Efficient Protocols for Set Membership and Range Proofs

Jan Camenisch[1] Rafik Chaabouni[1,2] abhi shelat[3]

[1]IBM ZRL [2]EPFL LASEC [3]U. of Virginia

ASIACRYPT 2008 December 9, 2008

Our Focus Interest

New Efficient Protocols for Set Membership and Range Proofs

- Set Membership

Public parameters: set Φ of integer elements, $C = Com(m)$

Prover		**Verifier**
$m \in \Phi$		
	$\xrightarrow{PK\{m \,:\, C=Com(m) \wedge m\in\Phi\}}$	

- Range (Interval) Proof: $\Phi = [a, b)$
- *m* must not be revealed (zero-knowledge)
- Honest Verifier Model (Malicious Verifier possible)
- Asymptotically Better Efficiency

  Practically Competitive

Community Interest

Usefulness?

- Cryptography Primitives
- Revocation Credentials (Freshness of a Token)
- Anonymous Credentials (Identity and Authentication Proofs)

Example: Use of Range Proof

- Offer from IACR to travel to Melbourne, Australia for the Asiacrypt 2008 conference.
- Restriction for young PhD candidates: under 26, but older than 18.
- Strict age anonymity for the airplane company.
- Bob wants to go (he has a paper accepted).

1. Introduction
   - Our Focus Interest
   - Community Interest
2. Prior State of the Art
   - Common Range Proofs
   - Berry Schoenmakers' Scheme
3. Our New Solutions
   - Better Solutions?
   - Breeding Ground
   - New Set Membership
   - Application to Range Proof
4. Conclusion

Common Range Proofs

Boudot's range proof with RSA assumption

- Positivity proofs: $x \in (a, b) \Leftrightarrow \begin{cases} 0 < x - a; \\ 0 < b - x. \end{cases}$
- In presentation: Sum of four square.
- Lagrange Theorem ∼1770: Any positive number can be represented as the sum of four square

Sum of square method

- Rabin and Shallit 1986: probabilistic polynomial time (PPT) algorithm (4 square method)
  - $\longrightarrow$ Some numbers can be represented as the sum of three square (Numbers that cannot be the sum of 3 squares: $4^n(8x+7)$)
- Application to positivity proofs by Lipmaa in 2001 for the 4 square method
- Application to positivity proofs by Groth in 2005 for the 3 square method

Disadvantages

- RSA Assumption
- Large Complexity: $O\left(k^4\right)$

Folklore Bit Commitment

Public parameters: $\Phi = \left[0, 2^k\right)$, C and C_i

Prover | **Verifier**

$m \in \Phi,\ m = \prod_{i=0}^{k-1} m_i 2^i$

$C = Com(m),\ C_i = Com(m_i)$

$$\xrightarrow[OR-Proof\ \sim 2\ Schnorr\ proofs]{PK\{(m_i,\ \forall i)\ :\ C_i = Com(m_i)\ \wedge\ m_i \in \{0,1\}\}}$$

Prior State of the Art
Common Range Proofs

Schnorr proof

Prover		Verifier
$x = \log_g h$		h
$d = g^u,\ u \in_R \mathbb{Z}_p$	$\xrightarrow{\ d\ }$	
	$\xleftarrow{\ c\ }$	$c \in_R \mathbb{Z}_p$
$r = u + cx$	$\xrightarrow{\ r\ }$	$g^r \stackrel{?}{=} dh^c$

Folklore Bit Commitment

Public parameters: $\Phi = \left[0, 2^k\right)$, $C = Com(m)$ and $C_i = Com(m_i)$

Prover | **Verifier**

$m \in \Phi$, $m = \prod_{i=0}^{k-1} m_i 2^i$

$$\xrightarrow[OR-Proof\ \sim 2\ Schnorr\ proofs]{PK\{(m_i,\ \forall i)\ :\ C_i = Com(m_i)\ \wedge\ m_i \in \{0,1\}\}}$$

Properties

- No RSA Assumption
- Still Large Complexity: $O(k)$

Berry Schoenmakers' Scheme

Building Blocks

- Improvments of folklore bit decomposition
- Exact proofs for small intervals
- Reduction of arbitrary ranges $[0, b)$ into 2 bit decompositions
  - AND-composition: $[0, b) = [0, 2^k) \cap [b - 2^k, b)$
  - OR-composition: $[0, b) = [0, 2^{k-1}) \cup [b - 2^{k-1}, b)$

Earlier Work

- [*LAN*02]

Berry Schoenmakers' Scheme

Decomposition of Upper Bound

- Product case $b = de$
- Sum case $b = d + e$
- Recursion down to Schnorr proofs
- Complexity of number b: minimal number of element 1 in order to write b with products and sums of element 1, including parentheses $7 = (1 + 1) * (1 + 1 + 1) + 1$.

Complexity?

- Asymptotic Complexity Still: $O(\log b) \sim O(k)$

1. Introduction
   - Our Focus Interest
   - Community Interest
2. Prior State of the Art
   - Common Range Proofs
   - Berry Schoenmakers' Scheme
3. Our New Solutions
   - Better Solutions?
   - Breeding Ground
   - New Set Membership
   - Application to Range Proof
4. Conclusion

Better Solutions?

Our Solution

- $Com(u, \ell) = O\left(\frac{k}{\log k - \log\log k}\right)$
- No RSA Assumptions
- Very competitive solution.

Breeding Ground

Shaking the Tree of Knowledge

- Why bit decomposition? What about base 3?

  $\longrightarrow$ Generalization to base u...

Base u Commitment

Public parameters: $\Phi = \left[0, u^\ell\right)$, $C = Com(m)$ and $C_i = Com(m_i)$

Prover | **Verifier**

$m \in \Phi$, $m = \prod_{i=0}^{\ell-1} m_i u^i$

$$\xrightarrow[\ell\ OR-Proofs\ \sim\ O(u) Schnorr\ proofs]{PK\{(m_i,\ \forall i)\ :\ C_i = Com(m_i)\ \wedge\ m_i \in \{0,\ldots,u-1\}\}}$$

Not Enough...

- Asymptotic Complexity: $O(u \cdot \ell)$

Shaking the Tree of Knowledge

- Why Schnorr proofs for basic set membership?
  - $\longrightarrow$ Signature based solution (Boneh-Boyen signatures in the Adaptive Oblivious Transfer of Jan Camenisch, Gregory Neven, and abhi shelat)
  - $\longrightarrow$ Cryptographic accumulators based solution (elements compression into a single accumulator with a witness on the accumulator membership for each element)

Set Membership Protocol

- Reduction of Set Membership to proving knowledge of signed messages without revealing them

Prover		**Verifier**
$m \in \Phi,\ C = Com(m)$		C
$(e.g.\ Pedersen)$		
	$\xleftarrow[(e.g.\ Boneh-Boyen\ Sign.)]{\{A_i\}}$	$A_i = Sign(i),\ \forall i \in \Phi$
$V = Blind(A_m)$	$\xrightarrow{V}$	

$$\xleftrightarrow{PK\{(m,r,z): C = g^m h^r \ \wedge\ e(V,y) = e(V,g)^{-m} e(g,g)^z\}}$$

Application to Range Proof

Use Set Membership to efficiently solve Range Proof.

Application to Range Proof

Insight

- u-ary decomposition $\left[0, u^{\ell}\right)$
  e.g. for $u = 5 \Rightarrow 334 = 2 \cdot 5^3 + 3 \cdot 5^2 + 1 \cdot 5^1 + 4 \cdot 5^0$
- Signature based Set Membership for set $\mathbb{Z}_u = \{0, 1, ..., u-1\}$

Application to Range Proof

Range Proof Protocol

Public parameters: $\Phi = \left[0, u^\ell\right)$, $C = Com(m)$ and $C_j = Com(m_j)$

Prover | **Verifier**

$m \in \Phi,\ m = \prod_{j=0}^{\ell-1} m_j u^j$

$\xleftarrow{\{A_i\}}$ $A_i = Sign(i),\ \forall i \in \mathbb{Z}_u$

$V_j = Blind(A_{m_j}),\ \forall j$ $\xrightarrow{\{V_j\}}$

$\xleftrightarrow{PK\{(m_j, r_j, z_j): C_j = g^{m_j} h^{r_j} \wedge e(V_j, y) = e(V_j, g)^{-m_j} e(g,g)^{z}_{j}\}}$

Communication Complexity

$O(u) + O(\ell) + O(\ell) \cdot O(1) = O(u + \ell)$ v.s. $O(u \cdot \ell)$

Application to Range Proof

Asymptotic Communication Complexity

- Relation to security parameter: $u^\ell \geqslant 2^{k-1}$
- Possible optimal choice for u could be $u = \dfrac{k}{\log k}$
- $Com(u, \ell) = O\left(\dfrac{k}{\log k - \log\log k}\right)$

Application to Range Proof

Practical Communication Complexity

- Concrete optimization possible in the choice of u
- Minimize $Com(u, \ell)$ under constraint $u \log^2 u = \frac{c_2 \log b}{c_1} = B$
- Vaudenay's hint: $u = \frac{B}{\log^2 u} = \frac{B}{(\log B - 2 \log \log u)^2}$

Application to Range Proof

Handling arbitrary ranges $[a, b)$

- General case (AND-composition): $u^{\ell-1} < b < u^{\ell}$
- $m \in [a, b) \Leftrightarrow m \in [a, a + u^{\ell}) \cap m \in [b - u^{\ell}, b)$
- 2 other potential optimizations
- If $b - a = u^{\ell}$, $m \in [a, b) \Leftrightarrow m - a \in [0, u^{\ell})$
- If $a + u^{\ell-1} < b$ OR-composition:
  $[a, b) = [b - u^{\ell-1}, b) \cup [a, a + u^{\ell-1})$

Application to Range Proof

Recall Bob's Example

- Bob wants to apply for IACR offer (free trip to Asiacrypt 08 for PhD candidates with $18 \leqslant age < 26$).
- Using the Unix Epoch system to encode the birth date, we obtain the following allowed range: $[347184000, 599644800)$

Application to Range Proof

Potential Example

- Communication load comparison for range proof $[347184000, 599644800)$:
- For very large ranges,
  Boudot's method wins with the strong RSA assumption
- If no RSA assumption made, our scheme performs better.
- Complexity varies with range and setup assumptions.

Scheme	*Communication Complexity*
Our new range proof	45824 bits
Boudot's method	48946 bits
Standard bit-by-bit method	96768 bits
Schoenmakers' method	50176 bits

- Further work in progress by Helger Lipmaa for general case of arbitary ranges.
- Bob can travel safely without being bothered with age anonymity
- Questions?

\end{session}