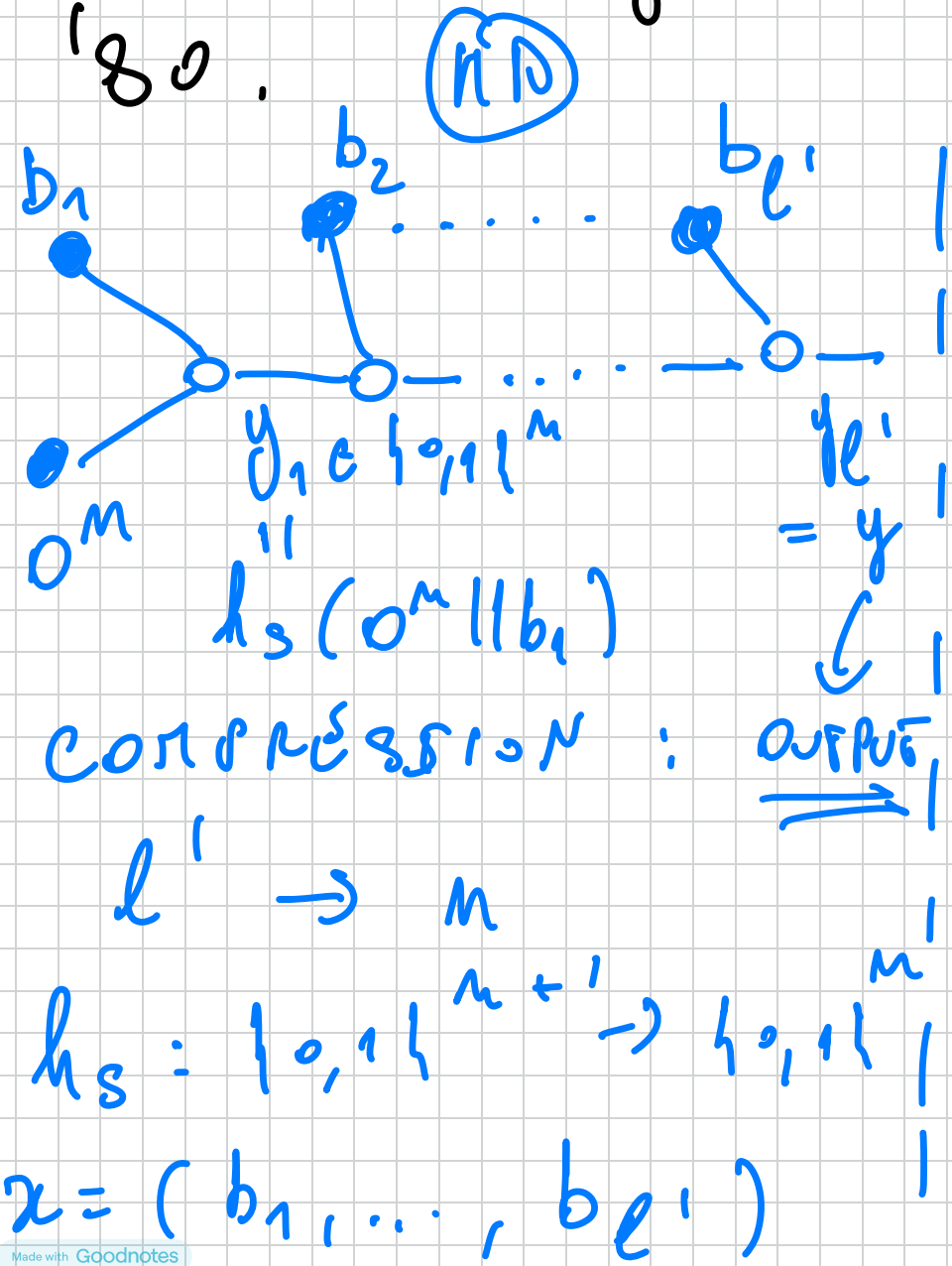
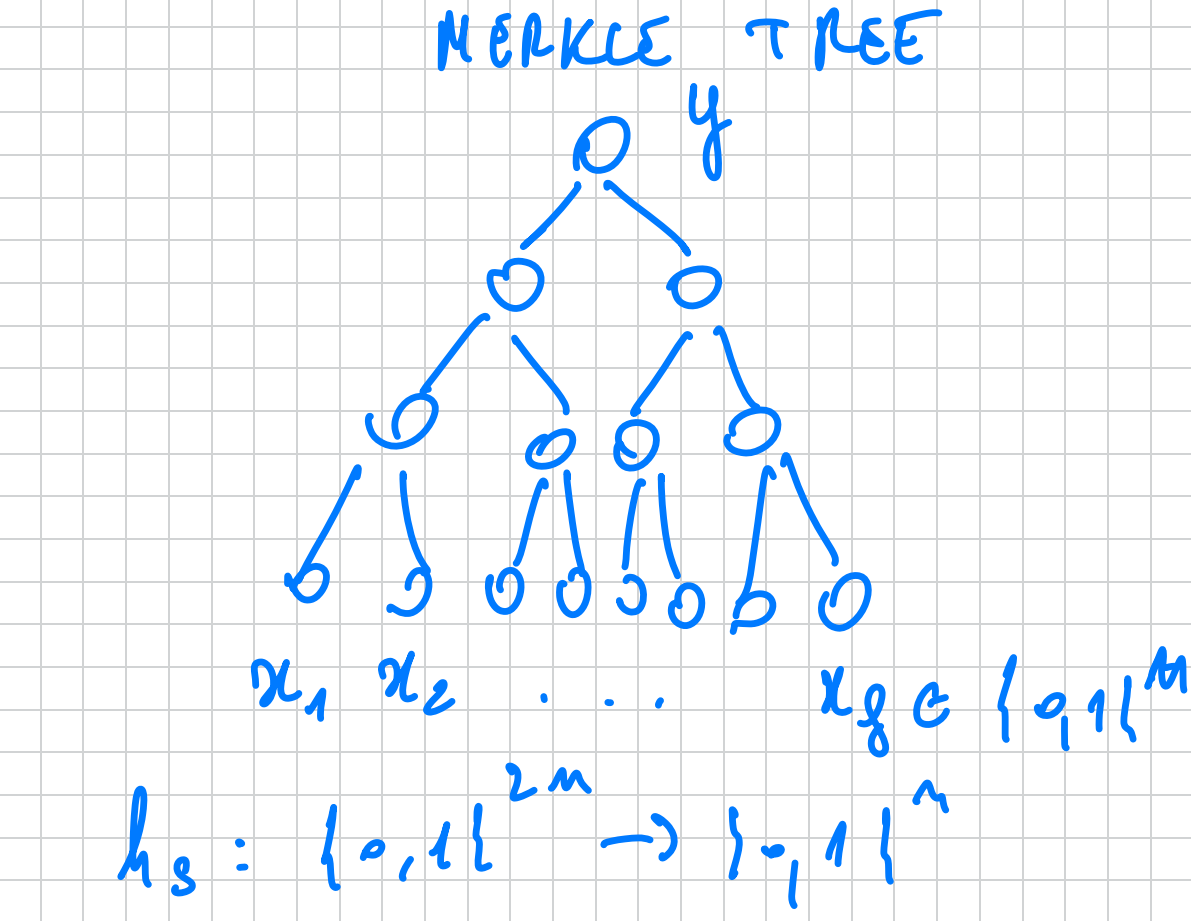
Let's start with step 2. It comes from a result by Merkle and Damgård around '80.



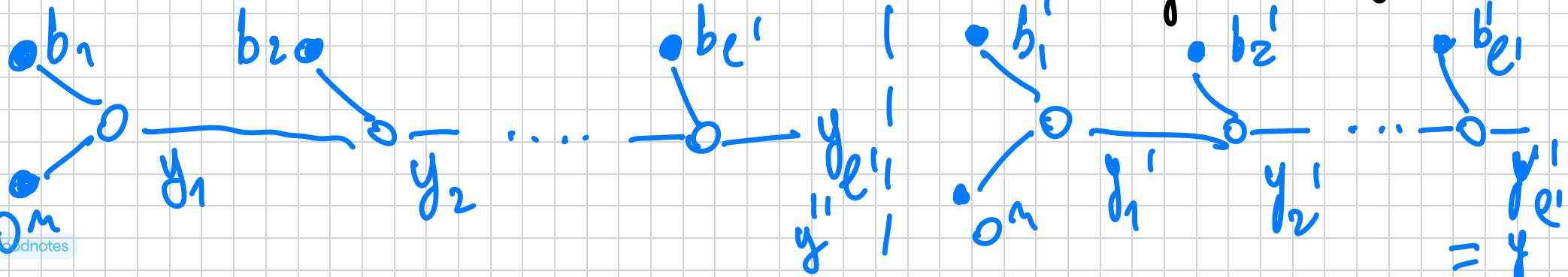


THM The MD construction goes a CRH H' from $\ell'(\lambda)$ into $n(\lambda)$ assuming H is CRH from $\ell(\lambda) = n+1$ into $n(\lambda)$ bits.

Proof. We assume FIL $\ell'(\lambda)$ for now. Say $\exists$ PPT A' finding a collision:

$$x = (b_1, \ldots, b_{\ell'}) \neq (b'_1, \ldots, b'_{\ell'}) = x'$$

s.t. $h'_s(x) = h'_s(x')$ where $h'_s(\cdot)$ is the MD construction using $h_s(\cdot)$.



Running backwards let i be the largest index s.t. $(b_i, y_{i-1}) \neq (b_i', y_{i-1}')$.

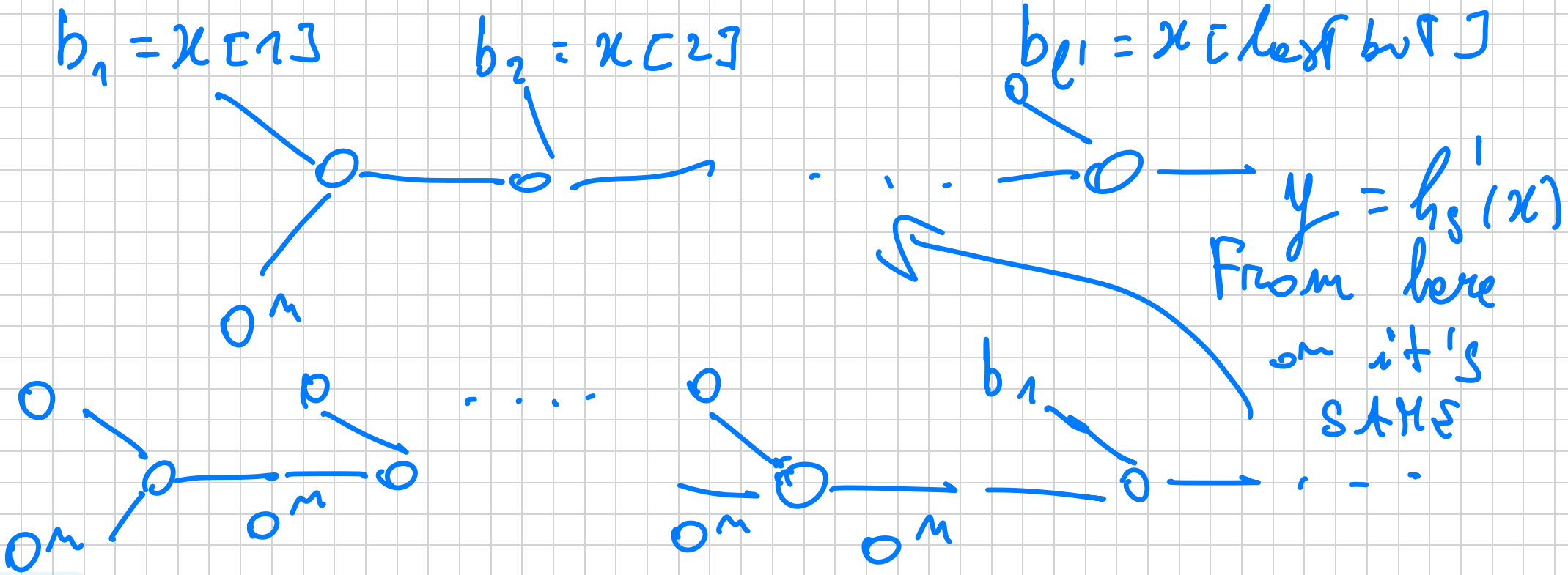
Because this is the largest i, it must be the case that $h_s(b_i \| y_{i-1}) = h_s(b_i' \| y_{i-1}')$

$\Rightarrow$ $b_i \| y_{i-1}$, $b_i' \| y_{i-1}'$ are a collision for $h_s(\cdot)$.

This observation immediately implies a PPT reduction from A breaking H. ∎

Why FIL? Because the above construction is actually not secure for VIL.

In fact, consider $\mathcal{H}$ with the property that $h_s(0^{n+1}) = 0^n$ for every s. Now, for every x: $h'_s(0^n \| x) = h'_s(x)$.



The fix: Make sure that no "legal" input is a suffix of another "legal" input.

"Legal": Encode it with this. Assume for simplicity $h_s : \{0,1\}^{2n} \to \{0,1\}^n$. Then if $x = (x_1, \dots, x_{\ell'})$ encode x to

$(x_1, \dots, x_{\ell'}, \leq \ell' >_2)$

↳ binary encoding of ℓ' using n bits.

T1+M The above strengthening of MD vs

a CRH for VIL.

Proof. Let A' be a PPT adversary finding a collision $x \neq x'$ s.t.

$$h'_s(x) = h'_s(x').$$

Consider two cases:

1) $|x| = |x'|$. The proof is as before.

2) $|x| \neq |x'|$. Say x is made of l_1 blocks and x' is made of l_2 blocks. Then, $\langle l_1 \rangle \neq \langle l_2 \rangle$ and we have found a collision on $h_s(\cdot)$! ☐

It remains to instantiate $h_s(\cdot)$. Two approaches:

1) Practice: Use AES (or similar):

$$H(\underbrace{x_1}_{n}, \underbrace{x_2}_{n}) = AES_{x_1}(x_2) \oplus x_2$$

$2n \to n$ COMPRESSION.

This can be proven secure assuming AES is an IDEAL CIPHER (i.e. random permutation for every choice of the key!).

2) Theory: Instantiate $h_s(\cdot)$ from your favourite hard problem (FACTORING, DL, ...)

Let $(\mathbb{G}, g, q)$ be a cyclic group where DL is hard, but q needs to be PRIME.

Say $g_1 = g$, and $g_2 (= g^x)$

$$h_{g_1, g_2}(x_1, x_2) = g_1^{x_1} g_2^{x_2} \in \mathbb{G}$$

$$\mathbb{Z}_q^2 \longrightarrow \mathbb{G} \quad (\simeq \lambda \text{ bits of compression})$$

Why is this collision resistant? Assume not: $\exists$ PPT A that outputs (x_1, x_2)

and (x_1', x_2') s.t. $(x_1, x_2) \neq (x_1', x_2')$

$$g_1^{x_1} g_2^{x_2} = g_1^{x_1'} g_2^{x_2'}$$

$$\Rightarrow g_2^{x_2 - x_2'} = g_1^{x_1' - x_1}$$

WLOG assume $x_2 \neq x_2'$, otherwise $x_1 = x_1'$.

$$\Rightarrow g_2 = g_1^{(x_1' - x_1) \cdot (x_2 - x_2')^{-1}}$$

$x_2 \neq x_2'$ and the inverse exists as q is PRIME!

$\Rightarrow (x_1' - x_1)(x_2 - x_2')^{-1}$ is the DL of f_2!

This gives a reduction to DL.