On (impracticality of) transfinite symmetric encryption with keys smaller than messages under GCH

Sergij V. Goncharov*

June 2020

Abstract

In this short trivial note we argue that, assuming Generalized Continuum Hypothesis to be true, it is impractical to use encryption with $Key \in \{0,1\}^K$ and $Message \in \{0,1\}^M$ such that $\aleph_0 \leqslant \operatorname{card} K < \operatorname{card} M$, because "complexity" of the known-plaintext bruteforce attack equals "complexity" of a single $En/Decrypt(Key, Message)$ "computation" then.

Keywords: transfinite cryptology, generalized continuum hypothesis, bruteforce

Preliminaries

For the sake of completeness and to lessen ambiguity, we (re)establish some basic denotations and recall some basic properties. See e.g. [12, 1, 3, 5], [8, 2.1, 2.6], [13, 1.2].

As usual, set theory is ZFC, with Zermelo-Fraenkel axioms (ZF) and Axiom of Choice (AC).

$\operatorname{card} A$ denotes the *cardinality*, or *cardinal number*, of the set A. $\operatorname{card} A = \operatorname{card} B$ iff $A \leftrightarrow B$. $\operatorname{card} A < \operatorname{card} B$ iff $A \leftrightarrow B' \subset B$ and $A \not\leftrightarrow B$. If A is finite, $\operatorname{card} A$ is identified with the number of elements in A. $\aleph_0 = \operatorname{card} \mathbb{N}$. $\operatorname{card} A \times \operatorname{card} B$ is $\operatorname{card}(A \times B) = \operatorname{card}\{(a;b) \mid a \in A, b \in B\}$. If non-empty sets A and/or B are infinite, $\operatorname{card} A \times \operatorname{card} B = \max\{\operatorname{card} A, \operatorname{card} B\}$.

Trichotomy: $\forall \mathfrak{a}(= \operatorname{card} A), \forall \mathfrak{b}(= \operatorname{card} B)$ we have $\mathfrak{a} < \mathfrak{b}$ or $\mathfrak{a} = \mathfrak{b}$ or $\mathfrak{a} > \mathfrak{b}$.

2^A is the *power set* of A, that is, the set of all subsets of A. $\operatorname{card} 2^A$ is denoted by $2^{\operatorname{card} A}$. By Cantor's theorem, $2^{\mathfrak{a}} > \mathfrak{a}$.

Generalized Continuum Hypothesis, GCH: "$2^{\aleph_\alpha} = \aleph_{\alpha+1}$ for any ordinal α" $\Leftrightarrow$ "If $\mathfrak{b} > \mathfrak{a} \geqslant \aleph_0$, then $\mathfrak{b} \geqslant 2^{\mathfrak{a}}$" $\Leftrightarrow$ "No cardinalities exist between $\operatorname{card} A$ and $2^{\operatorname{card} A}$ if A is infinite". Gödel [9] and Cohen [4] showed that GCH is independent of ZFC: it cannot be proved or refuted in ZFC (Sierpínski [22] showed that ZF+GCH implies AC). See also [5], [12, 14], [16].

(Bit)data over A is a mapping $\mathcal{A}\colon A \to \{0,1\}$, the set of all such bitdatas is $\{0,1\}^A$. a-th bit of $\mathcal{A}$ is $\mathcal{A}(a)$. *Size* of $\mathcal{A}$ is $\operatorname{card} A$. We say that $\mathcal{A}$ over A is *smaller* than $\mathcal{B}$ over B if $\operatorname{card} A < \operatorname{card} B$.

Key $\mathcal{K}$ is a bitdata over K, $\operatorname{card} K = \mathfrak{k}$. *Message* $\mathcal{M}$ is a bitdata over M, $\operatorname{card} M = \mathfrak{m}$. The set of all keys is $\mathbb{K}$, the set of all messages is $\mathbb{M}$. There are trivial bijections $\mathbb{K} \leftrightarrow 2^K$, $\mathbb{M} \leftrightarrow 2^M$.

Encryption and *decryption* are the mappings $\mathfrak{E}\colon \mathbb{K} \times \mathbb{M} \to \mathbb{M}$ and $\mathfrak{D}\colon \mathbb{K} \times \mathbb{M} \to \mathbb{M}$ respectively. The message to encrypt is *plaintext*, the message to decrypt is *ciphertext*.

$\mathfrak{E}$ and $\mathfrak{D}$ must have certain properties, $\mathfrak{D}(\mathcal{K}, \mathfrak{E}(\mathcal{K}, \mathcal{P})) = \mathcal{P}$ being perhaps the simplest of them. Here we state few other essential properties informally:

♣ It is "easy" (takes a short time) to determine $\mathcal{C} = \mathfrak{E}(\mathcal{K}, \mathcal{P})$ if $\mathcal{K}$ and $\mathcal{P}$ are known; it is "easy" to determine $\mathcal{P} = \mathfrak{D}(\mathcal{K}, \mathcal{C})$ if $\mathcal{K}$ and $\mathcal{C}$ are known.

♣ It is "hard" (takes a long time or impossible) to determine $\mathcal{P}$ such that $\mathfrak{E}(\mathcal{K}, \mathcal{P}) = \mathcal{C}$ if only $\mathcal{C}$ is known; this is *ciphertext-only attack*.

♣ It is "hard" to determine $\mathcal{K}$ such that $\mathfrak{E}(\mathcal{K}, \mathcal{P}) = \mathcal{C}$ if $\mathcal{C}$ and $\mathcal{P}$ are known; this is *known-plaintext attack*. Particularly, here *bruteforce attack* is to try all $\mathcal{K}' \in \mathbb{K}$ until one or all $\mathcal{K}'$ such that $\mathfrak{E}(\mathcal{K}', \mathcal{P}) = \mathcal{C}$ (or $\mathfrak{D}(\mathcal{K}', \mathcal{C}) = \mathcal{P}$) are found.

*Faculty of Mechanics and Mathematics, Oles Honchar Dnipro National University, 72 Gagarin Avenue, 49010 Dnipro, Ukraine. *E-mail: goncharov@mmf.dnu.edu.ua*

More notions defined and assumptions motivated vaguely, although, we suppose, naturally:

♠ To determine — compute — $\mathfrak{E}$ and $\mathfrak{D}$ for a given pair of their arguments, a party (Alice, Bob, etc.) has to perform the set of "elementary computations" in a finite time. We consider the cardinality of this set as the *complexity* of encryption and decryption, and we assume it is not greater than $\mathfrak{k} \times \mathfrak{m}$. For short, we say *"complexity of cryption is* $\mathfrak{k} \times \mathfrak{m}$*"*.[1]

♠ The complexity of the bruteforce attack as described above is $2^{\mathfrak{k}} \times \mathfrak{k} \times \mathfrak{m}$ — one cryption-and-comparison per each key from $\mathbb{K}$.

♠ In $\mathbb{R}$-time worlds we consider, we say *"party is* $(\mathfrak{a}, \mathfrak{b}, T)$*-able"* if this party is able to store a bitdata of size $\mathfrak{a}$ and to perform a computation of complexity $\mathfrak{b}$, in a time not longer than $T \in \mathbb{R}_+$. If a party is $(\mathfrak{a}, \mathfrak{b}, T)$-able, it is $(\mathfrak{a}', \mathfrak{b}', T')$-able for any $\mathfrak{a}' \leqslant \mathfrak{a}$, $\mathfrak{b}' \leqslant \mathfrak{b}$, $T' \geqslant T$.

Cf. [10], [14, 2], [2, 2] with increasing "abilities" of hypercomputers (provided with infinite time though), also [17, 2], [20, 2], [23, 3, 4]... and [6].

♠ $\mathfrak{k} < \mathfrak{m}$. We are going to speculate on circumstances this limitation may occur under; the reader may skip these speculations. At that, we distinguish between "storage" and "communication" contexts, or, in terms of [13, 1.2], between "time" and "space" separations.

The usual assumption of the *storage context* (cf. [13, Fig. 1.2]) is that the key $\mathcal{K}$ is known only to one party, Alice, who stores some data $\{\mathcal{P}_i\}_{i \in I}$ in encrypted form $\mathcal{C}_i = \mathfrak{E}(\mathcal{K}, \mathcal{P}_i)$ in public storage. So, Alice stores $\mathcal{K}$ too, only in her private long-term storage (PriLTS). All ciphertexts $\mathcal{C}_i$ and at least one plaintext $\mathcal{P}_0$ are known to the adversarial party, Bob. As soon as Bob gets $\mathcal{K}$, he decrypts all $\mathcal{C}_i$ and obtains entire original data. When $\mathfrak{k} \geqslant \mathfrak{m}$, it is probably easier for Alice to store $\mathcal{P}_i$ in PriLTS right away and do not deal with public storage, $\mathcal{K}$, $\mathfrak{E}$, $\mathfrak{D}$ at all.[2]

We suppose PriLTS is too small to contain bitdata of size $\mathfrak{m}$. Then Alice stores privately only $\mathcal{K}$ of size $\mathfrak{k} < \mathfrak{m}$.

In the *communication context* (cf. [13, Fig. 1.1]), $\mathcal{K}$ is shared in secrecy at some point of time between involved parties, Alice and Bob, who store it in their PriLTSes, so that only they know $\mathcal{K}$. We call the way this sharing is done "private short-term channel" (PriSTC). Afterwards they are able to communicate only over public channel, with the adversary, Cynthia, eavesdropping all bitdata they exchange. Therefore they exchange $\mathcal{C}_i = \mathfrak{E}(\mathcal{K}, \mathcal{P}_i)$. Similarly, Cynthia knows at least one $\mathcal{P}_0$, and as soon as she gets $\mathcal{K}$, the Alice$\leftrightarrows$Bob communication is compromized entirely.

We suppose either a) PriSTC does not have enough "bandwidth" to share bitdata of size $\mathfrak{m}$, or b) PriLTSes are too small to contain bitdata of size $\mathfrak{m}$.[3] So Alice and Bob use $\mathcal{K}$ of size $\mathfrak{k} < \mathfrak{m}$.

Sometimes these contexts combine.[4] Either way, smaller secrets are presumed easier to keep.[5]

Now we separate finite and transfinite cryptology.

Alice is the party who knows $\mathcal{K}$, $\mathcal{P}$, $\mathcal{C} = \mathfrak{E}(\mathcal{K}, \mathcal{P})$, and wants to keep $\mathcal{K}$ secret; Bob is the adversarial party who does not know $\mathcal{K}$, knows $\mathcal{C}$, $\mathcal{P}$, and wants to reveal $\mathcal{K}$ or any $\mathcal{K}'$ such that $\mathcal{C} = \mathfrak{E}(\mathcal{K}', \mathcal{P})$. If Alice is $(\mathfrak{a}, \mathfrak{b}, T)$-able, then Bob is $(\mathfrak{a}, \mathfrak{b}, T)$-able too.

[1] When "every bit of key and every bit of plaintext affect every bit of ciphertext". For one-time-pad-like ciphers, complexity is $\mathfrak{m}$. However, due to $\mathfrak{k} \leqslant \mathfrak{m}$, in transfinite case these complexities are equal.

[2] To be more precise, when $\mathfrak{k} \geqslant \operatorname{card} I \times \mathfrak{m}$. We assume $\operatorname{card} I \leqslant \mathfrak{m}$ in transfinite case.

[3] If Alice and Bob retain PriSTC and it has enough bandwidth to exchange bitdata of size $\mathfrak{m}$, the public channel becomes redundant as well as $\mathcal{K}$, $\mathfrak{E}$, $\mathfrak{D}$. If PriSTC is available only once, at sharing $\mathcal{K}$ (when all plaintexts to be encrypted are unknown yet), and has enough bandwidth, then $\mathfrak{k} = \mathfrak{m}$ is quite appropriate, even $\mathfrak{k} > \mathfrak{m}$ is possible. E.g. transfinite one-time pads are considered in [1], [3], [17, 3], [18].

[4] "Communication for storage transfer", where Alice provides Bob with data access, or "storage as communication over time", where Bob is Alice in future. In both examples, storage reasonings fit better.

[5] Cf. the common "cryptography reduces large secrets to smaller ones" idea [21, 10.4, afterword].

1 Finite case

The "real world" one. $\operatorname{card} K = k \in \mathbb{N}$, $\operatorname{card} M = m \in \mathbb{N}$, $k < m$.

Complexity of cryption is km, complexity of bruteforce is $2^k \cdot km$.

Alice can crypt, thus she is (m, km, T)-able, and so is Bob; we can even assume that Bob is (cm, ckm, T')-able for some c. He will have found the key in a finite time, the principal obstacle is its *amount*: $T' \sim 2^k \cdot km$ increases exponentially in k, and very soon (k in few hundreds nowadays) we get classical results based on laws of physics, kind of "even if all matter in the observable universe is involved, the search will not finish before that matter ceases to exist".

Up to now, as long as underlying cipher isn't broken, protocols are implemented correctly etc. etc., such encryption provides a secrecy.[6]

2 Transfinite case

"Real" as well... to those who live there, presumably. Be that as it may, the concept of transfinite cryptology has been studied for a long time: [15], [1], [3], [24], [19], [18], [17], [7].

$\operatorname{card} K = \mathfrak{k}$, $\operatorname{card} M = \mathfrak{m}$, $\aleph_0 \leqslant \mathfrak{k} < \mathfrak{m}$. Due to GCH, $2^{\mathfrak{k}} \leqslant \mathfrak{m}$.

Complexity of cryption is $\mathfrak{k} \times \mathfrak{m} = \mathfrak{m}$.

Complexity of bruteforce is $2^{\mathfrak{k}} \times \mathfrak{k} \times \mathfrak{m} = 2^{\mathfrak{k}} \times \mathfrak{m} = \mathfrak{m}$.

Since Alice can crypt, she is $(\mathfrak{m}, \mathfrak{m}, T)$-able. Then Bob is $(\mathfrak{m}, \mathfrak{m}, T)$-able too, and he completes the entire bruteforce in the same time as a single crypt by Alice.

Such encryption provides no secrecy.

Remarks

- Preliminaries took up most of it... Again, this "result" is trivial. Also, cf. [20] and [24, p. 149, par. 2]. Perhaps it is an exercise in books such as [23]?
- What conclusion the parties with transfinite abilities who inhabit worlds under GCH can draw from this note? — In storage context, store privately the data right away; in communication context, do not use keys smaller than messages.

But this note is finite, and even $(\aleph_0, \aleph_0, T)$-able parties can consider and verify all such notes in a finite time (they should not come of age without doing so), thus they probably know it already.

- Under ¬GCH, complexity of bruteforce $2^{\mathfrak{k}} \times \mathfrak{m}$ greater than complexity of cryption $\mathfrak{m}$ for $\mathfrak{k} < \mathfrak{m}$ is possible, if, unsurprisingly, $2^{\mathfrak{k}} > \mathfrak{m}$. Then such transfinite encryption may provide a secrecy, at least against bruteforce.
- What if some parties live in worlds under GCH and some under ¬GCH (see [11])? Can they exchange bitdata to communicate, perform passive and active attacks? Perhaps, at least, the bitdatas of "common" sizes pass the GCH/¬GCH barrier? The simplest answer is: any "leakage" between worlds is impossible as it leads to contradictions; otherwise, some basic concepts have to be reconsidered even before cryption enters.[7]

[6] This very file, while having been transferred to the reader through the network, was probably encrypted with keys much smaller than itself. Of course, there were also authentications, integrity checks etc.

[7] $(2^{\aleph_0}, 2^{\aleph_0}, 1)$-able Alice lives under ¬CH ($\not\Rightarrow$ ¬GCH), $(2^{2^{\aleph_0}}, 2^{2^{\aleph_0}}, 1)$-able Bob lives under GCH. Alice sends to Bob $\mathcal{A} = \chi_{\mathfrak{I}}$ (the "description", or "bit mask", of $\mathfrak{I}$) over $\mathbb{R} \leftrightarrow 2^{\mathbb{N}}$ such that for $\mathfrak{I} = \mathcal{A}^{-1}(1)$: $\aleph_0 < \operatorname{card} \mathfrak{I} < 2^{\aleph_0}$. Bob makes the masks $\mathcal{N} = \{\mathcal{N}_\iota\}$ describing all countable subsets of $\mathbb{R}$ (there are $2^{\aleph_0}$ of them) and $\mathcal{R} = \{\mathcal{R}_\iota\}$ describing all subsets of $\mathbb{R}$ equinumerous to $\mathbb{R}$ (there are $2^{2^{\aleph_0}}$ of them). Then he performs $2^{2^{\aleph_0}}$ computations, bit-for-bit comparisons, to verify that $\mathcal{A}$ is included neither in $\mathcal{N}$ nor in $\mathcal{R}$. Now Bob has the set $\mathfrak{I}$, which violates CH (thus GCH), impossible in his world, — a "paradox". Where these reasonings relying on familiar meanings became inconsistent (babble) is left as an exercise to the reader; see [5, IV.10], [12, 15, 26].

References

[1] G.R. Blakley, L. Swanson: *Infinite Structures in Information Theory*, Advances in Cryptology, 1983. doi:10.1007/978-1-4757-0602-4_4

[2] M. Carl, S. Ouazzani, P. Welch: *Taming Koepke's Zoo*, Sailing Routes in the World of Computation. CiE 2018. LNCS **10936**, 2018. doi:10.1007/978-3-319-94418-0_13

[3] B. Chor, E. Kushilevitz: *Secret Sharing over Infinite Domains (Extended Abstract)*, Advances in Cryptology — CRYPTO 89, LNCS **435**:299–306, 1990.

[4] P.J. Cohen: *The independence of the continuum hypothesis I, II*, Proc. Nat. Acad. Sci. USA **50(6)**:1143–1148, 1963; **51(1)**:105–110, 1964.

[5] P.J. Cohen: Set theory and the continuum hypothesis, W. A. Benjamin, Inc., 1966.

[6] M. Davis: *Why there is no such discipline as hypercomputation*, Applied Mathematics and Computation **178**:4–7, 2006.

[7] A. Dibert, L. Csirmaz: *Infinite secret sharing – Examples*, J. Math. Cryptol. **8**:141–168, 2014. doi:10.1515/jmc-2013-0005

[8] N. Ferguson, B. Schneier, T. Kohno: Cryptography Engineering, Wiley, 2010.

[9] K. Gödel: *The consistency of the axiom of choice and of the generalized continuum hypothesis*, Proc. Nat. Acad. Sci. USA **24**:556–557, 1938.

[10] J. Hamkins, A. Lewis: *Infinite time Turing machines*, J. of Symbolic Logic **65(2)**:567–604, 2000. doi:10.2307/2586556

[11] J. Hamkins: *The set-theoretic multiverse*, The Review of Symbolic Logic **5(3)**:416–449, 2012. doi:10.1017/S1755020311000359

[12] T. Jech: Set theory. 3rd Millennium ed., Springer, 2003.

[13] J. Katz, Y. Lindell: Introduction to Modern Cryptography. 2nd ed., CRC Press, 2015.

[14] P. Koepke, B. Seyfferth: *Ordinal machines and admissible recursion theory*, Annals of Pure and Applied Logic **160(3)**:310–318, 2009. doi:10.1016/j.apal.2009.01.005

[15] B. Makar: *Transfinite Cryptography*, Cryptologia **4(4)**:230–237, 1980. doi:10.1080/0161-118091855176

[16] G.H. Moore: *Early history of the Generalized Continuum Hypothesis: 1878–1938*, Bull. Symbolic Logic **17(4)**:489–532, 2011.

[17] J. Patarin: *Transfinite Cryptography*, Cryptology ePrint Archive **2010**:001, 2010.

[18] R.C.W. Phan, S. Vaudenay: *On the Impossibility of Strong Encryption Over* $\aleph_0$, Coding and Cryptology. IWCC 2009. LNCS **5557**, 2009. doi:10.1007/978-3-642-01877-0_17

[19] L. Poinsot: *Perfect nonlinear S-boxes on the real-line*, J. of Discrete Mathematical Sciences and Cryptography **10(6)**:793–813, 2007. doi:10.1080/09720529.2007.10698158

[20] A. Powell: *A Universal Hypercomputer*, 2018. arXiv:1806.08747

[21] B. Schneier: Applied Cryptography. 2nd ed., Wiley, 1996.

[22] W. Sierpínski: *L'hypothèse généralisée du continu et l'axiome du choix*, Fund. Math. **34**:1–5, 1947.

[23] A. Syropoulos: Hypercomputation, Springer, 2008.

[24] D.P. Woodruff, M. van Dijk: *Cryptography in an Unbounded Computational Model*, EUROCRYPT 2002, LNCS **2332**:149–164, 2002. doi:10.1007/3-540-46035-7_10