



What is LINTHRIDICK

1. Super compression!
Using QiS Losses CPU Compression process.
Using QiS Polymorphic Digital Signature
To achieve super compression, 3,000,000 to 1 avg. More data, more compression.
2. It's FAST.

Example;
Tickets or could be a serial number, for Cash, Credit Cards, Hardware, Software, Contracts, Stock Certificates, Warranties, Policies, navigation, profiles, positioning, dual 2FE identification with password to CAG/EAC process or for anything and mixed. Able query in parallel with out scanning, only limited by the network and hardware use, infinite in speed.
3. In your database, the following information is stored, based on usage for example Event tickets are used in this example. Ticket Set Id, Date and Time of Venue, and the ticket totals. That is it! [1020],[20201225],[11:00AM],[2,000,000]
4. Using Linthridick, simply calculate, and compare Linthridick ID to the ticket.

1 Try, no collisions, no permutation alternatives, calculates, formulate exactly the ID number of the Ticket number 1,2,3,3, ... 1,984,615, along with Ticket ID: X2PVY
5. If your using 3rd party service, you can use our check your ticket to see if it locked. Don't buy it if it's locked, counterfeit. Buy it then lock it.

Works with QRcodes, Barcodes, Email, Phone numbers, Text messages.
Since Ticket ID's not stored in the database, your employees cannot copy it or counterfeit it. The Insider threat is eliminated.
6. When Ticket is used, indicate in DB Ticket Id is Used, that it. Get the ticket, not that counterfeit.

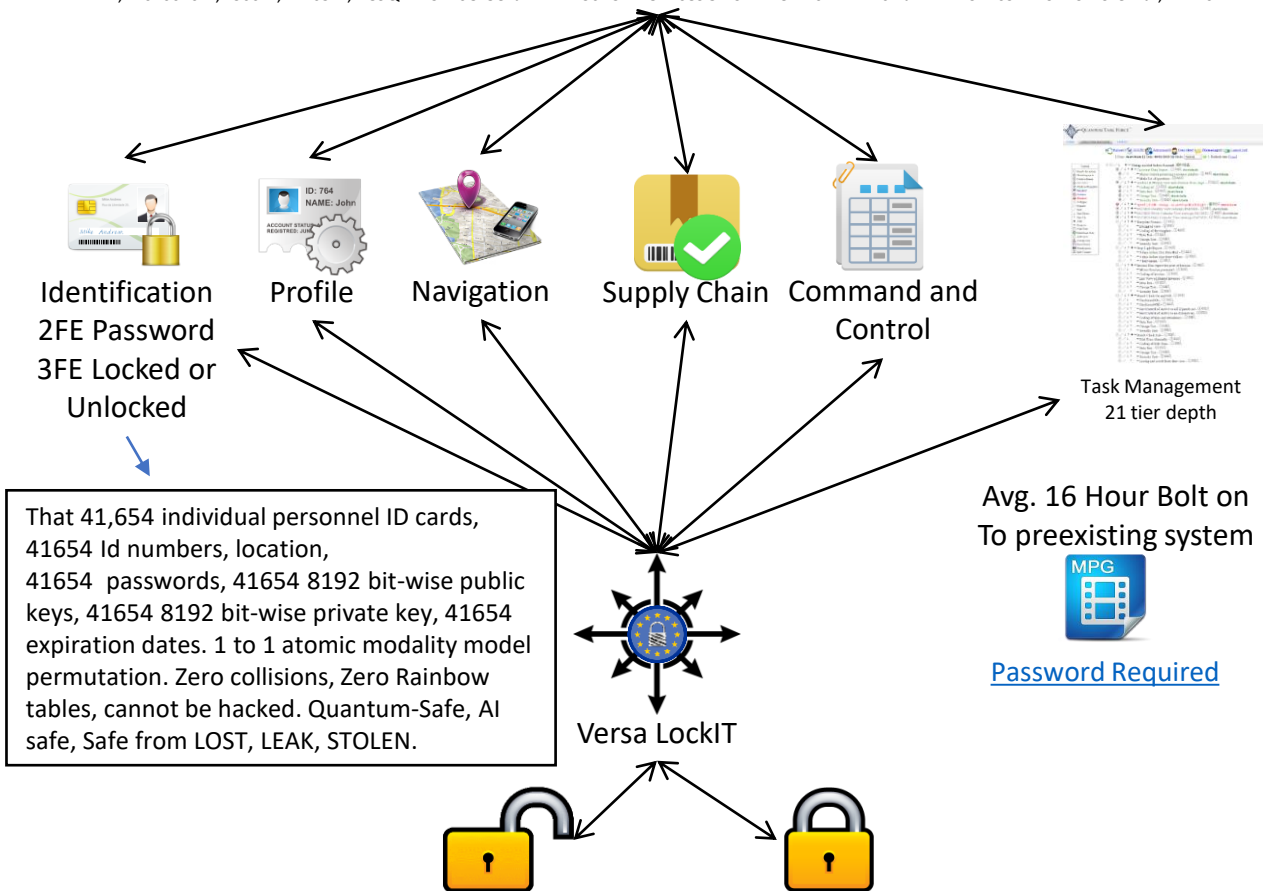


Super CPU Compressed DB Encrypted Entry. IoT, Desktop, or Cloud.



The only entry in the database "COMPRESS MODALITY MODEL"

"1", "20200101", "3601", "41654", "89QMIR3440OI082JETNN4P36D5PMGB1089GMSRPF8M20LR1EDK6IRJ7EHNSMB109HINCPBC419IOL2J", "HLK0"



Secured by 8192 bitwise Polymorphic Digital Signatures, with transaction recover keys of 8192 bitwise.



QiS™

QUANTUM INFORMATION SECURITY™



LINTRIDICK™

Reversible Atomic Digital Signature (RADS)

ODS8192 standard hash;

5fe4178509c34879191c035502a8baa64ef3be1eec7a615896340160708f2c80e9e2cd6c233de3b9affb2b841f4
 a5e08d65bc005a162285ac99cad2e755dfc67a489f61a2a40b7a00418f4077251dd201b3a41c2637d4f9bb1331
 4b247c88ce8e0b36d5ccf36ea8d52d3c1da9700664595a3b4290f733ce7229e15883877bc747692e6dfa9d137ff
 576b9424d07f217e8e6a16c7ccf746a70bdeac3efe913f81ab25f56f0ca286d868bf0d30ed359fc4ae504399fa1d
 267c2d820ec6f8c5f1bbaace782f32e5b642d798cb93cab8db8bb0870ad59053d4e14427dc4dee06645449d256
 d9f9f0bd4b396559fd12eb4c11b57bef3b9a133183a59d6ef2108a69719fcdc1734cc746e28baa3b1d883c701b8
 7b611068c5fbbcc09032310f3e82ccca0ba60a3a836eb0a265b8796da0f447664d2934cbf5ef6c8a94f8ea0fc5b
 a85dcb784bd9c976a367c3fe9e7501ae0ee6192c82fdb0d01f60762d6ad49fd8e1274542596d91e5a75956076c
 000af931319b943b19e86ebd76bb2debf99dd054e8951a3d4270cc24b2458ae16b455045d3de568da5bc977b3
 417b72ab0e02a5382602307102117584871102010425070027016760771414001154aa16f401c4f2bff1
 f446432a756edd2c9191217afcd031e3a9f
 12cce451518f0e6d
 737d18888ec6915f
 5f62697ce07e509a
 f4ba9d8c257dfc54a41a6e92bac9bef25b1d33ccfee49dc32d775783f0c8f2e60cb66caea2065db7994f08f1019
 acd2df41d173b22904828b6e694cc53f32413676154232a466a00fac77e95b3f8ed34b250f77ce1d0fd6c3584c9
 123afc6882c38c04f574af7be7aba170da1e15471105adc1b48683eb10969efe36dbb9319cfb52a7b0ec52108bc
 d92512f1ca8900eca37a9de58c95dd1f3a1f59c284525b88c3edcd37e2edb18095a98672ab68aaa84d906d7ed4
 01e437a216d57f6010de6bbad6e4accb2319368b4991665ab34e2c8c3f1e03bdd1930c18db11bd8899d50f7f4a
 388556c050bd43c17efc091c23f61423978bc46005fdacf1f141a871172027f327b4d0fe541d2ebfa64e7470480
 dffd22864e776f9ac5d5cb6a945e2bd015032496a52074b02656076212fbfe736bbdb35c59e9352d3882e8d6e4
 8f7db99ba28e4c81e3f9ffc6b5c44433853d63ae0c9fba1308549769a07076f03a2cb795c7af5336f8aC66834fbf
 7c4b9e7579a4fcbe60291deaae4971ce0aa7e1a623f25b4827

Reversible Atomic Digital Signature

RADS Stored Transaction space;
 5956076c000

This computes to that and is Atomic.

ODS8192 90X more compressible and 16X stronger in bitwise detection compared to SHA512 & KECCAK512. RDS 100% Round trip verification process achieve CPU compression.



Commence Digital Fencing



Setup Signatures / Fingerprint

Input a word or data, that will be signed / digital fingerprint, then it will be inserted into a rainbow table. All signature types will be used, in an attempt to find a collision. The victor will be the Signature/fingerprint that can be verified by the A. word/data and B. the digital signature/fingerprint, finally, A creating duplicated digital signature/fingerprint and compare B to C. the newly created digital signature/fingerprint. D. Testing the signature confirmed Signature for security against rainbow table attack. Totalling the score of not found in the rainbow table. The digital signature/fingerprint with the most not found digital signature/fingerprint in the rainbow table wins. The results placed in a leader board for 1st, 2nd, 3rd place.

Data or Word: Sig / Fingerprint



 HmacSHA256	 EDONR512	 SHABAL512	 HAMSII	 KECCAK512
 SHAVITE3	 FUGUE512	 ODS8192V3	 LUFFA512	 JH256
 SIMD512	 SKEIN1024	 ECHO512	 BLAKE2	 GROESTL512
 CUBEHASH	 BLAKE512	 SHA512	 MD5	 SHA256



COMPARE AT

Feature	Polymorphic	NIST Legacy
Bitwise	Y	Y
Native Encrypted	Y	Y
3 Factor Authentication Internally	Y	N
3 rd Party Exposure Eliminated	Y	N
Bad Actor protection	Y	N
Bitwise to the size of the signature	Y	N
Compression	Y	N
Default profile customizable	Y	N
Default programable customization	Y	N
Detached BlockChain	Y	N
Dmask Customizable	Y	N
Email Phishing Defensible	Y	N
Forever Immutable	Y	N
Framework	Y	N
Ghosting Attack Eliminated	Y	N
Incoming binary trap consensus	Y	N
Insider Threat Eliminated	Y	N
Keygen and Warez attack Eliminated	Y	N
Linthridick	Y	N
Lintricity	Y	N
Ofiscatable	Y	N
Origin Nth permutation control	Y	N
Outgoing binary trap consensus	Y	N
Overpowered authority attack protection	Y	N
Parallel Processing	Y	N
Protected from middle man attack	Y	N
Protection from malicious users	Y	N
Rainbow Table Defensible	Y	N
Random Asynchronist Signature	Y	N
Reversible Atomic Digital Signature compatible	Y	N
Safe from Artificial Intelligence	Y	N
Safe from being leaked	Y	N
Safe from being lost	Y	N
Safe from being stolen	Y	N
Safe from brute force attack	Y	N
Safe from computer viruses	Y	N
Safe from Hackers	Y	N
Secure from malware viruses	Y	N
Self Entangle Chain of Authority	Y	N
Social Engineering Defensible	Y	N
Spear Phishing Defensible	Y	N
Third-Party Verification Eliminated	Y	N
Unidirectional Entropy deterministic	Y	N
Whaling Defensible	Y	N

Quantum Information Security (QiS), P.O. Box 407, Oconomowoc WI 53066
 Wisconsin: +1(262) 370-1624, Nevada: +1(702) 518-9092, Seattle: +1(206) 383-9160
sales@quantuminformationsecurity.com



NO COLLISIONS

Polymorphic Digital Signature

No collisions in Polymorphic digital signature and hash.



Polymorphic Digital Signature has 1 more benefit. It has “**Zero Collisions**”. It has 3 tier one-way encrypted hash / shape shifter result system. 100% Serialized, 100% Encrypted, 100% ambiguous, and throws away “**randomly**” certain number parts of the digital signature so that cannot be rainbow table, based on size.

Legacy systems have collisions.

Classic example of a collision:

<https://www.mscs.dal.ca/~selinger/md5collision/>

Collision Attack.

https://en.wikipedia.org/wiki/Collision_attack



THE PROTECTION

Polymorphic Digital Signature

Protection and Prevention automatic vigilance.



Rainbow Table Attack Eliminated



Secure from Lost, Leakage, Stolen



Social Engineering Eliminated



Safe from Hackers



Email Phishing Eliminated



Protection from malicious users



Spear Phishing Eliminated



Secure from malware viruses



Whaling Eliminated



Immutable and 8192 bitwize



3rd Party Exposure Eliminated



Middleman Attack Eliminated



3 Factor Authentication Internally



Ghosting Attack Eliminated



Third Party Verification Eliminated



Unidirectional Entropy deterministic



Safe from computer viruses



Bad Actor Eliminated



Insider Threat Eliminated



Overpowered authority attack Eliminated



Safe from brute force attack



Keygen and Warez attack Eliminated



Safe from Artificial Intelligence



The SECURITY

Polymorphic Digital Signature

Polymorphic Digital Security and Methods of Thereof



Default security setting is 8192 security bitwise or 1024 bytes or 1 kilo byte.

Typical Usage of

Polymorphic Digital Security is system login using the digital Signature.



Using a simple Soft token file, like a certificate or a PEM file.



Typical USB device can be used as hard token.



Simple Sim Card placed inside of Identification and use as Cage Card



Still requires a valid Username and Password, creating simple and effective 3FA system with out and any external resource or certificate of authority.



Some USAGES

Seemly endless supply of data collection sensor and package combinations.

Token Control
CAG Control
Social Sensing
Supply Chain
Custody Control
Serial Inventory
Voting
Point of Sales
QRC reader
Crypto Tickets
Radar detector
Geiger counter
Smart contracts
Crypto Receivers
NFC ID
Chip Reader ID
QR Code ID
Currency
Mass Bio Classer
Mortgages
Bank Accounts
Savings Accounts
General Loans
Home Loans
Car Loans
Credit Cards
Debit Cards
Car Titles
Boat Titles
Home Titles
Medical Records
Licenses
Corporate Entity's
Etc.

Localized Intrusion Detection System
Biometric Enhancement Sensors
Geo ID location recorder
Common Track Protocol
Lightweight and Compact Beam Projector
Provably Unclonable Functions
Instruction Protocol, 100% AI, Virus safe
Quantum Locks, Validation, Verification
Tandem ID check, facial recognition check
Autonomous Measurement and Reporting
Small Airflow Measurement System
Drop in HIVE Data Servers
Airborne Infrared Signature
Airborne Abstracted Signature to ID Object
Infrared Detector & Monitoring
Inertial Measurement Unit
Lock control, doors, windows, etc.
Switch control, On/Off, lights, water, etc.
Damage or Debris detection
Music storage & player with DRM control
Video storage & player with DRM control
Photo storage & player with DRM control
Books storage & player with DRM control
Blackbox for Planes, Trains, Ships, Cars, etc.
Farmer grow, PH, Moisture, temp, etc.
Lic. Fish Catcher, weight, picture, fish.
Attic Watcher, vermin & change detection
Crawl space, vermin & change detection
Water Heater & plumbing leak detection
Autonomous insect killer, 1-watt laser
You got mail, mailbox watcher
Info grabber, looks like rock
Smart Contracts and Regulations Controls
Etc.

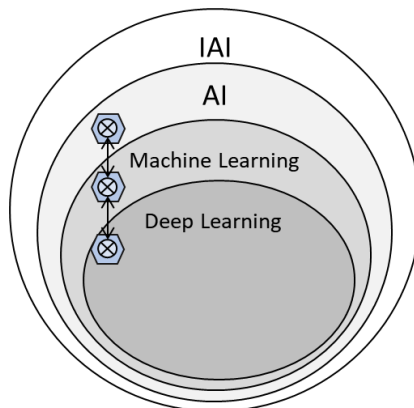
Snap to Devices
W-Band RF Monitor
Drop in HIVE network
Inventory buffering
Time and Attendance
Micro Weather Station
Temperature control
Security, the stick
Sensor Data Confidence
Isolate remote monitor
LF sound detector
HF sound detector
Audio Lie detector
Thermal Lie detector
Metal detector
Optical Obfuscator
Optical Abstractor
Optical Thermal ID
Audio Obfuscator
Audio Abstractor
Audio Range and ID
Checking Accounts
Trade Names
Slogan Names
Birth Certificates
Death Certificates
Office Building Titles
Mineral Rights
Land Titles
Water Rights
Serial Numbers
Warranty Information
Leasing and Rentals
Etc.



The Specification

Polymorphic Digital Signature


1. The framework will support, No expire feature.
2. The framework will support, individual expirations, up 65,535 days also know as recession control.
3. Each signature individual assigned a category. Example, Identification, Navigation, Profiles, Tickets, Serial numbers. Up to 256 categories.
4. Each signature can be assigned a function. Up to 4.2 billion.
5. Each signature represent all legacy signatures individual or at the same time, randomly.
6. Each signature has ability of Nth control. Replacing the need of Line Graph Math, with Line graph poly. An atomic modality model, 1 to 1 permutation mathematical/textual deterministic.





Thank You

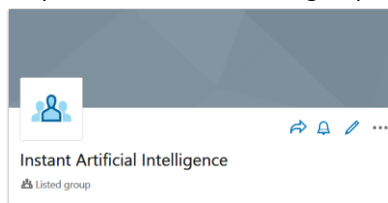
Name	Chris Thorsen CEO & Founder of Short Chain™ ct@quantuminformationsecurity.com +1(262) 370-1624	
Highlights	<ul style="list-style-type: none"> • Co-Founder of Short Chain™ • One of strategic developers of the Atomic Blockchain toolset • 27 years of cutting-edge Technology and OEM products with Intel and Microsoft. • 12 Identifying and developing strategic partners. • 10 years CEO/President and leading the way. • 12 years of Consulting and Business development. 	

Name	Timothy Fletcher CTO & Founder tf@quantuminformationsecurity.com +1(206) 383-9160	
Highlights	<ul style="list-style-type: none"> • Founder of Short Chain™ • Original developer of the Atomic Blockchain toolset • 27 years of digital signature development expertise. • 20 years of Artificial Intelligence automated programming. • 18 years Chief of Security, IT Director, FSO, and Computer Scientist. • Patent holder & Inventor. 	

<https://www.linkedin.com/groups/13857075/>



<https://www.linkedin.com/groups/13870025/>



Under Construction