Vorlesung (WS 2014/15)

Sicherheit: Fragen und Lösungsansätze

Dr. Thomas P. Ruhroth

TU Dortmund, Fakultät Informatik, Lehrstuhl XIV

Ziele

- Ein Beispiel für „Backdoors“ die abhören vereinfachen
- Problem der Grundrechte/ Abhören

DUAL-EC-DRBG

DUAL-EC-DRBG

EC: Elliptic Curve
DRGB: Deterministic Random Bit Generator

Vorgestellt von NIST im Jahre 2006:
Special Publication 800-90

zusammen mit 3 „traditionellen“ PRNG veröffentlicht

später: ISO-Standard 18031

Initialisierung

p Primzahl

$\Rightarrow$ Z/pZ Moduloring

$\Rightarrow$ EC elliptische Kurve

P, Q Punkte auf EC

s_o Startzustand, kleiner als p

Arbeitsschritt

$$s_{i+1} \,/\, s_i \longrightarrow \varphi(s_i P) \longrightarrow r_i \longrightarrow \varphi(r_i Q) \longrightarrow t_i \longrightarrow LSB_{\text{bitlen-16}}(t_i)$$

$$r_i \longrightarrow \varphi(r_i P) \longrightarrow s_{i+1}$$

- φ extrahiert die x-Koordinate eines Punktes und stellt sie als Bitzahl dar.
- LSB = „Least Signifikant Bit“ entfernt die ersten Stellen eines Bitstrings anhand der gegebenen Vorschrift

Beispiel: Initialisierung

Es sei die elliptische Kurve EC wie in den mathematischen Folien gebildet worden. *(p=17, a=1, b=7)*

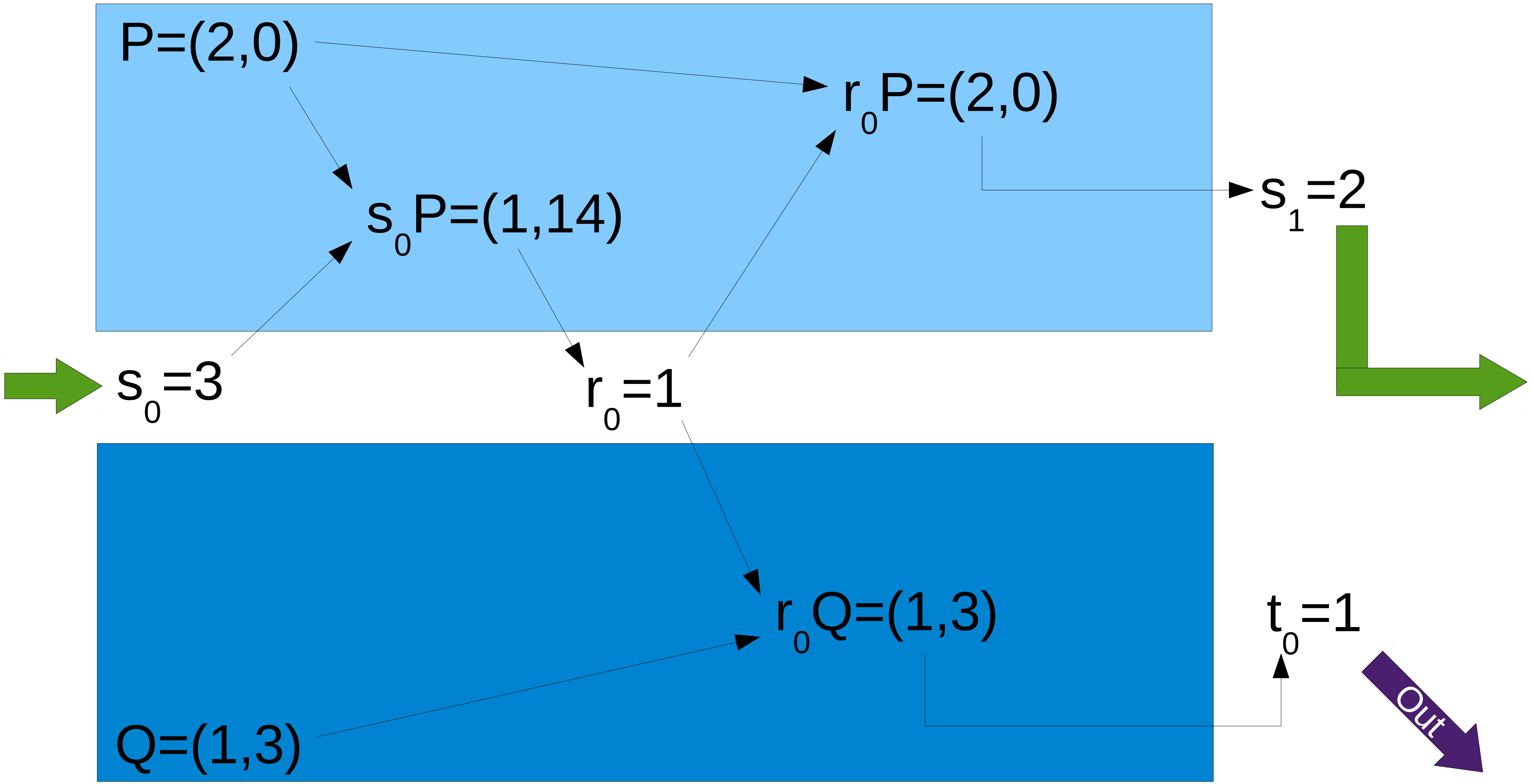
$P=(2,0) \in EC$:
$0^2 = 0$
$2^3 + 1 \cdot 2 + 7 \bmod 17$
$= 8 + 2 + 7 \bmod 17$
$= 17 \bmod 17$
$= 0$

$Q=(1,3) \in EC$:
$3^2 = 9$
$1^3 + 1 \cdot 1 + 1 \bmod 17$
$= 1 + 1 + 7 \bmod 17$
$= 9 \bmod 17$
$= 9$

Sei $s_0 = 3$

LEHRSTUHL 14
SOFTWARE ENGINEERING

Beispiel: Erster Arbeitsschritt



technische universität
dortmund

fakultät für
informatik

Vorteile des DUAL-EC-DRBG

DUAL-EC-DRBG basiert auf einem Problem der Algebra:

Diskrete Logarithmus Problem

Sicherheit algebraisch Beweisbar

Leider „etwas“ langsam

Geeignete Nutzung:
besonders sicherheitskritische Bereiche

Problem: Verfälschung der Ausgabe

$LSB_{bitlen-16}(t_i)$ heißt, dass t_i bis auf 16 Bits ausgegeben wird

16 von 256: nur etwa 6% „Verfälschung“

$LSB_{bitlen-16}(t_i) =: x$?

$t_i = 0000\ 0000\ 0000\ 0001\ x$

$t_i = 0000\ 0000\ 0000\ 0010\ x$

.

.

.

$t_i = 1111\ 1111\ 1111\ 1111\ x$

2^{16}
=
65536

$t = \{\text{mögliche } t_i\}$,

wähle ein $x \in t$

$z = x^3 + ax + b \bmod p$

$y = \sqrt{z} \bmod p$,
falls es existiert

$A = \{A \mid A = (x,y) \in EC, x = t_i\}$

$|t| = 2^{16} \Rightarrow |A| \approx 2^{15}$

$$
\begin{tikzcd}
 & \varphi(r_i P) \arrow[dl] & & & & \\
s_{i+1} \,/\, s_i \arrow[r] & \varphi(s_i P) \arrow[r] & r_i \arrow[ul] \arrow[r] & \varphi(r_i Q) \arrow[r] & t_i \arrow[r] & LSB_{bitlen-16}(t_i)
\end{tikzcd}
$$

Einfach bestimmbar!

Lösung: Verfälschung der Ausgabe

$r_i Q$ und sogar Q seien jetzt bekannt

Diskreter Logarithmus Problem:
nicht effizient lösbar!

r_i = **???**

Außerdem: wirksamere Verfälschung leicht machbar

$$
\begin{tikzcd}
 & \varphi(r_iP) \arrow[dl] & & & & \\
s_{i+1} / s_i \arrow[r] & \varphi(s_iP) \arrow[r] & r_i \arrow[ul] \arrow[r] & \varphi(r_iQ) \arrow[r] & t_i \arrow[r] & LSB_{bitlen-16}(t_i)
\end{tikzcd}
$$

Einfach bestimmbar!

Bringt aber nicht viel!

Problem: P=eQ

EC basiert auf Moduloring Z/pZ
p ist eine Primzahl

$\xrightarrow{\exists\ e}$ P=eQ

Sei A=rQ:

eA=erQ=reQ=rP

Aber: P,Q bekannt $\longrightarrow$ e = **???**

$\varphi(r_i P)$

Schwer bestimmbar!

$s_{i+1} / s_i \longrightarrow \varphi(s_i P) \longrightarrow r_i \longrightarrow \varphi(r_i Q) \longrightarrow t_i \longrightarrow LSB_{bitlen-16}(t_i)$

Einfach bestimmbar!

Bringt aber nicht viel!

Problem: P, Q sind fest gewählt

P,Q sind in der Definition von DUAL-EC-DRNG fest vorgeben

ließen sich relativ leicht selber herstellen

kein Gegenargument angegeben

keine Erklärung, woher sie stammen

Gefahr: P als eQ gewählt

Gefahr: e extrem nützlich

$\varphi(r_i P)$

Schwer bestimmbar!
Es sei denn: e mit
P=eQ bekannt!

Durchaus möglich!!!

$$s_{i+1} / s_i \longrightarrow \varphi(s_i P) \longrightarrow r_i \longrightarrow \varphi(r_i Q) \longrightarrow t_i \longrightarrow LSB_{bitlen-16}(t_i)$$

Einfach bestimmbar!

Bringt aber nicht **(?)** viel!

NIST closed
Ende 2013/Anfang 2014

National Institute of Standards and Technology

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

NIST Closed, NIST and Affiliated Web Sites Not Available

Due to a lapse in government funding, the National Institute of Standards and Technology (NIST) is closed and most NIST and affiliated web sites are unavailable until further notice. We sincerely regret the inconvenience.

The National Vulnerability Database and the NIST Internet Time Service web sites will continue to be available. A limited number of other web sites may also be available.

Notice will be posted here (www.nist.gov) once operations resume. You may also get updates on NIST's operating status by calling (301) 975-8000.

Conferences and other events scheduled during the shutdown are postponed or cancelled. Even after NIST reopens, some NIST events may need to be rescheduled. Once access to NIST Web sites resumes, please see the Conferences and Events (http://www.nist.gov/allevents.cfm) list for updated information on specific events.

Grundrechte

Grundrechte

- Schutz jedes Menschen
  - Vor staatlicher Willkür (z.B. Diktaturen)
  - Willkür von bessergestellten (z.B. gegen Sklaverei, Ausbeutung)
- Schaffung von Entfaltungsmöglichkeiten
  - Meinungsäußerung
  - Wohnung
  - ….

Geschichte: Grundrechte

- Zuerst: Schutz vom Adel vor Willkür des König (Engl. 1215)
- Auswanderer in Virginia kodieren Grundrechte in den Virginia Bill of Rights
  - Gleichheit der Menschen
  - Freiheit
  - Eigentum unverletzlich

1789 – Ein wichtiges Jahr

- Im Rahmen der französischen Revolution:

Französischen Erklärung der Menschen- und Bürgerrechte

- Im Rahmen der Amerikanischen Unabhängigkeit:

Bill of Rights

Erste einklagbare Grundrechte

(Ratifiziert 1791)

Deutschland

- 1848: Frankfurter Nationalversammlung
  Grundrechte des deutschen Volkes
- 1851: Aufhebung
- 1919: Weimarer Reichsverfassung enthalten Grundrechte
- 1933: Außerkraftsetzung der meisten Grundrechte
- 1949: Heute gültige Grundrechte in Deutschland:
  Grundgesetz für die Bundesrepublik Deutschland

Grundrechte D - Auswahl

- Schutz der Menschenwürde (Artikel 1)
- Recht auf die freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt. (Artikel 2)
- Recht auf Leben und körperliche Unversehrtheit. Die Freiheit der Person ist unverletzlich. In diese Rechte darf nur auf Grund eines Gesetzes eingegriffen werden.

  (Artikel 2)
- Grundrecht auf wirkungsvollen Rechtsschutz bzw. Verfahrensgrundrecht auf Gewährung wirkungsvollen Rechtsschutzes (Artikel 2 zusammen mit Artikel 20)

Gefahr ohne Grundrechte

- Verfolgung:
  - 3. Reich: 5,6 bis 6,3 Millionen Menschen ermordet
  - China: „Der große Sprung nach vorn“ 20 Millionen Tote
  - Völkermord in Ruanda: 800.000 Tote
  - DDR: Politische Gefangene: 200.000–250.000
  - DDR: Staatssicherheit

Abhören - NSA

- Ziel.
  - Totale Überwachung aller Bereiche
  - Offizielles Ziel: Verhinderung von Terrortoten
  - Vermutete weitere Ziele:
    - Staatsspionage
    - Wirtschaftsspionage

Gebrochene Grundrechte

- Selbstverwirklichung (z.B. bei Homosexualität)
- Prüfung durch Gerichte und Überprüfung der Gerichte
  - Geheimgerichte – keine Öffentlichkeit
  - Keine Revision und kein Widerspruch durch Betroffene
- Gleichheitsprinzip - Schutz der eigenen Staatsbürgen
- Schutz der Privatsphäre

This is the Ende

ENDE