channel [Cré97] and under the assumption that the receiver owns a bounded amount of memory [CCM98]. In multiparty scenarios [GMW91, BOGW88, CCD88], commitments are usually achieved through Verifiable Secret Sharing Schemes [CGMA85]. However, the two-prover case [BOGKW88] does not require the verifiable property because the provers are physically isolated from each other during the life span of the commitments.

In a quantum computation model it was first believed that commitment schemes could be implemented with unconditional security for both parties [BCJL93] but it was later demonstrated that if the sender is equipped with a quantum computer, then any unconditionally concealing commitment cannot be binding [May97, LH97].

Commitments exist with various extra properties: chameleon/trapdoor commitments [BCC88, FS89], commitments with equality (attributed to Bennett and Rudich in [Kil92, CGT95]), non-malleable commitments [DDN91] (with respect to unveiling [CIO98]), mutually independent commitments [LLM^{+}01], universally composable commitments [CF01].

References

[BCC88] G. Brassard, D. Chaum, and C. Crépeau. Minimum disclosure proofs of knowledge. *JCSS*, 37:156–189, 1988.

[BCJL93] G. Brassard, C. Crépeau, R. Jozsa, and D. Langlois. A quantum bit commitment scheme provably unbreakable by both parties. In 29^{th} *Symp. on Found. of Computer Sci.*, pages 42–52. IEEE, 1993.

[Blu82] M. Blum. Coin flipping by telephone. In Allen Gersho, editor, *Advances in Cryptography*, pages 11–15, Santa Barbara, California, USA, 1982. University of California, Santa Barbara.

[BOGKW88] M. Ben-Or, S. Goldwasser, J. Kilian, and A. Wigderson. Multi-prover interactiev proofs: How to remove intractability assumptions. In *Proceedings of 20th Annual*

AMC Symposium on Theory of Computing 1988, pages 113–122, 1988.

[BOGW88] M. Ben-Or, S. Goldwasser, and A. Wigderson. Completeness theorems for fault-tolerant distributed computing. In *Proc. 20th ACM Symposium on Theory of Computing*, pages 1–10, Chicago, 1988. ACM.

[CCD88] D. Chaum, C. Crépeau, and I. Damgård. Multi-party unconditionally secure protocols. In *Proc. 20th ACM Symposium on Theory of Computing*, Chicago, 1988. ACM.

[CCM98] C. Cachin, C. Crépeau, and J. Marcil. Oblivious transfer with a memory-bounded receiver. In IEEE, editor, *39th Annual Symposium on Foundations of Computer Science: proceedings: November 8–11, 1998, Palo Alto, California*, pages 493–502. IEEE Computer Society Press, 1998.

[CF01] Ran Canetti and Marc Fischlin. Universally composable commitments. In Joe Kilian, editor, *Advances in Cryptology – CRYPTO ' 2001*, volume 2139 of *Lecture Notes in Computer Science*, pages 19–40. International Association for Cryptologic Research, Springer-Verlag, Berlin Germany, 2001.

[CGMA85] Benny Chor, Shafi Goldwasser, Silvio Micali, and Baruch Awerbuch. Verifiable secret sharing and achieving simultaneity in the presence of faults (extended abstract). In *Proc. of 26th FOCS*, pages 383–395, Portland, Oregon, 21–23 October 1985. IEEE.

[CGT95] C. Crépeau, J. van de Graaf, and A. Tapp. Committed oblivious transfer and private multi-party computation. In Don Coppersmith, editor, *Advances in Cryptology - Crypto '95*, pages 110–123, Berlin, 1995. Springer-Verlag. Lecture Notes in Computer Science Volume 963.

[CIO98] Giovanni Di Crescenzo, Yuval Ishai, and Rafail Ostrovsky. Non-interactive and non-malleable commitment. In *30th Symposium on the Theory Of Computing*, pages 141–150, 1998.

[Cré97] C. Crépeau. Efficient cryptographic protocols based on noisy channels. In Walter Fumy, editor, *Advances in Cryptology - EuroCrypt '97*, pages 306–317, Berlin, 1997. Springer-Verlag. Lecture Notes in Computer Science Volume 1233.

[DDN91] D. Dolev, C. Dwork, and M. Naor. Non-malleable cryptography. In ACM, editor, *Proceedings of the twenty third annual ACM Symposium on Theory of Computing, New Orleans, Louisiana, May 6–8, 1991*, 1109 Spring Street, Suite 300, Silver Spring, MD 20910, USA, 1991. IEEE Computer Society Press. Full version available from authors.

[Eve82] S. Even. Protocol for signing contracts. In Allen Gersho, editor, *Advances in Cryptography*, pages 148–153, Santa Barbara, California, USA, 1982. University of California, Santa Barbara.

[FS89] U. Feige and A. Shamir. Zero knowledge proofs of knowledge in two rounds. In Gilles Brassard, editor, *Advances in Cryptology - Crypto '89*, pages 526–544, Berlin, 1989. Springer-Verlag. Lecture Notes in Computer Science Volume 435.

[GMW91] Oded Goldreich, Silvio Micali, and Avi Wigderson. Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proof systems. *Journal of the Association for Computing Machinery*, 38(3):691–729, July 1991.

[HILL98] Hastad, Impagliazzo, Levin, and Luby. A pseudorandom generator from any one-way function. *SICOMP: SIAM Journal on Computing*, 28, 1998.

[HM96] S. Halevi and S. Micali. Practical and provably-secure commitment schemes from collision-free hashing. In Neal Koblitz, editor, *Advances in Cryptology - Crypto '96*, pages 201–215, Berlin, 1996. Springer-Verlag. Lecture Notes in Computer Science Volume 1109.

[Kil88] J. Kilian. Founding cryptography on oblivious transfer. In *Proc. 20th ACM Symposium on Theory of Computing*, pages 20–31, Chicago, 1988. ACM.

[Kil92] Joe Kilian. A note on efficient zero-knowledge proofs and arguments (extended abstract). In *Proceedings of the Twenty-Fourth Annual ACM Symposium on the Theory of Computing*, pages 723–732, Victoria, British Columbia, Canada, 4–6 May 1992.

[LH97] H.-K. Lo and F. Chau H.˙ Is quantum bit commitment really possible. *Physical Review Letters*, 78(17):3410–3413, April 1997.

[LLM+01] Moses Liskov, Anna Lysyanskaya, Silvio Micali, Leonid Reyzin, and Adam Smith. Mutually independent commitments. *Lecture Notes in Computer Science*, 2248:385–??, 2001.

[May97] Dominic Mayers. Unconditionally secure quantum bit commitment is impossible. *Physical Review Letters*, 78(17):3414–3417, April 1997.

[Nao91] Moni Naor. Bit commitment using pseudorandomness. *Journal of Cryptology*, 4(2):151–158, 1991.

[NOVY93] M. Naor, R. Ostrovsky, R. Venkatesan, and M. Yung. Perfect zero-knowledge arguments for NP can be based on general complexity assumptions. In *Advances in Cryptology: Proceedings of Crypto '92*, Lecture Notes on Computer Science. Springer-Verlag, 1993. to appear. This work was first presented at the DIMACS workshop on cryptography, October 1990.

[SRA81] A. Shamir, R. L. Rivest, and L. M. Adleman. Mental poker. In D. Klarner, editor, *The Mathematical Gardner*, pages 37–43. Wadsworth, Belmont, California, 1981.