Reducing HSM Reliance in Payments through Proxy Re-Encryption

Siva Gaddam, Atul Luykx, Rohit Sinha and Gaven Watson
PINs and PIN Translation

First, what is a PIN?

User Authentication

Common method for cardholder verification
Transporting PINs
Securing delivery to verifier
Routing a Transaction

Point of Sale/PoS Partner → Payment Gateway → Merchant Bank → Network Processor → Issuer Bank
What happens to PINs during a transaction?

How we use Hardware Security Modules (HSM)
Can we do better?
What are the requirements?

**Aim:** Reduce reliance on HSMs

**Restrictions:**
- PINs only in clear inside an HSM
- Pairwise Key Setup
- Ensure backwards compatibility
Finding a Different Solution...

**Why not just use Public-Key Encryption?**

- PoS encrypts under Issuer Bank Public Key provided by the card.
- No PIN translation required.
- *Problem:* Requires significant changes to EMV standard and card re-issuance.

**Can we use more advanced techniques?**

- Let’s try *Proxy Re-Encryption*!
What is Proxy Re-encryption (PRE)?

Delegate decryption ability to someone else

Alice $\rightarrow C_A \rightarrow$ Proxy $\rightarrow C_B \rightarrow$ Bob
PKE to PRE

\[ \text{KeyGen}(1^\lambda) \rightarrow (sk_i, pk_i) \]

\[ \text{ReKeyGen}(sk_i, sk_j) \rightarrow rk_{i,j} \]

\[ \text{ReKeyGen}(sk_i, pk_j) \rightarrow rk_{i,j} \]

Bidirectional

Unidirectional

\[ \text{Encrypt}(pk_i, m) \rightarrow c \]

\[ \text{Decrypt}(sk_i, c) \rightarrow m \]

\[ \text{ReEncrypt}(rk_{i,j}, c) \rightarrow c' \]
Apply PRE to Payments

Recall the previous setting
Our Approach
Removing HSMs from the online flow
What are the advantages of PRE?

**Plan:** Replace HSMs with PRE

**Advantages:**
- Don’t need specialized hardware
- Pure software solution so better scaling, elasticity and reduced costs
- Equivalent Security - re-encrypt operation ensures PIN never exposed
Our Construction: High-Level Perspective

Bidirectional PRE

- Borrows ideas from BBS PRE

Hybrid Encryption
- KEM-DEM
  - Backwards Compatible with existing PIN Blocks

Our scheme is provably secure in a model which accurately represents the payment setting & extends recent HRA models
## Performance Evaluation

Eliminating the Network Latency

<table>
<thead>
<tr>
<th></th>
<th>PoS Terminal</th>
<th>Gateway</th>
<th>Merchant Bank</th>
<th>Network</th>
<th>Issuer Bank</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>HSM-based</td>
<td>98</td>
<td>920</td>
<td>920</td>
<td>920</td>
<td>900</td>
<td>3758</td>
</tr>
<tr>
<td>PRE-based</td>
<td>348</td>
<td>161</td>
<td>-</td>
<td>161</td>
<td>934</td>
<td>1604</td>
</tr>
</tbody>
</table>

### Latency (μs)

<table>
<thead>
<tr>
<th></th>
<th>Network/Gateways</th>
<th>Issuer Bank</th>
</tr>
</thead>
<tbody>
<tr>
<td>HSM-based</td>
<td>1086</td>
<td>1110</td>
</tr>
<tr>
<td>PRE-based</td>
<td>6240</td>
<td>1025</td>
</tr>
</tbody>
</table>

### Throughput (txs/sec)
Meeting Our Goals

Reduce Number of HSMs

PINs only in clear inside an HSM

Ensure backwards compatibility

Pairwise Key Setup

All but eliminated in online flow

Yes

Yes

Partially

Solution: Unidirectional PRE

Roadblock: Efficiency
Thank You!