Curves

四种形式的椭圆曲线

Short Weierstrass 形式的椭圆曲线表示 $y^2 = x^3 + ax + b$

蒙哥马利曲线 (Montgomery Curve) $BY^2 = X^3 + AX^2 + X$

爱德华曲线 (Edwards Curves) $x^2 + y^2 = 1 + dx^2y^2$

扭曲爱德华曲线(Twisted Edwards Curves) $aX^2 + Y^2 = 1 + dX^2Y^2$

> 四种形式的曲线构造可以转换，约束关系、映射关系的详细推导 **见此**

Curve25519

Curve25519 是基于素数域 $\mathbb{F}_q$, $q = 2^{255} - 19$ 上的蒙哥马利曲线, 曲线方程为 $y^2 = x^3 + 486662x^2 + x$.

Curve25519 曲线双向有理等价于 (Birational Equivalent) 扭曲爱德华曲线 Edwards25519:
$x^2 + y^2 = 1 + (121665/121666)x^2y^2$,

扭曲爱德华曲线则同构于 (Isomorphic) 爱德华曲线 untwisted-Edwards25519:
$-x^2 + y^2 = 1 - (121665/121666)x^2y^2$.

单位元：(0,1)

完备加法运算：$(x_1, y_1) + (x_2, y_2) = (\frac{x_1y_2 + x_2y_1}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - ax_1x_2}{1 - dx_1x_2y_1y_2})$

Sign

EdDSA 的基本定义

EdDSA (Edwards-Curve Digital Signature Algorithm) 是 Schnorr 签名方案在 **Edwards 曲线** 上实现的一种变体。常见的实例有 Ed25519、Ed448 等。 Ed25519 是在扭曲爱德华兹曲线（Twisted Edwards curves）上实现的。它具有速度快，密钥较短，安全性高等优点。

EdDSA 具有以下 11 个参数:

1. 奇质数幂 p ，为有限域 $\mathbb{GF}(p)$ 的阶
2. $b \in \mathbb{Z}$， $2^{b-1} > p$

   EdDSA 公钥恰好具有 b 位，而 EdDSA 签名恰好具有 $2b$ 位。
   建议 b 为 8 的倍数，可使公钥和签名长度是八位字节的整数。
3. 有限域 $\mathbb{GF}(p)$ 的元素的 $b - 1$ 位编码
4. 杂凑函数 H，具有 $2b$ 位输出

   建议使用保守的杂凑函数（即在其中不可能产生冲突的杂凑函数），并且对 EdDSA 的总成本没有太大影响。
5. $c \in \mathbb{Z}$，取值为 2 或 3

   椭圆曲线的余因子，EdDSA 中的秘密标量是 2^c 的倍数。整数 c 是辅因子的以 2 为底的对数。
6. $n \in \mathbb{Z}$ $c \leq n < b$

EdDSA 中的秘密标量具有 n + 1 位，最高位（第 2^n 位）始终预设，最低 c 位始终清零。

7. $d \in \mathbb{GF}(p)$，非平方元素

   $\mathbb{F}_p$ 中的二次非剩余，常建议将其取为最接近零的值。

8. $a \in \mathbb{GF}(p)$，$a \neq 0$，非零平方元素

   通常的最佳性能建议是：
   如果 $p \mod 4 = 1$，则 $a = -1$；
   如果 $p \mod 4 = 3$，则 $a = 1$ 。

9. $B \neq (0,1), B \in E = \{(x,y) \in \mathbb{GF}(p)^2 | ax^2 + y^2 = 1 + dx^2y^2\}$

10. 奇数质数 L，使得 $[L]B = 0$，$2^c L = \#E$

    $[L]B$ 表示 B 自身相加 L 次。
    *数字 $\#E$（曲线上的点数）是为椭圆曲线 E 提供的标准数据的一部分，或可由【**辅因子 阶数 *】计算得到。*

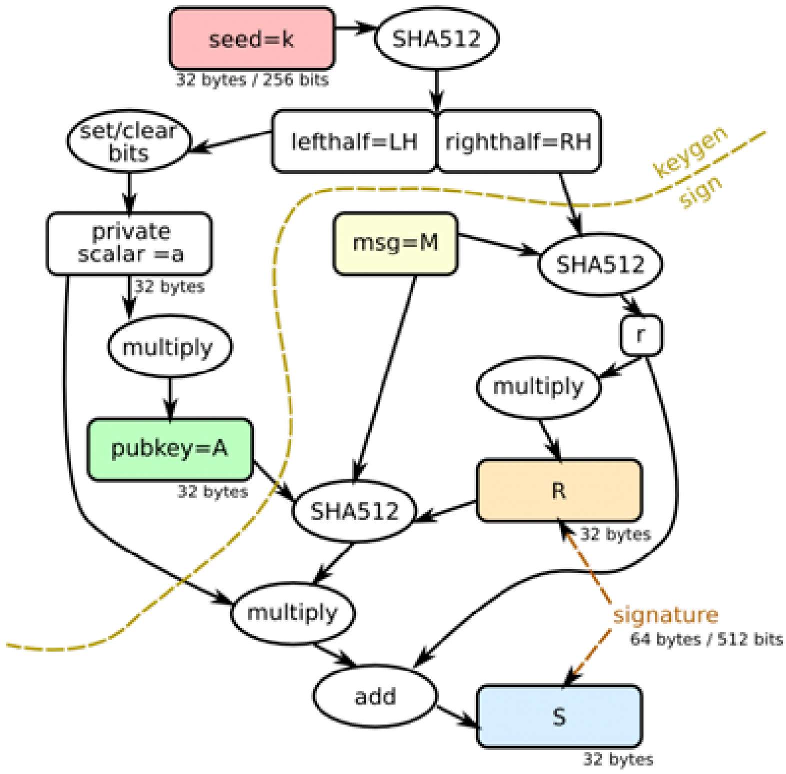
11. “预杂凑”函数 PH

    PureEdDSA 指使用恒等函数作为 PH 的方案，即 $PH(M) = M$
    HashEdDSA 指无论消息有多长，PH 都会生成短输出的方案，
    如 $PH(M) = SHA-512(M)$。
    因此在出现哈希碰撞的情况下，HashEdDSA 无法保证安全性，而 PureEdDSA 则不会受到影响。

这里给出 Ed25519 采取的参数：

> $p = 2^{255} - 19$
>
> $b = 256$
>
> $encoding\ of\ \mathbb{GF}(p)$: 255-bit little-endian encoding of $\{0, 1, \ldots, p-1\}$
>
> $H(x)$ =SHA-512(x)
>
> $c = 3$
>
> $n = 254$
>
> $d = -121665/121666 = 37095705934669439343138083508754565189542113879843219016388785533085940283555$
>
> $a = -1$
>
> $B = (15112221349535400772501151409588531511454012693041857206046113283949847762202, 46316835694926478169428394003475163141307993866256225615783033603165251855960)$
>
> $L = 2^{252} + 27742317777372353535851937790883648493$
>
> $PH(x)$：恒等函数

签名过程



$KeyGen$:

输入：参数 $(p, b, ENC, h, c, n, d, a, B, L, PH)$

输出：密钥对 $(k, ENC(A))$

1. 随机生成长度为 b 的二进制数 k 作为私钥
2. 对 k 计算哈希 $h = H(k) = (h_0, \ldots, h_{2b-1})$
3. 计算 $a = 2^n + \sum_{c \le i \le n-1} 2^i h_i$
4. 计算 $A = (x_A, y_A) = aB$
5. 计算 A 的编码 $\underline{A} = ENC(A)$ 作为公钥

方法：首先计算 y_A 的 $(b-1)$ 位编码；若 x 为负，则将其与 1 相连；如果 x 不为负，则与 0 相连。

6. 返回密钥对 $(k, ENC(A))$

$Sign$:

输入：参数 $(p, b, ENC, h, c, n, d, a, B, L, PH)$，消息 M

输出：签名 $(ENC(R)||ENC(S))$

1. 计算 $r = H(h_b, \ldots, h_{2b-1}, M) \in \{0, \ldots, 2^{2b} - 1\}$
2. 计算 $R = [r]B$
3. 计算 $S = (r + H(ENC(R)||ENC(A)||PH(M))a) \ \ mod \ \ L$
4. 返回签名 $(ENC(R)||ENC(S))$

$Verify$:

输入：参数 $(p, b, ENC, h, c, n, d, a, B, L, PH)$，消息 M ，密钥对 $(k, ENC(A))$，签 名 $(ENC(R)||ENC(S))$

输出：1 （签名通过验证），0 （签名未通过验证）

1. 分别由 $ENC(A)$，$ENC(R)$ 计算出A, R
2. 若 $A \notin E$ 或 $R \notin E$ 或 $S \notin \{0, 1, \ldots, L-1\}$，返回 0

> 3. 计算 $H(ENC(R), ENC(A), M)$
> 4. 判断方程组 $[2^cS]B = 2^cR + [2^ch]A$ 是否成立
> 5. 若方程成立，返回 1；若不成立，返回 0

RFC

RFC 774811 ：

- 椭圆曲线 Curve25519 和 Curve448
- 基于这两条曲线 的 ECDH 协议规范: X25519 和 X448.

RFC 803212 ：

- EdDSA 签名机制
- 基于椭圆曲线 Edwards25519 和 Edwards448 的 EdDSA 算法的具体实例化:
    - Ed25519, Ed25519ph, Ed25519ctx, Ed448, Ed448ph.

ed25519 **原理及密码库性能对比**