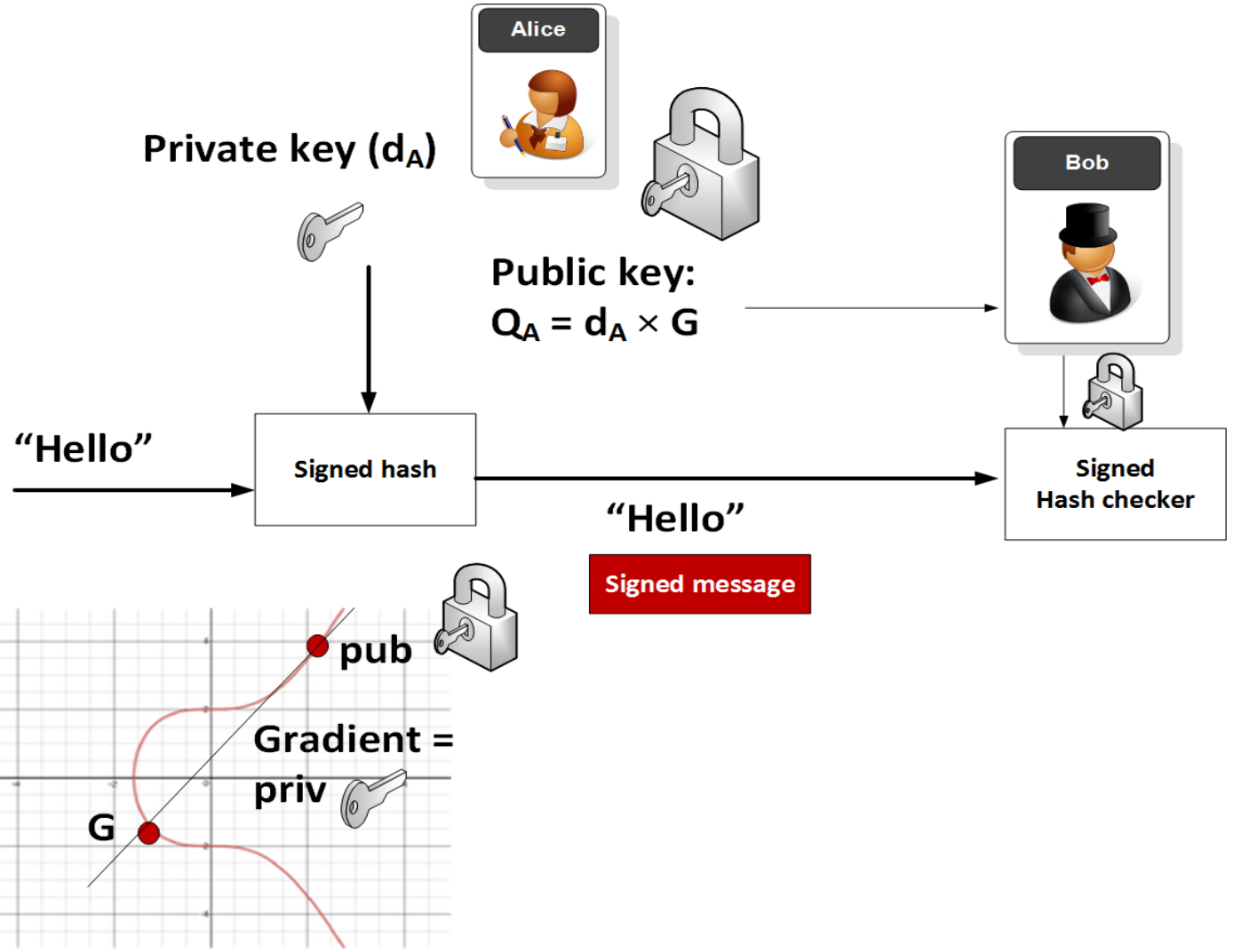
عملکرد ECDSA

درس: امنیت سایبری

استاد: سلمان نیک صفت

تهیه کننده: زهرا باقرزاده خلخالی

امضا دیجیتال

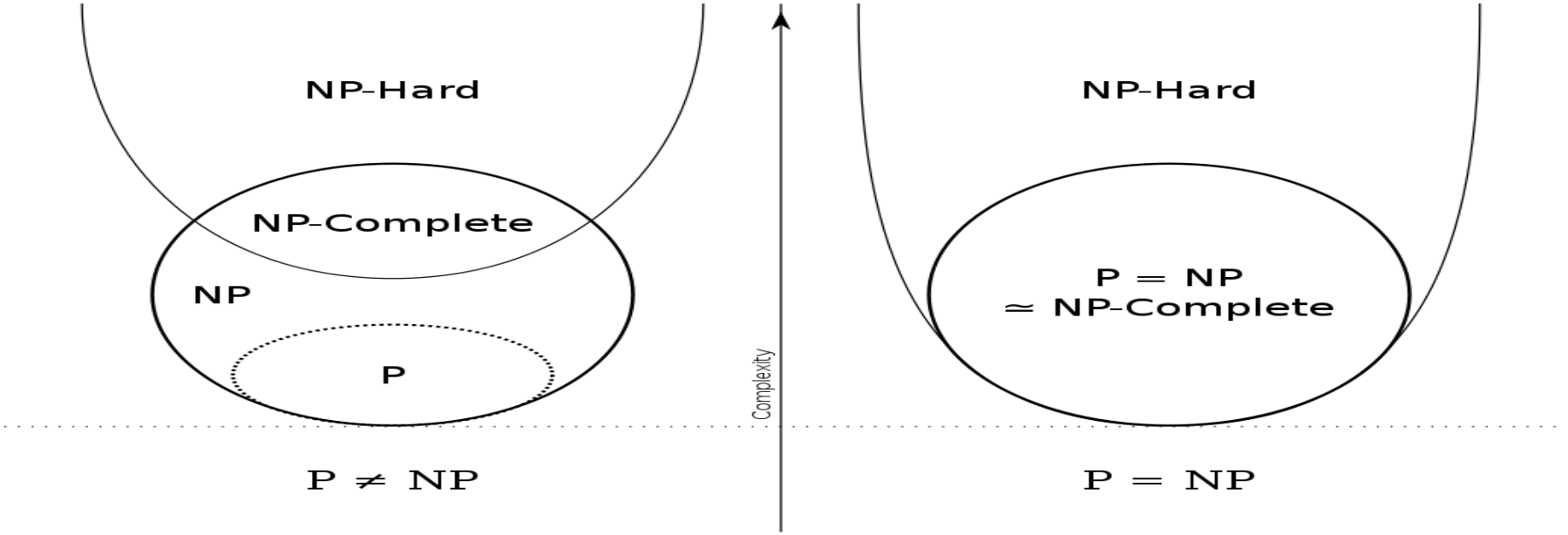


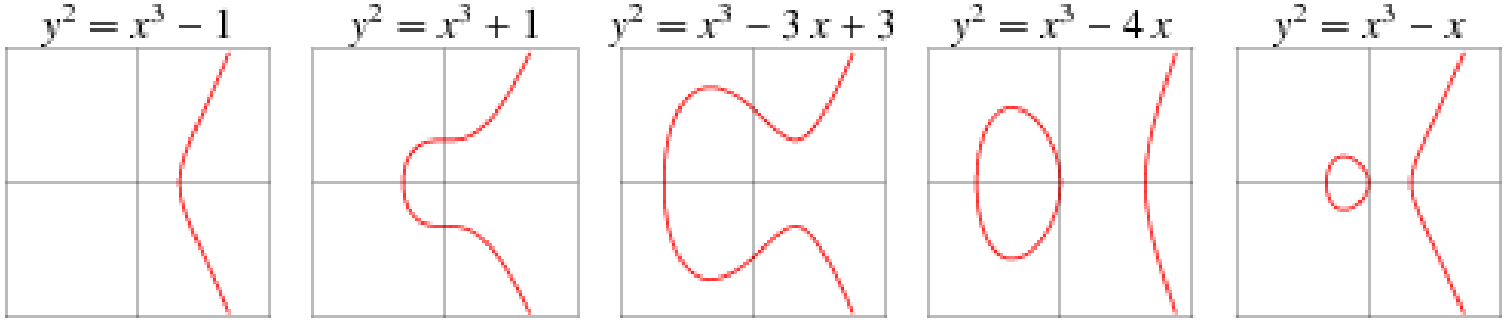
- تایید اعتبار امضا
- فقط امضا کننده امکان ایجاد آن را دارد.
- یک امضا دیجیتال شامل سه الگوریتم :

1. ایجاد کلید عمومی و خصوصی
2. امضا سند یا پیام
3. تایید امضا توسط شخص گیرنده

چرا استفاده از منحنی بیضوی

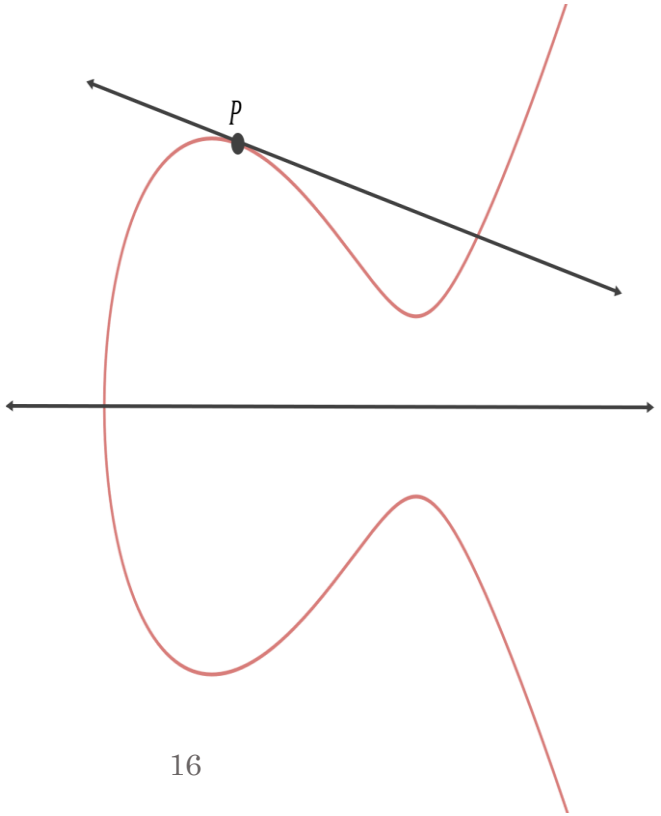
- امضا دیجیتال باید دارای دو شرط تایید امضا بر روی سند یا پیام ارسالی و نیز جعل ناپذیری باشد.
- یک روش برای تولید کلید های رمز نگاری استفاده از مسئله np-hard خم بیضوی

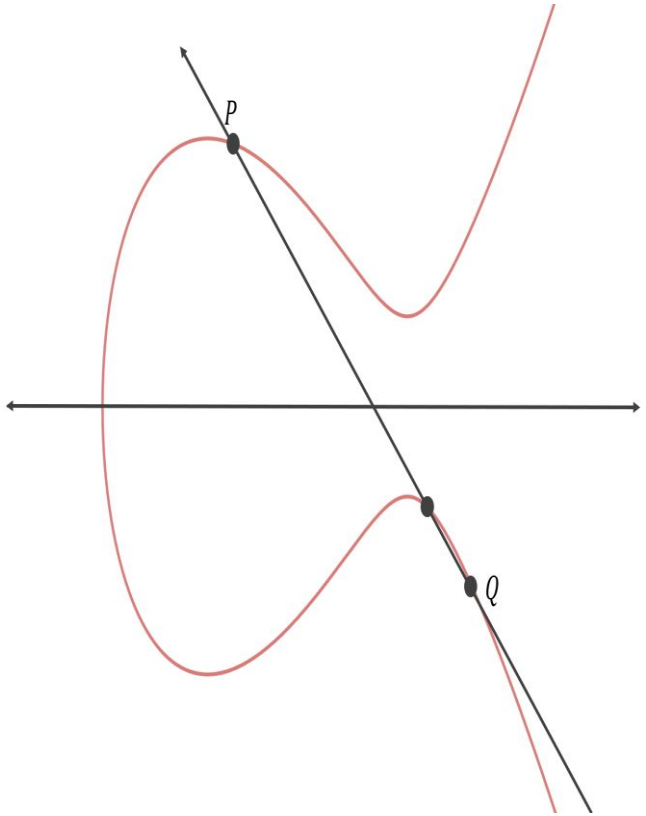


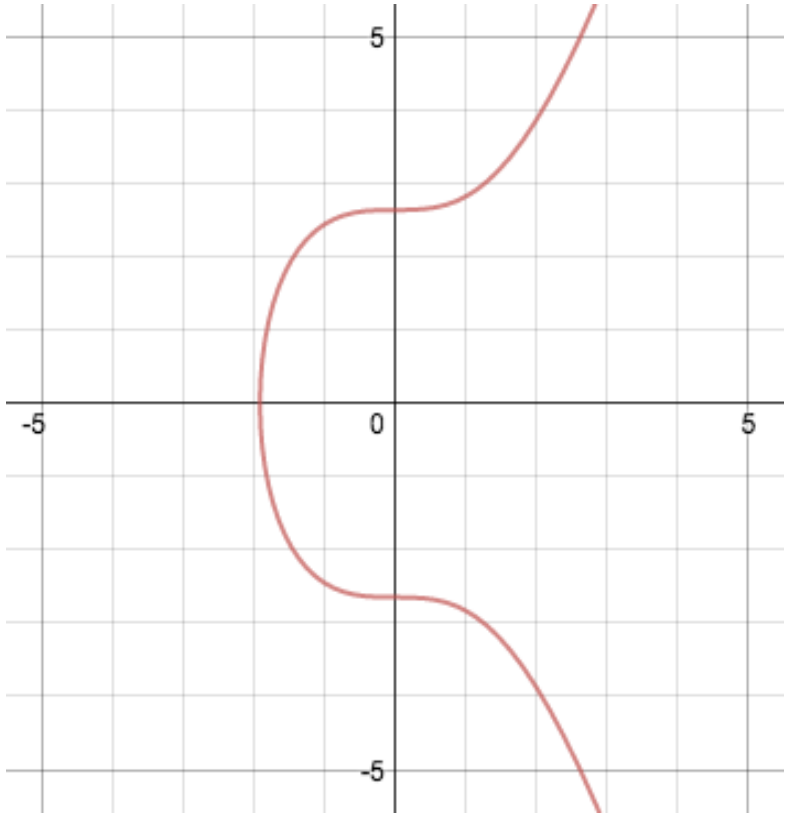


خم بیضوی

- $y^2 = x^3 + ax + b$
- قرینگی

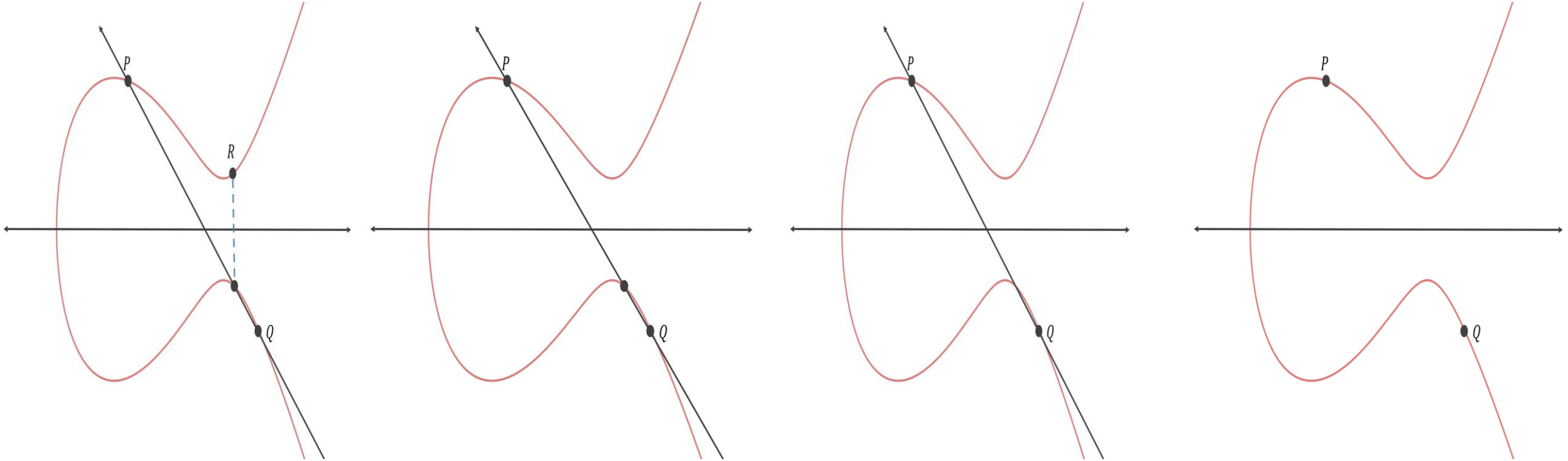




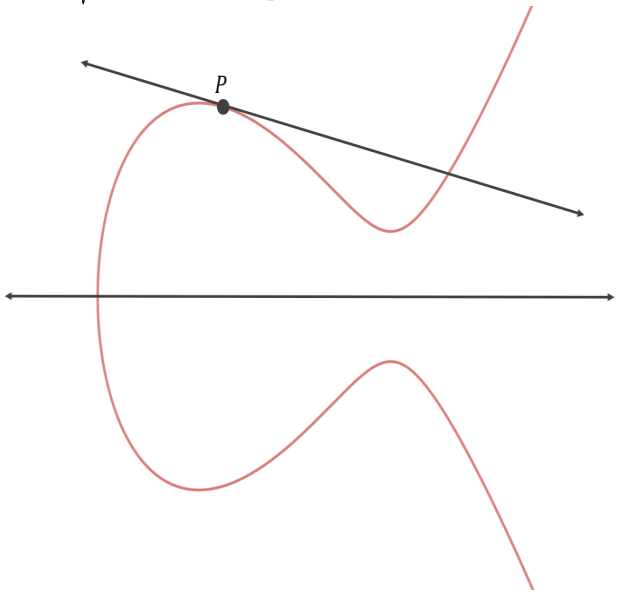


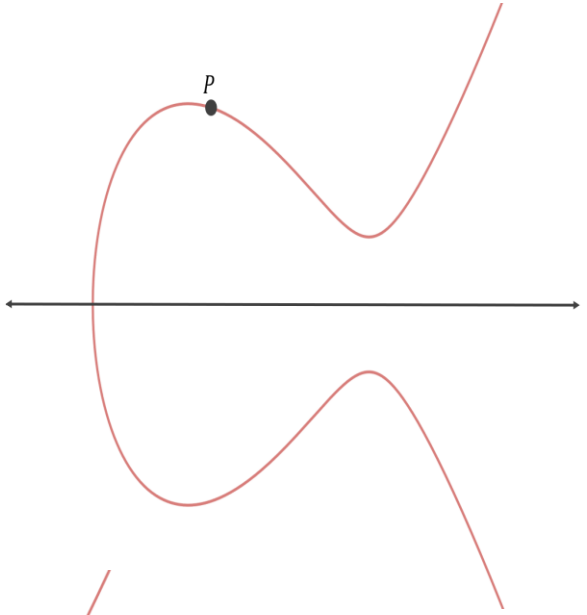
16

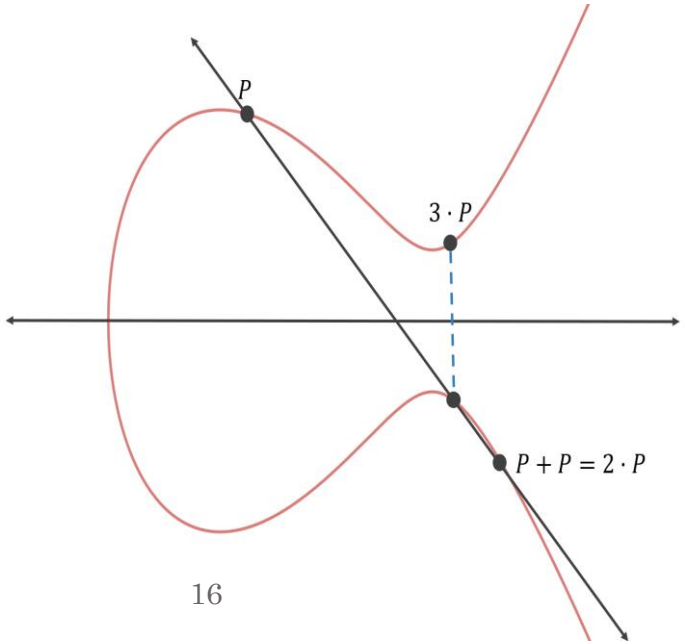
جمع نقاط روی منحنی

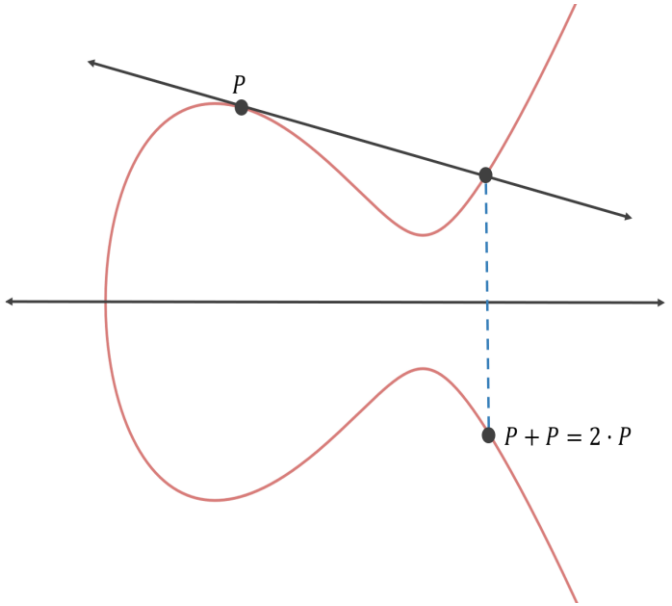


رمزنگاری با استفاده از خم بیضوی







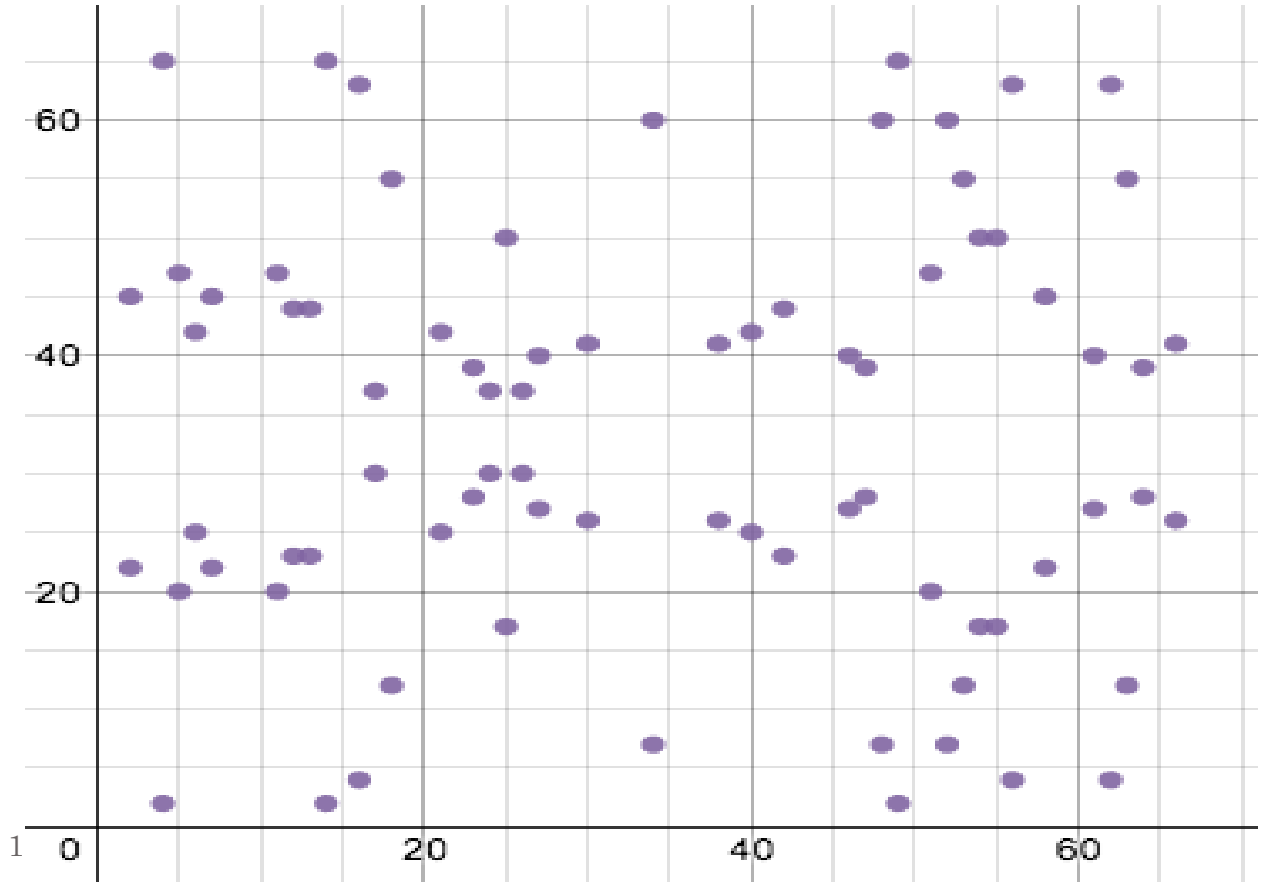


تعداد محاسبات لازم برای جمع نقاط

- 10P = P+P+P+P+P+P+P+P+P+P
- 10p = p+9p
- p+3(3p)
- p+3(p+2p)
- ؟ $x \in [0,2^{256}-1]$ => Number of calculation steps x*P <= 510

میدان های متناهی

- میدان متناهی در بافت ECDSAرا می‌توان به صورت طیف از پیش تعیین شده ای از اعداد مثبت در نظر گرفت که در این طیف هر محاسبه‌ای قابل انجام است. هر عددی خارج از این محدوده گرد می‌شود و داخل طیف قرار می‌گیرد.
- $x \in N, y \in R, z = y \,\%\, x \in [0, x-1]$
- منحنی های بیضوی در بافت میدانی $\mod 67$



عملکرد الگوریتمECDSA

- در مورد بیت کوین شرایط زیر برقرار است:
- **معادله منحنی بیضوی:**
- $y^2 = x^3 + 7$
- **ماژول اصلی:** $2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1$
- **نقطه پایه ای:**
- **ترتیب:**

کلیدهای خصوصی و کلیدهای عمومی

- کلید خصوصی = یک عدد غیر قابل حدس بین 1 تا ترتیب
- کلید عمومی= کلید خصوصی * نقطه پایه ای
- محاسبه $r= p+q$ ،p,q دو نقطه روی منحنی بیضوی

- $c = (q_y - p_y) / (q_x - p_x)$
  $r_x = c^2 - p_x - q_x$
  $r_y = c\,(p_x - r_x) - p_y$

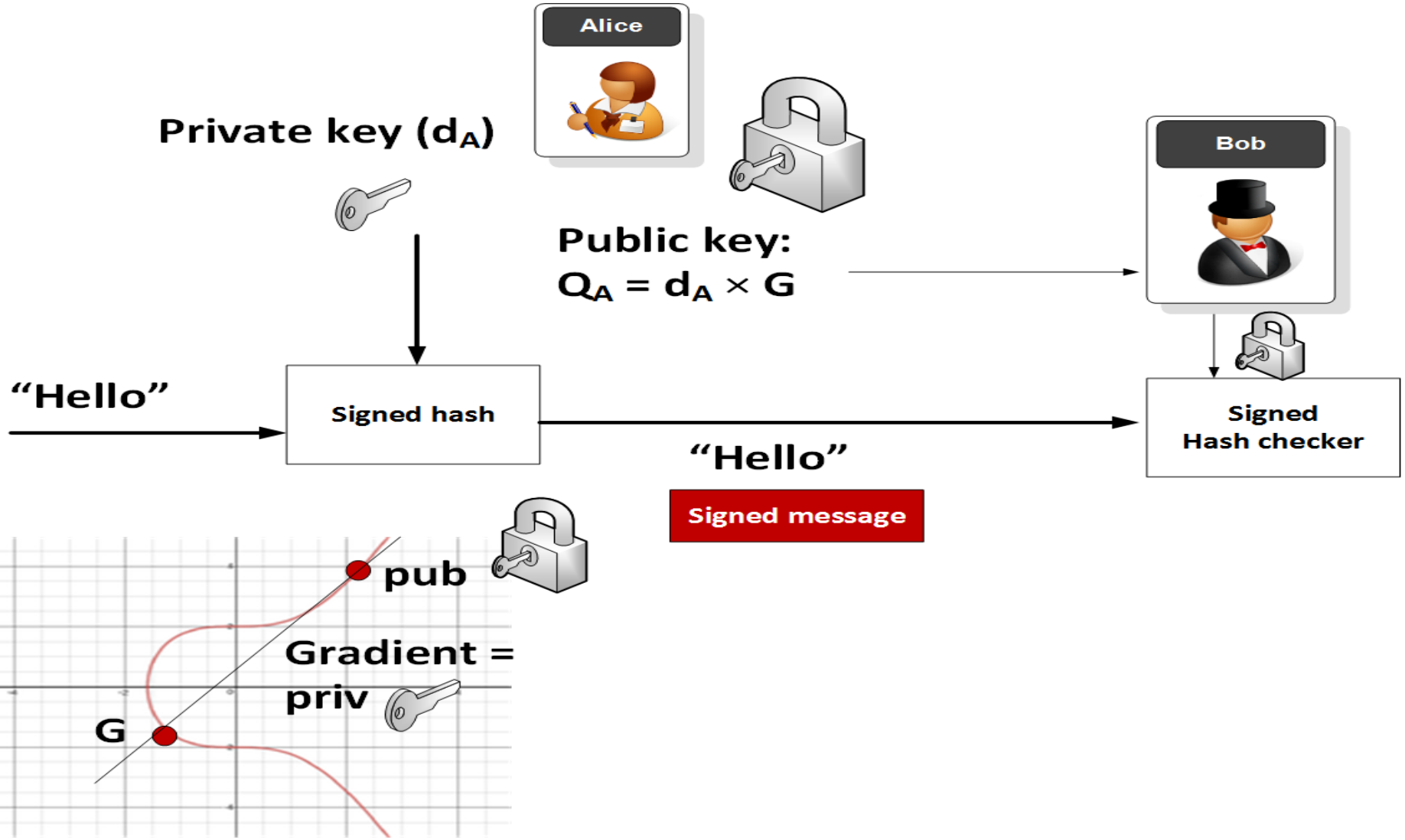
- محاسبه $r= 2p$ که p نقطه ای مماس بر منحنی بیضوی

- $c = (3p_x^{\,2} + a) / 2p_y$
  $r_x = c^2 - ۲p_x$
  $r_y = c\,(p_x - r_x) - p_y$

مثال ساده از نحوه عملکرد الگوریتم

- $y^2 = x^3 + 7$ ، ماژول اصلی ۶۷ ، نقطه پایه ای (۲و۲۲) ،تکرار ۷۹ و کلید خصوصی ۲
- $c = \frac{3*2^2+0}{2*22} mod(67) = \frac{12}{44} mod(67)$
- $44^{-1} = 32$ پس داریم:
- $c = 12 * 32 \, mod(67) = 49$
- $r_x = (49^2 - 2 * 2) mod(67) = 2397 \, mode(67) = 52$
- $r_y = (49 * (2 - 52) - 22) mod(67) = -2472 \, mod(67) = 7$
- کلید عمومی ما متناظر با نقطه $(52,7)$ است. تمام این اقدامات برای کلید خصوصی ۲ می‌باشد.

مراحل امضا و تایید امضا



امضای اطلاعات با کلید خصوصی

- $k \in [1, n-1]$
- $R = k * G \; such \; that \; G \; is \; a \; random \; poin \; on \; EC$
- کلید عمومی : $r = R_x \% \, n$
- $s = \frac{z + r*d}{k} \%(n)$
- امضا (r,s)
- مثال: z=17, n=79,G = (2, 22), d=2, k = 3,(x,y)=3G = (62,63), r=62, s=47,

تایید امضا با استفاده از کلید عمومی

- Q کلید عمومی، مقدار پایه G، مقدار امضا (r,s)، z داده اصلی، میدان متناهی mod n
- $w = s^{-1} \bmod n$
- $u = z * w \bmod n$
- $v = r * w \bmod n$
- $(x,y) = uG + vQ$
- تایید $r = x \bmod n$. در غیر این صورت امضا نامعتبر است.
- مثال: $z=17,\ (r, s) = (62, 47), n=79,\ G = (2, 22),\ Q = (52, 7),$
- $w = s^{-1} \bmod n = 47^{-1} \bmod 79 = 37$
- $u = zw \bmod n = 17 * 37 \bmod 79 = 629 \bmod 79 = 76$
- $v = rw \bmod n = 62 * 37 \bmod 79 = 2294 \bmod 79 = 3$
- $(x, y) = uG + vQ = (x, y) = (62, 4) + (11, 20) = (62, 63)$

مثال دیگری از استفاده از ECDSA

- JWT Token Generation
  - بیت کوین و اتریوم و برخی رمز ارزهای دیگر از این منحنی ها به شکل استفاده می‌کنند(a=0, b=7) اصطلاحا به الگوریتمی که از آن استفاده می‌کند secp256k10 می‌گویند
  - در الگوریتم secp256k10 نقطه اولیه
  - مختصات x:
  - 55066263022277343669578718895168534326250603453777594175500187360389116729240
  - مختصات y:
  - 32670510020758816978083085130507043184471273380659243275938904335757337482424

مراجع

- آشنایی با رمزنگاری خم های بیضوی-مجتبی بهرامیان-فرهنگ و اندیشه ریاضی-سال 38 شماره 64-1398
- The Elliptic Curve Digital Signature Algorithm (ECDSA)-Don Johnson1, Alfred Menezes, Scott Vanstone-2001
- https://docs.mashery.com/connectorsguide/GUID-B5131DD5-C60F-4979-81C3-E0FC79ABA309.html
- https://fa.wikipedia.org/wiki/%D8%B1%D9%85%D8%B2%D9%86%DA%AF%D8%A7%D8%B1%DB%8C_%D9%85%D9%86%D8%AD%D9%86%DB%8C_%D8%A8%DB%8C%D8%B6%D9%88%DB%8C
- https://persianmine.com/math-behind-bitcoin/

16