Paillier-Based Publicly Verifiable (Non-interactive) Secret Sharing

Mahabir P. Jhanwar A. Venkateswarlu Rei Safavi-Naini
Presented by Santanu Sarkar

WCC 2013
April 15-19, 2013, Bergen (Norway)

Outline of the talk

Outline of the talk

- Secret Sharing
- Publicly Verifiable Secret Sharing
- Proposed Scheme
- Efficiency Comparison

(t, n)-threshold Secret Sharing

- **Secret Sharing:**

$$s \xrightarrow{\text{Share Distribution}} s_1, s_2, \ldots, s_n \xrightarrow[\text{any } t+1 \text{ shares}]{\text{Reconstruction}} s$$

- **Privacy (Perfect) :** Any t shares will give no information about s

$$s_{i_1}, \ldots, s_{i_t} \xrightarrow{\text{unlimited computation allowed}} ?$$

Example (Shamir Secret Sharing)

- **Secret:** $s \in \mathbb{F}$.
- **Shares:** $s_1 = f(1), s_2 = f(2), \ldots, s_n = f(n)$, where $f(x) = s + a_1 x + a_2 x^2 + \cdots + a_t x^t \in \mathbb{F}[x]$.

- **Privacy** and **Reconstructability** follows from Lagrange Interpolation.

Outline of the talk

Verifiable Secret Sharing [CGMA'85]

Verifiable Secret Sharing [CGMA'85]

$$s \xrightarrow[\textit{Distribution}]{\text{Share}} \overbrace{s_1, s_2, \ldots, s_n}^{\textit{Some are wrong}} \xrightarrow[\text{every set of } t+1 \text{ shares}]{\text{Reconstruction}} \textit{need not unique secret}!!$$

Verifiable Secret Sharing [CGMA'85]

$$s \xrightarrow[\textit{Distribution}]{\text{Share}} \overbrace{s_1, s_2, \ldots, s_n}^{\textit{Some are wrong}} \xrightarrow[\text{every set of } t+1 \text{ shares}]{\text{Reconstruction}} \textit{need not unique secret}!!$$

- Extra Verification Protocol (VP) !! It takes place between $\mathcal{D}$ and $P_1, \ldots, P_n$ and satisfy the following.

Verifiable Secret Sharing [CGMA'85]

$$s \xrightarrow[\textit{Distribution}]{\text{Share}} \overbrace{s_1, s_2, \ldots, s_n}^{\textit{Some are wrong}} \xrightarrow[\text{every set of } t+1 \text{ shares}]{\text{Reconstruction}} \textit{need not unique secret!!}$$

- Extra Verification Protocol (VP) !! It takes place between $\mathcal{D}$ and $P_1, \ldots, P_n$ and satisfy the following.
  - $\mathcal{D}$ follows share distribution, VP; P_i follows VP implies P_i accepts share with probability 1.
  - For all $S_1, S_2 \subset \{P_1, \ldots, P_n\}, (|S_i| = t)$ such that $\{P_i\}_{i \in S_1}$ and $\{P_i\}_{i \in S_2}$ accepted their shares in VP, the following holds: let s_i be the secret computed by$\{P_i\}_{i \in S_i} (i = 1, 2)$, then

$$\text{Prob}[s_1 \neq s_2] \leq \text{negligible}.$$

Publicly Verifiable Secret Sharing [Sta'96]

- Extra Verification Protocol (VP) !! It takes place between $\mathcal{D}$ and $P_1, \ldots, P_n$ and satisfy the following.
  - $\mathcal{D}$ follows share distribution, VP; P_i follows VP implies P_i accepts share with probability 1.
  - For all $S_1, S_2 \subset \{P_1, \ldots, P_n\}, (|S_i| = t)$ such that $\{P_i\}_{i \in S_1}$ and $\{P_i\}_{i \in S_2}$ accepted their shares in VP, the following holds: let s_i be the secret computed by$\{P_i\}_{i \in S_i} (i = 1, 2)$, then

$$\text{Prob}[s_1 \neq s_2] \leq \text{negligible}.$$

Publicly Verifiable Secret Sharing [Sta'96]

- Extra Verification Protocol (VP) !! It takes place between $\mathcal{D}$ and $P_1, \ldots, P_n$ and satisfy the following.
  - $\mathcal{D}$ follows share distribution, VP; P_i follows VP implies P_i accepts share with probability 1.
  - For all $S_1, S_2 \subset \{P_1, \ldots, P_n\}, (|S_i| = t)$ such that $\{P_i\}_{i \in S_1}$ and $\{P_i\}_{i \in S_2}$ accepted their shares in VP, the following holds: let s_i be the secret computed by$\{P_i\}_{i \in S_i}(i = 1, 2)$, then

$$\text{Prob}[s_1 \neq s_2] \leq \text{negligible}.$$

- The verification protocol can be executed by any third party.

Publicly Verifiable Secret Sharing [Sta'96]

- Extra Verification Protocol (VP) !! It takes place between $\mathcal{D}$ and $P_1, \ldots, P_n$ and satisfy the following.
  - $\mathcal{D}$ follows share distribution, VP; P_i follows VP implies P_i accepts share with probability 1.
  - For all $S_1, S_2 \subset \{P_1, \ldots, P_n\}, (|S_i| = t)$ such that $\{P_i\}_{i \in S_1}$ and $\{P_i\}_{i \in S_2}$ accepted their shares in VP, the following holds: let s_i be the secret computed by$\{P_i\}_{i \in S_i}(i = 1, 2)$, then

$$\text{Prob}[s_1 \neq s_2] \leq \text{negligible}.$$

- The verification protocol can be executed by any third party.
- Further, we consider the Non-interactive public verification.

Publicly Verifiable Secret Sharing [Sta'96]

- Extra Verification Protocol (VP) !! It takes place between $\mathcal{D}$ and $P_1, \dots, P_n$ and satisfy the following.
  - $\mathcal{D}$ follows share distribution, VP; P_i follows VP implies P_i accepts share with probability 1.
  - For all $S_1, S_2 \subset \{P_1, \dots, P_n\}, (|S_i| = t)$ such that $\{P_i\}_{i \in S_1}$ and $\{P_i\}_{i \in S_2}$ accepted their shares in VP, the following holds: let s_i be the secret computed by$\{P_i\}_{i \in S_i}(i = 1, 2)$, then

$$\text{Prob}[s_1 \neq s_2] \leq \text{negligible}.$$

- The verification protocol can be executed by any third party.
- Further, we consider the Non-interactive public verification.

Non-interactive Publicly Verifiable Secret Sharing !!

PVSS Applications

- PVSS offers an efficient alternative in many protocols which use VSS as a subroutine.
- PVSS gives a practical solution to (t, n)-threshold VSS assuming no broadcast channel.
- Useful primitive for multi-party computation.
- Various applications to electronic voting (and its variants).
- Play important roles in key-escrow systems and threshold cryptography.

Model for PVSS [Sch'99]

1. **Distribution.**
   - Share Distribution:
     - $\mathcal{D}$ generates shares $E_i(s_i)$ of s for P_i.
     - $\mathcal{D}$ also publishes $\text{PROOF}_{\mathcal{D}}$ to show each $E_i(s_i)$ encrypts s_i.
   - Shares Verification: Any party knowing the public keys of the participants may verify the shares.
2. **Reconstruction.**
   - Shares Decryption:
     - The participants decrypt their shares s_i from $E_i(s_i)$.
     - Every P_i releases s_i plus PROOF_{P_i} to show shares are correct.
   - Share Combining: PROOF_{P_i} are used to exclude dishonest participants. Reconstruction of s by any authorized set.

Security (Proposed Scheme)

- Unconditional Verifiability.
  - For all $S_1, S_2 \subset \{P_1, \ldots, P_n\}, (|S_i| = t)$ such that $\{P_i\}_{i \in S_1}$ and $\{P_i\}_{i \in S_2}$ accepted their shares in VP, the following holds: let s_i be the secret computed by $\{P_i\}_{i \in S_i} (i = 1, 2)$, then

$$\mathrm{Prob}[s_1 \neq s_2] = 0.$$

- Privacy. (Stronger Version by Indistinguishability of Secrets)

$$\left\| \begin{array}{c} \mathcal{A} \text{ has corrupted } t-1 \text{ players} \\ (s_0, s_1) \stackrel{\$}{\leftarrow} \mathcal{A}^{\mathrm{Dist}(\cdot)} \\ \{E_i(s_{b,i})\}_{i=1}^{n} \stackrel{\$}{\leftarrow} \mathrm{Dist}(s_b);\ b \stackrel{\$}{\leftarrow} \{0,1\} \\ b' \stackrel{\$}{\leftarrow} \mathcal{A}^{\mathrm{Dist}(\cdot)}(E_i(s_{b,i})) \end{array} \right\|$$

  - $\mathrm{Adv}^{\text{SA-IND}}_{\text{PVSS},\mathcal{A}}(\mu) = \left| \mathrm{Prob}[b' = b] - \frac{1}{2} \right| \leq$ negligible.

Some Existing Constructions

Schemes	Technique	Hardness	Secret Type
✓ [Sta'96]	Discret Log based	DDH	g^s
✓ [FO'98]	RSA	Modified RSA	s
✓ [Sch'99]	Discret Log based	Diffie-Hellman	g^s
✓ [HV'08]	Pairing	DBDH	$e(g,g)^s$
✓ [RV'05]	Paillier	DCRA	s
✓ Proposed	Paillier	DCRA	s

- Discrete log (Pairing) based schemes shares the secret g^s ($e(g,g)^s$) for secret s.
- Paillier based schemes have the advantage of sharing the secret s as it is.

Outline of the talk

- Secret Sharing
- Publicly Verifiable Secret Sharing
- Proposed Scheme
- Efficiency Comparison

Preliminaries

- Let $n = pq$ be such that $\gcd(\phi(n), n) = 1$. Let $\lambda = \mathrm{lcm}(p-1, q-1)$ be Carmichael's number.
- An element $x \in \mathbb{Z}^*_{n^2}$ is said to be an n-th residue modulo n^2 if there exists $y \in \mathbb{Z}^*_{n^2}$ such that $x \equiv y^n \bmod n^2$.
- Decisional Composite Residuosity Assumption (DCRA).

  Hard distinguishing n-th residues from non n-th residues !!

Proposed Scheme (Underlying Primitives)

- Paillier's Public Key Encryption [Pai'99].

KeyGen	Enc	Dec
$n = pq, \gcd(\phi(n), n) = 1$ $\lambda = \mathrm{lcm}(p-1, q-1)$; $g \in \mathbb{Z}^*_{n^2}$ with $n \mid o(g)$ $\mathsf{pk} = (n, g)$; $\mathsf{sk} = \lambda$	Msg $M \in \mathbb{Z}_n$ $r \in_R \mathbb{Z}^*_n$ $C = g^M r^n \mod n^2$	$M = \frac{L(C^\lambda \bmod n^2)}{L(g^\lambda \bmod n^2)} \mod n$ where $L(X) = \frac{X-1}{n}$.

- Chaum-Pedersen protocol [CP'93]: interactive proof of knowledge for equality of discrete logarithms.

$$(g_1, g_2, y_1, y_2) \; ; \; y_1 = g_1^{x} \text{ and } y_2 = g_2^{x}.$$

- Fiat-Shamir technique [FS'86]: from interactive to non-interactive.

Proposed Scheme

- Underlying Useful Observations/Results
  - Let $f(x) = \sum_{k=0}^{t-1} a_k x^k$ and $\{f(j)\}_{1 \leq j \leq t}$ be t points over $f(x)$. One can get (useful observation),

$$\{g^{a_k}\}_{0 \leq k \leq t-1} \text{ from } (g, \{g^{f(j)}\}_{1 \leq j \leq t}).$$

  - Let $n = pq$, where p, q are safe primes i.e., $p = 2 \cdot p' + 1$. Provide results to check if $v \in \mathrm{QR}_{n^2}$ is a generator or not.

Lemma

v is a generator of QR_{n^2} iff $\gcd(v-1, n) = 1$ and $\gcd(v^{p'q'} - 1, n) = 1$.

Proposed Scheme

- Initialization:
  - The dealer generates $n = pq$ with $p = 2p' + 1, q = 2q' + 1$ and $\gcd(n, \phi(n)) = 1$. Set $m = p'q'$.
  - Choose $(a, b) \in_R \mathbb{Z}_n^* \times \mathbb{Z}_n^*$ and set $g = (1 + n)^a b^n \pmod{n^2}$.
  - Choose $v \in_R \mathrm{QR}_{n^2}$ and check if v is a generator of QR_{n^2}.
  - Dealer publishes (n, g, v).
  - Every P_i selects $(m_i, r_i) \in_R \mathbb{Z}_n \times \mathbb{Z}_n^*$ and publish:

    $$T_i = g^{m_i} r_i^n \pmod{n^2} \text{ and } W_i = v^{\Delta m_i} \pmod{n^2}$$

    where $\Delta = \ell!$.
  - The pair (m_i, r_i) is kept secret with P_i.

Proposed Scheme

✓ Distribution:

- Share Distribution (among ℓ players $\{P_1, \ldots, P_\ell\}$):
  - Secret is $s \in \mathbb{Z}_n$.
  - Choose $x \in_R \mathbb{Z}_n^*$ and compute $C = g^s x^n \bmod n^2$.
  - Choose $\beta \in_R \mathbb{Z}_n^*$ and set $\theta = am\beta \mod n$.
  - Compute $m_i = \frac{L(T_i^\lambda \bmod n^2)}{L(g^\lambda \bmod n^2)} \pmod n$ for $1 \le i \le \ell$.
  - Choose a $t-1$ degree polynomial $f(x) \in \mathbb{Z}_{nm}[x]$:
    $$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{t-1} x^{t-1}$$
    where $a_0 = \beta m$ and $a_i \in \mathbb{Z}_{nm}$ for $1 \le i \le t-1$.
  - Compute $C_i = C^{2\Delta f_i + 2\Delta m_i}$, where $f_i = f(i) \bmod nm$, $1 \le i \le \ell$.
  - Compute $v^{\Delta a_0}, v^{\Delta a_1}, \ldots, v^{\Delta a_{t-1}}$.
  - Finally publish: $\{\theta, C, (C_i)_{1\le i\le \ell}, (v^{\Delta a_i})_{0\le i\le t-1}\}$.

Proposed Scheme

✓ Distribution:

- Share Verification:
  - Interactive Proof: Existence of the unique f_i, $1 \leq i \leq \ell$, satisfying:

$$C_i^2 = (C^{4\Delta})^{f_i+m_i} \text{ and } v_i \cdot W_i = (v^{\Delta})^{f_i+m_i}.$$

  - Make it non-interactive using Fiat-Shamir technique.

Proposed Scheme

✓ Reconstruction:

- Share Decryption:
  - Each P_i computes $C_i' = C^{2\Delta f_i}$ from C_i by computing $C_i' = C_i \cdot (C^{2\Delta m_i})^{-1}$.
  - Each P_i release C_i' with a proof string showing the existence of unique m_i's for $1 \leq i \leq \ell$, satisfying
  $$(C_i C_i'^{-1})^2 = (C^{4\Delta})^{m_i} \text{ and } W_i = (v^{\Delta})^{m_i}.$$
- Share Combining:
  - Let there be t valid shares $\{C_i'\}_{1 \leq i \leq t}$. The secret s can be obtained as follows:

$$L\left(\prod_{i \in S} (C_i')^{2\lambda_i^S(0)} \bmod n^2\right) \times \frac{1}{4\Delta^2\theta} \bmod n = s.$$

Security

- Verifiability: Unconditional verifiability.
- Privacy:

Theorem

In the random oracle model for H and assuming the Decisional Composite Residuosity Assumption (DCRA) holds, the proposed publicly verifiable secret sharing scheme is semantically secure against static adversary.

Outline of the talk

- Secret Sharing
- Publicly Verifiable Secret Sharing
- Proposed Scheme
- Efficiency Comparison

Efficiency Comparison

Scheme	Share Distribution	Broadcast Bandwidth	Verification
1 Ruiz and Villar [05]	$\ell(t+2)+2t+1$ exps	t many $\mathbb{Z}_{n^2}$ elts + 2ℓ many $\mathbb{Z}_n$ elts	$\ell(t+1)$ exps
2 Proposed Scheme	$4\ell+t+3$ exps	$(\ell+t+2)$ many $\mathbb{Z}_{n^2}$ elts + ℓ many $\mathbb{Z}_n$ elts	$\ell(t+3)$ exps
3 Schoenmakers [99]	$3\ell+t$ exps	$(\ell+t)$ order q group elts + ℓ many $\mathbb{Z}_q$ elts	$\ell(t+3)$ exps

- 1 is the only Paillier-based PVSS. 3 is based on Pairings.
- Improvement over 1 in Share Distribution.
- Comparable to 3.

Thank You !!