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

Introduction

Related Work

Protocol

Results and Simulations

Further Work

Conclusion
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

- Introduction
- Related Work
- Protocol
- Results and Simulations
- Further Work
- Conclusion
Key Agreement

Diagram

A

n and k

$ k_A = k^r \mod n $ 

$ k_B = k^s \mod n $ 

[true,false]

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

1 begin
2 A chooses two primes \( p \) and \( q \), and computes \( n = pq \)
3 A chooses \( 1 < k \in \mathbb{Z}_n \) such that \( \gcd(k, n) = 1 \)
4 A sends \((k, n)\) to B
5 A chooses \( r \in \mathbb{Z}_n \)
6 A calculates \( k^r \) and sends the result to B while keeping \( r \) secret
7 B chooses \( s \in \mathbb{Z}_n \)
8 B calculates \( k^s \) and sends the result to A while keeping \( s \) secret
9 Both A and B calculate \( e = (k^r)^s = (k^s)^r \)
10 if \( \gcd(e, \varphi(n)) \neq 1 \) then
11 \hspace{1em} A sends \textit{false} to B
12 \hspace{1em} A runs \textit{goto begin}
13 else
14 \hspace{1em} A sends \textit{true} to B
15 \hspace{1em} A calculates \( d = e^{-1} \)
# Table of Contents

- Introduction
- Related Work
- Protocol
- Results and Simulations
- Further Work
- Conclusion
Let \( p = 3 \) and \( q = 5 \), thus
\[
k = 7 \implies k^2 \equiv 4 \mod pq \quad \text{and} \quad \gcd(k^2 \mod pq, \varphi) = 4
\]

However, if we choose the next exponent \( k^3 \), then \( k^3 \equiv 13 \mod pq \) and
\[
\gcd(k^3, \varphi) = 1
\]
Algorithm 2: Constrained Diffie-Hellman on RSA

begin

1. A chooses two safe primes $p$ and $q$, and computes $n = pq$
2. A chooses $k < n$ with big order.
3. A sends $n$ and $k$ to B
4. B chooses a randomized $s \in \mathbb{Z}_n$
5. B calculates $k^s$ and sends the result to A while keeping $s$ secret
6. $e = 0$
7. while $\gcd(e, \varphi(n)) \neq 1$ do
8.     A chooses randomized $r \in \mathbb{Z}_n$
9.     A calculates $e = (k^s)^r$
10. A calculates $k^r$ and sends the result to B while keeping $r$ secret
11. B calculates $e = (k^r)^s = (k^s)^r$
12. A calculates $d = e^{-1}$
Table of Contents

Introduction

Related Work

Protocol

Results and Simulations

Further Work

Conclusion
Number of Messages

\[ k_A = k^r \mod n \]
\[ k_B = k^s \mod n \]

[true, false]...

Certificate

Mean Processing Time

Algorithm 1

Algorithm 2

Time (s)

Server

Client

5 \cdot 10^{-2}

0.1

0.15
Total Processing Time Required

Box plot without outliers

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Time (s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td></td>
</tr>
<tr>
<td>Client</td>
<td></td>
</tr>
<tr>
<td>Constrained Server</td>
<td></td>
</tr>
<tr>
<td>Constrained Client</td>
<td></td>
</tr>
</tbody>
</table>

Number of Failed Attempts

Box plot without outliers

Algorithm.
Failed attempts.

Table of Contents

Introduction

Related Work

Protocol

Results and Simulations

Further Work

Conclusion
Further Work

- New applications for constrained key agreements
- Variations over other cryptographic primitives like ECC
# Table of Contents

- Introduction
- Related Work
- Protocol
- Results and Simulations
- Further Work
- Conclusion
Conclusion

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