

Cryptographic applications of weak restricted integer compositions

Gustavo Zambonin



Laboratório de Segurança em Computação
Universidade Federal de Santa Catarina

July 13th, 2023

LabSEC Day 2023

Introduction

A partition of s is a representation of s as a sum

$$s = a_1 + a_2 + \cdots + a_t$$

with s, t positive; each a_i with $1 \leq i \leq t$ is called a *part*.

The order of the parts *does not matter* for partitions. When it does, we are discussing *compositions*.

We present an application of integer compositions in digital signature schemes.

Weak compositions

A composition where parts can be zero; there are infinitely many for any s .

We are interested in those with a limited number t of parts, denoted *weak t -compositions*.

Let $s = 7$ and $t = 5$. We can represent $4 + 0 + 1 + 2 + 0$ as shown below.

★ ★ ★ ★ | | ★ | ★ ★ |

In other words, we have a bijection to s stars and $t - 1$ bars. The number of weak t -compositions of s is $C(s, t) = \binom{s+t-1}{s}$.

Restricted compositions

Let S be a set of non-negative integers. An S -restricted composition is a composition of s such that all parts lie in S .

If $S = \{0, 1, \dots, n\}$ for n positive, we simply call the compositions n -restricted.

The number of n -restricted t -compositions of s is the coefficient of x^s in $(1 + x + x^2 + \dots + x^n)^t$, or equivalently

$$C(s, t, n) = \sum_{i=0}^{\min(t, \lfloor \frac{s}{n+1} \rfloor)} (-1)^i \binom{t}{i} \binom{s - (n+1)i + t - 1}{t-1}$$

as given by Eger [Ege13]. We note that $C(s, t, s) = C(s, t)$.

Ranking (combinatorial) objects

Let S be a finite set, $N = |S|$ and consider any distinct $s, t \in S$.

A *ranking function* is a bijection $\mathcal{R} : S \rightarrow \{0, \dots, N - 1\}$ which defines a total ordering $\prec$ on the elements of S , i.e. $s \prec t \Leftrightarrow \mathcal{R}(s) \prec \mathcal{R}(t)$.

An *unranking function* is a bijection $\mathcal{U} : \{0, \dots, N - 1\} \rightarrow S$ such that $\mathcal{R}(s) = i \Leftrightarrow \mathcal{U}(i) = s$ for all $0 \leq i \leq N - 1$.

The total ordering is usually taken to be the lexicographic order $\prec_{\text{lex}}$.

Winternitz one-time signature scheme

A quantum-safe signature scheme used as a building block for state-of-the-art hash-based signatures [BHK⁺19].

Let λ, w be positive integers that represent the security parameter and a performance trade-off, respectively.

Consider a message $0 \leq M \leq 2^\lambda - 1$ and $t = \lceil \frac{\lambda}{\log_2 w} \rceil$. To sign M , we initially divide it into a t -tuple of base- w integers.

Due to its design, the cost of operating on Winternitz signatures will be *proportional to the magnitude of M* .

Creating a Winternitz signature

Let $\lambda = 32$, $w = 16$ and $M = 1\,996\,026\,778$. By converting M to binary, we have

$$\underbrace{\underbrace{0111}_{\log_2 w} \ 0110 \ 1111 \ 1000}_{\lambda} \ 1111 \ 0011 \ 1001 \ 1010$$

which is mapped to $(7, 6, 15, 8, 15, 3, 9, 10)$.

In other words, we obtain a w -restricted t -composition of some integer $0 \leq k \leq t(w - 1)$.

This is a way of unranking M into t -tuples of base- w integers in $\prec_{\text{lex}}$.

“Constant-sum” Winternitz

We want a cryptographic algorithm to be useful in several situations, e.g., hardware tokens or document silos for long-term preservation.

We replace the Winternitz “base- w ” unranking with a bijection between messages and n -restricted t -compositions of s such that $C(s, t, n) \geq 2^\lambda$.

Hence, $k = s$ for any message, and the computational effort to generate signatures becomes constant and predictable.

We provide new unranking algorithms **DCS** and **DBCS**, practical experiments and a tight security proof [PZC⁺21].

Efficiency of constant-sum unranking

The “base- w ” unranking is extremely efficient, consisting only of bit manipulations.

However, the calculation of $C(*, *, n)$ in the main loop of **DCS** implies in several costly binomial computations.

When signing M , the “constant-sum” unranking overhead is non-trivial, and neither **DCS** nor **DBCS** solve this completely.

In this talk, we give preliminary results on a new algorithm based on **DCS**.

Rationale on the improved algorithm

We store partial values of $C(s, t-1, n)$ to calculate $C(s-b, t-1, n)$ with only integer operations.

For $0 \leq i \leq \min(t-1, \lfloor \frac{s-b}{n+1} \rfloor)$ and $1 \leq b \leq s$, this ratio is

$$\frac{(-1)^i \binom{t-1}{i} \binom{(s-b)-(n+1)i+t-2}{t-2}}{(-1)^i \binom{t-1}{i} \binom{s-(n+1)i+t-2}{t-2}}.$$

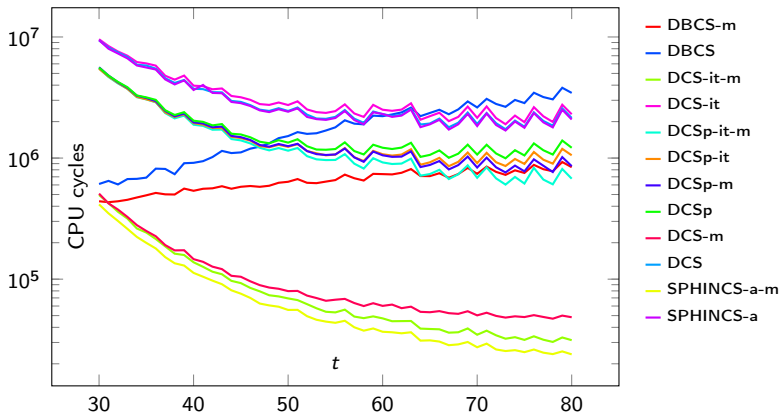
Expanding the binomials gives us

$$\prod_{g=1}^b \frac{(s-g+1) - (n+1)i + t - 2}{(s-g+1) - (n+1)i},$$

which is a constant ratio for fixed g and i .

Unranking performance for $\lambda = 256$

Algorithms are implemented in C with the GMP library. The “-m” modifier represents the addition of a cache.



Conclusion

We discussed some particular cases of integer compositions that make their enumeration and generation harder.

We showed an instance of integer compositions appearing in the Winternitz one-time signature scheme.

We replaced its underlying “base- w ” unranking function by a more predictable, but slower alternative based on compositions.

We are currently looking into more efficient methods to unrank such restricted compositions via probabilistic methods and using other orders.

References I



Daniel J. Bernstein, Andreas Hülsing, Stefan Kölbl, Ruben Niederhagen and Joost Rijneveld, and Peter Schwabe.

The SPHINCS⁺ Signature Framework.

In *CCS '19: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, pages 2129–2146, November 2019.



Steffen Eger.

Stirling's Approximation for Central Extended Binomial Coefficients.

Journal of Integer Sequences, 16(13.1.3), 2013.

References II



Lucas Pandolfo Perin, Gustavo Zambonin, Ricardo Custódio, Lucia Moura, and Daniel Panario.

Improved constant-sum encodings for hash-based signatures.

Journal of Cryptographic Engineering, 11(4):329–351, November 2021.