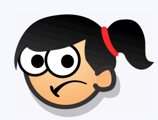
Error Correcting Codes
and
Cryptography

Group 10

Chengze He 

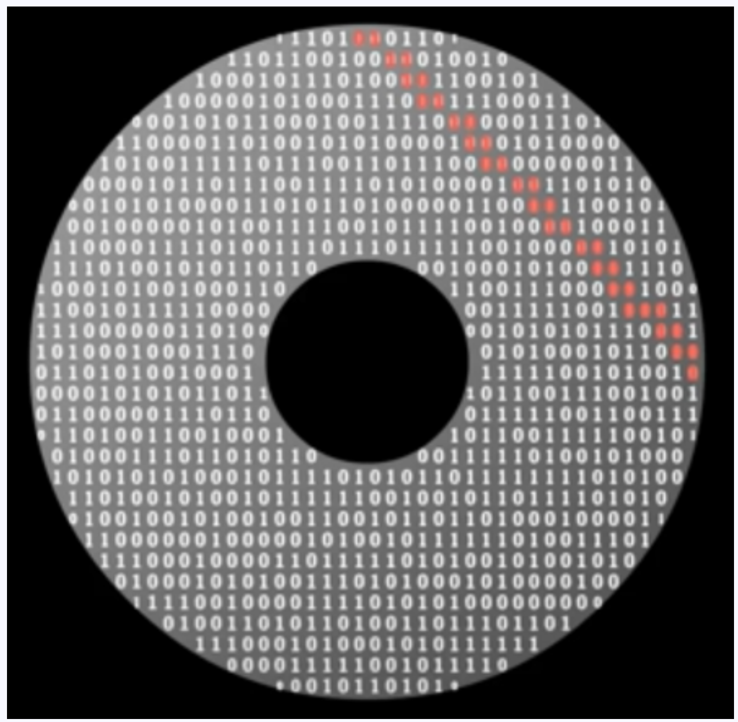
 Qinhang Wu

Yong Li 

 Yuxuan Xia

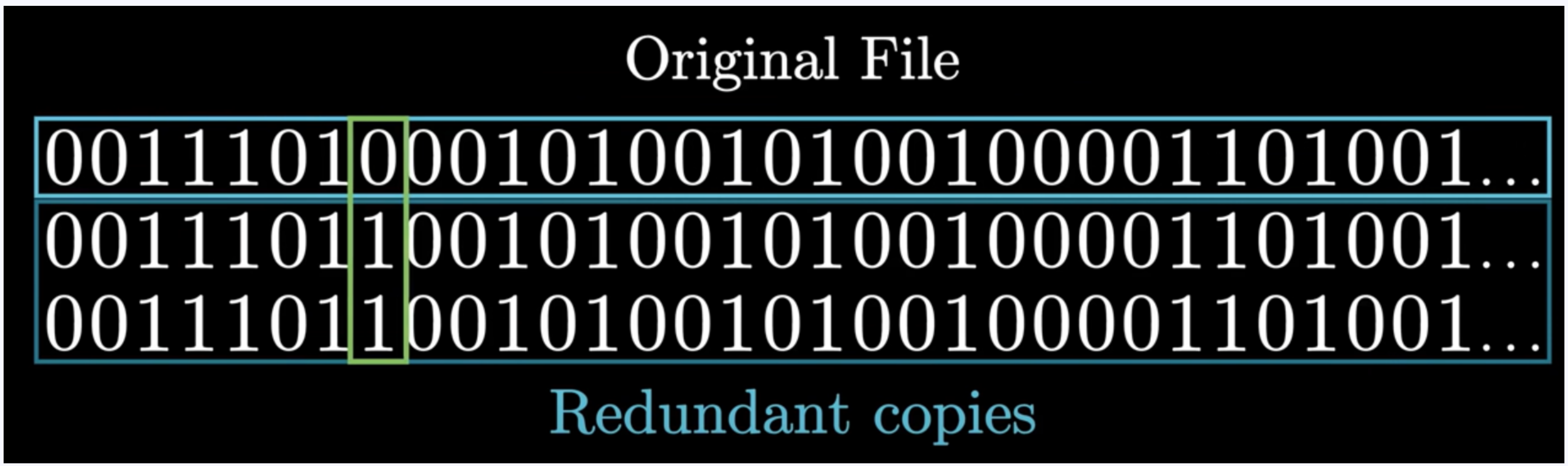
ECC and cryptography Part I

Qinhang Wu



Intro. to Error Correcting Code

- Preliminary Goal: detect partial error during transmission and correct them as an encoding scheme
- Naïve example: repetition

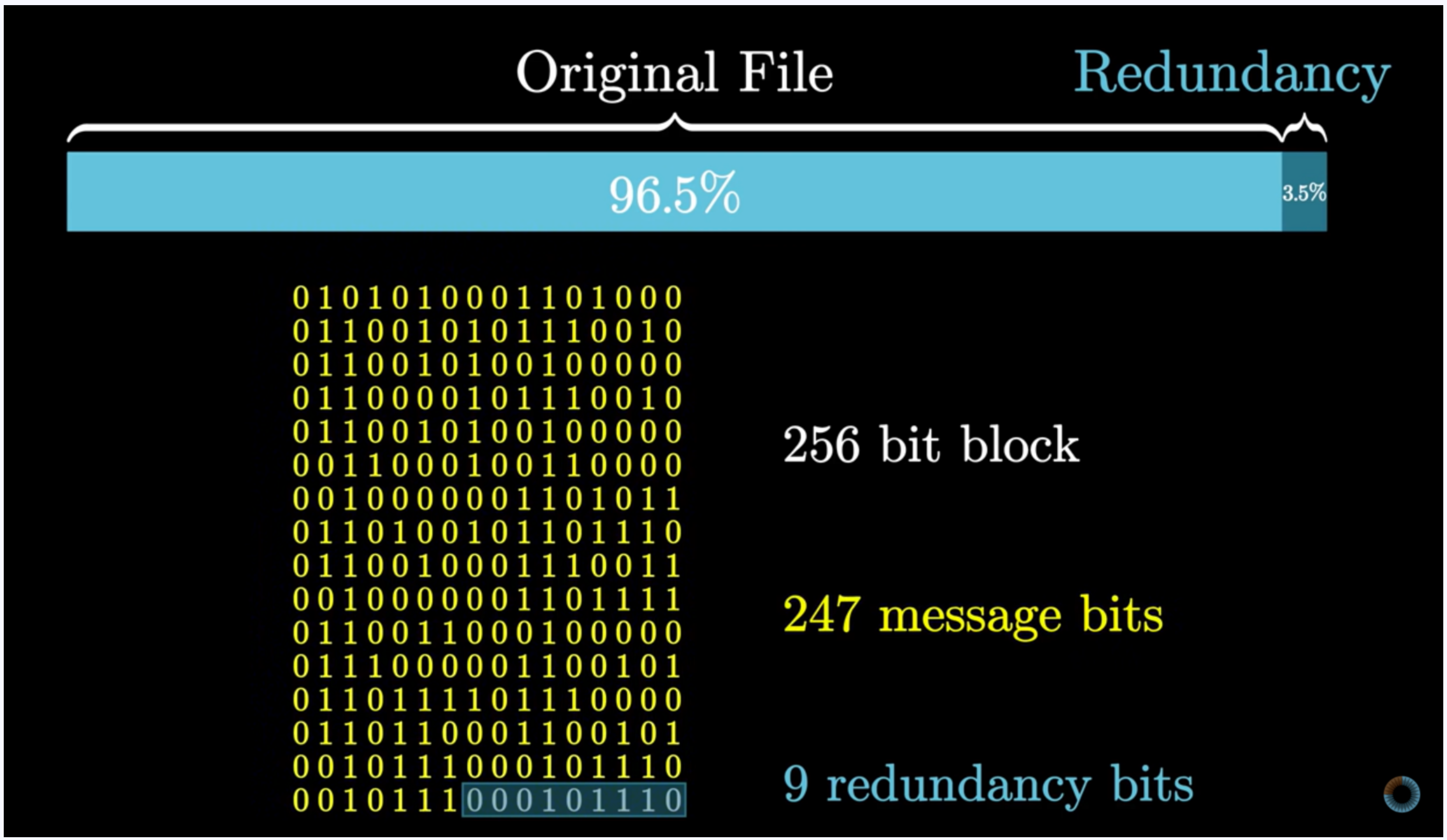


Intro. to Error Correcting Code

- Revised Goal: detect partial error during transmission and correct them as an encoding scheme, while ensuring …
  - 1) **large hamming distance** for code words, and
  - 2) **large transmission rate** for the code
- Hamming Distance: number of positions that two codewords disagree
- Transmission Rate: $\log(M)\ /n$, M as # of possible messages, n as length of each codeword

Intro. to Error Correcting Code

- Parity Checking
- Tradeoff: Redundancy vs. Tolerance



Linear Error Correcting Code

- Hamming Code (1940s)
- Reed-Solomon Code (1960s)
  - Basis of QR Code
- Goppa Code (1970s)
  - McEliece Cryptosystem
- Shor Code (1990s)
  - Quantum error correction

Hamming Code: General Algorithm

- Number the bits starting from 1: bit 1, 2, 3, 4, 5, 6, 7, etc.
- Write the bit numbers in binary: 1, 10, 11, 100, 101, 110, 111, etc.
- All bit positions that are powers of two (have a single 1 bit in the binary form of their position) are parity bits: 1, 2, 4, 8, etc. (1, 10, 100, 1000)
- All other bit positions, with two or more 1 bits in the binary form of their position, are data bits.
- Each data bit is included in a unique set of 2 or more parity bits, as determined by the binary form of its bit position.
- Parity bit 1 covers all bit positions which have the least significant bit set: bit 1 (the parity bit itself), 3, 5, 7, 9, etc.
- Parity bit 2 covers all bit positions which have the second least significant bit set: bits 2-3, 6-7, 10-11, etc.
- Parity bit 4 covers all bit positions which have the third least significant bit set: bits 4–7, 12–15, 20–23, etc.
- Parity bit 8 covers all bit positions which have the fourth least significant bit set: bits 8–15, 24–31, 40–47, etc.
- In general each parity bit covers all bits where the bitwise AND of the parity position and the bit position is non-zero.

Hamming Code: an Example

- 4 bits for redundancy, 1 extra parity bit on the top

			1
	0	1	0
	0	1	0
1	0	0	1

	0		1
	0	1	0
	0	1	0
1	0	0	1

	0	0	1
	0	1	0
	0	1	0
1	0	0	1

	0	0	1
1	0	1	0
	0	1	0
1	0	0	1

	0	0	1
1	0	1	0
1	0	1	0
1	0	0	1

Hamming Code: an Example

- 4 bits for redundancy, 1 extra parity bit on the top

			1
	0	1	0
	0	1	0
1	0	0	1

1	0	0	1
1	0	1	0
1	0	1	0
1	0	0	1

Hamming Code: an Example

- 4 bits for redundancy, 1 extra parity bit on the top

1	0	0	1
1	0	1	0
1	0	1	0
1	0	0	1

noise $\longrightarrow$

1	0	0	1
1	0	1	1
1	0	1	0
1	0	0	1

Hamming Code: an Example

- 4 bits for redundancy, 1 extra parity bit on the top

1	0	0	1
1	0	1	1
1	0	1	0
1	0	0	1

1	0	0	1
1	0	1	1
1	0	1	0
1	0	0	1

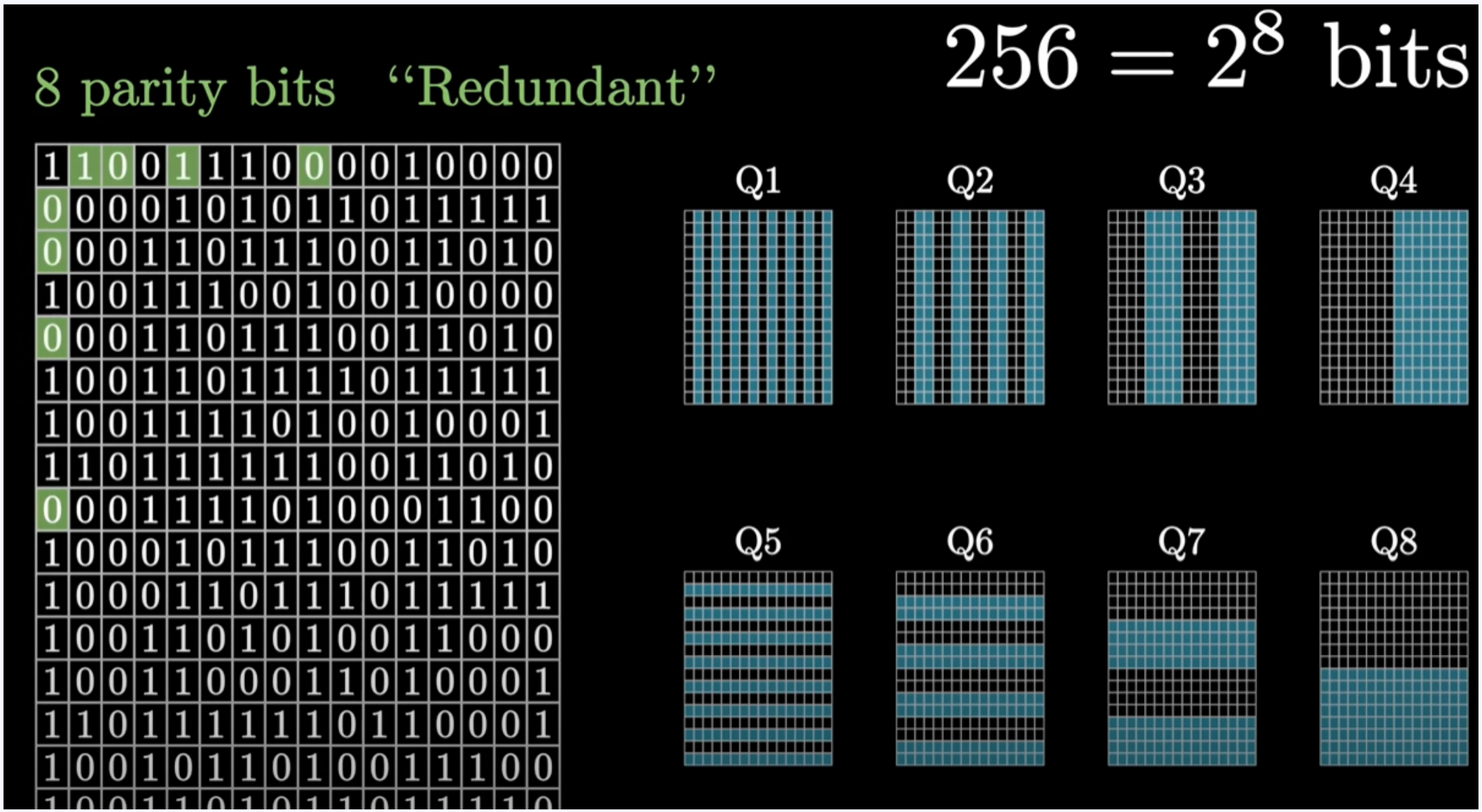
1	0	0	1
1	0	1	1
1	0	1	0
1	0	0	1

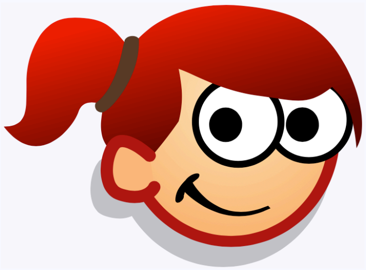
1	0	0	1
1	0	1	1
1	0	1	0
1	0	0	1

1	0	0	1
1	0	1	1
1	0	1	0
1	0	0	1

Hamming Code: an Example

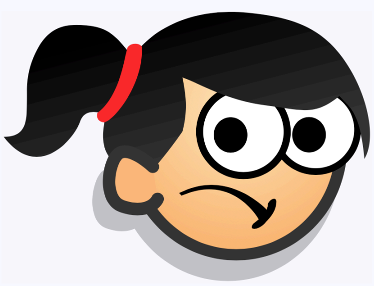
- Extended to 2^8 bits





ECC and cryptography Part II

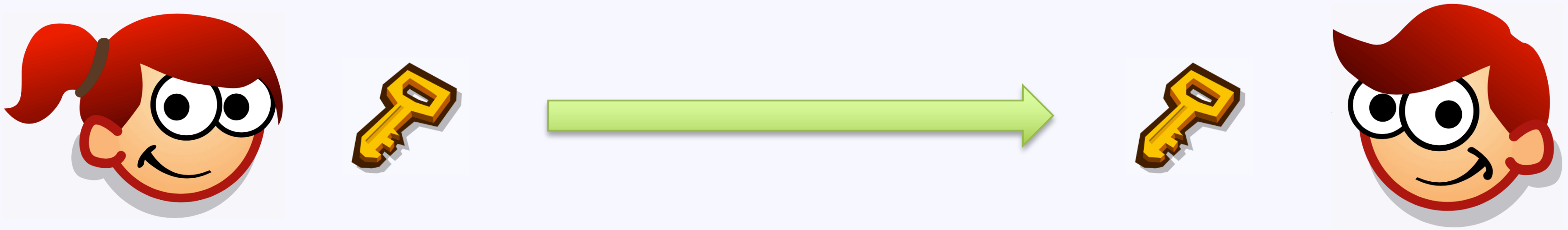
Chengze He



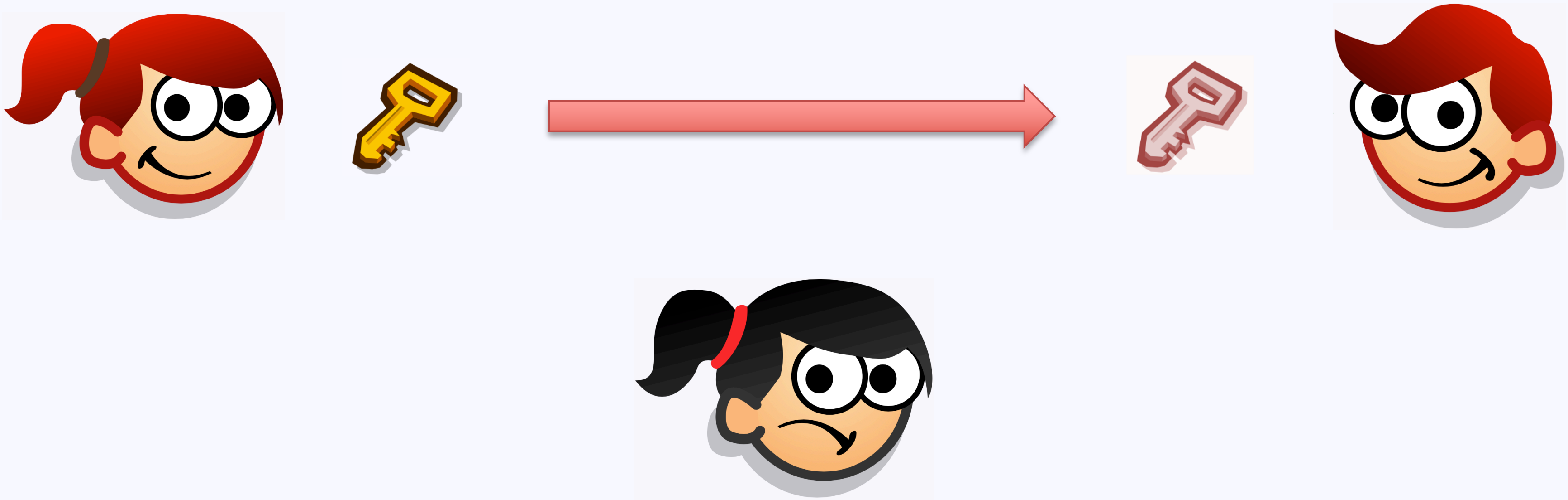
Applications of ECC in cryptography

- Quantum cryptography
- Prevent corruption of encrypted messages
  - Parity check in DES keys
- Cryptosystems based on ECC designs
  - McEliece cryptosystem
  - Neiderreiter cryptosystem

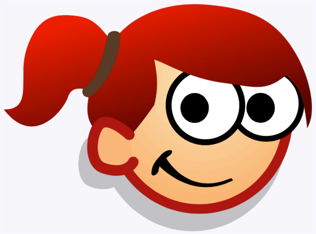
Quantum key distribution



Quantum key distribution



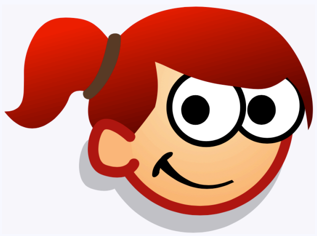
Corruption prevention



We have too much homework for VE475!

We have too much homework for VE475!

Corruption prevention

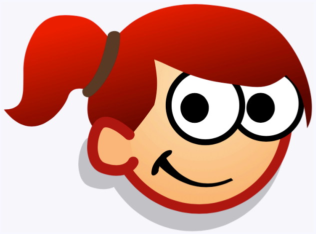


We have too much homework for VE475!

noise

We have too much hlcework for VE475!

Corruption prevention



We have too much homework for VE475!

encryption

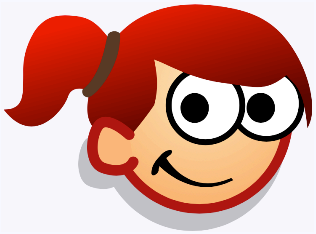
942dd7970986c7a3ae34a3c071f6c5678936cbc605bd02b57004da5631a70b0
49b64154d4e9feee232bc4713b1ac0a8f97e9b4fbe6d7f7f4808a3f17201debcd

942dd7970986c7a3ae34a3c071f6c5678936cbc605bd02b57004da5631a70b0
49b64154d4e9feee232bc4713b1ac0a8f97e9b4fbe6d7f7f4808a3f17201debcd

decryption

We have too much homework for VE475!

Corruption prevention



We have too much homework for VE475!

encryption

942dd7970986c7a3ae34a3c071f6c5678936cbc605bd02b57004da5631a70b0
49b64154d4e9feee232bc4713b1ac0a8f97e9b4fbe6d7f7f4808a3f17201debcd

noise

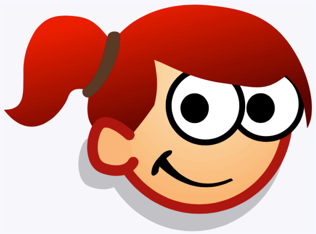
can be fixed using ECC

942dd7970986c7a3ae34a3c071f6c5678936abc605bd02b57004da5631a70b0
49b64154d4e9feee232bc4713b1ac0a8f97e9b4fbe6d7f7f4808a3f17201debcd

decryption

C_]ﺗ͂zynpa~q6ﻫhb

Making use of “noise”?



We have too much homework for VE475!

encryption

942dd7970986c7a3ae34a3c071f6c5678936cbc605bd02b57004da5631a70b0
49b64154d4e9feee232bc4713b1ac0a8f97e9b4fbe6d7f7f4808a3f17201debcd

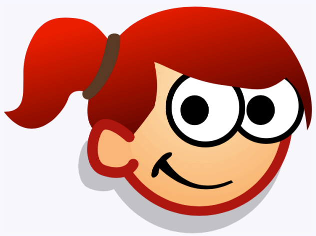
noise

942dd7970986c7a3ae34a3c071f6c5678936abc605bd02b57004da5631a70b0
49b64154d4e9feee232bc4713b1ac0a8f97e9b4fbe6d7f7f4808a3f17201debcd

decryption

C_]ؿzynpa~q6وِhb

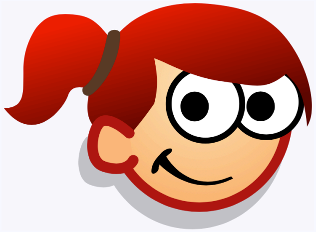
Building a ECC-based cryptosystem



Agree on one ECC scheme

- Introduce artificial noise when encrypting
- Combine encryption and disturbance

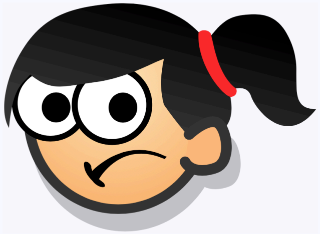
Artificial noise



We have too much homework for VE475!

encryption

942dd7970986c7a3ae34a3c071f6c5678936abc605bd02b57004da5631a70b0
49b64154d4e9feee232bc4713b1ac0a8f97e9b4fbe6d7f7f4808a3f17201debcd



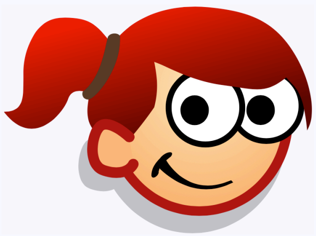
fix

942dd7970986c7a3ae34a3c071f6c5678936cbc605bd02b57004da5631a70b0
49b64154d4e9feee232bc4713b1ac0a8f97e9b4fbe6d7f7f4808a3f17201debcd

decryption

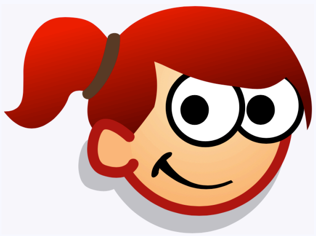
We have too much homework for VE475!

Building a ECC-based cryptosystem



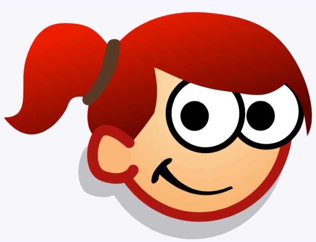
Agree on one ECC scheme

ECC-based public key infrastructure: (Simplified) McEliece cryptosystem



Encoding matrix E
Decoding function D, $D(mE + z) = m$ if z is "small"
Random matrix W
Private key $X = \langle D, W^{-1} \rangle$

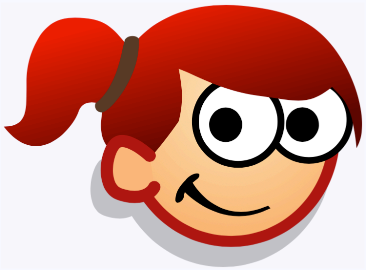
Public key $F = EW$ from Alice
Message m
"small" random noise z
Encryption: $c = mF + z$



Ciphertext c from Bob
Decryption: $D(cW^{-1}) = D((mEW + z)W^{-1}) =$
$D(mEWW^{-1} + zW^{-1}) = D(mE + z') = m$

(Simplified) McEliece cryptosystem

- Randomness in the ciphertexts
  - Encrypting the same message yields different ciphertexts
- Eve can infer neither D nor W^{-1} from F
- Only Alice can correct the errors
  - Eve cannot locate the errors (consider the One Time Pad)
  - Eve does not know the decoding algorithm
- Randomness is important



Thank you