Syfer Sangraal : Holy Grail of Cryptography in the Arc of the Combinant

Raze Buckbriar

2026.08.29 | octade.net | ORCiD 0009-0009-5144-3278

DOI : 10.5281/zenodo.22158384

SUMMARY

Embark on the quest for the Syfer Sangraal system, or the holy grail of cryptography hidden in the arc of the combinant. One system to roll them all is the holy grail of cryptography. One algorithm to perform every kind of cryptographic function is the new wine within the Syfer Sangraal system.

CONTENTS

[1] About OCTADE

Octade is the umbrella term for the research of Byrl Raze Buckbriar (Raze). This research encompasses a variety of interests, especially cryptology and cryptography as an art form, a mode of truth expression and exploration rather than merely as software tooling. This exploration births the quest for the Syfer Sangraal, or the Holy Grail of Cryptography in the Arc of the Combinant.

[2] Fields of Research

A. cryptology
B. textual criticism
C. theology
D. poetry
E. computer science
F. history
G. antiquities
H. philology

[3] Scope of Research

A. identifying essential patterns in text
B. Holy Grail of Cryptography in the Arc of the Combinant
C. iconoclasm and myth busting
D. simplification of complexity
E. expressing the arcane via the mundane
F. translation accuracy
G. multi-layered idioms and parables

[4] Syfer Sangraal : Holy Grail of Cryptography in the Arc of the Combinant.

The Combinant is the class of functions that are able to emulate algebraic commutativity and combinatrics without necessarily having actual numerical commutativity. Non-commutative operations can be extended in ways to emulate commutative or modular arithmetic possessing hard invertibility or secure trapdoor functions. The Arc of the Combinant is the whole range of such commutative emulation.

The Holy Grail of Cryptography is a single, simple algorithm that performs all necessary functions of computational cryptography with provable security sans assumptions in the model, while avoiding mental intractability as much as possible. The necessary functions include secure hashing, digital signatures, verification, key exchanges, ciphers, random generation, authentication, access control, secret sharing, confidentiality, proofs, vector commitments, and other aspects of common usage in cryptography. The desirable properties of the universal Syfer Sangraal would presage the pending obsolescence and replacement of most or even all cryptosystems and their primitives. The Syfer Sangraal would replace all cryptographic primitives and systems with one singular algorithm and cryptosystem for the ages ahead. Syfer Sangraal would be based upon one mathematical function that can perform all the tasks of the obsoleted artifacts in perpetuity.

This idealized system is desirable as the unrelenting burgeoning of cryptosystems and their complexity creates a paradox. It becomes infeasible to even know if cryptosystems are secure. As complexity grows the difficulty of cryptanalysis grows more than linearly requiring ever growing numbers of personnel, money, time, and resources to analyze and (hopefully) secure the growing collection of cryptosystems and their complex layers of implementation. Syfer sages have rightly predicted the breaking of cryptosystems and the insurmountable difficulty of provable security in a storm of growing complexity. Syfer Sangraal would pacify this weather pattern.

If one single algorithm were to be employed to replace all cryptosystems, that would be the 'end of cryptography'. In that event no further cryptology research would be needed for securing and maintaining the fund of existing cryptosystems. And the mountainous volumes of work maintaining current cryptographic infrastructure would be eliminated to free up resources for other discoveries and inventions.

In sum, discovery of the Syfer Sangraal would render computational cryptology a very boring field of

endeavor and much safer and more secure than its current state. The Syfer Sangraal would render modern cryptography and cyber-security models superfluous.

[5] Candidates for Syfer Sangraal Vintage

So far OCTADE research leads to several candidate algorithm classes as the grapes for the wine within the Syfer Sangraal.

a. rhizome functions
b. holoalphabetic (perfect pangram) functions
c. ouroboros functions
d. shingle functions
e. mushroom functions
f. spore functions
g. sharx functions

These functions are aptly named to approximate their structure and operation to avoid mental intractability common with maths and number theory. The functions can 'emulate' algebraic properties in interesting and useful ways. Some of these functions provide commutative emulation in the Arc of the combinant. Neither the novel functions nor commutative emulation are described herein. The functions are the topics of research papers and simple programs of demonstration code being slowly cobbled together. Much research and testing indicates that one or more of these function classes will potentially satisfy the required properties of a Syfer Sangraal system that uses commutative emulation for multiple kinds of cryptographic primitives.

[6] Simplementation : Avoiding Complexity Confusion and Mental Intractability

At the core of a Syfer Sangraal system is the idea that the system must be mentally simple and tractable and easy to teach and grasp and implement in computer systems. This is termed, 'simplementation'. In developing a Syfer Sangraal the researcher, inventor, and teacher should take pains to avoid mucking up the works with strange acronyms and endlessly-mutating numerical prefixes and abbreviations. Names for things should be descriptive rather than creating an impenetrable jargon only comprehended by caffeinated, seasoned experts.

In our modern society the average human brain is already greatly over-taxed by the requirement to make far more decisions and distinctions in a day than in prior generations. The sheer volume of daily mental input is vastly larger than previous generations and contrary to the human cognitive constitution. Syfer Sangraal Simplementation is an idea for rolling back from that precipice of stress and analysis paralysis to render cryptology simpler and easier rather than more complex or harder. Rather than remedy uncountable bugs and mistakes in cryptosystems and software, clear the field of all the dross and noise that makes the mistakes and pitfalls possible. This is akin to replacing the cryptographic football game with billiards or miniature golf.

[7] Breakdown : Boot the Binary Bureaucrats of Byzantium

The discovery of the Syfer Sangraal system would allow many security research bodies, conferences, educational institutions, standards bodies, and implementers to clear their tables and their calendars. The Syfer Sangraal system would make possible the elimination of entire classes of software bugs and security failures.

Cryptographic complexity and mental intractability benefit binary Byzantine bureaucrats and hostile actors. Simplicity benefits their victims. A Syfer Sangraal system puts power in the hands that need and deserve it the most. There is much more to be said yet the more must wait until another time.

[8] Project Links and Resources

```
Website   : https://octade.net
Fediverse : @8@star.octade.net | https://star.octade.net/@8
ORCiD     : https://orcid.org/0009-0009-5144-3278
Academia  : https://independent.academia.edu/RazeBuckbriar
Archive   : https://archive.org/details/@buckbriar
Zenodo    : https://zenodo.org/search?q=metadata.identifiers:%27octade%27
Git       : https://codeberg.org/OCTADE
```