Constructing Ideal Secret Sharing Schemes based on Chinese Remainder Theorem

Yu Ning, Fuyou Miao,…*

University of Science and Technology of China

Contributions

- ✓ Generalization of existing CRT-based (t,n)-SS from Integer Ring to Polynomial Ring
- ✓ Ideal (t,n)-SS based on CRT for Poly. Ring
- ✓ Shamir's (t,n)-SS : a special case
- ✓ Weighted (t,n)-SS

Outline

- (t,n)-Threshold Secret Sharing (i.e., (t,n)-SS)
- Two Typical Secret Sharing Schemes
- Secret Sharing based on Polynomial Ring over F_p
- Both Types of SS as Special Cases
- Weighted (t,n)-SS
- Conclusion

(t,n)-Threshold Secret Sharing

- t-Threshold, n- number of all shareholders
- A dealer divides a secret s into n pieces, allocates each piece to a shareholder as the share such that
  - 1) any t or more than t shares can recover the secret;
  - 2) less than t shares cannot obtain the secret;

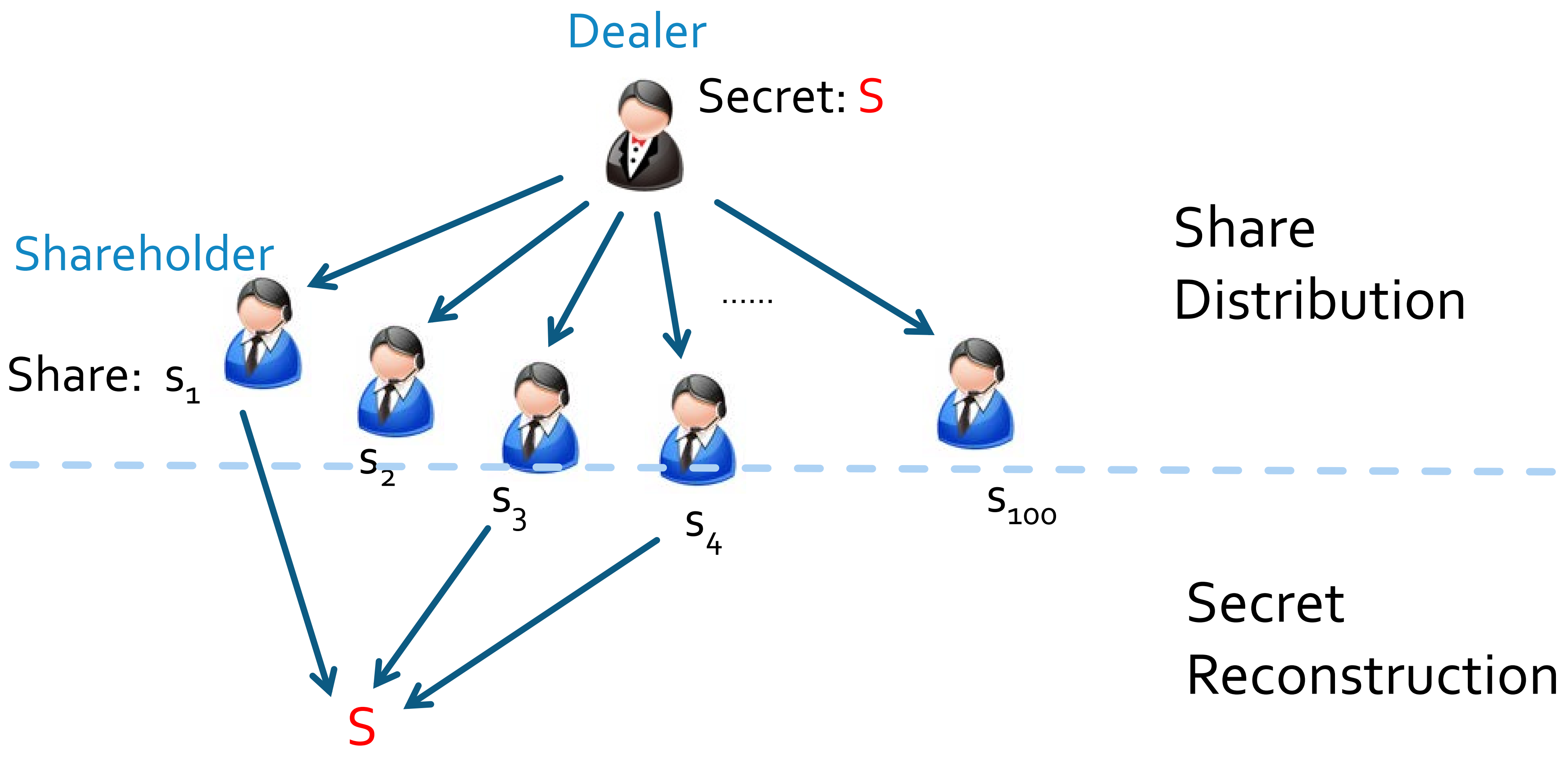


Fig 1. An example of (3,100)-SS

Applications of (t,n)-SS

- ✓ Threshold Encryption
- ✓ Threshold Signature
- ✓ Secure Multiparty Computation
- ✓ Many security-related application protocols…

2 Typical (t,n)-SSs

- Shamir's (t,n)-SS [23]*
  - *Share Distribution*
    - $f(x)=a_0+a_1x+a_2x^2+\ldots+a_{t-1}x^{t-1} \bmod p$

      Secret: $s=a_0$
    - *Each Shareholder U_i: Public information-$x_i \in F_p$, private share--$f(x_i)$*
  - *Secret Reconstruction*
    - *m （m≥t） shareholders, e.g. $\{U_1,U_2,\ldots U_m\}$, compute the secret as:*

$$s=\sum_{i=1}^{m} f(x_i)\prod_{\substack{j=1,\\ j\neq i}}^{m}\frac{x_j}{x_j-x_i} \bmod p, \qquad (m\geq t)$$

*[23] Shamir, A.: How to share a secret. Communications of the ACM **22**(11), 612-613 (1979)

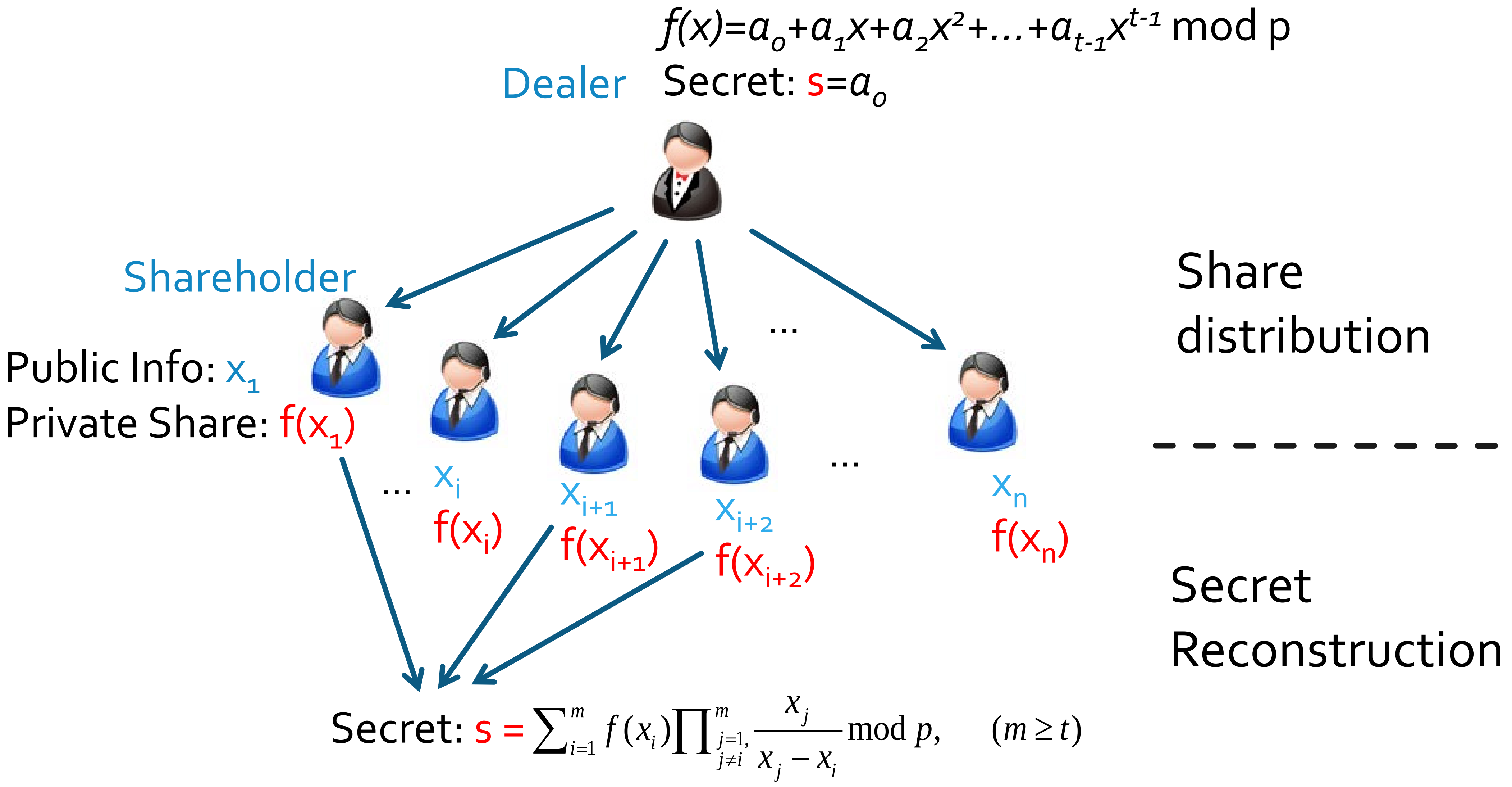


Fig 1. Shamir's (t,n)-SS

✓ Remarks

- Shamir's (t,n)-SS uses Lagrange Interpolation over finite field F_p to recover the secret.
- Ideal scheme:
  - Information rate 1;
  - No information leaks to t-1 participants
- Most popular (t,n)-SS scheme cited over 13000 times -- google scholar

2 Typical (t,n)-SS

✓ Asmuth-Bloom's (t,n)-SS[1] over 600 times of citation

- Share distribution:

secret : $s \in Z_{m_0}$, modulus of shareholder$_i$: $m_i \in Z$

$m_0 < m_1 < m_2 < \ldots < m_n, \gcd(m_i, m_j) = 1,$ (Increasing sequence, pairwise coprime)

$m_0 m_{n-t+2} \bullet \ldots \bullet m_n \le m_1 m_2 \bullet \ldots \bullet m_t \quad (*)$ (gap creation)

$B = s + \alpha m_0 < m_1 m_2 \bullet \ldots \bullet m_t$ (range extension)

$s_i = B \bmod m_i;$ (share evaluation)

[1]Asmuth, C., Bloom, J.:A modular approach to key safeguarding. IEEE transactions on information theory 29(2), 208-210 (1983)

- Secret Reconstruction

For authorized subset A, $|A| \geq t$ $\quad B = \sum_{i \in A} s_i \frac{M}{m_i} (\frac{M}{m_i})^{-1} \bmod m_i \bmod M$

secret: $s = B \bmod m_0$;

✓ Remark:

- Based on Chinese Remainder Theorem(CRT) for Integer Ring
- Not Ideal—information rate < 1
- Hard to choose moduli due to the condition

$$m_0 m_{n-t+2} \bullet \ldots \bullet m_n \leq m_1 m_2 \bullet \ldots \bullet m_t \qquad (*)$$

✓ Awkward scheme→[13-20][33]...

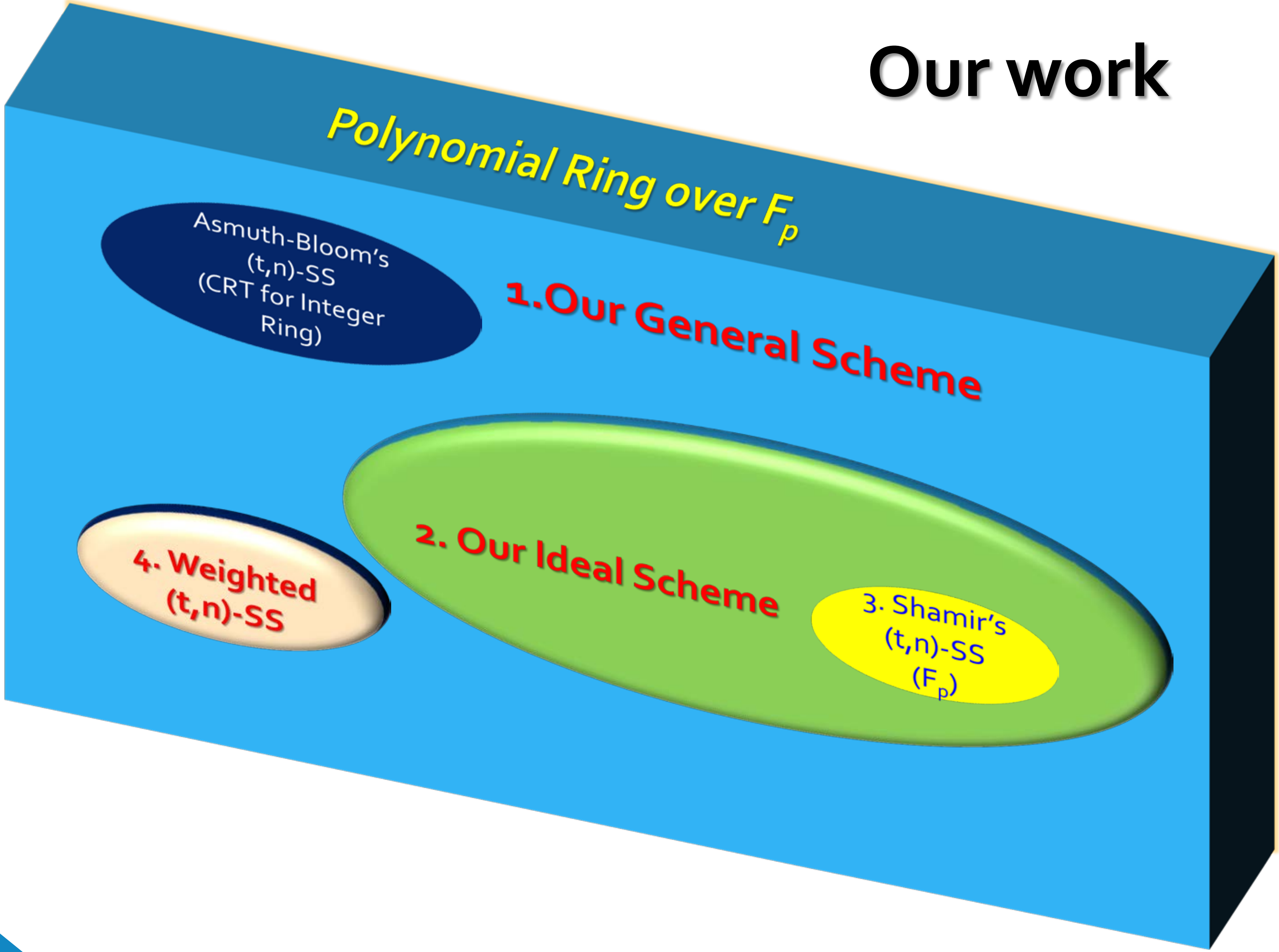
Questions

- ✓ Can we use CRT to build a (t,n)-SS as ideal as Shamir's scheme?
- ✓ What is the **connection** between **CRT based (t,n)-SSs** and **Shamir's (t,n)-SS**?

Our work

- ✓ Generalize Asmuth-Bloom's (t,n)-SS from Integer Ring to Polynomial Ring
  - ***General Scheme***
  - ***Ideal Scheme***
  - Prove Shamir's (t,n)-SS is a ***special case*** of our ***Ideal Scheme***
  - Construct a ***weighted (t,n)-SS*** from ***General Scheme***

Our work


Polynomial Ring over F_p
Asmuth-Bloom's (t,n)-SS (CRT for Integer Ring)
1.Our General Scheme
2. Our Ideal Scheme
3. Shamir's (t,n)-SS (F_p)
4. Weighted (t,n)-SS

(t,n)-SS based on CRT for Polynomial Ring over F_p

- ✓ General scheme
- ✓ Ideal scheme

Our General Scheme

✓ Setup

prime p, an integer $d_0 \geq 1$, $m_0(x) = x^{d_0}$,

pairwise coprime polynomials $m_i(x) \in F_p[x]$,

$d_i = \deg(m_i(x))$ for $i \in [0, n]$ such that

$d_0 \leq d_1 \leq d_2 \leq \ldots \leq d_n$ and $d_0 + \sum_{i=n-t+2}^{n} d_i \leq \sum_{i=1}^{t} d_i$ (*ascending sequence, gap production*)

✓ Share Distribution

The Dealer pick secret $s(x)$, $\deg(s(x)) < d_0$, random $\alpha(x)$, such that

$f(x) = s(x) + \alpha(x) m_0(x)$, $\deg(\alpha(x)) + d_0 < \sum_{i=1}^{t} d_i - 1$

share for ith shareholder:

$$s_i(x) = f(x) \bmod m_i(x)$$

Our General Scheme

✓ Secret Reconstruction

any k participants, e.g., $\{1, 2, \ldots, k\}$, $k \geq t$ recover the secret $s(x)$:

$$\begin{cases} f(x) = s_1(x) \bmod m_1(x) \\ f(x) = s_2(x) \bmod m_2(x) \\ \ldots \\ f(x) = s_k(x) \bmod m_k(x) \end{cases} \rightarrow \quad f(x), \quad \text{(by CRT for polynomial ring)}$$

$$\rightarrow \; s(x) = f(x) \bmod m_0(x)$$

Our Ideal Scheme

✓ Only Difference in Setup

prime p, an integer $d_0 \geq 1$, $m_0(x) = x^{d_0}$,

pairwise coprime polynomials $m_i(x) \in F_p[x]$,

$d_i = \deg(m_i(x))$ for $i \in [0, n]$ such that

$$d_0 = d_1 = d_2 = \ldots = d_n \text{ and } d_0 + \sum_{i=n\text{-}t+2}^{n} d_i = \sum_{i=1}^{t} d_i$$

$$d_0 \leq d_1 \leq d_2 \leq \ldots \leq d_n \text{ and } d_0 + \sum_{i=n\text{-}t+2}^{n} d_i \leq \sum_{i=1}^{t} d_i$$

(in general scheme)

Surprising Gains from Our Ideal Scheme

- ✓ Information rate=**1**, no info. leak →Ideal scheme
- ✓ Quite easy to choose pairwise coprime modulus polynomials
  - e.g. $x^{d_0}+1,\ \ x^{d_0}+2,\ldots,\ \ x^{d_0}+n$
- ✓ Shamir's (t,n)-SS as a special case

Shamir's (t,n)-SS as our special case

- ✓ An instantiation of our ideal scheme with

$$d_o=1$$

Shamir's (t,n)-SS as our special case

CRT for Polynomial Ring over F_p

$$\begin{cases} f(x) = s_1(x) \bmod m_1(x) \\ f(x) = s_2(x) \bmod m_2(x) \\ \ldots \\ f(x) = s_k(x) \bmod m_k(x) \end{cases}$$

$$\rightarrow \; s(x) = f(x) \bmod m_0(x)$$

Our Ideal scheme

Lagrange Interpolation over F_p

$$s = \sum_{i=1}^{m} f(x_i) \prod_{\substack{j=1, \\ j \neq i}}^{m} \frac{x_j}{x_j - x_i} \bmod p$$

Shamir's (t,n)-SS

x_i : Public info. of shareholder U_i

$$\text{since } f(x_i) = f(x) \bmod (x - x_i), \; m_i(x) = x - x_i \in F_p$$

(Remainder Theorem for Polynomial)

Weighted (t,n)-SS based on our General Scheme

- ✓ What is Weighted (t,n)-SS
  - Each shareholder U_i in subset A has a weight w_i ;
  - secret can be recovered if

$$\sum_{i \in A} w_i \geq t$$

Weighted (t,n)-SS based on our General Scheme

✓ More natural and easier to realize Weighted (t,n)-SS based on our scheme

$$\text{weight}=\deg(m_i(x))= w_i$$

Shareholder with weight w_i is allocated a modulus polynomial of degree w_i

Conclusions

- ✓ **General (t,n)-SS Scheme** (Poly. Ring)← Asmuth-Bloom's (t,n)-SS (Integer Ring)
- ✓ **Ideal (t,n)-SS Scheme** ← General (t,n)-SS Scheme
- ✓ Shamir's scheme as a **special case** of Ideal (t,n)-SS Scheme
- ✓ Weighted **(t,n)-SS ←** General (t,n)-SS Scheme

Conclusions

Our scheme

Potential as an alternative of both schemes


Thank You
Efharisto
Merci
Arigato
Grazie
Gracias
Danke
Cheers
Hvala
Spasiba
Toda
Obrigado
Tanmirt
Nuhun
Taiku
Kiitos
Omol
Madlobt
Ahsante
Bayarlalaa
Shukran
Tenki
Aitäh
Nandri
Köszönöm
Sobodi
Dekuji
Buznyg
Salamat
Bedankt
Supas
Dankewol
Tanemirt
Mahalo
Zikomo
Obrigada
Mèsi
Manjuthe
Takk
Barkal
Paldies
Aabar
Merkzi
Trugéré
Multumesc
Matondi
Blagodaram
Rahmat
Spas


感謝