Toward Efficient Certificateless Signcryption from (and without) Bilinear Pairings

Paulo S. L. M. Barreto, Alexandre M. Deusajute, Eduardo S. Cruz, Geovandro C. F. Pereira, Rodrigo R. Silva

Departamento de Engenharia de Computação e Sistemas Digitais, Escola Politécnica, Universidade de São Paulo, Brasil

Agenda

- Introduction
- The proposed scheme
- Efficiency
- Conclusion

Agenda

- Introduction
- The proposed scheme
- Efficiency
- Conclusion

Introduction

- Conventional or certificate-based cryptosystems
- Identity based cryptosystems
- Certificateless cryptosystems

Conventional cryptosystems

- Users choose their own private keys and compute their public keys
- Certification authorities link user's identity and user-generated public keys through a certificate
- Need of a Public Key Infrastructure (PKI): high maintenance costs
- Bandwidth consumption makes costs and usability prohibitive in a resource limited cenary

Identity-based cryptosystems

- Introduced by Shamir (1984) as an attempt do mitigate the burden of a PKI
- Private keys generated by a Key Generation Bureau (KGB) or Trust Authority (TA)
- Public keys are arbitrary strings, usually representing the user's identity into the system (e-mail, cell phone number)
- No need for certificates, but KGB/TA-generated private keys implicitly raise a key escrow mechanism

Certificateless cryptosystems

- CL cryptosystems to address the key escrow issue
- Partitioned private keys: an IB partial key (known to the KGB) and one conventional non-certified partial key (unknown to the KGB)
- Best features of IB and CB combined

Certificateless cryptosystems

- CL encryption schemes successfully derived from IB algorithms
- CL signcryption schemes face tough efficiency problems

Signcryption

- Integrated method to encrypt and sign a message in a more efficient or robust way [Zheng 1997]
- Efficiency: processing time, bandwidth occupation, key management

Our approach

- Usually IB encryption plus IB signature are converted into a CL protocol
- Hybrid key authentication mechanism
- Conventional encryption and signature mechanism
- Public verification key validated by IB techniques
- Self-Certified rather than Certificateless: user must interact with KGB before broadcasting public keys

Underlying schemes

- BLMQ: identity-based signature scheme
- Schnorr: conventional signature scheme, combined with a CL encryption scheme – CL signcryption
- Zheng: conventional signcryption method
- The formal security proofs for the underlying schemes are still valid with slight modifications

- Other protocols could have been used

Motivation

- Current cryptosystems didn't satisfy the requirements of a Secure SMS environment
- Constrained bandwidth and processing resources environment

Agenda

- Introduction
- The proposed scheme
- Efficiency
- Conclusion

The proposed scheme

The main idea:

- BLMQ, Zheng and Schnorr combined into a self-certified signcryption scheme: BDCPS
- User chosen key pairs validated by identity-based mechanism

The proposed scheme

- **Set-Secret-Value**: Alice may choose her own secret value x_A
- **Set-Public-Value**: public value y_A computed by Alice from her secret value
- **Private-Key-Extract**: IB private key Q_A computed by KGB from Alice's public value and identifier
  - KGB doesn't know Alice's secret value
- Alice's complete private key is composed by secret value x_A and partial private key Q_A

The proposed scheme

- **Set-Public-Key**: Alice computes her public key from her partial IB public key and her secret value
- **Public-Key-Validate**: the validation process combines the verification of a Schnorr signature with that of a BLMQ signature. A public value y_E is validated against an identity ID_E.

The proposed scheme

- **Signcrypt**: Alice signcrypts message m to Bob under his public key y_B (previously validated), x_A, y_A and ID_A

- **Unsigncrypt**: given y_A (previously validated), $x_{B,}$ y_B and ID_B,Bob can unsigncrypt m

- Completely conventional algorithms

The proposed scheme

- Signatures are untransferable - the recipient cannot convince third parties that the sender really signed the message, since the verification depends on the recipient’s private key
- Key validation mecanism can be used with other signcryption protocols which address this issue.

Agenda

- Introduction
- The proposed scheme
- Efficiency
- Conclusion

Efficiency

- Pairing computation is the most expensive operation
- Removing pairings may mean to sacrifice some functionality
- A balance between these two constraints lead to a satisfactory result

Efficiency

- Costs comparison:
  - Barbosa-Farshim (Certificateless signcryption)
  - BLMQ (Identity-based signcryption)
  - LHX (Self-Certified signcryption)
  - CLPKE (CL encryption-only)
- Efficiency inherited from Zheng signcryption with a Schnorr-style signature

Efficiency

- Tests run on an AMD TurionTM64 X2 platform at 2.3 Ghz
- 256-bit BN and 256-bit MNT curves
- Java implementations

Efficiency

- Key validation/processing (ms)

	B-F	BLMQ	LHX	CLPKE	ours
BN-256	97.0	11.5	197.8	41.7	195.5
MNT4-256	65.5	15.7	133.4	5.4	93.5

- Signcryption efficiency (ms)

	B-F	BLMQ	LHX	CLPKE	ours
BN-256	104.8	76.1	122.3	124.3	41.2
MNT4-256	77.6	44.3	57.8	16.0	5.3

- Unsigncryption efficiency (ms)

	B-F	BLMQ	LHX	CLPKE	ours
BN-256	399.0	236.0	236.0	124.3	54.8
MNT4-256	280.0	142.1	142.1	26.4	10.4

Agenda

- Introduction
- The proposed scheme
- Efficiency
- Conclusion

Conclusion

- BDCPS is an efficient certificateless signcryption scheme based on the BLMQ identity-based signature, the Schnorr conventional signature, and the Zheng signcryption protocol
- Pairings limited to key validation
- The overall result is much faster than existing alternatives and uses less bandwidth than many of them
- There is a work in progress aiming at the practical application of BDCPS

Contact info

- pbarreto@larc.usp.br
- adeusajute@larc.usp.br
- eduardo.cruz@poli.usp.br
- geovandro.pereira@poli.usp.br
- rodrigo.silva1@poli.usp.br

- Presentation available at http://stoa.usp.br/rodrigors/files

Thank you!

Efficiency

- Barbosa-Farshim bandwidth overhead only matches our method for pairings on supersingular elliptic curves – otherwise we take less bandwidth
- The bandwidth occupation of our method and CLPKE are approx-imately the same
- Heavy key validation cost is amortized, although a cheaper alternative is still desirable

Contact info

- pbarreto@larc.usp.br
- adeusajute@larc.usp.br
- eduardo.cruz@poli.usp.br
- geovandro.pereira@poli.usp.br
- rodrigo.silva1@poli.usp.br

- Presentation available at http://stoa.usp.br/rodrigors/files

Thank you!