SANDIA REPORT
SAND2019-11819
Unlimited Release
Printed October 2019

Arms Control Opportunities for Inherently Safe and Secure Nuclear Command, Control, and Communications

Geoffrey E. Forden

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Issued by Sandia National Laboratories, operated for the United States Department of Energy by National Technology and Engineering Solutions of Sandia, LLC.

Available to DOE and DOE contractors from

U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865) 576-8401
Facsimile: (865) 576-5728
E-Mail: reports@osti.gov
Online ordering: http://www.osti.gov/scitech

Available to the public from

U.S. Department of Commerce
National Technical Information Service
5301 Shawnee Rd
Alexandria, VA 22312

Telephone: (800) 553-6847
Facsimile: (703) 605-6900
E-Mail: orders@ntis.gov
Online order: https://classic.ntis.gov/help/order-methods/

SAND2019-11819
Printed October, 2019
Unlimited Release

Arms Control Opportunities from Inherently Safe and Secure Nuclear Command, Control, and Communications

Geoffrey E. Forden
Global Security Research and Analysis
Sandia National Laboratories
P. O. Box 5800
Albuquerque, New Mexico 87185-MS1371

Abstract

The Department of Defense Science Board has stated that the United States is "not prepared to defend against" cyber-attacks and that the military could lose "trust in the information and ability to control U.S. systems and forces [including nuclear forces]." One potential weak spot in cyber-security is storing encryption keys in computer memory. This paper explores the use of hardware devices (so-called Physical Unclonable Functions, or PUFs) to generate, in the nuclear weapon itself, unique encryption keys each time they are needed. Not only do we find that this has the potential to mitigate a number of cyberthreats, but such hardware has the potential to greatly diminish the total uncertainty associated with radiation-based warhead authentication procedures; a procedure many analysts feel will be key to future arms control regimes. After outline the use of PUFs in nuclear command, control, and communications—and indicating some of the areas that still require further research—we discuss their application to arms control and warhead authentication

TABLE OF CONTENTS

NOMENCLATURE

Abbreviation	Definition
Abbreviation	Definition
CC	Command Center
CL	Confidence Level
CRP	Challenge/Response Pair
DCA	Dual Capable Aircraft
EAM	Emergency Action Message
ICBM	Intercontinental Ballistic Missile
K	Number of nuclear weapons diverted from an arms control regime
M	Total number of nuclear weapons in a stockpile subject to an arms control regime.
MEMS	Micro-Electro-Mechanical System
N	Number of nuclear weapons authenticated
NC3	Nuclear Command, Control, and Communications. This refers to the "collection of activities, process, and procedures performed by appropriate commanders and support personnel who, through the chain of command, allow for decisions to be made based on relevant information, and allow those decisions to be communicated to forces for execution."[1]
NCA	National Command Authority
OCONUS	Outside the Continental United States
P_K	The probability that there are K diverted nuclear weapons and none of them are detected during N authentications in a total arsenal of M.
PUF	Physically Unclonable Function
SLBM	Submarine Launch Ballistic Missile
SRAM	Static Random Access Memory
WH	Nuclear warhead or bomb

1. INTRODUCTION

There is renewed concern that our nuclear command, control, and communications system (NC3) might be attacked with cyber weapons, potentially triggering a war.[2] These concerns have been present since at least 1972 when the Air Force Computer Security Technology Planning Study found that the "current systems provide no protection [against] a malicious user."[3, p. 32] The situation has not improved in the intervening years! A recent Department of Defense Science Board report stated that they were "not prepared to defend against" cyber-attacks and that the military could lose "trust in the information and ability to control U.S. systems and forces [including nuclear forces]."[4, pp. 1–2] Clearly, something must be done to rectify the situation.

Because of this danger –possibly losing control over our nuclear forces—many people have suggested a variety of solutions to address this issue. Former Secretary of the Air Force, Mike Wynne, has suggested returning to analog computers, something that was state-of-the-art in the 1950s, to combat cyber-attacks on NC3.[5] Such computers use a set of discrete electronic circuit elements—resistors, capacitors, and solenoids—to process information. Fixed in place, these circuits cannot be "hacked" by malicious, off-site users because their physical position or parameters would need to be changed.[1] The philosophy behind such proposals is the realization that entry into any computer or communications system is inevitable. However, returning to analog computers would have tremendous limitations on how much information could be processed and would almost certainly require two entirely separate systems. One for processing highly classified information gathered about the real-world situation, and another completely separate system, for sending emergency action messages directing the targeting and launch of nuclear weapons. The lack of flexibility of such a system might likely limit the ability to tailor the U.S. deterrence.

The concept discussed here also assumes that our NC3 will be inevitably broken into and that our launch codes, and the ability to use them, must not depend on preventing hacking. Instead, the launch codes are not stored in memory in any computer but rely on unclonable physical devices (located at the National Command Authority) to generate them when and only when needed. These are interpreted only by the nuclear weapons themselves and then only by another physically unclonable device that generates the decryption key when needed. As will be discussed, this does not eliminate the possibility that hacking might mislead our leaders into believing either that we were being attacked when we were not or the opposite: that we were not being attacked when we were indeed being attacked. Those possible attacks on the "nuclear infosphere" must still be analyzed and defended against and are outside the scope of this paper.[2] Instead, concepts discussed here are intended to ensure that outside actors cannot launch our nuclear weapons nor prevent them from being launched.

In this structure, the warhead (or bomb) generates its own public/private encryption key without saving the private key anywhere, either inside or outside the weapon. It uses a Physical Unclonable Function (PUF) [6] [7] [8] which is an electronic circuit that reproducibly creates the same set of unique "random" numbers based on inherent variations in the circuits manufacture each time it is turned on. If a PUF is embedded in a warhead, these numbers could be used as the

[1] It is not clear how vulnerable such systems would be to malicious insiders.

[2] Since the situational awareness required to make such decisions is so far reaching and varied, it is impossible to process that information using analog computers.

seed for generating the public/private encryption keys. Such an implementation would improve the national security of the United States by mitigating several whole classes of cyberattacks on our nuclear weapons.

Embedded NC3 also has direct advantages to the most likely future arms control agreements through warhead accounting (as opposed to simply counting launch vehicles).[9] Implementing warhead accounting using embedded NC3 is the subject of this paper. Arms control applications for PUFs have been suggested in the past, though without the NC3 application.[10] This paper will briefly discuss the cyber threat and how implementing NC3 inside the weapon through PUFs might be used to lessen that danger. More research will be needed to take these concepts further. In particular, there are questions about the stability of PUF-based devices over the lifetime of nuclear weapons that requires further work to address. However, their potential seem worthwhile enough that their use in warhead accountancy be further explored.

2. CYBER-DANGERS

Nuclear weapons systems—including everything from early warning systems to national command authority centers to the delivery systems themselves—are increasingly dependent on computers. All of these components of our, and other nations', NC3 systems become targets for adversaries during and immediately prior to war. They are also subject to cyberterrorist attacks at any time. Andrew Futter[11] has suggested a systematic way of thinking about these threats and describes them by three general threat categories: misinformation introduced to the nuclear "infosphere" that might make command authorities either unaware of a nuclear attack or believe there is one when there is not; cyberattacks intended to disable or destroy nuclear weapons, preventing them from being launched when the national authority wants them to be launched; and cyberattacks intended to launch nuclear weapons under false circumstances, such as issuing counterfeit launch orders. These cyberthreats are illustrated in Figure 1, which shows these three categories and the various targets they might be aimed at with a notional assessment of the danger that might be associated with each.

	Cyber Threat		
Delivery System	Misinformation in the Nuclear Infosphere	Disable & Destruct Nuclear Weapons	Enable Launch Under False Circumstances
Missile Silos	Dedicated Comm links (Danger still present in computer systems)	Dedicated Comm links (Danger still present in computer systems)	Dedicated Comm links (Danger still present in computer systems)
SLBM	Communication by Radio	Communication by Radio	Communication by Radio
Strategic Bombers	Dedicated Comm links	Dedicated Comm links	Dedicated Comm links
DCA/Nonstrategic Weapons OCONUS	Comm links but susceptible to interference	Comm links but susceptible to interference	Comm links but susceptible to interference
Command Centers	High Consequences	High Consequences	High Consequences

Figure 1. Three arenas of cyberattack on any country's NC3 and their various targets. A notional assessment of the danger each target faces. Many of these targets' have dedicated communication lines but the Defense Science Board still is concerned about their control under cyber-attack. Those cyberthreats that might be addressed by moving NC3 into the warhead are circled in red.

Some of these attacks, particularly planting misinformation into the nuclear infosphere, are more relevant for national command centers than the nuclear weapons themselves. As an illustration of a cyberattack in the misinformation category, Futter cites an actual example of a cyberattack on an air defense system that intercepted signals sent from the radar to the command center and prevented the controllers from even knowing there was an attack underway. Others could be directly aimed at the launch systems themselves. It is these later cases where embedded NC3 becomes most important. If the warheads themselves generate public/private encryption keys—and do not share the private key with other elements of the nuclear enterprise—the cybersecurity of launch control can be greatly enhanced. Not doing so continues to leave the command system for launching nuclear weapons susceptible to a number of cyberattacks that have been known to jump even "air gaps" [12] [13] like those separating NC3 networks from the public internet.

3. IMPLEMENTING EMBEDDED NC3

Physical Unclonable Functions (PUFs) have been studied and implemented in personal electronic devices for nearly twenty years.[14] A PUF is an electrical circuit, such as a Static Random Access Memory (SRAM) chip, that utilizes the random but reproduceable initial state when it is turned on. These reproduceable, random set of 1s and 0s (one at each memory location in a SRAM) can be used to generate either a seed for an encryption key pair—one private and one public—generation or a set of challenge/response pairs (CRPs). The later are a set of randomly selected initial states of the PUF. In both cases, the random responses or states are caused by small manufacturing fluctuations in such things as transistor threshold values vary even within a production run of the chip. Turning the PUF on (almost[3]) always results in the

same physical state and since they cannot be predicted, they form the basis for authenticating the circuit, and the device containing it, as well as being used to generate public/private encryption keys.

In the implementation suggested here for using the PUF in NC3, the warhead uses the PUF to generate a "public" and a private encryption keys. The public key is sent to the national command authority while the warhead generates the same private key to decrypt messages each time the weapon is signaled. The weapon's public key is then used by the command authority to encrypt its commands to that warhead.[4] The national command authority further encrypts the Emergency Action Message to the warhead with its private key, which the warhead authenticates by using the command authority's public key. This is illustrated in Figure 2.

[3] There is "noise" in the generation of these physical states where a small number of states do not always return to the canonical value. Mechanisms have been worked out to compensate for this.[15]

[4] Once encrypted with the warhead's public key, only the warhead's private key can decode it. Hacking the command center and stealing the warhead's encryption keys does not risk enabling the hacker to launch nuclear weapons. Extreme care must, of course, be taken with the command center's private key. It is possible that a PUF implementation of that might also be a good idea.

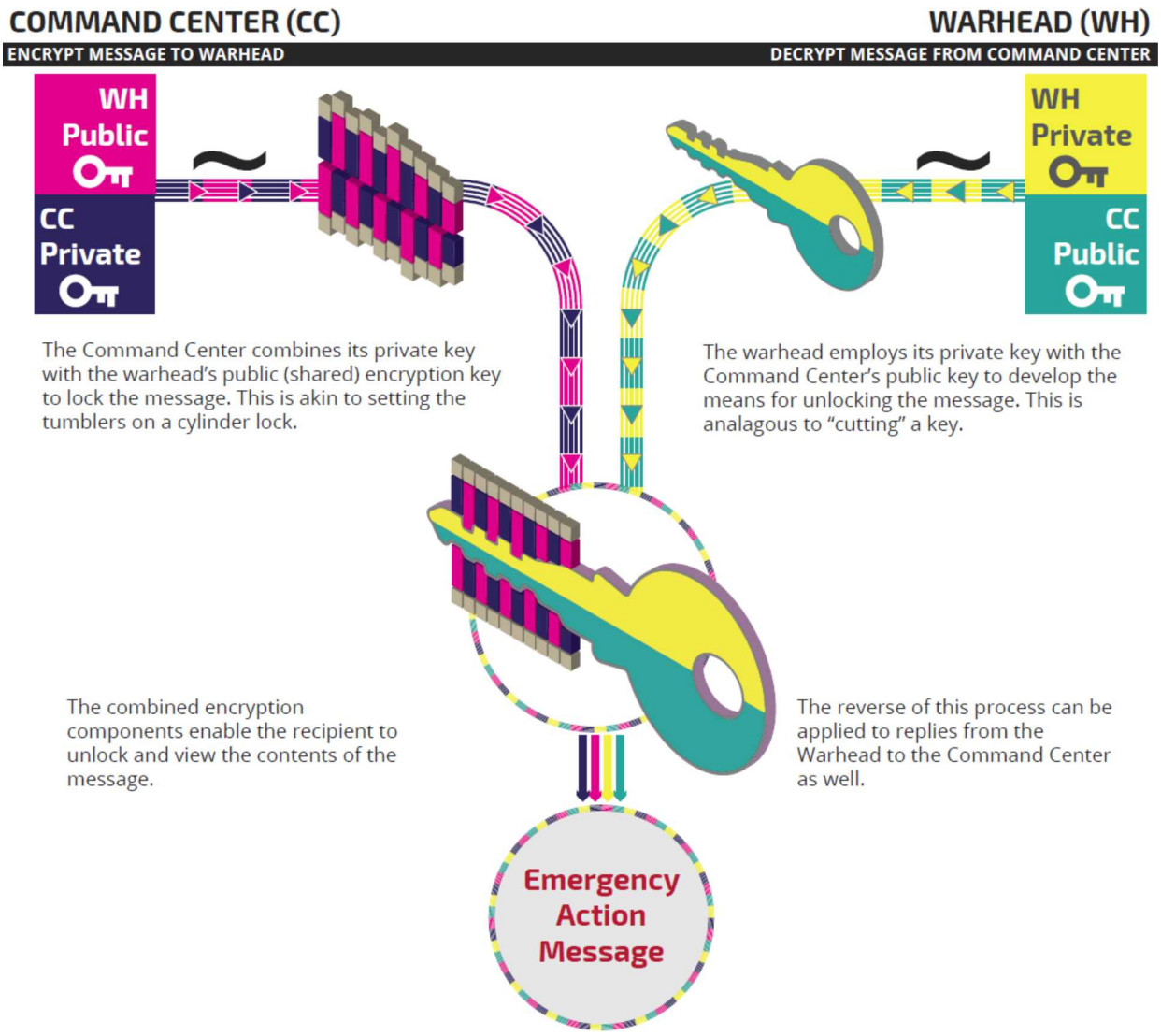

Figure 2. An illustration of how a country's national command authority sends a launch command (the Emergency Action Message, or EAM) to the warhead. The EAM is encrypted with the warhead's public key and the command center's private key in the upper left-hand corner. The warhead re-generates its private key—from the PUF-based device—each time it is needed and combines it with a stored copy of the Command Center's public key (upper right-hand corner). These are combined to unlock the Emergency Action Message in the center. See the text for a more detailed discussion.

Issues have been raised about how cloneable (or, rather, unclonable) these PUFs really are.[16] If an entity has unlimited access to the PUF, it should be possible to send it enough CRPs that another device could be constructed to respond to the inspectors in exactly the right way. This is why the PUFs used here will have a limit on the number of times CRPs can be sent to the warhead. As discussed below, once that limit is reached, the warhead has to be sent back to the warhead assembly/disassembly facility to have its PUF replaced. However, if the right type of PUF is used, this limit can be set high enough so that this should almost never be necessary. In fact, the limit can be high enough so that only if the owner of the warhead tries to hack it—while, for instance, trying to break the arms control aspects and cheat on any treaty agreement—will the warhead have to be sent back.

While it is theoretically possible to use the same PUF-based device for the NC3 and arms control mission, we have chosen instead to have two separate PUF-based devices in the nuclear weapon. One, the NC3 devoted PUF-based device, generates the public/private key pair and decodes emergency action messages from the national command authority. The other PUF-based device, the arms control-dedicated PUF, uses the communications infrastructure internal to the weapon that the NC3 PUF-based device does, is based on a large number of CRPs generated at the time the warhead was assembled. As will be discussed below, the inspectors will have a record of those CRPs but not the owner of the weapon. Cheating by testing the PUF with enough queries will be prevented by breaking the arms control PUF after a fixed number of queries have been sent to it. A possible implementation of this is discussed below.

Separating these two functions into two different devices completely removes any possibility that the treaty partner could access the weapon's private launch code during the proposed treaty-mandated manufacturing process while still facilitating the arms control aspects.

4. ARMS CONTROL OPPORTUNITIES: WARHEAD ACCOUNTING

As mentioned above, the most likely direction for future arms control treaties is a move from limiting the number of delivery systems a country may possess to limiting the actual number of warheads allowed. The basic idea behind these treaties is to prevent a treaty partner from either having extra warheads it has not declared or by ensuring that declared warheads have not been diverted to a covert stockpile. In previous concepts of operations for such a treaty, each country would periodically declare where each nuclear weapon was (e.g. if it was mounted on a missile as a specific base or in storage at a declared weapon depot). On a random, but controlled basis, inspectors from a treaty partner country would come and "verify" that a randomly selected subset of weapons declared to be at that facility were actually present. Most of the concepts for verification being studied involve some sort of radiation measurement with extreme care being taken to prevent classified information about the weapon from being revealed.[17] [18] [19] While these measurements can individually be done quickly (perhaps in a minute or less[20]), they all require the selected nuclear weapons to be moved to a central location for verification. This significantly limits the number of nuclear weapons that can be verified during any visit. Furthermore, few if any of these concepts of operations, envision verifying deployed warheads—an obvious gap if you are looking for undeclared weapons. As will be seen below, the confidence that a significant number of warheads have not been diverted increases rapidly with the number verified. Furthermore, any method for the discovery of warheads not declared at the facility is less natural under these concepts of operations.

The probability that there are K diverted warheads in an arsenal with a total of M weapons after N are authenticated (assuming no "dud" is found) is given by

$$P_K(N,M) = \frac{M-K}{M} \times \frac{M-K-1}{M-1} \times \frac{M-K-2}{M-2} \times \ldots \times \frac{M-K-N+1}{M-N+1}$$

Setting this expression equal to the desired confidence level can reveal how large a fraction of the entire stockpile might have been diverted. This is shown in Figure 3. If an inspection process could authenticate just 50 warheads, out of the assumed 1550 allowed in the arsenal, it would have a 95%[5] confidence level that not more than 5.7% (or 89) warheads could possibly have

[5] This means that there is only a 5% chance that the country could divert any warhead without it being detected. It

been diverted without this diversion being detected. Of course, if a higher confidence level is demanded, say 99.9%, then the inspectors might be concerned that more warheads had been diverted (in this case, 12.7% or 197 warheads).

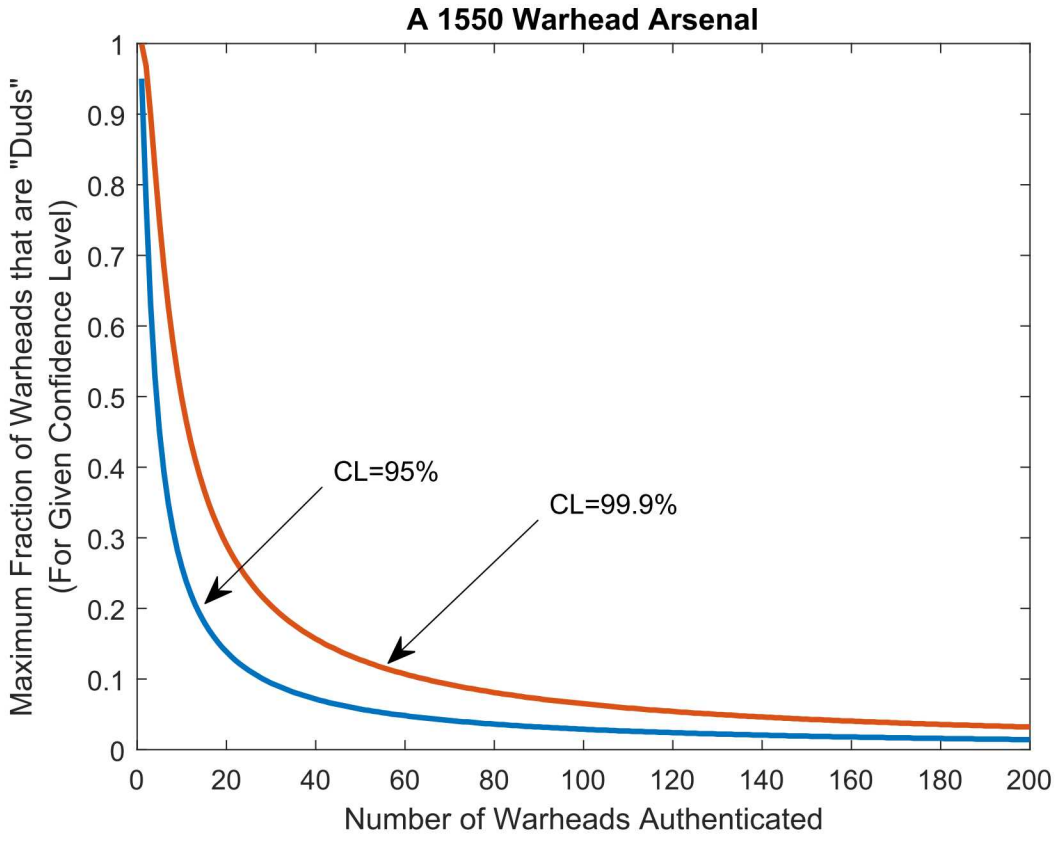

Figure 3. The maximum fraction of diverted warheads, for a given confidence level, as a function of number of warheads authenticated. The arsenal size, 1550, is the number of warheads allowed under New START, ignoring the complications of bomber counting rules.

Much of the power of warhead accounting comes from authenticating warheads over a period of time and at a variety of facilities. This is the way confidence is built up between treaty partners. However, it always pays to be able to authenticate more warheads at each facility and with a simple CRP interrogation it should be possible to measure a large number of warheads, including warheads mounted on missiles and even on alert (but not, of course, on SLBMs that are at sea). This PUF-based method of warhead authentication will greatly increase the immediate confidence that a treaty partner has not diverted any weapons. It will also be able to verify any warhead present at the facility—not just those requested based on declarations—is actually a warhead.

---

should be noted that many policy makers feel that a country would be very unlikely to risk even a 50% chance of being caught cheating on a treaty.

5. IMPLEMENTATION: HOW TO PREVENT THE WARHEAD FROM LYING

An immediate objection to this plan is the possibility that a fake warhead might lie about its identity. A treaty partner might wish to do this because it wants to risk having two (or more) warheads with the same "identity," thereby building up a larger arsenal than it has declared. Here, the treaty partner is risking that the inspectors might have a very small chance of testing warheads with the same "identity." (Of course, using PUF-based accounting increases this risk since so many more warheads can be verified.) Or the treaty partner might want to move a real warhead to a covert facility and, perhaps, declare it as being dismantled by sending a fake warhead to a dismantlement facility, again increasing the number of actual warheads in its arsenal above the agreed upon limit. However, there are both technical and procedural measures that can be implemented that prevent such lying. First, the PUF circuit—which would be developed and produced in cooperation with the treaty partners and therefore should be trusted by all[6]—will not allow the host country (the owner of the warhead) to interrogate the PUF enough times that it could be cloned. One possible implementation of this is illustrated in Figure 4.

Micro-Electro-Mechanical Systems (MEMS) have been developed in recent years to implement a wide variety of electronically triggered mechanical activities (or, in some cases, mechanically triggered electronic signals) on scales normally associated with the integrated circuit chips.[23] The implementation envisioned here uses a MEMS gear chain to count every time the power is turned on to a PUF, which is when the CRPs are generated. Electronics inside the PUF-based device will allow only one CRP to be requested each time the circuit is turned on. When the gears have counted the pre-set number of times, say a total of 10,000 CRPs, they will move the rod attached to them to break all the internal micro connections needed to interrogate the PUF. Presumably, 5,000 of these CRP interrogations were used when the PUF-based device was manufactured and the results given to the inspecting party for later use. That still leaves the inspectors another 5,000 times to interrogate the warhead during inspections. This number can be set large enough to allow all the possible times inspectors might interrogate the warhead while still being low enough that the host nation cannot use them to clone the device. The entire PUF plus MEMS system can be packaged on a single "chip" in such a way that opening it to reset it would destroy the chip, forcing it to be sent back to the warhead assembly facility.

[6] There have been previous projects that have explored joint development projects. The Joint Verification Experiment, where the two sides developed technical means of "calibrating" the seismic signals from underground nuclear tests at their respective test sites is one such example.[21] The Warhead Safety and Security Exchange (WSSX) project explored joint scientific research between Russian and US nuclear weapons laboratories where the countries worked together, among other things, on safety and security of nuclear warheads during transportation and storage; safety issues associated with the aging of high explosives; and the assurance of the safety and security of nuclear warheads during dismantlement.[22]

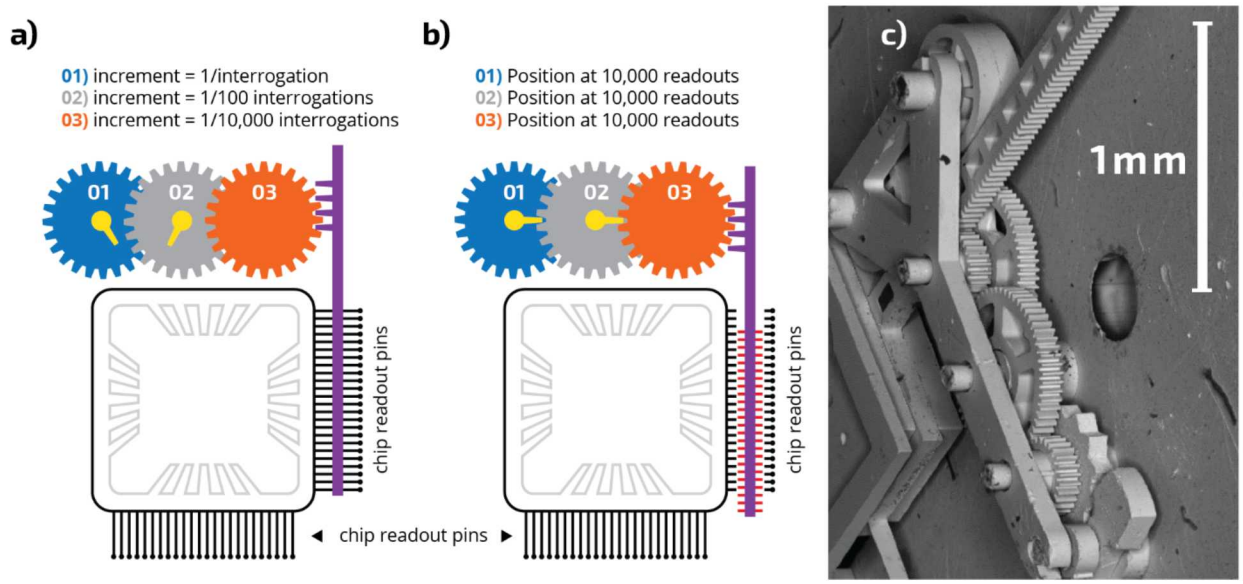

Figure 4. A possible implementation of limiting the number of times a PUF-based device can be interrogated for CPRs. Each time the PUF is turned on, a micromotor turns the blue gear in a) one notch. After 100 times the PUF-based device has been activated, the orange gear is moved one notch. After 10,000 times, the red gear in b) is moved enough so that the rod breaks all the microcircuit leads to the PUF chip. This prevents the PUF from ever being accessed enough that it could be cloned. Image c) illustrates an actual Micro-Electro-Mechanical System (MEMS) gear chain.[7] A 1 mm long rule is shown to indicate scale.

To fully implement this, the PUF would need to be placed in a location in the warhead which would require it to be sent to a warhead assembly/disassembly facility to be replaced. This could be ensured by including a simple radiation detector that would report whether or not a threshold amount of radiation was met or surpassed, though further work needs to be done on this assurance.

When the PUF circuits are manufactured, their library of CRPs is recorded in a secure memory storage unit with the capability of interrogating each warhead and authenticating them by comparing their responses to this library. The information they contain is prevented from being disclosed or changed by only communicating with the inspection tool through information diodes.[25] These units are stored in a tamper proof container and placed under dual control where both treaty partners need to be present to access the device.

Finally, in any treaty that counts warheads, there must be perimeter monitoring implemented that checks all the containers going into and out of the warhead assembly/disassembly facility without revealing any classified information (other than that a warhead(s) is present.)[8] When a new or refurbished warhead leaves the assembly/disassembly facility, the treaty partners monitoring the facility can authenticate each warhead—using the PUF mechanisms—as they leave. If there are doubts about whether or not a shipment leaving the assembly/disassembly facility contains a warhead, other measures can be taken, such as measuring the radioactivity or even a visual search. This perimeter monitoring is illustrated in Figure 5. This concept of perimeter monitoring is not new and was fully implemented under the INF treaty when U.S. and

[7] This image is from "Introduction to MEMS (MicroElectroMechancial Systems)."[24]

[8] Information needed to protect the warhead in transit—such as when it leaves the facility—can be maintained by staging the warheads at a secure part of the assembly/disassembly facility before they are shipped to their final location.

Soviet inspectors monitored everything that left the Votkinsk (in the Soviet Union) and the Magna (in the United States) missile production plants.[26, pp. 73–75]

Figure 5. Pantex, the warhead assembly/disassembly facility, is shown with a perimeter monitoring system shown (in yellow). The only gate allowed under a hypothetical warhead accounting treaty is indicated by the double bars in the right of the picture. Treaty partners would then interrogate every warhead leaving the facility.[9]

6. CONCLUDING THOUGHTS

We have discussed moving important aspects of NC3—the creation and utilization of each weapon's use control code—into the weapon itself without storing it anywhere. A specific implementation, using PUF-based devices, was used to implement it. PUF-based devices have a considerable number of advantages including: 1) the weapon provides is own private encryption key that does not have to be stored anywhere else; 2) the same unique private encryption key is generated each time it is needed (and hence cannot be accessed at other times by unauthorized users); 3) this concept mitigates the danger of either a malicious insider or a foreign or terrorist actor to launch or prevent the launching of U.S. nuclear weapons even if they have gained access to the NC3 system; and 4) this concept imposes no barriers to tailoring deterrence.

While much work remains to be done to prove that PUF-based NC3 in the warhead is feasible for both cybersecurity and arms control purposes, it appears possible that it could benefit both. As a cybersecurity measure, it mitigates two important cyberthreats: the risk of a disabling and/or destruction attack on nuclear weapons; and the risk of a cyberattack that might launch nuclear weapons under false circumstances. The same concept of PUF-based circuits could be used in an arms control role that, because of their speed of measurements and the small amount of infrastructure required, can be taken into warhead storage areas as well as, potentially, used on deployed warheads. This would improve the confidence all the treaty partners have that nobody is secretly diverting warheads out of the declared stockpiles. Radiation based warhead authentication cannot achieve the number of warheads tested and hence the level of confidence

[9] Figure is from Google Earth. Yellow "boundaries" are the author's addition to illustrate a possible arms control perimeter.

in the treaty partner's stockpile that the PUF-based warhead authentication can. Finally, both procedural measures very similar to those implemented in previous treaties and technological advances using MEMS technology can be used to ensure that the warheads are not simply lying.

7. REFERENCES

[1] SECRETARY OF THE AIR FORCE, "Nuclear, Space, Missile, Command and Control," Washington, D.C., Air Force Instruction 13–550, Apr. 2019.

[2] E. Gartzke and J. R. Lindsay, "Thermonuclear cyberwar," *J. Cybersecurity*, vol. 3, no. 1, pp. 37–48, 2017.

[3] James P. Anderson, "Computer Security Technology Planning Study (Vol. 1) Executive Summary," U.S. Air Force, HQ Electronic Systems Division, L. G. Hanscom Field, Bedford, Massachusetts, ESD-TR-73-51, Vol. 1, Oct. 1972.

[4] Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, "Resilient Military Systems and the Advanced Cyber Threat," Defense Science Board, Washington, D.C., Jan. 2013.

[5] Mike Wynne, "Trump DepSecDef Prospect Urges Federal Cyber To Go Analog," *Breaking Defense*, 23-Nov-2016. .

[6] T. Bauer and J. Hamlet, "Physical unclonable functions: A primer," *IEEE Secur. Priv.*, vol. 12, no. 6, pp. 97–101, 2014.

[7] B. Gassend, D. Lim, D. Clarke, M. van Dijk, and S. Devadas, "Identification and authentication of integrated circuits," *Concurr. Comput. Pract. Exp.*, vol. 16, no. 11, pp. 1077–1098, 2004.

[8] Ahmad-Reza Sadeghi, David Naccache, and Pim Tuyls, Eds., *Towards Hardware-Intrinsic Security: Foundations and Practice (Information Security and Cryptography)*, 2010th ed. Springer-Verlag Berlin and Heidelberg GmbH & Co., 2010.

[9] S. Pifer, "The Next Round: the United States and Nuclear Arms Reductions After New START," *Brook. Arms Control Ser.*, vol. 4, 2010.

[10] Janson Wu and Lee Clemon, "Integrating Potential Requirements for Arms Control Monitoring and Transparency into Nuclear Weapons Stockpile Planning (OUO)," Sandia National Laboratories, Albuquerque, NM, SAND2014-17937R, Sep. 2014.

[11] A. Futter and D. Browne, *Hacking the Bomb: Cyber Threats and Nuclear Weapons*. Georgetown University Press, 2018.

[12] M. Guri and Y. Elovici, "Bridgeware: The Air-gap Malware," *Commun ACM*, vol. 61, no. 4, pp. 74–82, Mar. 2018.

[13] M. Guri, B. Zadov, A. Daidakulov, and Y. Elovici, "xled: Covert data exfiltration from air-gapped networks via router leds," *ArXiv Prepr. ArXiv170601140*, 2017.

[14] B. Gassend, D. Clarke, M. Van Dijk, and S. Devadas, "Controlled physical random functions," in *18th Annual Computer Security Applications Conference, 2002. Proceedings.*, 2002, pp. 149–160.

[15] C. Herder, M.-D. Yu, F. Koushanfar, and S. Devadas, "Physical unclonable functions and applications: A tutorial," *Proc. IEEE*, vol. 102, no. 8, pp. 1126–1141, 2014.

[16] S. Katzenbeisser, Ü. Kocabaş, V. Rožić, A.-R. Sadeghi, I. Verbauwhede, and C. Wachsmann, "PUFs: Myth, fact or busted? A security evaluation of physically unclonable functions (PUFs) cast in silicon," in *International Workshop on Cryptographic Hardware and Embedded Systems*, 2012, pp. 283–301.

[17] J. Yan and A. Glaser, “Nuclear warhead verification: A review of attribute and template systems,” *Sci. Glob. Secur.*, vol. 23, no. 3, pp. 157–170, 2015.
[18] Craig R. Tewell, “Trusted Processing--Trusted Radiation Indtification System (TRIS) (SAND2014-18394PE),” presented at the U.S.-China Workshop on Monitoring and Verification of Nuclear Materials, 09-Oct-2014.
[19] P. Marleau and E. Brubaker, “An Implementation of Zero Knowledge Confirmation using a Two-dimensional Time-Encoded Imaging System.,” Sandia National Lab.(SNL-CA), Livermore, CA (United States), 2016.
[20] Thomas M. Weber, “how long does it take TRIS to make a measurement?,” 06-Jun-2019.
[21] C. Paul Robinson, “The Joint Verification Experiment and the Nuclear Testing Talks,” in *Doomed to Cooperate: How American and Russian Scientists Joined Forces to Avert Some of the greatest Post-Cold War Nuclear Dangers*, vol. 1, Bathtub Row Press, 2016.
[22] Paul C. White, “Nuclear Warhead Safety and Security: An Overview,” in *Doomed to Cooperate: How American and Russian Scientists Joined Forces to Avert Some of the Greatest Post-Cold War Nuclear Dangers*, vol. 1, 2 vols., Bathtub Row Press, 2016.
[23] Gilbert V. Herrera, “The History of MEMS at Sandia,” Sandia National Laboratories, Albuquerque, NM, SAND2011-7860C, Oct. 2011.
[24] “Introduction to MEMS (MicroElectroMechanical Systems),” Sandia National Laboratories, Albuquerque, NM, SAND2007-4521C.
[25] J. L. Cooke, T. M. Staples, P. A. Schmidt, V. H. Fleming, and J. Walsh, “Method For Connecting Unclassified And Classified Information Systems,” Oct-2009.
[26] Joseph P. Harahan, *On-Site Inspection Under the Inf Treaty: A History of the On-Site Inspections Agency & INF Implementation, 1988-1991*. Diane Pub Co, 1994.

DISTRIBUTION

1	MS0701	Jennifer Gaudioso	6160
1	MS1371	Dianna Blair	6830
1	MS1371	Amir Mohagheghi	6833
1	MS0899	Technical Library	9536 (electronic copy)

Sandia National Laboratories