Worlds of HSS

Algo < Minicrypt < Lapland < Cryptomania < Gentria

trivial — Point fns ++ — Branching programs — Spooky

Lapland → Constant deg. multivariate polynomials

Related notion: **P**seudorandom **C**orrelation **G**enerators

PCGs

What are "correlations" here?

Recall 2PC:

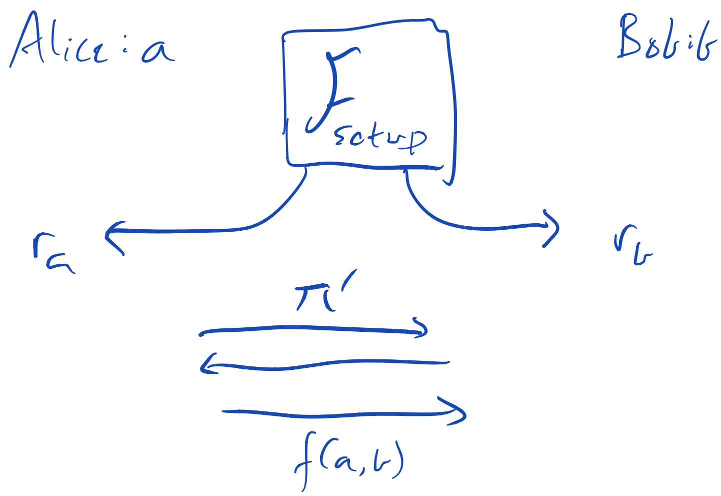
Alice: a $\xrightarrow{\pi}$ Bob: b

$\leftarrow$

$\rightarrow$

f(a,b)

2PC with correlated randomness



π' is cheaper than π

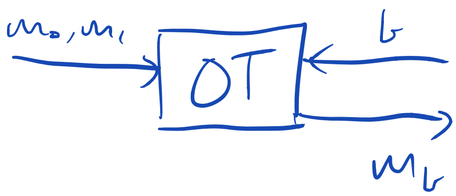
e.g. $\downarrow$ information theoretic

$\downarrow$ public key crypto

Classic example: Oblivious Transfer (OT)

OT : Two parties

S: m_0, m_1 $\qquad\qquad$ R: $b \in \{0,1\}$



OT is complete for secure computation

$\Rightarrow$ cryptomania object, i.e. requires public key operations [IR]

But information-theoretic w. preprocessing (Beaver 96)

$\mathcal{F}_{setup}$:

$\hat{b} \leftarrow \{0,1\}$

$\hat{m}_0, \hat{m}_1 \leftarrow \{0,1\}$

R: b | S: m_0, m_1

$\hat{b}, m_{\hat{b}}$ | $\hat{m}_0, \hat{m}_1$

$\beta = b \oplus \hat{b}$

$\xrightarrow{\beta}$

$M_0 = m_0 \oplus \hat{m}_\beta$

$M_1 = m_1 \oplus \hat{m}_{1-\beta}$

$\xleftarrow{M_0, M_1}$

output $M_b \oplus m_{\hat{b}}$

$= m_b$

Correctness: By inspection

Security: $\hat{b}$ is OTP for b

$\hat{m}_{1-\hat{b}}$ is OTP for m_{1-b}

OT correlation:

$(\vec{b}, \vec{m}_{\vec{b}}), \ (\vec{m}_0, \vec{m}_1)$

Δ-OT correlation: [IKNP03] $\xrightarrow[\text{Hash}]{\text{Cor Rob.}}$ OT

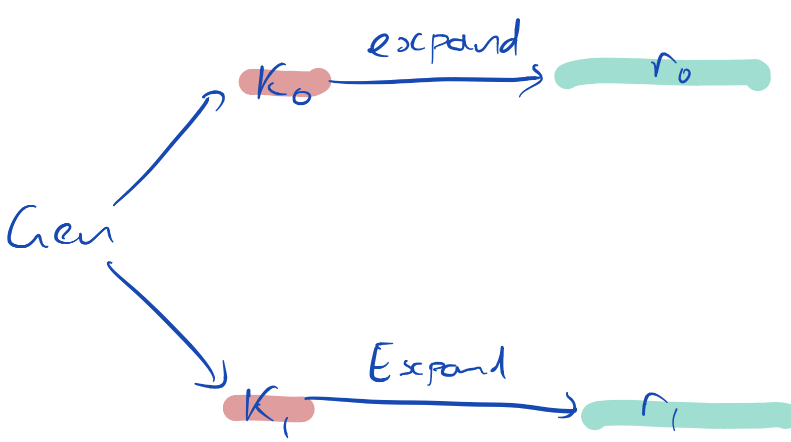
$$\underbrace{(b_i, w_i \oplus b_i \cdot \Delta)}_{R_0}{}_{i \in [n]}, \ \underbrace{(w_i, w_i \oplus \Delta)}_{R_1}{}_{i \in [n]}$$

$R_0, R_1 \leftarrow \mathrm{GenCor}(1^\lambda, n)$

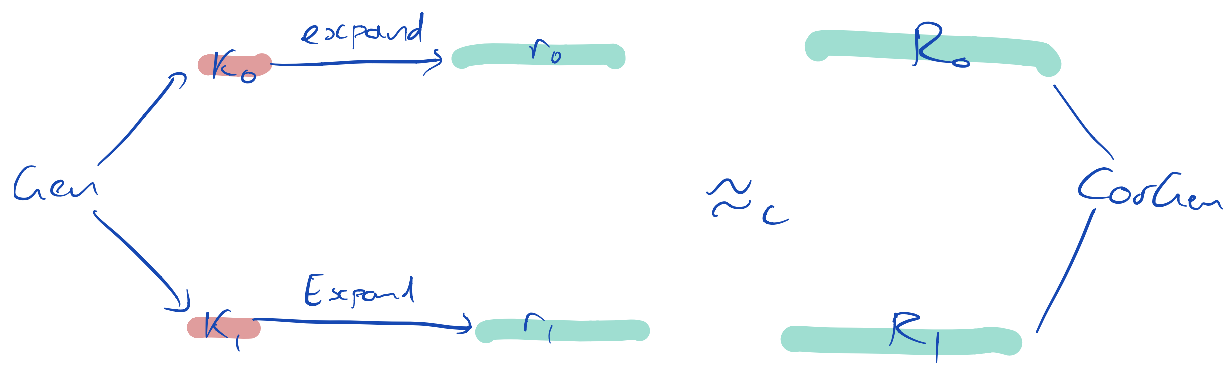
$\boxed{\text{Task}}$ compress R_0, R_1 into short seeds

$\Rightarrow$ succinct generation of correlations

PCG: Two algorithms



Correctness:



Security:

Tricky to define. Simulation-based definition not possible

~~Intuition: due to Yao incompressible entropy of protocol that simply outputs R_0, R_1 by expanding seeds.~~

Reverse samplability: $\forall \sigma \in \{0,1\}$

$R_0, R_1 \leftarrow \text{CorGen}(1^\lambda)$

$R'_{1-\sigma} \leftarrow \text{RSample}(\sigma, R_\sigma)$

$R'_\sigma = R_\sigma$

$(R_0, R_1) \approx_c (R'_0, R'_1)$

For OT: RSample:

Given $(w_i, w_i \oplus \Delta)$, sample $b_i \leftarrow \{0,1\}$

output $(b_i, w_i \oplus b_i \Delta)$

Given $(b_i, m_{i b_i})$, sample $\Delta \leftarrow \{0,1\}^\lambda$

set each $m_{i, 1-b_i} = m_{i b_i} \oplus \Delta$

output (m_{i0}, m_{i1})

PCG Security: $\forall \sigma \in \{0,1\}$

World 0:

$k_0, k_1 \leftarrow Gen(1^\lambda)$

$R_\sigma \leftarrow Expand(\sigma, k_\sigma)$

output $(k_{1-\sigma}, R_\sigma)$

World 1:

$k_0, k_1 \leftarrow Gen(1^\lambda)$

$R_{1-\sigma} \leftarrow Expand(1-\sigma, k_{1-\sigma})$

$R_\sigma \leftarrow RSample(\sigma, R_{1-\sigma})$

output $(k_{1-\sigma}, R_\sigma)$

Distributions $\approx_c$

Intuition: captures that other party's correlation "as good as" sampled by Corr even when given one key

Turns out to be good enough when setup oracle distributes expanded randomness

Relation to HSS:

Given a PCG for general, additive degree-d correlations (for constant d), we can construct an HSS scheme for deg-d n-variate polynomials, share size is linear in n

Not going to cover transformation or PCG for deg-d correlations, but will cover core idea & applications to OT PCG

Recall OT correlation:

$R_0 = (w_i, w_i \oplus \Delta)_{i \in [n]}$, $R_1 = (b_i, w_i \oplus b_i \Delta)_{i \in [n]}$

$\Downarrow$ Sender $\qquad\qquad$ $\Downarrow$ Receiver

Define functions

$$f_S(i) = w_i$$

$$f_R(i) = w_i \oplus b_i \cdot \Delta$$

$$(\Delta, f_S) \Rightarrow R_0 \quad , \quad (\vec{b}, f_R) \Rightarrow R_1$$

Combining them,

$$f(i) = f_S(i) \oplus f_R(i) = \begin{cases} \Delta & \text{if } b_i = 1 \\ 0 & \text{if } b_i = 0 \end{cases}$$

Look familiar? Looks like Multi-point function

But it's not sparse $\Rightarrow$ unclear how to compress

Dual-LPN : (specific instantiation used here)

Fix integers m, n, t based on λ.

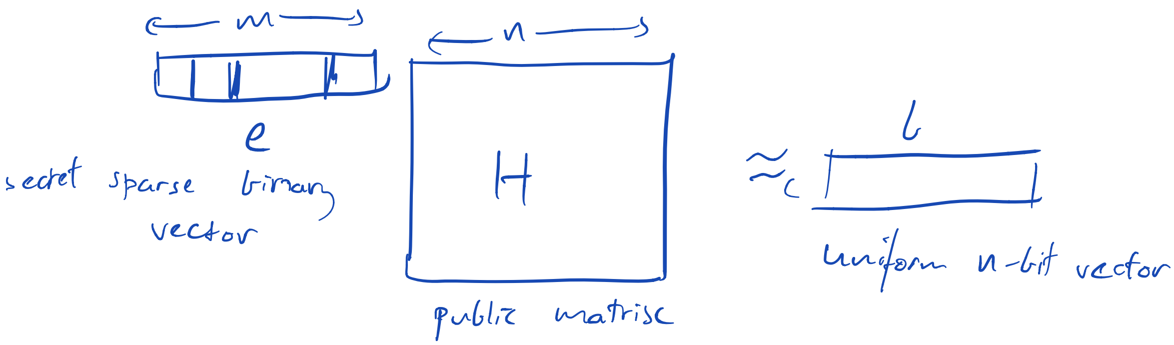
$HW_{m,t}$: set of all bit vectors of size 'm', and Hamming Weight 't'

C : probabilistic generation algorithm that outputs $m \times n$ binary matrix H

Assumption:

World 0:	World 1:
$H \leftarrow C,\ e \leftarrow HW_{m,t}$	$H \leftarrow C$
$b = e \cdot H$	$b \leftarrow \mathbb{F}_2^n$
output (H, b)	output (H, b)

$$W_0 \approx_c W_1$$



Each $b_i = \langle e, H_i \rangle$

Sparse MPF

compressible via FSS

public weights

Local evaluation

PCG Gen:

$\Delta \leftarrow \{0,1\}^\lambda$

$e \leftarrow \mathcal{HW}_t$

Set $\hat{f}_{e,\Delta}(j) = \begin{cases} \Delta & \text{if } e_j = 1 \\ 0 & \text{otherwise} \end{cases}$

$\hat{f}_0, \hat{f}_1 \leftarrow \text{MPFSS}(\hat{f}_{e,\Delta})$

Output $\underset{\text{Sender}}{\underline{K_0 = (\hat{f}_0, \Delta)}}, \underset{\text{Recvr}}{\underline{K_1 = (\hat{f}_1, e)}}$

Expand(σ, k_σ)

If $\sigma = 0$ (Sender): $(\hat{f}_0, \Delta) := k_0$

Set $\hat{w}$ s.t. $(\hat{w}_j = \hat{f}_0(j))_{j \in [m]}$ (full dom. eval)

$w = \hat{w} \cdot H = (\langle \hat{w}, H_i \rangle)_{i \in [n]}$

$R_0 = (w_i, w_i \oplus \Delta)_{i \in [n]}$

else $\sigma = 1$ (Receiver.): $(\hat{f}_1, e) := k_1$

Set $b = e \cdot H = (\langle e_j, H_i \rangle)_{i \in [n]}$

$\hat{v} = (\hat{v}_j = \hat{f}_1(j))_{j \in [m]}$

$v = \hat{v} \cdot H = (\langle \hat{v}, H_i \rangle)_{i \in [n]}$

$R_1 = (b, v)$

Correctness:

$$v_i = \langle \hat{v}, H_i \rangle = \sum_{j \in [m]} \hat{f}_1(j) \cdot H_{ij} = \sum (\hat{f}_0(j) \oplus e_j \Delta) \cdot H_{ij}$$

$$= \underbrace{(\sum \hat{f}_0(j) H_{ij})}_{w_i} \oplus \Delta \underbrace{\sum e_j H_{ij}}_{b_i}$$

$v_i = w_i \oplus b_i \Delta$

Need to argue $\approx_c (R_0, R_1) \leftarrow \text{CorGen}$

$(w_i)_{i\in[n]}, \Delta \quad , \quad (b_i)_{i\in[n]} \quad , (w_i \oplus b_i \Delta)_{i\in[n]}$

uniform

PCG:

$(w_i)_{i\in[n]}, \Delta \quad , \quad (b_i)_{i\in[n]} \quad , (w_i \oplus b_i \Delta)_{i\in[n]}$

$\approx_c U_1$ By LPN

$\sum_{j\in[m]} \hat{f}_0(j) \cdot H_{ij}$

MPFSS pseudorandomness

$\approx_c \sum U_\lambda \cdot H_{ij}$

H must be full-rank w. overwhelming prob. for LPN

$\approx_s U_\lambda$

Security:

Receiver: given $K_1 \longrightarrow (b_i, w_i \oplus b_i \Delta)$

Ideal: (Rsample(R_1))

$\Delta \leftarrow \{0,1\}^\lambda$

$R_0 = (w_i, w_i \oplus \Delta)_{i \in [n]}$

Real

$\Delta \leftarrow \{0,1\}^\lambda$

By correctness, $R_0 = (w_i, w_i \oplus \Delta)$

Identical

Conditioned on K_1, R_0 is set by Δ

Sender: given $K_0 \longrightarrow (w_i, w_i \oplus \Delta)_{i \in [n]}$

Ideal: (Rsample(R_0)):

$b \leftarrow \{0,1\}^n$

$R_1 = (b_i, w_i \oplus b_i \Delta)_{i \in [n]}$

Real

$e \leftarrow HW_{t,m}$, $b = e \cdot H$

⋮

$\hat{f}_0, \hat{f}_1 \leftarrow \text{MPFSS}(f_{e\Delta})$

⋮

$R_1 = (b_i, w_i \oplus b_i \Delta)_{i \in [n]}$

depends on e

$\Rightarrow$ Hybrid: $\hat{f}_0 \leftarrow \text{SimFSS}(1^\lambda)$

Efficiency: (seed size)

Pay to transmit FSS keys for t-pt. fn.

$$\Rightarrow \underbrace{t}_{\approx\lambda}\cdot\lambda\log\underbrace{m}_{\lambda^{c}} \in O(\lambda^2\log\lambda)$$

Correlation size $= \lambda\cdot\underbrace{n}_{\lambda^{c'}} = O(\lambda^{c'+1})$

Protocol for setup [Ds17]: $O(t\log m)$ OTs

$\Rightarrow O(\lambda^2\log\lambda)$ comm.