This is the full version of the extended
Proceedings of the Cryptographers Tra
(29 February – 4 March 2016, San Fra
Kazue Sako Ed. Springer-Verlag, LNCS

Sh

I

[1] Écol
[2] (

Abstract. Digital signat
the development of pairin
proposed. Among them,
flexible and has been used
suffers from a linear size
situations.
In this paper, we propos
without the linear-size dra
length, and our algorithn
pairings, that are already
We prove the security of o
we show that protocols u
more efficient constructio

1 Introduction

Digital signature is one of th
to provide the electronic v
more complex primitives. W
usually requires a signature
block, signatures must not j
the other building blocks c
require a signature scheme
with zero-knowledge proofs.

1.1 Related Works

Constructing a versatile sig
of the first construction sp
proposed by Camenisch an
RSA assumption [BP97], all
of a signature.

The emergence of pairin
nature schemes compatible
use bilinear groups, *i.e.* a
$e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$. In 200
nature scheme [CL04] whos
group signatures [BCN+10]

This is the full version of the extended
Proceedings of the Cryptographers Tra
(29 February – 4 March 2016, San Fra
Kazue Sako Ed. Springer-Verlag, LNC

Sh

I

[1] Éco
[2] (

Abstract. Digital signat
the development of pairin
proposed. Among them,
flexible and has been used
suffers from a linear size
situations.
In this paper, we propos
without the linear-size dra
length, and our algorithn
pairings, that are already
We prove the security of o
we show that protocols u
more efficient constructio

1 Introduction

Digital signature is one of t
to provide the electronic v
more complex primitives. W
usually requires a signature
block, signatures must not
the other building blocks c
require a signature scheme
with zero-knowledge proofs.

1.1 Related Works

Constructing a versatile si
of the first construction sp
proposed by Camenisch an
RSA assumption [BP97], all
of a signature.

The emergence of pairin
nature schemes compatible
use bilinear groups, *i.e.* a
$e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$. In 200
nature scheme [CL04] whos
group signatures [BCN+10]

This is the full version of the extended
Proceedings of the Cryptographers Tra
(29 February – 4 March 2016, San Fra
Kazue Sako Ed. Springer-Verlag, LNC

Sh

I

[1] Éco
[2] (

Abstract. Digital signat
the development of pairin
proposed. Among them,
flexible and has been used
suffers from a linear size
situations.
In this paper, we propos
without the linear-size dra
length, and our algorithn
pairings, that are already
We prove the security of o
we show that protocols u
more efficient constructio

1 Introduction

Digital signature is one of t
to provide the electronic v
more complex primitives. W
usually requires a signature
block, signatures must not
the other building blocks c
require a signature scheme
with zero-knowledge proofs.

1.1 Related Works

Constructing a versatile si
of the first construction sp
proposed by Camenisch an
RSA assumption [BP97], all
of a signature.

The emergence of pairin
nature schemes compatible
use bilinear groups, *i.e.* a
$e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$. In 200
nature scheme [CL04] whos
group signatures [BCN+10]

This is the full version of the extended
Proceedings of the Cryptographers Tra
(29 February – 4 March 2016, San Fra
Kazue Sako Ed. Springer-Verlag, LNC

Sh

I

[1] Éco
[2] (

Abstract. Digital signat
the development of pairin
proposed. Among them,
flexible and has been used
suffers from a linear size
situations.
In this paper, we propos
without the linear-size dra
length, and our algorithn
pairings, that are already
We prove the security of o
we show that protocols u
more efficient constructio

1 Introduction

Digital signature is one of t
to provide the electronic v
more complex primitives. W
usually requires a signature
block, signatures must not
the other building blocks c
require a signature scheme
with zero-knowledge proofs.

1.1 Related Works

Constructing a versatile si
of the first construction sp
proposed by Camenisch an
RSA assumption [BP97], all
of a signature.

The emergence of pairin
nature schemes compatible
use bilinear groups, *i.e.* a
$e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$. In 200
nature scheme [CL04] whos
group signatures [BCN+10]

This is the full version of the extended
Proceedings of the Cryptographers Tra
(29 February – 4 March 2016, San Fra
Kazue Sako Ed. Springer-Verlag, LNC

Sh

I

[1] Éco
[2] (

Abstract. Digital signat
the development of pairin
proposed. Among them,
flexible and has been used
suffers from a linear size
situations.
In this paper, we propos
without the linear-size dra
length, and our algorithn
pairings, that are already
We prove the security of o
we show that protocols u
more efficient constructio

1 Introduction

Digital signature is one of t
to provide the electronic v
more complex primitives. W
usually requires a signature
block, signatures must not
the other building blocks c
require a signature scheme
with zero-knowledge proofs.

1.1 Related Works

Constructing a versatile si
of the first construction sp
proposed by Camenisch an
RSA assumption [BP97], all
of a signature.

The emergence of pairin
nature schemes compatible
use bilinear groups, *i.e.* a
$e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$. In 200
nature scheme [CL04] whos
group signatures [BCN+10]

This is the full version of the extended
Proceedings of the Cryptographers Tra
(29 February – 4 March 2016, San Fra
Kazue Sako Ed. Springer-Verlag, LNC

Sh

I

[1] Éco
[2] (

Abstract. Digital signat
the development of pairin
proposed. Among them,
flexible and has been used
suffers from a linear size
situations.
In this paper, we propos
without the linear-size dra
length, and our algorithn
pairings, that are already
We prove the security of o
we show that protocols u
more efficient constructio

1 Introduction

Digital signature is one of t
to provide the electronic v
more complex primitives. W
usually requires a signature
block, signatures must not
the other building blocks c
require a signature scheme
with zero-knowledge proofs.

1.1 Related Works

Constructing a versatile si
of the first construction sp
proposed by Camenisch an
RSA assumption [BP97], all
of a signature.

The emergence of pairin
nature schemes compatible
use bilinear groups, *i.e.* a
$e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$. In 200
nature scheme [CL04] whos
group signatures [BCN+10]

This is the full version of the extended
Proceedings of the Cryptographers Tra
(29 February – 4 March 2016, San Fra
Kazue Sako Ed. Springer-Verlag, LNC

Sh

I

[1] Éco
[2] (

Abstract. Digital signat
the development of pairin
proposed. Among them,
flexible and has been used
suffers from a linear size
situations.
In this paper, we propos
without the linear-size dra
length, and our algorithn
pairings, that are already
We prove the security of o
we show that protocols u
more efficient constructio

1 Introduction

Digital signature is one of t
to provide the electronic v
more complex primitives. W
usually requires a signature
block, signatures must not
the other building blocks c
require a signature scheme
with zero-knowledge proofs.

1.1 Related Works

Constructing a versatile si
of the first construction sp
proposed by Camenisch an
RSA assumption [BP97], all
of a signature.

The emergence of pairin
nature schemes compatible
use bilinear groups, *i.e.* a
$e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$. In 200
nature scheme [CL04] whos
group signatures [BCN+10]

This is the full version of the extended
Proceedings of the Cryptographers Tra
(29 February – 4 March 2016, San Fra
Kazue Sako Ed. Springer-Verlag, LNC

Sh

I

[1] Éco
[2] (

Abstract. Digital signat
the development of pairin
proposed. Among them,
flexible and has been used
suffers from a linear size
situations.
In this paper, we propos
without the linear-size dra
length, and our algorithn
pairings, that are already
We prove the security of o
we show that protocols u
more efficient constructio

1 Introduction

Digital signature is one of t
to provide the electronic v
more complex primitives. W
usually requires a signature
block, signatures must not
the other building blocks c
require a signature scheme
with zero-knowledge proofs.

1.1 Related Works

Constructing a versatile si
of the first construction sp
proposed by Camenisch an
RSA assumption [BP97], all
of a signature.

The emergence of pairin
nature schemes compatible
use bilinear groups, *i.e.* a
$e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$. In 200
nature scheme [CL04] whos
group signatures [BCN+10]

This is the full version of the extended
Proceedings of the Cryptographers Tra
(29 February – 4 March 2016, San Fra
Kazue Sako Ed. Springer-Verlag, LNC

Sh

I

[1] Éco
[2] (

Abstract. Digital signat
the development of pairin
proposed. Among them,
flexible and has been used
suffers from a linear size
situations.
In this paper, we propos
without the linear-size dra
length, and our algorithn
pairings, that are already
We prove the security of o
we show that protocols u
more efficient constructio

1 Introduction

Digital signature is one of t
to provide the electronic v
more complex primitives. W
usually requires a signature
block, signatures must not
the other building blocks c
require a signature scheme
with zero-knowledge proofs.

1.1 Related Works

Constructing a versatile si
of the first construction sp
proposed by Camenisch an
RSA assumption [BP97], all
of a signature.

The emergence of pairin
nature schemes compatible
use bilinear groups, *i.e.* a
$e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$. In 200
nature scheme [CL04] whos
group signatures [BCN+10]

This is the full version of the extended
Proceedings of the Cryptographers Tra
(29 February – 4 March 2016, San Fra
Kazue Sako Ed. Springer-Verlag, LNC

Sh

I

[1] Éco
[2] (

Abstract. Digital signat
the development of pairin
proposed. Among them,
flexible and has been used
suffers from a linear size
situations.
In this paper, we propos
without the linear-size dra
length, and our algorithn
pairings, that are already
We prove the security of o
we show that protocols u
more efficient constructio

1 Introduction

Digital signature is one of t
to provide the electronic v
more complex primitives. W
usually requires a signature
block, signatures must not
the other building blocks c
require a signature scheme
with zero-knowledge proofs.

1.1 Related Works

Constructing a versatile si
of the first construction sp
proposed by Camenisch an
RSA assumption [BP97], all
of a signature.

The emergence of pairin
nature schemes compatible
use bilinear groups, *i.e.* a
$e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$. In 200
nature scheme [CL04] whos
group signatures [BCN+10]

This is the full version of the extended
Proceedings of the Cryptographers Tra
(29 February – 4 March 2016, San Fra
Kazue Sako Ed. Springer-Verlag, LNC

Sh

I

[1] Éco
[2] (

Abstract. Digital signat
the development of pairin
proposed. Among them,
flexible and has been used
suffers from a linear size
situations.
In this paper, we propos
without the linear-size dra
length, and our algorithn
pairings, that are already
We prove the security of o
we show that protocols u
more efficient constructio

1 Introduction

Digital signature is one of t
to provide the electronic v
more complex primitives. W
usually requires a signature
block, signatures must not
the other building blocks c
require a signature scheme
with zero-knowledge proofs.

1.1 Related Works

Constructing a versatile si
of the first construction sp
proposed by Camenisch an
RSA assumption [BP97], all
of a signature.

The emergence of pairin
nature schemes compatible
use bilinear groups, *i.e.* a
$e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$. In 200
nature scheme [CL04] whos
group signatures [BCN+10]

This is the full version of the extended
Proceedings of the Cryptographers Tra
(29 February – 4 March 2016, San Fra
Kazue Sako Ed. Springer-Verlag, LNC

Sh

I

[1] Éco
[2] (

Abstract. Digital signat
the development of pairin
proposed. Among them,
flexible and has been used
suffers from a linear size
situations.
In this paper, we propos
without the linear-size dra
length, and our algorithn
pairings, that are already
We prove the security of o
we show that protocols u
more efficient constructio

1 Introduction

Digital signature is one of t
to provide the electronic v
more complex primitives. W
usually requires a signature
block, signatures must not
the other building blocks c
require a signature scheme
with zero-knowledge proofs.

1.1 Related Works

Constructing a versatile si
of the first construction sp
proposed by Camenisch an
RSA assumption [BP97], all
of a signature.

The emergence of pairin
nature schemes compatible
use bilinear groups, *i.e.* a
$e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$. In 200
nature scheme [CL04] whos
group signatures [BCN+10]

This is the full version of the extended
Proceedings of the Cryptographers Tra
(29 February – 4 March 2016, San Fra
Kazue Sako Ed. Springer-Verlag, LNC

Sh

I

[1] Éco
[2] (

Abstract. Digital signat
the development of pairin
proposed. Among them,
flexible and has been used
suffers from a linear size
situations.
In this paper, we propos
without the linear-size dra
length, and our algorithn
pairings, that are already
We prove the security of o
we show that protocols u
more efficient constructio

1 Introduction

Digital signature is one of t
to provide the electronic v
more complex primitives. W
usually requires a signature
block, signatures must not
the other building blocks c
require a signature scheme
with zero-knowledge proofs.

1.1 Related Works

Constructing a versatile si
of the first construction sp
proposed by Camenisch an
RSA assumption [BP97], all
of a signature.

The emergence of pairin
nature schemes compatible
use bilinear groups, *i.e.* a
$e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$. In 200
nature scheme [CL04] whos
group signatures [BCN+10]

This is the full version of the extended
Proceedings of the Cryptographers Tra
(29 February – 4 March 2016, San Fra
Kazue Sako Ed. Springer-Verlag, LNC

Sh

I

[1] Éco
[2] (

Abstract. Digital signat
the development of pairin
proposed. Among them,
flexible and has been used
suffers from a linear size
situations.
In this paper, we propos
without the linear-size dra
length, and our algorithn
pairings, that are already
We prove the security of o
we show that protocols u
more efficient constructio

1 Introduction

Digital signature is one of t
to provide the electronic v
more complex primitives. W
usually requires a signature
block, signatures must not
the other building blocks c
require a signature scheme
with zero-knowledge proofs.

1.1 Related Works

Constructing a versatile si
of the first construction sp
proposed by Camenisch an
RSA assumption [BP97], all
of a signature.

The emergence of pairin
nature schemes compatible
use bilinear groups, *i.e.* a
$e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$. In 200
nature scheme [CL04] whos
group signatures [BCN+10]

This is the full version of the extended
Proceedings of the Cryptographers Tra
(29 February – 4 March 2016, San Fra
Kazue Sako Ed. Springer-Verlag, LNC

Sh

I

[1] Éco
[2] (

Abstract. Digital signat
the development of pairin
proposed. Among them,
flexible and has been used
suffers from a linear size
situations.
In this paper, we propos
without the linear-size dra
length, and our algorithn
pairings, that are already
We prove the security of o
we show that protocols u
more efficient constructio

1 Introduction

Digital signature is one of t
to provide the electronic v
more complex primitives. W
usually requires a signature
block, signatures must not
the other building blocks c
require a signature scheme
with zero-knowledge proofs.

1.1 Related Works

Constructing a versatile si
of the first construction sp
proposed by Camenisch an
RSA assumption [BP97], all
of a signature.

The emergence of pairin
nature schemes compatible
use bilinear groups, *i.e.* a
$e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$. In 200
nature scheme [CL04] whos
group signatures [BCN+10]

This is the full version of the extended
Proceedings of the Cryptographers Tra
(29 February – 4 March 2016, San Fra
Kazue Sako Ed. Springer-Verlag, LNC

Sh

I

[1] Éco
[2] (

Abstract. Digital signat
the development of pairin
proposed. Among them,
flexible and has been used
suffers from a linear size
situations.
In this paper, we propos
without the linear-size dra
length, and our algorithn
pairings, that are already
We prove the security of o
we show that protocols u
more efficient constructio

1 Introduction

Digital signature is one of t
to provide the electronic v
more complex primitives. W
usually requires a signature
block, signatures must not
the other building blocks c
require a signature scheme
with zero-knowledge proofs.

1.1 Related Works

Constructing a versatile si
of the first construction sp
proposed by Camenisch an
RSA assumption [BP97], all
of a signature.

The emergence of pairin
nature schemes compatible
use bilinear groups, *i.e.* a
$e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$. In 200
nature scheme [CL04] whos
group signatures [BCN+10]

This is the full version of the extended
Proceedings of the Cryptographers Tra
(29 February – 4 March 2016, San Fra
Kazue Sako Ed. Springer-Verlag, LNC

Sh

I

[1] Éco
[2] (

Abstract. Digital signat
the development of pairin
proposed. Among them,
flexible and has been used
suffers from a linear size
situations.
In this paper, we propos
without the linear-size dra
length, and our algorithn
pairings, that are already
We prove the security of o
we show that protocols u
more efficient constructio

1 Introduction

Digital signature is one of th
to provide the electronic v
more complex primitives. W
usually requires a signature
block, signatures must not
the other building blocks c
require a signature scheme
with zero-knowledge proofs.

1.1 Related Works

Constructing a versatile si
of the first construction sp
proposed by Camenisch an
RSA assumption [BP97], all
of a signature.

The emergence of pairin
nature schemes compatible
use bilinear groups, *i.e.* a
$e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$. In 200
nature scheme [CL04] whos
group signatures [BCN+10]

This is the full version of the extended
Proceedings of the Cryptographers Tra
(29 February – 4 March 2016, San Fra
Kazue Sako Ed. Springer-Verlag, LNC

Sh

I

[1] Éco
[2] (

Abstract. Digital signat
the development of pairin
proposed. Among them,
flexible and has been used
suffers from a linear size
situations.
In this paper, we propos
without the linear-size dra
length, and our algorithn
pairings, that are already
We prove the security of o
we show that protocols u
more efficient constructio

1 Introduction

Digital signature is one of t
to provide the electronic v
more complex primitives. W
usually requires a signature
block, signatures must not
the other building blocks c
require a signature scheme
with zero-knowledge proofs.

1.1 Related Works

Constructing a versatile si
of the first construction sp
proposed by Camenisch an
RSA assumption [BP97], all
of a signature.

The emergence of pairin
nature schemes compatible
use bilinear groups, *i.e.* a
$e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$. In 200
nature scheme [CL04] whos
group signatures [BCN+10]

This is the full version of the extended
Proceedings of the Cryptographers Tra
(29 February – 4 March 2016, San Fra
Kazue Sako Ed. Springer-Verlag, LNC

Sh

I

[1] Éco
[2] (

Abstract. Digital signat
the development of pairin
proposed. Among them,
flexible and has been used
suffers from a linear size
situations.
In this paper, we propos
without the linear-size dra
length, and our algorithn
pairings, that are already
We prove the security of o
we show that protocols u
more efficient constructio

1 Introduction

Digital signature is one of t
to provide the electronic v
more complex primitives. W
usually requires a signature
block, signatures must not
the other building blocks c
require a signature scheme
with zero-knowledge proofs.

1.1 Related Works

Constructing a versatile si
of the first construction sp
proposed by Camenisch an
RSA assumption [BP97], all
of a signature.

The emergence of pairin
nature schemes compatible
use bilinear groups, *i.e.* a
$e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$. In 200
nature scheme [CL04] whos
group signatures [BCN+10]