Math Resistant Cryptography

"Trans Vernam:" a New Class of Ciphers may bring the current era to its end

Encryption technology today suffers from an unspoken vulnerability: math-attack. Security is based on mathematical complexity, which becomes math-simplicity in the eyes of a mathematician smarter than its designer. For this very reason all governments recruit their smartest mathematicians to secretly crack those ciphers. The Germans did not know how smart Alan Turing -- their WW-II crypto attacker -- was, and lost the war. Likewise we don't know how smart is *our* attacker -- to what extent has our privacy been violated. In reality, we know. We can't prove it, of course, but those legions of dark room mathematicians don't work for nothing.

So what can we do? How do you remove math vulnerability?

By avoiding math complexity!

Mathematical complexity is where our vulnerability lies. If we limit our ciphers to very simple math -- then we remove the risk of making it simpler. A fragile box left on the top shelf is at risk of falling down and cracking. The solution: leave the box on the floor -- no more risk of crashing to the ground. This is the new cyber strategy -- use math so simple, that smart attackers cannot undercut it.

But if the math is so simple, then the cipher will be cracked straight on!

Well, here comes the other part of the Trans Vernam Solution: the simple math is applied onto large amounts of randomness -- making it necessary for the attacker to figure out all this randomness. And since we are confident that the attacker will not use more efficient math than we do (he cannot undercut us because we are too simple to go simpler), we can then very credibly estimate how fast will our attacker break our secrecy. And what is more -- we can very easily make the task more difficult for our attacker, by simply piling on more and more randomness. And what is so attractive about all this, is that it is easy to do, so easy that the user, the secret owner, can do it all by herself. To make the math more complex, you need a professional mathematician, to make the Trans Vernam cipher more complex you just need to line up more random bits! And remember -- at any point you can credibly estimate how secure you are. And if needed, you can throw in so much randomness that your secret will be "Vernam Secure" -- which means mathematically secure. Absolutely secure -- regardless of how smart or how powerful your attacker. Gilbert S. Vernam was the first to offer such a cipher. The new crop, called "Trans-Vernam," are more elegant, more versatile, more convenient products, well positioned to revolutionize cyber security. Imagine a world where any John Doe can protect his privacy with a Trans Vernam cipher, and decide on his own how much randomness to use, how much secrecy to put up -- and be peacefully assured that all the smart hackers out there are destined to fail. Math is not intimidated by force. When a mathematical proof keeps your secret - it is kept a secret.

All these wonders are enabled through technological advances that emerged very recently. Mainstream cryptography has not yet realized that the dominance of mathematical complexity is quietly being challenged.

Reference:

"Randomness Rising"
14th International Conference on Foundations of Computer Science (FCS'18: July 30 - August 2, 2018, Las Vegas, USA)
G. Samid, "Randomness as Absence of Symmetry",
THE 17TH INTERNATIONAL CONFERENCE ON INFORMATION & KNOWLEDGE ENGINEERING (IKE'18: JULY 30 - AUGUST 2, 2018, LAS VEGAS, USA)
BitFlip: A Randomness Rich Cipher.
Threat Adjusting Security.
Emergence of Randomness.
Equivoe-T: Transportation Equivocation Cryptography
Denial Cryptography based on Graph Theory
The Ultimate Transposition Cipher (UTC)
T-Proof: Secure Communication via Non-Algorithmic Randomization
Cryptography of Things: Cryptography Designed for Low Power, Low Maintenance Nodes in the Internet of Things
Redividing Complexity Between Algorithms and Keys
Encryption Sticks (Randomats)
Essential Shannon Security with Keys Smaller Than the Encrypted Message
Tailored Key Encryption
Cyber Passport: Preventing Massive Identity Theft
Shannon Revisited: Considering a More Tractable Expression to Measure and Manage Intractability, Uncertainty, Risk, Ignorance, and Entropy
Hush Functions Extended to Any Size Input versus Any Size Output

Gideon Samid, CTO, BitMint
gideon@BitMint.com