The Abe-Okamoto Partially Blind Signature Scheme Revisited

Julia Kastner
ETH Zürich
Switzerland

Julian Loss
CISPA
Germany

Jiayu Xu
Oregon State University
USA
Partially Blind Signatures [AF96]

e.g. 1$^s$ "best before 24. 12."

\[ \text{info} \]

\[ \text{sk} \]

\[ R \]

\[ e \]

\[ s \]

\[ \text{pk}, m \]

\[ \sigma \]
Electronic Cash

Diagram:
- Bank
  - Green arrow: 1
  - Purple arrow: 5
  - Purple arrow: 5
  - Purple arrow: Unicorn (blue)
  - Green arrow: Unicorn (black)
Electronic Cash

Bank

1 $ → 5 $ → 5 $ → 5 $ → ?
Partial Blindness

\[ pk, mo, ma, info \]
Partial Blindness

\[ pk, mo, ma, \text{ info} \]

\[ b, 1-b \]
Partial Blindness

pk, mo, ma, info

b

1-b
Partial Blindness

\[ \text{pk, mo, mu, info} \]

\[ b \quad 1-b \]

\[ \{ (m_0, \sigma_0), (m_1, \sigma_1) \}

or \[ L \]
Partial Blindness

\[ pk, mo, ma, \text{info} \rightarrow \text{unicorn} \]

\[ b \quad \Lambda \rightarrow \text{b} \]

\[ \begin{cases} (m_0, \sigma_0) \\ (m_1, \sigma_1) \end{cases} \] or \[ \perp \]

m_0 \quad m_a

or \[ m_0 \quad m_a \]?
Electronic Cash
Electronic Cash

Bank

\[ \text{5$} \rightarrow \text{5$} \rightarrow \text{5$} \]

\[ \text{1$} \rightarrow \text{3x 5$} \]
One-more Unforgeability

sk \xrightarrow{pk} \text{unicorn}
One-more Unforgeability

\[ \text{sk} \rightarrow pk \]

\[ \text{sk} \leftrightarrow \text{pk} \]
One-more Unforgeability
One-more Unforgeability

\[ \text{sk} \rightarrow pk \rightarrow \text{sk} \]

\[ \text{Red arrows} \]

\[ \text{Green arrows} \]

\[ \text{Blue arrows} \]
One-more unforgeability

\[ \text{sk} \rightarrow \text{pk} \rightarrow \text{entity} \]

\[ \text{sk} \leftarrow \text{pk} \leftarrow \text{entity} \]

\[ \text{sk} \rightarrow \text{pk} \rightarrow \text{entity} \]

\[ \text{sk} \leftarrow \text{pk} \leftarrow \text{entity} \]
One-more Unforgeability

\[ sk \xrightarrow{pk} (m_1, \sigma_1, \text{info}) \]

\[ \vdots \]

\[ (m_e, \sigma_e, \text{info}) \]
Motivation

- [40'00] efficient DL-based PBS

- inspiration for several other schemes
e.g. [Abe 01], [BL13], [AHJ21]

- Proof strategy of interest for other similar schemes
Our Contribution

- Identify gap in original proof
- Mend gap
- Achieve similar bounds to original work
The Abe-Okamoto Scheme [AO00]

\[ \text{sk} = x \quad \text{e.g.} \quad 1 \$

\[ z = H^*(\text{info}) \]

\[ \text{pk} = g^x = y \]

\[ z = H^*(\text{info}) \]
The Abe-Okamoto Scheme [AO00]

\[ \text{sk} = x \]
\[ z = H^*(\text{info}) \]

\[ \text{pk} = g^x = y \]
\[ z = H^*(\text{info}) \]
The Abe–Okamoto Scheme [AO00]

\[ \text{pk} = g^x = y \]
\[ z = H^*(\text{info}) \]
\[ \text{sk} = x \]
\[ z = H^*(\text{info}) \]

\[ a, b \rightarrow \text{a, b} \rightarrow a \rightarrow b \rightarrow a \rightarrow x \]
\[ b \rightarrow \beta \]
\[ e = H(x, \beta, m, \text{info}) \]
The Abe-Okamoto Scheme [AO00]

\[ \text{pk} = g^x = y \]
\[ z = H^*(\text{info}) \]

\[ a, b \]
\[ a, b \]
\[ a \rightarrow x \]
\[ b \rightarrow \rho \]
\[ e \leftarrow H(x, \rho, m, \text{info}) \]

\[ c, r, \alpha, s \]
\[ c, r \sim \omega, \rho \]
\[ d, s \sim \delta, \sigma \]
The Abe-Okamoto Scheme [AO00]

\[ \text{sk} = x \]
\[ z = H^*(\text{info}) \]

\[ \text{pk} = g^x = y \]
\[ z = \text{h}^c(\text{info}) \]

\[ a, b \]
\[ a, b \]
\[ a \rightarrow x \]
\[ b \rightarrow \rho \]
\[ c, r, d, s \]
\[ c, r \rightarrow \omega, \rho \]
\[ d, s \rightarrow \delta, \sigma \]

\[ \text{sig} = (\omega, \rho, \delta, \sigma) \]
Verification

\[ \omega + \delta = H(1^\omega \cdot \mathcal{g}^p, 2^\delta \cdot \mathcal{g}^m, m, \text{info}) \]

"OR-Proof of two Schnorr-Signatures"
Proving One-more Unforgeability

Idea:

Simulate using $x$, extract $\text{dlog}_2$

OR

Simulate using $\text{dlog}_2$, extract $x$
Reduction strategy

1. Pick "secret key" $x$ or $\log z$
Reduction strategy

1. Pick "secret key" $x$ or $\text{dkg} \ z$

2. Run adversary once
Reduction strategy

1. Pick "secret key" $x$ or $\text{dlog } z$

2. Run adversary once

3. Re-program RO
Reduction strategy

1. Pick "secret key" $x$ or $\text{dkog}_z$

2. Run adversary once

3. Re-program PO

4. Run adversary another time
Reduction strategy
1. Pick "secret key" $x$ or $\text{dkog} z$
2. Run adversary once
3. Re-program PO
4. Run adversary another time
5. Hope to get "other key"
Reduction strategy

1. Pick "secret key" $x$ or $\text{dlog} z$
2. Run adversary once
3. Re-Program PO
4. Run adversary another time
5. Hope to get "other key"
6. Return "other key" as solution to $x$
Reduction strategy

1. Pick "secret key" $x$ or $\text{dlog } z$

2. Run adversary once

3. Re-program PO

4. Run adversary another time

5. Hope to get "other key" $\triangle$

6. Return "other key" as solution to DL
Forking [PS96]

\[ H \]

\[ \varepsilon(\text{signature 1}, \text{signature 2}) \leadsto x \varepsilon \Rightarrow d\log z \]
Forking with an OR Proof

OR

get \times

get \log z
Reduction Goal

has "secret key"

reveals "other key"
Abstraction in progress...
\[ \text{dlog } z \]
Triangles [40'00']

- Potentially less nice
- Likely to sample

- Nice properties
- Unlikely to sample
Triangles [AO'00]

can use either $x$ or $\text{dlog} z$

potentially less nice likely to sample

nice properties unlikely to sample
Triangle Properties
Triangle Properties

\[
\begin{align*}
\text{or} & \quad \text{or} \\
\end{align*}
\]
The gap in [A0 '00] △

"if $\frac{4}{5}$ of triangle sides yield the bad witness
then $\frac{3}{5}$ of triangle bases yield the bad witness."

[Diagrams of triangles with different colors and line thicknesses]
Sharing Triangle "Bases"
Sharing Triangle "Sides"
Bounding

Can't happen "too often" by combinatorics
Summary

- [AO '00] efficient partially blind signature scheme
Summary

- [AO '00] efficient partially blind signature scheme

- Mending some gaps in proof
Summary

- \([\text{AO}'00]\) efficient partially blind signature scheme
- Mending some gaps in proof
- Similar reduction loss to original work
Summary

- [AO ’00] efficient partially blind signature scheme

- Mending some gaps in proof

- Similar reduction loss to original work
  \[ \rightarrow \text{small nr of signing sessions} \]
Summary

- [AO '00] efficient partially blind signature scheme
- Mending some gaps in proof
- Similar reduction loss to original work
  \( \Rightarrow \) Small nr of signing sessions

Open Questions

- Schemes with polynomial nr of signing sessions?
  \( \Rightarrow \) Overcome loss
Summary

- [AO'00] efficient partially blind signature scheme
- Mending some gaps in proof
- Similar reduction loss to original work

Open Questions

- Schemes with polynomial nr of signing sessions?

  \( \downarrow \) candidate: [Abe01]