THE CROWN SOVEREIGN

Freedom Resides in the Sovereignty of the Digital Domain

Lite Paper
2021

CROWN STERLING LIMITED
www.crownsterling.io

TABLE OF CONTENTS

I. ABSTRACT

The next generation of data security relies on future-proof cryptography thats ensures the timeless protection of data. It is essential that cryptography be evaluated with respect to the growing capabilities of quantum computers. One of the only proven encryption protocols left that remains unconditionally resistant to quantum technology is One-Time Pad encryption. While One-Time Pad encryption enables quantum-resistant protection of data, it has not previously been fit for scalable use because of the large size of the associated private key, which is required to have at least as many characters as the dataset itself.

Leveraging new discoveries in compression technology and mathematical constants, the team of mathematicians at Crown Sterling have engineered CrownEncryptOTP™, an enhanced One-Time Pad encryption technology that allows for practical and scalable use of One-Time Pads. Crown Sterling has also designed, tested and launched the Crown Sovereign, a cryptocurrency that employs CrownEncryptOTP™ as its encryption protocol, making the token resistant to the capabilities of quantum computers. The Crown Sovereign serves alongside the Crown Sterling Wallet, which is an expandable platform for the encryption, storage, and quantum-secure transmission of data. CrownEncryptOTP™ serves as a much-needed solution for outdated encryption protocols, and the Crown Sovereign achieves ever-resilient value as an intermediary for data storage and distribution.

II. CROWN STERLING SUMMARY

Based in the United States, Crown Sterling delivers next-generation cryptography in the form of random number generators and encryption products. From irrational numbers that modernize existing cryptography, to leading-edge encryption products and developer tools, the team of mathematicians at Crown Sterling are changing the face of digital security with non-integer-based encryption algorithms that leverage time, artificial intelligence and irrational numbers. Crown Sterling has successfully engineered the first viable utility for One-Time Pad encryption, coined CrownEncryptOTP™, and built a quantum-proof digital asset, the Crown Sovereign (CSOV). Crown Sterling has also pioneered the “Data Bill of Rights,” declaring that digital assets, including the data created by tracking and monitoring one's online activities, are the intangible personal property of original producers and are therefore protected under various existing laws in the United States and around the world.

“With data now globally recognized as the world’s most valuable asset, the stakes for quantum-proof encryption have never been higher or more necessary.” said Robert E. Grant, Founder and CEO of Crown Sterling Limited LLC.

a. Mission and Vision

Crown Sterling’s mission is to enable a future of seamless personal data sovereignty.

In a world where data is constantly flowing, data is being increasingly recognized as the world's most valuable asset. Yet, as data collection grows, much of the population remains unaware of the extent to which their own data is being collected, distributed and harnessed in favor of big tech, governments, and potentially malicious contenders. Hidden within lengthy and seldom read terms and conditions, consumers are unwittingly permitting their data to be collected, stored and sometimes even used against them, empowering the interests of those who seek to exploit user data for their advantage.

No matter how much we want to believe that our personal data is in trustworthy hands or that it is only being collected by companies who will use it in responsible ways, numerous recent examples indicate that consumers must be more vigilant. The track records for governments and technology companies, along with the storage and use of consumer data, is abysmal and getting worse. Additionally, the encryption that protects consumer data is growing progressively weak and is provenly vulnerable to hacking by malicious contenders, with advancements in quantum computing only increasing that vulnerability.

To protect the future of personal sovereignty, the world must be equipped to control and protect their own data. Crown Sterling exists to empower data producers with both economic and cryptographic control over their digital assets and identity.

III. CRYPTOGRAPHY POWERS DIGITAL ASSETS

At the forefront of the data sovereignty conversation is the decentralized and secure nature of blockchain technology. Properly encrypted blockchain-based digital assets offer a way to intermediate and securitize data exchanges without the surveillance of a third party or those with a vested interest in data control.

Cryptocurrencies use cryptography to safely and securely privatize transactions, or data, exchanged on the blockchain. Some cryptocurrencies are protected by symmetric and asymmetric encryption, while the most popular cryptocurrency, Bitcoin, uses a form of asymmetric encryption called Elliptic Curve Diffie Hellman (ECC-DH) cryptography. With the rise of quantum computing, the encryption standards that protect digital assets such as Bitcoin are growing more and more vulnerable to quantum hackers.

a. Overview of Encryption and One-Time Pads

One-Time Pads are the gold standard of encryption as they are unconditionally secure in any computation model when used properly. One-time Pad cryptography has remained impractical as it requires the use of private keys that are at least the same size as the data being encrypted, making one-time pad encryption infeasible for scalable use cases because of the large storage size required to hold both the data and the encryption.

In the dawn of quantum computing, cryptographers are seeking encryption solutions that will ensure the timeless protection of data. The future of data sovereignty relies on quantum-proof cryptography.

b. CrownEncryptOTP™

The widespread implementation of One-Time Pad cryptography has remained impractical for decades, until now. Through the use of irrational numbers to enable shortened keys and gradient descent supervised machine learning to ensure that no decryption keys are ever used twice, CrownEncryptOTP™ delivers the practical and scalable implementation of One-Time Pad technology.

IV. CrownEncryptOTP™: ONE-TIME PAD CRYPTOGRAPHY

One-Time Pad (OTP) Cryptography is an encryption proven to be resilient to cracking.[1,2] The message is encrypted via a secret pad-key such that every character of the message is combined with a corresponding character from the pad-key using some mathematical function (the XOR function in our case). The resulting ciphertext is impossible to break given the one-pad key satisfies the following four conditions:

a. Be truly random.
b. Be at least as long as the plaintext.
c. Never be reused in whole or in part
d. Be kept completely secret.

Even though it offers unbreakable encryption, OTP cryptography has not been widely used due to the difficulty of sharing the pad-key, which is as large or larger than the message itself.

All the above four conditions are met in CrownEncryptOTP™ as it uses unrepeated keys generated from the square root function, which is mathematically proven to produce irrational numbers that are highly random when their arguments are non-perfectly square numbers[3] (NPSN), such as 7, 15, 137, etc. (By definition, any number ending with [2, 3, 7, 8] is certain to be an NPSN.) Additionally, CrownEncryptOTP™ solved the problem of sharing the large key-pad by sharing the number that generates it instead, the NPSN, which is much smaller than the message and can be securely and easily exchanged. Therefore, by exploiting the irrationality of mathematical functions, CrownEncryptOTP™ succeeded in transforming OTP cryptography from being impractical to being very practical and dependable.

I. CrownEncryptOTP™ Design

The CrownEncryptOTP™ is made of the following three main units:

a. CrownRNG™ with entropy gathering Daemon.
b. The ECC-DH unit.
c. Message encryption unit.

a. The CrownRNG™ Unit

The CrownRNG™ is a cryptographically secured pseudo-random number generator (CSPRNG) designed to exploit the by-default randomness of irrational numbers. Mathematical functions known to generate irrational numbers include the square roots of non-perfect square numbers and trigonometric functions having natural numbers for their arguments, among many others. The CrownRNG™ unit is made of three main components:

i. Xeno Unit.
ii. Functions Table.
iii. Random Bits Generator (RBG).

i. The Xeno Unit: A Non-Sequential Randomizer

CrownRNG™ utilizes an entropy gathering Daemon that gathers CPU metrics such as heap, stack, and memory, along with other random system processes, e.g., mouse movements and clicks, keyboard strokes, etc. The Daemon ensures 2048 bits of random data. The Xeno unit is initialized by these metrics, using them as features to predict new labels via a linear regression estimator and then captures the randomized bits of the predictions' mantissas.

The Xeno unit is made of two main sub-units: MusicSU and MathSU. MusicSU transforms the predicted numeric values into a set of three numbers labeled octave, note, and tempo. These three values are then converted, via digital root arithmetic, into specific ranges of mod (13), mod(8), and mod(7), respectively. The MathSU creates random non-perfect square numbers (N). The square roots of these numbers create irrational numbers with infinite mantissas. The MathSU shares the same algorithm as the MusicSU; however, for MathSU, the predicted values are converted to single digits via mod(10), and the digits are concatenated to form one single number of a specific length designated by the programmer. In summary, the Xeno unit outputs the following parameters:

1. The irrational seed: an infinite irrational number N truncated to a specific length and converted into an NPSN. The seed is then found from the square root of this number.
2. The note, tempo, and octave parameters, in the ranges of (0-7), (0-6), and (0-12), respectively.
3. Other required numbers and parameters, such as the index at which the mantissas are truncated and also the range or length of the mantissas that will be included in the key.

ii. The Functions Table

The Functions Table is defined by a set of horizontal and vertical variables that are mathematical functions proven to always produce perfect irrational numbers. The arguments of these functions are not fixed, determined by the random internal states, mainly the timestamp of the current operation time, as well as the tempo variable. The tempo, note, and octave parameters coming out of the Xeno unit will be used to determine which two cells on the vertical and horizontal axis will be utilized for the current run. The output of these cells (the irrational mantissas) are truncated accordingly and used to compute the arithmetic mode through which the RBG will operate. The current model uses square root functions for the horizontal axis of the table and trigonometric ones for the vertical axis. When the two irrational values of the horizontal and the vertical cells (the square root and trig function) are calculated, they will be truncated to specific lengths and then passed on to the RBG as variables I1 and I2, along with the seed N.

iii. The Random Bit Generator (RBG)

The RBG general design is based on the cryptographically secure Blum-Blum-Shub (BBS) generator.[4] The RBG utilizes a specific mathematical function that takes the seed output of the Xeno unit as its initial argument and the product of the two truncated irrational numbers of the Functions Table (I1 and I2) as the arithmetic mod parameters. The RBG then iterates on each calculated value to calculate new ones that are concatenated to create a randomized sequence of bits. The only modification the RBG introduces to the original BBS is replacing prime numbers with irrational ones. The usage of prime numbers in the original BBS is a must if we want to have the ability to reverse the direction of the generator, e.g., when the BBS system is used as an encryption/decryption algorithm. However, as we do not want to reverse the operation in our system, there is no problem using numbers that are not prime. In fact, this introduces additional security to the system because when we compare the limited amount of prime numbers having specific bit-length to the infinite amount of potential irrational numbers of the same bit-lengths, the infinity factor introduces an extra advantage when it comes to the security of the generator against cyber-attacks that try to predict these values.

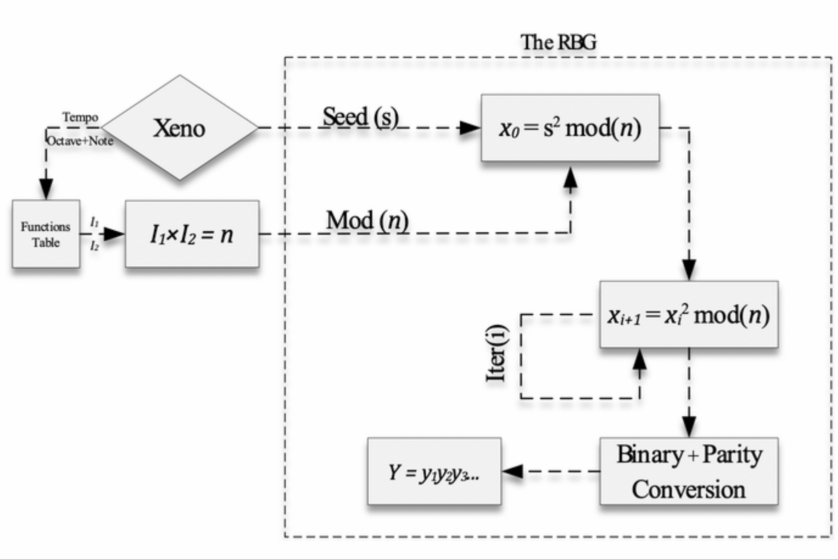


Figure 1: A schematic representation of the RBG workflow.

b. The ECC-DH Unit

This unit is based on the elliptic curve-Diffie-Hellman Protocole (ECC-DH), where the key provided by the CrownRNG™ unit is used to create a public key shared with the other party. Together, both parties will form a larger, privately shared key (α×β×G), which will be passed on to the next unit to encrypt the message with. Along with the public key and the ECC metrics, the last digit (2, 3, 7, or 8) and range numbers are also exchanged with the other party via an AES encryption.

c. The Encryption Unit

The newly generated private key (α×β×G) will undergo mathematical operations before being passed on to the XOR operation. First, the key is converted into a 10-base system. The random, last digit provided by the CrownRNG™ will be attached to its end to ensure it is converted into an NPSN. Next, the square root of this number is calculated. The range number will determine from which index of the mantissa the pad-key starts, whereas the length of the message will determine the last index. Therefore, in CrownEncryptOTP™, the pad-key length is equal to that of the message. The message and the pad-key are then converted into binary forms before they are added together using a function based on the XOR logical function. The message is then shared with the other party via the CrownEncrypt API where the same exact mathematical operations are performed on their privately shared key (α×β×G) to recreate the encryption pad-key. By applying a reversed XOR logical function, the encrypted message is deciphered, and the original message is retrieved. Below is a schematic drawing for the CrownEncryptOTP™ workflow:

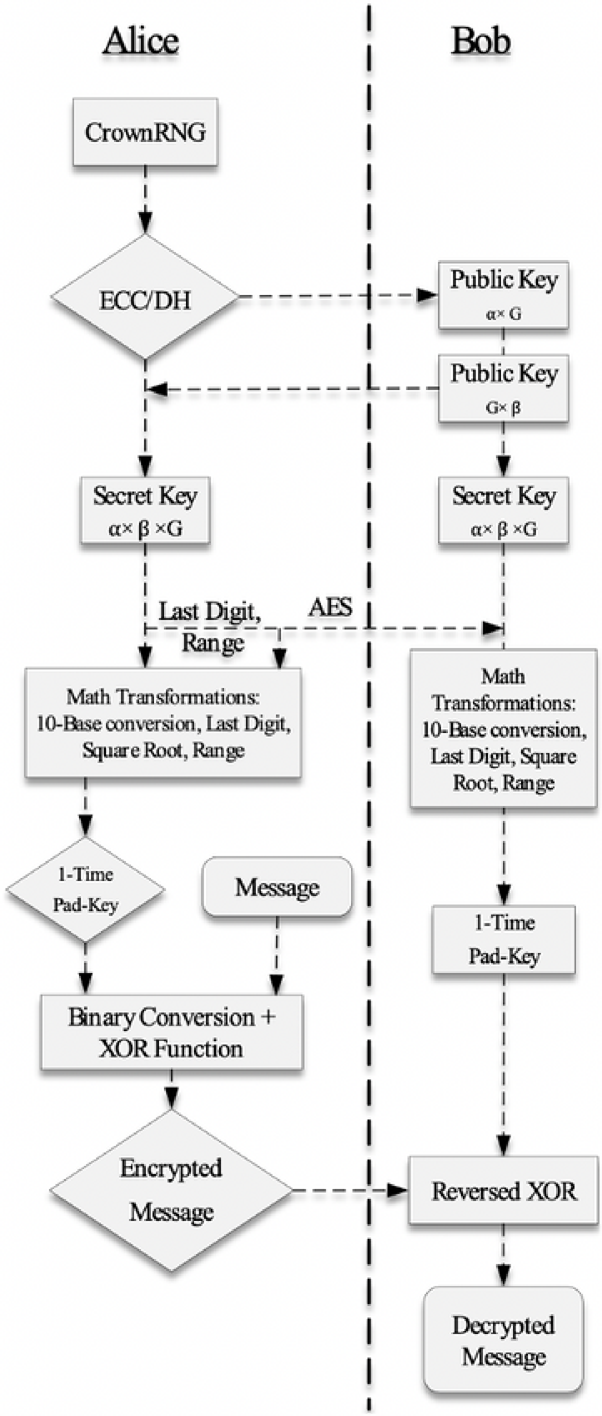


Figure 2: A schematic representation of the workflow of the CrownEncryptOTP™ encryption platform.

V. THE CROWN SOVEREIGN: CSOV

The Crown Sovereign (CSOV) is a cryptocurrency that embraces the power of CrownEncryptOTP™ to ensure the timeless protection and value of users' sensitive data. With one use per token, token holders pay for the secure transmission of their data with Crown Sovereigns.

The Crown Sovereign has a total supply of 10,000,000,000 tokens, which are used to intermediate and afford encrypted data exchanges on the Crown Sterling Mobile Wallet. The Crown Sovereign will be launched on exchanges under the ticker CSOV.

a. Crown Sterling Blockchain

The Crown Sterling blockchain is built using the RUST programming language as a substrate of the Polkadot blockchain, and is independent of the Polkadot consensus mechanism. Crown Sovereign equips a Proof of Stake consensus, and targets a block time of 6 seconds for each Crown Sterling block. CrownEncryptOTP™ has been integrated into the Crown Sterling blockchain, and works to ensure full privacy of users' sensitive data as demonstrated by One-Time Pad encryption.

b. Crown Sterling Wallet

The Crown Sterling Wallet is the native wallet to the Crown Sterling chain. With the wallet, token holders can encrypt and exchange messages and data with each other as well as securely store NFTs and other digital assets using the CSOV token as payment for secure encryption and transfers.

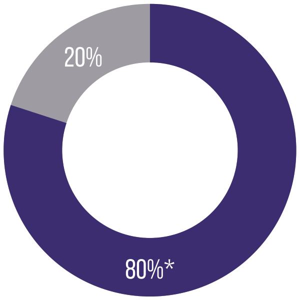
c. Blockchain Explorer

https://bit.ly/3t6Yi3d

VI. TOKENOMICS

Total Token Supply: 10,000,000,000
Fixed Supply: Yes
Released Supply: 8,000,000,000
Unreleased Supply: 2,000,000,000
Anticipated Token List Price: $0.06
Token Type: Polkadot Substrate
Exchanges: Bitcoin.com Exchange, HitBTC, Changelly, Changelly Pro, Bequant
Trading Pairs: CSOV/BTC, CSOV/USDT

Total Token Supply: Released (80%) vs. Unreleased (20%)



* Lockup release schedule below

Token Distribution

	Lockup	Total Tokens	Percentage of Supply
Available for Exchange Listing	No Lockup	190,184,840	1.90%
Investors/ Private Sales/ Employees/ Contractors	Lockup period is 1 year from the time of distribution beginning in December 2020	7,809,815,160	78.10%
Tokens to be Approved for Future Sale	Locked for Crown Sterling Foundation	2,000,000,000	20.00%
Sum	--	10,000,000,000	100.00%

Lockup Release Schedule

	Tokens to Unlock	% of Total Supply Entering Market	% of Locked Tokens Remaining	Total Remaining Locked Tokens
Tokens Locked Up and Release Dates	--	--	--	7,809,815,160
December 2021	147,485,333	1.47%	98.11%	7,662,329,827
January 2022	1,470,213,000	14.70%	79.29%	6,192,116,827
February 2022	46,505,000	0.47%	78.69%	6,145,611,827
March 2022	16,568,000	0.17%	78.48%	6,129,043,827
April 2022	1,708,000	0.02%	78.46%	6,127,335,827
May 2022	11,643,000	0.12%	78.31%	6,115,692,827
June 2022	6,017,388,160	60.17%	1.26%	98,304,667
July 1-14, 2022	37,314,000	0.37%	0.78%	60,990,667
Beyond July, 2022	60,990,667	0.61%	0.00%	0

Price History

Seed Funder's Price	First Private Sale Price	Second Private Sale Price	Anticipated Exchange Listing Price
$0.03 / token	$0.03 / token	$0.04 / token	$0.06 / token
--	Dec. 2020 - Mar. 2021	Mar. 2021 - Sept. 2021	September 2021

VII. CONCLUSION

The Crown Sovereign (CSOV), is the brainchild of Robert Grant and his team of mathematicians at Crown Sterling. Robert and his team share a passion for individual data sovereignty and encryption. They have set out to reverse an alarming trend of deteriorating individual privacy occurring as we spend more time online. The surveillance, data sharing and collection that occurs at the hands of big tech has led to an erosion of personal privacy, sometimes with devastating results. In response, Crown Sterling has authored a Data Bill of Rights that has been included in the genesis block of the Crown Sterling blockchain. This project seeks to put the individual back in control of their personal data and offer the user enhanced security from cyber exploitation and quantum computing threats.

IX. REFERENCES:

[1] Schneier, Bruce. Applied Cryptography: Protocols, Algorithms, and Source Code in C. John Wiley and Sons, Inc. (1996).

[2] Menezes, Alfred J., Paul C. van Oorschot, and Scott A. Vanstone. Handbook of Applied Cryptography, CRC Press (1997).

[3] Luka Milinković , Marija Antić , and Zoran Čiča. Pseudo-random number generator based on irrational numbers. 10th International Conference on Telecommunication in Modern Satellite Cable and Broadcasting Services (TELSIKS) (2011).

[4] L. Blum, M. Blum, and M. Shub. A simple unpredictable pseudo-random number generator. SIAM J. Comput. Vol. 15, No. 2 (1986).