

# Smart card implementation of a digital signature scheme for Twisted Edwards curves

By Niels Duif



**TU/e** Technische Universiteit  
Eindhoven  
University of Technology

Where innovation starts

# Remark

- Ask questions



# Structure

- **Signature schemes**
- **Smart cards**
- **Elliptic curves**
- **My signature scheme**
- **Side channel attacks**
- **Improvements**
- **New findings**



# Smart card

- **Tamper resistant**
- **Cheap**
- **Limited capacity**
  - **64 kB EEPROM**
  - **1536 bytes RAM**



# Smart card

- Tamper resistant
- Cheap
- Limited capacity
  - 64 kB EEPROM
  - 1536 bytes RAM



# Smart card

- Tamper resistant
- Cheap
- Limited capacity
  - 64 kB EEPROM
  - 1536 bytes RAM



# Signature schemes



# Signature schemes

- **Authentication**



# Analog signatures

- **Authentication**



- **Authen**

Eindhoven, 09-05-2011

Dear all,

Today there will be free drinks for everyone at 17.30 hours at Schootsestraat 65, Eindhoven.

Kind regards,

Niels Duif

- **Authen**

Eindhoven, 09-05-2011

Dear all,

Today there will be free drinks for everyone at 17.30 hours at Schootsestraat 65, Eindhoven.

Kind regards,

A handwritten signature in blue ink, appearing to read 'Niels Duif', enclosed within a light blue oval shape.

Niels Duif

- **Authen**

Eindhoven, 09-05-2011

Dear all,

Today there will be free drinks for everyone at 17.30 hours at Schootsestraat 65, Eindhoven. Also, I'm donating €10.000 to Compumatica.

Kind regards,

A handwritten signature in blue ink, appearing to read 'Niels Duif', enclosed within a hand-drawn blue oval.

Niels Duif

# Analog signatures

- **Authentication**
- **Integrity**



# Digital signatures



# Digital signatures

- **Input: message ( $m$ )**
- **Output: signature ( $S$ )**

# Digital signatures

- **Input: message ( $m$ )**
- **Output: signature ( $S$ )**
- **Authentication**
  - Only Niels Duif can sign the message
- **Integrity**
  - Changing the message is detected



# Digital signatures

Niels Duif



# Digital signatures

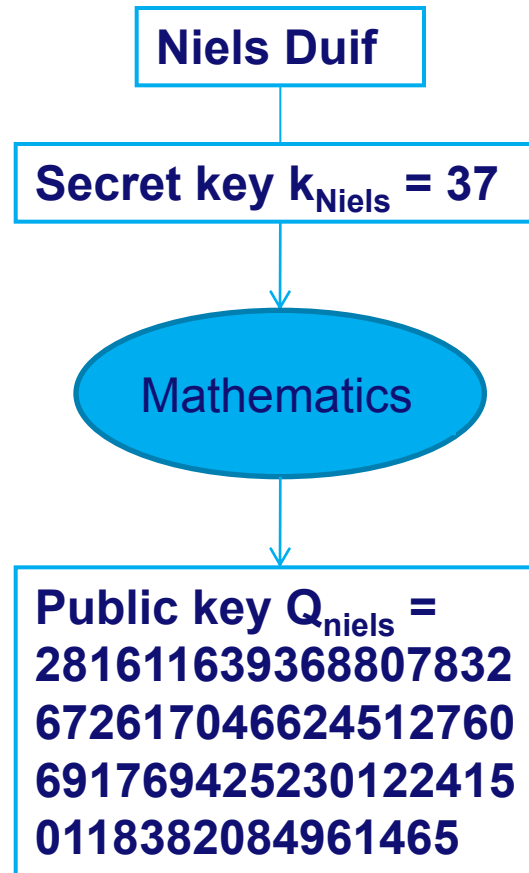


# Digital signatures

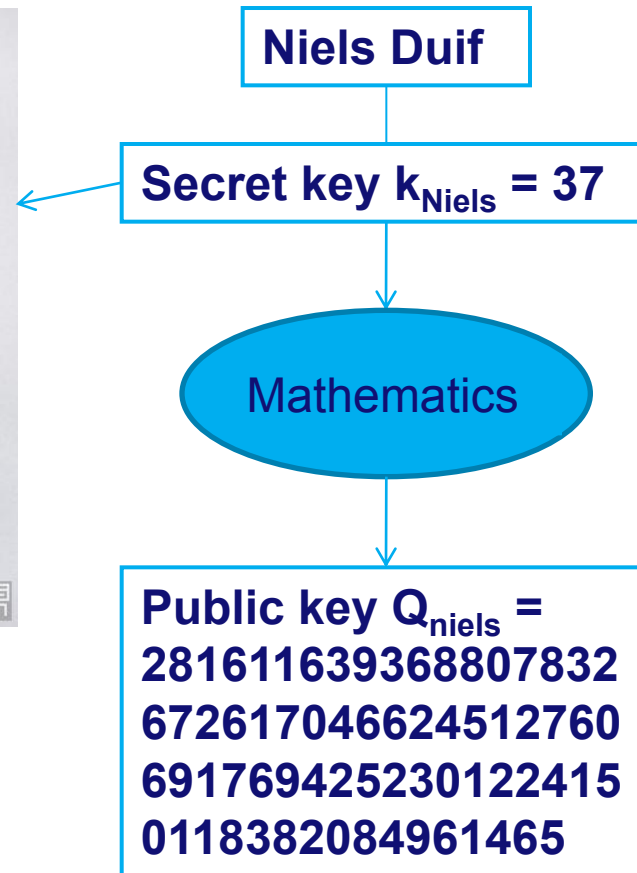
Niels Duif

Secret key  $k_{\text{Niels}} = 37$

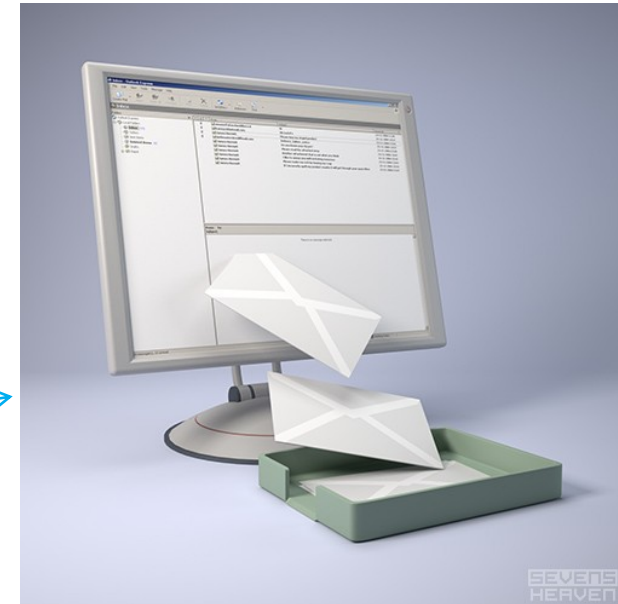
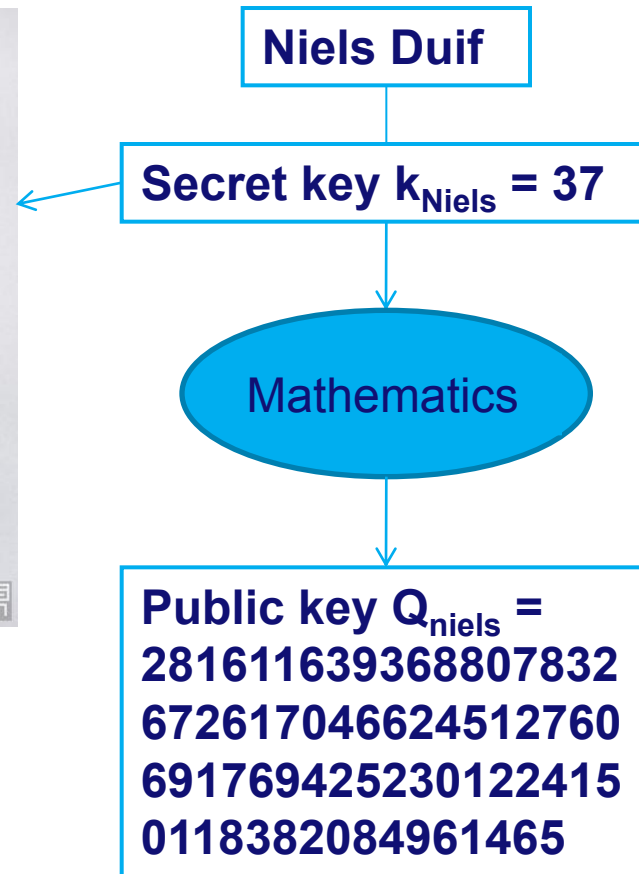
# Digital signatures



# Digital signatures



# Digital signatures



# Sign

**Niels Duif**

**Eindhoven, 09-05-2011  
Dear all, Today there will  
be free drinks for  
everyone at 17.30 hours  
at Schootsestraat 65,  
Eindhoven. Kind regards,  
Niels Duif**



# Sign



Niels Duif

Secret key  $k_{\text{Niels}} = 37$

Eindhoven, 09-05-2011  
Dear all, Today there will be free drinks for everyone at 17.30 hours at Schootsestraat 65, Eindhoven. Kind regards,  
Niels Duif

# Sign



Niels Duif

Secret key  $k_{\text{Niels}} = 37$

Eindhoven, 09-05-2011  
Dear all, Today there will be free drinks for everyone at 17.30 hours at Schootsestraat 65, Eindhoven. Kind regards, Niels Duif

# Sign



Niels Duif

Secret key  $k_{\text{Niels}} = 37$

Eindhoven, 09-05-2011  
Dear all, Today there will  
be free drinks for  
everyone at 17.30 hours  
at Schootsestraat 65,  
Eindhoven. Kind regards,  
Niels Duif

**Signature:** E1 B8 AD 2F 12  
BF 3D F8 C3 B9 32 88 6F A1  
76 78 3A 9E 0D 68 2F 8B BF  
1A 49 F6 15 AE 14 EC 9F 5A  
16 71 06 13 12 21 F1 05 06  
5F 23 4E F9 61 15 EA 00 07  
89 81 86 76 0F 0B CD 7F 31  
CE 79 87 AC D4

# Verify

Someone

**Eindhoven, 09-05-2011**  
**Dear all, Today there will**  
**be free drinks for**  
**everyone at 17.30 hours**  
**at Schootsestraat 65,**  
**Eindhoven. Kind regards,**  
**Niels Duif**

**Signature:** E1 B8 AD 2F 12  
BF 3D F8 C3 B9 32 88 6F A1  
76 78 3A 9E 0D 68 2F 8B BF  
1A 49 F6 15 AE 14 EC 9F 5A  
16 71 06 13 12 21 F1 05 06  
5F 23 4E F9 61 15 EA 00 07  
89 81 86 76 0F 0B CD 7F 31  
CE 79 87 AC D4



# Verify



Someone

Public key  $Q_{\text{niels}} =$   
281611639368807832  
672617046624512760  
691769425230122415  
0118382084961465

Eindhoven, 09-05-2011  
Dear all, Today there will  
be free drinks for  
everyone at 17.30 hours  
at Schootsestraat 65,  
Eindhoven. Kind regards,  
Niels Duif

Signature: E1 B8 AD 2F 12  
BF 3D F8 C3 B9 32 88 6F A1  
76 78 3A 9E 0D 68 2F 8B BF  
1A 49 F6 15 AE 14 EC 9F 5A  
16 71 06 13 12 21 F1 05 06  
5F 23 4E F9 61 15 EA 00 07  
89 81 86 76 0F 0B CD 7F 31  
CE 79 87 AC D4

# Verify



Someone

Public key  $Q_{\text{niels}} =$   
281611639368807832  
672617046624512760  
691769425230122415  
0118382084961465

Eindhoven, 09-05-2011  
Dear all, Today there will  
be free drinks for  
everyone at 17.30 hours  
at Schootsestraat 65,  
Eindhoven. Kind regards,  
Niels Duif

Signature: E1 B8 AD 2F 12  
BF 3D F8 C3 B9 32 88 6F A1  
76 78 3A 9E 0D 68 2F 8B BF  
1A 49 F6 15 AE 14 EC 9F 5A  
16 71 06 13 12 21 F1 05 06  
5F 23 4E F9 61 15 EA 00 07  
89 81 86 76 0F 0B CD 7F 31  
CE 79 87 AC D4

# Verify



Someone

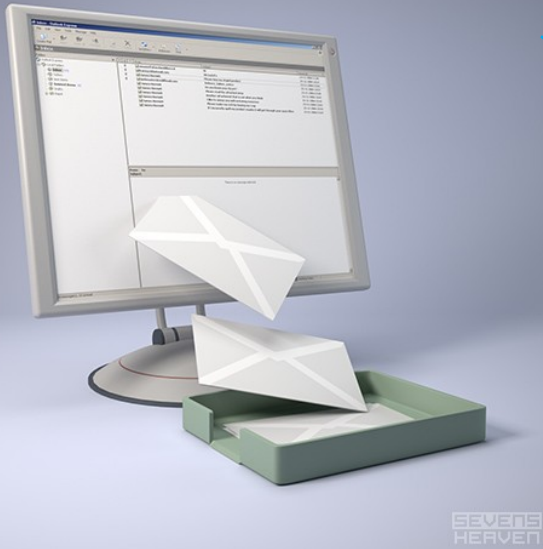
Public key  $Q_{\text{niels}} =$   
281611639368807832  
672617046624512760  
691769425230122415  
0118382084961465

Eindhoven, 09-05-2011  
Dear all, Today there will  
be free drinks for  
everyone at 17.30 hours  
at Schootsestraat 65,  
Eindhoven. Kind regards,  
Niels Duif

Signature: E1 B8 AD 2F 12  
BF 3D F8 C3 B9 32 88 6F A1  
76 78 3A 9E 0D 68 2F 8B BF  
1A 49 F6 15 AE 14 EC 9F 5A  
16 71 06 13 12 21 F1 05 06  
5F 23 4E F9 61 15 EA 00 07  
89 81 86 76 0F 0B CD 7F 31  
CE 79 87 AC D4

Correct

# Verify



Someone

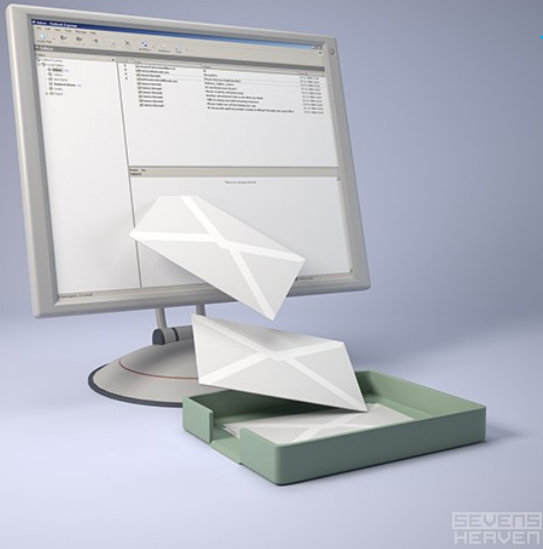
Public key  $Q_{\text{niels}} =$   
281611639368807832  
672617046624512760  
691769425230122415  
0118382084961465

Eindhoven, 09-05-2011  
Dear all, Today there will  
be free drinks for  
everyone at 17.30 hours  
at Schootsestraat 65,  
Eindhoven. Also, I'm  
donating €10.000 to  
Compumatica. Kind  
regards, Niels Duif

Signature: E1 B8 AD 2F 12  
BF 3D F8 C3 B9 32 88 6F A1  
76 78 3A 9E 0D 68 2F 8B BF  
1A 49 F6 15 AE 14 EC 9F 5A  
16 71 06 13 12 21 F1 05 06  
5F 23 4E F9 61 15 EA 00 07  
89 81 86 76 0F 0B CD 7F 31  
CE 79 87 AC D4



# Verify



Someone

Public key  $Q_{\text{niels}} =$   
281611639368807832  
672617046624512760  
691769425230122415  
0118382084961465

Eindhoven, 09-05-2011  
Dear all, Today there will  
be free drinks for  
everyone at 17.30 hours  
at Schootsestraat 65,  
Eindhoven. Also, I'm  
donating €10.000 to  
Compumatica. Kind  
regards, Niels Duif

Signature: E1 B8 AD 2F 12  
BF 3D F8 C3 B9 32 88 6F A1  
76 78 3A 9E 0D 68 2F 8B BF  
1A 49 F6 15 AE 14 EC 9F 5A  
16 71 06 13 12 21 F1 05 06  
5F 23 4E F9 61 15 EA 00 07  
89 81 86 76 0F 0B CD 7F 31  
CE 79 87 AC D4

# Verify



Someone

Public key  $Q_{\text{niels}} =$   
281611639368807832  
672617046624512760  
691769425230122415  
0118382084961465

Eindhoven, 09-05-2011  
Dear all, Today there will  
be free drinks for  
everyone at 17.30 hours  
at Schootsestraat 65,  
Eindhoven. Also, I'm  
donating €10.000 to  
Compumatica. Kind  
regards, Niels Duif

Signature: E1 B8 AD 2F 12  
BF 3D F8 C3 B9 32 88 6F A1  
76 78 3A 9E 0D 68 2F 8B BF  
1A 49 F6 15 AE 14 EC 9F 5A  
16 71 06 13 12 21 F1 05 06  
5F 23 4E F9 61 15 EA 00 07  
89 81 86 76 0F 0B CD 7F 31  
CE 79 87 AC D4

Wrong

# Applications

- **Signing bank transactions (iDeal)**
- **Signing your tax declaration (DigID)**
- **Secure e-mail**
- **And many more**



# Elliptic curves



# Elliptic curves

- Elliptic curve over a prime field  $F_p$

# Elliptic curves

- Elliptic curve over a prime field  $F_p$
- $p = 2^{255} - 31$  is prime

# Elliptic curves

- Elliptic curve over a prime field  $F_p$
- $p = 2^{255} - 31$  is prime

$$y^2 \equiv x^3 + a_2x^2 + a_4x + a_6 \pmod{p}$$

# Elliptic curves

- **Elliptic curve over a prime field  $F_p$**
- **$p = 2^{255} - 31$  is prime**

$$y^2 \equiv x^3 + a_2x^2 + a_4x + a_6 \pmod{p}$$

- **Twisted Edwards curve**

# Elliptic curves

- **Elliptic curve over a prime field  $F_p$**
- **$p = 2^{255} - 31$  is prime**

$$y^2 \equiv x^3 + a_2x^2 + a_4x + a_6 \pmod{p}$$

- **Twisted Edwards curve**

$$ax^2 + y^2 \equiv 1 + dx^2y^2 \pmod{p}$$

# Elliptic curves

- **Elliptic curve over a prime field  $F_p$**
- **$p = 2^{255} - 31$  is prime**

$$y^2 \equiv x^3 + a_2x^2 + a_4x + a_6 \pmod{p}$$

- **Twisted Edwards curve**

$$ax^2 + y^2 \equiv 1 + dx^2y^2 \pmod{p}$$

- **$a = -1$**

# Elliptic curves

- **Elliptic curve over a prime field  $F_p$**
- **$p = 2^{255} - 31$  is prime**

$$y^2 \equiv x^3 + a_2x^2 + a_4x + a_6 \pmod{p}$$

- **Twisted Edwards curve**

$$ax^2 + y^2 \equiv 1 + dx^2y^2 \pmod{p}$$

- **$a = -1$**
- **Fast arithmetic**

# My signature scheme



# My signature scheme

- **Similar to Schnorr signatures**



# My signature scheme

- **Similar to Schnorr signatures**
- **Inversion-free**

# My signature scheme

- **Similar to Schnorr signatures**
- **Inversion-free**
- **No point compression**
  - $(X:Y:Z)$
  - $(X:Y:Z:T)$

# Side channel attacks



# Side channel attacks

- **Get secret information by:**



# Side channel attacks

- **Get secret information by:**
  - **Measuring power consumption, radiation, etc**

# Side channel attacks

- **Get secret information by:**
  - **Measuring power consumption, radiation, etc**
  - **Disturbing the computation**

# Improvements



# Improvements

- $p = 2^{255} - 31$ 
  - -59%
- Signed byte representation
  - -11%
- Twisted Edwards curves
  - -2%
- Extended coordinates
  - -1%
- Fast squaring
  - -5%



# Improvements

- **Schnorr variant instead of ECDSA variant**
  - **-2%**
- **Side channel attack resistance**
  - **+46%**
- **Java Card**

# Improvements

- **Schnorr variant instead of ECDSA variant**
  - **-2%**
- **Side channel attack resistance**
  - **+46%**
- **Java Card**
  - **+700000%**
  - **That means: 7000 times slower**



# New findings



# New findings

- Precomputed points are not presented as  $(X:Y:Z:T)$  but as  $(Y-X : Y+X : 2Z : kT)$ , where  $k = 2d$

# New findings

- **Precomputed points are not presented as  $(X:Y:Z:T)$  but as  $(Y-X : Y+X : 2Z : kT)$ , where  $k = 2d$** 
  - **Saves 2 additions, a multiplication by 2 and a multiplication by  $k$**

# New findings

- **Precomputed points are not presented as  $(X:Y:Z:T)$  but as  $(Y-X : Y+X : 2Z : kT)$ , where  $k = 2d$** 
  - **Saves 2 additions, a multiplication by 2 and a multiplication by  $k$**
  - **Helps to prevent side channel attacks**

# New findings

- Precomputed points are not presented as  $(X:Y:Z:T)$  but as  $(Y-X : Y+X : 2Z : kT)$ , where  $k = 2d$ 
  - Saves 2 additions, a multiplication by 2 and a multiplication by  $k$
  - Helps to prevent side channel attacks
- The scalar  $r$  is represented as
$$r = r_0 + r_1 * 2^4 + \dots + r_{63} * 2^{252},$$
where  $r_0, r_1, \dots, r_{63}$  are taken at random in  $\{1,2,\dots,16\}$   
This avoids the neutral element  $(0:1:1:0)$

# Acknowledgements

- **Thanks Tanja!**



# Acknowledgements

- **Thanks Tanja!**
- **Thanks Cees!**



# Acknowledgements

- **Thanks Tanja!**
- **Thanks Cees!**
- **Thanks Henk and Aart!**



# Acknowledgements

- **Thanks Tanja!**
- **Thanks Cees!**
- **Thanks Henk and Aart!**
- **Thanks Eline!**



# Acknowledgements

- **Thanks Tanja!**
- **Thanks Cees!**
- **Thanks Henk and Aart!**
- **Thanks Eline!**
- **Thanks to all my friends and family!**



# End of presentation

## Twisted Edwards curves

$$ax^2 + y^2 \equiv 1 + dx^2y^2 \pmod{p}$$

## Java Card



## Precomputing

$$(Y-X : Y+X : 2Z : kT)$$

## Signatures

Eindhoven, 09-05-2011

Dear all,

Today there will be free drinks for everyone at 17.30 hours at Schootsestraat 65, Eindhoven.

Kind regards,

A handwritten signature in blue ink, appearing to read 'Niels Duif', is written over a light blue circular background.

Niels Duif

## Smart cards

