Automated Search for Round 1 Differentials for SHA-1

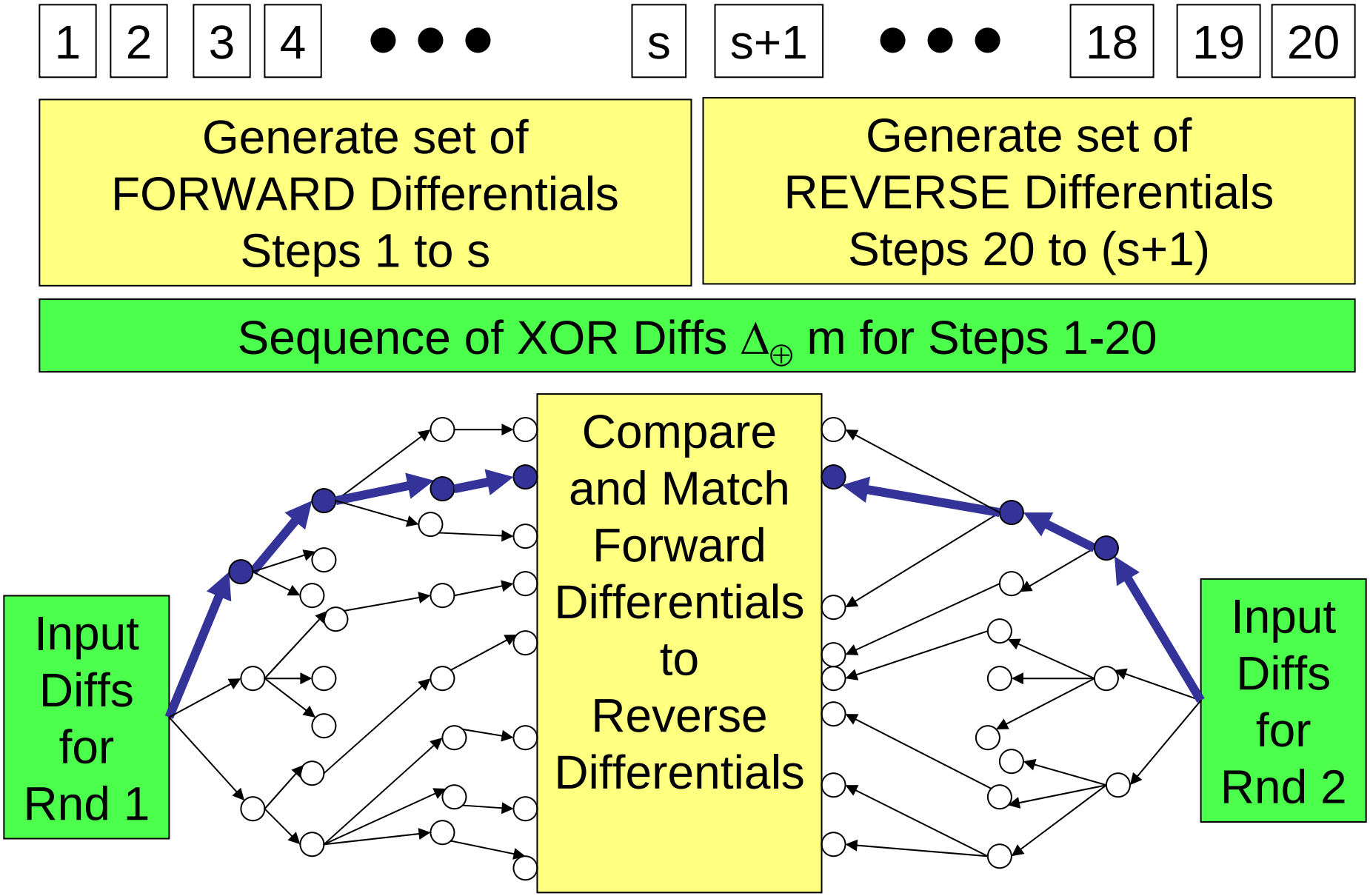
Phil Hawkes, Michael Paddon, Greg Rose

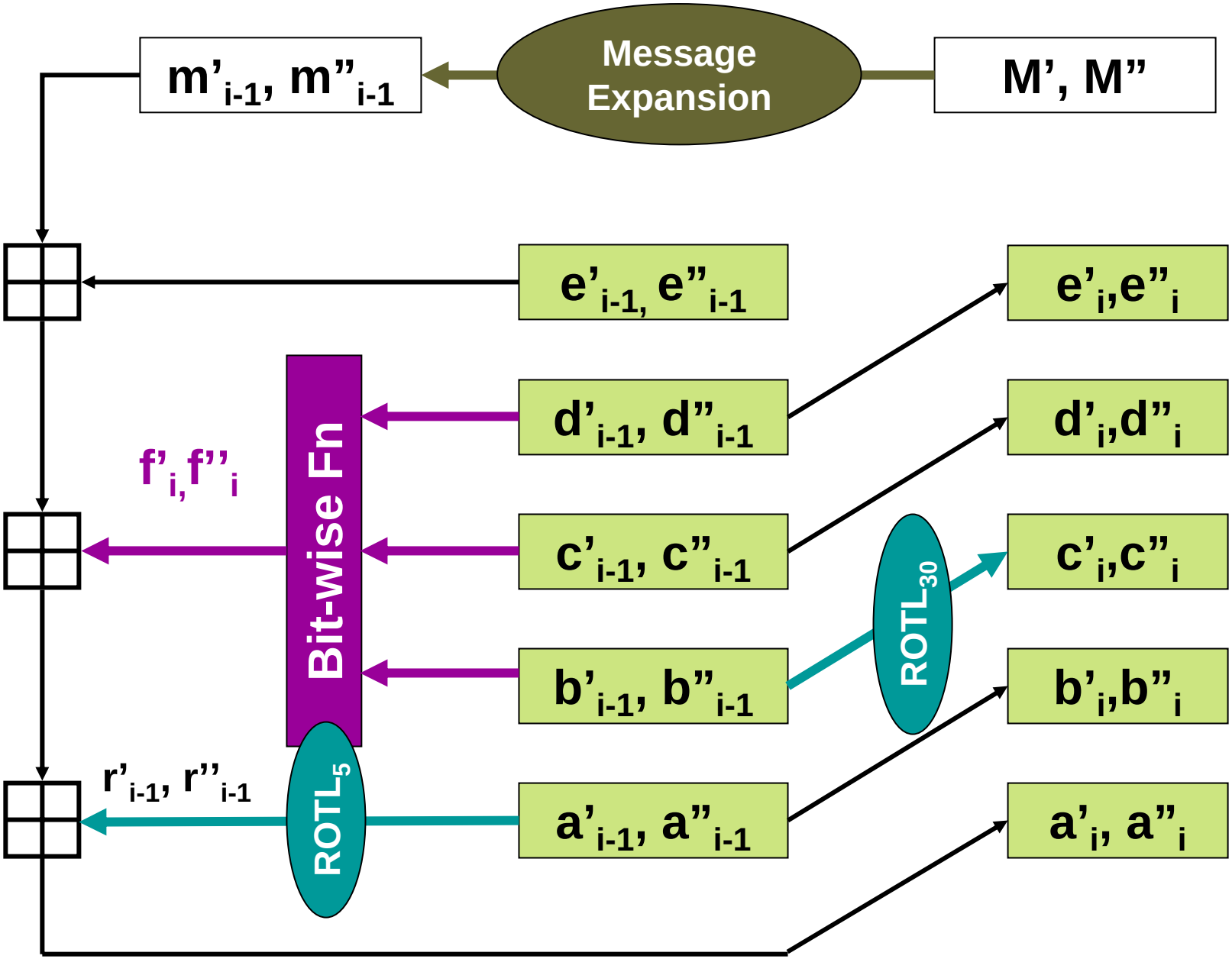
QUALCOMM

{phawkes,mwp,ggr}@qualcomm.com

Motivation for Research

- Given:
  - Disturbance vector (XOR diffs in msg words),
  - Input difference to Round 1,
  - Input difference for Round 2, …
- …is there a differential path?
- Which Round 1differential path is optimal?
  - E.g. improvements to MD5 attacks
- How do we find optimal paths?
  - **Automate search**!

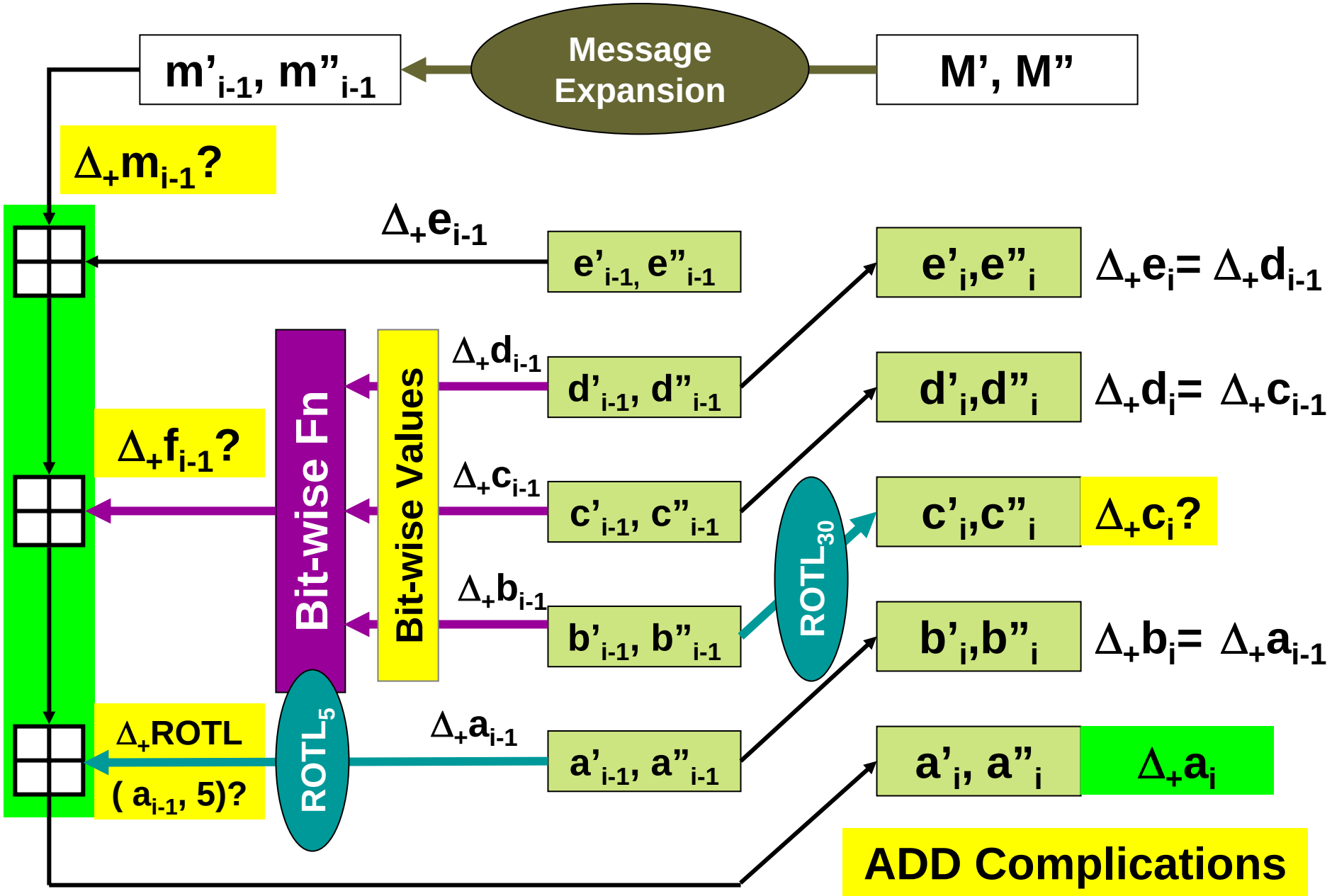

1
2
3
4
s
s+1
18
19
20
Generate set of FORWARD Differentials Steps 1 to s
Generate set of REVERSE Differentials Steps 20 to (s+1)
Sequence of XOR Diffs $\Delta_{\oplus}$ m for Steps 1-20
Input Diffs for Rnd 1
Compare and Match Forward Differentials to Reverse Differentials
Input Diffs for Rnd 2

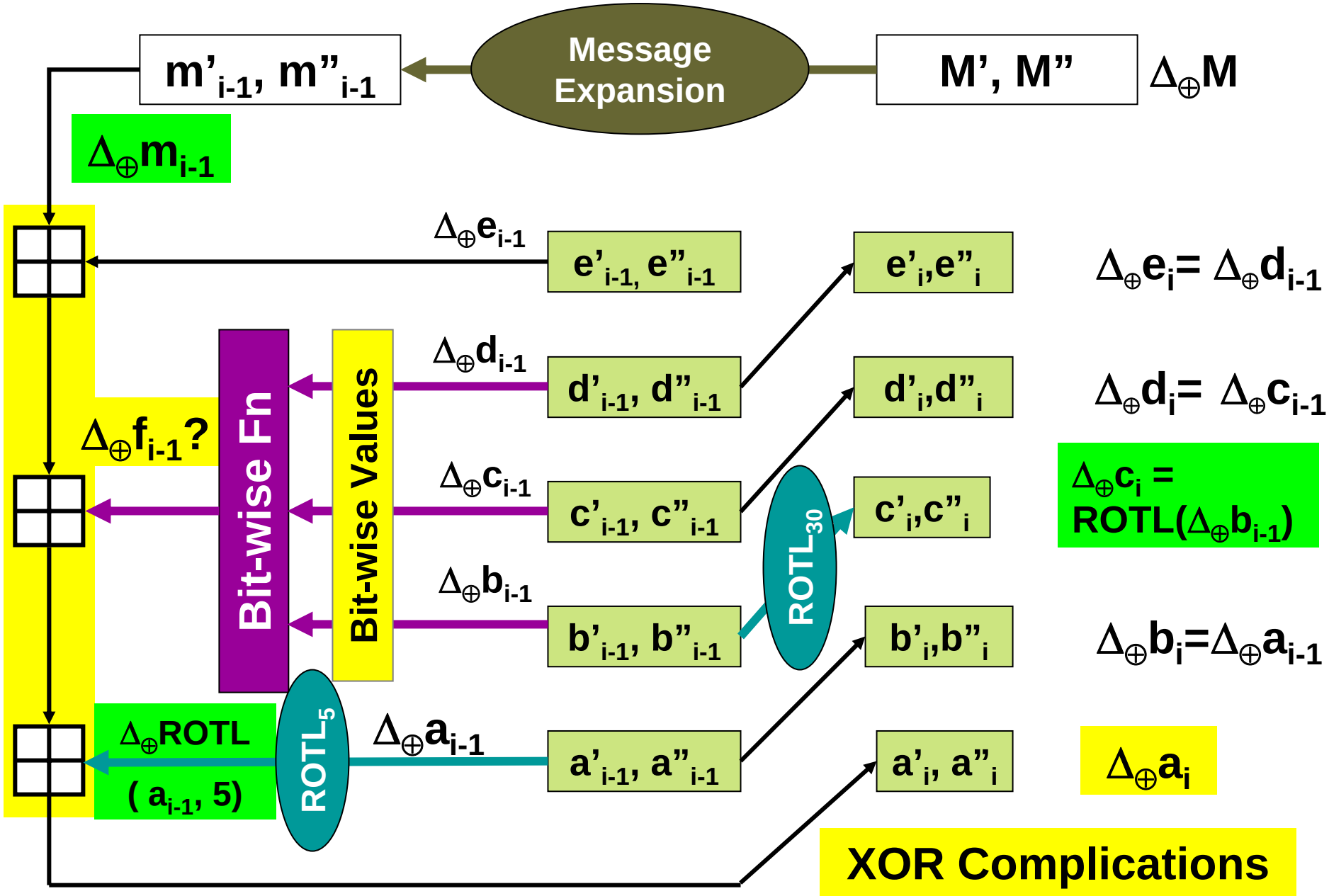


Phil Hawkes
phawkes@qualcomm.com

ADD & XOR Differences

- **ADD difference**
  - $\Delta_{+}X = X'' - X'$ (mod 2^{32})
- **XOR Difference**
  - $\Delta_{\oplus}X = X'' \oplus X'$
- **Properties**
  - $\Delta_{+}(X+Y) = \Delta_{+}X + \Delta_{+}Y$
  - $\Delta_{\oplus}(X \oplus Y) = \Delta_{\oplus}X \oplus \Delta_{\oplus}Y$
  - $\Delta_{\oplus}ROTL(X,r) = ROTL(\Delta_{\oplus}X, r)$: r *fixed*


m'i-1, m"i-1
Message Expansion
M', M"
Δ+mi-1?
Δ+ei-1
e'i-1, e"i-1
e'i,e"i
Δ+ei= Δ+di-1
Δ+di-1
d'i-1, d"i-1
d'i,d"i
Δ+di= Δ+ci-1
Δ+fi-1?
Bit-wise Fn
Bit-wise Values
Δ+ci-1
c'i-1, c"i-1
c'i,c"i
Δ+ci?
ROTL30
Δ+bi-1
b'i-1, b"i-1
b'i,b"i
Δ+bi= Δ+ai-1
Δ+ROTL
(ai-1, 5)?
ROTL5
Δ+ai-1
a'i-1, a"i-1
a'i, a"i
Δ+ai
ADD Complications


m'i-1, m"i-1
Message Expansion
M', M"
ΔM
ΔmI-1
ΔeI-1
e'I-1, e"I-1
e'I,e"I
ΔeI= ΔdI-1
ΔdI-1
d'I-1, d"I-1
d'I,d"I
ΔdI= ΔcI-1
ΔfI-1?
Bit-wise Fn
Bit-wise Values
ΔcI-1
c'I-1, c"I-1
ROTL30
c'I,c"I
ΔcI = ROTL(ΔbI-1)
ΔbI-1
b'I-1, b"I-1
b'I,b"I
ΔbI=ΔaI-1
ΔROTL
(aI-1, 5)
ROTL5
ΔaI-1
a'I-1, a"I-1
a'I, a"I
ΔaI
XOR Complications

Nabla representation ∇X

- $\nabla X[j]$ =
  - @ if $\mathbf{X''[j]} \neq \mathbf{X'[j]}$
  - **+** if $(\mathbf{X''[j]},\mathbf{X'[j]}) = (1,0) \leftrightarrow \mathbf{X''[j]} - \mathbf{X'[j]} = +1$
  - **-** if $(\mathbf{X''[j]},\mathbf{X'[j]}) = (0,1) \leftrightarrow \mathbf{X''[j]} - \mathbf{X'[j]} = -1$
  - ***** if $\mathbf{X''[j]} = \mathbf{X'[j]}$
  - **0** if $\mathbf{X''[j]} = \mathbf{X'[j]} = 0$
  - **1** if $\mathbf{X''[j]} \neq \mathbf{X'[j]} = 1$
- $\Delta_{+}\mathbf{X} = \sum_{+,-} \nabla X[j]\ 2^{j}$

Example

```
Bit3322222222211111111111
   1098765432109876543210987654321 0
X'=0011101010101010010110101010100 0
X"=1010101001101001010110010010100 0
∇X=+01-1010-+1010-+010110-+-0101000 0
Δ⊕=1001000011000011000000111000000 0
```

$\Delta+= +2^{31} -2^{28} -2^{23} +2^{22} -2^{17} +2^{16} -2^{9} +2^{8} -2^{7}$

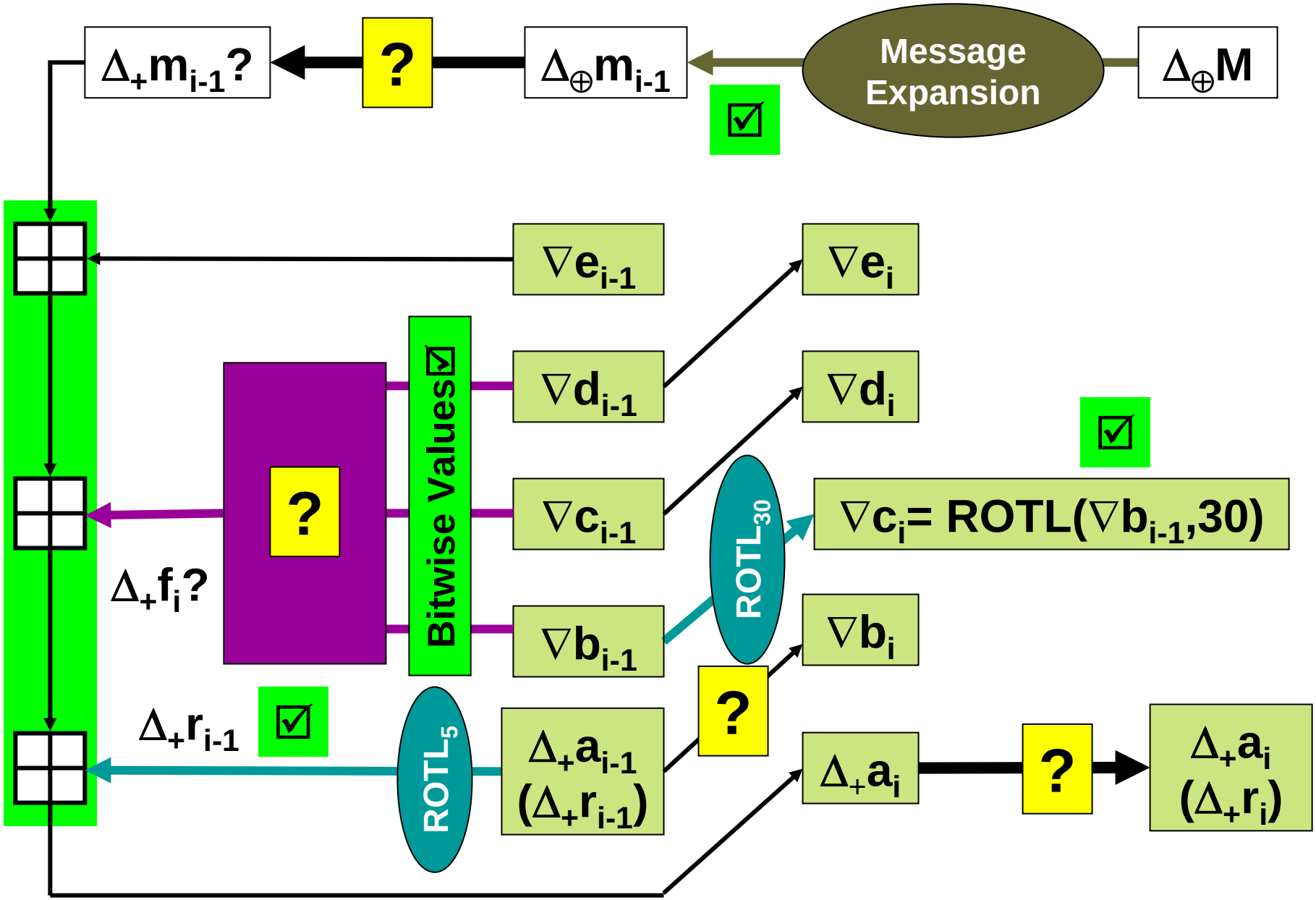
= 1874787968 = 0x6FBEFE80

= 01101111 10111110 11111110 10000000

- **X', X" → ∇X → Δ_{+}X, $\Delta_{\oplus}$X**

Observations

- ∇ ROTL(X,r) = ROTL(∇X,r)
- XOR diffs only where **`@,+,-`**
  - **`@,+,-`** = **dynamic** bits
  - **`*,1,0`** = **static** bits
- ADD diff fully defined by **`+,-`** (& **`@`** MSB only)
- Values of static bits don't affect XOR diff or ADD diff
  - Static bits only of interest in IF function



Phil Hawkes
phawkes@qualcomm.com

Branching Points

- Given **XOR** diff, ∃ multiple **ADD** diffs
- Given **ADD** diff, ∃ multiple **ADD** diffs for **ROTL**
- Given **ADD** diff, ∃ multiple **XOR** diffs
- Given **XOR & ADD diff** in, ∃ multiple **ADD** diff out (IF)

Know:	Want:	Fn	Choice:
$\Delta_{\oplus}m$	$\Delta_{+}m$		?
$\Delta_{+}a$	$\Delta_{+}r$	ROTL	?
$\Delta_{+}a$, $\Delta_{+}r$	∇b		?
∇b,∇c, ∇d	$\Delta_{+}f$	IF	?

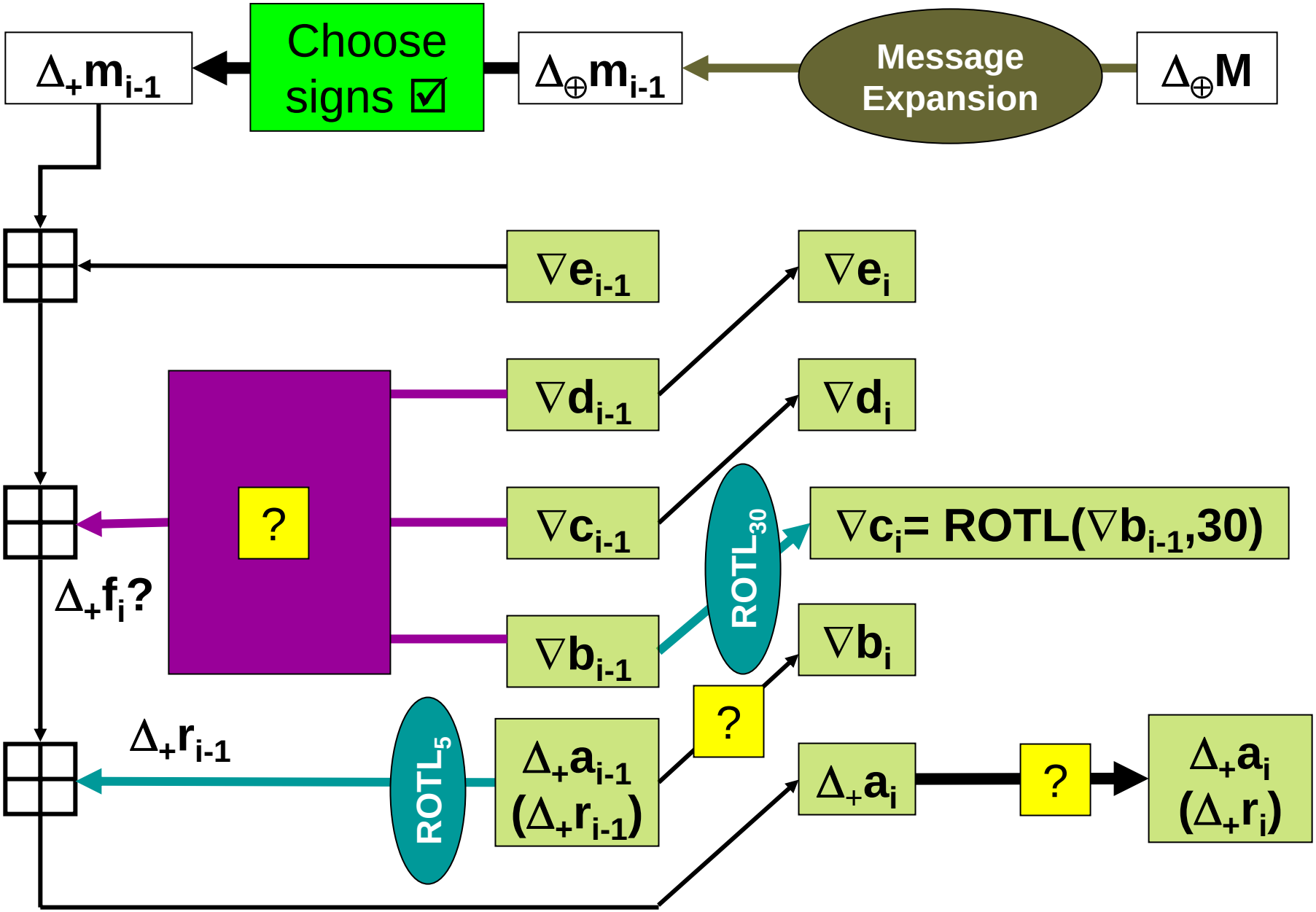
Given **XOR** diffs find **ADD** diffs

Bit33222222222…
10987654321 0…

$\Delta\oplus$=0001000011 00…0

∇0=*+*****++**…** $\Delta+=+2^{28}+2^{23}+2^{22}$
∇1=*+*****+-**…** $\Delta+=+2^{28}+2^{23}-2^{22}$
∇2=*+*****-+**…** $\Delta+=+2^{28}-2^{23}+2^{22}$
∇3=*+*****--**…** $\Delta+=+2^{28}-2^{23}-2^{22}$
∇4=*-*****++**…** $\Delta+=-2^{28}+2^{23}+2^{22}$
∇5=*-*****+-**…** $\Delta+=-2^{28}+2^{23}-2^{22}$
∇6=*-*****-+**…** $\Delta+=-2^{28}-2^{23}+2^{22}$
∇7=*-*****--**…** $\Delta+=-2^{28}-2^{23}-2^{22}$

Each is a distinct addition difference


$\Delta_+ m_{i-1}$
Choose signs ☑
$\Delta_\oplus m_{i-1}$
Message Expansion
$\Delta_\oplus M$
∇e_{i-1}
∇e_i
∇d_{i-1}
∇d_i
?
∇c_{i-1}
$\nabla c_i = ROTL(\nabla b_{i-1},30)$
$ROTL_{30}$
$\Delta_+ f_i$?
∇b_{i-1}
∇b_i
?
$\Delta_+ r_{i-1}$
$ROTL_5$
$\Delta_+ a_{i-1}$ ($\Delta_+ r_{i-1}$)
$\Delta_+ a_i$
?
$\Delta_+ a_i$ ($\Delta_+ r_i$)

Given $\Delta+=2^{28} + 2^{25}$ find XOR diffs

∇0=***+**+*…	Δ⊕=00010010…
∇1=***+*+-*…	Δ⊕=00010110…
∇2=***++--*…	Δ⊕=00011110…
∇3=**+*---*…	Δ⊕=00101110…
∇4=**+-**+*…	Δ⊕=00110010…
∇5=**+-*+-*…	Δ⊕=00110110…
∇6=**+-+--*…	Δ⊕=00111110…
∇7=*+--**+*…	Δ⊕=01110010…
∇8=*+--*+-*…	Δ⊕=01110110…
∇9=*+--+--*…	Δ⊕=01111110…
∇A=*+-*---*…	Δ⊕=01101110…
∇B=+---**+*…	Δ⊕=11110010…
∇C=----**+*…	Δ⊕=11110010…
∇D=+---*+-*…	Δ⊕=11110110…
∇E=----*+-*…	Δ⊕=11110110…

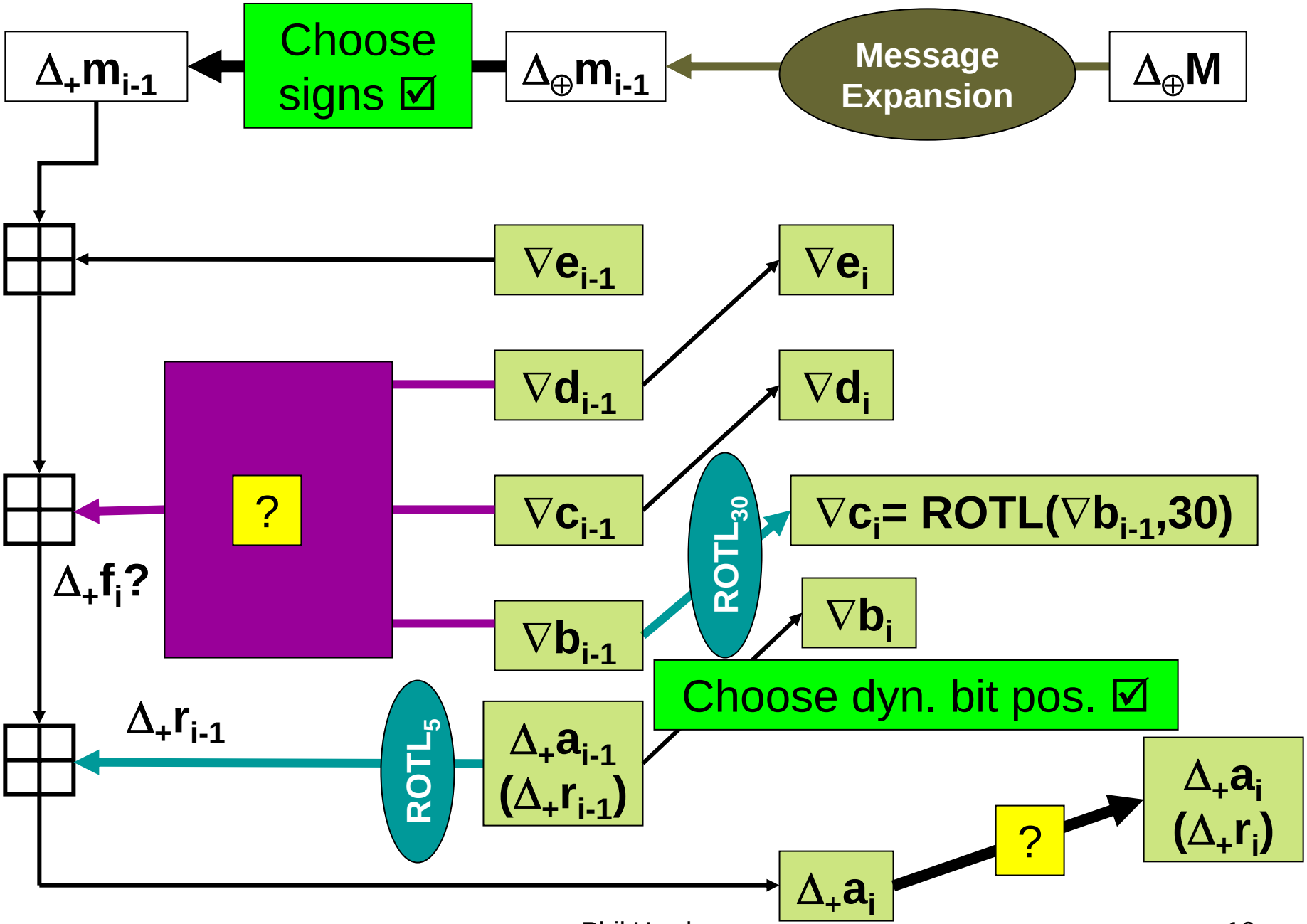
- Carry addition differences up to higher order bits
- Cancel with existing higher order differences

or…

- Add to higher order differences

etc

Phil Hawkes
phawkes@qualcomm.com

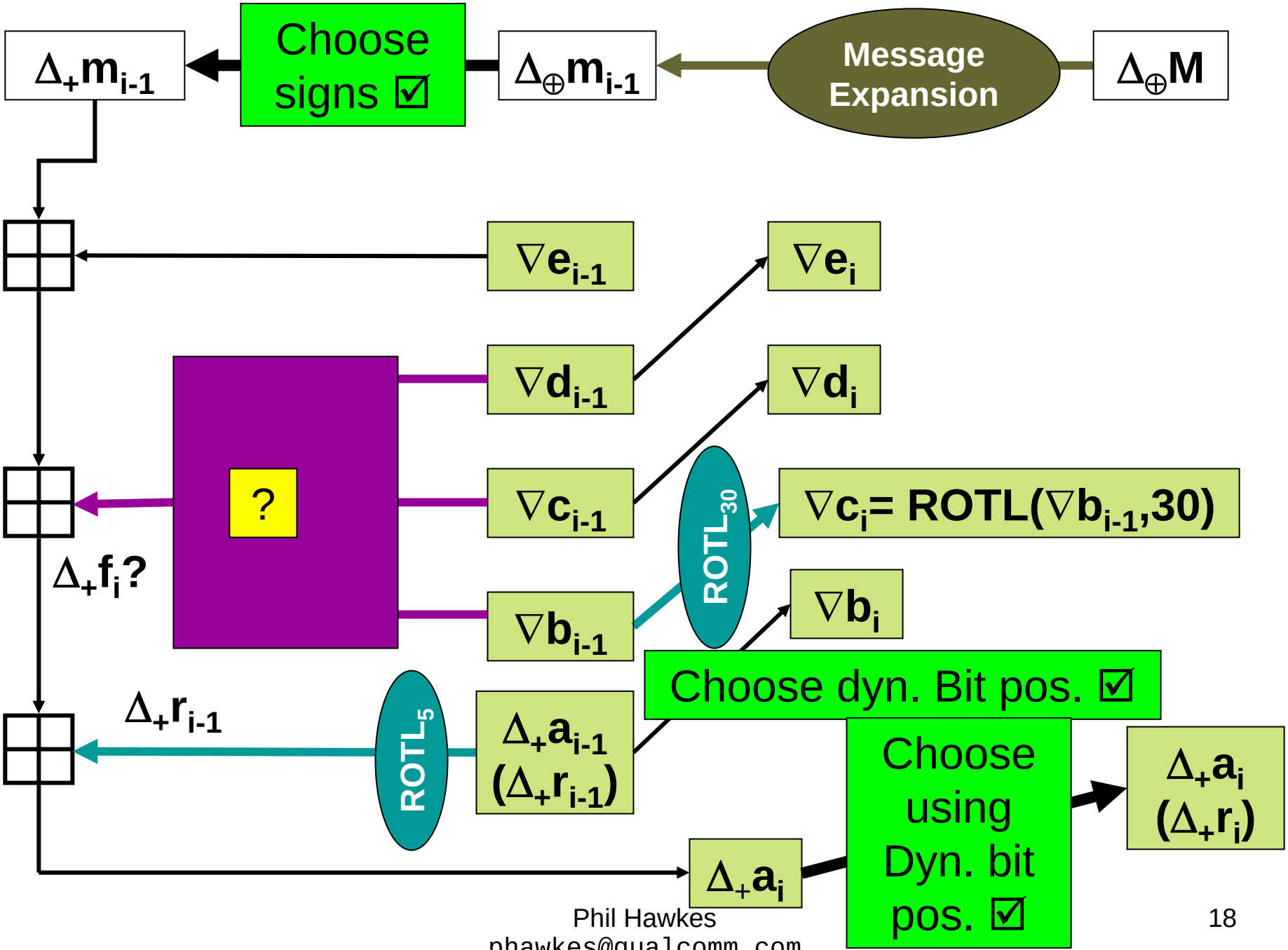


Phil Hawkes
phawkes@qualcomm.com

$\Delta_+a_{i-1} = 2^{28} + 2^{25}$, $\Delta_+ROTL(a_{i-1},5)=?$

$\nabla 0$=***+**+*...	$\nabla R0$=*+*...***+*	$=2^{30}+2^{1}$
$\nabla 1$=***+*+-*...	$\nabla R1$=+-*...***+*	$\cong \Delta_+R0$
$\nabla 2$=***++--*...	$\nabla R2$=--*...***++	$=2^{30}+2^{1}+2^{0}$
$\nabla 3$=**+*-**-*...	$\nabla R3$=--*...**+*-	$\cong \Delta_+R2$
$\nabla 4$=**+-**+*...	$\nabla R4$=*+*...**+-*	$\cong \Delta_+R0$
$\nabla 5$=**+-*+-*...	$\nabla R5$=+-*...**+-*	$\cong \Delta_+R0$
$\nabla 6$=**+-+--*...	$\nabla R6$=--*...**+-+	$\cong \Delta_+R2$
$\nabla 7$=*+--**+*...	$\nabla R7$=*+*...*+--*	$\cong \Delta_+R0$
$\nabla 8$=*+--*+-*...	$\nabla R8$=+-*...*+--*	$\cong \Delta_+R0$
$\nabla 9$=*+--+--*...	$\nabla R9$=--*...*+--+	$\cong \Delta_+R2$
∇A=*+-*-**-*...	∇RA=--*...*+-*-	$\cong \Delta_+R2$
∇B=+---**+*...	∇RB=*+*...+---*	$\cong \Delta_+R0$
∇C=----**+*...	∇RC=*+*...----*	$=2^{30}-2^{4}-2^{3}-2^{2}-2^{1}$
∇D=+---*+-*...	∇RD=+-*...+---*	$\cong \Delta_+R0$
∇E=----*+-*...	∇RE=+-*...----*	$\cong \Delta_+RC$ etc

Phil Hawkes
phawkes@qualcomm.com



Phil Hawkes
phawkes@qualcomm.com

IF function

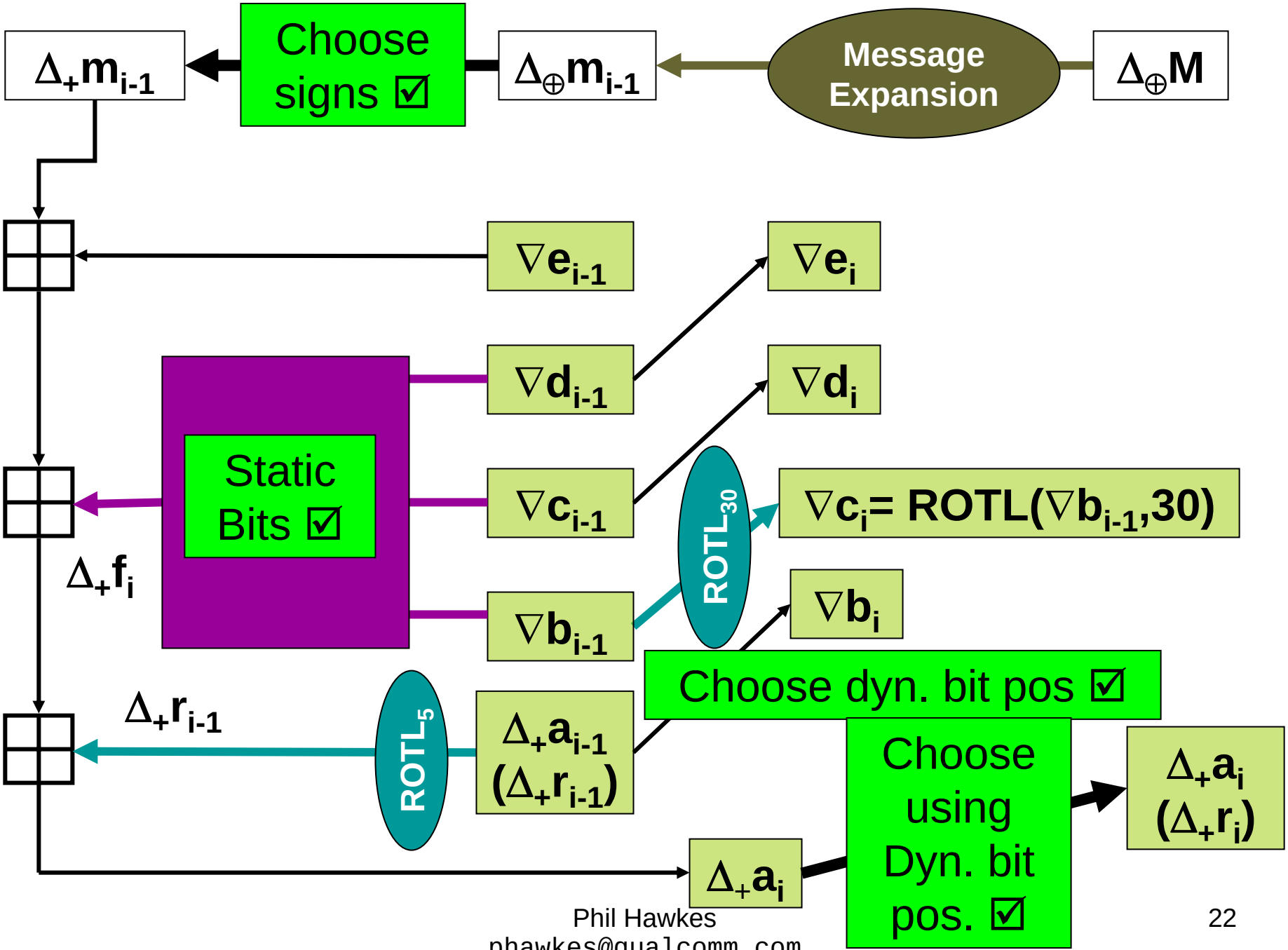
- What is known about inputs
  - Position of Dynamic & Static bits
  - Sign of Dynamic bits
- Static bits are left to specify
  - Initially ∇**b**[j]='***'
  - Assign values {0,1} to static bits of **b**[j],**c**[j],**d**[j]
  - static bits of **c**[j] and ∇**d**[j] may have been assigned earlier

b[j] is Static

b	**c**	**d**	**f**	Options
Static	Static	Static	Static	
Static	Static	**Dyn.**	**Dyn.**	**b**=0
			Static	**b**=1
Static	**Dyn.**	Static	Stat	**b**=0
			Dyn.	**b**=1
Static	**Dyn.**	**Dyn.**	**Dyn.**	**b**∈{*,0,1}

b[j] is Dynamic

<table>
<tr><th>b</th><th>c</th><th>d</th><th colspan="2">f</th><th>Options</th></tr>
<tr><td rowspan="3">Dyn.</td><td rowspan="3">Static</td><td rowspan="3">Static</td><td colspan="2">Static</td><td>c = d</td></tr>
<tr><td rowspan="2">Dyn.</td><td>{+, -}</td><td>(c,d)∈{ (0,1),(1,0) }</td></tr>
<tr><td>@</td><td>c ≠ d</td></tr>
<tr><td>Dyn.</td><td>Static</td><td>Dyn.</td><td colspan="2">Static/Dyn.</td><td>c∈{0,1}</td></tr>
<tr><td>Dyn.</td><td>Dyn.</td><td>Static</td><td colspan="2">Static/Dyn.</td><td>d∈{0,1}</td></tr>
<tr><td>Dyn.</td><td>Dyn.</td><td>Dyn.</td><td colspan="2">Static/Dyn.</td><td></td></tr>
</table>

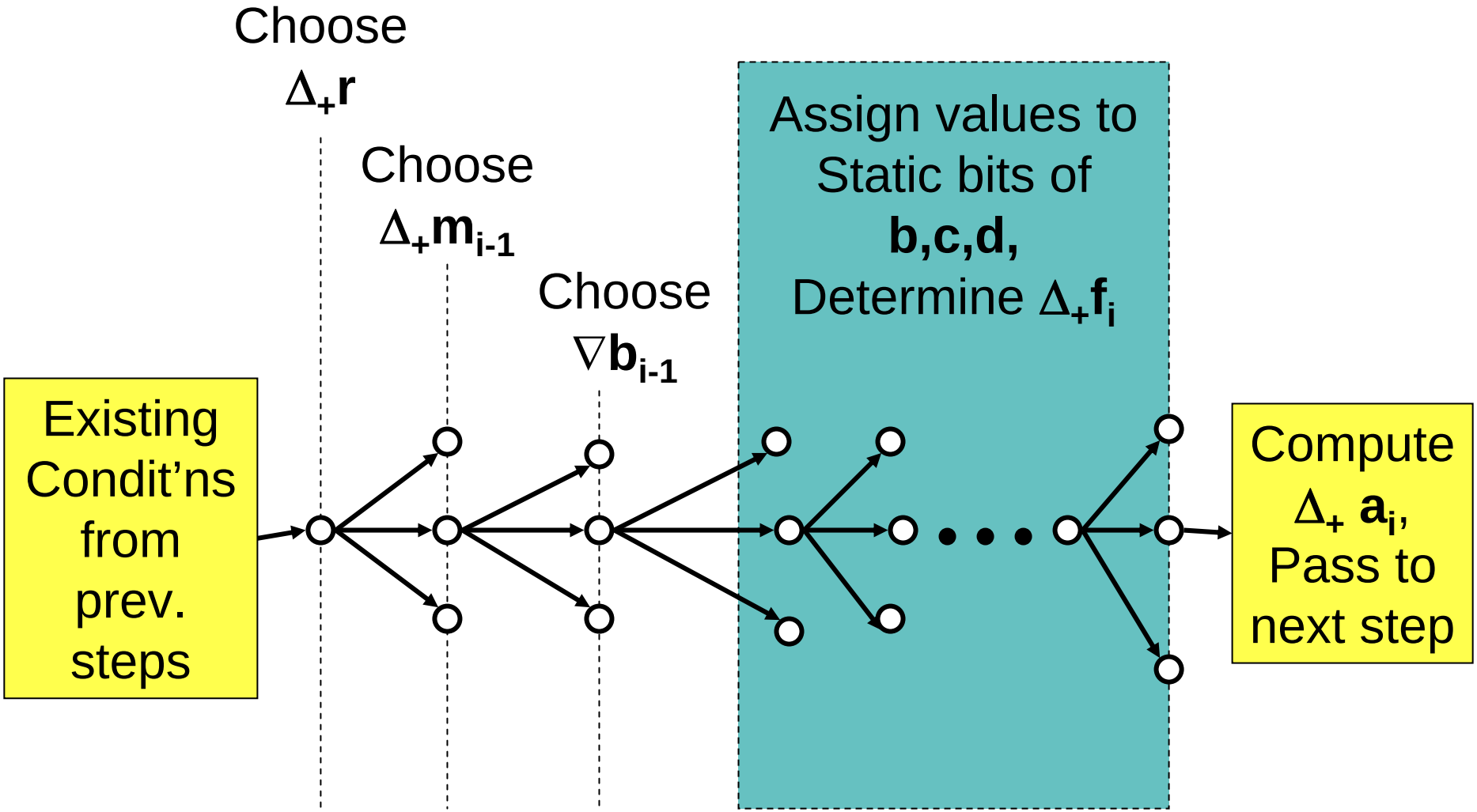


Phil Hawkes
phawkes@qualcomm.com

Options at Branching Points

Know:	Want:	Fn	Choice:
$\Delta_+ a_{i-1}$	$\Delta_+ r_{i-1}$	**ROTL**	Positions of Dynamic bits
$\Delta_\oplus m_{i-1}$	$\Delta_+ m_{i-1}$		"Sign" of dynamic bits {+,-}
$\Delta_+ a_{i-2}$, $\Delta_+ r_{i-2}$	∇b_{i-1}		Positions of Dynamic bits
∇b,∇c, ∇d	$\Delta_+ f$	**IF**	Values of Static Bits

Branching within Forward Step



Progress

- Implemented Forward search and Reverse search
- Designed comparison/matching
  - Not implemented at time of writing