### Using Cryptol to explore NIST's Dual\_EC\_DRNG

Cohesive Project - FMSE 13/14

#### Ana Carvalho

pg25335@alunos.uminho.pt

SA ni+2 -

#### Catarina Correia

pg19643@alunos.uminho.pt

Z ... 1(0)

### J.N. Oliveira J. Hendrix

3 July 2014

galois

### Project Proposal

#### Main goals:

Use Cryptol to explore random number generators with a backdoor based on elliptic curves.

### Project Proposal

#### Main goals:

- Use Cryptol to explore random number generators with a backdoor based on elliptic curves.
- Show how the internal state can be recovered after observing a few bits of output.

2 / 32

# We will get to the **interesting** stuff in just a minute.

### But first...

theguardian

## NSA FILES: DECODED

#### What the revelations mean for you.



Ana Carvalho and Catarina Correia (UM)

NIST works to publish the strongest cryptographic standards possible, and uses a transparent, public process to rigorously vet its standards and guidelines. If vulnerabilities are found, NIST works with the cryptographic community to address them as quickly as possible.

In light of the concerns expressed regarding Dual\_EC\_DRBG, ITL is taking the following actions:

Recommending against the use of SP 800-90A Dual Elliptic Curve Deterministic Random Bit Generation: 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.



Ana Carvalho and Catarina Correia (UM)

NIST works to publish the strongest cryptographic standards possible, and uses a transparent, public process to rigorously vet its standards and guidelines. If vulnerabilities are found, NIST works with the cryptographic community to address them as quickly as possible.

In light of the concerns expressed regarding Dual\_EC\_DRBG, ITL is taking the following actions:

Recommending against the use of SP 800-90A Dual Elliptic Curve Deterministic Random Bit Generation: 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.

NIST	NIST Time   NIS	T Home About NIST	Contact Us A-Z Site	Index Search	
Information Technology	Laboratory	11100960	C'Out	DOD01100110100110100010	10
About ITL 🔻 Publications Topi	ic/Subject Areas 🔻 🛛 Produ	ucts/Services 🔻 News/M	fultimedia Programs/P	Projects	

NIST Home > ITL > Computer Security Division > NIST Removes Cryptography Algorithm from Random Number Generator Recommendations

#### NIST Removes Cryptography Algorithm from Random Number Generator Recommendations From NIST Tech Beat: April 21, 2014

#### Contact: Jennifer Huergo 301-975-6343

Following a public comment period and review, the National Institute of Standards and Technology (NIST) has removed a cryptographic algorithm from its draft guidance on random number generators. Before implementing the change, NIST is requesting final public comments on the revised document, Recommendation for Random Number Generation Using Deterministic Random Bit Generators (NIST Special Publication 800-90A, Rev. 1).

The revised document retains three of the four previously available options for generating pseudorandom bits needed to create secure cryptographic keys for encrypting data. It omits an algorithm known as Dual\_EC\_DRBG, or Dual Elliptic Curve Deterministic Random Bit Generator. NIST recommends that current users of Dual\_EC\_DRBG transition to one of the three remaining approved algorithms as quickly as possible.

Ana Carvalho and Catarina Correia (UM) Elliptic Curve Cry

### Back to the technicalities

### **Evolution Diagram**



Ana Carvalho and Catarina Correia (UM)

An **elliptic curve** is given by the following equation:

$$\mathbf{y}^2 = \mathbf{x}^3 + \mathbf{a}\mathbf{x} + \mathbf{b} \tag{1}$$

where a, b satisfies  $-16(4a^3 + 27b^2) \neq 0$ .



Properties of the addition law on an elliptic curve *E*:

• 
$$P \oplus \mathcal{O} = \mathcal{O} \oplus P = P, \forall P \in E$$
 [Identity]

▶ 
$$P \oplus (-P) = O, \forall P \in E$$
 [Inverse]

▶  $(P \oplus Q) \oplus R = P \oplus (Q \oplus R), \forall P, Q, R \in E$  [Associative]

Properties of the addition law on an elliptic curve *E*:

• 
$$P \oplus \mathcal{O} = \mathcal{O} \oplus P = P, \forall P \in E$$
 [Identity]

▶ 
$$P \oplus (-P) = O, \forall P \in E$$
 [Inverse]

▶  $(P \oplus Q) \oplus R = P \oplus (Q \oplus R), \forall P, Q, R \in E$  [Associative]

#### It's a Group

Properties of the addition law on an elliptic curve *E*:

• 
$$P \oplus \mathcal{O} = \mathcal{O} \oplus P = P, \forall P \in E$$
 [Identity]

▶ 
$$P \oplus (-P) = O, \forall P \in E$$
 [Inverse]

▶  $(P \oplus Q) \oplus R = P \oplus (Q \oplus R), \forall P, Q, R \in E$  [Associative]

#### It's a Group

▶  $P \oplus Q = Q \oplus P, \forall P, Q \in E$  [Commutative]

8 / 32

Properties of the addition law on an elliptic curve E:

• 
$$P \oplus \mathcal{O} = \mathcal{O} \oplus P = P, \forall P \in E$$
 [Identity]

▶ 
$$P \oplus (-P) = O, \forall P \in E$$
 [Inverse]

▶  $(P \oplus Q) \oplus R = P \oplus (Q \oplus R), \forall P, Q, R \in E$  [Associative]

#### It's a Group

▶ 
$$P \oplus Q = Q \oplus P, \forall P, Q \in E$$
 [Commutative]

#### It's an abelian Group

**Note**: in this group, multiplication,  $n * P, \forall P \in E$ , can be seen as adding P n times to itself.

### Elliptic Curves in cryptography

In order to apply the theory of elliptic curves to cryptography the elliptic curve is defined over a finite field  $\mathbb{F}_p$ .

$$E: y^2 = x^3 - 3x + b$$
 (2)

with  $b \in \mathbb{F}_p$  satisfying  $432 + 27b^2 \neq 0$ .

$$E(\mathbb{F}_p) = \{(x, y) : x, y \in \mathbb{F}_p \land y^2 = x^3 - 3x + b\} \cup \mathcal{O}$$

### Elliptic Curves in cryptography

The plot of the elliptic curve over a finite field  $\mathbb{F}_p$  turns out to be:



#### Observations

- The elliptic curve addition law is closed over  $\mathbb{F}_p$ .
- ► The addition law **satisfies** all properties listed before.

### **Evolution Diagram**



### Cryptol Implementation

Projective System - Jacobian Coordinates  $Y^2 = X^3 - 3XZ^4 + bZ^6$ 

- ec\_affinify(  $(X_1, Y_1, Z_1)$ ) =  $(\frac{X_1}{Z_1^2}, \frac{Y_1}{Z_1^3})$  with  $Z_1 \neq 0$
- The point at infinity  $\mathcal{O} = (X, Y, 0)$
- The inverse of  $(X_1, Y_1, Z_1)$  is  $(X_1, -Y_1, Z_1)$ .

## Projective system increases efficiency in computation!

### Cryptol Implementation

#### Elliptic Curve and Finite Field operations

- Scalar multiplication in  $E(\mathbb{F}_p)$  using Montgomery Ladder;
- Exponentiation in F<sub>p</sub>;
- Square-root in  $\mathbb{F}_p$  (for NIST's  $p_{256}$ );

### Cryptol Implementation

#### Elliptic Curve and Finite Field operations

- Scalar multiplication in  $E(\mathbb{F}_p)$  using Montgomery Ladder;
- Exponentiation in F<sub>p</sub>;
- Square-root in  $\mathbb{F}_p$  (for NIST's  $p_{256}$ );

#### Simple Dual\_EC\_DRNG and computation of the backdoor!

### **Evolution Diagram**



Ana Carvalho and Catarina Correia (UM)

#### $Dual_EC_DRNG$



Ana Carvalho and Catarina Correia (UM)

### $Dual_EC_DRNG$

#### Implementation

- NIST curve p 256
- small curve p-5

#### Curve data

• 
$$y^2 = x^3 - 3x + 7$$
 over  $\mathbb{F}_{23}^*$ 

• Input points: P = (22,3) Q = (14,15)

**seed:** 7 (hidden)

P = 5\*Q! (secret)



Ana Carvalho and Catarina Correia (UM)

Elliptic Curve Cryptography - DRNG

milestone 4 - 3/Jul/2014 17 / 32



Ana Carvalho and Catarina Correia (UM)

Elliptic Curve Cryptography - DRNG

JG milestone 4 - 3/Jul/2014 18 / 32



Ana Carvalho and Catarina Correia (UM)

Elliptic Curve Cryptography - DRNG

milestone 4 - 3/Jul/2014 19 / 32



Ana Carvalho and Catarina Correia (UM)

Elliptic Curve Cryptography - DRNG

milestone 4 - 3/Jul/2014 20 / 32



Ana Carvalho and Catarina Correia (UM)

Elliptic Curve Cryptography - DRNG

milestone 4 - 3/Jul/2014 21 / 32

- ▶ There are 2<sup>*n*</sup> alternatives for the random number.
- Some of the alternatives can be excluded.
- ▶ In the example, it only took 2 blocks to be 100% sure

#### We can make an educated guess if we know how P and Q are related!

### **Evolution Diagram**



Ana Carvalho and Catarina Correia (UM)

Correctness properties can be explicitly checked by the Cryptol toolset.

Correctness properties can be explicitly checked by the Cryptol toolset.

:prove property

Proves properties automatically.

24 / 32

Correctness properties can be explicitly checked by the Cryptol toolset.

:prove property

Proves properties automatically.

:check property

 Tests the property at random values to give a quick feedback. The check command will alert for bugs.

Correctness properties can be explicitly checked by the Cryptol toolset.

:prove property

Proves properties automatically.

:check property

Tests the property at random values to give a quick feedback. The check command will alert for bugs.

:sat property

Find arguments to a bit-valued function such that the property will be satisfied.

Ana Carvalho and Catarina Correia (UM)

### Proving the standards

#### Identity

 $\blacktriangleright P \oplus \mathcal{O} = \mathcal{O} \oplus P = P, \forall P \in E$ 

```
Main> :check point_add_ident curve23
Using exhaustive testing.
passed 1024 tests.
QED
Main> :check point_add_ident_II curve23
Using exhaustive testing.
passed 1024 tests.
QED
```

Checks for the identity properties. Each one of them took less than a minute.

### Proving the standards

#### Commutativity

 $\blacktriangleright P \oplus Q = Q \oplus P, \forall P, Q \in E$ 

```
Main> :check point_add_is_comm curve23
Using exhaustive testing.
passed 1048576 tests.
QED
```

Checks for the commutativity property. The full execution took less than five minutes.

26 / 32

### Proving the standards

#### Associativity

 $\blacktriangleright (P \oplus Q) \oplus R = P \oplus (Q \oplus R), \forall P, Q, R \in E$ 

```
Main> :check point_add_is_comm curve23
Using random testing.
passed 10800000 tests.
Coverage: 1.01% (4000000 of 2^30 values)
```

Ana Carvalho and Catarina Correia (UM) Ellip

Elliptic Curve Cryptography - DRNG

milestone 4 - 3/Jul/2014

27 / 32

#### Pros

 Cryptol is polymorphic over word sizes, great for cryptographic applications;

#### Pros

- Cryptol is polymorphic over word sizes, great for cryptographic applications;
- Cryptol reuses the specifications to check and prove properties.

#### Pros

- Cryptol is polymorphic over word sizes, great for cryptographic applications;
- Cryptol reuses the specifications to check and prove properties.

BUT ...

#### Pros

- Cryptol is polymorphic over word sizes, great for cryptographic applications;
- Cryptol reuses the specifications to check and prove properties.

#### BUT ...

#### Cons

Inability to use the :prove command;

#### Pros

- Cryptol is polymorphic over word sizes, great for cryptographic applications;
- Cryptol reuses the specifications to check and prove properties.

#### BUT ...

#### Cons

- Inability to use the :prove command;
- Could not load a reasonable size files;

#### Pros

- Cryptol is polymorphic over word sizes, great for cryptographic applications;
- Cryptol reuses the specifications to check and prove properties.

#### BUT ...

#### Cons

- Inability to use the :prove command;
- Could not load a reasonable size files;
- Dual\_EC is not polymorphic because of type variables.

#### Achievements

Implementation of Dual\_EC\_DRNG for multiple curves;

#### Achievements

- Implementation of Dual\_EC\_DRNG for multiple curves;
- Testing of elliptic curve operations with NIST examples;

Ana Carvalho and Catarina Correia (UM) Elliptic Curve Cryptography - DRNG milestone 4 - 3/Jul/2014

#### Achievements

- Implementation of Dual\_EC\_DRNG for multiple curves;
- Testing of elliptic curve operations with NIST examples;
- Check (and proving) of group laws;

#### Achievements

- Implementation of Dual\_EC\_DRNG for multiple curves;
- Testing of elliptic curve operations with NIST examples;
- Check (and proving) of group laws;
- Report of running bugs in Cryptol.

#### Future Work

Extend the proofs to bigger curves;

### Future Work

- Extend the proofs to bigger curves;
- Develop an elliptic curve DiffieHellman key-agreement (ECDH);

### Future Work

- Extend the proofs to bigger curves;
- Develop an elliptic curve DiffieHellman key-agreement (ECDH);
- Compare Crytpol proof system with other theorem provers.

Ana Carvalho and Catarina Correia (UM) Ellipt

Elliptic Curve Cryptography - DRNG

milestone 4 - 3/Jul/2014 31 / 32

#### Mr. Joe Hendrix (supervisor)

Ana Carvalho and Catarina Correia (UM) Ell

Elliptic Curve Cryptography - DRNG

milestone 4 - 3/Jul/2014 31 / 32

Mr. Joe Hendrix (supervisor)
 Prof. José Nuno Oliveira (tutor)

- Mr. Joe Hendrix (supervisor)
- Prof. José Nuno Oliveira (tutor)
- Formal Methods community!

- Mr. Joe Hendrix (supervisor)
- Prof. José Nuno Oliveira (tutor)
- Formal Methods community!

### Thank you!

### **Questions?**