Secure and Privacy-Friendly Public Key Generation and Certification

IEEE TrustCom 2014

Fábio Borges, Leonardo A. Martucci, Filipe Beato, and Max Mühlhäuser

Technische Universität Darmstadt – Telecooperation Lab
Center for Advanced Security Research Darmstadt (CASED)

Table of Contents

Outline

Problems

Application Scenarios

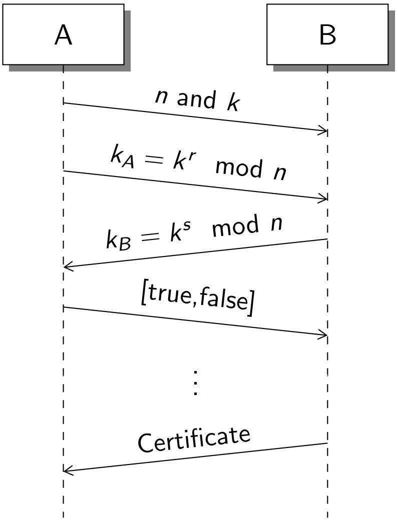
Key Generation and Certification:

- Electronic Identity Cards
- The Smart Grid - 80% of households by 2020 in EU
- Insecure Cryptographic Parameters
  - Servers should guarantee that key parameters are safe
  - Clients do not disclose any secret information to the servers

Table of Contents

Key Agreement

Diagram



Key Agreement

Algorithm

Algorithm 1: DH for an RSA public key [Klima et al., 2007]

begin
    A chooses two primes p and q, and computes $n = pq$
    A chooses $1 < k \in \mathbb{Z}_n$ such that $\gcd(k, n) = 1$
    A sends (k, n) to B
    A chooses $r \in \mathbb{Z}_n$
    A calculates k^r and sends the result to B while keeping r secret
    B chooses $s \in \mathbb{Z}_n$
    B calculates k^s and sends the result to A while keeping s secret
    Both A and B calculate $e = (k^r)^s = (k^s)^r$
    if $\gcd(e, \varphi(n)) \neq 1$ **then**
        A sends **false** to B
        A runs **goto begin**
    else
        A sends **true** to B
        A calculates $d = e^{-1}$

Table of Contents

Core Idea

Let $p = 3$ and $q = 5$, thus
$k = 7 \Rightarrow k^2 \equiv 4 \mod pq$ and

$$\gcd(k^2 \mod pq, \varphi) = 4$$

However, if we choose the next exponent k^3, then $k^3 \equiv 13 \mod pq$ and

$$\gcd(k^3, \varphi) = 1$$

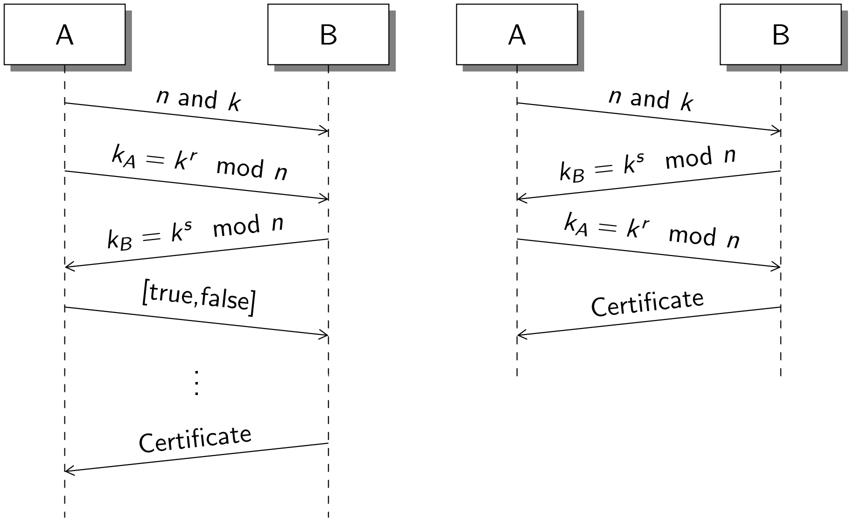
Constrained Key Agreement

Algorithm 2: Constrained Diffie-Hellman on RSA

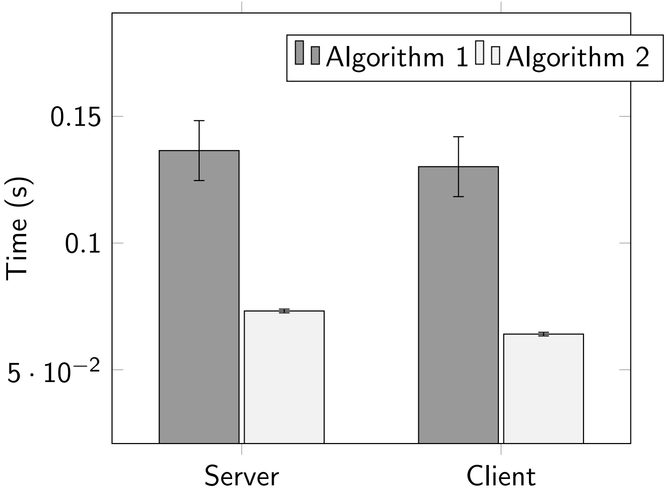
```
begin
    A chooses two safe primes p and q, and computes n = pq
    A chooses k < n with big order.
    A sends n and k to B
    B chooses a randomized s ∈ ℤ_n
    B calculates k^s and sends the result to A while keeping s secret
    e = 0
    while gcd(e, φ(n)) ≠ 1 do
        A chooses randomized r ∈ ℤ_n
        A calculates e = (k^s)^r
    A calculates k^r and sends the result to B while keeping r secret
    B calculates e = (k^r)^s = (k^s)^r
    A calculates d = e^{-1}
```

Table of Contents

Number of Messages

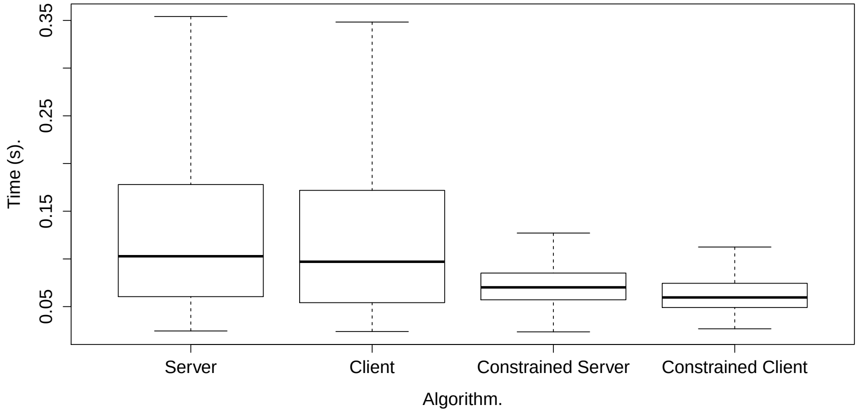


Mean Processing Time



Total Processing Time Required

Box plot without outliers



Number of Failed Attempts

Box plot without outliers

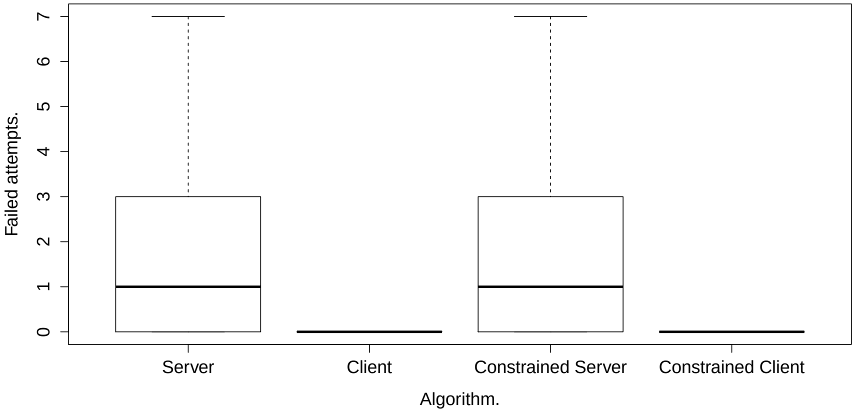


Table of Contents

Further Work

- New applications for constrained key agreements
- Variations over other cryptographic primitives like ECC

Table of Contents

Conclusion

TECHNISCHE UNIVERSITÄT DARMSTADT

- Key Generation and Certification protocols should have:
  - Transparency for security
  - Privacy for the clients
  - Guarantees for the servers

Thank You!

Any comments and suggestions are welcomed.
Contact: fabio.borges@cased.de

Bibliography

Borges, F., Martucci, L. A., Beato, F., and Mühlhäuser, M. (2014).
Secure and privacy-friendly public key generation and certification.
In *Proceedings of the 13th IEEE TrustCom 2014*. IEEE CS.
To Appear.

Klima, R., Sigmon, N., and Stitzinger, E. (2007).
Applications of Abstract Algebra With Maple And Matlab.
Number Bd. 1 in Discrete Mathematics And Its Applications. Chapman & Hall/CRC.