

Random generation of combinatorial objects in cryptographic systems

Gustavo Zambonin



Universidade Federal de Santa Catarina

October 21st, 2024

SECCOM 2024

Motivation

Underlying security of usual digital signature schemes is based on hard problems from number theory.

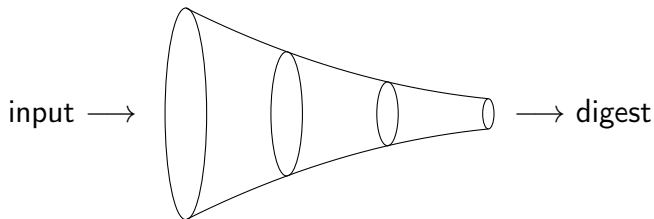
- Insufficient considering the threat of quantum algorithms
- Quantum-safe cryptography is independent from these problems

Particularly, one-way functions are necessary and sufficient to build digital signature schemes [Rom90].

- Cryptographic hash functions are derived from one-way functions
- Digital signature schemes built only from such functions

Cryptographic hash function

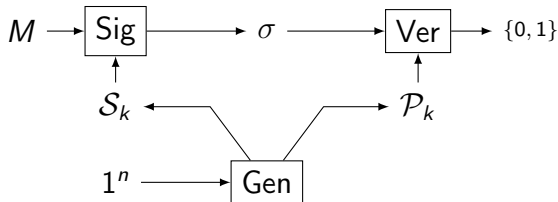
Consider a function $\mathcal{H} : \{0, 1\}^* \longrightarrow \{0, 1\}^n$.



Must be pre-image, second-pre-image and collision resistant.
Usually, $n \in \{224, 256, 384, 512\}$.

Digital signature scheme

Based on public-key cryptography; provides authentication, integrity and non-repudiation.



There are schemes in which the key pair is used only once to prevent signature forgeries.

Winternitz one-time signature scheme

Key generation

Take any message M , $w \in \mathbb{N}$, $w > 1$, $f : \{0, 1\}^n \longrightarrow \{0, 1\}^n$ and $\mathcal{H} : \{0, 1\}^* \longrightarrow \{0, 1\}^n$. Then,

$$t_1 = \left\lceil \frac{n}{w} \right\rceil, t_2 = \left\lceil \frac{\lfloor \log_2 t_1 \rfloor + 1 + w}{w} \right\rceil \text{ and } t = t_1 + t_2.$$

The private and public keys are, respectively,

$$\begin{aligned} \mathcal{S}_k &= (x_{t-1}, \dots, x_0) \xleftarrow{\$} \{0, 1\}^n \text{ and} \\ \mathcal{P}_k &= (f^{2^w-1}(x_{t-1}), \dots, f^{2^w-1}(x_0)) \\ &= (y_{t-1}, \dots, y_0). \end{aligned}$$

Winternitz one-time signature scheme

Signature generation

The values $\epsilon_i \in \{0, 1\}^w$ are obtained as follows:

$$\mathcal{H}(M) = \epsilon_{t-1} \parallel \dots \parallel \epsilon_{t-t_1}, \quad c = \sum_{i=t-t_1}^{t-1} 2^w - 1 - \epsilon_i, \\ \mathcal{B}_1 = (\epsilon_{t-1}, \dots, \epsilon_{t-t_1}), \quad \mathcal{B}_2 = (\epsilon_{t_2-1}, \dots, \epsilon_0).$$

Finally, the one-time signature is built:

$$\sigma = (f^{\epsilon_{t-1}}(x_{t-1}), \dots, f^{\epsilon_0}(x_0)).$$

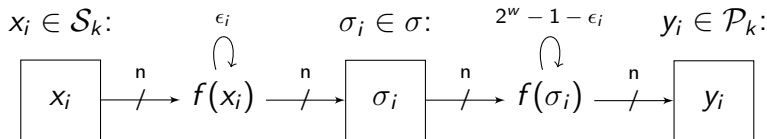
Winternitz one-time signature scheme

Signature verification

The ϵ_i are also used to verify σ :

$$\forall \sigma_i \in \sigma, f^{2^w - 1 - \epsilon_i}(\sigma_i) = y_i.$$

In short,



Winternitz one-time signature scheme

Some intuitions

We have that $w \geq 1$ is a performance trade-off, controlling how many bits are signed “in parallel”.

To sign a message $M \in \{1, \dots, 2^\lambda\}$, it must first be divided into a t -tuple of base- w integers via the “base- w ” algorithm.

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

Therefore, we cannot foresee the time taken to generate or verify a signature. We address that in the following.

Integer partitions and compositions

Let $s, t, a_1, \dots, a_t \geq 1$. A partition of s with t parts is a set $\{a_1, \dots, a_t\}$ such that $\sum_{i=1}^t a_i = s$.

A composition of s with t parts, or t -composition, is a *sequence* $(a_1, \dots, a_t)$ that sums to s .

If a_i are allowed to be zero, such compositions are called *weak*.

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

★ ★ ★ ★ | | ★ | ★ ★ | .

A bijection to s stars and $t - 1$ bars gives the number of weak t -compositions of s : $C(s, t) = \binom{s+t-1}{s}$.

Restricted compositions

Let $S \subseteq \{0, 1, \dots, n\}$. An S -restricted composition is a composition of s such that $a_i \in S$ for all $1 \leq i \leq t$.

If $S = \{0, 1, \dots, n\}$, we call 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

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

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 any $s, t \in S$ with $s \neq t$.

A *ranking function* is a bijection $\mathcal{R} : S \rightarrow \{1, \dots, N\}$ which defines a total order $\prec$ on the elements of S , i.e.

$$s \prec t \Leftrightarrow \mathcal{R}(s) \prec \mathcal{R}(t).$$

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

The total order is usually the lexicographic order $\prec_{\text{lex}}$.

Recalling the base- w algorithm

Take $\lambda = 32$, $w = 16$ 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 $k \in \{0, \dots, t(w-1)\}$.

The message can then be signed after k evaluations of the underlying cryptographic hash function.

Constant-sum Winternitz

In a recent paper [PZC⁺21], we replace base- w by unranking to 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** (in $\prec_{\text{lex}}$), practical experiments and a tight security proof.

In the case of **DCS**, the algorithm is based on the recursion

$$C(s, t, n) = \sum_{j=0}^n C(s - j, t - 1, n). \quad (2)$$

Efficiency of unranking to restricted compositions

The base- w algorithm is extremely efficient, consisting only of bit manipulations.

However, **DCS** needs to compute Eq. 1 for several choices of s and t , which may not fit a standard computer word.

This is because, for each part, we must find the largest j such that Eq. 2 does not exceed M .

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

We give preliminary results on a new algorithm based on **DCS**, which we call **DCSp**.

Rationale of DCSp

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

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

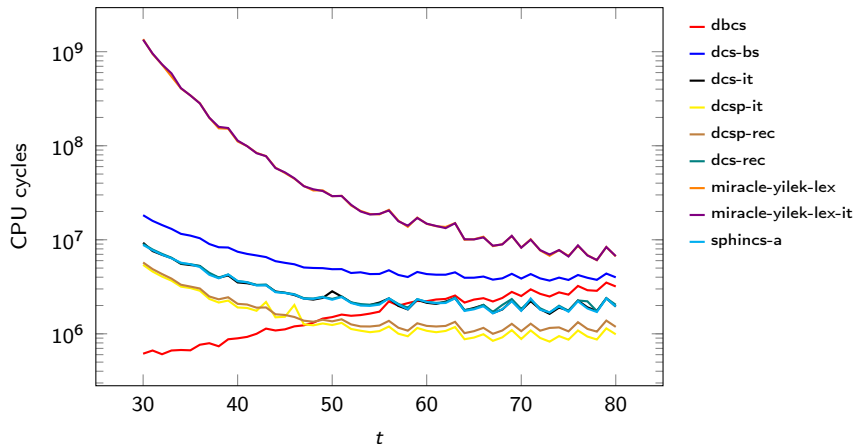
Expanding the binomials gives us

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

which is a constant ratio for fixed g and i .

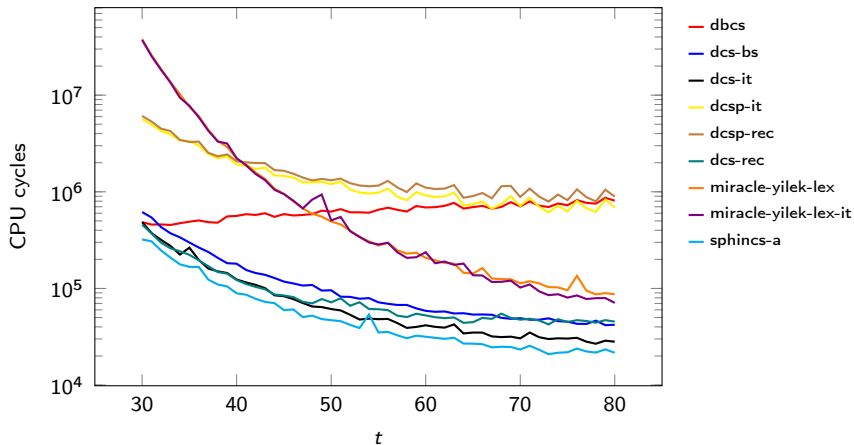
Unranking performance for $\lambda = 256$

Algorithms are implemented in C with the GMP library.



Unranking performance for $\lambda = 256$ (cached)

Algorithms are implemented in C with the GMP library.



We are currently dropping GMP; experiments show that `_BitInt()` (C23) is faster for $\lambda \leq 512$.

We are also evaluating other ideas:

- unranking to restricted compositions in Gray orders;
- decomposing compositions into permutations of partitions and unranking such objects.

We are always accepting interested students to join our efforts!

References I



Steffen Eger.

Stirling's Approximation for Central Extended Binomial Coefficients.

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



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.

References II



J. Rompel.

One-way Functions Are Necessary and Sufficient for Secure Signatures.

In H. Ortiz, editor, *Proceedings of the Twenty-second Annual ACM Symposium on Theory of Computing*, pages 387–394, May 1990.