"Larger Keys, Less Complexity"
A Strategic Proposition

Gideon Samid
Department of Electrical Engineering and Computer Science
Case Western Reserve University, Cleveland, Ohio
gideon.samid@case.edu

Abstract—**Cryptographic security is built on two ingredients: a sufficiently large key space, and sufficiently complex processing algorithm. Driven by historic inertia we use fixed size small keys, and dial up the complexity metric in our algorithms. It's time to examine this trend. Effective cryptographic complexity is difficult to achieve, more difficult to verify, and it keeps the responsibility for security in the hands of a few cipher implementers and fewer cipher designers. By contrast, adding more key bits over simple-to-analyze mathematics may guarantee a security advantage per increased key size. What is more revolutionary is the fact that the decision how much randomness to deploy may be relegated to the owner of the protected data, (the cipher user) which is where it should reside. Such shift of security responsibility will deny government the ability to violate its citizens privacy on a wholesale basis. In order to catch on, we need a new class of ciphers. We point to several published options, and invite a community debate on this strategic proposition**.

Keywords:—user-centric cryptography, randomness, mathematical intractability, combinatorics.

I. Introduction

Unwittingly we have navigated ourselves into a deep security hole. Cryptography proved to be so hard, so full of hidden cracks, that cyberspace dwellers gravitated towards a handful of ciphers, which we all use, and trust. These super popular ciphers claim their status on account of the long time they were exposed to public scrutiny. AES, RSA, ECC effectively brush off their competition and have become the security choice for virtually everyone. This gives hackers a stationary target. They can attack the math, or exploit any implementation flaw, and if they succeed, they can see almost everything that comes and goes in cyberspace. This unhealthy situation also allures governments to secretly collude with the few security providers to establish privacy busting side doors.

Given this vulnerability we can indulge in wishful thinking and describe a world where a user has a *'security dial'* at hers or his disposal. She can dial it up, or down as she sees fit, and do so with pin-pointed accuracy. Say, inject a sensitive business letter with medium security, but protect the financial data therein with extra high security. Let this "security dial" range from "zero security" (plaintext) to perfect security "Vernam grade" -- security state proven mathematically to be 'perfect' in as much as having the content of the ciphertext offers no advantage over knowing its existence only. We might consider an element of cost associated with the level of security we project on our data, and hence users would optimize their security strategy and decide per case how much they are willing to pay to buy the security they think they need. Let's top this imagined world with the premise that the level of data security does not leak, namely one has to actually attempt to cryptanalyze data in order to conclude how much security is there to overcome.

I submit that this "*dial-up security scenario*" will devastate the community of hackers and cryptanalysts. First, it will deny any government the ability to violate the security of its citizens on a wholesale basis. There will not be a handful of security providers to be in cahoots with. There will also not be any single mathematical puzzle that upon cracking it, all ciphertexts become plaintexts. In fact, an attacker, examining some encrypted data to crack, will not know if this piece of data is "Vernam grade" protected, in which case all cryptanalytic efforts are for naught, or if it is a bluff, namely superficially protected. Dark days are coming to security violators. That is, if this dial-up security scenario can be realized.

II. Migrating security from the algorithm to the key

We project security through (i) a large key space and (ii) through algorithmic intractability. The balance between the two is a product of historic inertia. Early in the history of cryptography keys were memorized, or hand-written, and hence they had to be small. This was compensated through ever-increased algorithmic complexity. The trend continued. While cryptographic keys increased modestly in size, the main thrust was invested in ever more complex algorithms.

These two elements of security have distinct characteristics. Any additional complexity to an algorithm is a-priori suspect of hidden flaws. So often in the history of cryptography, a brilliant design that was considered an intellectual feat, has turned out to hide fatal flaws that were exploited by a cunning adversary over a smug designer. This does not happen with the cryptographic key. As long as the random number generator is sufficiently robust, more key material means more

security -- no 'hidden flaws'. And what's more: you have to be a top-notch mathematician to dream up added algorithmic complexity. But to add random bits to your key, you just need to press a button.

The idea of giving the user the power to project more security by injecting more randomness may be extended to non-key options. While key bits must be shared by the parties, non-key bits may be deployed *unilaterally*, resulting in a larger ciphertext, for which only the recipient knows how to pare it down to the part that should be decrypted by the shared key. It is the transmitter who can best appraise the sensitivity of the secured data, and who can selectively increase security over the more sensitive data elements. Some of the ciphers discussed ahead can extend this ciphertext inflation into a continuous ciphertext flow, the contents of which may range from meaningless randomness to zero-inflated ciphertext. Such constant flow rate will prevent traffic analysis of the communication pattern.

As the key is allowed to grow in size (and keep that size as part of the secret), so one may expect the corresponding mathematical complexity to roll back. As is really the case for all the ciphers discussed ahead. This shift down in computational complexity reduces the risk of a mathematical shortcut, which is the hidden threat behind the more complex algorithms. The simpler the math, the less is there to shortcut. Computational complexity directly relates to power consumption, and hence the new growth area for cryptography, the Internet of Things, will have an extra argument to embrace “larger keys, less complexity” ciphers.

This disparity between these two pillars of cyber security suggests a strategic turn, away from the historic trend of small fixed size keys combined with ever more complex algorithms. Steering into a direction where the key is allowed to vary in size, while processed with a simple trusted algorithm. If we do so we allow one to increase security without fear of hidden math flaws, relying instead on the robustness of the source of randomness. And lo and behold, this new crypto vista will be one where the user, the owner of the data to be protected, has the power to decide how much security to bring to bear, simply by determining how much randomness to throw in.

III. Technological Parameters for "larger key please", "user-centric" security

To build this new security universe we need (i) readily available sources for high quality randomness, (ii) convenient, inexpensive means to store as much randomness as needed (iii) high-throughput communication channels to pass around the necessary randomness, (iv) ciphers that work efficiently with as much key material as is served on them, (v) effective communication protocols between transmitter and recipient to coordinate the secure communication.

We argue that all these parameters are in place. Technology-wise we are ready. The challenge is to face the resistance of the power-houses of today's security marketplace, where a few vendors susceptible to government pressure, control the security of the citizens. History proves that technology can’t be stopped, but it sure can be denied a quick triumph. We present ahead a few published "larger key please", "user-centric" ciphers.

IV. Literary Track Record

Back in 2001 The Second International Conference in India published a pioneering article: "Re-Dividing Complexity between Algorithms and Keys” [1]. It raised the specter described herein. Many cryptographers have treated it as forgettable curiosity, but some like Bruce Schneier, have been concerned, and even alarmed. In 2002 the cipher now known as "Walk in the Park" [6] was published, [2], and a version of it was patented in 2004 (US Patent #6,823,068). It was based on a simple algorithm that tracked a pathway on a map (a graph), switching between describing it as a series of vertices (plaintext) to a series of edges (ciphertext). The map was the key. The larger the map, the greater the security, while processing time remains proportionally related to the size of the message. In 2008, and then in 2012 two patents were issued (US Patents #8,229,859, #9,471,906) for randomness based digital money, where security is determined by the measure of randomness deployed in the minting process. In 2015 another cipher was presented [3]; based on an effective transposition algorithm where n data items face a key space of size $|K|=n!$ to cover all possible permutations. The polynomial processing effort allows for a user-determined security level, by deciding the size of permutation blocks (n). In 2016 the Cyber Passport cipher was published, [4], achieving security through breaking a bit string to various size substrings which are then transposed. The user determines the size of the transposed string, and the corresponding key size. In 2017 a new cipher, BitFlip, was published, [5], and then enhanced [7]. Its algorithm is very simple, (and hence fast). It requires only counting, comparing, and flipping bits. It is based on a key of user-determined size, and for which the processing effort is strictly polynomial. Performance validated by the German Bureau of Standards, TÜV.

V. Prospective Path Ahead

As quantum computers are secretly being developed around the world, and as cryptography increasingly underlies our civil order, the inherent flaws of mathematical intractability cryptography will come to the fore. The flip side of the "old and trusted" ciphers is that, they have also been at the cross-hair of world-class cryptanalytic shops for that long, and by now are probably secretly compromised. Add to this the public resentment to government snooping after its citizens, and the terms are ripe for this strategic turn to emerge.

REFERENCES

[1] Samid, 2001 “Re-Dividing Complexity between Algorithms and Keys”: http://link.springer.com/chapter/10.1007/3- 540-45311-3 31#page1

[2] Samid 2002: " At-Will Intractability Up to Plaintext Equivocation Achieved via a Cryptographic Key Made As Small, or As Large As Desired - Without Computational Penalty " G. Samid, 2002 International Workshop on CRYPTOLOGY AND NETWORK SECURITY San Francisco, California, USA September 26 -- 28, 2002

[3] Samid 2015: “The Ultimate Transposition Cipher (UTC)” Oct. 2015 International Association of Cryptology Research, ePrint Archive https://eprint.iacr.org/2015/1033

[4] Samid 2016: “Cyber Passport: Identity Theft Strategic Countermeasure Cryptographic Solutions; Administrative Framework”. G. Samid International Conference on Security and Management (SAM'16) http://worldcomp.ucmss.com/cr/main/papersNew/LFSCSREApapers/SAM 6275.pdf

[5] Popov Samid 2017 “BitFlip: A Randomness-Rich Cipher” https://eprint.iacr.org/2017/366.pdf

[6] Samid, 2016 “Cryptography of Things” Int'l Conf. Internet Computing and Internet of Things | ICOMP'16 |

[7] Samid, 2017, “Threat Adjusting Security” https://eprint.iacr.org/2018/084.pdf

[8] Schneier 2008: “Schneier on Security” Wiley Publishing. Inc.

[9] Shannon 1949: “Communication Theory of Secrecy Systems” Claude Shannon http://netlab.cs.ucla.edu/wiki/files/shannon1949.pdf

[10] Smart, Nigel 2015, “Cryptography (an Introduction)” 3rd Edition http://www.cs.umd.edu/~waa/414-F11/IntroToCrypto.pdf

[11] Vernam 1918, Gilbert S. Vernam, US Patent 1310719, 1918.