Oblivious Transfer and Linear Functions

Ivan Damgård, Louis Salvail, Christian Schaffner
(BRICS, University of Aarhus, Denmark)

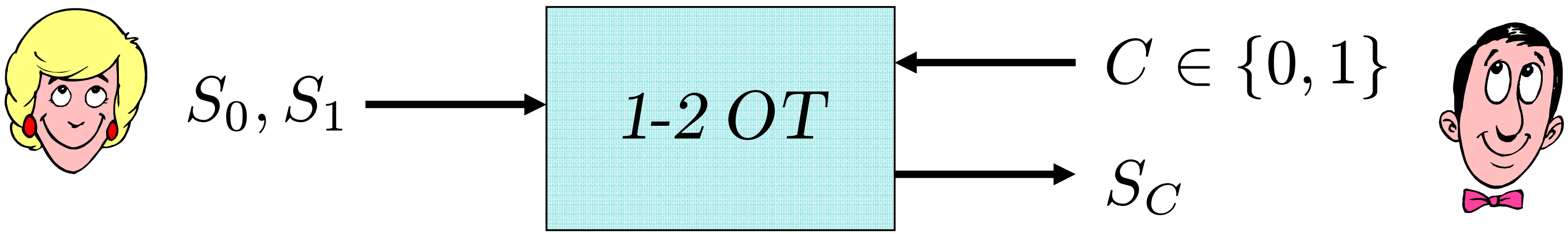
Serge Fehr (CWI Amsterdam, The Netherlands)

CRYPTO 2006, Santa Barbara
Wednesday, August 23, 2006

Agenda

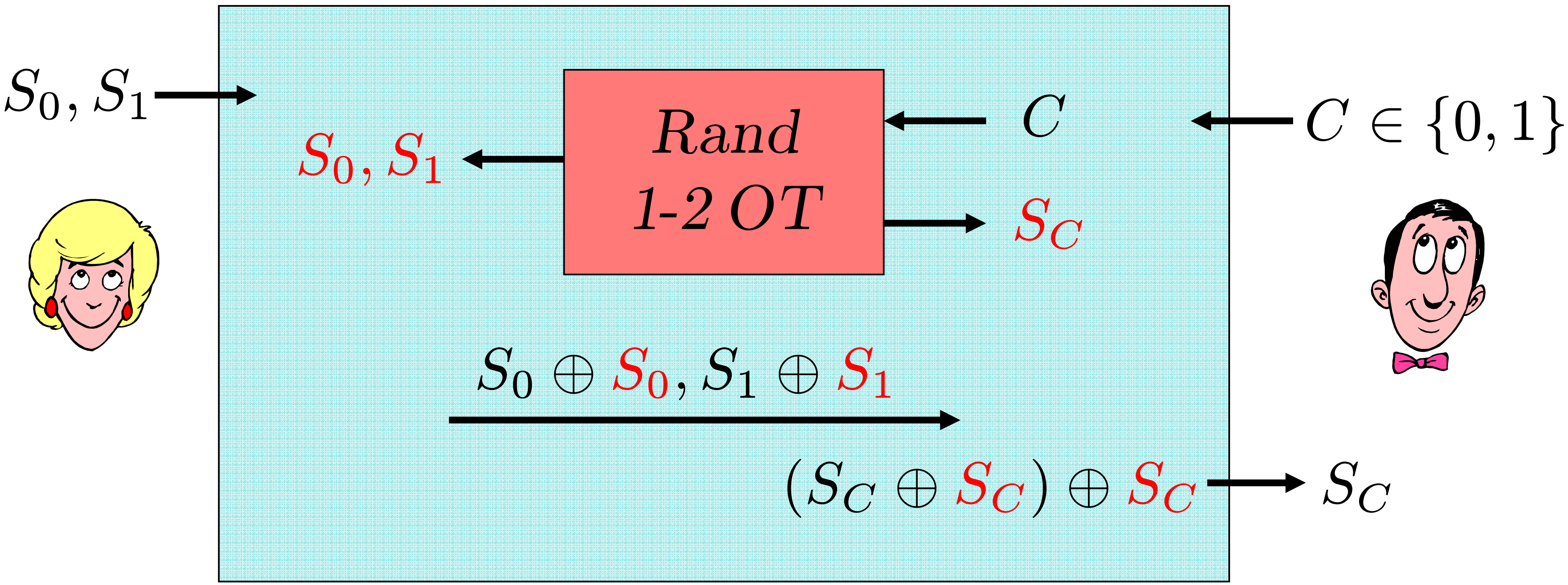
- OT and Randomized OT
- Characterisation of Sender-Security with Linear Functions
- Application: Universal OT
- Conclusion

1-2 Oblivious Transfer



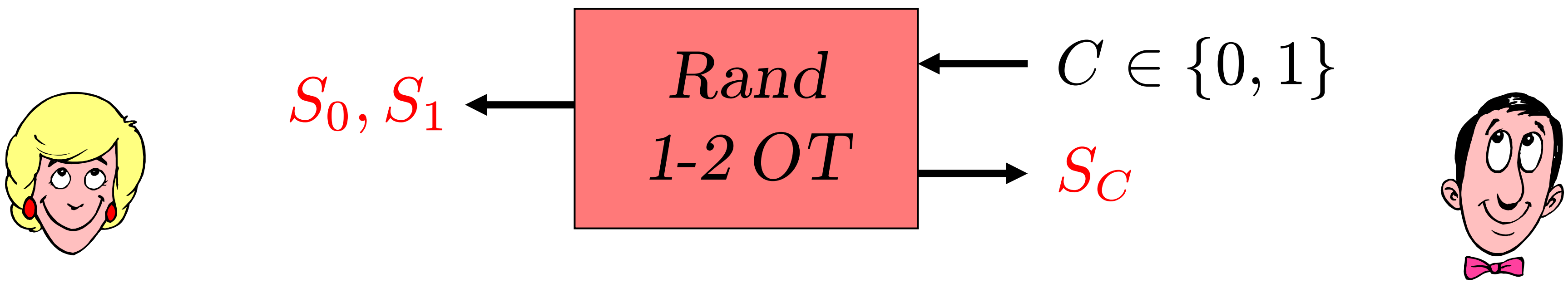
- **correctness:** works for honest players,
- **receiver-security:** $\forall \tilde{\mathsf{A}}$ dishonest senders, $\tilde{\mathsf{A}}$ should not learn C,
- **sender-security:** $\forall \tilde{\mathsf{B}}$ dishonest receivers, $\tilde{\mathsf{B}}$ should not learn S_{1-C}.

Randomized 1-2 Oblivious Transfer



Definition Rand 1-2 OT

[Crépeau Savvides Schaffner Wullschleger 06]

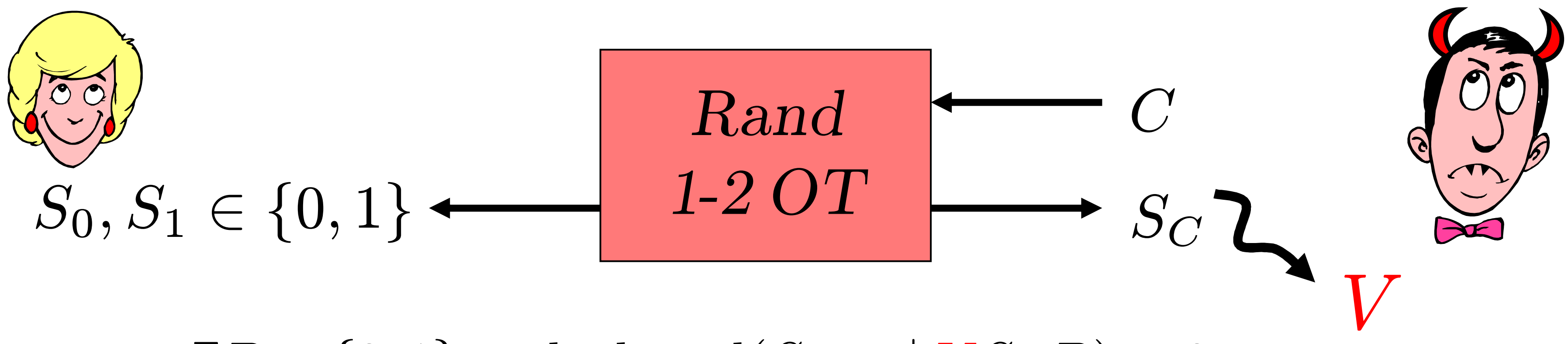


Protocol Π computes *Rand 1-2 OT* securely, if $\forall$ inputs C
Π produces outputs such that

- **correctness:** If A and B honest, A gets S_0, S_1, B gets S_C.
- **receiver-security:** $\forall \tilde{\mathsf{A}}$ dishonest senders with view U, $P_{UC} = P_U \cdot P_C$.
- **sender-security:** $\forall \tilde{\mathsf{B}}$ dishonest receivers with view V, $\exists D \in \{0, 1\}$ s.t. $d(S_{1-D} \mid V S_D D) = 0$.

$$\left\| P_{S_{1-D} V S_D D} - P_{\text{UNIF}} \cdot P_{V S_D D} \right\| = 0$$

Sender-Security for Rand OT of Bits



$$\exists D \in \{0,1\} \text{ such that } \mathrm{d}(S_{1-D} \mid V S_D D) = 0$$

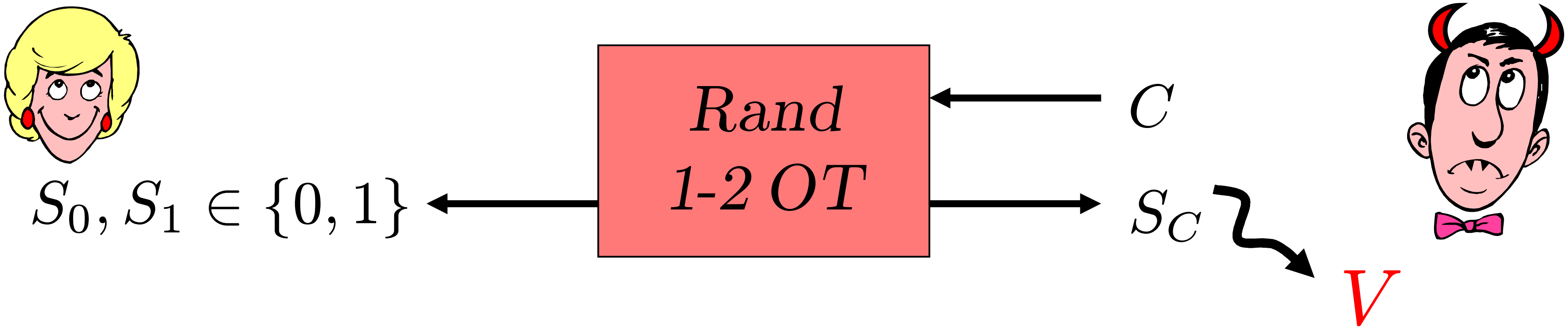
$$\Leftrightarrow \mathrm{d}(S_0 \oplus S_1 \mid V) = 0$$

S_0 \ S_1	0	1
0	½	¼
1	¼	0

$P_{S_0 S_1 V}(\cdot, \cdot, v)$

D ?

Sender-Security for Rand OT of Bits



$$\exists D \in \{0,1\} \text{ such that } d(S_{1-D} \mid V S_D D) = 0$$

$$\Leftrightarrow d(S_0 \oplus S_1 \mid V) = 0$$

S_0 \ S_1	0	1
0	½	¼
1	¼	0

$P_{S_0 S_1 V}(\cdot,\cdot,v)$

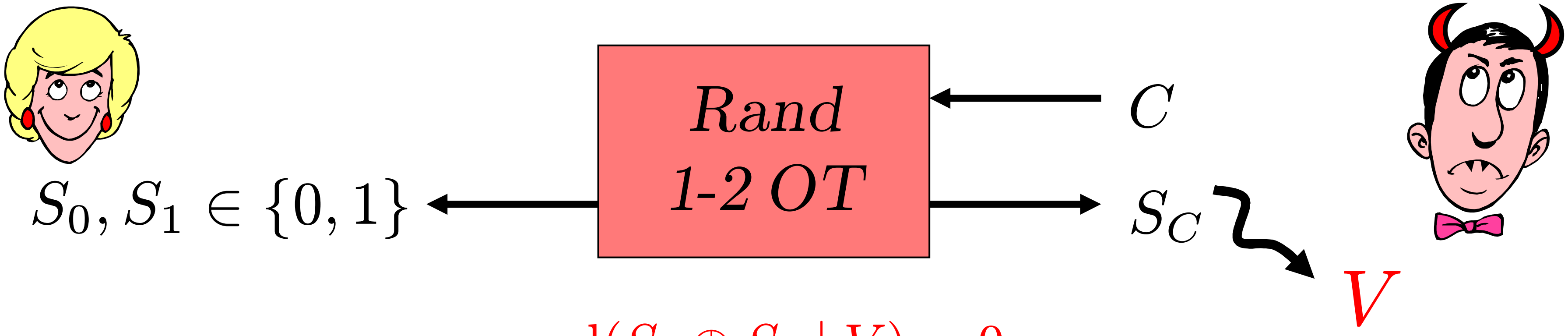
S_0 \ S_1	0	1
0	¼	¼
1	0	0

$P_{S_0 S_1 D V}(\cdot,\cdot,0,v)$

S_0 \ S_1	0	1
0	¼	0
1	¼	0

$P_{S_0 S_1 D V}(\cdot,\cdot,1,v)$

Sender-Security for Rand OT of Bits



$$d(S_0 \oplus S_1 \mid V) = 0$$

$\Rightarrow$ $\exists D \in \{0,1\}$ such that $d(S_{1-D} \mid V S_D D) = 0$

S_0 \ S_1	0	1
0	a	b
1	c	d

$P_{S_0 S_1 V}(\cdot, \cdot, v)$

S_0 \ S_1	0	1
0	a	a
1	c	c

$P_{S_0 S_1 D V}(\cdot, \cdot, 0, v)$

S_0 \ S_1	0	1
0	0	b-a
1	0	b-a

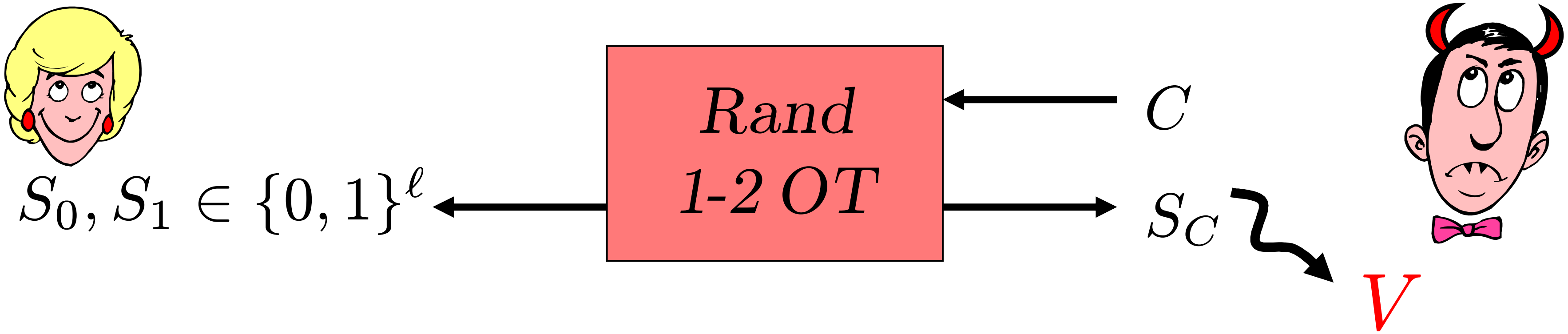
$P_{S_0 S_1 D V}(\cdot, \cdot, 1, v)$

$a + d = c + b$

$c + (b - a) = d$

wlog: $b \geq a$

Characterisation of Sender-Security



$$\exists D \in \{0,1\} \text{ such that } \mathrm{d}(S_{1-D} \mid V S_D D) \leq \varepsilon.$$

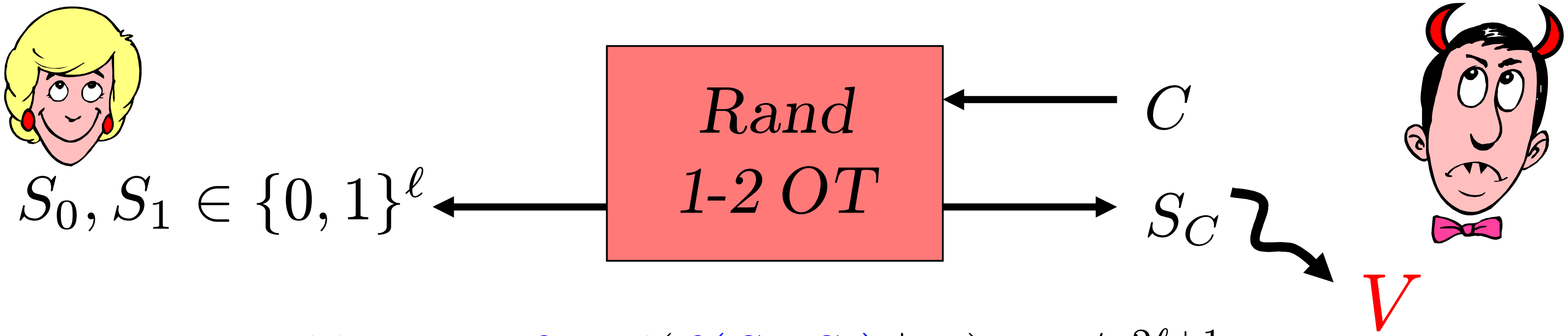
$$\Rightarrow \forall \text{ NDLF } \beta \;:\; \mathrm{d}(\beta(S_0, S_1) \mid V) \leq \varepsilon$$

Def: *A non-degenerate linear function (NDLF) is a function*

$$\beta : \{0,1\}^\ell \times \{0,1\}^\ell \to \{0,1\}$$
$$(s_0, s_1) \mapsto \langle a_0, s_0 \rangle \oplus \langle a_1, s_1 \rangle$$

for non-zero $a_0, a_1 \in \{0,1\}^\ell$, *i.e., it is linear and non-trivially depends on both inputs.*

Characterisation of Sender-Security



$$\forall \text{ NDLF } \beta \; : \; \mathrm{d}(\beta(S_0, S_1) \mid V) \leq \varepsilon / 2^{2\ell+1}$$

$$\Rightarrow \exists D \in \{0,1\} \text{ such that } \mathrm{d}(S_{1-D} \mid V S_D D) \leq \varepsilon.$$

Theorem: If for all NDLF β, $\mathrm{d}(\beta(S_0, S_1) \mid V) \leq \varepsilon / 2^{2\ell+1}$ holds, then there exists $D \in \{0,1\}$ such that $\mathrm{d}(S_{1-D} \mid V S_D D) \leq \varepsilon$.

Proof for $\ell = 2$, perfect case

Theorem: If for all NDLF β, $\mathrm{d}(\beta(S_0, S_1) \mid V) = 0$ holds, then there exists $D \in \{0,1\}$ such that $\mathrm{d}(S_{1-D} \mid V S_D D) = 0$.

$S_0 \backslash S_1$	00	01	10	11
00	a	b	c	d
01	e	f	g	h
10	i	j	k	l
11	m	n	o	p

$P_{S_0 S_1 V}(\cdot, \cdot, v)$

$S_0 \backslash S_1$	00	01	10	11
00	a	a	a	a
01	e	e	e	e
10	i	i	i	i
11	m	m	m	m

$P_{S_0 S_1 D V}(\cdot, \cdot, 0, v)$

$S_0 \backslash S_1$	00	01	10	11
00	0	b-a	c-a	d-a
01	0	b-a	c-a	d-a
10	0	b-a	c-a	d-a
11	0	b-a	c-a	d-a

$P_{S_0 S_1 D V}(\cdot, \cdot, 1, v)$

Proof for $\ell = 2$, perfect case

Theorem: If for all NDLF β, $d(\beta(S_0, S_1) \mid V) = 0$ holds, then there exists $D \in \{0,1\}$ such that $d(S_{1-D} \mid V S_D D) = 0$.

$S_0 \backslash S_1$	00	01	10	11
00	a	b	c	d
01	e	f	g	h
10	i	j	k	l
11	m	n	o	p

$P_{S_0 S_1 V}(\cdot, \cdot, v)$

$S_0 \backslash S_1$	00	01	10	11
00	a	a	a	a
01	e	e	e	e
10	i	i	i	i
11	m	m	m	m

$P_{S_0 S_1 D V}(\cdot, \cdot, 0, v)$

$S_0 \backslash S_1$	00	01	10	11
00	0	b-a	c-a	d-a
01	0	b-a	c-a	d-a
10	0	b-a	c-a	d-a
11	0	b-a	c-a	d-a

$P_{S_0 S_1 D V}(\cdot, \cdot, 1, v)$

$b+e=a+f$

Proof for $\ell = 2$, perfect case

Theorem: If for all NDLF β, $\mathrm{d}(\beta(S_0, S_1) \mid V) = 0$ holds, then there exists $D \in \{0,1\}$ such that $\mathrm{d}(S_{1-D} \mid V S_D D) = 0$.

$S_0 \backslash S_1$	00	01	10	11
00	a	b	c	d
01	e	f	g	h
10	i	j	k	l
11	m	n	o	p

$P_{S_0 S_1 V}(\cdot, \cdot, v)$

$S_0 \backslash S_1$	00	01	10	11
00	a	a	a	a
01	e	e	e	e
10	i	i	i	i
11	m	m	m	m

$P_{S_0 S_1 D V}(\cdot, \cdot, 0, v)$

$S_0 \backslash S_1$	00	01	10	11
00	0	b-a	c-a	d-a
01	0	b-a	c-a	d-a
10	0	b-a	c-a	d-a
11	0	b-a	c-a	d-a

$P_{S_0 S_1 D V}(\cdot, \cdot, 1, v)$

$b + e = a + f$

$c + e = a + g$

Proof for $\ell = 2$, perfect case

Theorem: If for all NDLF β, $\mathrm{d}(\beta(S_0, S_1) \mid V) = 0$ holds, then there exists $D \in \{0, 1\}$ such that $\mathrm{d}(S_{1-D} \mid V S_D D) = 0$.

$S_0 \backslash S_1$	00	01	10	11
00	a	b	c	d
01	e	f	g	h
10	i	j	k	l
11	m	n	o	p

$P_{S_0 S_1 V}(\cdot, \cdot, v)$

$b + e = a + f$

$S_0 \backslash S_1$	00	01	10	11
00	a	a	a	a
01	e	e	e	e
10	i	i	i	i
11	m	m	m	m

$P_{S_0 S_1 D V}(\cdot, \cdot, 0, v)$

$c + e = a + g$

$S_0 \backslash S_1$	00	01	10	11
00	0	b-a	c-a	d-a
01	0	b-a	c-a	d-a
10	0	b-a	c-a	d-a
11	0	b-a	c-a	d-a

$P_{S_0 S_1 D V}(\cdot, \cdot, 1, v)$

$d + e = a + h$

Proof for $\ell = 2$, perfect case

Theorem: If for all NDLF β, $\mathrm{d}(\beta(S_0, S_1) \mid V) = 0$ holds, then there exists $D \in \{0,1\}$ such that $\mathrm{d}(S_{1-D} \mid V S_D D) = 0$.

$S_0 \backslash S_1$	00	01	10	11
00	a	b	c	d
01	e	f	g	h
10	i	j	k	l
11	m	n	o	p

$P_{S_0 S_1 V}(\cdot,\cdot,v)$

$S_0 \backslash S_1$	00	01	10	11
00	a	a	a	a
01	e	e	e	e
10	i	i	i	i
11	m	m	m	m

$P_{S_0 S_1 D V}(\cdot,\cdot,0,v)$

$S_0 \backslash S_1$	00	01	10	11
00	0	b-a	c-a	d-a
01	0	b-a	c-a	d-a
10	0	b-a	c-a	d-a
11	0	b-a	c-a	d-a

$P_{S_0 S_1 D V}(\cdot,\cdot,1,v)$

$+ \quad b + e = a + f$
$- \quad b + i = a + j$
$+ \quad b + m = a + n$

$- \quad c + e = a + g$
$+ \quad c + i = a + k$
$- \quad c + m = a + o$

$+ \quad d + e = a + h$
$- \quad d + i = a + l$
$+ \quad d + m = a + p$

$$b + d + e + g + j + l + m + o = a + c + f + h + i + k + n + p$$

Proof for $\ell = 2$, perfect case

Theorem: If for all NDLF β, $d(\beta(S_0, S_1) \mid V) = 0$ holds, then there exists $D \in \{0, 1\}$ such that $d(S_{1-D} \mid V S_D D) = 0$.

$S_0 \backslash S_1$	00	01	10	11
00	a	b	c	d
01	e	f	g	h
10	i	j	k	l
11	m	n	o	p

$P_{S_0 S_1 V}(\cdot, \cdot, v)$

$\beta(s_0, s_1) := s_0^2 \oplus s_1^2$

$P_{S_0 S_1 D V}(\cdot, \cdot, 0, v)$

01	10	11
b-a	c-a	d-a
b-a	c-a	d-a
b-a	c-a	d-a
b-a	c-a	d-a

$P_{S_0 S_1 D V}(\cdot, \cdot, 1, v)$

$+\ b + e = a + f$	$-\ c + e = a + g$	$+\ d + e = a + h$
$-\ b + i = a + j$	$+\ c + i = a + k$	$-\ d + i = a + l$
$+\ b + m = a + n$	$-\ c + m = a + o$	$+\ d + m = a + p$

$$b + d + e + g + j + l + m + o = a + c + f + h + i + k + n + p$$

Proof for $\ell = 2$, perfect case

Theorem: If for all NDLF β, $\mathrm{d}(\beta(S_0, S_1) \mid V) = 0$ holds, then there exists $D \in \{0,1\}$ such that $\mathrm{d}(S_{1-D} \mid V S_D D) = 0$.

$S_0 \backslash S_1$	00	01	10	11
00	a	b	c	d
01	e	f	g	h
10	i	j	k	l
11	m	n	o	p

$P_{S_0 S_1 V}(\cdot,\cdot,v)$

$S_0 \backslash S_1$	00	01	10	11
00				
01				
10				
11				

$P_{S_0 S_1 D V}(\cdot,\cdot,0,v)$

$S_0 \backslash S_1$	00	01	10	11
		b-a	c-a	d-a
		b-a	c-a	d-a
		b-a	c-a	d-a
		b-a	c-a	d-a

$P_{S_0 S_1 D V}(\cdot,\cdot,1,v)$

$\beta(s_0, s_1) := s_0^2 \oplus s_1^2$

$\beta(s_0, s_1) = 1$

$\beta(s_0, s_1) = 0$

$+ \quad b + e = a + f$	$-\quad c + e = a + g$	$+\quad d + e = a + h$
$-\quad b + i = a + j$	$+\quad c + i = a + k$	$-\quad d + i = a + l$
$+\quad b + m = a + n$	$-\quad c + m = a + o$	$+\quad d + m = a + p$

$$\underbrace{b + d + e + g + j + l + m + o}_{\beta(s_0,s_1)=1} = \underbrace{a + c + f + h + i + k + n + p}_{\beta(s_0,s_1)=0}$$

Proof for $\ell = 2$, perfect case

Theorem: If for all NDLF β, $\mathrm{d}(\beta(S_0, S_1) \mid V) = 0$ holds, then there exists $D \in \{0,1\}$ such that $\mathrm{d}(S_{1-D} \mid V S_D D) = 0$.

$S_0 \backslash S_1$	00	01	10	11
00	a	b	c	d
01	e	f	g	h
10	i	j	k	l
11	m	n	o	p

$P_{S_0 S_1 V}(\cdot,\cdot,v)$

$\beta(s_0, s_1) := s_0^1 \oplus s_1^2$

$\beta(s_0, s_1) = 1$

$\beta(s_0, s_1) = 0$

$P_{S_0 S_1 D V}(\cdot,\cdot,0,v)$

$S_0 \backslash S_1$	00	01	10	11
[illegible]	[illegible]	b-a	c-a	d-a
[illegible]	[illegible]	b-a	c-a	d-a
[illegible]	[illegible]	b-a	c-a	d-a
[illegible]	[illegible]	b-a	c-a	d-a

$P_{S_0 S_1 D V}(\cdot,\cdot,1,v)$

$b+e=a+f$	$c+e=a+g$	$d+e=a+h$
$b+i=a+j$	$c+i=a+k$	$d+i=a+l$
$b+m=a+n$	$c+m=a+o$	$d+m=a+p$

$$b+d+e+g+j+l+m+o = a+c+f+h+i+k+n+p$$

$$b+d+f+h+i+k+m+o = a+c+e+g+j+l+n+p$$

Proof for $\ell = 2$, perfect case

Theorem: If for all NDLF β, $\mathrm{d}(\beta(S_0, S_1) \mid V) = 0$ holds, then there exists $D \in \{0,1\}$ such that $\mathrm{d}(S_{1-D} \mid V S_D D) = 0$.

$S_0 \backslash S_1$	00	01	10	11
00	a	b	c	d
01	e	f	g	h
10	i	j	k	l
11	m	n	o	p

$P_{S_0 S_1 V}(\cdot,\cdot,v)$

$S_0 \backslash S_1$	00	01	10	11
00	a	a	a	a
01	e	e	e	e
10	i	i	i	i
11	m	m	m	m

$P_{S_0 S_1 D V}(\cdot,\cdot,0,v)$

$S_0 \backslash S_1$	00	01	10	11
00	0	b-a	c-a	d-a
01	0	b-a	c-a	d-a
10	0	b-a	c-a	d-a
11	0	b-a	c-a	d-a

$P_{S_0 S_1 D V}(\cdot,\cdot,1,v)$

$$\begin{cases} b+e=a+f & c+e=a+g & d+e=a+h \\ b+i=a+j & c+i=a+k & d+i=a+l \\ b+m=a+n & c+m=a+o & d+m=a+p \end{cases}$$

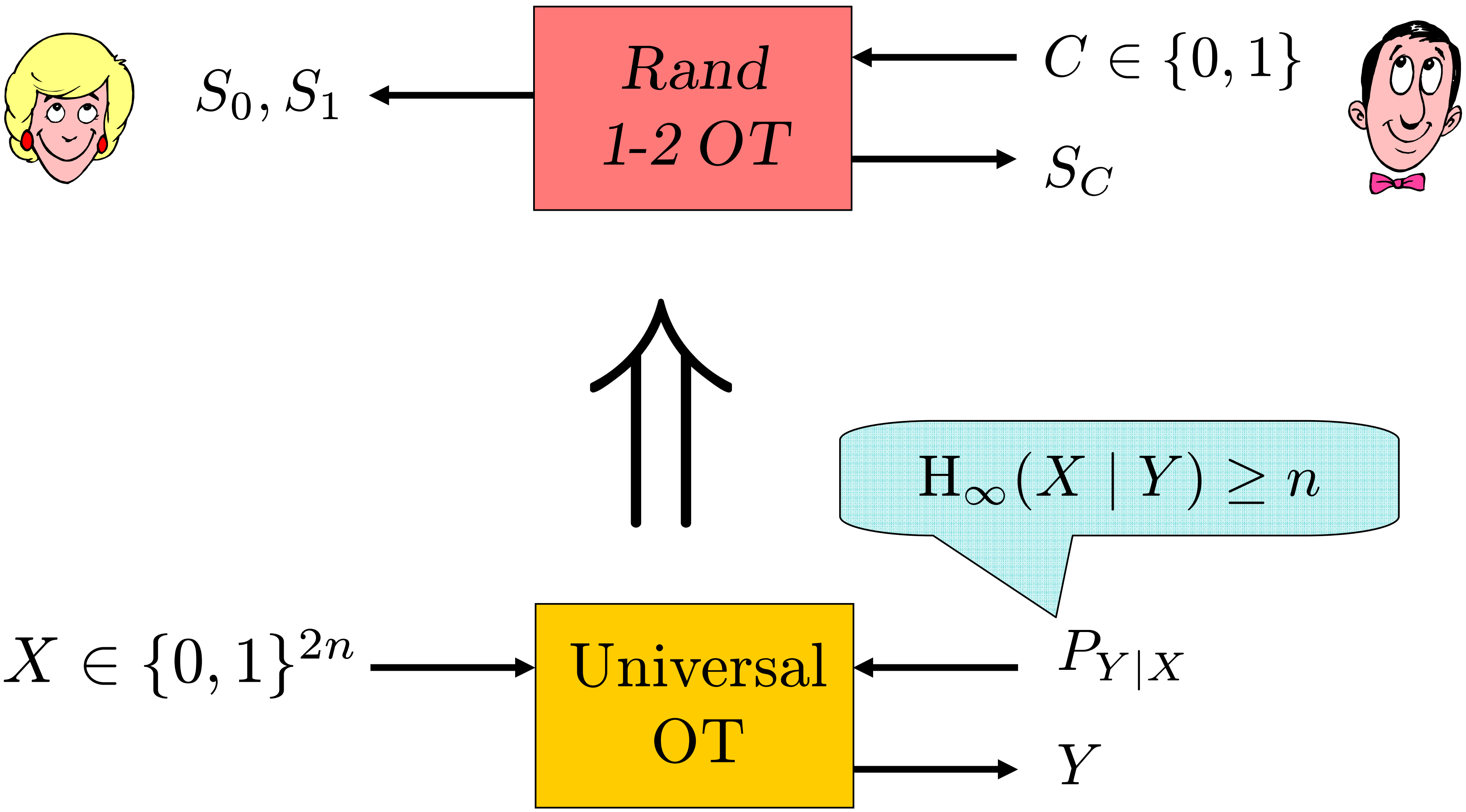
$$\begin{cases} b+d+e+g+j+l+m+o=a+c+f+h+i+k+n+p \\ b+d+f+h+i+k+m+o=a+c+e+g+j+l+n+p \\ \vdots \end{cases}$$

□

Agenda

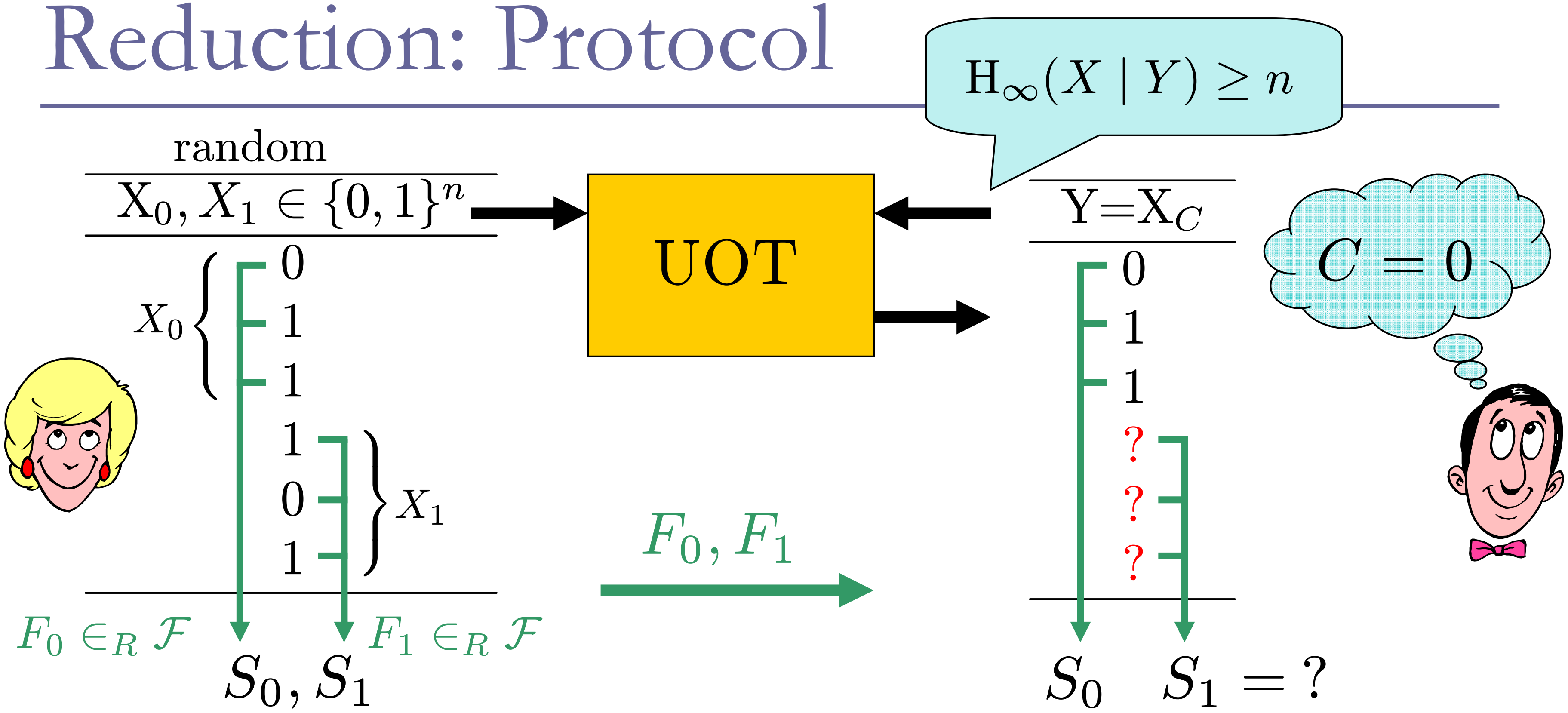
- ✓ OT and Randomized OT
- ✓ Characterisation of Sender-Security with Linear Functions
- **Application: Universal OT**
- Conclusion

Application: Universal OT



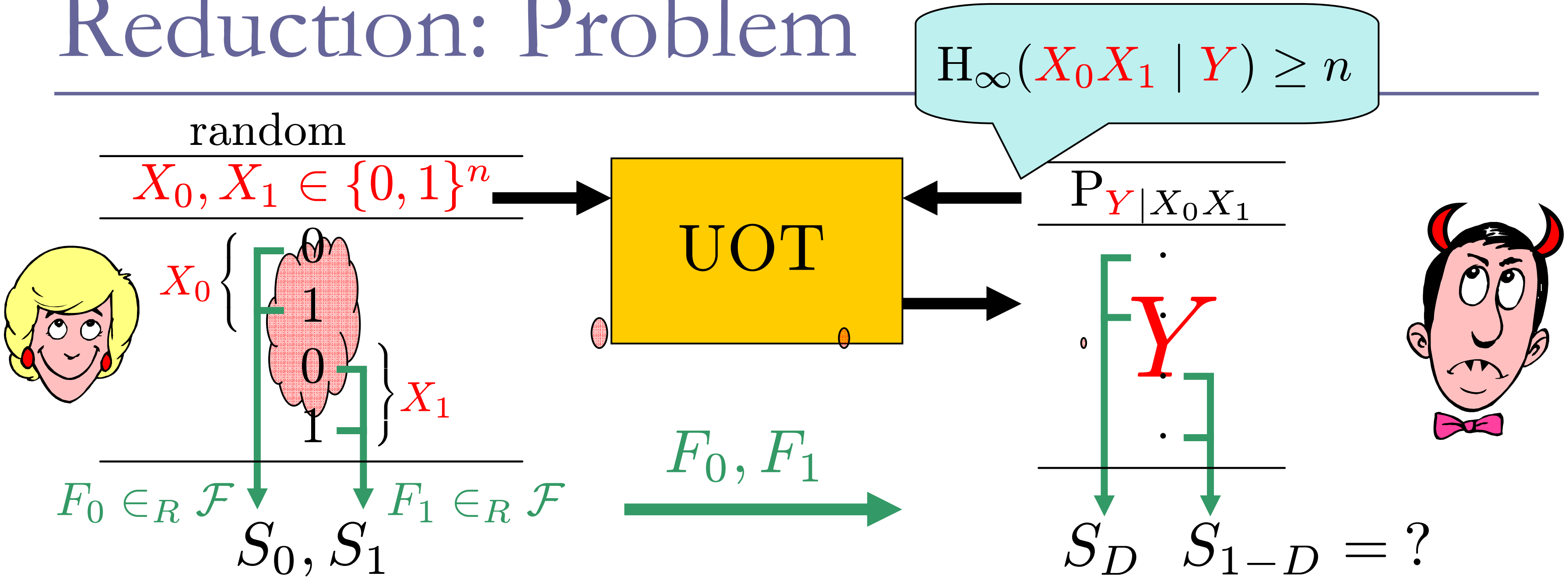
[Cachin 98]

Reduction: Protocol



- **correctness:** If A and B honest, A gets S_0, S_1, B gets S_C. ✓
- **receiver-security:** $\forall \tilde{A}$ dishonest senders with view U, $P_{UC} = P_U \cdot P_C$. ✓

Reduction: Problem



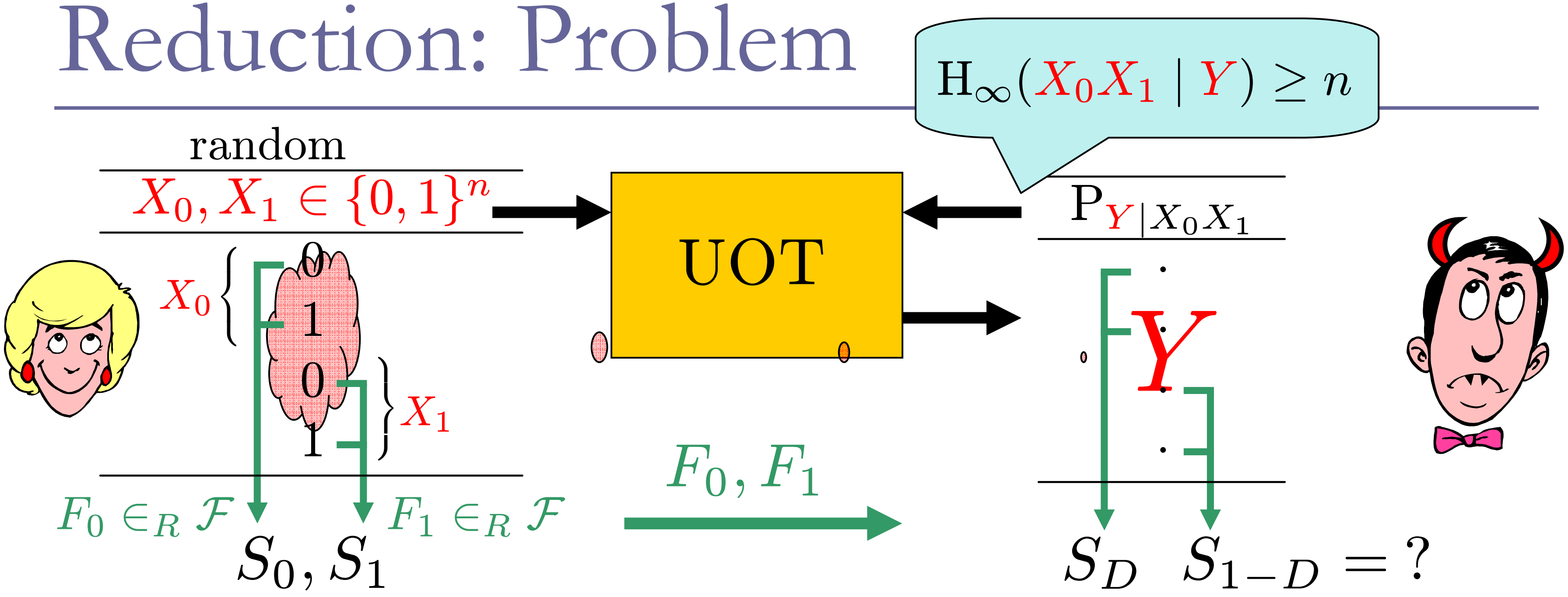
sender-security: $\exists D$ s.t. $d(S_{1-D} \mid V D S_D) \leq \varepsilon$

$X_0 \in \{0,1\}^n \xrightarrow{F_0 \in_R \mathcal{F}} S_0 \in \{0,1\}^\ell$

$x \neq x' \Rightarrow F(x), F(x')$ independent and uniform.

$H_\infty(X_0 \mid V)$ big $\Rightarrow d(S_0 \mid V F)$ small **Privacy Amplification**

Reduction: Problem



Theorem: $\forall$ NDLF β : $d(\beta(S_0, S_1) \mid V)$ small

$\Rightarrow$ **sender-security:** $\exists D$ s.t. $d(S_{1-D} \mid VDS_D) \leq \varepsilon$

$X_0 \in \{0,1\}^n \xrightarrow{F_0 \in_R \mathcal{F}} S_0 \in \{0,1\}^\ell$

$X_1 \in \{0,1\}^n \xrightarrow{F_1 \in_R \mathcal{F}} S_1 \in \{0,1\}^\ell$

$\Rightarrow \beta(S_0, S_1) \in \{0,1\}$

Observe: The class $\mathcal{F}^\beta := \{\beta(F_0(\cdot), F_1(\cdot)) \mid F_0 \in \mathcal{F}, F_1 \in \mathcal{F}\}$ is strongly two-universal.

$H_\infty(X_0 \mid V)$ big $\Rightarrow d(S_0 \mid V, F)$ small **Privacy Amplification**

$H_\infty(X_0X_1 \mid V)$ big $\Rightarrow d(\beta(S_0, S_1) \mid V)$ small **PA**

Conclusion

- **Characterisation of sender-privacy:**
  A protocol for Rand-OT is secure against a cheating receiver, iff he gets no information about any non-degenerate linear function.
- **Observation:**
  NDLF compose well with strongly two-universal hash functions.
- **yields powerful technique:**
  Enough min-entropy suffices to get an OT via (strongly) two-universal hashing,
  also works in quantum settings.
- **Reductions:**
  Simpler analyses of reductions from String-OT to weaker primitives, better parameters.

Thank you

The Bottom Line

Alice   Bob

$X \in \{0,1\}^n$

view $V = v$.

01100101010110

$F_0 \in_R \mathcal{F}$ $F_1 \in_R \mathcal{F}$

F_0, F_1

101 , 001

$S_0, S_1 \in \{0,1\}^\ell$

$H_\infty(X \mid V = v) \geq \alpha n$

$\exists C'$ s.t.

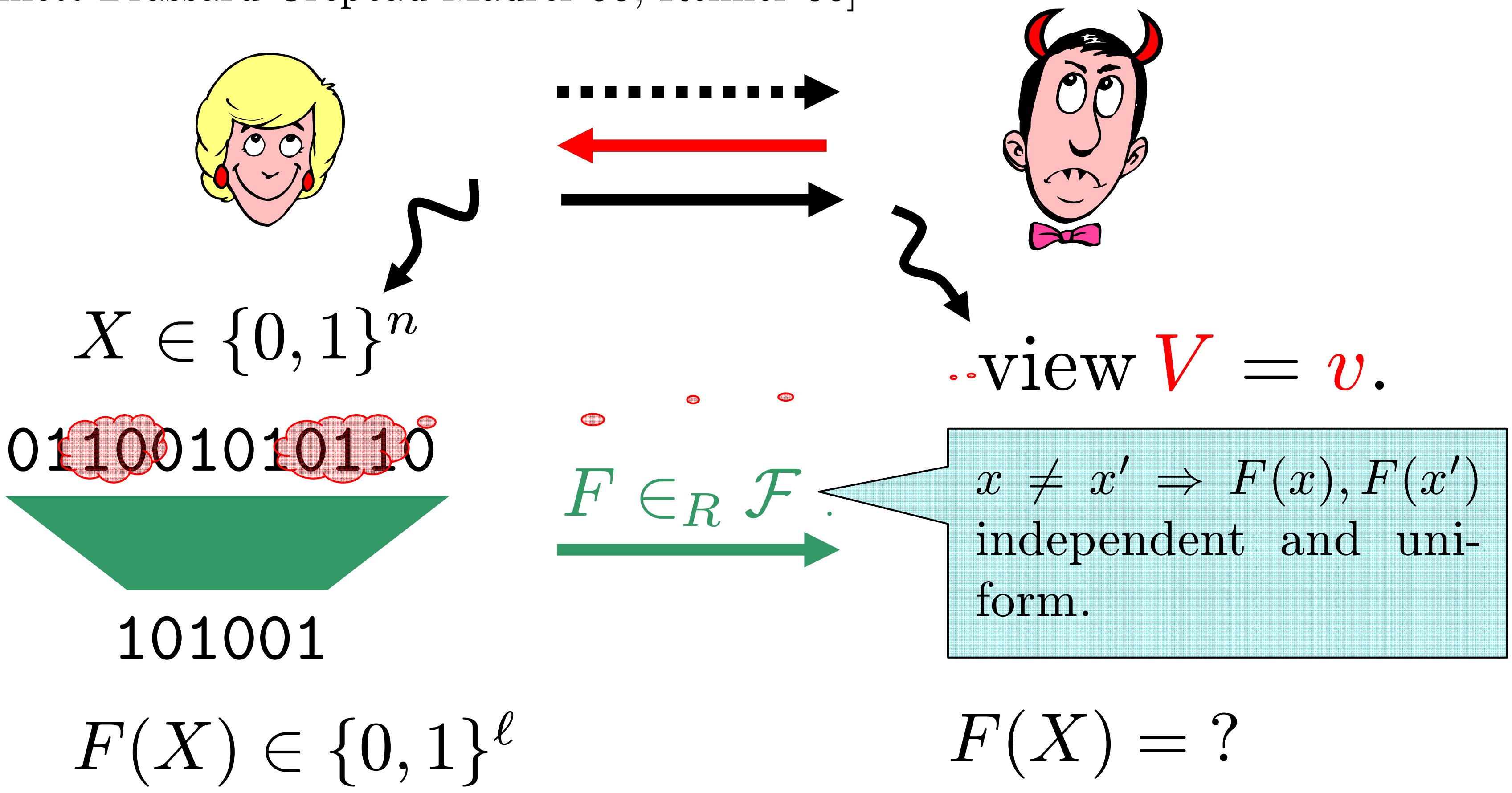
$d(S_{1-C'} \mid V C' S_{C'}) \leq \varepsilon$

$F \in_R \mathcal{F}^\beta := \{\beta(F_0(\cdot), F_1(\cdot)) \mid F_0 \in \mathcal{F}_0, F_1 \in \mathcal{F}_1\}$

$$\text{PA: } d(\underbrace{F(X)}_{\beta(S_0,S_1)} \mid \underbrace{F, V = v}_{V}) \leq 2^{-\frac{1}{2}\left(H_\infty(X|V=v)-1\right)} \leq \varepsilon \cdot 2^{-2\ell-1}$$

Privacy Amplification (PA)

[Impagliazzo Levin Luby 89, Håstad ILL 99,
Bennett Brassard Crépeau Maurer 95, Renner 06]



Thm: $\mathrm{d}(F(X) \mid F, V = v) \leq 2^{-\frac{1}{2}\left(\mathrm{H}_\infty(X|V=v)-\ell\right)}$