When Vernam is not Enough

How can the celebrated One-Time-Pad Vernam cipher not be enough?

Hasn't Claude Shannon proved that Vernam is unbreakable?

Vernam is the only cipher that comes with mathematical proof of efficacy: The Turing machine algorithm that resists any attack from quantum computers and beyond.

How is that not enough? Anyone who needs to absolutely guarantee communication security is using no other means. US nuclear submarines communicate Vernam. Embassies in Washington DC fully realize that any bit that goes in and out of their building is NSA 'vacuum cleaned' and hammered with the most advanced computing machinery -- they use Vernam and sleep well at night.

Good
Better
Best

Ordinary Cipher is Good. Except it eventually yields everything

Vernam Cipher hides contents but leaves foot-prints (meta data)

Unary Cipher is clean, as if nothing ever happened

How then can Vernam be improved upon? The sobering reality is that cyber spying is mainly traffic analysis. Cracking code is too laborious and very often superfluous. Productive spying is carried out by tracking who one talks to, how often, how much -- after talking to whom else, etc. Known as "meta data," these cyber footprints are crunched by ever improving AI machines that strip their targets like onions. So while it is very nice that Vernam hides content perfectly, as far as footprints are concerned, it leaves them behind like any other cipher. Enter BitMint Unary Cipher. It may deliver the same mathematical secrecy as Vernam, but it does hide its footprints. The user of the BitMint unary cipher denies its snooper any information regarding who they talked to, how much they communicated, how often -- nothing leaks. The Unary users keep their trackers blind. And since this meta data is the stuff cyber espionage operates on, eliminating it -- eliminates spying. Freedom, privacy, and old-fashioned confidentiality are here again.

BitMint Unary Cipher represents a series of Trans-Vernam ciphers developed by BitMint. Security is projected through lavish use of high-quality randomness – by the user, who knows best how sensitive is the message they send over insecure lines.

https://www.BitMintalk.com