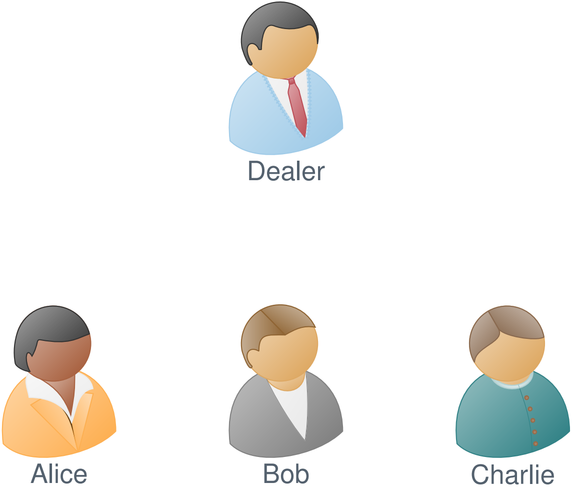
Improved Bounds on the Threshold Gap in Ramp Secret Sharing

August 6th 2019

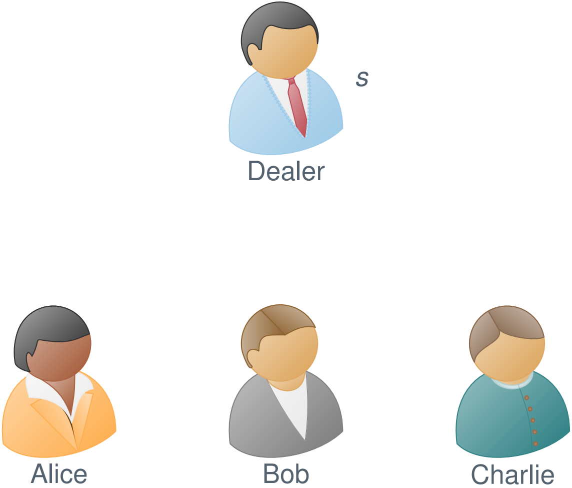
Jaron Skovsted Gundersen
(Joint work with Ignacio Cascudo and Diego Ruano)

Department of Mathematical Sciences
Aalborg University
Denmark

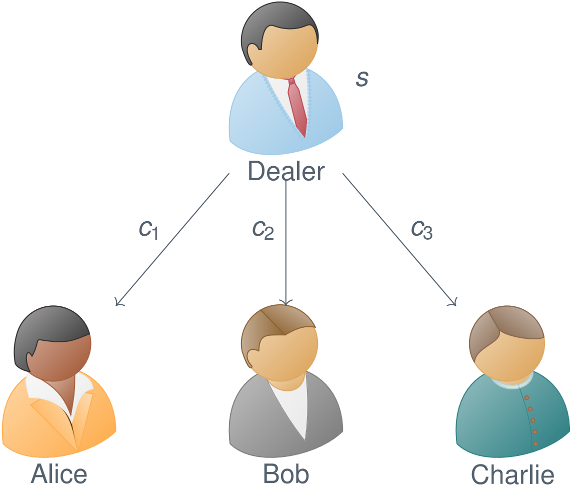
Secret Sharing – Illustrated



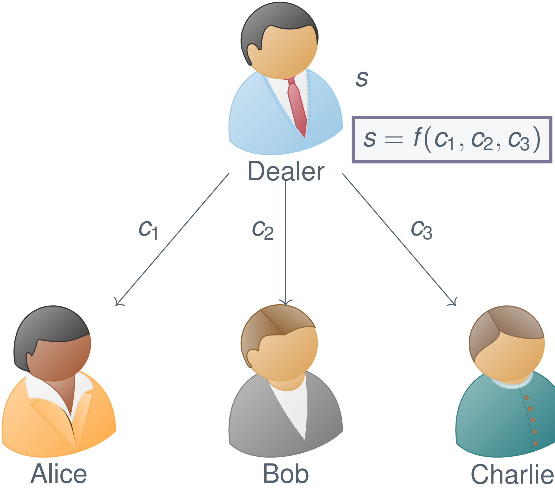
Secret Sharing – Illustrated



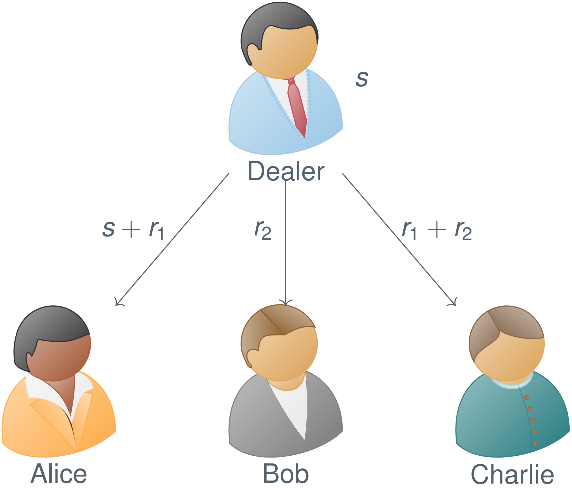
Secret Sharing – Illustrated



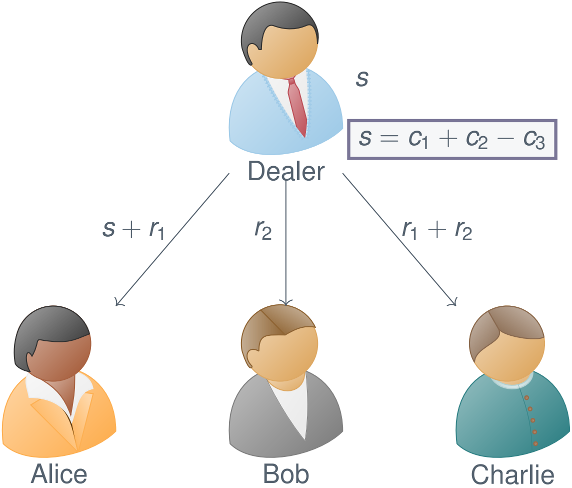
Secret Sharing – Illustrated



Secret Sharing – Example



Secret Sharing – Example



About Secret Sharing

- Invented by Shamir [Shamir, 1979] and Blakley [Blakley, 1979]
- Applications:
  - Distributed storage
  - Multiparty computation

Example of Linear Scheme

Consider the secret sharing scheme from before

- Dealer shares s and $\hat{s}$:
  - Alice holds $c_1 = s + r_1$ and $\hat{c}_1 = \hat{s} + \hat{r}_1$
  - Bob holds $c_2 = r_2$ and $\hat{c}_2 = \hat{r}_2$
  - Charlie holds $c_3 = r_1 + r_2$ and $\hat{c}_3 = \hat{r}_1 + \hat{r}_2$
- A share for $\tilde{s} = as + b\hat{s}$ can be constructed in the following way:
  - Alice computes $\tilde{c}_1 = ac_1 + b\hat{c}_1 = a(s + r_1) + b(\hat{s} + \hat{r}_1)$
  - Bob computes $\tilde{c}_2 = ac_2 + b\hat{c}_2 = ar_2 + b\hat{r}_2$
  - Charlie computes $\tilde{c}_3 = ac_3 + b\hat{c}_3 = a(r_1 + r_2) + b(\hat{r}_1 + \hat{r}_2)$
- Now $\tilde{s} = \tilde{c}_1 + \tilde{c}_2 - \tilde{c}_3$
- Linear secret sharing: Linear combination of shares results in a share corresponding to the same linear combination of secrets

Privacy and Reconstruction

- We consider ramp secret sharing: Secret $\mathbf{s} = (s_1, s_2, \ldots, s_\ell) \in \mathbb{F}_q^\ell$ and shares $c_i \in \mathbb{F}_q$
- If Alice and Bob can obtain something like $f(c_1, c_2) = s_1$ or $f(c_1, c_2) = s_1 + s_2$ then we say that they possess 1 q-bit information.
- Having m linearly independent equations yields m q-bits information
- A privacy set is a set of participants having 0 q-bits information
- A reconstructing set is a set of participants having ℓ q-bits information

Thresholds

Let $\mathcal{P}$ be the set of participants, $\mathcal{A} \subseteq 2^{\mathcal{P}}$ the set of all privacy sets and $\Gamma \subseteq 2^{\mathcal{P}}$ the sets of all reconstructing sets

- $t = \max\{m : \forall A \in 2^{\mathcal{P}} \text{ s.t. } |A| = m, A \in \mathcal{A}\}$
- $r = \min\{m : \forall A \in 2^{\mathcal{P}} \text{ s.t. } |A| = m, A \in \Gamma\}$
- Threshold gap: $g = r - t$

Ramp Secret Sharing – Goals

- A dealer, a secret $\mathbf{s} \in \mathbb{F}_q^\ell$, and n participants
- Dealer construct shares $\mathbf{c} = (c_1, c_2, \ldots, c_n) \in \mathbb{F}_q^n$
- Linearity of the scheme
- Low r, high t. That is, low g

Construction – Linear Codes

Definition (Linear Code)

Let C be a $\mathbb{F}_q$-linear subspace of $\mathbb{F}_q^n$. Then C is called a linear code

- The dimension of the code $\dim(C)$ is the dimension of the subspace
- The Hamming weight: $w(\mathbf{x}) = |\operatorname{supp}(\mathbf{x})|$
- The Hamming distance: $d(\mathbf{x}, \mathbf{y}) = w(\mathbf{x} - \mathbf{y})$
- Minimum distance: $d(C) = \min_{\mathbf{x} \neq \mathbf{y} \in C}\{d(\mathbf{x}, \mathbf{y})\} = \min_{\mathbf{x} \in C \setminus \{0\}}\{w(\mathbf{x})\}$
- $[n, k, d]_q$ code, $k = \dim(C)$ and $d = d(C)$
- Dual code: $C^{\perp} = \{\mathbf{x} \in \mathbb{F}_q^n : \langle \mathbf{x}, \mathbf{y} \rangle = 0, \forall \mathbf{y} \in C\}$
- Generator matrix: $k \times n$ matrix having a basis for C as rows

Example Linear Codes

$$G = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} \in \mathbb{F}_2^{2\times 3}, \quad H = \begin{bmatrix} 1 & 1 & 1 \end{bmatrix} \in \mathbb{F}_2^{1\times 3}$$

- G generator matrix for C, a $[3, 2, 2]_2$ code
- H generator matrix for $C^\perp$, a $[3, 1, 3]_2$ code
- $\dim(C) + \dim(C^\perp) = n$
- Originally used for error and erasure-correcting
- Encode $(m_1, m_2) \in \mathbb{F}_2^2$ using C:

$$(m_1, m_2)G = (m_1, m_2, m_1 + m_2)$$

Construction – Nested Codes

Let $C_2 \subsetneq C_1$ be $[n, k_2, d_2]_q$ and $[n, k_1, d_1]_q$ codes s.t. $\ell = k_1 - k_2$

- To share a secret $\mathbf{s} \in \mathbb{F}_q^\ell$, let $C_1 = L \oplus C_2$
- Let G_2 be a generator matrix for C_2 and $G_1 = \begin{bmatrix} G_L \\ G_2 \end{bmatrix}$ be a generator matrix for C_1
- The dealer chooses $r_1, r_2, \ldots, r_{k_2}$ at random in $\mathbb{F}_q$ and compute

$$(s_1, s_2, \ldots, s_\ell, r_1, r_2, \ldots, r_{k_2})G_1 = (c_1, c_2, \ldots, c_n)$$

- Every linear ramp scheme can be represented in this way

Relative Generalized Hamming Weights (RGHW)

- [Kurihara et al., 2012] and [Geil et al., 2014] showed that t and r are determined by the relative generalized Hamming weights defined as

$$M_i(C_1, C_2) = \min\{w_S(D) : D \subseteq C_1, D \cap C_2 = \{0\}, \dim(D) = i\}$$

- For $i = 1$:

$$M_1(C_1, C_2) = \min\{w(\mathbf{x}) : \mathbf{x} \in C_1 \text{ and } \mathbf{x} \notin C_2\}$$

- $t = M_1(C_2^\perp, C_1^\perp) - 1$
- $r = n - M_1(C_1, C_2) + 1$
- $g = n - (M_1(C_1, C_2) + M_1(C_2^\perp, C_1^\perp)) + 2$

Our Main Contribution

- The generalized Griesmer bound from [Zhuang et al., 2011]:

$$n \geq k_2 + M_i(C_1, C_2) + \sum_{j=1}^{\ell-i} \left\lceil \frac{q-1}{q^j(q^i-1)} M_i(C_1, C_2) \right\rceil \Rightarrow$$

$$n - k_1 + 1 + m \geq M_1(C_1, C_2) \left(1 + \sum_{j=1}^{m} \frac{1}{q^j} \right) \Rightarrow$$

$$n - k_1 + 1 + m \geq M_1(C_1, C_2) \left(1 + \frac{q^m - 1}{q^{m+1} - q^m} \right) \Rightarrow$$

$$M_1(C_1, C_2) \leq \frac{q^{m+1} - q^m}{q^{m+1} - 1} (n - k_1 + 1 + m),$$

where $m \in \{0, 1, \ldots, \ell - 1\}$.

Our Main Contribution

Bounds on t, r and g:

Theorem ([Cascudo et al., 2019])

Let $C_2 \subsetneq C_1$ define a linear secret sharing scheme. Then

$$t \leq \frac{q^{m+1} - q^m}{q^{m+1} - 1}(k_2 + m) - \frac{q^m - 1}{q^{m+1} - 1}$$

$$r \geq \frac{q^{m+1} - q^m}{q^{m+1} - 1}(k_1 - m) + \frac{q^m - 1}{q^{m+1} - 1}(n + 1)$$

for $m \in \{0, 1, \ldots, \ell - 1\}$ and

$$g \geq \frac{q^{m+1} - q^m}{q^{m+1} - 1}(\ell - 2m) + \frac{q^m - 1}{q^{m+1} - 1}(n + 2) =: B_{Gr}^{(m)},$$

for $m \in \{0, 1, \ldots, \ell - 1\}$.

Special Cases

- $g \geq B_{Gr}^{(m)} = \frac{q^{m+1}-q^m}{q^{m+1}-1}(\ell - 2m) + \frac{q^m-1}{q^{m+1}-1}(n+2)$
- $B_{Gr}^{(0)} = \ell$
- $B_{Gr}^{(1)} = \frac{q}{q+1}(\ell - 2) + \frac{n+2}{q+1}$

Bounds from Literature

- Other bounds:

$$g \geq \ell =: B_{Sin} = B_{Gr}^{(0)},$$

see for instance [Blundo et al., 1993], and

$$g \geq \frac{n+2}{2q-1} =: B_{CCX_1} \quad \text{if } 1 \leq t < r \leq n-1$$

$$g \geq \frac{2q}{2q+1}(\ell - 1) + \frac{n+2}{2q+1} =: B_{CCX_2} \quad \text{if } \ell \geq 2$$

both from [Cascudo et al., 2013].

- For $\ell \geq 2$
  - $B_{Gr}^{(1)} \geq B_{CCX_1}$
  - $B_{Gr}^{(0)} \geq B_{CCX_2}$ when $\ell \geq n - 2(q-1)$
  - $B_{Gr}^{(1)} \geq B_{CCX_2}$ when $\ell \leq n - 2(q-1)$

Example

Let $q = 2$, $n = 100$, and $\ell = 10$. Then

	B_{Sin}	B_{CCX_1}	B_{CCX_2}	$B_{Gr}^{(1)}$	$B_{Gr}^{(4)}$
$g \geq$	10	34	28	40	51

Let $q = 7$, $n = 1000$, and $\ell = 20$. Then

	B_{Sin}	B_{CCX_1}	B_{CCX_2}	$B_{Gr}^{(1)}$	$B_{Gr}^{(3)}$
$g \geq$	20	78	85	141	155

Conclusion

- A new family of bounds improving on existing bounds for ramp secret sharing when $\ell \geq 2$
- One bound for each m
- In [Cascudo et al., 2019] we considered partial thresholds and the bounds asymptotically as well

References

[Blakley, 1979] Blakley, G. R. (1979).
Safeguarding cryptographic keys.
Managing Requirements Knowledge, International Workshop on, 00:313.

[Blundo et al., 1993] Blundo, C., Santis, A. D., and Vaccaro, U. (1993).
Efficient sharing of many secrets.
Proceedings of the 10th Annual Symposium on Theoretical Aspects of Computer Science, pages 692–703.

[Cascudo et al., 2013] Cascudo, I., Cramer, R., and Xing, C. (2013).
Bounds on the threshold gap in secret sharing and its applications.
IEEE Transactions on Information Theory, 59(9):5600–5612.

[Cascudo et al., 2019] Cascudo, I., Gundersen, J. S., and Ruano, D. (2019).
Improved bounds on the threshold gap in ramp secret sharing.
IEEE Transactions on Information Theory, 65(7):4620–4633.

[Geil et al., 2014] Geil, O., Martin, S., Matsumoto, R., Ruano, D., and Luo, Y. (2014).
Relative generalized hamming weights of one-point algebraic geometric codes.
IEEE Transactions on Information Theory, 60(10):5938–5949.

[Kurihara et al., 2012] Kurihara, J., Uyematsu, T., and Matsumoto, R. (2012).
Secret sharing schemes based on linear codes can be precisely characterized by the relative generalized hamming weight.
IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 95(11):2067–2075.

[Shamir, 1979] Shamir, A. (1979).
How to share a secret.
Commun. ACM, 22(11):612–613.

[Zhuang et al., 2011] Zhuang, Z., Luo, Y., Vinck, A. J. H., and Dai, B. (2011).
Some new bounds on relative generalized hamming weight.
2011 IEEE 13th International Conference on Communication Technology, pages 971–974.