# EdDSA For Baby Jubjub Elliptic Curve with MiMC-7 Hash

Jordi Baylina[1] and Marta Bellés[1,2]

[1] *iden3*, [2] *Universitat Pompeu Fabra*

## Contents

# 1 Scope

This proposal aims to standarize the elliptic curve signature scheme Edwards-curve Digital Signature Algorithm (EdDSA) for Baby Jubjub Edwards elliptic curve using MiMC-7 hash function.

# 2 Motivation

EdDSA is a variant of Schnorr's signature scheme and it provides high performance on a variety of platforms [4].

# 3 Background

There are many implementations of EdDSA with Edwards elliptic curves such as Ed25519 or Ed448-Goldilocks and most of them use hash SHA-512. This is the first document specifying a protocol for implementing EdDSA using MiMC-7 and we describe it on the Baby Jubjub Elliptic curve.

The choice of the MiMC-7 hash function makes computations inside circuits very efficient and it has a big potential in zero knowledge protocols such as zk-SNARK.

# 4 Terminology

The table below summarizes the terminology used across the document. Each element is explained in greater detail in the following sections.

| **Notation** | **Description** |
|---|---|
| $p$ | Prime number. |
| $\mathbb{F}_p$ | Finite field with $p$ elements. |
| $E$ | Baby Jubjub elliptic curve (defined over $Fp$) in Edwards form. |
| $E_M$ | Baby Jubjub elliptic curve (defined over $Fp$) in Montgomery form. |
| $l$ | Large prime number dividing the order of Baby Jubjub. |
| $\mathbb{F}_l$ | Finite field with $l$ elements. |
| $\mathbb{G}$ | Group of $\mathbb{F}_p$-rational points of order $l$. |
| $B$ | Base point (generator of $\mathbb{G}$) of Baby Jubjub. |
| $A = (A_x, A_y)$ | Public key. $A$ is a point on $E$. |
| $k$ | Private key. |
| $M$ | Message. $M$ is an element of $\mathbb{F}_l$. |
| $(R, S) = ((R_x, R_y), S)$ | Signature on $M$. $R$ is a point on $E$ and $S$ and element of $\mathbb{F}_l$. |
| $H$ | Hash function MiMC-7. |
| $r$ | Number of rounds of MiMC-7. |
| $c_0, c_1, \dots, c_r$ | Constants used in MiMC-7. |

### 4.1 Baby-Jubjub

Consider the prime number

$$p = 21888242871839275222246405745257275088548364400416034343698204186575808495617$$

and let $\mathbb{F}_p$ be the finite field with $p$ elements. We define $E_M$ as the *Baby-Jubjub* Montgomery elliptic curve defined over $\mathbb{F}_p$ given by equation

$$E : v^2 = u^3 + 168698u^2 + u.$$

The order of $E_M$ is $n = 8 \times l$, where

$$l = 2736030358979909402780800718157159386076813972158567259200215660948447373041$$

is a prime number. Denote by $\mathbb{G}$ the subgroup of points of order $l$, that is,

$$\mathbb{G} = \{\, P \in E(\mathbb{F}_p) \mid lP = O \,\}.$$

Let

$$\begin{aligned} B = (&17777552123799933955779906779655732241715742912184938656739573121738514868268,\\ &2626589144620713026669568689430873010625803728049924121243784502389097019475) \end{aligned}$$

be a generator of $\mathbb{G}$.

$E_M$ is birationally equivalent to the Edwards elliptic curve

$$E : x^2 + y^2 = 1 + dx^2y^2$$

where $d = 9706598848417545097372247223557719406784115219466060233080913168975159366771$.

The birational equivalence [3, Thm. 3.2] from $E$ to $E_M$ is the map

$$(x, y) \to (u, v) = \left( \frac{1+y}{1-y}, \frac{1+y}{(1-y)x} \right)$$

with inverse from $E_M$ to $E$

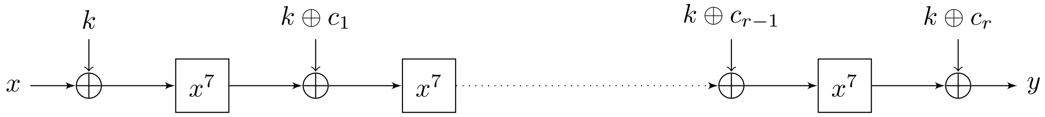
$$(u, v) \to (x, y) = \left( \frac{u}{v}, \frac{u-1}{u+1} \right).$$

### 4.2 MiMC-7

The hash function used in EdDSA is MiMC-7 based in paper [1], which describes the hash using exponent 3. In this specification, we use exponent 7 (hence the name MiMC-7) as 3 and $l-1$ are not coprime and 7 is the optimal choice for exponentiation [1, Sec. 6].

Let $\mathbb{F}_l$ be the finite field with $l$ elements. The block cipher is constructed by iterating a round function $r$ times where each round consists of a key addition with the key $k$, the addition of a round constant $c_i \in \mathbb{F}_r$, and the application of a non-linear function defined as $F(x) := x^7$ for $x \in \mathbb{F}_l$. The ciphertext is finally produced by adding the key $k$ again to the output of the last round. Hence, the round function is described as $F_i(x) = F(x) \oplus k \oplus c_i$ where $c_0 = c_r = 0$ and the encryption process is defined as

$$E_k(x) = (F_{r-1} \circ F_{r-2} \circ ... \circ F_0)(x) \oplus k.$$



As the random constants $c_i$ do not need to be generated for every evaluation of MiMC-7, they are hard-coded into the implementation. The generation of these constants and the required number of rounds is described in section 6.2.

### 4.3 EdDSA

The description of this protocol is based in [4]: Let the public key be a point $A = (A_x, A_y) \in E$ of order $l$ and $M$ a message we wish to sign. The signature on $M$ by $A$ consists of a par $(R, S)$ where $R = (R_x, R_y)$ is a point of order $l$ of $E$ and $S \in \mathbb{F}_l \backslash \{0\}$ such that

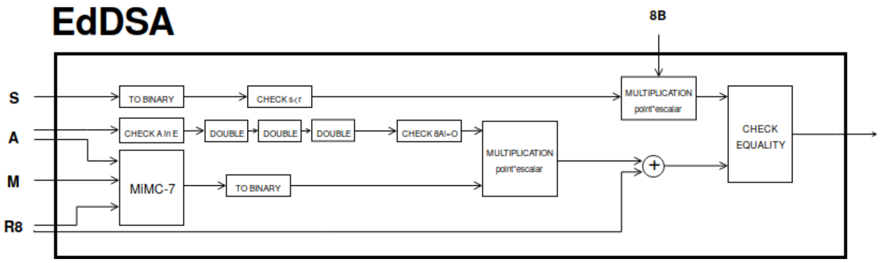
$$8SB = 8R + 8H(R, A, M)A.$$

## 5 Challenges and security

One of the main challenges to create this standard and to see it adopted by the community is to provide correct, usable, and well-maintained implementations in as many languages as possible. Some effort is also required to audit and verify code coming from the community and claiming to implement EdDSA for Baby Jubjub to prevent the propagation of potentially insecure implementations. Part of the work in progress of looking batch verification of short signatures. Lastly, the proposal as it stands uses MiMC-7 as hash function as it works very optimal inside circuits. We believe some work is required to determinate the security MiMC hash functions.

# 6 Implementation

In this section, we specify how each of the main operations in the following EdDSA circuit are computed:



## 6.1 Operations in the elliptic curve

### 6.1.1 Addition of points

When adding points of elliptic curves in Montgomery form, one has to be careful if the points being added are equal (doubling) or not (adding) and if one of the points is the point at infinity [5]. Edwards curves have the advantage that there is no such case distinction and doubling can be performed with exactly the same formula as addition [3]. In comparison, operating in Montgomery curves is cheaper. In this section, we summarize how addition and doubling is performed in both forms. For the exact number of operations required in different forms of elliptic curves, see [3].

- Edwards: Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be points of the Baby-Jubjub twisted Edwards elliptic curve $E$. The sum $P_1 + P_2$ is a third point $P_3 = (x_3, y_3)$ with

  $$\begin{aligned} \lambda &= dx_1x_2y_1y_2, \\ x_3 &= (x_1y_2 + y_1x_2)/(1 + \lambda), \\ y_3 &= (y_1y_2 - x_1x_2)/(1 - \lambda). \end{aligned}$$

  Note that the neutral element is the point $O = (0, 1)$ and the inverse of a point $(x, y)$ is $(-x, y)$.

- Montgomery: Let $P_1 = (x_1, y_1) \neq O$ and $P_2 = (x_2, y_2) \neq O$ be two points of the Baby-JubJub elliptic curve $E_M$ in Montgomery form.

  If $P_1 \neq P_2$, then the sum $P_1 + P_2$ is a third point $P_3 = (x_3, y_3)$ with coordinates

  $$\begin{aligned} \Lambda &= (y_2 - y_1)/(x_2 - x_1), \\ x_3 &= \Lambda^2 - A - x_1 - x_2, \\ y_3 &= \Lambda(x_1 - x_3) - y_1. \end{aligned} \tag{1}$$

If $P_1 = P_2$, then $2 \cdot P_1$ is a point $P_3 = (x_3, y_3)$ with coordinates

$$\begin{aligned} \Lambda &= (3x_1^2 + 2Ax_1 + 1)/(2y_1), \\ x_3 &= \Lambda^2 - A - 2x_1, \\ y_3 &= \Lambda(x_1 - x_3) - y_1. \end{aligned} \tag{2}$$

### 6.1.2 Multiplication of a point of $E$ by a scalar

Let $P \neq O$ be a point of the Edwards curve $E$ of order strictly greater than 8 (i.e. $P \in \mathbb{G}$) and let $k$ a binary number representing an element of $\mathbb{F}_p$. We describe the circuit used to compute the point $k \cdot P$.

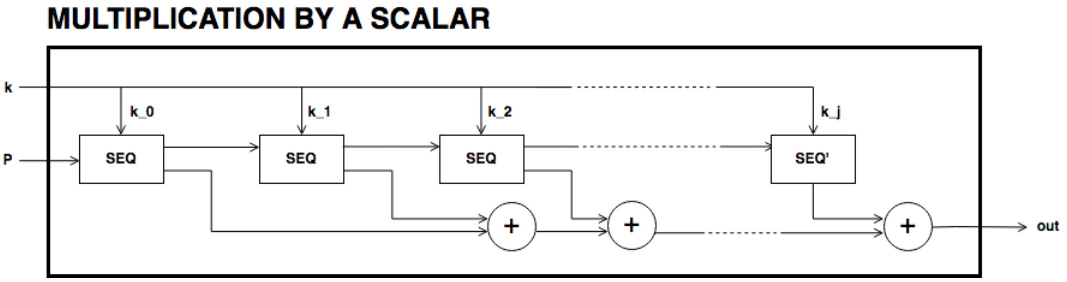
1. First, we divide $k$ into chunks of 248 bits. If $k$ is not a multiple of 248, we take $j$ segments of 248 bits and leave a last chunk with the remaining bits. More precisely, write

$$k = k_0 k_1 \ldots k_j \quad \text{with} \quad \begin{cases} k_i = b_0^i b_1^i \ldots b_{247}^i & \text{for } i = 0, \ldots, j-1, \\ k_j = b_0^j b_1^j \ldots b_s^j & \text{with } s \leq 247. \end{cases}$$

Then,

$$k \cdot P = k_0 \cdot P + k_1 \cdot 2^{248} P + \cdots + k_j \cdot 2^{248j} P. \tag{3}$$

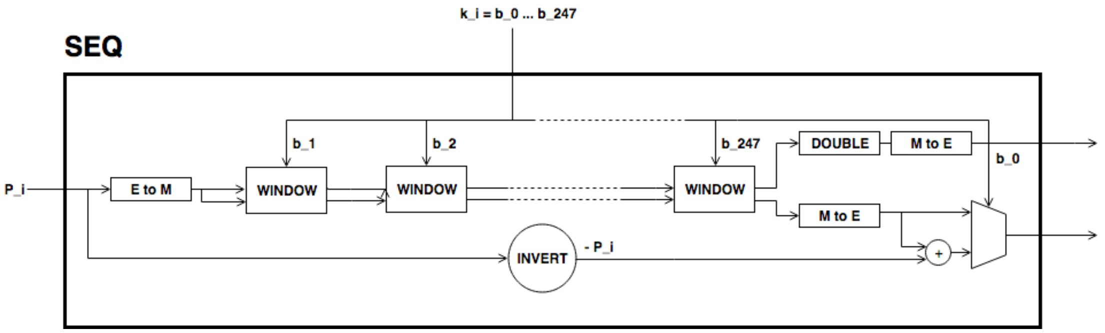
This sum is done using the following circuit. The terms of the sum are calculated separately inside the SEQ boxes and then added together.

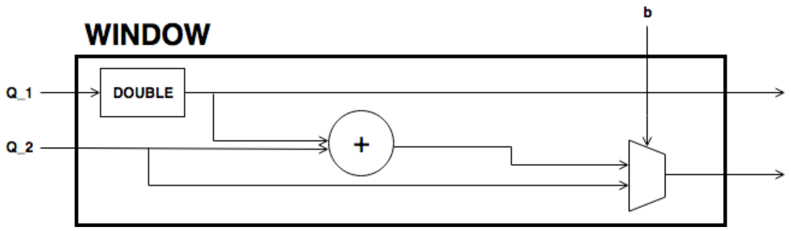


2. Each SEQ box takes a point of $E$ of the from $P_i = 2^{248i} P$ for $i = 0, \ldots, j-1$ and outputs two points

$$2^{248} \cdot P_i \quad \text{and} \quad \sum_{n=0}^{247} b_n \cdot 2^n \cdot P_i.$$

The first point is the input of the next $(i+1)$-th SEQ box (note that $2^{248} \cdot P_i = P_{i+1}$) whereas the second output is the computation of the $i$-th term in expression (3). The precise circuit is depicted in next two figures SEQ and WINDOW.





The idea of the circuit is to first compute

$$Q = P_i + b_1 \cdot (2P_i) + b_2 \cdot (4P_i) + b_3 \cdot (8P_i) + \cdots + b_{247} \cdot (2^{247} P_i),$$

and output the point

$$Q - b_0 \cdot P_i.$$

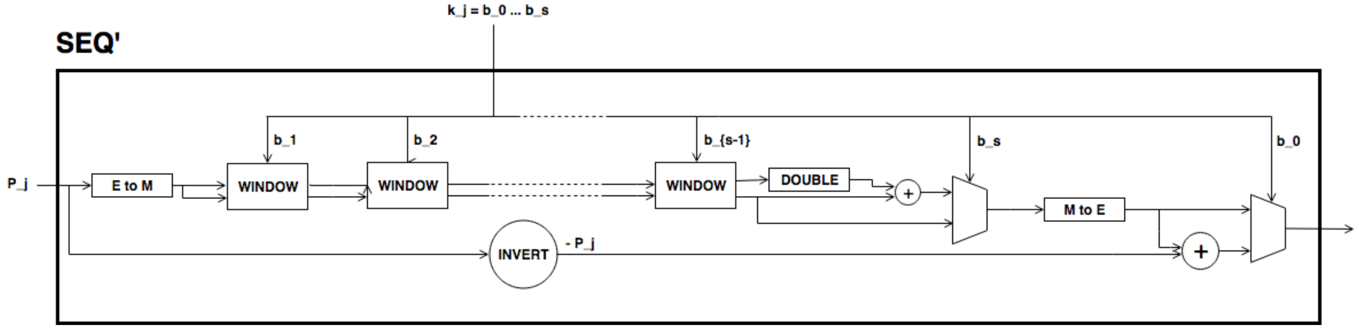
This permits the computation of $Q$ using the Montgomery form of Baby-Jubjub and only use twisted Edwards for the second calculation. The reason to change forms is that, in the calculation of the output, we may get a sum with input the point at infinity if $b_0 = 0$.

Still, we have to ensure that none of the points being doubled or added when working in $E_M$ is the point at infinity and that we never add the same two points.

- By assumption, $P \neq O$ and $\mathrm{ord}(P) > 8$. Hence, by Lagrange theorem [2, Corollary 4.12], $P$ must have order $r$, $2r$, $4r$ or $8r$. For this reason, none of the points in $E_M$ being doubled or added in the circuit is the point at infinity, because for any integer $m$, $2^m$ is never a multiple of $r$, even when $2^m$ is larger than $r$, as $r$ is a prime number. Hence, $2^m \cdot P \neq O$ for any $m \in \mathbb{Z}$.
- Looking closely at the two inputs of the sum, it is easy to realize that they have different parity, one is an even multiple of $P_i$ and the other an odd multiple of $P_i$, so they must be different points. Hence, the sum in $E_M$ is done correctly.

3. The last term of expression (3) is computed in a very similar manner. The difference is that the number of bits composing $k_j$ may be shorter and that there is no need to compute $P_{j+1}$, as there

is no other SEQ box after this one. So, there is only output, the point $k_j \cdot P_j = k_j \cdot 2^{248j} P$. This circuit is named SEQ'.



### 6.2 MiMC-7

The specifications we use in the hash are (*we are working in explaining this section in greater detail*):

1. Number of rounds: $r = \left\lceil \frac{\log_2 l}{\log_2 7} \right\rceil = 91$.
2. Inputs:
   - Coordinates of the public key: $(A_x, A_y)$.
   - Coordinates of the point $8R$: $(R8_x, R8_y)$.
   - Message $M$.
3. Number of inputs: 5.
4. Generation of constants: `https://github.com/iden3/circomlib/blob/master/src/mimc7.js`.

### 6.3 Example and test vectors

*Work in progress.*

### 6.4 Existing implementations

EdDSA for Baby Jubjub implemented by Jordi Baylina in circom (zero knowledge circuit compiler):
`https://github.com/iden3/circomlib/blob/master/circuits/eddsamimc.circom`

## 7 Intellectual Property

We will release the final version of this proposal under creative commons, to ensure it is freely available to everyone.

# References

[1] Albrecht, M., Grassi, L., Rechberger, C., Roy, A., and Tiessen, T. Mimc: Efficient encryption and cryptographic hashing with minimal multiplicative complexity. Cryptology ePrint Archive, Report 2016/492, 2016. https://eprint.iacr.org/2016/492.

[2] Baumslag, B., and Chandler, B. *Schaum's outline of Theory and Problems of Group Theory.* Schaum's outline series. McGraw-Hill Book Company, New York, 1968. http://poincare.matf.bg.ac.rs/~zarkom/Book_Shaums_Group_theory.pdf.

[3] Bernstein, D. J., Birkner, P., Joye, M., Lange, T., and Peters, C. Twisted edwards curves. Cryptology ePrint Archive, Report 2008/013, March 13, 2008. https://eprint.iacr.org/2008/013.

[4] Josefsson, S., and Liusvaara, I. Edwards-curve digital signature algorithm (eddsa). RFC 8032, January, 2007. https://tools.ietf.org/html/rfc803.

[5] Okeya, K., Kurumatani, H., and Sakurai, K. Elliptic curves with the montgomery-form and their cryptographic applications. In *Proceedings of the Third International Workshop on Practice and Theory in Public Key Cryptography: Public Key Cryptography* (London, UK, UK, 2000), PKC '00, Springer-Verlag, pp. 238–257.