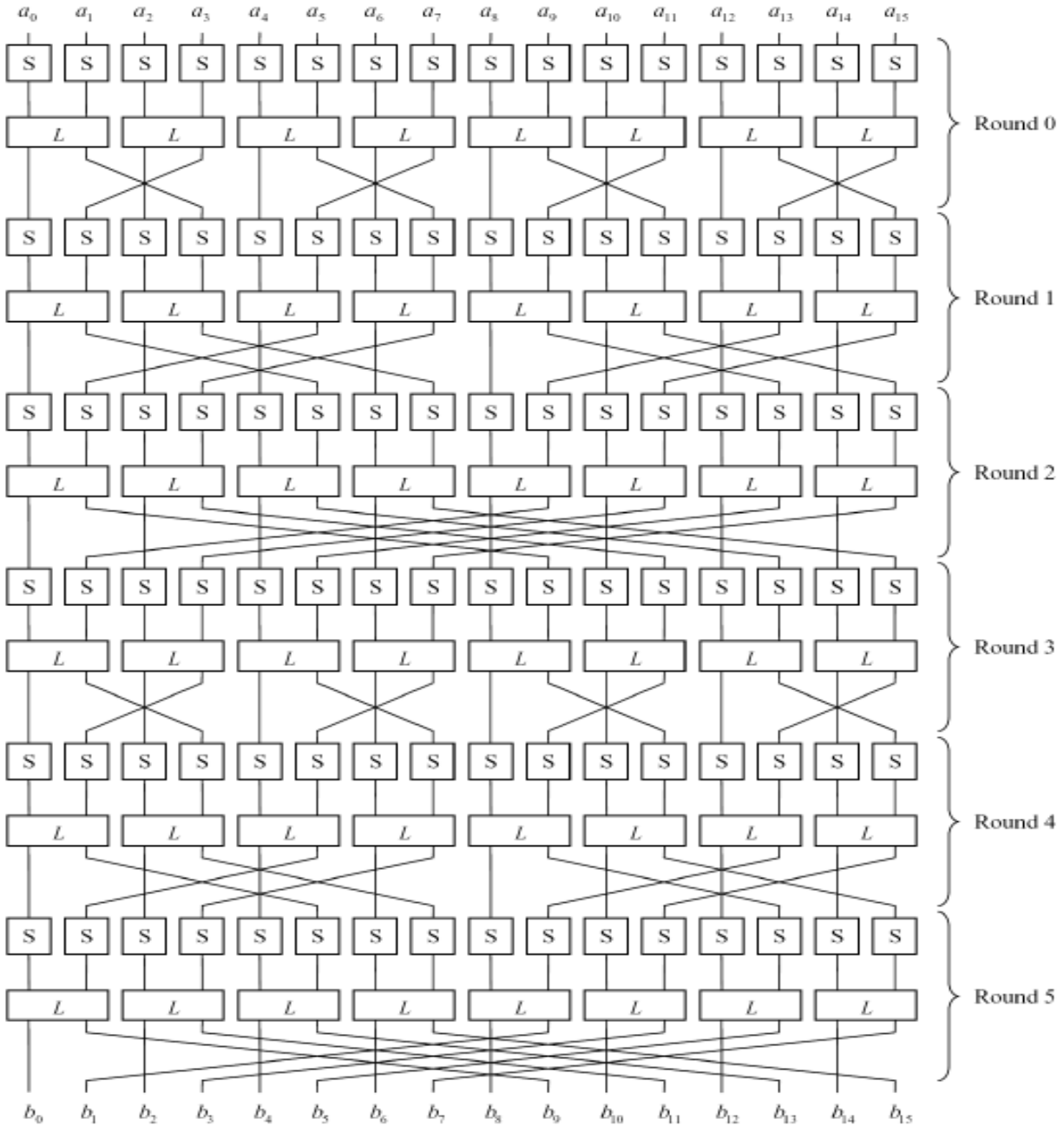
Re-arrange the round function for bit-slice (4D example):

d-1 different round functions for bit slice;

identical round functions for hardware



3. The Bijective Function E_8

Bijective function $\boldsymbol{E}_8$ –

EDP design: SPN + MDS code (to an 8-dimensional array)

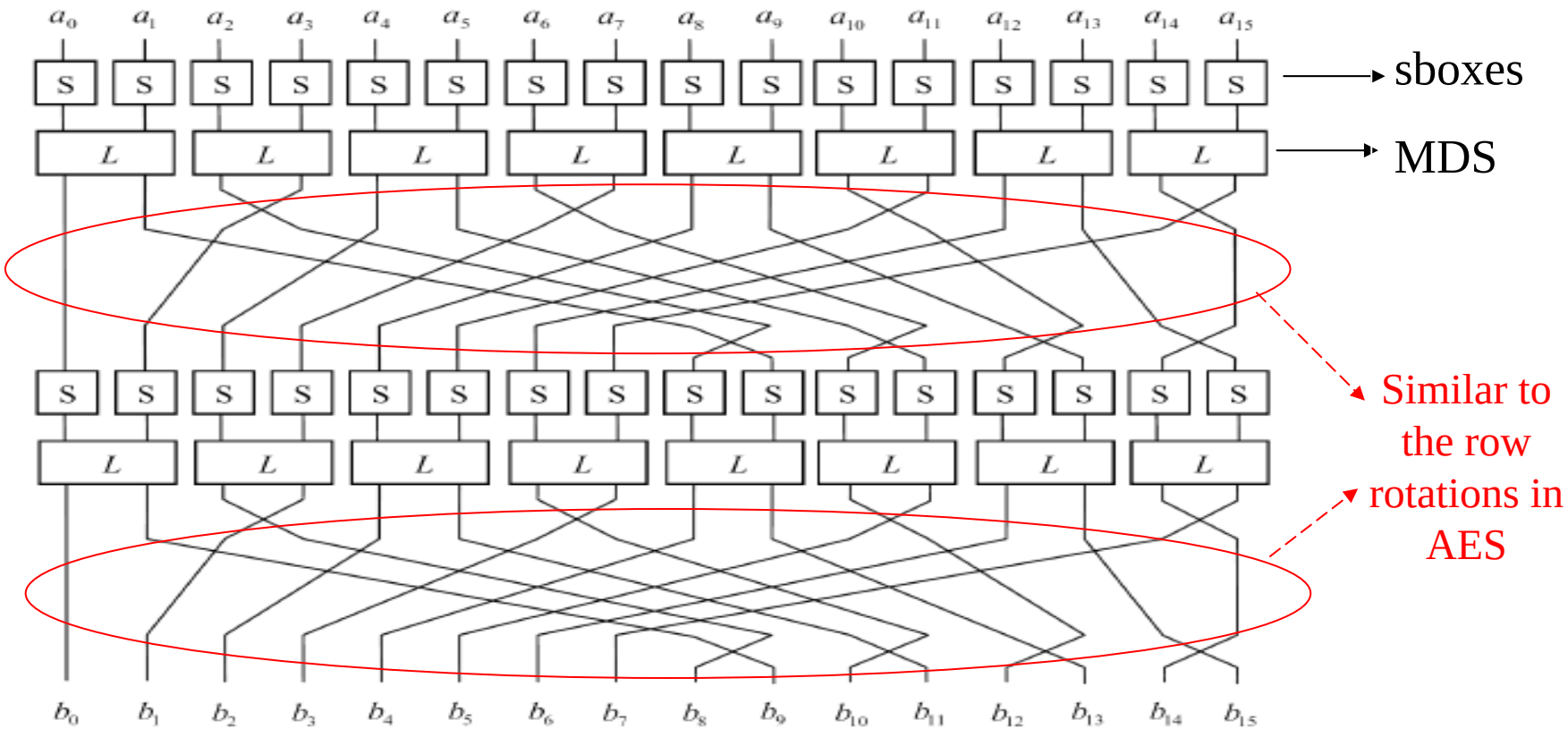
divide the 1024-bit input into 256 4-bit elements,
these 256 elements form an 8-dimension array

- Substitution: two 4-bit-to-4-bit Sboxes
  - Each round constant bit selects which Sbox is used
- Permutation: (4, 2, 3) MDS code over GF(2^4)
  - Applied along the ($\boldsymbol{i}$ mod 8)-th dimension in the $\boldsymbol{i}$-th round
- 35.5 rounds

3. The Bijective Function E_8

4-dimensional example $\boldsymbol{E}_4$ (two rounds, round constant not shown):

(identical round functions , except for different round constants)



6. Security Analysis of JH

Differential cryptanalysis

most powerful attack against hash function

a compression function in JH involves 9216 Sboxes.

any differential path in JH involves more than 600 active Sboxes, the large number of active Sboxes ensures that JH is strong against differential attack.

8. Advantages of JH

- JH will be more efficient on the incoming Intel microprocessors (2010)
  - Intel 256-bit Advanced Vector eXtensions (AVX), extension to SSE
  - 256 Sboxes can be computed in parallel

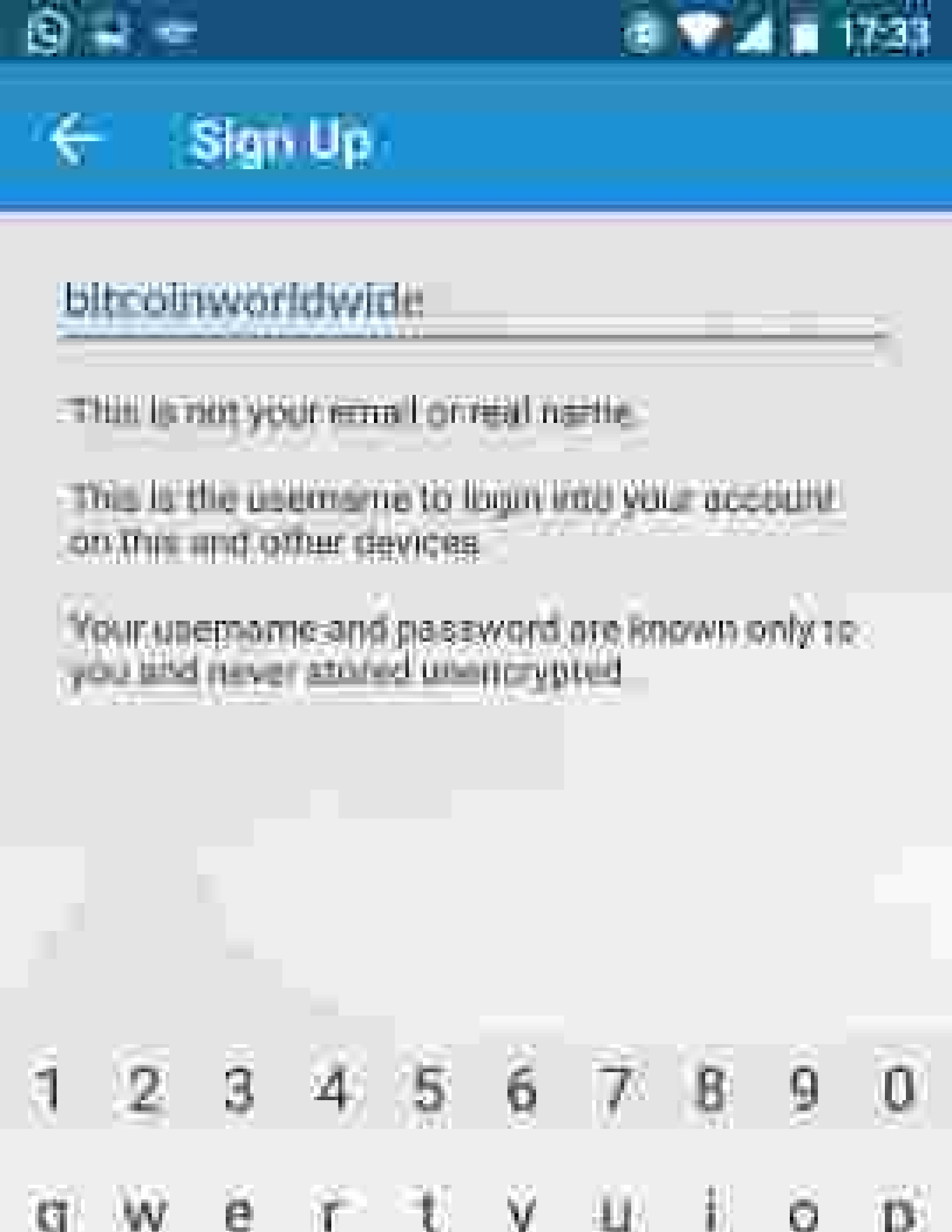
5. The Hash Function JH

- Iterated construction
  - message block size: 512 bits
  - hash value: 1024 bits
- Pad the message with at least 512 bits (message length included)
- Different initial hash values for different digest sizes
- Truncate the 1024-bit final hash value to 224, 256, 384 or 512 bits to obtain message digest

According to the official website of Fire Coin Global Station, Fire Coin Global Station is scheduled to open Dogecoin (DOGE) recharge operations on April 4 at 9:00. Open DOGE/USDT, DOGE/BTC, DOGE/ETH trading on April 4 at 17:00. Dogecoin (DOGE) withdrawals are open at 17:00 on 4 April.
Robinhood, a zero-fee trading platform, has just tweeted that it has launched a dog coin Dogecoin deal. The platform currently offers BTC, ETH, BCH, LTC and DOGE.
It's not just a dog coin convention, one delegate made it clear. DogeCoin is a serious cryptocurrency economics conference that focuses on gamification, performance and participatory elements.
DOGE has a positive message on the coin, ZG. TOP Online Dogecoin (DOGE). DOGE Charge: September 10th, 18:00 (UTC-8); DOGE/USDT Market Trading: September 11th, 15:00 (UTC-8)
Dogecoin recharge is now available, according to the FCoin announcement. FOne will open the DOGE/ETH, DOGE/USDT trading pairs at 18:00 today in the Dog Coin Zone.
The price of the popular dog coin DogeCoin soared after it was announced that it was about to go online on the Binance Exchange.
Restauran

ts in Maryland accept e-money dogecoin, MyFoxDC reported. Iron Rail Restaurant in Mount Savage, Maryland, officially accepts Dogecoin. Owner Terry Ii says the use of dogecoin has benefited restaurants, including the need not to pay for credit cards. Cumberland Times.
Dogecoin trend analysis In the past year, the popularity of Dogecoin has been very stable. As you can see in the figure below, the currency even gained a surge in popularity for the search term "dogecoin". In September 2018, Google users were very interested in Dogecoin. There were some less obvious peaks in July and December. At the beginning of 2019, the popularity was about the same as in the same period in 2018
Stellar (Star), Ripple (Ripple), and Dogecoin (Dog Coin) co-founder.
Metal Pay Marketplace has added coin security currency BUSD.
According to bitinfocharts, the recent hot dark coin Darkcoin has reached $4 million a day and has caught up with the $500 daily average for Dog Coin Dogecoin. Darkcoin is now the world's fourth largest virtual currency. DarkCoin (Dark Coin) has no pre-forecast.
Bitcoin cash, Dogecoin, Ethereum and

Ripple.
Elon Musk, co-founder of Tesla and SpaceX, tweeted again today about the dog coin "Is Dogecoin really an effective form of money?" "
Substitute money is the representative of metal currency, which is usually issued by the government or bank instead of metal currency circulation of paper money. This substitute currency is in fact a tradable real currency receipt, such as the cross-country of the Northern Song Dynasty, early bank bills.
Dogs in China community action frequently, coin security has been free to coins, and the official twt publicity, ok also in close cooperation with the community. Can you tell me what you think about dogecoin dog coin follow-up?
Blockchain payment platform Metal Pay has acquired the multi-functional EOSIO platform Blox.io. Bloks.io originally launched as a simple chunk browser for EOS, it has been expanded to support multiple networks of EOSIO platforms. A Metal Pay spokesman said Bloks.io was the company's first and only block browser acquisition. With the deal, Metal Pay is expected to benefit from a large number of real token holders on Blox.io. (Cointelegraph)


17:33
Sign Up
bloodinworldwide
This is not your email or real name.
This is the username to login into your account on this and other devices.
Your username and password are known only to you and never stored unencrypted.
1 2 3 4 5 6 7 8 9 0
q w e r t y u i o p

2. JH Compression Function Structure

$M^{(i)}$: m bits

$H^{(i)}$: $2m$ bits

New, simple

efficient

=> does not discard

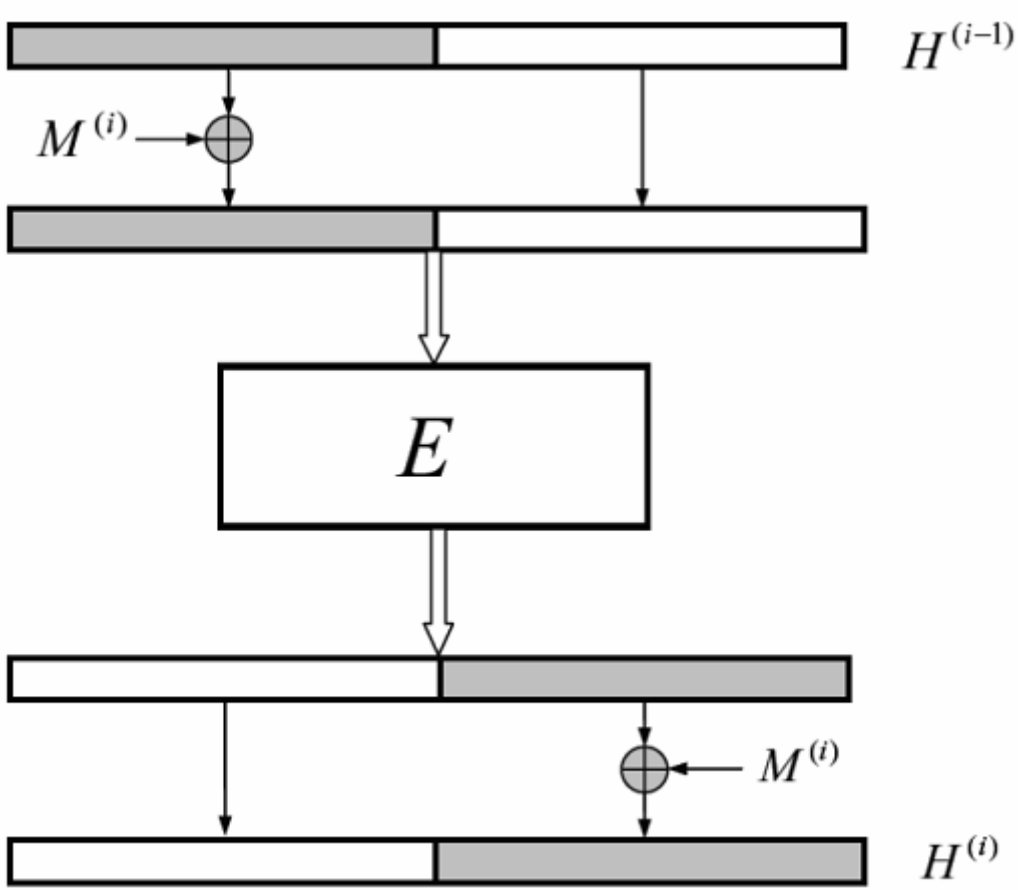
part of the output of ***E***

easy to analyze

=> no extra variables

being introduced into

the middle of ***E***



4. Bit-slice Implementation of E_8

The bit-slice implementation of $\boldsymbol{E_8}$ makes full use of the 128-bit SIMD architecture (powerful SIMD is available on many platforms):

128 Sboxes can be computed in parallel
128 MDS codes can be computed in parallel

16.8 cycles/byte on 64-bit Core 2 processor,
21.3 cycles/byte on 32-bit Core 2 processor