Cibersegurança e Confiança: Alguns Aspectos Criptográficos

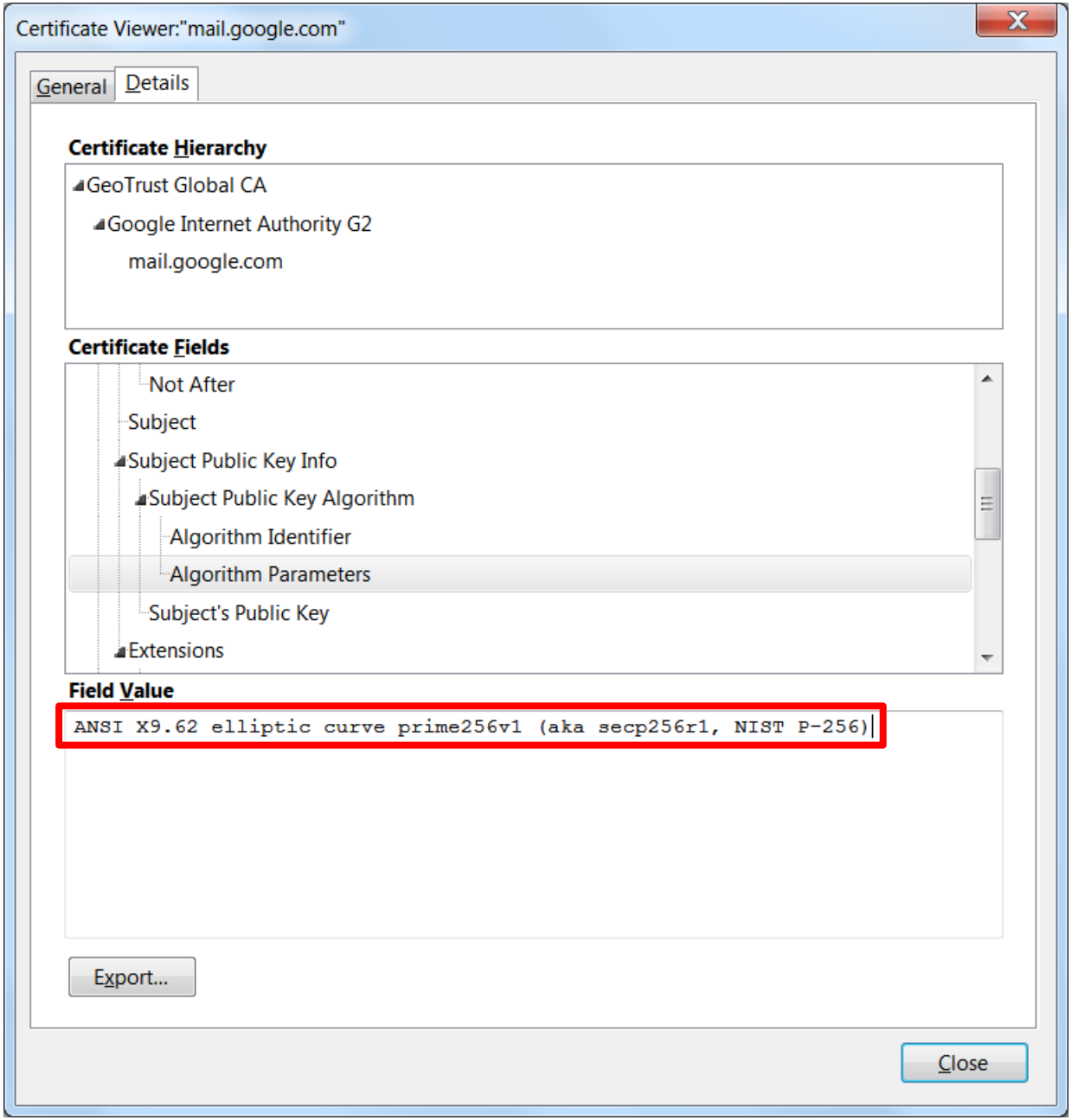
Paulo S. L. M. Barreto

Professor Associado
Poli/USP

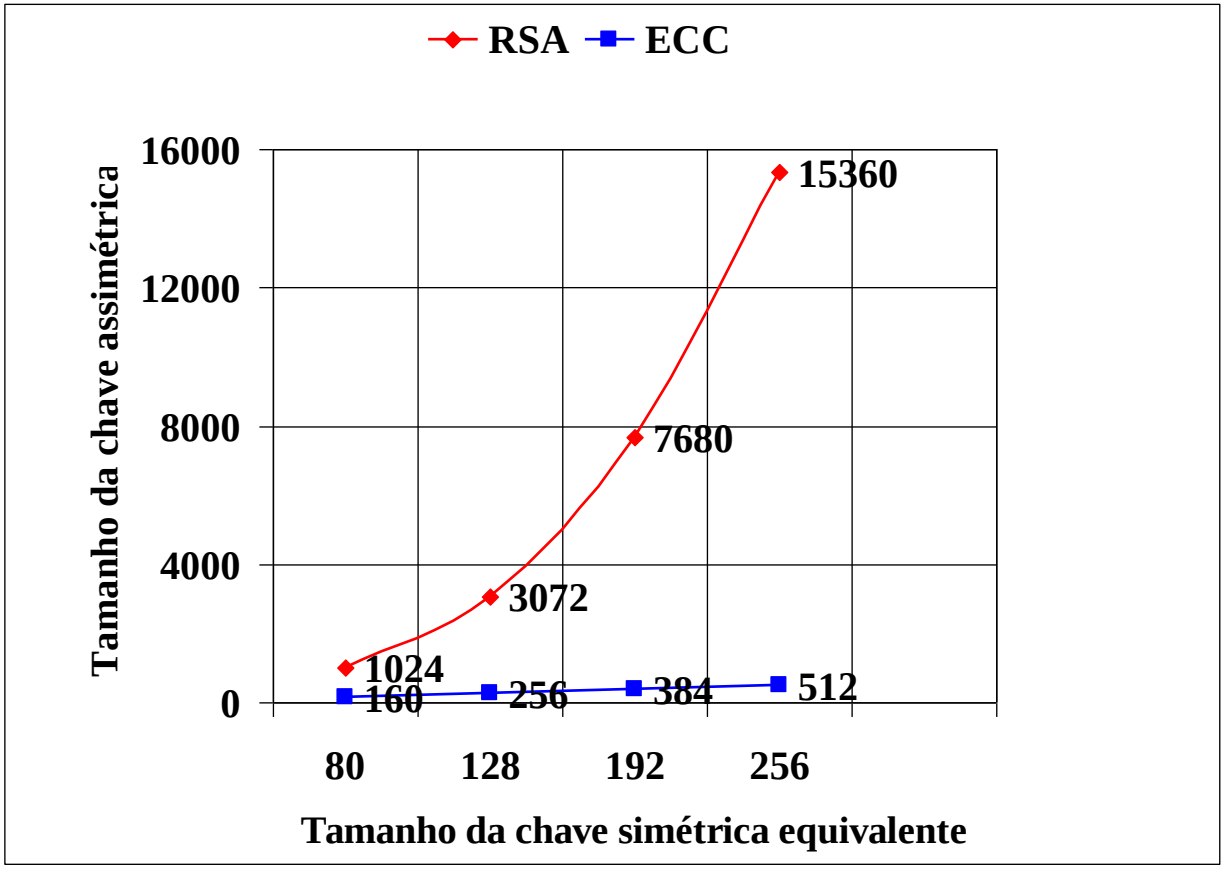
Universidade de São Paulo
USP

Curvas Elípticas

- Grandes provedores de serviços em nuvem oferecendo acesso “seguro”.
  - NB: segurança de protocolos do tipo TLS é um assunto à parte…
- Tendência: substituição de criptografia RSA por curvas elípticas (ECC).


Certificate Viewer:"mail.google.com"
General
Details
Certificate Hierarchy
GeoTrust Global CA
Google Internet Authority G2
mail.google.com
Certificate Fields
Not After
Subject
Subject Public Key Info
Subject Public Key Algorithm
Algorithm Identifier
Algorithm Parameters
Subject's Public Key
Extensions
Field Value
ANSI X9.62 elliptic curve prime256v1 (aka secp256r1, NIST P-256)
Export...
Close

RSA vs ECC



Fonte: NIST Special Publication 800-57, Recommendation for Key Management – Part 1: general, 2007.

Curvas Elípticas

- ***QUAIS CURVAS?***

- ***QUAIS ALGORITMOS?***

Curvas NIST/NSA

- Grande número de normas internacionais adoptam um conjunto comum de curvas (NIST FIPS 186, ANSI X9.62/X9.63, SECG)
- Tecnologia de projeto de curvas data do final dos anos 1990's.
- Construídas efetivamente por Jerry Solinas (funcionário da NSA).

Curvas NIST/NSA

Curve P-256 ($p = 2^{256} - 2^{224} + 2^{192} + 2^{96} - 1$)

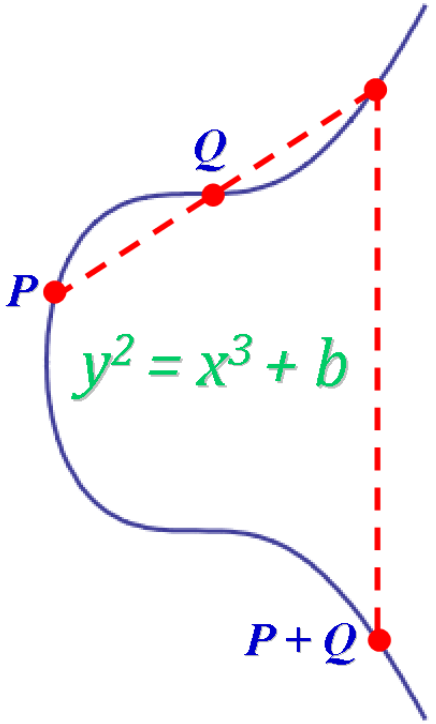
```
p      11579208921035624876269744694940757353008614341529031419553363130886709785395 1
seedE  0x c49d3608 86e70493 6a6678e1 139d26b7 819f7e90
r      0x 7efba166 2985be94 03cb055c 75d4f7e0 ce8d84a9 c5114abc af317768 0104fa0d
a      -3
b      0x 5ac635d8 aa3a93e7 b3ebbd55 769886bc 651d06b0 cc53b0f6 3bce3c3e 27d2604b
xG     0x 6b17d1f2 e12c4247 f8bce6e5 63a440f2 77037d81 2deb33a0 f4a13945 d898c296
yG     0x 4fe342e2 fe1a7f9b 8ee7eb4a 7c0f9e16 2bce3357 6b315ece cbb64068 37bf51f5
n      11579208921035624876269744694940757352999695522413576034242225906106851204
       4369
h      1
```

- Vulnerabilidade rara (~1 a cada 10^{12} curvas) ?
- Potencial porta dos fundos conhecida somente por quem construiu a curva.

Sistemas de e-Cash

- Exemplo: Bitcoin.

- Assinaturas digitais ECDSA com a curva **`secp256k1`**: $y^2 = x^3 + 7$ sobre $\mathbb{F}_{2^{256}-2^{32}-977}$.



- Segurança $\sim 2^{36}$ (tempo para quebrar num PC comum: ~62 s) em vez de $\sim 2^{128}$ se um teste crítico for omitido!

Sistemas de e-Cash

```
416                 if (!EC_POINT_set_affine_coordinates_GFp(group, point, x, y, ctx)) goto err;
417                 }
418 #ifdef DEBUG
419         if (!EC_POINT_is_on_curve(group, point, ctx)) /* test required by X9.62 */
420                 {
421                 ECerr(EC_F_EC_GFP_SIMPLE_OCT2POINT, EC_R_POINT_IS_NOT_ON_CURVE);
422                 goto err;
423                 }
424 #endif
425         ret = 1;
426
427 err:
428         BN_CTX_end(ctx);
429         if (new_ctx != NULL)
430                 BN_CTX_free(new_ctx);
```

- Um número muito elevado de vulnerabilidades deve-se a erros de programação (vide HeartBleed).

Gerador Dual EC 

- Geração “segura” de números aleatórios.
- NSA pagou US$ 10^7 para pelo menos uma empresa adotar o gerador Dual EC como default (fonte: Snowden).
- Depois de 7 anos em uso, NIST retirou o algoritmo da norma SP 900-90A.

Direções?

- Esforço corrente do Crypto Forum Research Group (CRFG) e da IETF para escolher novas curvas.
- Obstáculos (migração de padrões)!
- Vantagens (tecnologia ~20 anos mais moderna e robusta que as curvas NIST).

Curve	algorithm	security	signing	verification
Ed25519	EdDSA	2^{128}	**63.5**	**205.7**
P-224	ECDSA	2^{112}	**264.9**	**553.8**

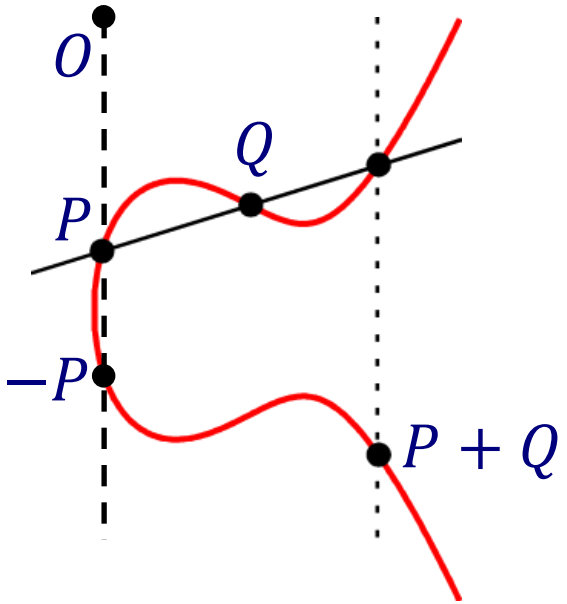
Fonte: eBACS – ECRYPT Benchmarking of Cryptographic Systems; SAC 2015

OBRIGADO!

APÊNDICE

Grupos Elípticos

- Exemplo: conjunto de pontos de uma curva elíptica $y^2 = x^3 + ax + b$.
- Lei de secantes e tangentes.
- Fórmulas para calcular diretamente as coordenadas do ponto $(x_P, y_P) + (x_Q, y_Q)$:



Problema do Logaritmo Discreto (Elíptico)

- Dados P e x, é "fácil" calcular $Y = xP$.
- Dados P e Y, é "difícil" calcular x.
- Com valores de k bits, $\approx k^3$ passos para calcular Y (esforço *polinomial*).
- Para calcular x, são necessários $\approx 2^{k/2}$ passos computacionais (esforço *exponencial*).

Gerador Dual EC 

- Geração de números aleatórios.
- Escolher pontos "aleatórios" P e Q.
- Escolher semente aleatória r_0.
- Para $i = 1, 2, 3, \ldots$:
  - Calcular $r_i \leftarrow (r_{i-1}P)_x$, // NB: $N_i = r_{i-1}P$
  - Usar $k_i \leftarrow (r_i Q)_x$ como i-ésimo número aleatório. // NB: $K_i = r_i Q$

Gerador Dual EC 

- O detalhe crítico é que P e Q são especificados diretamente na norma.

- Exatamente como ocorre em ElGamal, o conhecimento de s tal que $Q = sP$ permite recuperar mais informação sobre o sistema.

Gerador Dual EC

- Obtendo um único aleatório $k_i = (r_i Q)_x$, a entidade que conhece s (*aka* NSA) pode reconstruir $r_i Q = r_i s P = s(r_i P) = s N_{i+1}$, recuperar $N_{i+1} = s^{-1}(r_i Q)$, e prever todos os números "aleatórios" posteriores $r_{i+d} = (N_{i+d})_x$, $d = 1, 2, 3, \ldots$