DOI: 10.15439/2019F313
ISSN 2300-5963 ACSIS, Vol. 18

Cryptographic keys management system based on DNA strands

Marek Miśkiewicz
Maria Curie-Sklodowska University
Plac Marii Curie-Skłodowskiej 5
20-031 Lublin, Poland
Email: marek.miskiewicz@umcs.pl

Bogdan Księżopolski
Maria Curie-Sklodowska University
Plac Marii Curie-Skłodowskiej 5
20-031 Lublin, Poland
Email: bogdan.ksiezopolski@umcs.pl

***Abstract*—Security of cryptographic keys is one of the most important issues in a key management process. The question arises whether modern technology really allows for a high level of physical protection and security of sensitive data and cryptographic keys. The article considers various contemporary types of threats associated with the storage of secret keys. We present an innovative way to store sensitive data, using DNA strands as a medium, which significantly reduces hazard connected with electronic devices based data storage and makes the key management process independent of third parties.**

I. Introduction

SECRET keys are usually stored in hard drives placed in computer devices with access secured with a simpler several-character password or on portable flash drives. Such solutions have many disadvantages and really do not guarantee a high level of data security or even in some cases usability. There are a few important reasons why the cryptographic data is not completely safe if it is stored on portable devices (in NAND memory chips) or magnetic storage devices. It is obvious that access to stored cryptographic keys needs at least computer devices with access to wider resources eg. Internet network. With the current complexity of digital systems, we can not fully guarantee security, which to some extent, relies on trust in the integrity of digital system manufacturers and designers. Absolute security, at least theoretically, can only be guaranteed by the lack of participation of third parties in the process of managing and storage of cryptographic keys (creation, storage, use and destruction). If we consider it necessary to use electronic devices, this entails additional risks, in particular, due to the lack of access to stored data during power system failure caused for example by Solar Storm. In the article, the new cryptographic keys management system based on DNA strands is presented. The contributions of our concept are as follows:

- security increase by excluding third parties from the process of storing and reading the key,
- lack of weaknesses and vulnerabilities associated with storing cryptographic keys on portable electronic devices,
- no susceptibility to data destruction caused by strong electromagnetic fields,
- enormous difficulty in accessing data (e.g. cryptographic keys) by unauthorised persons in case of loss of control,
- no need to use DNA sequencing devices to read stored data (minimal resources infrastructure),
- data transferability in a way that can be almost completely undetectable in physical form.

II. Related work

In the domain of cryptography key management systems based on biosystems one can analyse three issues: bio cryptography, third-party key management and environmental threats.

A. *Bio cryptography*

The use of DNA strands to store information and even perform simple "calculations" is not a completely new idea. Adelman in his work showed the possibility of using fragments of specially prepared DNA strands to solve the problem of Hamilton's path [1]. Gehani together with others created the basis of DNA-based cryptosystem based on the idea of One Time Pad [2]. In the work of Y. Zhang, X. Lui and M. Sun a practical implementation of the problem of key distribution for the OTP method was shown [3]. The sequence of nucleotides in a randomly selected fragment of DNA is used as the key to encrypt the message. The explicit text has been replaced with a sequence of bits and using the XOR function joined with the key string. The key, based on the DNA sequence can be obtained by using one of the possible substitutions of nucleotides: A - 00, C - 01, T - 11, G - 10. Next, the ”DNA key“ was „glued” to the plasmid and placed in the bacterial cell. The environment inside the bacteria allows you to stably hold the information contained in the DNA strand, which is very sensitive to changes in the temperature and pH of the solution in which it is located. The stability of the DNA accumulated in bacterial cells carried out in the state of spore is impressive. Scientists have been able to read genetic material from Subtilis bacteria, which is millions of years old [4], [5]. Modern laboratory techniques allow for stable storage synthetic DNA in Silica for thousands of years [6], [7]. This may be important if it is necessary to store relevant information (in particular cryptographic information) for a very long period of time. Traditional storage technologies such as magnetic devices and optical discs are not reliable for really long-term data storage. Their lifespan is estimated to be about 50 years [8].

Halvorsen and Wong in his paper [9] showed an interesting, simple and secure system for encrypting and decrypting information using self-assembly DNA structures and PCR based decoded information reading method. Tanaka, Okamoto and Saito presented a system for public key distribution based on DNA as a one-way function [10]. Using the methods and algorithms described in the works of A. Leier [11] and H. J. Shiu [12], one can hide the message in a DNA sequence in an encrypted or unencrypted way. Such stenographic techniques require active synthesis of deoxyribonucleic acid chains. The text is encrypted directly in the series of A, C, T and G, or special groups are identified later as counterparts of binary zeros and ones. The presented methods require both synthesis and sequencing devices at almost every stage of work with data stored in DNA, which seems to be an inconvenience in a certain class of applications. Some ideas presented in the last two publications are applied further. The DNA chain can also be successfully used in forensics [13] as well as for invisible product tagging [14].

B. *Third-sparties keys management*

A user who really cares about the security of his or her data cannot be sure that the data storage devices, produced by third parties, do guarantee real security. This is due to the fact that the average user does not have access to the exact device specification and is not able to check if the electronic systems controlling the memory chips do not allow easy access to data stored by unauthorized entities. In other words, strong cryptography and ultimate cryptographic keys security require the assumption of complete distrust in the devices that are used. The continuous reduction in the size of integrated circuits leads to increased production costs. This forces a vast majority of chid design companies to trust an external third party in chip fabrication, but outsourcing of chip fabrication opens-up hardware to attack. The way of preparing post fabrication tests leave an open door for implementing malicious modifications and backdoors. Even if there are no equipment manufacturers bad intentions there is always a possibility that there has been interference of third parties.

Researchers at the University of Michigan showed in their paper [15], that there is a possibility to create a novel fabrication-time attack based on modifications of the semiconductor structure in integrated circuits. It can be done by adding even single component to "mask" - a blueprint of the chip before its production. Such modifications are hardly detected during the test procedure. This kind of attack is triggered by special *unlike* sequence of commands and allows to give a malicious program the full operating system access.

Other, pernicious fabrication-time attack named dopant-level Trojan bases on conversion trusted circuits into malicious circuitry in chip structure by changing the dopant ratio on the input pins to transistors [16], [17]. Circuits converted to Trojans are very difficult to detect due to the lack of added circuit elements and require imaging with a scanning electron microscope.

Spiegel Online reports in his article [18] that the US National Security Agency (NSA) is in possession of specially prepared "computer buggung" devices that look like typical USB plugs. These devices are capable of sending and receiving data via radio link being undetected.

In October 2018 Bloomberg reported that special microchips were inserted into server motherboards during the production process. The motherboards are components of servers operating in many companies inside their datres. Some of these chips were built as if they were necessary elements for the proper operation of the entire system. Installed chips have enough processing power to carry out an attack or be used to gain unauthorized access to data [19].

C. *Environmental threats*

One of the important factors that should be taken into account when cryptographic data is stored on electronic devices and magnetic storage devices is their relatively high sensitivity to strong electromagnetic fields. These kinds of fields can be produced in two ways: as EMP pulses (Electro-Magnetic Pulse) or during the Electromagnetic Solar Storm, especially in the so-called Coronal Mass Ejection.

It is worth to mention at least about two cases of CME, which had a significant impact on the human created infrastructure. The first one is The Solar Storm of 1859 (known as Carrington Effect). During this storm, Earth's magnetic field disturbances caused by CME led to telegraph network failures throughout Europe and North America in some cases giving telegraph operators electric shocks. The second one took place on March 13, 1989. A severe geomagnetic storm struck Earth causing nine hours blackout in Quebec, Canada.

Report prepared by Metatech Corporation [20] describes the threat of the early-time (E1) High-altitude Electromagnetic Pulse (HEMP) produced by nuclear detonations above an altitude of 30 km. The pulse is driven by gamma photons produced in nuclear reactions within the nuclear burst. The main impact has such impulse on the power grid that can be totally damaged, but as the report shows, computers and small electronic devices are also at risk of damage what can make them unusable.

III. The method

In this paper, we use and extend the concept presented in the work of [11], where the single bits of information are represented by groups of nucleotides. With certain restrictions, this solution allows to easily generate sequences of data stored in DNA without the need to use synthesis devices. If the prepared data contain secret information, for example, password or cryptographic keys then, as it was mentioned earlier, the lack of third parties engagement during the synthesis process significantly increases data security.

A. *DNA data structure*

DNA strand with data stored within, consist of a series of specially prepared components – some kind of building blocks which in fact are shorter fragments of double-stranded DNA

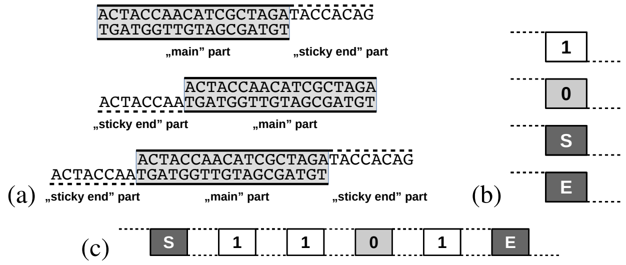

Fig. 1. (a) Structure of simple DNA component. Structural components to build simple DNA data strand. (b) Structural components to build simple DNA data strand. (c) Example of structure of four bit DNA strand.

ended with single-stranded regions called sticky ends. The general shape of a single components is presented in Figure 1 (a). The main part identifies some sort of data stored as a series of nucleotides. These nucleotides can represent a bit or index of extracting parts. Sticky ends are free fragments of one-sided DNA strand that can easily bind to other complementary part connected to the other fragments to producing longer strands.

In the simplest case to store data in DNA as a series of 0 and 1 bits one needs at least four structurally different fragments (see Figure 1 (b)). Two of them named S and E starts and ends DNA strand containing data. "0" and "1" fragments represent bis of data. An example of general structure of four bits single DNA strand is shown in the Figure 1 (c).

Every DNA strand containing data bits always starts with n-numbered S fragment. Start fragment (S_n) is a double-stranded fragment of DNA with length about 30 bp (nucleobase pairs). It consists of the "main” part and sticky end part. The main part (approximately 22 bp) carries information that can be used to identifying bit sequence as a part of a larger amount of data. It can be also used as a primer for the PCR procedure. Sticky end part (length about 8 bp - depended on the total length of the whole strand - explained later in the text) allows binding with next structure fragment - bit fragment.

Bit fragment (B_{0k} or B_{1k}) is a double-stranded fragment of DNA of length about 20 - 30 bp. It consists of Bit identification part and two sticky end parts. There are two different types of Bit identification part - one for bit "1” and the other for bit "0”. In the simplest approach the internal structure of every bit "1” and "0” are the same for the whole data strand. In this case, there is no need to use sequencing devices to read data from DNA. Data sequence from the specified strand can be retrieved only by gel electrophoresis.

End fragment is about 20 bp length and it is the last structure element of data DNA strand. Like other fragments, it contains an identification part and a sticky end part.

B. Sticky ends

The sticky end is a short single-stranded fragment of DNA placed on its end that allows binding DNA fragments into longer strands. The Special design of the sticky ends nucleotide sequence allows the complementary fragments to join generating a fixed order of components. The idea of how the sticky ends work is presented on Figure 2.

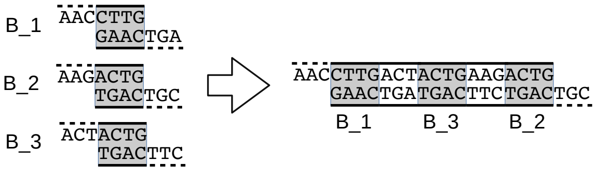

Fig. 2. Shorts three fragments of DNA with complementary sticky ends before ligation.

N bits data string encoded into DNA strand requires at least:

- DNA start component (S) with sticky end marked as s_0,
- N pair of "Bit" components:
  - first pair of bits with structure: $s_0 - 0 - s_1$ and $s_0 - 1 - s_1$, where s_n means n'th sticky end,
  - second pair of bits with structure: $s_1 - 0 - s_2$, $s_1 - 1 - s_2$,
  - n'th bits pair structure: $s_{n-1} - 0 - s_n$, $s_{n-1} - 1 - s_n$,
- end component (E) with sticky end marked as s_n.

DNA data strand structure looks like this: $S - s_0 - B_1 - s_1 - B_2 - s_3 - \ldots - s_{n-1} - B_n - s_n - E$. B_n denotes "0" or "1" bit component. As one can see n different sticky ends s_i are required. Due to the fact that sticky ends consist of k nucleotides, only $4k$ different nucleotide sets can be produced. From the statistical point of view, for data strand containing n bits minimal length of each sticky end should be at least: $k = \frac{1}{2}\log_2 n$. For example, 64-bit data strand requires sticky ends that consist of only 3 nucleotides. In fact, as it could be seen in [11], even for 8-bit data strands structure of individual DNA components is more complicated and requires sticky ends of length 10 nt (nucleotides). This is due to the fact that biochemical conditions and processes play a significant role in the problem of sticky end creation and use. The simplest case of minimal required sticky ends length is insufficient and do not lead to the successful creation of longer data strands. Biological limitations related to the procedure of creation data stands from DNA fragment and read them by gel electrophoresis cause that the number of bits carried by DNA strand is not enough to store for example long cryptographic key (1024 to 4096 bits) in a single strand. The reasonable total length of DNA strand that can be used for data storage considered in this paper is about 1000 bp. For such strands number of stored bits is about 32, so 1024 bit keys require 32 different DNA strands. It is, therefore, necessary to introduce a system of indexing individual strands or even individual keys if the multi-key system is introduced.

C. Single n-length key DNA data strand preparation

Let us consider the user that wants to store $n = 2^k$ bits long cryptographic key in the DNA strand, that can carry only $m = 2^{k-l}$ bits. Thus he requires 2^l DNA strands, where every one of them contains m bits of key called subkey. Structure of a single DNA strand from the given set is as follows: $s_i - S_i - s_0 - B_1 - s_1 - B_2 - s_2 - \ldots - s_{m-1} - S_{m-1} - s_m - B - s_m - E_j - s_j$. i and j denote subkey number and vary from 1 to 2^l. As one can see 2^l S and E fragments must be synthesised with different unique

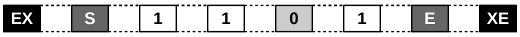

Fig. 3. Example of 4 bit data strand with Extractor fragments bounded ant the ends.

sticky ends. The purpose of that will be explained further. Finally, the procedure of preparation DNA strands for store n bit length key has following steps:

1) Generation and synthesis of 2^l unique DNA Start fragments S: $s_i - S_i - s_0$.
2) Generation and synthesis of m pairs of Bit fragments $s_0 - 0_1 - s_1$ to $s_{m-1} - 0_m - s_m$ and $s_0 - 1_1 - s_1$ to $s_{m-1} - 1_m - s_m$. All Bit fragments are called Bit Library.
3) Generation and synthesis of 2^l unique DNA End fragments E: $s_m - E_i - s_j$.
4) Preparation of subkeys $K_{m:i}$ for $i = 1 \text{to} 2^l$ by splitting key K into 2^l fragments. Subkey $K_{m:i} = \{B_1, B_2, \ldots, B_m\}_{m:i}$ where B_1, $B_2, \ldots$ represent individual bits of subkey.
5) For the firs subkey of key K mix in the reaction tube Start fragments S_1, End fragments E_1, and a set of Bit fragments chosen from Bit Library in a way to match the corresponding first subkey bits. Then incubate mixture according to biotechnological protocols to obtain double-stranded DNA.
6) Repeat previous step for next subkey of key K.

After a procedure of generating key K one should have 2^l reaction tubes with subkeys. Content of reaction tubes can be mixed together in one tube after DNA purification. The final tube contain all the key K stored in DNA as a series of its bits. Presented procedure can be extended to store more than one key K just in one tube. Comments require the presence of sticky ends denoted as s_i and s_j at the beginning and at the end of the strand. This is straightly connected with subkey extraction and the read procedure described below.

D. Subkey extraction

To read a sequence of bits of key K a sequence of each subkey must be read. All subkey are stored in one tube so the procedure of extraction single subkey must exist. This can be done by preparing a special set of extractors called EX and XE which are in fact fragments of double-stranded DNA ended by sticky ends at one side. The extractors are designed to bind to a selected strand representing subkey both at the start (EX) and the end (XE). It provides to extend the length of the subkey strand as it is shown on a Figure 3.

There is a pair of primers designed to be complementary to extractor pair. Primers are needed for the PCR procedure to increase the number of DNA strands carried extracted subkey. Primers are called PEX and PXE. The general procedure to extract subkey $K_{m:i}$ is as follows: i. get a small amount of mixture containing the key K ad put it into another reaction tube, ii. add pair of extractors EX_i and XE_i to the reaction tube and ligate them, iii. prepare and proceed electrophoresis on an agarose gel to separate strands extended by the extractors, vi. isolate from gel DNA strands, that the length corresponds to the length of subkey DNA plus the length of both extractors, v. for extracted DNA material provide the PCR process with primers PEX_i and PXE_i relevant to extractors EX_i and XE_i to amplify a number of copies of DNA strand.

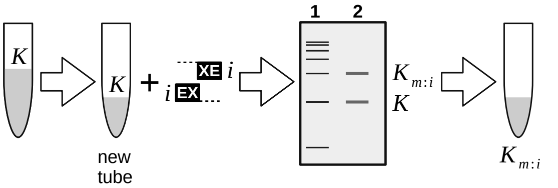

Fig. 4. Schematic process of subkey $K_{m:i}$ extraction.

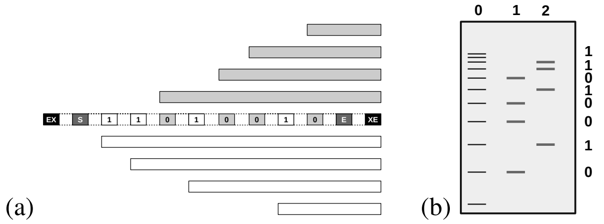

Fig. 5. (a) Expected primer length after elongation in case of 8 bit encoding DNA strand after PCR procedure. (b) An example picture of gel electrophoresis performed for strands set on the left side. Lane 0 symbolize distribution of molecular weight marker, lane 1: distribution of strands length elongated with "0" primer, lane 2: distribution of strands length elongated with primer "1". Reading from bottom to top reveals an encoded bit sequence.

E. Subkey reading

To determine a series of bits in extracted and isolated subkey one must perform two-step procedure used by [11] in his work. The first step is to carry out PCR procedure with two types of primers. Solution with isolated and replicated subkey must be split into two reactions tubes. To the first tube one has to add primers corresponding to "0" bit DNA fragment, to the second reaction tube primers corresponding to "1" bit fragment must be added. Next for both tubes PCR must be performed to elongate the primers. After PCR reaction tubes should contain shorter DNA strands with length matching to the position of "0" and "1" fragments. Figure 5 a. shows example of PCR performed for strand encoding 8 bit sequence: 1 1 0 1 0 0 1 0. The second step requires the implementation of gel electrophoresis for PCR'ed mixture with a subkey. Contents of both reaction tubes must be put into gel separately on different lanes to visualize "0" bit bands and "1" bit bands. Positions of each band are related to DNA strand length in the analysed sample. Due to the fact that Bit fragments forming subkey consist of a determined number of nucleotides, some kind of "quantisation" must occur after electrophoresis. In other way bands on the gel always should come up at the fixed positions indicating positions of zeroes and ones in the analysed subkey. Picture 5 (b) shows expected bands distribution for example from picture 5 (a). To read a sequence of entire key K every subkey must be read in mentioned way.

F. Molecular keyring

A tube containing many keys (stored in DNA) could be considered to be "a molecular keyring". The idea of storing multiple keys in DNA bands is not very different from the method of storing a single key, that can be expanded relatively easy. Such approach requires the creation of a revocation key mechanism and an extractors database for keys identification. As it was mentioned earlier, information about the key number and its subkeys is stored in the first segment of each strand containing sticky ends. A user of this system needs to know which extractors use to obtain a chosen key (i.e. subkeys belonging to this key), so the external information binding extractors (with specified sticky ends) with key structure (subkeys sequence) must exist. This could be done for example by signing tubes containing extractors with a signature like this: $K_{k:m:i}$ that means: extractor for i-th subkey of length m of key k.

For storing, extracting and reading four 1024 bit keys as a series of many 32 bit sequences (which is, in fact, one 4096 bit key - mostly use in e.g. RSA system) user needs in total less than 512 tubes of oligonucleotides to perform simple operations.

A simple revocation mechanism can be proposed for keys that were used and are no longer valid. Other teys for further processing (e.g. reading) need to be extracted by binding them with EX and XE extractors. The sticky ends of S and E fragments can be blocked against using them as binding sites by adding to the main tube containing keys short single-stranded DNA fragments called caps. Caps are complementary to the sticky ends that need to be blocked. After ligation using ligase enzyme sticky ends at both ends of selected strands (subkeys) should become inactive and no longer can be used for the key extraction. Revocation system for keyring from the above example needs to manage additional $4 * 32 * 2 = 256$ tubes of oligonucleotides.

IV. Conclusions and future work

A simple cryptographic keys creation and management system based on DNA strands was presented. Despite the considerable complexity due to the relatively large number of necessary elements the system does not require the participation of third parties in very important steps such as the key creation and reading. These features make it resistant to attacks of stealing data through untrusted (unsecured) elements of IT infrastructure or through access by unauthorized entities. In addition, data stored as molecular structures are not susceptible to EMP or SolarStorms and are largely independent of power grids. The next step should focus on experimental verification of the whole process.

References

[1] L. M. Adleman, "Molecular computation of solutions to combinatorial problems." *Science*, vol. 266, no. 5187, pp. 1021–1024, Nov 1994. doi: 10.1126/science.7973651. [Online]. Available: https://doi.org/10.1126/science.7973651

[2] A. Gehani, T. LaBean, and J. Reif, *DNA-based Cryptography*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2004, pp. 167–188. ISBN 978-3-540-24635-0. [Online]. Available: https://doi.org/10.1007/978-3-540-24635-0_12

[3] Y. Zhang, X. Liu, and M. Sun, "Dna based random key generation and management for otp encryption." *Biosystems*, vol. 159, pp. 51–63, Sep 2017. doi: 10.1016/j.biosystems.2017.07.002. [Online]. Available: https://doi.org/10.1016/j.biosystems.2017.07.002

[4] R. Cano and M. Borucki, "Revival and identification of bacterial spores in 25- to 40-million-year-old dominican amber," *Science*, vol. 268, no. 5213, pp. 1060–1064, 1995. doi: 10.1126/science.7538699 Cited By 348. [Online]. Available: https://doi.org/10.1126/science.7538699

[5] R. Vreeland, W. Rosenzweig, and D. Powers, "Isolation of a 250 million-year-old halotolerant bacterium from a primary salt crystal," *Nature*, vol. 407, no. 6806, pp. 897–900, 2000. doi: 10.1038/35038060 Cited By 414. [Online]. Available: https://doi.org/10.1038%2f35038060

[6] R. N. Grass, R. Heckel, M. Puddu, D. Paunescu, and W. J. Stark, "Robust chemical preservation of digital information on dna in silica with error-correcting codes," *Angewandte Chemie International Edition*, vol. 54, no. 8, pp. 2552–2555, 2015. doi: 10.1002/anie.201411378. [Online]. Available: https://doi.org/10.1002/anie.201411378

[7] J. P. Cox, "Long-term data storage in dna," *Trends in Biotechnology*, vol. 19, no. 7, pp. 247 – 250, 2001. doi: 10.1016/S0167-7799(01)01671-7. [Online]. Available: https://doi.org/10.1016/S0167-7799(01)01671-7

[8] S. B. Shah and J. G. Elerath, "Reliability analysis of disk drive failure mechanisms," *Annual Reliability and Maintainability Symposium, 2005. Proceedings.*, pp. 226–231, 2005. doi: 10.1109/RAMS.2005.1408366. [Online]. Available: http://doi.org/10.1109/RAMS.2005.1408366

[9] K. Halvorsen and W. P. Wong, "Binary dna nanostructures for data encryption," *PLOS ONE*, vol. 7, no. 9, pp. 1–4, 09 2012. doi: 10.1371/journal.pone.0044212. [Online]. Available: https://doi.org/10.1371/journal.pone.0044212

[10] K. Tanaka, A. Okamoto, and I. Saito, "Public-key system using dna as a one-way function for key distribution," *Biosystems*, vol. 81, no. 1, pp. 25 – 29, 2005. doi: 10.1016/j.biosystems.2005.01.004. [Online]. Available: https://doi.org/10.1016/j.biosystems.2005.01.004

[11] A. Leier, C. Richter, W. Banzhaf, and H. Rauhe, "Cryptography with dna binary strands." *Biosystems*, vol. 57, no. 1, pp. 13–22, Jun 2000. doi: 10.1016/S0303-2647(00)00083-6. [Online]. Available: https://doi.org/10.1016/S0303-2647(00)00083-6

[12] H. Shiu, K. Ng, J. Fang, R. Lee, and C. Huang, "Data hiding methods based upon dna sequences," *Information Sciences*, vol. 180, no. 11, pp. 2196 – 2208, 2010. doi: 10.1016/j.ins.2010.01.030. [Online]. Available: https://doi.org/10.1016/j.ins.2010.01.030

[13] J.-M. Oh, D.-H. Park, and J.-H. Choy, "Integrated bio-inorganic hybrid systems for nano-forensics," *Chem. Soc. Rev.*, vol. 40, pp. 583–595, 2011. doi: 10.1039/C0CS00051E. [Online]. Available: http://dx.doi.org/10.1039/C0CS00051E

[14] S. Cormier, J. Shearman, and M. Hogan, "Dna in your jeans? effect of abrasion and bleaching on dna tagged denim," *AATCC Review*, vol. 18, pp. 44–48, 09 2018. doi: 10.14504/ar.18.5.4. [Online]. Available: https://doi.org/10.14504/ar.18.5.4

[15] K. Yang, M. Hicks, Q. Dong, T. Austin, and D. Sylvester, "A2: Analog malicious hardware," in *2016 IEEE Symposium on Security and Privacy (SP)*, May 2016. doi: 10.1109/SP.2016.10. ISSN 2375-1207 pp. 18–37. [Online]. Available: https://doi.org/10.1109/SP.2016.10

[16] G. T. Becker, F. Regazzoni, C. Paar, and W. P. Burleson, "Stealthy dopant-level hardware trojans: extended version," *Journal of Cryptographic Engineering*, vol. 4, no. 1, pp. 19–31, Apr 2014. doi: 10.1007/s13389-013-0068-0. [Online]. Available: https://doi.org/10.1007/s13389-013-0068-0

[17] R. Kumar, P. Jovanovic, W. Burleson, and I. Polian, "Parametric trojans for fault-injection attacks on cryptographic hardware," in *2014 Workshop on Fault Diagnosis and Tolerance in Cryptography*, Sep. 2014. doi: 10.1109/FDTC.2014.12 pp. 18–28. [Online]. Available: https://doi.org/10.1109/FDTC.2014.12

[18] J. Appelbaum, J. Horchert, O. Reissmann, M. Rosenbach, J. Schindler, and C. Stöcker. (2013, 12) Unit offers spy gadgets for every need. [Online]. Available: http://www.spiegel.de

[19] J. Robertson and M. Riley. (2018, 11) The big hack: How china used a tiny chip to infiltrate u.s. companies. [Online]. Available: https://www.bloomberg.com

[20] E. Savage, J. Gilbert, and W. Radasky, "The early-time (e1) high-altitude electromagnetic pulse (hemp) and its impact on the u.s. power grid," Metatech Corporation, 358 S. Fairview Ave., Suite E Goleta, CA 93117, Tech. Rep., January 2010.