Breaking Pairing-based Cryptosystems using η_T Pairing over GF(3^{97})

Takuya Hayashi†, Takeshi Shimoyama‡
Naoyuki Shinohara*, Tsuyoshi Takagi†

†Kyushu University
‡FUJITSU LABORATORIES Ltd.
*National Institute of Information and Communications Technology

e-mail: t-hayashi@math.kyushu-u.ac.jp

Fujitsu Laboratories, NICT and Kyushu University Achieve World Record Cryptanalysis of Next-Generation Cryptography

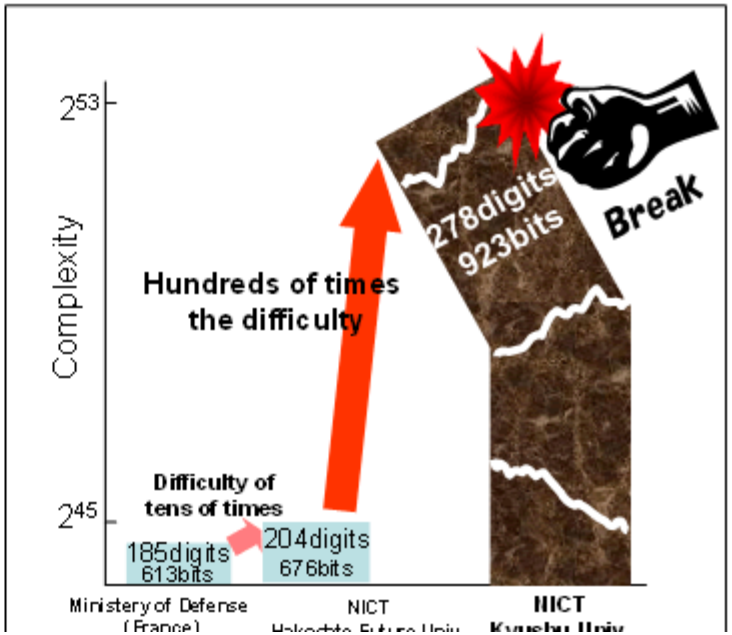
Establishes security of pairing-based cryptography and contributes to its standardization as the next-generation cryptography

June 18, 2012 — Fujitsu Laboratories Limited(1), National Institute of Information and Communications Technology (NICT)(2) and Kyushu University(3) jointly broke a world cryptography record with the successful cryptanalysis of a 278-digit (923-bit)-long pairing-based cryptography(4), which is now becoming the next generation cryptography standard.

Until now, cryptanalysis of pairing-based cryptography of this length was thought impossible as it was estimated to take several hundred thousand years to break. Indeed, despite numerous efforts to use and spread this cryptography at the development stage, it wasn't until this new way of approaching the problem was applied that it was proven that pairing-based cryptography of this length was fragile and could actually be broken in 148.2 days. This result is used as the basis of selecting secure encryption technology, and is proving useful in the standardization of next-generation cryptography in electronic government systems in Japan and international standardization organizations.

Background

Many cryptography systems are used from the viewpoint of information security on a modern information system. Recently, much attention has been paid to the new "pairing-based" cryptography system, which is being standardized as a next-generation encryption system. The technology is attractive as it can be used for various useful applications such as "Identity-based encryption(5)", "keyword searchable encryption(6)", and "functional encryption(7)", which were impossible using previous public key cryptography(8).



Technological Issues

As cryptanalytic techniques and computers become more advanced, cryptanalytic speed accelerates, and conversely, cryptographic

Fujitsu Laboratories, NICT and Kyushu University Achieve World Record Cryptanalysis of Next-Generation Cryptography

Estab… …tography and contributes to its standardization as the next-

PBC has vulnerability!

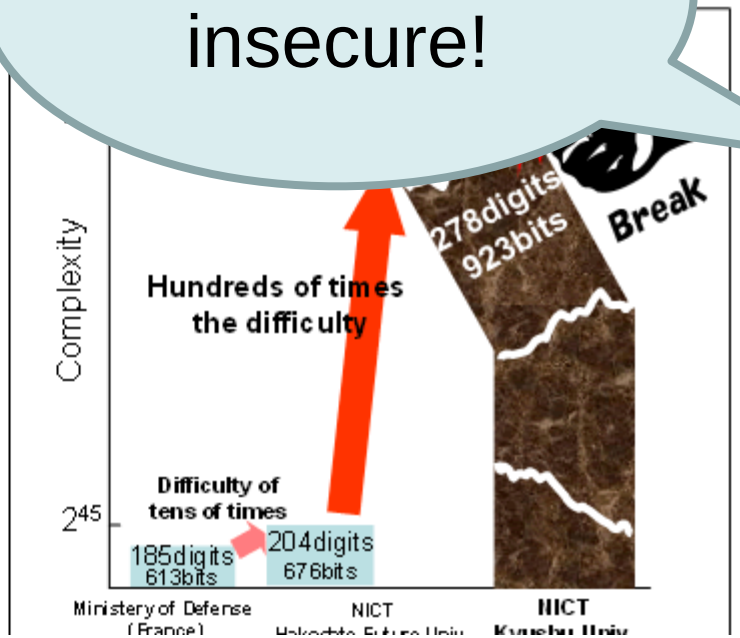
…e of Information and Communications Technology (NICT)[(2)] and …h the successful cryptanalysis of a 278-digit (923-bit)-long pairing-…ation cryptography standard.

…phy of this length was thought impossible as it was estimated to take several hundred thousand years to break. Indeed, despite numerous efforts to use and spread this cryptography at the development stage, it wasn't until this new way of approaching the problem was applied that it was proven t… …f this length was fragile and could actually be broken in 148.2 days. This result is used as the … …and is proving useful in the standardization of next-generation cryptography in el… standardization organizations.

PBC is insecure!

Background

Many cryptography systems are used from the viewpoint of information security on a modern information system. Recently, much attention has been paid to the new "pairing-based" cryptography system, which is being standardized as a next-generation encryption system. The technology is attractive as it can be used for various useful applications such as "Identity-based encryption[(5)]", "keyword searchable encryption[(6)]", and "functional encryption[(7)]", which were impossible using previous public key cryptography[(8)].



Technological Issues

As cryptanalytic techniques and computers become more advanced, cryptanalytic speed accelerates, and conversely, cryptographic

Fujitsu Laboratories, NICT and Kyushu University Achieve World Record Cryptanalysis of Next-Generation Cryptography

Estab… …tography and contributes to its standardization as the next-

PBC has vulnerability!

…e of Information and Communications Technology (NICT)[(2)] and …h the successful cryptanalysis of a 278-digit (923-bit)-long pairing-…ation cryptography standard.

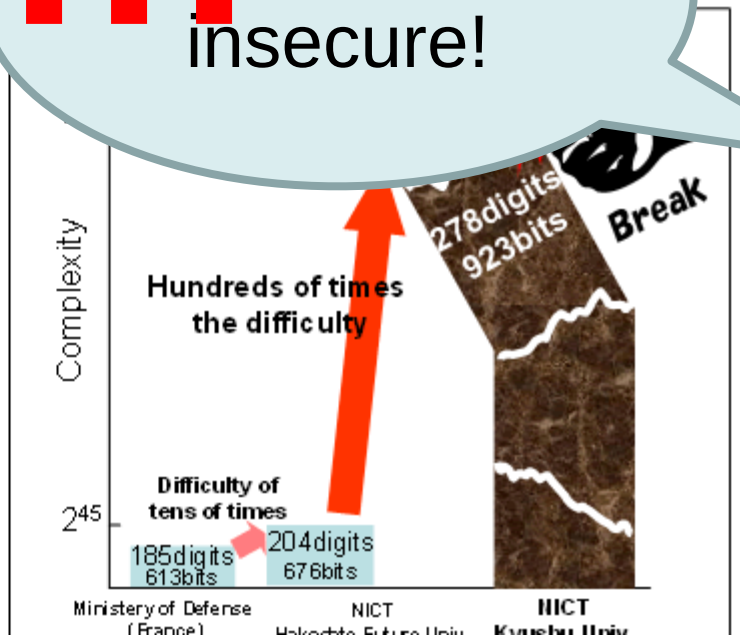
…phy of this length was thought impossible as it was estimated to take several hundred thousand years to break. Indeed, despite numerous efforts to use and spread this cryptography at the development stage, it wasn't until this new way of approaching the problem was applied that it was proven t… …f this length was fragile and could actually be broken in 1… …days. …is re… …d as t… …and is proving useful in the standardization of n… …gener…n c…tography …el… standardization organizations.

NO!!!

PBC is insecure!

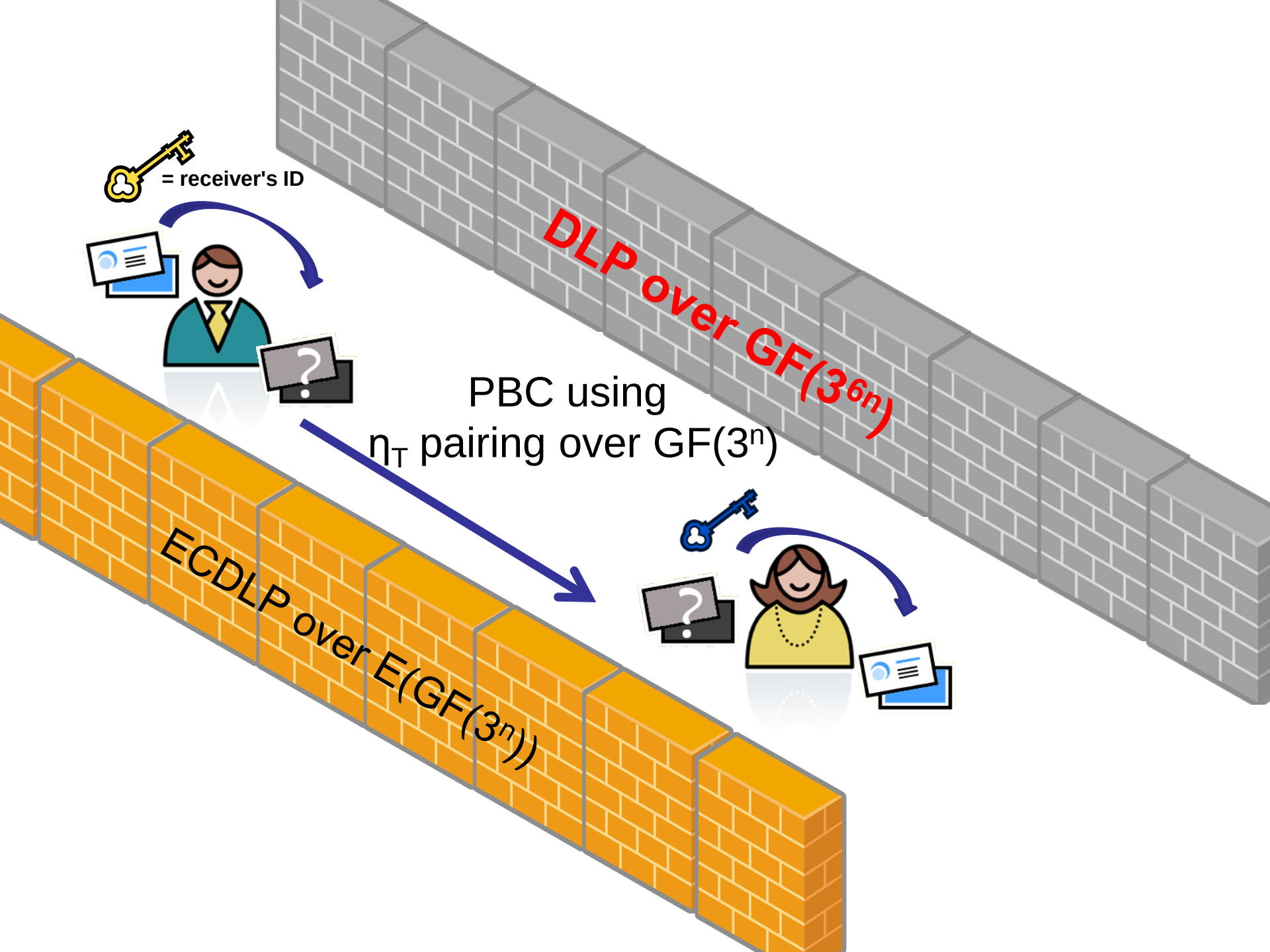
Background

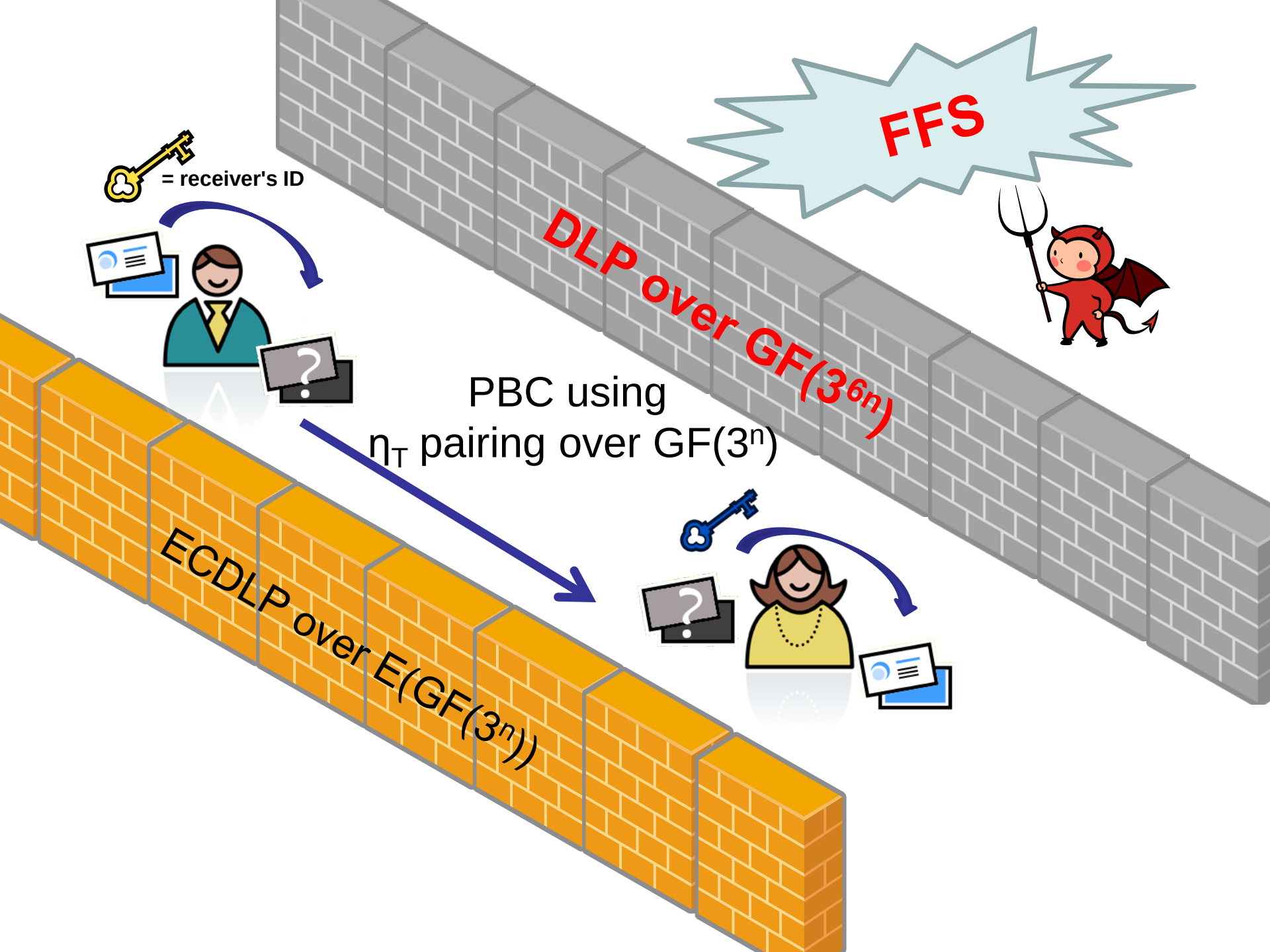
Many cryptography systems are used from the viewpoint of information security on a modern information system. Recently, much attention has been paid to the new "pairing-based" cryptography system, which is being standardized as a next-generation encryption system. The technology is attractive as it can be used for various useful applications such as "Identity-based encryption[(5)]", "keyword searchable encryption[(6)]", and "functional encryption[(7)]", which were impossible using previous public key cryptography[(8)].

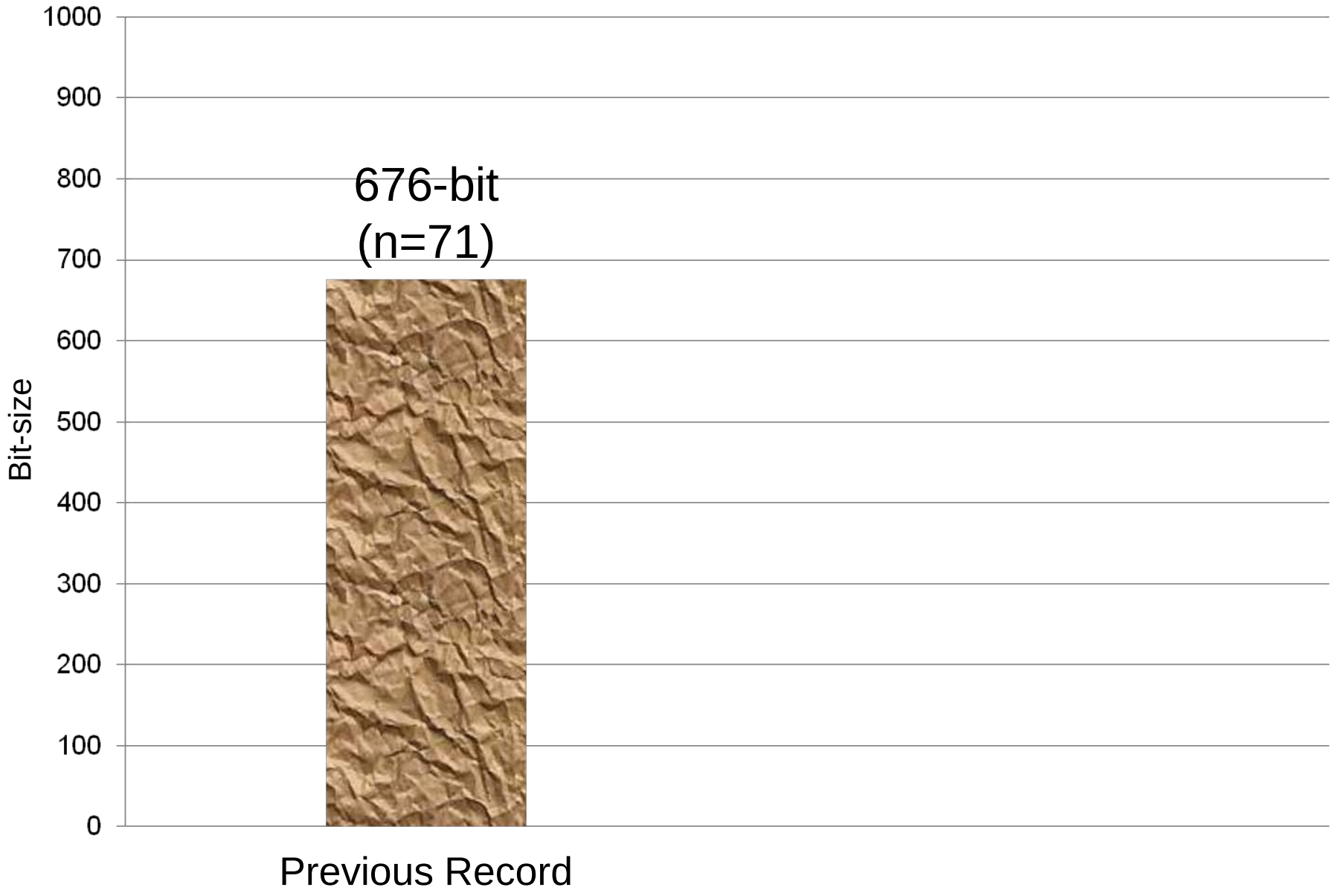


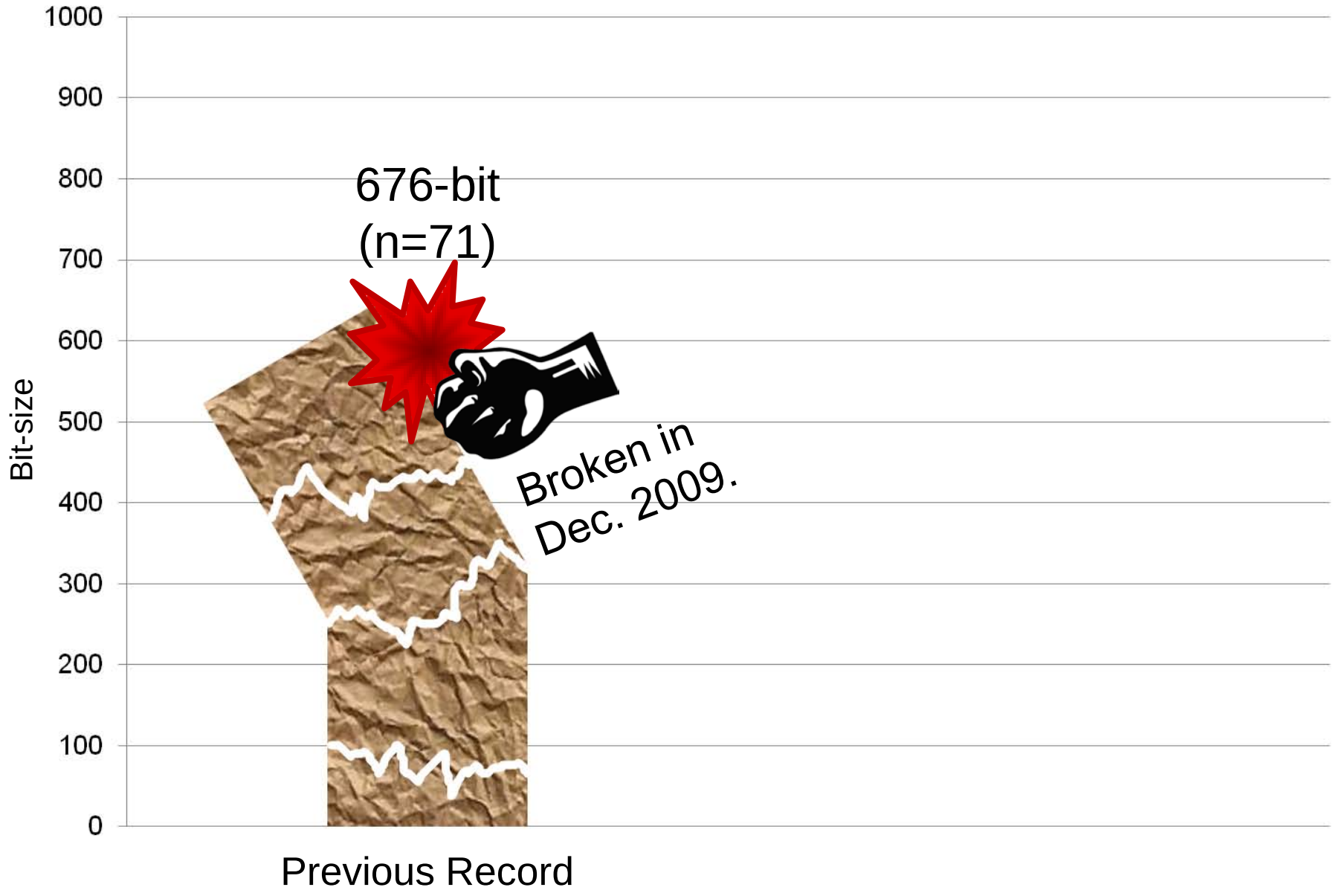
Technological Issues

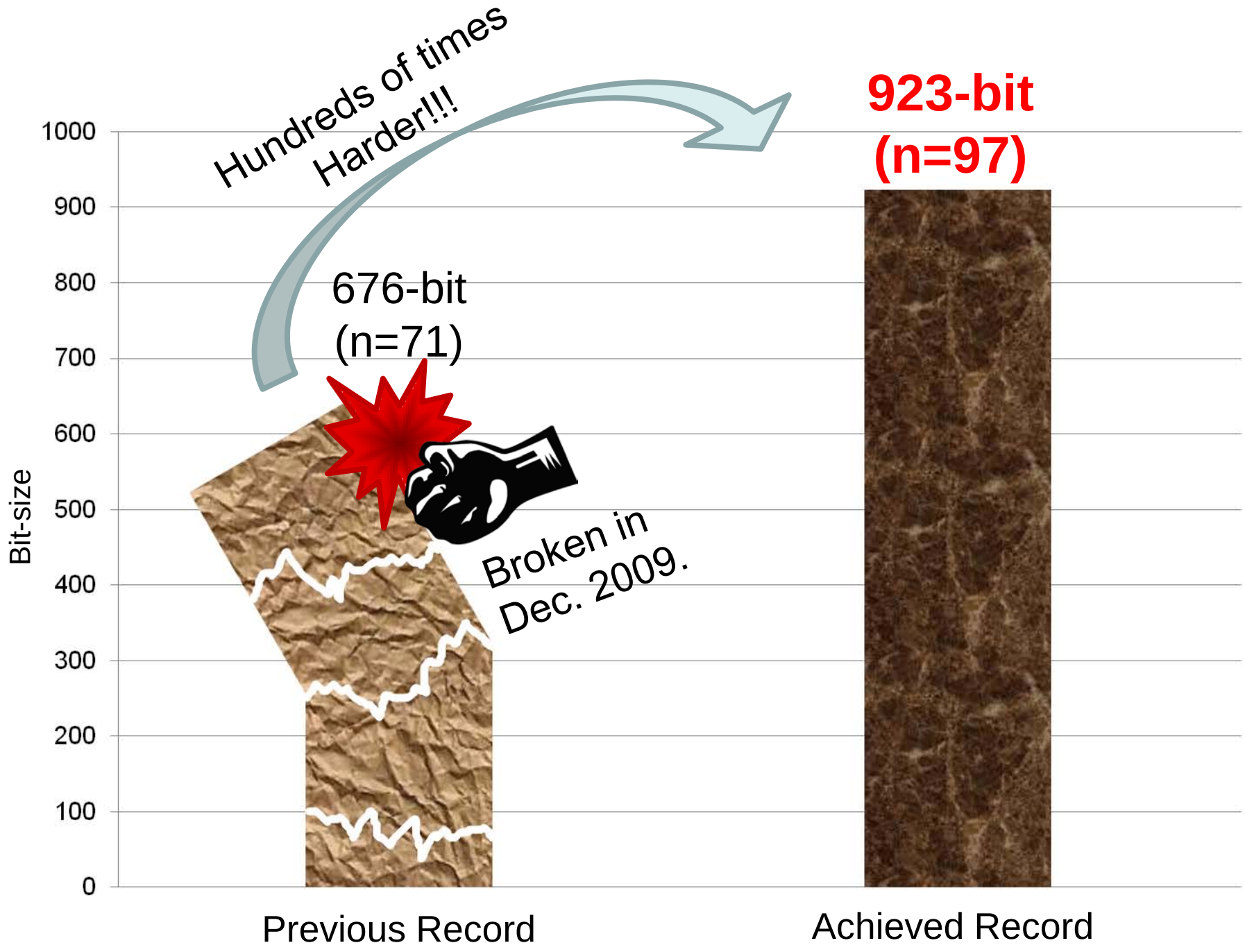
As cryptanalytic techniques and computers become more advanced, cryptanalytic speed accelerates, and conversely, cryptographic

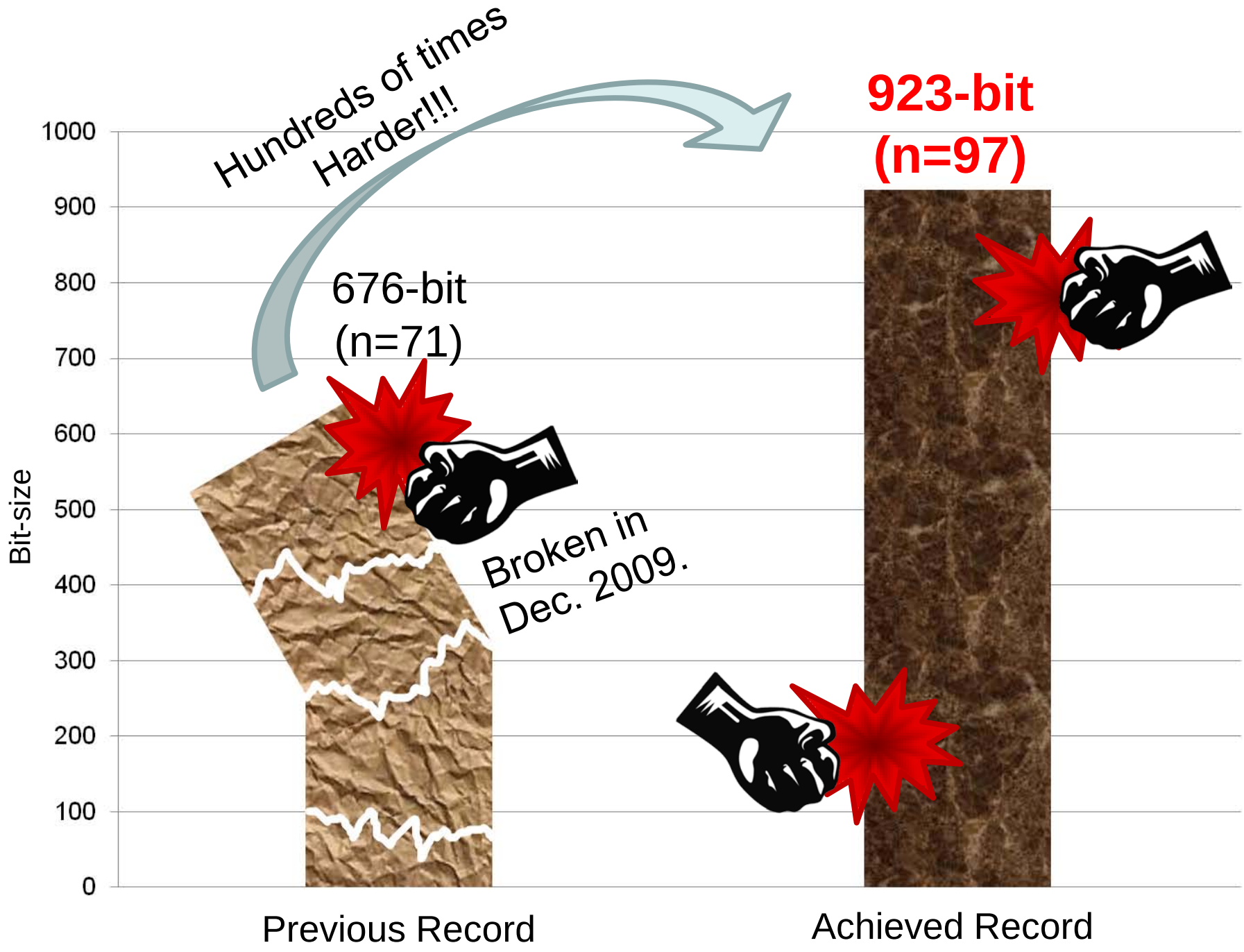

= receiver's ID
DLP over GF(3^6n)
PBC using
η_T pairing over GF(3^n)
ECDLP over E(GF(3^n))

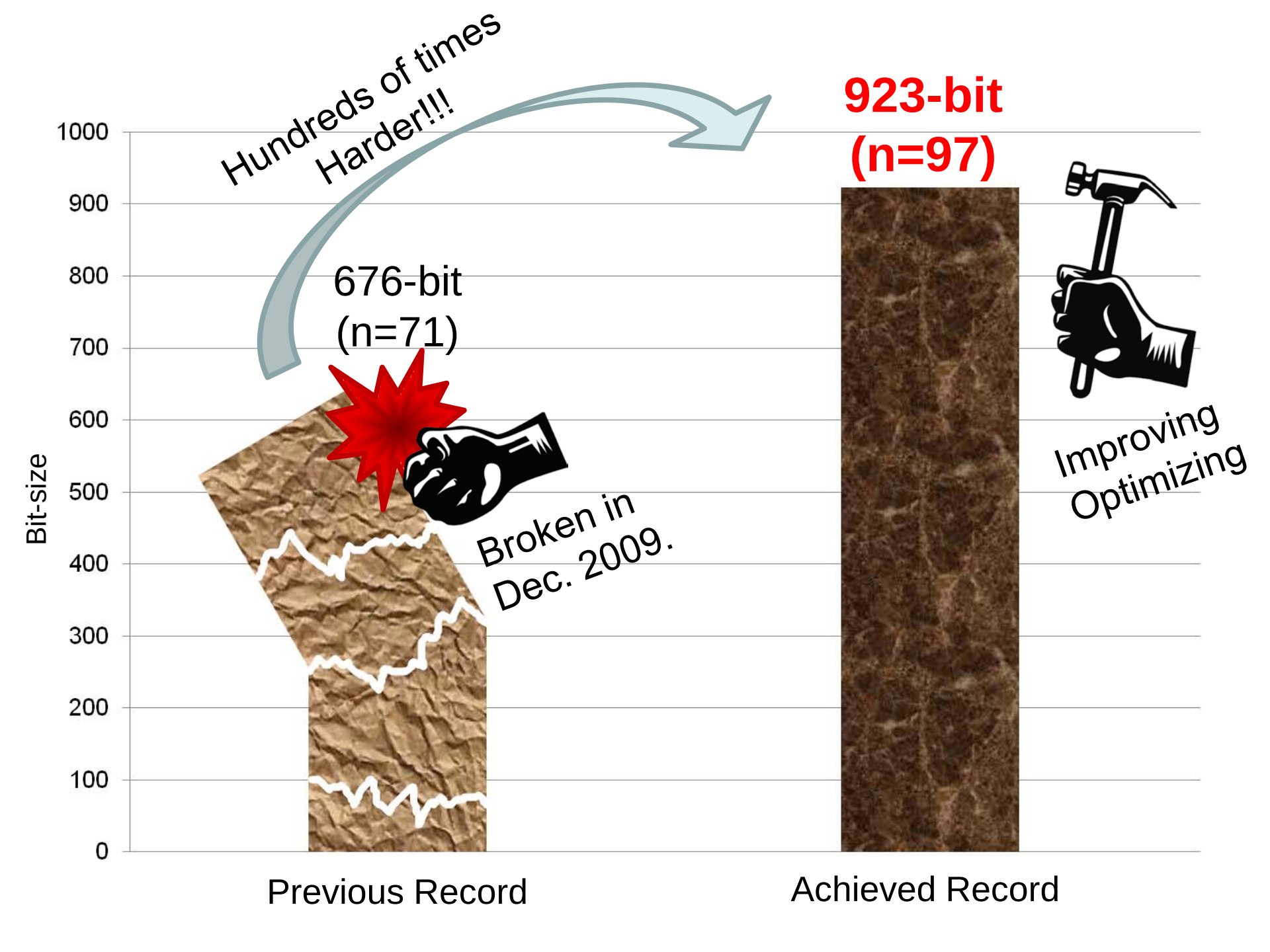

FFS
DLP over GF(3^6n)
= receiver's ID
PBC using
η_T pairing over GF(3^n)
ECDLP over E(GF(3^n))

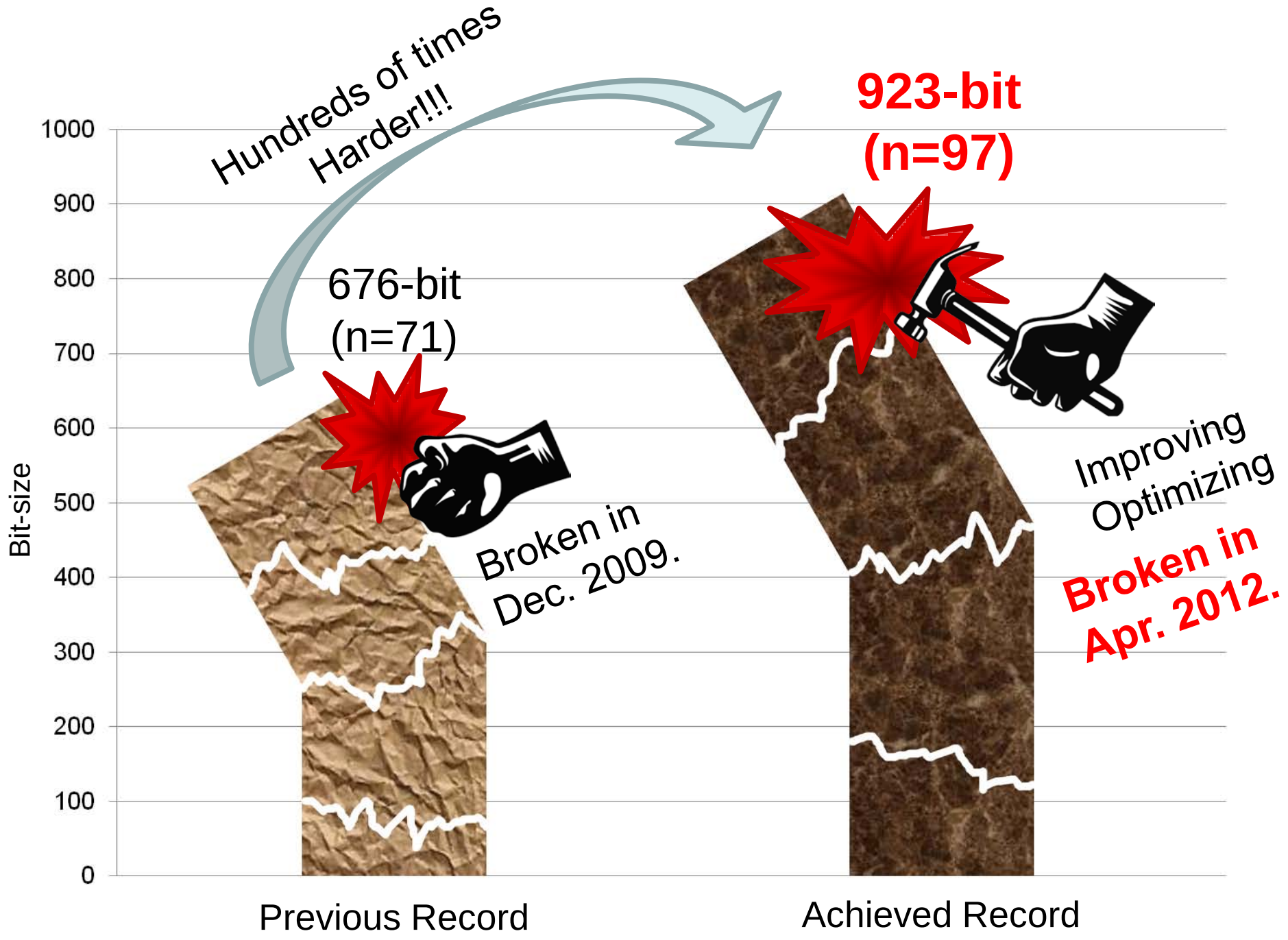

1000
900
800
700
600
500
400
300
200
100
0
Bit-size
676-bit
(n=71)
Previous Record


1000
900
800
700
600
500
400
300
200
100
0
Bit-size
676-bit
(n=71)
Broken in
Dec. 2009.
Previous Record


Hundreds of times Harder!!!
923-bit
(n=97)
676-bit
(n=71)
Broken in
Dec. 2009.
Bit-size
1000
900
800
700
600
500
400
300
200
100
0
Previous Record
Achieved Record


Hundreds of times Harder!!!
923-bit (n=97)
676-bit (n=71)
Broken in Dec. 2009.
Bit-size
1000
900
800
700
600
500
400
300
200
100
0
Previous Record
Achieved Record


Hundreds of times
Harder!!!
923-bit
(n=97)
676-bit
(n=71)
Broken in
Dec. 2009.
Improving
Optimizing
Bit-size
1000
900
800
700
600
500
400
300
200
100
0
Previous Record
Achieved Record


Hundreds of times Harder!!!
923-bit (n=97)
676-bit (n=71)
Broken in Dec. 2009.
Improving Optimizing
Broken in Apr. 2012.
Bit-size
1000
900
800
700
600
500
400
300
200
100
0
Previous Record
Achieved Record

Improvements

- Parameter optimization
- Lattice sieve for JL06-FFS
- SIMD implementation
- Large prime variation
- Omitting sieving for tiny primes
- Fast sieving for factor base of specific degree
- Tau-adic structure
- Overlapping communication and computation
- etc…

Results

Phase	Algorithm	Time	Environment
Collecting Relations	Lattice Sieve	53.1 days	212 CPU cores
Linear Algebra	Parallel Lanczos Method	80.1 days	252 CPU cores
Individual Log	Rationalization and Special-Q Descent	15.0 days	168 CPU cores
Total		**148.2 days**	**252 CPU cores**

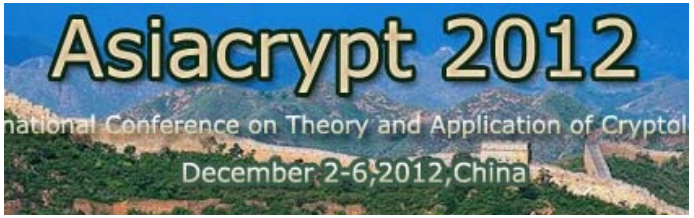
Concluding Remarks

- We can break PBC using η_T pairing over GF(3^{97}) in 148.2 days using 252 CPU cores.
- We estimate:
  - n = 193: 82-bit security level
  - n = 509: 121-bit security level

- I'll talk more details at

  ECC 2012, México, Querétaro

  Asiacrypt 2012, China, Beijing



Thank you for your attention!