Separating Sources for Encryption and Secret Sharing

Yevgeniy Dodis
NYU

Krzysztof Pietrzak
ENS Paris

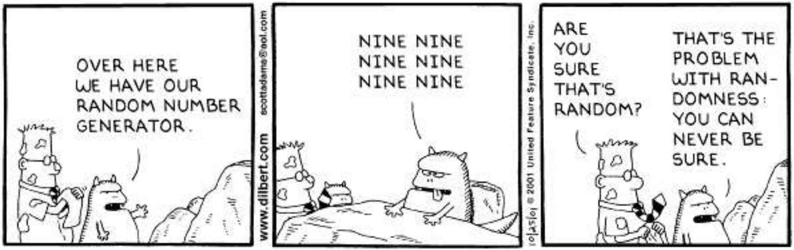
Bartosz Przydatek
ETH Zurich

Introduction

- Randomness is essential, not only in cryptography

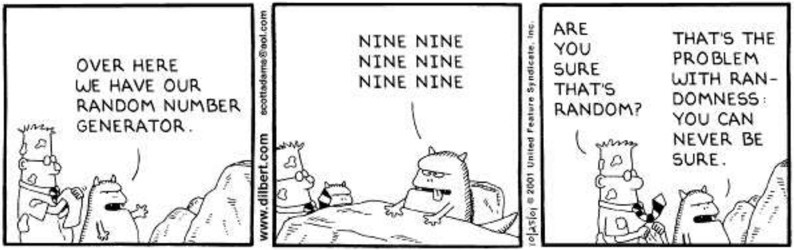
Introduction

- Randomness is essential, not only in cryptography
- Perfect random bits not always available



Introduction

- Randomness is essential, not only in cryptography
- Perfect random bits not always available



$\Rightarrow$ characterize randomness necessary/sufficient for concrete tasks

Imperfect Sources

- Random source: a set of distributions over some set $\mathcal{X}$

Imperfect Sources

- Random source: a set of distributions over some set $\mathcal{X}$
- d-weak sources: distributions with min-entropy $\geq d$
  $\Rightarrow$ no value appears with prob. greater than $1/2^d$

Imperfect Sources

- Random source: a set of distributions over some set $\mathcal{X}$
- d-weak sources: distributions with min-entropy $\geq d$

  $\Rightarrow$ no value appears with prob. greater than $1/2^d$
- Cryptographic sources:

  $\Rightarrow$ sufficient for specific cryptographic application

Imperfect Sources

- Random source: a set of distributions over some set $\mathcal{X}$
- d-weak sources: distributions with min-entropy $\geq d$

  $\Rightarrow$ no value appears with prob. greater than $1/2^d$
- Cryptographic sources:

  $\Rightarrow$ sufficient for specific cryptographic application

- extremely weak sources are sufficient for BPP [ACRT'99]

Imperfect Sources

- Random source: a set of distributions over some set $\mathcal{X}$
- d-weak sources: distributions with min-entropy $\geq d$

  $\Rightarrow$ no value appears with prob. greater than $1/2^d$
- Cryptographic sources:

  $\Rightarrow$ sufficient for specific cryptographic application

- extremely weak sources are sufficient for BPP [ACRT'99]
- $(n/2 + \tau)$-weak sources over $\{0,1\}^n$ are sufficient for authentication [MW'97]

Separating sources

- $(n/2 - \epsilon)$-weak sources over $\{0, 1\}^n$ are **not** sufficient for authentication [DS'02]

Separating sources

- $(n/2 - \epsilon)$-weak sources over $\{0,1\}^n$ are **not** sufficient for authentication [DS'02]
- $(n-1)$-weak sources over $\{0,1\}^n$ are **not** sufficient for encryption [MP'90] or extraction

Separating sources

- $(n/2-\epsilon)$-weak sources over $\{0,1\}^n$ are **not** sufficient for authentication [DS'02]
- $(n-1)$-weak sources over $\{0,1\}^n$ are **not** sufficient for encryption [MP'90] or extraction
- there exist sources allowing perfect encryption but **not** extraction [DS'02]

Separating sources

- $(n/2 - \epsilon)$-weak sources over $\{0,1\}^n$ are **not** sufficient for authentication [DS'02]
- $(n-1)$-weak sources over $\{0,1\}^n$ are **not** sufficient for encryption [MP'90] or extraction
- there exist sources allowing perfect encryption but **not** extraction [DS'02]

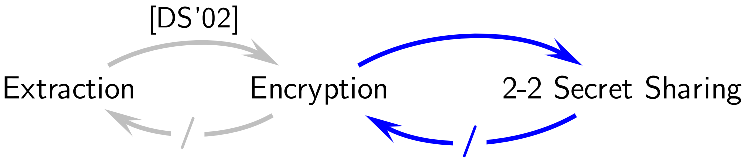
$\Rightarrow$ Entropy not enough for 1-bit encryption, but perfect randomness not necessary as well!

Separating sources

- $(n/2 - \epsilon)$-weak sources over $\{0,1\}^n$ are **not** sufficient for authentication [DS'02]
- $(n-1)$-weak sources over $\{0,1\}^n$ are **not** sufficient for encryption [MP'90] or extraction
- there exist sources allowing perfect encryption but **not** extraction [DS'02]

$\Rightarrow$ Entropy not enough for 1-bit encryption, but perfect randomness not necessary as well!

This work: compare sources for secret sharing and encryption of 1 bit



Outline

- More formal statement of the results
- Encryption $\longrightarrow$ 2-2 Secret Sharing
- 2-2 Secret Sharing $\not\longrightarrow$ Encryption
- 2-2 Secret Sharing $\longrightarrow$ $(1/2)$-Encryption
- Computational aspects of separation
- Open problems
- Conclusions

δ-encryption with source $\mathscr{S}$

$$\mathrm{Enc}\colon \mathcal{K} \times \mathcal{M} \to \mathcal{C}, \;\; \mathrm{Dec}\colon \mathcal{K} \times \mathcal{C} \to \mathcal{M}, \; \mathcal{M} = \{0, 1\}$$

δ-encryption with source $\mathscr{S}$

$$\mathsf{Enc}\colon \mathcal{K} \times \mathcal{M} \to \mathcal{C}, \;\; \mathsf{Dec}\colon \mathcal{K} \times \mathcal{C} \to \mathcal{M}, \; \mathcal{M} = \{0,1\}, \text{ such that}$$

$$\forall k \in \mathcal{K}, m \in \mathcal{M} : \;\; \mathsf{Dec}_k(\mathsf{Enc}_k(m)) = m$$

δ-encryption with source $\mathscr{S}$

$$\mathrm{Enc}\colon \mathcal{K} \times \mathcal{M} \to \mathcal{C}, \quad \mathrm{Dec}\colon \mathcal{K} \times \mathcal{C} \to \mathcal{M},\ \mathcal{M} = \{0,1\}, \text{ such that}$$

$$\forall k \in \mathcal{K}, m \in \mathcal{M} : \ \mathrm{Dec}_k(\mathrm{Enc}_k(m)) = m$$

statistical distance of encryptions of 0 & 1 is at most δ

$$\max_{\Omega \in \mathscr{S}} \frac{1}{2} \sum_{c \in \mathcal{C}} \left| \Pr_{k \in_\Omega \mathcal{K}}[\mathrm{Enc}_k(0) = c] - \Pr_{k \in_\Omega \mathcal{K}}[\mathrm{Enc}_k(1) = c] \right| \leq \delta$$

δ-encryption with source $\mathscr{S}$

$$\mathrm{Enc}\colon \mathcal{K} \times \mathcal{M} \to \mathcal{C}, \;\; \mathrm{Dec}\colon \mathcal{K} \times \mathcal{C} \to \mathcal{M},\; \mathcal{M} = \{0,1\}, \text{ such that}$$

$$\forall k \in \mathcal{K}, m \in \mathcal{M} : \; \mathrm{Dec}_k(\mathrm{Enc}_k(m)) = m$$

statistical distance of encryptions of 0 & 1 is at most δ

$$\max_{\Omega \in \mathscr{S}} \frac{1}{2} \sum_{c \in \mathcal{C}} \left| \Pr_{k \in_\Omega \mathcal{K}}[\mathrm{Enc}_k(0) = c] - \Pr_{k \in_\Omega \mathcal{K}}[\mathrm{Enc}_k(1) = c] \right| \leq \delta$$

$\Rightarrow$ 0-encryption $\equiv$ perfect encryption

$\Rightarrow$ 1-encryption $\equiv$ identity (no encryption)

2-2 Secret Sharing with source $\mathscr{S}$

$$\text{Share}\colon \mathcal{K} \times \mathcal{M} \to \mathcal{X}^2, \quad \text{Rec}\colon \mathcal{X}^2 \to \mathcal{M},\ \mathcal{M} = \{0, 1\}$$

2-2 Secret Sharing with source $\mathscr{S}$

$$\text{Share}\colon \mathcal{K} \times \mathcal{M} \to \mathcal{X}^2, \quad \text{Rec}\colon \mathcal{X}^2 \to \mathcal{M},\ \mathcal{M} = \{0,1\},\ \text{such that}$$

$$\forall\ k \in \mathcal{K},\ m \in \mathcal{M} :\ \text{Rec}(\text{Share}_k(m)) = m$$

2-2 Secret Sharing with source $\mathscr{S}$

$$\text{Share}\colon \mathcal{K} \times \mathcal{M} \to \mathcal{X}^2, \quad \text{Rec}\colon \mathcal{X}^2 \to \mathcal{M},\ \mathcal{M} = \{0,1\}, \text{ such that}$$

$$\forall\ k \in \mathcal{K},\ m \in \mathcal{M} :\ \text{Rec}(\text{Share}_k(m)) = m$$

perfect secrecy: $\forall\ \Omega \in \mathscr{S},\ K \in_\Omega \mathcal{K},\ (S_1, S_2) \leftarrow \text{Share}_K(M)$

$$H(M \mid S_i) = H(M)$$

Encryption $\longrightarrow$ 2-2 Secret Sharing

Given

$$\mathsf{Enc}\colon \mathcal{K} \times \mathcal{M} \to \mathcal{C} \qquad \mathsf{Dec}\colon \mathcal{K} \times \mathcal{C} \to \mathcal{M}$$

define

$$\begin{aligned} \mathsf{Share}_k(m) &\longrightarrow (k, \mathsf{Enc}_k(m)) \\ \mathsf{Rec}(s_1, s_2) &\longrightarrow \mathsf{Dec}_{s_1}(s_2) \end{aligned}$$

2-2 Secret Sharing $\not\to$ Encryption

Theorem

1. There exist sources which allow for perfect 2-2 secret sharing, but do not allow for δ-encryption for any $\delta < 1/3$.

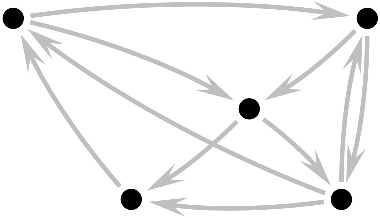
2-2 Secret Sharing $\not\to$ Encryption

Theorem

1. There exist sources which allow for perfect 2-2 secret sharing, but do not allow for δ-encryption for any $\delta < 1/3$.
2. Any source which allows for perfect 2-2 secret sharing allows for $(1/2)$-encryption.

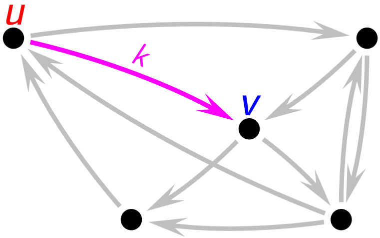
Graph Representation: 1-bit encryption [DS'02]

- nodes $\equiv$ ciphertexts, edges $\equiv$ keys



Graph Representation: 1-bit encryption [DS'02]

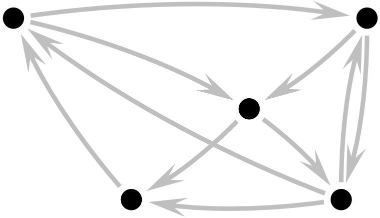
- nodes $\equiv$ ciphertexts, edges $\equiv$ keys



- for a key $k \in \mathcal{K}$: $\mathrm{Enc}_k(0) = u$, $\mathrm{Enc}_k(1) = v$

Graph Representation: 1-bit encryption [DS'02]

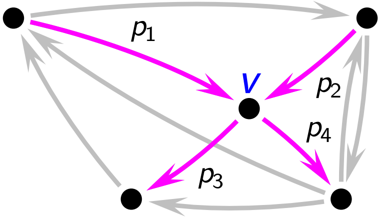
- nodes $\equiv$ ciphertexts, edges $\equiv$ keys



- distribution on $\mathcal{K} \equiv$ weights on edges

Graph Representation: 1-bit encryption [DS'02]

- nodes $\equiv$ ciphertexts, edges $\equiv$ keys



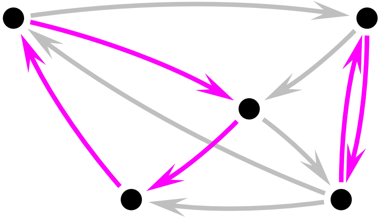
- **perfect encryption** under distribution Ω:

$$\forall v : \text{weighted in-flow}(v) = \text{weighted out-flow}(v)$$

$$p_1 + p_2 = p_3 + p_4$$

Graph Representation: 1-bit encryption [DS'02]

- nodes $\equiv$ ciphertexts, edges $\equiv$ keys



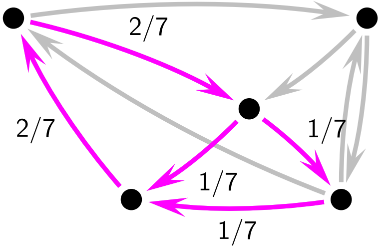
- **perfect encryption** under distribution Ω:

$$\forall v : \text{weighted in-flow}(v) = \text{weighted out-flow}(v)$$

$\Rightarrow$ Ω forms a **circulation**

Graph Representation: 1-bit encryption [DS'02]

- nodes $\equiv$ ciphertexts, edges $\equiv$ keys



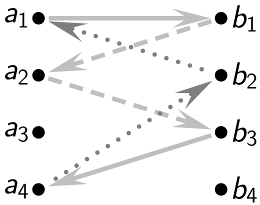
- **perfect encryption** under distribution Ω:

$$\forall v : \text{weighted in-flow}(v) = \text{weighted out-flow}(v)$$

$\Rightarrow$ Ω forms a **circulation**

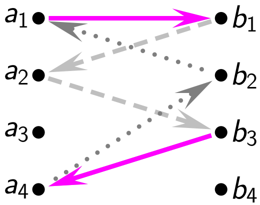
Graph Representation: 2-2 secret sharing

- nodes $\equiv$ shares, **edge-pairs** $\equiv$ randomness



Graph Representation: 2-2 secret sharing

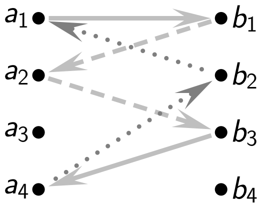
- nodes $\equiv$ shares, **edge-pairs** $\equiv$ randomness



- for randomness $k \in \mathcal{K}$:
  $\mathsf{Share}_k(0) = (a_1, b_1)$, $\quad \mathsf{Share}_k(1) = (a_3, b_4)$

Graph Representation: 2-2 secret sharing

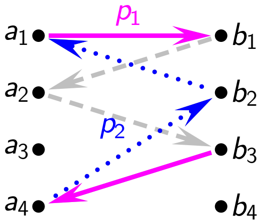
- nodes $\equiv$ shares, **edge-pairs** $\equiv$ randomness



- distribution on $\mathcal{K}$ $\equiv$ weights on edge-pairs

Graph Representation: 2-2 secret sharing

- nodes $\equiv$ shares, **edge-pairs** $\equiv$ randomness



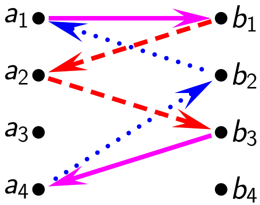
- **perfect secret sharing** under distribution Ω:

$$\forall v : \text{weighted in-flow}(v) = \text{weighted out-flow}(v)$$

$$\text{in } a_1\text{: } p_1 = p_2$$

Graph Representation: 2-2 secret sharing

- nodes $\equiv$ shares, **edge-pairs** $\equiv$ randomness



- **perfect secret sharing** under distribution Ω:

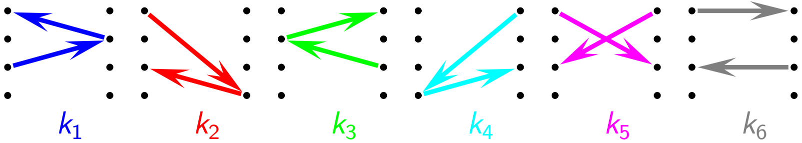
$$\forall v : \text{weighted in-flow}(v) = \text{weighted out-flow}(v)$$

$\Rightarrow$ Ω forms a **circulation**

2-2 Secret Sharing $\not\to$ Encryption (proof)

a source $\mathscr{S} = \{\Omega_1, \ldots, \Omega_4\}$ good for sharing:

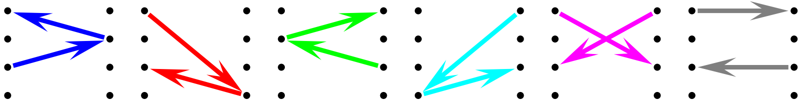
$\Rightarrow$ 6 keys, $\mathcal{K} = \{k_1, \ldots, k_6\}$:



2-2 Secret Sharing $\not\to$ Encryption (proof)

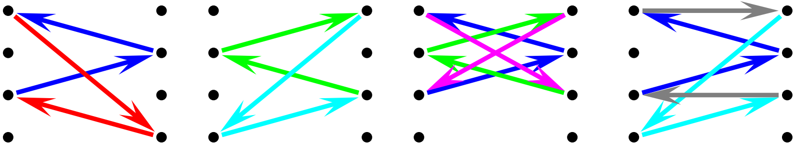
a source $\mathscr{S} = \{\Omega_1, \ldots, \Omega_4\}$ good for sharing:

$\Rightarrow$ 6 keys, $\mathcal{K} = \{k_1, \ldots, k_6\}$:



k_1 k_2 k_3 k_4 k_5 k_6

$\Rightarrow$ 4 distributions (Ω_i uniform on $\mathcal{S}_i$):



$\mathcal{S}_1 = \{k_1, k_2\}$ $\mathcal{S}_2 = \{k_3, k_4\}$ $\mathcal{S}_3 = \{k_1, k_3, k_5\}$ $\mathcal{S}_4 = \{k_1, k_4, k_6\}$

2-2 Secret Sharing $\not\to$ Encryption (cont.)

$\mathscr{S}$ is good for sharing ... but bad for encryption!

- $G = (V, E)$ — hypothetical encryption graph
  E labeled with elements of $\mathcal{K} = \{k_1, \ldots, k_6\}$

2-2 Secret Sharing $\not\to$ Encryption (cont.)

$\mathscr{S}$ is good for sharing ... but bad for encryption!

- $G = (V, E)$ — hypothetical encryption graph
  E labeled with elements of $\mathcal{K} = \{k_1, \ldots, k_6\}$
- **perfect encryption**:
  $\forall i = 1..4$, Ω_i forms a cycle in G

2-2 Secret Sharing $\not\to$ Encryption (cont.)

$\mathscr{S}$ is good for sharing ... but bad for encryption!

- $G = (V, E)$ — hypothetical encryption graph
  E labeled with elements of $\mathcal{K} = \{k_1, \ldots, k_6\}$
- **perfect encryption**:
  $\forall i = 1..4$, Ω_i forms a cycle in G
- will show:
  for at least one $\mathcal{S}_i$ edges $E(\mathcal{S}_i)$ do not form a cycle

2-2 Secret Sharing $\not\to$ Encryption (cont.)

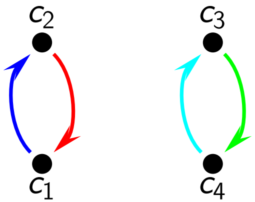
$$\mathcal{S}_1\colon\{k_1, k_2\},\ \mathcal{S}_2\colon\{k_3, k_4\},\ \mathcal{S}_3\colon\{k_1, k_3, k_5\},\ \mathcal{S}_4\colon\{k_1, k_4, k_6\}$$

- assume for each $\mathcal{S}_i$ edges $E(\mathcal{S}_i)$ forms a cycle

2-2 Secret Sharing $\not\to$ Encryption (cont.)

$\mathcal{S}_1 \colon \{k_1, k_2\},\ \mathcal{S}_2 \colon \{k_3, k_4\},\ \mathcal{S}_3 \colon \{k_1, k_3, k_5\},\ \mathcal{S}_4 \colon \{k_1, k_4, k_6\}$

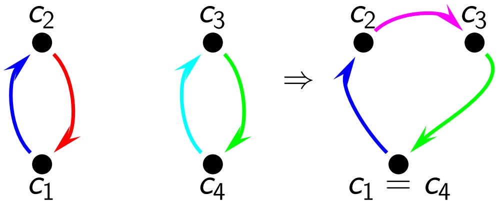
- assume for each $\mathcal{S}_i$ edges $E(\mathcal{S}_i)$ forms a cycle



2-2 Secret Sharing $\not\to$ Encryption (cont.)

$$\mathcal{S}_1\colon\{k_1, k_2\},\ \mathcal{S}_2\colon\{k_3, k_4\},\ \mathcal{S}_3\colon\{k_1, k_3, k_5\},\ \mathcal{S}_4\colon\{k_1, k_4, k_6\}$$

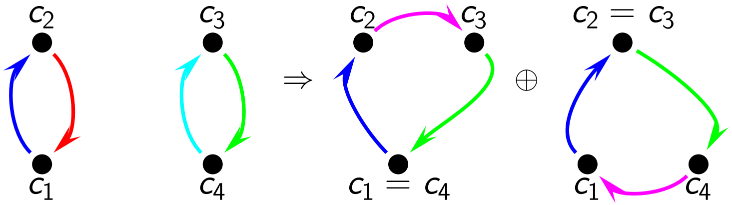
- assume for each $\mathcal{S}_i$ edges $E(\mathcal{S}_i)$ forms a cycle



2-2 Secret Sharing $\not\to$ Encryption (cont.)

$$\mathcal{S}_1\colon\{k_1, k_2\},\ \mathcal{S}_2\colon\{k_3, k_4\},\ \mathcal{S}_3\colon\{k_1, k_3, k_5\},\ \mathcal{S}_4\colon\{k_1, k_4, k_6\}$$

- assume for each $\mathcal{S}_i$ edges $E(\mathcal{S}_i)$ forms a cycle

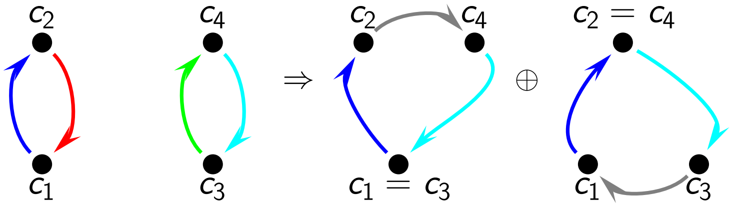


$$(c_1 = c_4 \ \oplus \ c_2 = c_3)$$

2-2 Secret Sharing $\not\to$ Encryption (cont.)

$$\mathcal{S}_1\colon\{k_1, k_2\},\ \mathcal{S}_2\colon\{k_3, k_4\},\ \mathcal{S}_3\colon\{k_1, k_3, k_5\},\ \mathcal{S}_4\colon\{k_1, k_4, k_6\}$$

- assume for each $\mathcal{S}_i$ edges $E(\mathcal{S}_i)$ forms a cycle

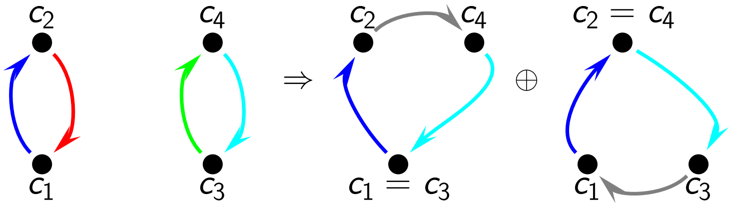


$$(c_1 = c_4 \ \oplus\ c_2 = c_3)$$

2-2 Secret Sharing $\not\to$ Encryption (cont.)

$$\mathcal{S}_1\colon\{k_1, k_2\},\ \mathcal{S}_2\colon\{k_3, k_4\},\ \mathcal{S}_3\colon\{k_1, k_3, k_5\},\ \mathcal{S}_4\colon\{k_1, k_4, k_6\}$$

- assume for each $\mathcal{S}_i$ edges $E(\mathcal{S}_i)$ forms a cycle

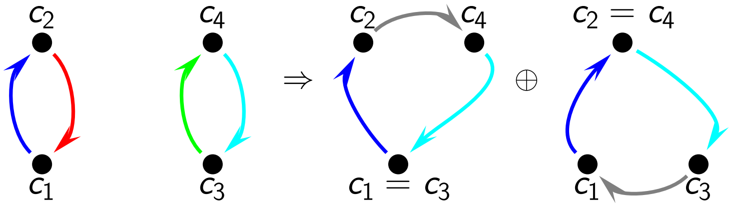


$$(c_1 = c_4 \ \oplus \ c_2 = c_3) \text{ and } (c_1 = c_3 \ \oplus \ c_2 = c_4)$$

2-2 Secret Sharing $\not\rightarrow$ Encryption (cont.)

$$\mathcal{S}_1\colon\{k_1, k_2\},\ \mathcal{S}_2\colon\{k_3, k_4\},\ \mathcal{S}_3\colon\{k_1, k_3, k_5\},\ \mathcal{S}_4\colon\{k_1, k_4, k_6\}$$

- assume for each $\mathcal{S}_i$ edges $E(\mathcal{S}_i)$ forms a cycle



$$(c_1 = c_4 \ \oplus\ c_2 = c_3) \text{ and } (c_1 = c_3 \ \oplus\ c_2 = c_4)$$

$\Rightarrow$ Contradiction!

2-2 Secret Sharing $\not\to$ Encryption (cont.)

- take Ω_i such that $E(\mathcal{S}_i)$ don't form a cycle

2-2 Secret Sharing $\not\to$ Encryption (cont.)

- take Ω_i such that $E(\mathcal{S}_i)$ don't form a cycle
- since $|\mathcal{S}_i| \leq 3$ we get

$$\frac{1}{2}\sum_{c\in\mathcal{C}}\left|\Pr_{k\in_{\Omega_i}\mathcal{K}}[\mathrm{Enc}_k(0)=c] - \Pr_{k\in_{\Omega_i}\mathcal{K}}[\mathrm{Enc}_k(1)=c]\right| \geq \frac{1}{3}$$

2-2 Secret Sharing $\not\to$ Encryption (cont.)

- take Ω_i such that $E(\mathcal{S}_i)$ don't form a cycle
- since $|\mathcal{S}_i| \leq 3$ we get

$$\frac{1}{2}\sum_{c\in\mathcal{C}} \left| \Pr_{k\in_{\Omega_i}\mathcal{K}}[\mathsf{Enc}_k(0)=c] - \Pr_{k\in_{\Omega_i}\mathcal{K}}[\mathsf{Enc}_k(1)=c] \right| \geq \frac{1}{3}$$

- there is no δ-encryption for $\mathscr{S}$ with $\delta < 1/3$. $\square$

2-2 Secret Sharing $\not\to$ Encryption (cont.)

- take Ω_i such that $E(\mathcal{S}_i)$ don't form a cycle
- since $|\mathcal{S}_i| \leq 3$ we get

$$\frac{1}{2}\sum_{c\in\mathcal{C}}\left|\Pr_{k\in_{\Omega_i}\mathcal{K}}[\mathsf{Enc}_k(0)=c] - \Pr_{k\in_{\Omega_i}\mathcal{K}}[\mathsf{Enc}_k(1)=c]\right| \geq \frac{1}{3}$$

- there is no δ-encryption for $\mathscr{S}$ with $\delta < 1/3$. $\square$

$\Rightarrow$ Theorem holds also for high min-entropy sources.

2-2 Secret Sharing $\longrightarrow$ (1/2)-Encryption

Given

$$\mathsf{Share}\colon \mathcal{K} \times \mathcal{M} \to \mathcal{X}^2, \qquad \mathsf{Rec}\colon \mathcal{X}^2 \to \mathcal{M}$$

let

$$(a_{m,k}\,, b_{m,k}) \leftarrow \mathsf{Share}_k(m) \ .$$

2-2 Secret Sharing $\rightarrow$ (1/2)-Encryption

Given

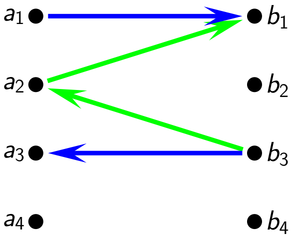
$$\mathsf{Share}\colon \mathcal{K} \times \mathcal{M} \rightarrow \mathcal{X}^2, \qquad \mathsf{Rec}\colon \mathcal{X}^2 \rightarrow \mathcal{M}$$

let

$$(a_{m,k}\,,\, b_{m,k}) \leftarrow \mathsf{Share}_k(m)\ .$$

Define

$$\mathsf{Enc}_k(m) = \begin{cases} a_{m,k} & \text{if } a_{0,k} \neq a_{1,k} \\ b_{m,k} & \text{otherwise} \end{cases}$$



Computational aspects of separation

Some efficiency requirements:

(i) the secret sharing is **efficient**

Computational aspects of separation

Some efficiency requirements:

(i) the secret sharing is **efficient**

(ii) for every δ-encryption scheme the source contains an **efficiently samplable** distribution breaking the encryption

Computational aspects of separation

Some efficiency requirements:

(i) the secret sharing is **efficient**

(ii) for every δ-encryption scheme the source contains an **efficiently samplable** distribution breaking the encryption

(iii) there exists an **efficient** algorithm breaking the encryption under distribution from (ii)

Computational aspects of separation

Some efficiency requirements:

(i) the secret sharing is **efficient**

(ii) for every δ-encryption scheme the source contains an **efficiently samplable** distribution breaking the encryption

(iii) there exists an **efficient** algorithm breaking the encryption under distribution from (ii)

(iv) distribution from (ii) can be found **efficiently**

Computational aspects of separation

Some efficiency requirements:

(i) the secret sharing is **efficient**

(ii) for every δ-encryption scheme the source contains an **efficiently samplable** distribution breaking the encryption

(iii) there exists an **efficient** algorithm breaking the encryption under distribution from (ii)

(iv) distribution from (ii) can be found **efficiently**

$\Rightarrow$ Can extend our separation to satisfy (i)-(iv) simultaneously!

Open problems

- Separations for larger domains

  $\Rightarrow$ open even for $\mathcal{M} = \{0, 1, 2\}$!

Open problems

- Separations for larger domains

  $\Rightarrow$ open even for $\mathcal{M} = \{0, 1, 2\}$!

- Sources for other cryptographic primitives

  $\Rightarrow$ position authentication wrt. encryption or sharing

Conclusions

- Separation between 2-2 secret sharing and encryption . . .

Conclusions

- Separation between 2-2 secret sharing and encryption . . .
- . . . but not as strong as between encryption and extraction.

Conclusions

- Separation between 2-2 secret sharing and encryption ...
- ... but not as strong as between encryption and extraction.
- Many interesting open problems.