PRNG vs. CSPRNG – Part III

Michaela Kučerová

MFF UK

November 22, 2014 / Autumn school of algebra

Introduction to Dual_EC_DRBG

Dual_EC_DRBG Dual Elliptic Curve Deterministic Random Bit Generator

- so-called cryptographically secure pseudorandom number generator (CSPRNG)
- created by NSA
- standardized by NIST, ANSI and ISO
- based on the elliptic curve discrete logarithm problem (ECDLP), i.e. given points P and Q on an elliptic curve of order n , find a such that $Q = aP$
- for some time one of the four (now three) CSPRNGs standardized in NIST SP 800-90A.

Organizations

NIST National Institute of Standards and Technology – a non-regulatory agency of the United States Department of Commerce

ANSI American National Standards Institute

ISO International Organization for Standardization

FIPS Federal Information Processing Standards – United States government standards (many FIPS pronouncements are modified versions of standards used in the technical communities, such as ANSI or ISO)

NSA National Security Agency

RSA American computer and network security company named after the initials of its co-founders, Ron **R**ivest, Adi **S**hamir and Len **A**dleman

What happened?

- At Crypto 1997 Adam L. Young and Moti Yung present paper *The Prevalence of Kleptographic Attacks on Discrete-Log Based Cryptosystems*. The paper **gives a recipe on how to build asymmetric backdoors into crypto algorithms based on discrete logs**.
- After September 11, 2001 NSA drives to include Dual_EC_DRBG in the ANSI X9.82 standard.

What happened?

- The possibility of the backdoor in Dual_EC_DRBG by carefully chosen P and Q values was brought up at an ANSI X9.82 meeting.
- As a result, a way was specified for implementers to choose their own P and Q values.

What happened?

- It turned out later that the specific subtle formulation that NIST put into the standard meant that you could only get the crucial FIPS 140-2 validation of your implementation if you used the original compromised P and Q values.
- NIST Special Publication 800-90A from January 2012 says:

  "The Dual_EC_DRBG requires the specifications of an elliptic curve and two points on the elliptic curve. One of the following NIST approved curves with associated points shall be used in applications requiring certification under [FIPS 140]. More details about these curves may be found in [FIPS 186]. If alternative points are desired, they shall be generated as specified in Appendix A.2."

What happened?

- In 2004
  - A draft of ANSI X9.82, Part 3 is published, which includes Dual_EC_DRBG.
  - **RSA makes Dual_EC_DRBG the default CSPRNG in BSAFE.**

What happened?

- In 2005
  - Daniel R. L. Brown and Scott Vanstone's patent application **describes the working of an elliptic curve CSPRNG backdoor** identical to the potential backdoor in Dual_EC_DRBG, and ways to neutralize such a hidden backdoor by choosing alternative curve points and more bit truncation in the output function.
  - ISO 18031 is published, and includes Dual_EC_DRBG.
  - The first draft of NIST SP 800-90A is released to the public, includes Dual_EC_DRBG.

What happened?

- In 2006
  - Kristian Gjøsteen publishes *Comments on Dual-EC-DRBG/NIST SP 800-90, Draft December 2005* showing that part of Dual_EC_DRBG is "not cryptographically sound", and constructing a bit-predictor with an advantage of 0.0011, which is considered **unacceptable for a CSPRNG**.
  - Daniel R. L. Brown publishes *Conjectured Security of the ANSI-NIST Elliptic Curve RNG*
    This paper proves that, if three conjectures are true, then the Dual_EC_DRBG is secure. The three conjectures are hardness of the elliptic curve decisional Diffie-Hellman problem and the hardness of two newer problems, the x-logarithm problem and the truncated point problem.

What happened?

- In 2006
  - NIST SP 800-90A is published, includes Dual_EC_DRBG with the defects pointed out by Kristian Gjøsteen and others not having been fixed.

What happened?

- In 2013
  - Existence of NSA's Bullrun program is revealed, based on the Snowden leaks. One of the purposes of Bullrun is described as being "to covertly introduce weaknesses into the encryption standards followed by hardware and software developers around the world."
  - New York Times reported that documents in their possession but never released to the public "appear to confirm" that the backdoor was real, and had been deliberately inserted by the National Security Agency as part of the NSA's Bullrun decryption program.

What happened?

- In 2013
  - **RSA Security advises** its customers to stop using Dual_EC_DRBG in RSA Security's BSAFE toolkit and Data Protection Manager, citing NIST guidance made Sept. 12, 2013 that indicated: "**NIST strongly recommends that**, pending the resolution of the security concerns and the re-issuance of SP 800-90A, **the Dual_EC_DRBG, as specified in the January 2012 version of SP 800-90A, no longer be used.**"
  - Reuters reports on the existence of a $10 million deal between RSA and NSA to set Dual_EC_DRBG as the default CSPRNG in BSAFE.

What happened?

- In 2014
  - **NIST removed Dual_EC_DRBG** as a cryptographic algorithm from its draft guidance on random number generators, recommending "that current users of Dual_EC_DRBG transition to one of the three remaining approved algorithms as quickly as possible."

What is Dual_EC_DRBG?

- **Let us focus at NIST Special Publication 800-90A from January 2012.**
- Let p be a specific large prime number and let x, y be unknown.
  Dual_EC_DRBG uses an elliptic curve given by equation

$$y^2 = x^3 - 3x + b$$

  over $\mathbb{Z}_p$.
- For an appropriate $b \in \mathbb{Z}_p$ the points of the curve with an addition create a group.
- Let n be an order of the elliptic curve group.
- In the Recommendation are three curves with specified values of p, n, b, P_x, P_y, Q_x, Q_y.

What is Dual_EC_DRBG?

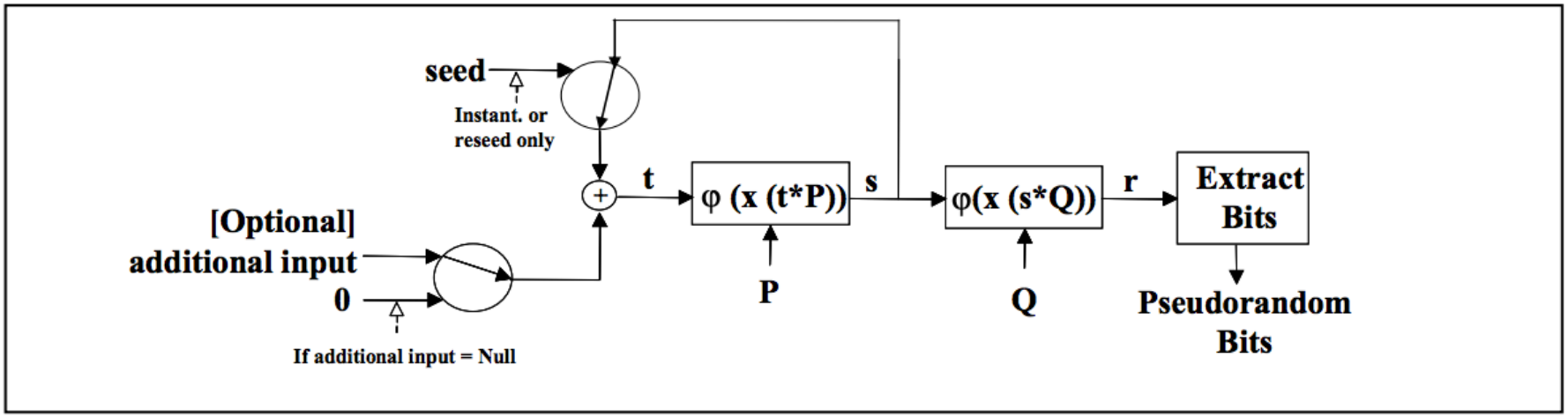
- *Security strength* is specified in bits and is a specific value from the set $\{112, 128, 192, 256\}$. If the *security strength* associated with an algorithm or system is S bits, then it is expected that (roughly) 2^S basic operations are required to break it.
- Let S be the security strength.
- Dual_EC_DRBG uses an initial seed that is $2S$ bits to initiate the generation of outlen-bit pseudorandom strings.
- The curve is defined over a field approximately 2^m in size, where m is at least $2S$ and never less than 256.

What is Dual_EC_DRBG?

- Let P, Q denote the specific points on a particular curve.
- Let $x(A)$ be the x-coordinate of the point A on the curve, given in affine coordinates.
- Let $\varphi(x)$ map field elements to non-negative integers, taking the bit vector representation of a field element and interpreting it as the binary expansion of an integer.

  B: $c_{m-1}|c_{m-2}|...|c_1|c_0$, a bitstring, with c_{m-1} being leftmost
  Z: $c_{m-1} \cdot 2^{m-1} + ... + c_2 \cdot 2^2 + c_1 \cdot 2^1 + c_0 \in \mathbb{Z}$
  F: $c_{m-1} \cdot 2^{m-1} + ... + c_2 \cdot 2^2 + c_1 \cdot 2^1 + c_0 \bmod p \in \mathbb{F}_p$

What is Dual_EC_DRBG?



What is Dual_EC_DRBG?

Two rounds of generation of bitstrings:

- $i_0 = \text{seed} \oplus \text{additional input}$
- $i_1 = \phi(x(i_0 P))$
- $o_0 = \phi(x(i_1 Q))$
- output 30 least significant bytes of o_0
- $i_2 = \phi(x(i_1 P))$
- $o_1 = \phi(x(i_2 Q))$
- output 30 least significant bytes of o_1

Backdoor attack

- Suppose we know $i_1 Q$.
- Suppose we know the backdoor, i.e. we know d such that $dQ = P$.
- Multiplying $i_1 Q$ by d gives $i_1 dQ = i_1 P$.

Backdoor attack

- We lost just the 2 most significant bytes in the output process.
- So we can do for all possible values of $o_0 = \phi(x(i_1 Q))$
  1. find the points with its x-coordinate being a candidate for a value of $x(i_1 Q)$
     (it is at most 2 points because of a degree
     of the polynomial $y^2 - x^3 + 3x - b$)
  2. multiply the points with d to get candidates for $i_1 P$ which imply candidates for $i_2 = \phi(x(i_1 P))$
  3. get candidates for o_1 from candidates for i_2 and compare with actual o_1

Backdoor attack

- Thank you for your attention!