The Bare Bounded-Storage Model: The Tight Bound on the Storage Requirement for Key Agreement

Stefan Dziembowski and Ueli Maurer, *Fellow, IEEE*

***Abstract*—In the bounded-storage model (BSM) for information-theoretically secure encryption and key-agreement one makes use of a random string R whose length t is greater than the assumed bound s on the adversary Eve's storage capacity. The legitimate parties, Alice and Bob, execute a protocol, over an authenticated channel accessible to Eve, to generate a secret key K about which Eve has essentially no information even if she has infinite computing power. The string R is either assumed to be accessible to all parties or communicated publicly from Alice to Bob. While in the BSM one often assumes that Alice and Bob initially share a short secret key, and the goal of the protocol is to generate a much longer key, we consider in this paper the *bare* BSM without any initially shared secret key. It is proved that in the bare BSM, secret key agreement is impossible unless Alice and Bob have themselves very high storage capacity, namely $O(\sqrt{t})$. This proves the optimality of a scheme proposed by Cachin and Maurer.**

***Index Terms*—cryptography, information-theoretic security, bounded-storage model, key agreement, lower bounds**

I. Introduction

The bounded-storage model, proposed initially by Maurer in 1992 [15], [16], is an approach to achieving provable security of cryptographic schemes even against an adversary with unlimited computational resources. This is called unconditional or information-theoretic security. The only assumption is that the adversary's storage capacity is bounded, say by s bits, where s can be very large. No computational hardness assumption, like the hardness of factoring large integers, is needed. The basic idea is to assume that a random t-bit string R is either temporarily available to the public (e.g. the signal of a deep space radio source) or broadcast by a satellite or by one of the legitimate parties. If $s < t$, then the adversary, called Eve, can store only partial information about R, but she is allowed to apply an arbitrary function $f : \{0,1\}^t \to \{0,1\}^s$ to R in order to compute the value she stores. No assumption about the feasibility of computing f is made.

The legitimate parties, called Alice and Bob, can each access a small fraction of the string R and execute a protocol, over an authenticated channel accessible to Eve, to generate a secret key K about which Eve has essentially no information, even if she has infinite computing power, and no matter which function f she applied. In the BSM one usually assumes that Alice and Bob initially share a short secret key that determines which bits of R they need to access and how they combine the accessed bits to result in the secret key K. In this model, which we call the standard BSM, the goal of a key-agreement protocol is that the derived key K is much longer than the initial key; in other words, the goal is key expansion rather than key generation. A long sequence of papers on key expansion [16], [2], [1], [9], [10], [12], [14], [19] has led from partial security proofs (for special adversary strategies) to complete security proofs, and to the understanding that a scheme secure in the BSM is a special type of randomness extractor.

One can also consider a model, which we call the *bare* BSM, where Alice and Bob share no secret key initially. This model was first considered by Cachin and Maurer [5] who proposed a scheme in this model which requires Alice and Bob to each access $O(\sqrt{t})$ bits of R, much more than in the standard BSM with a short secret key. In this paper we prove that this is essentially optimal, i.e., that no secure key-agreement protocol for the bare BSM exists in which Alice and Bob access fewer than $O(\sqrt{t})$ bits of R. Such lower bound proofs, apart from being of general scientific interest, are important because they prevent the search for schemes that do not exist.

The BSM was also studied in the context of oblivious transfer [4], [7] and time-stamping [18].

II. The Bare Bounded-Storage Model and the Cachin-Maurer Scheme

Key agreement in the BSM, from the adversary's viewpoint, consists of two phases.

In the first phase, the string R is available to all parties. Alice and Bob execute a protocol over a public channel, resulting in transcript T which Eve obtains. Then, based on the transcript, Alice and Bob each store some information about R. The protocol can be randomized, where R_A and R_B denote their respective (independent) random strings. More precisely, Alice stores $M_A = f_A(R, T, R_A)$, and Bob stores $M_B = f_B(R, T, R_B)$, for some functions f_A and f_B. Eve also stores some information $M_E = f_E(R, T, R_E)$ about R, where R_E denotes her randomness (which is, of course, independent of (R_A, R_B)).

In the second phase, R has disappeared. Alice and Bob execute a second (probabilistic) protocol based on the stored

The results of this paper were presented at Eurocrypt 2004 [11]

S. Dziembowski is with the University of Rome *La Sapienza*. He is supported by an EU Marie-Curie project MEIF-CT-2006-024300-CRYPTOSENSORS.

U. Maurer is with ETH Zurich. He is supported by the Swiss National Science Foundation, project no. 200020-113700/1.

values M_A and M_B, resulting in a second transcript T'. Then Alice and Bob compute a secret key, K_A and K_B, respectively. It is not necessary to formalize this further, i.e., to make the functions used to compute K_A and K_B explicit.

The two security requirements are:

(i) *Correctness:* The probability $P(K_A \neq K_B)$ that the keys are different should be negligible.

(ii) *Secrecy:* The amount of information, $I(K_A; M_E T')$, obtained by Eve about the secret key (say K_A), must be negligible.

A scheme for key-agreement in the bare BSM was proposed by Cachin and Maurer in [5]. In their protocol, both Alice and Bob store an (independent) random subset of r bits of R, where r is on the order of $\sqrt{t}$. After R has disappeared for all parties, they publicly agree on which bits they have both stored. With very high probability, Eve has only partial information about these bits, and therefore Alice and Bob can apply privacy amplification (i.e., randomness extraction using a strong extractor with a public extractor parameter) to distill an essentially perfect key K. We prove in Section III that the protocol of [5] is essentially optimal.

III. Limitations of Key-Agreement in the Bare BSM

A. Statement of the Lower Bound

We prove the following result, which shows that the practicality of such an approach without shared initial key is inherently limited: Alice or Bob must have storage capacity around $\sqrt{s}$. The proof is given in Section III-B. Let h be the binary entropy function defined as $h(p) = -p\log_2(p) - (1-p)\log_2(1-p)$.

Theorem 1: For any key-agreement protocol secure in the BSM for which $I(K_A; M_E T') \leq \delta$ and $P(K_A \neq K_B) \leq \epsilon$, the entropy of the secret key K_A generated by Alice is upper bounded by

$$H(K_A) \leq \frac{s_A s_B}{s} + h(\epsilon) + \epsilon s_A + \delta, \tag{1}$$

where s_A and s_B are Alice's and Bob's required storage capacities, respectively, and s is Eve's assumed storage capacity.

Observe that for small ϵ and δ, the right hand side of (1) becomes approximately equal to $(s_A s_B)/s$, and hence in any secure key agreement at least one of the parties needs to have memory of a size at least $\sqrt{s}$.

We note that this bound also implies a bound on the memory of the adversary in the protocol for the oblivious transfer in the bounded-storage model.[1] Namely, if the memory of the honest parties is s_A, then the memory of a cheating party has to be much smaller than s_A^2. This shows that the protocol of [7] is essentially optimal and answers the question posed in [7], [8].

B. Proof of Theorem 1

Definition 1: A list $Z_0, \ldots, Z_n$ of random variables are *symmetric with respect to a random variable* Y if for every two sequences $i_1, \ldots, i_w$ and $i'_1, \ldots, i'_w$ of distinct indices we have

$$P_{Y,Z_{i_1},\ldots,Z_{i_w}}(y, z_1, \ldots, z_w) = P_{Y,Z_{i'_1},\ldots,Z_{i'_w}}(y, z_1, \ldots, z_w), \tag{2}$$

for all $y, z_1, \ldots, z_w$.

In other words, the distribution of $(Y, Z_{i_1}, \ldots, Z_{i_w})$ does not depend on the choice of the indices $i_1, \ldots, i_w$.

Lemma 1: If $Z_0, \ldots, Z_n$ are symmetric with respect to Y, then there exists $i \in \{0, \ldots, n\}$ such that

$$I(Y; Z_0 | Z_1 \cdots Z_i) \;\leq\; \frac{H(Y)}{n+1}.$$

Proof: The chain rule for conditional information[2] implies that

$$\sum_{i=0}^{n} I(Y; Z_i | Z_{i-1}, \ldots, Z_0) = I(Y; Z_0, \ldots, Z_n), \tag{3}$$

which is at most $H(Y)$. Therefore there must exist i such that

$$\frac{H(Y)}{n+1} \geq I(Y; Z_i | Z_{i-1}, \ldots, Z_0)$$

By the symmetry condition (2) this last value can be replaced by $I(Y; Z_0 | Z_1, \ldots, Z_i)$. This completes the proof. ∎

A simple example of such symmetric variables is given below (we will use it later in the proof of the theorem).

Observation 1: Let Y and Z be random variables. Suppose the random variables $Z_1, \ldots, Z_n$ are sampled independently, each according to the distribution $P_{Z|Y}$. Then $Z, Z_1, \ldots, Z_n$ are symmetric with respect to Y.

The following observation will also be useful.

Observation 2: If $Z_0, \ldots, Z_n$ are symmetric with respect to Y, then for an arbitrary function g the random variables $Z_0, \ldots, Z_n$ are symmetric with respect to $g(Y)$.

Proof: For every y' from the domain of g, all sequences $i_1, \ldots, i_w$ and $i'_1, \ldots, i'_w$ of distinct indices, and every sequence $z_1, \ldots, z_w$ we have

$$\begin{aligned} P_{g(Y),Z_{i_1},\ldots,Z_{i_w}}(y', z_{i_1}, \ldots, z_{i_w}) &= \\ \sum_{y: g(y)=y'} P_{Y,Z_{i_1},\ldots,Z_{i_w}}(y, z_{i_1}, \ldots, z_{i_w}) &= \\ \sum_{y: g(y)=y'} P_{Y,Z_{i'_1},\ldots,Z_{i'_w}}(y, z_{i'_1}, \ldots, z_{i'_w}) &= \\ P_{g(Y),Z_{i'_1},\ldots,Z_{i'_w}}(y', z_{i_1}, \ldots, z_{i_w}), & \end{aligned} \tag{4}$$

where (4) follows from the assumption that $Z_0, \ldots, Z_n$ are symmetric with respect to Y. ∎

To prove Theorem 1, recall that s_A, s_B, and s are the storage capacities of Alice, Bob, and Eve, respectively. We have to specify a strategy for Eve to store information (i.e., the function f_E). Such an admissible strategy is the following. For the fixed observed randomizer $R = r$ and transcript

[1] This is because there exists a black-box reduction of the key-agreement problem to the oblivious transfer problem [13]. (It is easy to see that the reduction of [13] works in the bounded-storage model.)

[2] Recall that the chain rule for information (see eg. [6], Theorem 2.5.2) states that for arbitrary random variables $V_1, \ldots, V_n$, and U we have

$$I(U; V_0, \ldots, V_n) = \sum_{i=0}^{n} I(U; V_i | V_{i-1}, \ldots, V_0)$$

$T = t$, consider $\lfloor s/s_B \rfloor$ independent copies $M_B^1, \ldots, M_B^{\lfloor s/s_B \rfloor}$ of what Bob stores, sampled independently according to the distribution $P_{M_B|R=r,T=t}$. (Clearly such sampling can be done by a computationally-unbounded Eve.)

Lemma 2: The random variables $M_B, M_B^1, \ldots, M_B^{\lfloor s/s_B \rfloor}$ are symmetric with respect to M_A.

Proof: Recall that M_A is a randomized function of (R, T), namely $M_A = f_A(R, T, R_A)$ for a random R_A. By Observation 1 the random variables $M_B, M_B^1, \ldots, M_B^{\lfloor s/s_B \rfloor}$ are symmetric with respect to (R, T), and hence also with respect to (R, T, R_A) since $R_A \rightarrow (R, T) \rightarrow M_B, M_B^1, \ldots, M_B^{\lfloor s/s_B \rfloor}$ form a Markov chain. Thus by Observation 2 the random variables $M_B, M_B^1, \ldots, M_B^{\lfloor s/s_B \rfloor}$ are symmetric also with respect to $M_A = f_A(R, T, R_A)$. ■

Hence Lemma 1 implies that there exists $i \in \{0, \ldots, \lfloor s/s_B \rfloor\}$ such that

$$I(M_A; M_B | M_B^1, \ldots, M_B^i) \leq \frac{H(M_A)}{\left\lfloor \frac{s}{s_B} \right\rfloor + 1} \leq \frac{H(M_A)}{\frac{s}{s_B}} \leq \frac{s_A s_B}{s}.$$

The last step follows from $H(M_A) \leq s_A$. Clearly an infinitely powerful Eve can compute such an index i. We hence assume that Eve stores $M_E := M_B^1, \ldots, M_B^i$.[3] Now we can apply Theorem 1 in [17] which considers exactly this setting, where Alice, Bob, and Eve have some random variables M_A, M_B, and M_E, respectively, jointly distributed according to some distribution $P_{M_A M_B M_E}$. The theorem states that the entropy of a secret key K that can be generated by public discussion is upper bounded as

$$H(K_A) \leq \underbrace{I(M_A; M_B | M_E)}_{\leq \frac{s_A s_B}{s}} + H(K_A | K_B) + \underbrace{I(K_A; M_E T')}_{\leq \delta}$$

Now, by Fano's lemma (cf. [3], p. 156)

$$H(K_A | K_B) \leq h(\epsilon) + \epsilon \log_2(2^{s_A} - 1) \leq h(\epsilon) + \epsilon s_A,$$

and we obtain (1). This concludes the proof of Theorem 1.

ACKNOWLEDGEMENTS

We would like to thank Louis Salvail and Christian Schaffner for pointing out an error in the proof stated in [11].

REFERENCES

[1] Y. Aumann, Y. Z. Ding, and M. O. Rabin. Everlasting security in the bounded storage model. *IEEE Transactions on Information Theory*, 48(6):1668–1680, 2002.

[2] Y. Aumann and M. O. Rabin. Information theoretically secure communication in the limited storage space model. In *Advances in Cryptology – CRYPTO '99*, Lecture Notes in Computer Science, Springer-Verlag, vol. 1666, pp. 65–79, 1999.

[3] R. E. Blahut. Principles and practice of information theory, 1987 Addison-Wesley Longman Publishing Co., Inc.

[4] C. Cachin, C. Crepeau, and S. Marcil. Oblivious Transfer with a Memory Bounded Receiver. In *Proc. of 39th Annual Symposium on Foundations of Computer Science*, IEEE Computer Society, pp.493–502, 1998.

[3] It may perhaps look a bit counter-intuitive that, for the sake of this proof, Eve does not necessarily store as many values as she could fit in her memory, i.e. set $M_E := M_E^{\lfloor s/s_B \rfloor}$. However, in principle it can be the case that $I(M_A; M_B | M_E^{\lfloor s/s_B \rfloor}) > I(M_A; M_B | M_E^i)$ (for $i < \lfloor s/s_B \rfloor$) because conditioning may actually increase a mutual information between random variables, i.e., $I(U; V) < I(U; V|W)$ is possible.

[5] C. Cachin and U. Maurer. Unconditional security against memory-bounded adversaries. In *Advances in Cryptology – CRYPTO '97*, Lecture Notes in Computer Science, Springer-Verlag, vol. 1294, pp. 292-306, 1997.

[6] T. M. Cover and J. A. Thomas. *Elements of Information Theory*. John Wiley and Sons, Inc., 1991.

[7] Y. Z. Ding. Oblivious transfer in the bounded storage model. In *Advances in Cryptology – CRYPTO 2001*, Lecture Notes in Computer Science, Springer-Verlag, vol. 2139, pp. 155–170, 2001.

[8] Y. Z. Ding. *Provable Everlasting Security in the Bounded Storage Model*. PhD thesis, Harvard University, 2001.

[9] Y. Z. Ding and M. O. Rabin. Hyper-encryption and everlasting security. In *STACS 2002, 19th Annual Symposium on Theoretical Aspects of Computer Science*, pp. 1–26, 2002.

[10] S. Dziembowski and U. Maurer. Tight security proofs for the bounded-storage model. In *Proceedings of the 34th Annual ACM Symposium on Theory of Computing*, pp. 341–350, 2002.

[11] S. Dziembowski and U. Maurer. On generating the initial key in the bounded-storage model. In *Advances in Cryptology – EUROCRYPT 2004*, Lecture Notes in Computer Science, Springer-Verlag, vol. 3027, pp. 126–137, 2004.

[12] S. Dziembowski and U. Maurer. Optimal randomizer efficiency in the bounded-storage model *Journal of Cryptology*, 17(1):5–26, 2004.

[13] Y. Gertner, S. Kannan, T. Malkin, O. Reingold, and M. Viswanathan. Relationship between public key encryption and oblivious transfer. In *Proc. 41st Annual Symposium on Foundations of Computer Science*, IEEE Computer Society, pp. 325–339, 2000.

[14] C. Lu. Hyper-encryption against space-bounded adversaries from on-line strong extractors. In *Advances in Cryptology – CRYPTO 2002*, Lecture Notes in Computer Science, Springer-Verlag, vol. 2442, pp. 257–271, 2002.

[15] U. Maurer. A provably-secure strongly-randomized cipher. *Advances in Cryptology – EUROCRYPT '90*, Lecture Notes in Computer Science, Springer-Verlag, vol. 473, pp. 361–373, 1990.

[16] U. Maurer. Conditionally-perfect secrecy and a provably-secure randomized cipher. *Journal of Cryptology*, 5(1):53–66, 1992.

[17] U. Maurer. Secret key agreement by public discussion. *IEEE Transactions on Information Theory*, 39(3):733–742, 1993.

[18] T. Moran, R. Shaltiel, and A. Ta-Shma. Non-interactive Timestamping in the Bounded Storage Model. In *Advances in Cryptology – CRYPTO 2004*, Lecture Notes in Computer Science, Springer-Verlag, vol. 3152, pp. 460–476, 2004.

[19] S. Vadhan. On constructing locally computable extractors and cryptosystems in the bounded storage model. In *Advances in Cryptology – CRYPTO 2003*, Lecture Notes in Computer Science, Springer-Verlag, vol. 2729, pp. 61–77, 2003.

Stefan Dziembowski was born in Warsaw, Poland in 1973. Currently he is a Marie-Curie Fellow at the University of Rome *La Sapienza*. He is interested in theoretical and applied cryptography.

Dziembowski received his MSc degree in computer science in 1996 from the Warsaw University, and his PhD degree in computer science in 2001 from the University of Århus. He spent 18 months as a post-doctoral fellow at the Swiss Federal Institute of Technology (ETH), Zurich. Afterwards, for 3 years he was an assistant professor at the Warsaw University.

He served as a PC member of several international conferences, including EUROCRYPT, and the International Colloquium on Automata, Languages and Programming (ICALP).

Ueli Maurer (S'85, M'90, SM'94, F'03), born in St. Gallen, Switzerland, in 1960, is professor of computer science and head of the Information Security and Cryptography Research Group at the Swiss Federal Institute of Technology (ETH), Zurich. His research interests include information security, the theory and applications of cryptography, information theory, theoretical computer science, and discrete mathematics.

Maurer graduated in electrical engineering (1985) and received his Ph.D. degree in Technical Sciences (1990) from ETH Zurich. From 1990 to 1991 he was a DIMACS research fellow at the Department of Computer Science at Princeton University, and in 1992 he joined the CS Department at ETH Zurich.

He has served extensively as an editor, including as Associate Editor of the IEEE Transactions on Information Theory, and as a member of program committees. Currently he is the Editor-in-Chief of the Journal of Cryptology, Editor-in-Chief of Springer Verlag's book series in Information Security and Cryptography, and serves on the Board of Directors of the International Association for Cryptologic Research (IACR).

Maurer holds several patents for cryptographic systems and has served as a consultant for many companies and government organisations. He serves on a few management and scientific advisory boards and is co-founder of Visonys, a Zurich-based security software company.