PROTECT

a Platform for Robust Threshold Cryptography

Jason Resch, Christian Cachin, Hugo Krawczyk, Tal Rabin, Chrysa Stathakopoulou
• PROTECT is an open source (MIT Licensed) platform for threshold-secure operations
  • Tolerates \(\frac{n}{3} - \frac{n}{2}\) Byzantine faults
  • Operates over eventually synchronous networks
  • Self-heals and self-secures after faults and breaches

• Supported operations:
  • (O)PRF, ECIES, BLS, RSA (Blind)Sign/Decrypt
  • Generate, Store, Read, Delete, Enable, Disable

• Future enhancement goals:
  • Share conversion, Schnorr signatures, ECDSA
  • Share multiplication, MPC, Threshold AES
  • RSA (DKG/Refresh/Recover)
  • Post-Quantum Cryptography
System Model

Asynchronous Bound

?  

1/3  

1/2  

Synchronous Bound
\[
\begin{align*}
    f &= \frac{1}{3} \\
    f_S &= n - 2f_L - 1 \\
    f_L &= \frac{(n - f_S - 1)}{2}
\end{align*}
\]
<table>
<thead>
<tr>
<th>Setting</th>
<th>Safety</th>
<th>Liveness</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conventional Setting ($f = 2$)</td>
<td>❌</td>
<td>❌</td>
</tr>
<tr>
<td>Tunable Security ($f_L = 1$, $f_S = 3$)</td>
<td>❌</td>
<td>❌</td>
</tr>
</tbody>
</table>

**Tunability in Practice**
System Architecture
Performance Results
1. Downloading
2. Installing
3. Configuration
4. Launching Servers
5. Client Setup
6. Secret Management:
   a. Distributed Generation
   b. Proactive Refresh
   c. Share Recovery
7. Cryptographic Operations:
   a. Decryption
   b. Signing
1. Downloading
2. Installing
3. Configuration
4. Launching Servers
5. Client Setup
6. Secret Management:
   a. Distributed Generation
   b. Proactive Refresh
   c. Share Recovery
7. Cryptographic Operations:
   a. Decryption
   b. Signing

https://youtu.be/9sDgPOUpADw
1. Downloading
2. Installing
3. Configuration
4. Launching Servers
5. Client Setup
6. Secret Management:
   a. Distributed Generation
   b. Proactive Refresh
   c. Share Recovery
7. Cryptographic Operations:
   a. Decryption
   b. Signing

https://youtu.be/Cz9VV0FzW10
1. Downloading
2. Installing
3. Configuration
4. Launching Servers
5. Client Setup
6. Secret Management:
   a. Distributed Generation
   b. Proactive Refresh
   c. Share Recovery
7. Cryptographic Operations:
   a. Decryption
   b. Signing

https://youtu.be/BHM17XE6ZhQ
1. Downloading
2. Installing
3. Configuration
4. Launching Servers
5. Client Setup
6. Secret Management:
   a. Distributed Generation
   b. Proactive Refresh
   c. Share Recovery
7. Cryptographic Operations:
   a. Decryption
   b. Signing

https://youtu.be/H4rX3gtqjrI
1. Downloading
2. Installing
3. Configuration
4. Launching Servers
5. Client Setup
6. Secret Management:
   a. Distributed Generation
   b. Proactive Refresh
   c. Share Recovery
7. Cryptographic Operations:
   a. Decryption
   b. Signing

https://youtu.be/DXvrh1b8GH4
1. Downloading
2. Installing
3. Configuration
4. Launching Servers
5. Client Setup
6. Secret Management:
   a. Distributed Generation
   b. Proactive Refresh
   c. Share Recovery
7. Cryptographic Operations:
   a. Decryption
   b. Signing

https://youtu.be/ZMjMlC52MJc
1. Downloading
2. Installing
3. Configuration
4. Launching Servers
5. Client Setup
6. Secret Management:
   a. Distributed Generation
   b. Proactive Refresh
   c. Share Recovery
7. Cryptographic Operations:
   a. Decryption
   b. Signing

https://youtu.be/hVjxZmUPwlU
Q&A + Discussion

• Further Reading:

  • The “PROTECT” open source project:
    • New contributors, testers, implementers welcome!

  • Our eprint “Tunable Protocols for Threshold and Proactive Cryptography”
    • Provides details of the underlying protocols
    • Coming soon!